



Archivos electrónicos.  
Textos y contextos

Alicia Barnard Amozorrutia

Coordinadora







Red Nacional de Archivos de  
Instituciones de Educación Superior



Archivo Histórico  
BUAP

Archivos electrónicos.  
Textos y contextos

Alicia Barnard Amozorrutia  
Coordinadora

Serie Formación Archivística

*Rector de la Benemérita Universidad Autónoma de Puebla,*  
Enrique Agüera Ibáñez

*Directora del Archivo Histórico Universitario,*  
Georgina Maldonado Lima

*Director de la Serie Formación Archivística,*  
Cuidado y revisión de la obra  
Gustavo Villanueva Bazán

*Diseño*  
Armando López Vázquez

Primera Edición  
© Benemérita Universidad Autónoma de Puebla.  
Archivo Histórico Universitario  
Reforma 531  
Centro Histórico  
Tel: 2327479  
e-mail: tiempo@siu.buap.mx  
ISBN 978-607-487-259-0  
Impreso y hecho en México  
*Printed and made in Mexico*

# Presentación

En el entorno de los países hispanoparlantes los temas sobre archivos electrónicos o digitales aún causan inquietud e incertidumbre, inclusive hasta resistencia por parte de archivistas y otros profesionales que tienen bajo su responsabilidad coordinar e instrumentar procesos para la organización y conservación de archivos. Esto no es de extrañar, por lo general el profesional de los archivos no tiene acceso al control y manejo de archivos electrónicos o digitales ya que los mismos pueden encontrarse en las computadoras personales de funcionarios o en los servidores de las instituciones, donde la práctica archivística aún no se ve como una disciplina útil para su manejo y organización. Acaso, cuando no se sabe qué hacer con estos materiales una vez que se acumulan en las oficinas, es cuando se llama al archivista a fin de darlos de baja o exigir que se transfieran a un archivo histórico. Es este uno de los momentos donde aparecen deficiencias, tanto de las instituciones como de los profesionales de la archivística. Por un lado y con seguridad, no existe una política, norma o lineamiento sobre el manejo de este tipo de archivos; por el otro, el archivista aún carece del conocimiento para hacerse cargo de los mismos. En ocasiones, cuando los archivos electrónicos en soportes como diskettes, discos compactos, cintas magnéticas, etc., se llegan a conservar en un archivo histórico uno se preguntará ¿son auténticos?, ¿es posible recuperar la información tal y como fue escrita la primera vez? ¿se tiene información acerca de los contextos donde este tipo de documentos fueron elaborados? Además, ¿se pueden leer? ¿se cuenta con los

recursos tecnológicos y financieros suficientes para su preservación en el largo plazo? Estas y muchas más preguntas han obligado a expertos a impulsar investigaciones para la creación, manejo, uso y preservación de archivos electrónicos/digitales.

El conocimiento sobre la materia tiene principalmente su origen en los países de habla inglesa por lo que aún no existe suficiente literatura sobre el tema en español. Ante ello y con el propósito de abordar desde diferentes perspectivas aspectos relacionados con los archivos electrónicos o digitales, es que nos dimos a la tarea de invitar a reconocidos profesores, investigadores, profesionales y técnicos involucrados en su estudio a escribir un texto para esta obra, y son ellos quienes con gran generosidad aceptaron, y con sus contribuciones hicieron posible la publicación de *Archivos Electrónicos. Textos y Contextos*. Todos los autores, latinoamericanos y de España, por primera vez en una publicación nacional, nos ofrecen sus experiencias y conocimientos sobre este tema, novedoso en nuestro entorno y joven por los años que se llevan en su estudio (no más allá de 25) aunque a la vez antiguo si se le mide en términos de obsolescencia tecnológica. Sin seguir un orden sobre los temas o ubicación en la obra, corresponde ahora hacer una breve introducción a los mismos.

Aida Luz Mendoza Navarro abogada, quien fuera por varios años directora del Archivo General de la Nación del Perú, actualmente investigadora y profesora reconocida, vincula sus conocimientos como abogada y archivista en su texto “La autenticidad del Documento Electrónico Jurídico y Diplomático” en el que hace una revisión sobre la autenticidad en términos jurídicos y de los documentos de archivo desde la perspectiva del análisis diplomático-archivístico propuesto por el Proyecto InterPARES.

Por su parte, Juan Voutssás Marqués Doctor en Bibliotecología, investigador del Centro Universitario de Investigaciones Bibliotecológicas de la UNAM y director del TEAM México del Proyecto InterPARES, quien ha orientado sus estudios a las bibliotecas digitales, a la preservación del patrimonio digital y recientemente a la investigación sobre archivos digitales y su preservación, en su artículo “La Cadena de Preservación en Archivos Digitales” hace una revisión sobre los riesgos y pérdida de documentos electrónicos y establece los factores que inciden en la preservación digital, revisa iniciativas para la preservación de

documentos digitales y describe el Modelo de la Cadena de Preservación del Proyecto InterPARES.

En el texto “Transfiriendo documentos electrónicos auténticos hacia un repositorio digital seguro: el caso catalán (la plataforma iArxiu)” Ramón Nualart responsable del servicio iArxiu de Cataluña y Miquel Serra, archivista de la Universidad de Girona y Director del TEAM Catalonia del Proyecto InterPARES, ambos destacados profesionales en el campo de los archivos electrónicos, abordan en primer término, aspectos teóricos y prácticos relacionados con la transferencia de archivos electrónicos auténticos para su preservación en el largo plazo, y más adelante nos ofrecen aspectos relacionados con la plataforma iArxiu de archivo electrónico y preservación digital de documentación electrónica para administraciones públicas en Cataluña.

Por lo que respecta al texto “El Documento Electrónico en la E-Administración: análisis de caso” de Carlos Alberto Zapata, profesor, investigador de la Universidad de la Salle en Colombia y Codirector del TEAM Colombia del Proyecto InterPARES, a partir de un estudio realizado por el Archivo General de la Nación de Colombia, cuyos resultados previstos respecto de los servicios tecnológicos en las oficinas gubernamentales y la carencia de políticas y disposiciones para la gestión del documento electrónico, se plantea cuestiones relativas a la gestión de documentos electrónicos y la administración pública, la administración electrónica y la gestión documental así como los avances logrados en la gestión de documentos en el gobierno electrónico de Bogotá. Concluye con recomendaciones para integrar la gestión de documentos electrónicos en la administración pública.

Alejandro Delgado del Ayuntamiento de Cartagena, España, destacado profesional de los archivos electrónicos, quien además ha dedicado esfuerzos importantes para divulgar el conocimiento sobre este tema como traductor de obras y artículos de autores relevantes del habla inglesa, en su texto “El Archivero Electrónico en el País de Nunca Jamás” describe en primer lugar el escenario del entorno de producción de documentos actual o en fase de desarrollo en el Ayuntamiento. En segundo lugar describe la solución de gestión de documentos y de archivo electrónico propuesta, así como los mecanismos de integración



con el entorno de producción. Por último ofrece algunas conclusiones derivadas de este proyecto para archivos electrónicos.

Alicia Barnard, participante del TEAM México del Proyecto InterPARES en su artículo “La valoración documental. De los archivos en papel a los archivos digitales” brinda un panorama general acerca del controvertido proceso de valoración documental a partir de las propuestas de principios de siglo XX en cuanto a archivos en papel, para concluir con los planteamientos para la preservación de archivos digitales del proyecto InterPARES y con ciertas conclusiones sobre riesgos que conlleva la falta de estrategias para determinar el destino final de los archivos digitales.

El lector cuenta en esta obra con principios teóricos y prácticos acerca de los archivos electrónicos o digitales. La variedad de los temas ofrece una perspectiva amplia y valiosa para conocer más acerca de los mismos y a la vez se espera que *Archivos Electrónicos. Textos y Contextos* no sea la única publicación sobre el tema sino que sirva de arranque de otras más.

Alicia Barnard Amozorrutia

---

Aída Luz Mendoza

---

**La autenticidad** del documento electrónico  
en los ámbitos jurídico y diplomático

---

# Navarro

Abogada y Magíster en Gestión de Políticas Públicas, consultora y capacitadora en archivos para entidades públicas y privadas. Autora de libros y artículos publicados en ediciones especializadas nacionales y extranjeras.  
Coordinadora de la Carrera Profesional de Archivística y Gestión Documental de la Universidad Católica Sedes Sapientiae.

## I. Introducción

La autenticidad del documento ha sido estudiada principalmente por dos áreas del conocimiento: el derecho y la diplomática. En ambos casos los tratadistas, doctrinarios y especialistas han realizado importantes aportes.

Tanto el derecho como la diplomática, tradicionalmente, se han ocupado de la autenticidad del documento en soporte de papel, sin embargo, desde hace un buen tiempo ambas áreas de conocimiento van dirigiendo su atención en torno al documento electrónico. En la misma línea, los archiveros en los últimos años vienen trabajando incansablemente en temas vinculados a los documentos electrónicos, éstos han motivado diversas reuniones de trabajo, congresos, seminarios, foros y otras variantes académicas en diversas partes del mundo.

Un buen número de textos trabajados por destacados archiveros son el resultado de su preocupación por los documentos electrónicos de archivo. En este amplio panorama los estudios se han visto complementados con el aporte de profesionales de áreas de conocimiento afines a la archivística, pero también de aquellos que no están tan cerca de ella. Los aportes cualesquiera sea su procedencia, vienen bien porque refuerzan el uso, preservación y manejo de los documentos electrónicos en las organizaciones públicas y privadas procurando mantener su autenticidad en todo momento.

De todas las áreas involucradas que coadyuvan al mejor uso del documento electrónico de archivo nos centraremos en dos, una de ellas es el derecho, donde se aborda la autenticidad del documento como elemento fundamental de la seguridad jurídica en el ámbito jurisdiccional o administrativo. La otra área de nuestra atención es la diplomática. Esta disciplina desde hace siglos ha contribuido sustancialmente al reconocimiento de la autenticidad del documento determinando las características y requisitos indispensables para las diferentes clases o tipos de documentos. Relativamente más recientes son los valiosos estudios de los especialistas y particularmente de la doctora Luciana Duranti sobre la autenticidad del documento electrónico a partir de la diplomática.

Presentado de este modo el tema que nos ocupa, en las siguientes líneas trataremos de hacer un apretado análisis de la autenticidad desde el punto de vista del derecho y la diplomática y procuraremos llegar a conclusiones que reflejarán nuestra posición respecto del documento electrónico de archivo apoyado por estas dos áreas del conocimiento.

## II. ¿Qué es la autenticidad?

La palabra “autenticidad” proviene del verbo griego “*authentéo*”, que significa tener autoridad, gobernar a alguien y del sustantivo “*authéntés*” el que obra por sí mismo, autor o ejecutor. En latín y ahora en castellano, la palabra significa el autorizado o quien hace fe de algo.

En sentido lato podemos afirmar que un documento es auténtico desde el punto de vista jurídico, cuando existe certeza sobre la persona a quien se le atribuye el haberlo elaborado, manuscrito o firmado, lo que significa que para que no se cuestione su calidad de auténtico debe contener estos requisitos, de lo contrario, jurídicamente la falta de autenticidad conlleva a declarar que el documento carece de valor probatorio.

Guillermo Federico Soria, Jorge Schiavone y Silvia Aletto, hacen el siguiente comentario: “Siguiendo a Núñez Lagos, documento auténtico es ‘aquél que eficazmente establece que su autor real es quien el mismo documento indica como su autor’.

Por su parte Felipe Pedro Villaró establece que desde un punto de vista material, el documento es auténtico cuando el autor indicado en él coincide con el autor real, puesto que si no coincide el documento es falso. Desde un punto de vista formal, la identidad entre el autor real y el indicado resulta del documento mismo.

Llambías refiriéndose al documento público dice que el mismo goza de la presunción de autenticidad que merece la actuación del oficial público interviniente, abonada por su firma y sellos.

Como decía antiguamente Dumoulin ‘*scripta publica probant se ipsa*’, es decir, el instrumento público se prueba por sí mismo.”<sup>1</sup>

<sup>1</sup> SORIA, Guillermo Federico; SCHIAVONE, Jorge, ALETTO, Silvia Anabella, *El principio de autenticidad*, 2003, [http://drhocobar.com/Documentos/\(27\)%20El%20Principio%20de%20Autenticidad.doc](http://drhocobar.com/Documentos/(27)%20El%20Principio%20de%20Autenticidad.doc) [Consulta: 14.12.09].

De las definiciones entregadas por los autores en referencia deducimos que en el ámbito jurídico, tratándose del documento en soporte de papel, el reconocimiento de la autenticidad consiste en comprobar quien lo firmó; luego en la legislación especializada sobre tecnología informática aplicada a los archivos se exige que los documentos gocen de autenticidad y otras características que en promedio se refieren al mismo requisito, agregándose la permanencia de la información, lo que en archivística podemos equiparar a la preservación a largo plazo del documento electrónico.

En la práctica administrativa y jurisdiccional cuando se requiere reconocer la autenticidad de los documentos electrónicos, el procedimiento no se reduce únicamente a demostrarla mediante la firma, en tanto su comprobación no se da solo por la identificación del firmante, sino que, además, deberán concurrir otros elementos que manifiesten, afirmen o permitan confiar en la autenticidad del documento electrónico, como veremos más adelante.

### **III. El acto administrativo**

Para centrarnos en el tema respecto del derecho y la diplomática, necesariamente, debemos referirnos al acto jurídico representado en un documento y para mejor focalizar nuestro propósito advertimos que estaremos ocupándonos del documento de archivo.

Nos situamos en la administración pública donde los actos administrativos para ser válidos deberán observar determinadas formas vigiladas por la administración, en cumplimiento de la legislación especializada que las regula.

Podemos decir que en la administración pública se realizan actos plurilaterales debido a que intervienen muchas voluntades; son actos jurídicos públicos donde participan los administrados que requieren los servicios del Estado, éste los atiende mediante las organizaciones públicas que tienen la responsabilidad, facultad y competencia para asumir su atención en representación del Estado.

### III. 1 El acto jurídico administrativo y la autenticidad

Si bien un documento administrativo para fines de un trámite, inicialmente, no lo concebimos de trascendencia jurídica, éste en algún momento puede constituirse en prueba jurídica y también histórica; entonces no podemos reducir su carácter solo a lo administrativo. Esencialmente el matiz jurídico está presente o latente en todo documento que se produzca en la gestión pública, más aun cuando sabemos que surge como resultado del ejercicio de las funciones oficiales encargadas a los funcionarios públicos en representación del Estado al servicio de los administrados; en consecuencia, cada acto administrativo siempre estará revestido del factor jurídico que lo regula. Podemos agregar que también es coincidente con su carácter archivístico.

De todos los documentos que se producen en la gestión pública algunos llegan a la categoría de históricos, lo que no significa que en ese estado los documentos pierden sus valores, por el contrario éstos se reafirman debido a que son concomitantes con él durante todo su ciclo vital.

La administración pública se desenvuelve realizando una serie de actos según las funciones asignadas a cada organismo y funcionario públicos, éstos específicamente denominados actos administrativos siguen siendo jurídicos. Cualquier decisión de un funcionario está respaldada por la ley, entonces, sus decisiones son válidas para sustentar los derechos y obligaciones de la administración y de los administrados.

Las potestades administrativas bajo las cuales actúa el funcionario público son un conjunto de poderes otorgados por las leyes, de los que está dotado el jerarca o la administración para que pueda cumplir sus funciones. El funcionario público se encuentra investido de potestad —derivado de *potestas* que significa poder o facultad<sup>2</sup>— bajo la cual realiza actos administrativos que constan, por lo general, en los documentos de la gestión pública que podríamos puntualizar como documentos de archivo.

<sup>2</sup> SILVA CIMMA, Enrique, *Derecho Administrativo chileno y comparado, introducción y fuentes*. Santiago, Editorial Jurídica de Chile, 1996, Cuarta Edición p. 31.

Según Roberto O. Bustillo Bolado los actos administrativos son todos aquellos jurídicos unilaterales, dictados por la administración, que se encuentran sometidos al derecho administrativo.<sup>3</sup> Una definición bastante amplia, y a nuestro modo de ver más completa, la encontramos en una cita del mismo autor, a saber: acto administrativo “es cualquier declaración de voluntad, deseo, conocimiento, o juicio realizada unilateralmente por la Administración, por otros órganos del Estado o por simples particulares en el ejercicio de una potestad administrativa, propia o delegada, distinta de la reglamentaria y que, de acuerdo con la naturaleza de esa potestad, producirá efectos de desigual extensión o alcance para los administrados y para la propia Administración”<sup>4</sup> El concepto hace algunas exclusiones, pero Bustillo Bolado aclara que los diferentes conceptos no marginan o eluden el tratamiento de figuras como dictámenes, informes, respuestas a consultas o certificaciones, los cuales clasifica como actos administrativos *lato sensu*, por tanto se esbozan claras líneas identificadoras del régimen jurídico, en tanto existen otros actos jurídicos unilaterales dictados por la administración y sometidos al derecho administrativo.<sup>5</sup> Este es el punto al que queríamos llegar porque, a nuestro entender, marca la confluencia entre el acto administrativo y los documentos de archivo para concretarse en el expediente administrativo, en el que no solamente tenemos los documentos emitidos por los funcionarios sino los presentados por las personas naturales o jurídicas dentro de lo que el derecho denomina el *negocio jurídico* (en la administración pública éste se cumple a través del trámite o gestión administrativa). Este instituto jurídico que se da entre particulares, a decir de Giovanni Battista Ferri desde el plano externo “se refiere al problema de las relaciones entre voluntad privada y poder constituido (instituciones, Estado, voluntad de la ley) donde es posible planear un problema de decisión política general o de clase donde se puede comprender la relación entre libertad y autonomía del particular (de la cual es expresión el negocio), así como la autoridad que el ordenamiento expresa”.<sup>6</sup>

<sup>3</sup> BUSTILLO BOLADO, Roberto O., “El Concepto de acto administrativo y la teoría del negocio jurídico. Santander”. En: *Escritos Jurídicos, homenaje a Luis Rojo Ajuría*, Universidad de Cantabria, 2002, p. 786.

<sup>4</sup> *Ibíd.* p. 789.

<sup>5</sup> *Ibíd.* p. 794.

<sup>6</sup> BATTISTA FERRI, Giovanni, *La idea de negocio jurídico*, Lima, ARA Editores, 2002, p. 77.



Es innegable que la administración pública no actúa sola, los actos unilaterales mencionados por Bustillo Bolado, citado líneas arriba, se producen por la voluntad de los funcionarios, entendida como la facultad que éstos poseen para actuar en nombre del Estado y bajo una legislación especial que les permite accionar, realizar actos y actividades administrativas, tomando decisiones respecto de las demandas de los diversos servicios requeridos por los administrados. En ese negocio jurídico los actos realizados de una y otra parte van generando los documentos de archivo, los que además deberán observar ciertos requisitos y formalidades para ser incorporados al expediente administrativo, o en su caso la misma legislación prevé los plazos dentro de los cuales se subsanarán las omisiones en que el accionante haya incurrido para cumplir con las formalidades o requisitos de la ley, hecho esto son incorporados para sustentar o diligenciar el asunto motivo del trámite tratándoseles como documentos auténticos.

José Bono señala que todo negocio jurídico es un acto de manifestación de la voluntad (*animus*) sea de la administración o del administrado, y detrás de este “hacer en Derecho” necesariamente hay un agente —otorgante—, el actor. Su otorgamiento garantiza la veritas *negotii* (*negotium verum*). De otra parte, la escrituración es, sencillamente, el acto de creación documental, la puesta por escrito de la actuación, y como tal creación, *augere*, exige un realizador de tal tarea, un autor: *auctor*. La autorización garantiza la *veritas scripturae*.<sup>7</sup>

Los elementos indicados por Bono para que el negocio jurídico sea tal, son fundamentales para aceptar la autenticidad de los documentos. Si hacemos una comparación con parte de las características que el Proyecto InterPARES<sup>8</sup> identificó en el documento electrónico de archivo a partir de los estudios diplomáticos, vemos que es relativamente coincidente con la participación de: autor (la persona responsable de emitir el documento

<sup>7</sup> BONO, José, “Diplomática notarial e historia del Derecho Notarial”, Madrid. Exposición de la conferencia impartida por el autor en el seminario de profesores del Departamento de Historia del Derecho en *Cuadernos de Historia del Derecho*, a.0 3, 171-190. Servicio de Publicaciones U. C. M., 1996, p. 180.

<sup>8</sup> Proyecto InterPARES <http://www.interpares.org/>.

que para Bono es el actor); un destinatario (la persona a quien el documento ha sido dirigido); el escritor (persona responsable de la articulación del contenido que para Bono es el autor); mientras que la acción es propiamente el negocio jurídico, que se puede verificar en el documento, éste lo sostiene y es la expresión material de la manifestación de la voluntad propia del acto jurídico administrativo.

Para Fernando de Velasco citado por Bustillo Bolado, el acto administrativo es “toda declaración jurídica unilateral y ejecutiva, en virtud de la cual la Administración, tiende a crear, reconocer, modificar o extinguir situaciones jurídicas subjetivas”.<sup>9</sup>

Las relaciones intersubjetivas entre los administrados y la administración pública se manifiestan de diversas maneras, una de ellas es la escrita donde los documentos de los archivos constituyen la realización de los actos efectuados, los que pueden revestir carácter jurídico o no. Si nos situamos en la autenticidad desde el punto de vista jurídico necesariamente tenemos que referirnos al acto jurídico, entonces nos centraremos en éste concepto a través del hecho jurídico en tanto aquél es una especie dentro de este último. El hecho jurídico a decir de Savigni, citado por Fernando Vidal Ramírez, es el hecho que produce una adquisición, modificación, transferencia o extinción de derechos, de donde se deriva en que el hecho jurídico produce una consecuencia de derecho, con efectos jurídicos y se constituye, mediata o inmediatamente, en fuente de toda relación jurídica o en causa de su extinción. No todo hecho es jurídico.<sup>10</sup> La consecuencia jurídica es la que configura el hecho jurídico. Al mediar la voluntad humana en un acto de la administración —facultada por la ley para actuar— estamos en presencia de un acto jurídico, esa manifestación de la voluntad registrada en un documento como resultado de una actividad cualquiera sea el soporte (aquí nos acercamos al documento de archivo en estricto), le otorga esa calidad.

<sup>9</sup> BUSTILLO BOLADO *Op. Cit.*, p. 789.

<sup>10</sup> VIDAL RAMÍREZ, Fernando, *El acto jurídico*, Lima, Gaceta Jurídica, Quinta Edición, 2002, p. 31.

### **III. 2 La formación del e-expediente en la administración pública: su autenticidad**

Tal como hemos adelantado, de acuerdo con la legislación y la doctrina administrativa la autenticidad de los documentos emitidos por los funcionarios públicos, en general no es cuestionable, pero ¿cómo se tiene la certeza de la autenticidad de los documentos de las personas naturales o jurídicas que pudieran incorporarse al expediente administrativo conforme avanza el trámite o la gestión de los asuntos que tratan? Los actos de los administrados no son 'administrativos' al no provenir de la administración pública, siendo frecuente que cada vez ésta exija de los administrados la formulación ante ella de declaraciones.<sup>11</sup> Estas declaraciones necesariamente deben constar en un documento.

La administración pública a través de los funcionarios tiene la responsabilidad de integrar todos los documentos presentados por los administrados presumiendo su autenticidad, lo cual puede resultar relativamente sencillo con los documentos en soporte de papel, pero si el administrado presenta documentos electrónicos en algún dispositivo de esa naturaleza (CDRom, CD, Memoria USB, etc., o a través de mensaje vía telemática) para ser incluidos en el e-expediente, aun cuando se trate de copias auténticas otorgadas por las entidades públicas, esa presunción de autenticidad ya no es tan inmediata, se tendrá que recurrir a ciertos auxilios para comprobar la existencia de determinados requisitos funcionales para admitirlos como auténticos a fin de ser utilizados en el asunto materia de gestión, jurídicamente válidos para sustentar las pretensiones del administrado. No obstante, en un sistema de gestión de documentos electrónicos integrado al e-gobierno, se entiende que los administrados ya no tendrán que presentar documentos que la administración pública custodia<sup>12</sup>. En ese contexto los documentos circularán a través del cyber espacio y podrán

<sup>11</sup> MORENO MOLINA, José Antonio, *Procedimiento y proceso administrativo práctico*, Madrid, La Ley, Volumen 3, 2006, p. 194.

<sup>12</sup> En sentido amplio y general en el concepto de administración pública comprende a todas las organizaciones de los poderes del Estado.

ser capturados para continuar el trámite también en medios electrónicos, lo que no los exceptúa de la comprobación de su autenticidad pues ésta deberá ser corroborada constante y obligatoriamente.

De otro lado, los documentos tradicionales de carácter privado que presentan los particulares para la tramitación de un determinado asunto para constituirse en elementos probatorios en la vía jurisdiccional, deben ser reconocidos jurídicamente antes de presentarse e integrarse al expediente, donde constarán en originales o copias certificadas o autenticadas otorgadas por la autoridad jurisdiccional competente. Similar procedimiento se cumple en el ámbito administrativo con la participación de un funcionario facultado por la ley a esa función.

En algunas ocasiones se solicitará una declaración jurada, regulada legalmente bajo sanción penal en caso de falsear información o datos del administrado para su presentación, sin perjuicio de posterior comprobación o fiscalización de oficio en caso de que la administración decida corroborar su autenticidad, lo cual la ley prevé. Pero, si se trata de documentos electrónicos, cabe preguntarse si su reconocimiento para ser integrado a un trámite ante instancia administrativa o jurisdiccional será o no otorgado por el órgano correspondiente. De ser esto posible se podrá integrar al e-expediente dentro del sistema de gestión documental en el que se tramite, donde se cuidará de su autenticidad y preservación por todo el tiempo que sea necesario.

Cabe precisar que el fuero jurisdiccional es más riguroso, en ese sector nada nos garantiza que se le otorgue validez al documento electrónico para ser usado como elemento probatorio dentro de un proceso o procedimiento, cualquiera sea la naturaleza del asunto en el que se gestione. En todo esto lo que está en juego es la autenticidad del documento electrónico y su calidad de prueba o simplemente de información para la continuación de un determinado trámite. En ambos casos para que el documento pueda surtir efectos legales o administrativos debe ser comprobadamente auténtico.

En otro lado de la práctica administrativa por medios electrónicos, encontramos los mensajes o envío a la administración de documentos privados sujetos a la legislación especializada para su incorporación al e-expediente. Si se encuentran firmados digitalmente,

según la legislación especializada, el documento formalizado bajo este tipo de firma ofrece garantía de su autenticidad. Por esta disposición legal debería ser de aceptación inmediata por el funcionario o juez que lo recibe. Pero, esto en la práctica, aun cuando se encuentra dentro del marco legal del ordenamiento jurídico de la mayoría de países, no es tan categórico, queda entonces en la decisión de la administración o el órgano jurisdiccional aceptar o rechazar los documentos electrónicos, hechas las comprobaciones o peritajes que decidan actuar, para finalmente tomar una posición —permitida por la ley— según el poder discrecional o las reglas de la sana crítica que les asiste respectivamente.

Como podemos apreciar tanto para el documento electrónico público como privado, como bien lo señala Mariliana Rico Carrillo: “el juez debe establecer su valoración según las normas procesales que determinan, en forma tasada, el valor de un documento, según se trate de un documento público o de un documento privado. También entran en juego las máximas de la sana crítica, si se llegare a dudar de la autenticidad del documento, si se ha solicitado experiencia o se ha practicado una inspección judicial”.<sup>13</sup> Las reglas de la sana crítica, que la mayoría de las legislaciones contempla, le confieren amplia discrecionalidad al juzgador y lo facultan a rechazar de plano cualquier elemento probatorio, que de acuerdo con su apreciación, no le otorgan el convencimiento y confianza de ser utilizado como prueba en juicio.

#### **IV. El documento electrónico de archivo**

En este rubro no entraremos a desarrollar un concepto o a ofrecer algunas de las múltiples definiciones que a lo largo de los últimos años se han construido sobre documento electrónico de archivo, solo nos remitiremos a expresar que éste es un documento que tiene la misma finalidad que cualquier documento de archivo en soporte de papel, con la diferencia que se encuentra en soporte electrónico.

<sup>13</sup> RICO CARRILLO, Mariliana, *Función procesal probatoria*, Bogotá, Legis, 2003, p. 229.

Debemos precisar que en todo el presente documento nos estamos refiriendo al documento electrónico de origen, es decir, el que se produce en ambiente electrónico, se mantiene, se preserva y se conserva en este medio durante todo su ciclo vital. Por tanto no nos referiremos a los documentos digitalizados a partir de documentos en soporte de papel aun cuando puede ser una forma de integrarlos a un sistema de gestión electrónica de documentos de archivo.

Lo que nos motiva en este momento es abordar la problemática del reconocimiento de la autenticidad del documento electrónico de origen tanto en lo jurídico como en el ámbito diplomático. Es decir, nos estamos refiriendo al documento electrónico que en ningún momento, está en soporte de papel. Se trata de aquel que siempre es electrónico, circula en ese medio, se preserva, custodia, mantiene, conserva en ambiente electrónico y se sirve en el mismo medio o excepcionalmente en una copia en soporte de papel lo que no desvirtúa su origen.

### **A. Reconocimiento jurídico**

Desde que se inició la emisión de leyes y normas de menor nivel jerárquico sobre tecnología electrónica aplicada a los archivos, éstas exigen que los documentos electrónicos garanticen su autenticidad, permanencia, integridad y otros requisitos utilizando diferentes términos de similar connotación o alcance. La legislación sobre aplicación de la firma digital (las denominaciones varían según el país: firma electrónica, firma avanzada, etc).<sup>14</sup> de un documento electrónico señala, en términos amplios y generales, que ésta garantiza su autenticidad y en consecuencia, legalmente la indicada autenticidad deberá verificarse a través de la firma digital del sujeto firmante. Como podemos advertir, legalmente la autenticidad del

<sup>14</sup> MENDOZA NAVARRO, Aída Luz: "Documentos electrónicos de archivo, una visión integradora" Capítulo VIII, Lima, Biblioteca Nacional del Perú, 2009, 215 pp.; y "Legislación sobre documentos electrónicos: diversidad terminológica" en: *Archivos en Formato Electrónico*, México publicación del Archivo General de la Nación, 2006, p. 43-68.

contenido del documento electrónico queda supeditada al procedimiento de identidad del firmante mediante la verificación de la firma digital.

En los procesos jurídicos normalmente se trata de demostrar la identidad del firmante de un documento que será utilizado como medio probatorio. Cuando estamos frente a un documento en soporte de papel al identificar al firmante automáticamente se corrobora la autenticidad del contenido, sin embargo si el elemento probatorio consta en un documento electrónico, nada nos asegura que éste no haya sufrido alteración alguna durante su existencia y que en el momento de surtir sus efectos probatorios se encuentra íntegro, en tanto la firma digital permanezca inalterable llegándose a la certeza *que es de quien dice ser*. Necesariamente pasará por un proceso de verificación. Luego se tendrá la identidad del firmante y según el procedimiento tecnológico de verificación amparada por la ley, también se reconoce el contenido, pero ¿por cuánto tiempo es posible garantizar esa identidad y con ella, que el contenido del documento electrónico no ha sufrido alteración o modificación alguna?

Mientras que para el reconocimiento de los documentos en soporte de papel bastará comprobar la relación existente entre la emisión del documento por un determinado sujeto a través de la firma autógrafa no importando el tiempo o data del documento —5, 10, 20 años o más— en los documentos en ambiente electrónico el tiempo juega un papel decisivo y por el momento es todo un reto mantenerlos inalterables y garantizar su autenticidad incuestionable por espacios más o menos prolongados de tiempo. Debemos advertir que en la administración pública todo documento firmado por funcionario público en ejercicio de sus funciones será auténtico y, ante alguna duda bastará cotejar la firma del documento, visualmente, contra el documento de identidad del sujeto firmante u otro en el que éste haya firmado. Pero si el documento se encuentra en soporte electrónico ningún juez lo acepta categóricamente si no queda verificada plenamente su autenticidad a diferencia del documento público en soporte de papel que goza de la confianza en el campo jurisdiccional sin necesidad de verificación expresa, excepto en casos en los que median actos de corrupción o se presume falsificación de documentos u otras modalidades que la ley penal prevé, pero este es un tema diferente al que concita nuestra atención en estos momentos.

La comprobación de una firma digital auténtica se refiere a la verificación de la cadena de bits como señala Alejandro Delgado: “La firma digital, pues, garantiza que una secuencia de bits es íntegra en un punto del tiempo, no que un documento digital conserva su integridad a lo largo del tiempo.” Por tanto es independiente de la autenticidad del contenido del documento en tanto no puede garantizar su integridad a largo plazo.<sup>15</sup> Siendo tan débil el sustento de la firma digital para enlazarla con la autenticidad del documento electrónico en su integridad y durante todo el tiempo que se le necesite, tendremos que abocarnos a preferir siempre la demostración de la autenticidad de todo el documento. Por tanto, jurídicamente, para tener la certeza de la autenticidad del documento electrónico no bastará la comprobación de la firma digital en tanto ésta no es garantía de la autenticidad de todo el documento, ergo se deberá prescindir de uno de los elementos que para la diplomática si es fundamental, la firma, como bien lo advierte Alejandro Delgado: “En diplomática, una firma es tradicionalmente uno de los componentes fundamentales que garantizan, bajo determinadas condiciones y en combinación unos componentes con otros, que un documento es auténtico”<sup>16</sup> Como resultado se deberá derivar la verificación de la autenticidad a otros elementos como por ejemplo los metadatos y a la ayuda de los requisitos funcionales archivísticos para mantener la autenticidad mientras el documento sea necesario. Esto es posible en los documentos que genera la administración, pero deberá extenderse a los que presenten los administrados para integrarse al e-expediente dentro de un sistema de gestión de documentos electrónicos de archivo.

Esta continuada e imprescindible comprobación de la autenticidad de los documentos electrónicos públicos o privados, agrega una actividad adicional al funcionario público que tomará una decisión respecto del documento presentado por el administrado o al juzgador que debe meritarse las pruebas presentadas a través de documentos electrónicos para ser

<sup>15</sup> DELGADO, Alejandro, “La conservación a largo plazo de firmas digitales auténticas: reflexiones para el debate desde el punto de vista archivístico”, [http://www.js-e.cat/site/arxius/pdf/ponencies\\_07/Delgado\\_Alejandro.pdf](http://www.js-e.cat/site/arxius/pdf/ponencies_07/Delgado_Alejandro.pdf) [Consulta: 04.12.09] p.9.

<sup>16</sup> *Ibíd.* p. 4.



incorporadas al e-expediente. Entonces, no bastará tener por cierto el contenido de un e-documento público por ser tal; en todos los casos se deberá proceder a aplicar los procedimientos tecnológicos, las auditorías electrónicas que sean necesarias o cualquier otro mecanismo de verificación de la autenticidad para que el documento electrónico sea aceptado como prueba irrefutable en la vía jurisdiccional e incluso en la administrativa, aun cuando se tenga la certeza que proviene de organismo público; en cambio si el documento está en soporte de papel bastará la copia autenticada por funcionario competente, notario público o autoridad facultada por la ley, por su calidad de público será suficiente para su admisión al proceso jurídico o administrativo correspondiente.

Insistimos en que la autenticidad de un documento en cualquier tipo de soporte no es cosa de momento, ésta deberá ser incuestionable mientras el documento sea necesario y de acuerdo con las técnicas de valoración documental; entendemos que los plazos de retención por lo general exceden a períodos cortos, antes bien, en promedio podemos afirmar que tales plazos en gran proporción sobrepasan los 10 años con lo cual estamos refiriéndonos al largo plazo.

Esta es una de las tantas razones por las que diversos proyectos nacionales e internacionales en el mundo están dirigidos a la investigación de la autenticidad y la preservación a largo plazo de los documentos en ambiente electrónico, sobre todo en estos momentos que para nadie es ajeno que la gestión pública y privada con el apoyo de las tecnologías de la información y comunicaciones (TIC) se van desarrollando de manera asombrosa.

## **B. La determinación de la autenticidad por la diplomática**

La diplomática, como ya hemos puntualizado, ha sido fundamental en el estudio de la autenticidad del documento electrónico. Uno de los principales estudios sobre el tema fue abordado por Luciana Duranti años atrás con trascendentes resultados y luego, a partir del año 1999 por InterPARES bajo su liderazgo. Al respecto, Luciana Duranti afirma

que la diplomática se encuentra estrechamente vinculada a la necesidad de determinar la autenticidad de los documentos, pero no coincide con la autenticidad legal. Los documentos diplomáticamente auténticos son los que fueron escritos según las prácticas del tiempo y lugar indicados en el texto y firmados por las personas competentes para crearlos.<sup>17</sup>

La diplomática estudia el documento, sus características internas y externas, las formas documentales, su estructura, sus cláusulas etc., para establecer las diferentes tipologías y sus orígenes con el fin de analizar su autenticidad.

La mayoría de los especialistas en el tema coinciden en que la diplomática no solo es aplicable a los documentos medievales sino a cualquiera de ellos, desde los más antiguos a los que se siguen produciendo.

La diplomática es la disciplina de los documentos, focaliza su atención en su naturaleza jurídica y averigua su autenticidad total o parcial, “tratando de encontrar la concordancia entre los elementos internos y externos que lo integran”.<sup>18</sup>

Para María Elena Bibriesca, tanto la validez como la autenticidad están representadas por la firma o rúbrica del autor o autores del documento, de los testigos y demás personas que intervienen, como por aquellos a quienes toca por oficio como son los notarios, cancilleres, cuya signatura o rúbricas pueden estar suplidas por una fórmula o por un sello.<sup>19</sup> La autora en referencia menciona ‘fórmula reconocida o sello’ que es el que permitirá acreditar la autoría de los documentos electrónicos que emitan las personas físicas y las personas jurídicas. Para esta época podríamos incluir la firma digital y el sello electrónico, no obstante, líneas arriba nos hemos referido a las implicancias de la firma digital y sus desventajas frente a la permanencia de este tipo de elementos digitales para la preservación de la autenticidad a largo plazo. Debemos mencionar que el sello digital, según la legislación de los países que han normado sobre el particular, quedan sujetos a la misma regulación aplicable al uso

<sup>17</sup> DURANTI, Luciana, *Diplomática, Usos nuevos para una antigua ciencia*, Carmona, S&C Ediciones, 1996, p. 29.

<sup>18</sup> BIBRIESCA SUMANO, María Elena, *Texto de Paleografía y diplomática*, México, Universidad Autónoma del Estado de México, 2002, p. 86.

<sup>19</sup> *Ibíd.* p. 108.

de una firma electrónica avanzada o digital, en consecuencia su naturaleza, verificación, exigencias legales de uso, certificación y el período de validez de la certificación, así como sus desventajas para garantizar la autenticidad en el largo plazo, serán las mismas. Por consiguiente, la firma digital o el sello electrónico no constituye un elemento a considerarse para la determinación de la autenticidad del documento electrónico desde el punto de vista de la diplomática, en el mismo sentido nos hemos expresado desde el ámbito jurídico aunque la legislación especializada así lo prevé.

En ese panorama, con el apoyo de la diplomática se fija la atención en otras características del documento electrónico. Jim Suderman explica los hallazgos de InterPARES a partir de la diplomática en el entorno electrónico e indica las características detectadas a la vez que agrega interesantes comentarios como sigue:

1. *Una forma fija* – esto no significa que el código binario del documento electrónico no pueda cambiar, sólo que cuando se rinde o reproduce el documento lo haga con la misma forma documental que tenía cuando se completó por primera vez.

2. *Contenido estable* – el mensaje no debe cambiar, lo que significa en el entorno electrónico, que tienen que ponerse en vigor medidas adecuadas de seguridad para asegurar que sólo individuos autorizados crean contenido, y que una vez creado no puede modificarse, o al menos no, sin que quede un registro de su modificación.

3. *Una acción* – de la que el documento es un instrumento o un producto de los procedimientos organizativos seguidos.

4. *Enlaces explícitos a otros documentos que pertenecen a la misma actividad*, por ejemplo, como los proporcionados por un código de clasificación de expedientes.

5. *Un contexto administrativo identificable*.

6. *Un autor, un destinatario y un escritor*.<sup>20</sup>

<sup>20</sup> SUDERMAN, Jim, "Estructurar el paradigma de conservación: un informe sobre los hallazgos del Proyecto InterPares", Fuente: Conferencia pronunciada en La Habana el 16 de marzo de 2005. Albergado en la base de documentos de InterPARES 2 (<http://www.interpares.org>) p. 8.

Las características anotadas han sido ampliamente analizadas y desarrolladas en los estudios de InterPARES sobre la base de la diplomática, con la finalidad de determinar la autenticidad del documento electrónico a lo largo de su ciclo vital.

La diplomática contemporánea es uno de los soportes esenciales de la investigación de InterPARES. Heather Mcneil al referirse a esta disciplina como método de investigación comenta que en los últimos años el problema del contexto<sup>21</sup> se convirtió en un tema fundamental que afecta a la autenticidad de los documentos electrónicos desde dos perspectivas: primero los documentos electrónicos están anidados dentro de múltiples contextos que se solapan, son complejos y sujetos a rápidos cambios, pero estos contextos tienen que comprenderse y describirse para establecer y proteger la autenticidad de los documentos; y segundo el límite entre los documentos y el contexto que los rodea tiende a desdibujarse en entornos de gestión electrónica de documentos, por lo que se dificulta la preservación de su autenticidad.<sup>22</sup> Las áreas, elementos, características o propiedades del documento electrónico deberán ser abordados en toda su dimensión para llegar a identificar los requisitos para ponderar y mantener la autenticidad de los documentos electrónicos, siendo la aplicación de la diplomática, con su metodología para analizar los aspectos del contexto del documento electrónico, la disciplina que permite el mejor análisis de los documentos y su gestión en marcos administrativos.<sup>23</sup> De acuerdo con la autora, en el contexto concurren una serie de circunstancias que analizadas contribuirán al reconocimiento de la autenticidad de los documentos electrónicos, de donde deducimos que pese a la complejidad que a ello conlleva, resulta de inminente necesidad la aplicación de la diplomática para seguir desarrollando la gestión documental en ambiente electrónico.

<sup>21</sup> Heather Macneil hace referencia a la explicación sobre el contexto de Goodwin y Duranti, a saber: "el contexto es (...) un marco que rodea el evento que se está examinando y proporciona recursos para su adecuada interpretación". MACNEIL, Heather, *La diplomática archivística contemporánea como método de pesquisa: lecciones aprendidas de dos proyectos de investigación*, Cartagena, Ayuntamiento. Concejalía de Cultura 3000 Informática, traducción: Alejandro Delgado; 2006.

<sup>22</sup> MACNEIL, Heather, *Op. Cit.* p. 63.

<sup>23</sup> *Ibid.* p. 66.

## V. La autenticidad elemento jurídico fundamental

La autenticidad jurídica es una de las características del documento original. Significa que el hecho jurídico responde a la intención del autor o mejor aun a la manifestación de la voluntad.

Cuando nos referimos a los actos jurídicos administrativos, amparados legalmente en la fe pública, entendemos que tienen valor suficiente porque se presume que gozan de integridad y veracidad por la fuerza que emana del propio Estado, por tanto la nota de autenticidad del acto público se refiere a la identidad del funcionario que otorga el documento y a los hechos que en él constan. En ese aspecto, la demostración de la gestión realizada se verifica mediante los documentos públicos, de este modo la administración pública o el Estado mismo, es capaz de proteger el interés general, social y ejerce su responsabilidad tuitiva porque deberá garantizar la seguridad jurídica de los administrados, de donde se desprende la importancia de los documentos públicos de archivo.

La legislación, dirigida al uso de las TIC, en vía reglamentaria o algunas veces dentro del cuerpo de la misma ley, se limita a establecer algunas consideraciones técnicas para garantizar las exigencias de autenticidad del documento electrónico, o por lo menos establece las formalidades para la recepción de los documentos presentados por los administrados. Solo a manera de ejemplo y por sus claras precisiones, citaremos el Real Decreto 1671/2009, de 6 de noviembre por el que se desarrolla parcialmente, en vía reglamentaria, la Ley 11/2007 de 22 de junio sobre el acceso electrónico de los ciudadanos a los servicios públicos (B.O.E. nº 278 de 18 de noviembre de 2009). Este Real Decreto en su artículo 29 legisla sobre las condiciones para que las administraciones públicas reciban los documentos que presenten los administrados.<sup>24</sup>

El numeral 1 del artículo en referencia establece:

1. Los registros electrónicos podrán rechazar los documentos electrónicos que se les presenten, en las siguientes circunstancias:

<sup>24</sup> Real Decreto 1671/2009, España, [http://www.informatica-juridica.com/anexos/RD\\_1671\\_2009\\_de\\_6\\_%20de%20noviembre.asp](http://www.informatica-juridica.com/anexos/RD_1671_2009_de_6_%20de%20noviembre.asp) [Consulta: 06.01.10].

- a) Que se trate de documentos dirigidos a órganos u organismos fuera del ámbito de la Administración General del Estado.
- b) Que contengan código malicioso o dispositivo susceptible de afectar a la integridad o seguridad del sistema.
- c) En el caso de utilización de documentos normalizados, cuando no se cumplimenten los campos requeridos como obligatorios en la resolución de aprobación del correspondiente documento, o cuando contenga incongruencias u omisiones que impidan su tratamiento.
- d) Que se trate de documentos que de acuerdo con lo establecido en los artículos 14 y 32 deban presentarse en registros electrónicos específicos.

2. En los casos previstos en el apartado anterior, se informará de ello al remitente del documento, con indicación de los motivos del rechazo así como, cuando ello fuera posible, de los medios de subsanación de tales deficiencias y dirección en la que pueda presentarse. Cuando el interesado lo solicite se remitirá justificación del intento de presentación, que incluirá las circunstancias de su rechazo.

3. Cuando concurriendo las circunstancias previstas en el apartado 1, no se haya producido el rechazo automático por el registro electrónico, el órgano administrativo competente requerirá la correspondiente subsanación, advirtiéndole que, de no ser atendido el requerimiento, la presentación carecerá de validez o eficacia.

Algunas de ellas, a nuestro parecer, encajan directamente en la calidad de autenticidad de los documentos a tramitarse. En mayor proporción las señaladas en el numeral 1 b, c, d, también el numeral 3 en el que se indica que el rechazo automático por el registro electrónico advierte sobre la carencia de validez o eficacia del documento, lo que para el derecho significa que el documento carece de autenticidad.

No negamos su necesidad y oportunidad, sin embargo, a la luz de los resultados de diversos proyectos internacionales trabajados sobre el tema, en nuestra opinión, el aspecto jurídico es rebasado por la incertidumbre de la imposibilidad de asegurar la permanencia de

ciertos requisitos de autenticidad durante todo el ciclo vital de los documentos electrónicos. Los peligros a los que están expuestos, por diversas circunstancias, ponen en riesgo la integridad e identidad del documento electrónico —estos elementos forman parte de la autenticidad según InterPARES con lo que coincidimos plenamente—. Es imperativo, entonces, incorporar otros elementos para minimizar los riesgos de pérdida de autenticidad o de pérdida de los documentos y con ellos de la información, que podría ser irrecuperable afectando las transacciones administrativas y jurídicas de los administrados. Esas medidas de protección para reducir los riesgos de pérdida de información —no nos atrevemos a manifestar la posibilidad de garantía absoluta de autenticidad del documento electrónico porque ésta por el momento no existe—, por ello convenimos en enfatizar sobre la necesidad de “disminuir o minimizar los riesgos”, que no están en el campo jurídico por lo que será necesario acudir a otras áreas de conocimiento para:

1. El reconocimiento e identificación de la autenticidad de los documentos con la finalidad de que puedan surtir sus efectos administrativos y/o jurídicos ante las instancias pertinentes; y
2. Aplicar determinados requisitos funcionales, como lo vienen haciendo algunos países desde el campo de la archivística y la diplomática, para apoyar la preservación de la autenticidad y la permanencia de los documentos electrónicos de manera integral durante todo su ciclo vital.

En esos aspectos, la diplomática y la archivística contribuyen a fortalecer las técnicas que posibilitan una mejor preservación de la autenticidad de los documentos electrónicos.

A la luz de los resultados de InterPARES sobre la identificación de la autenticidad quedan demostradas las bondades del apoyo de la diplomática en la identificación de las características del documento electrónico.

## VI. Confluencia de la autenticidad jurídica y diplomática en el documento electrónico de archivo

Los fines del derecho y la diplomática difieren sustancialmente, mientras el derecho persigue la autenticidad del documento para su utilización como medio probatorio o evidencia, la finalidad de la diplomática, tradicionalmente, siempre fue determinar su valor para la historia. Sin embargo, los diplomatas contemporáneos desde años atrás vienen aplicándola a los documentos de todas las épocas y Luciana Duranti demostró que esta disciplina también resulta valiosa para el estudio de la autenticidad de los documentos electrónicos. Ésta ha sido el soporte fundamental de la investigación que desarrolla InterPARES desde el año 1999 a la fecha con reconocidos resultados.

Al respecto Jim Suderman comenta: “Para apoyar la evaluación y la supervisión de los documentos, se identificaron siete requisitos de cota dentro de InterPARES. A los efectos de esta presentación, sólo esbozaré el de la identidad e integridad del documento.

La identidad se establece mediante los nombres de los individuos conectados a la formación del documento (autor, destinatario, etc.). También se requiere la fecha de creación o transmisión, la actividad con la que el documento está conectado, y la relación del documento con otros documentos. La integridad queda establecida tanto si el documento está completo como si su mensaje no ha sido modificado. Por ejemplo, un memo [memorando] donde el texto estuviera completo pero otro atributo, p. ej., si el autor estuviera ausente indicaría que la integridad del documento está comprometida.<sup>25</sup> Las circunstancias dentro de las cuales se llega a determinar la autenticidad y se fijan las acciones de preservación de los documentos electrónicos de archivo, pasan por una serie de procedimientos para finalmente llegar a la certeza que el documento no ha perdido su identidad e integridad, a diferencia de los documentos en soporte de papel que no necesitan de ello para que el juzgador o el funcionario de la administración pública lo acepte como auténtico.

<sup>25</sup> *Ibid.* p. 10.



## VI. 1 Comprobación de la autenticidad

Los documentos electrónicos, no obstante provenir de la función pública, tal como lo advertimos líneas atrás, deberán ser sometidos a exigentes procedimientos de comprobación de la autenticidad y no solamente en el momento de requerirse como instrumentos probatorios sino durante todo su ciclo vital, debido a que esa comprobación debe ser permanente para que el documento electrónico sea útil en el momento que se le necesite, sea o no requerido por una instancia jurisdiccional o administrativa.

Al no ser posible mantener una forma física del documento electrónico, el significado de la forma en el entorno tecnológico ha cambiado para el documento administrativo respecto del documento en soporte de papel. Si bien la forma permitía distinguir la autenticidad y su fiabilidad ahora ya no pues ésta ha entrado en 'crisis' al no existir una forma física del documento perceptible al ojo humano sino solamente códigos que lo han informatizado.<sup>26</sup> De esta manera, para mantener la autenticidad de un documento electrónico será necesario preservar el documento y su autenticidad; mientras que en el caso del documento en soporte de papel bastará con preservar el documento en tanto su autenticidad es concomitante con él durante toda su existencia.

Esa situación exige la comprobación de la autenticidad del documento electrónico a través de otros mecanismos más complejos que el documento tradicional no necesita. A pesar de la incertidumbre que aun rodea a la gestión de documentos por medios electrónicos, la realidad en la que se mueve la gestión pública y también la privada, donde día a día vemos el desarrollo progresivo y sostenido de la gestión electrónica de los documentos, demanda, desde varias áreas del conocimiento, trabajar intensamente para ir logrando cada vez más, confianza en los documentos electrónicos, utilizándolos con la certeza de que los derechos e información que ellos sustentan no corren riesgo de ningún tipo.

Joan Soler señala:

<sup>26</sup> JOAN Soler, p. 17.

Tradicionalmente la autenticidad residía en las características que la diplomática denomina extrínsecas e intrínsecas. En un entorno electrónico cada documento generado tiene que disponer de un perfil de documento, que engloba estas características. Para garantizar la autenticidad los elementos mínimos de información del perfil [perfil del documento e instrumento complementario como metadatos relativos al uso de los documentos] que hemos analizado anteriormente son: la fecha, el tiempo, el autor, el destinatario, la acción, el código de clasificación, el número de registro y la corroboración. Cada documento para ser transmitido de forma segura, tiene que estar protegido por un sello de tiempo o un sello criptográfico, por ejemplo.<sup>27</sup>

Más adelante el mismo autor expresa: La autenticidad de los documentos en ambiente electrónico viene conferida al documento por la forma y el estado de transmisión, y por la manera como éste se ha preservado y custodiado. En los sistemas electrónicos así como en los sistemas tradicionales, la autenticidad se asegura por el respeto a procedimientos administrativos, dificultando la reproducción de instrumentos técnicos e instalando dispositivos de seguridad. Luego menciona que la seguridad de la transmisión alcanza mediante articulación de métodos de transmisión y recepción desde un espacio a otro de forma automática y manual; además con la inclusión de un *audit. trail* [pista de auditorial] para determinar la trazabilidad de cada transmisión (fechas, tiempo, personas y sujeto).<sup>28</sup> No obstante lo anotado por el autor en referencia, sabemos que la autenticidad de los documentos electrónicos se ve amenazada cada vez más, cuando se transmiten en el espacio o en el tiempo (al almacenarlos o actualizarlos o reemplazar el software empleado, para procesarlos, almacenarlos o comunicarlos). Es así que el archivero podrá comprobar la autenticidad de los documentos electrónicos apoyándose en la evidencia de que éstos han sido mantenidos utilizando tecnologías y procedimientos que garanticen su identidad e integridad a lo largo del tiempo, o que los riesgos de cambios se han minimizado desde el momento de su creación hasta el instante en que se accede a ellos posteriormente.

<sup>27</sup> SOLER, Joan, *La preservación de los documentos electrónicos*, Barcelona, UOC, 2008, p. 59.

<sup>28</sup> *Ibíd.* p. 59.

## VI.2 Comprobación de la autenticidad por InterPARES

InterPARES es un proyecto de carácter internacional cuyas siglas significan: *Investigación internacional sobre documentos permanentes auténticos, en sistemas electrónicos*, dirigido por la doctora Luciana Duranti. Los resultados del referido proyecto de investigación, (aun se encuentra vigente, su tercera fase concluye en el año 2012) que es uno de los más ambiciosos —por la envergadura y dimensión de las distintas áreas que comprende así como por la calidad de los especialistas participantes— ha desarrollado una serie de requisitos que permiten ponderar la autenticidad de los documentos electrónicos. Por un lado tenemos requisitos de cota y por otro los requisitos de base. Los requisitos de cota sirven para la ponderación de la autenticidad por el archivero, identifica la información central acerca de un documento electrónico que establece su identidad y sienta un fundamento para demostrar su integridad.

Los requisitos de base se refieren a las condiciones elementales para capacitar al archivero y para atestiguar la autenticidad de las copias de documentos electrónicos inactivos.

Desde la perspectiva archivística-diplomática en los requisitos de cota destacamos: los nombres de las personas (autor, destinatario, escritor y generador); fecha o fechas de creación y transmisión; la indicación del asunto; la expresión de su vínculo archivístico que lo enlaza a otros documentos que participan de la misma acción, como también una indicación de los adjuntos (si los hubiera).

La integridad se refiere al estado de completo o solidez del documento en sus aspectos esenciales, esto significa que el mensaje permanece inalterado, pudiendo la cadena de bits quedar comprometida, pero a condición de que la articulación del contenido y cualquier elemento requerido de forma sigan siendo los mismos.<sup>29</sup> En el proyecto InterPARES confluyen varias áreas de conocimiento, siendo la diplomática uno de los fundamentales. El derecho también cumple su rol a través del marco jurídico de cada país involucrado. Ambas

<sup>29</sup> DURANTI Luciana, editora, *La conservación a largo plazo de documentos electrónicos auténticos*, Cartagena, Ayuntamiento de Cartagena. Tendencias 4, traducción de Alejandro Delgado, 2005, p. 265 y siguientes.

ramas del saber humano a las que nos hemos referido en este documento, mediante sus respectivos especialistas han aportado y seguirán aportando para lograr el reconocimiento, mantenimiento y permanencia de la autenticidad del documento electrónico de archivo, a fin de que éste pueda surtir sus efectos ante cualquier instancia que lo requiera disminuyendo la incertidumbre o desconfianza aun subsistente en las administraciones públicas y en el fuero jurisdiccional.

## VII. Conclusiones

Uno de los principales objetivos de mantener la autenticidad del documento electrónico, desde el ámbito jurídico, independientemente de la utilización de su denominación más acertada —electrónico o digital—, es el de permitir que pueda probar en juicio o ante cualquier otra autoridad facultada a meritara (fiscal, policial, administrativa, etc.) y que ésta reconozca su valor probatorio correspondiente.

La autenticidad del documento electrónico se erige como preocupación fundamental para los archiveros, sea cual fuere el uso que le de el usuario del documento debido a que el servicio a través de la entrega de los documentos en sus diversas modalidades debe estar revestido de las garantías suficientes para obtener una copia auténtica y autenticada del documento electrónico.

El auxilio de la diplomática y el elemento jurídico favorecen el reconocimiento de la autenticidad del documento de archivo. Sin embargo notamos que las exigencias jurídicas para determinar la autenticidad son menos rigurosas que la diplomática e inclusive que la archivística. Para el ámbito jurídico lo importante es reconocer al firmante del documento, pero las dudas y desconfianza del juzgador respecto de los documentos en ambiente electrónico, necesariamente lo llevarán a agenciarse de una serie de elementos tecnológicos para determinar la autenticidad, sin embargo su facultad discrecional puede incidir para que acepte o no el documento electrónico como prueba documental.



---

Carlos Alberto Zapata

---

**El documento electrónico** en la  
e-administración: análisis de caso



# Cárdenas

Director del Grupo de Investigación en Pensamiento Archivístico adscrito al Programa de Sistemas de Información y Documentación de la Universidad de la Salle – Colombia de la cual es profesor-investigador. Codirector del TEAM Colombia del Proyecto InterPARES.

## I. Introducción\*

En el año 2004 el Comité de Gestión de Documentos del Archivo General de la Nación de Colombia realizó un diagnóstico para determinar la situación de la gestión de documentos electrónicos en la administración pública, el cual se centró principalmente en entidades del orden nacional. Como resultado de esta investigación, se pudieron identificar diferentes aspectos de la gestión del documento electrónico que mostraban por un lado, un alto nivel de desarrollo de las Tecnologías de la Información y la Comunicación en las entidades analizadas, y por otro, un deficiente desarrollo en la implementación de programas de gestión de documentos electrónicos en dichas entidades. Lo anterior hizo evidente una hipótesis que se manejaba antes del estudio ya señalado, según la cual el nivel de implementación de las TIC en la administración pública no es consecuente con el desarrollo de modelos apropiados para la gestión de los documentos electrónicos, ocasionando serias dificultades en lo referente a la formación de archivos electrónicos, su organización, conservación y preservación.

Las principales conclusiones de este estudio<sup>1</sup> se refieren a la ausencia de una política estatal en materia del documento electrónico, a pesar de que en 1999 se promulgó la Ley 527 o Ley de Comercio Electrónico, en la cual se sentaron las bases para que las entidades del Estado comenzaran a incorporar nuevos elementos técnicos para la administración de los mensajes de datos. Entre las principales conclusiones de esta investigación se indican:

\* El presente trabajo muestra algunos de los resultados de la Investigación realizada por el autor en el desarrollo de la tesina presentada en el 2010 para optar el Grado de Salamanca, como parte de sus estudios de *Doctorado en Metodología y Líneas de Investigación en Biblioteconomía y Documentación de la Universidad de Salamanca* (España). Aunque el trabajo completo trata sobre la relación entre la administración electrónica y la gestión documental en el distrito de Bogotá, este ensayo resume aquellos aspectos que directamente tienen que ver con la gestión de documentos electrónicos, explicando el contexto en el cual se presenta dicha relación en la actualidad para el caso de Bogotá.

<sup>1</sup> ARCHIVO GENERAL DE LA NACIÓN. *Gestión de archivos electrónicos: situación en la administración central*, Bogotá: AGN, 2005. p. 93.



- No existe un adecuado conocimiento sobre la gestión del documento electrónico en la administración pública central. Si bien las entidades analizadas utilizan de manera generalizada las tecnologías de la información en sus procesos, la gestión de la información electrónica no obedece a un marco normativo uniforme.
- La mayoría de las entidades analizadas cuentan con un nivel de desarrollo tecnológico mínimo que permite la implementación de un programa de gestión de documentos electrónicos básico, pero este no se ha comenzado ni siquiera a formular.
- No hay armonización entre las políticas y normas de gestión de documentos impresos y las políticas y normas del documento electrónico; mientras el primero está dentro del ámbito profesional de los archivistas, el segundo se ha dejado en manos del personal de sistemas de las entidades públicas.
- El Archivo General de la Nación ha sido pasivo frente a los procesos de reglamentación de la Ley de Comercio Electrónico y la Ley General de Archivos, en lo atinente a la gestión del documento electrónico.

A partir de esta primera aproximación al estudio de la gestión de documentos electrónicos en la administración pública, fue creciendo el interés de los profesionales de la archivística así como de los entes responsables de la política archivística del país en este tema, situación que condujo a la formulación de diferentes propuestas en el campo de la investigación, la formulación de políticas, la expedición de normas técnicas y directrices que contribuyeran a poner orden al evidente caos.

## II. La gestión de documentos electrónicos frente a la modernización de la administración pública

De acuerdo con Yolanda Martín González,<sup>2</sup> el acceso a los documentos de la administración por parte de los ciudadanos es uno de los principales problemas que se dan dentro de la administración pública en cuanto a la publicación de la información y los documentos. Para Martín la Administración Pública es un sistema de información, compuesto por diferentes subsistemas, uno de los cuales es el Subsistema de Información Administrativo, integrado a su vez por otros subsistemas de información como el de gestión de documentación externa y gestión de documentación interna (Figura 1).

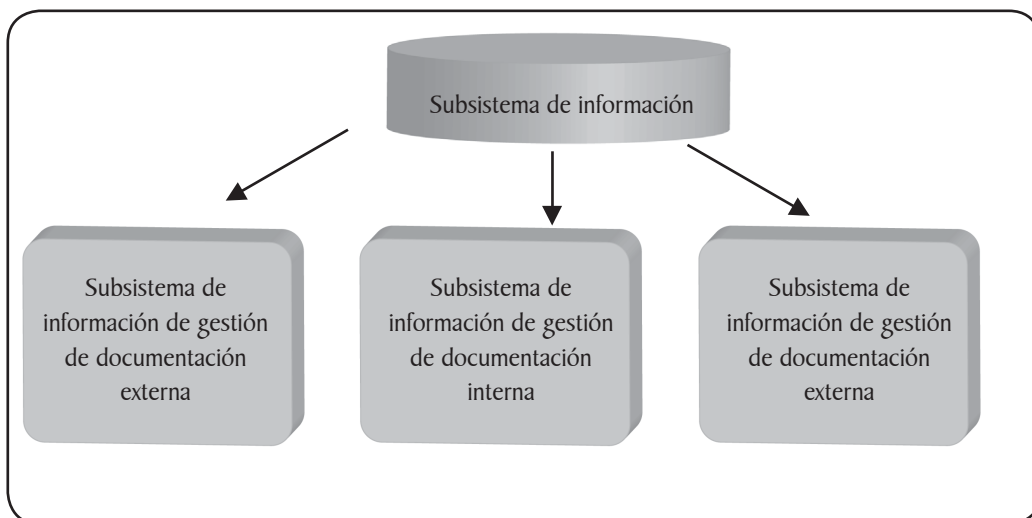


Figura 1. Subsistemas de información en la administración pública.

Fuente: Martín González, Yolanda (2007).

<sup>2</sup> MARTÍN GONZÁLEZ, Yolanda. *El acceso de los ciudadanos a la información y documentación administrativa en la Unión Europea*. Universidad Salamanca, 2007, p. 3.

Según su análisis, algunos de los principios que regulan el funcionamiento de la administración pública son el dar publicidad a los documentos administrativos y el libre acceso a éstos; sobre este particular Martín, citando a Muñoz,<sup>3</sup> identifica varios problemas informativos que se presentan en la mayoría de las organizaciones, tales como excesiva compartimentación de los servicios y la pérdida de calidad en el conjunto de las Administraciones, problemas de estructuración y dispersión de la información, compartimentación de los diferentes departamentos de las Administraciones, el silencio administrativo derivado de la demora en la tramitación de los asuntos y de inadecuados flujos de información, fallas en la estructuración de la información, lo que dificulta su localización e inadecuada comunicación entre Administraciones. Otros hallazgos relevantes del mismo estudio son la “discriminación, falta de información y transparencia, negligencia, incumplimiento de obligaciones, retrasos en los plazos, tratos injustos, abuso de poder y errores jurídicos”, siendo el primer motivo de reclamación la dificultad de acceso a los documentos y la ausencia o denegación de información por parte de las instituciones y órganos comunitarios. Sobre este aspecto la misma autora enfatiza en la obligatoriedad de facilitar la localización de la información, privilegiando el uso de Internet como mecanismo de acceso a los documentos de la administración, proponiendo como estrategia centralizar la información que se encuentra dispersa en distintas bases de datos o puntos de información diferentes.

Una de las principales conclusiones del estudio de la profesora Martín es que las nuevas tecnologías de la información y la comunicación, en particular Internet, han brindado una plataforma extraordinaria para difundir información sobre las actividades de las administraciones y proveer mecanismos que permitan la búsqueda y recuperación de sus documentos.

<sup>3</sup> MUÑOZ CAÑAVATE, A. “Una aproximación a la información del sector público: la información de las administraciones públicas”. En: *Revista General de Información y Documentación*, vol. 11, 1, 2001. p. 37. Citado por Yolanda Martín González.

### III. La Administración electrónica y la gestión documental

Jesús Barroso<sup>4</sup> ofrece una visión general de las iniciativas adelantadas por la Administración General del Estado para impulsar la administración electrónica en España, potenciando los beneficios de la sociedad de la información. Según este autor, la administración electrónica se refiere al uso de las tecnologías de la información y las comunicaciones y particularmente Internet para mejorar el funcionamiento de la administración pública, a través de tres niveles de desarrollo en cuanto a las tecnologías se refiere: un primer nivel que se limita al uso de la tecnología para automatizar los procesos del negocio; un segundo nivel en el cual las administraciones utilizan las tecnologías para gestionar la información, la cual es considerada como un activo estratégico; y, un tercer nivel que utiliza el potencial estratégico de las tecnologías de la información y de las comunicaciones para dar respuesta a problemas que no se habían planteado aún. Una de las causas para que este modelo tuviera éxito tiene que ver con el Plan de Acción e-Europa 2005, aprobado por el Consejo Europeo en 2002, en el cual se definieron 12 servicios públicos dirigidos a ciudadanos y 8 destinados a empresas los cuales debían ser ofrecidos en su totalidad de manera electrónica a través de Internet. En el cuadro siguiente se muestran los niveles de cobertura de los diferentes grupos de servicios implementados en España en la primera década de este siglo:

GRUPO	Servicios ofrecidos	Accesibilidad
GRUPO I	• Pago de impuestos	100%
	• Denuncias ante la policía	100%
	• Servicios de bibliotecas públicas	100%
	• Presentación de impuesto de sociedades	100%
	• Presentación del IVA	100%
	• Declaraciones de Aduana	100%
	• Certificados de nacimiento y matrimonio	100%

<sup>4</sup> BARROSO BARRERO, Jesús. *La administración electrónica en España: análisis de sectores claves. [Documento Electrónico]*. Bogotá: Ministerio de Comunicaciones, Madrid: ICE, 2004. p. 56. ([http://www.revistasice.com/cmsrevistasICE/pdfs/ICE\\_813\\_55-71\\_\\_935E069B5B7805A3C69170C22B198A84.pdf](http://www.revistasice.com/cmsrevistasICE/pdfs/ICE_813_55-71__935E069B5B7805A3C69170C22B198A84.pdf)) Consulta: 27 Abril 2008.

<b>GRUPO 2</b>	• Subsidio al desempleo	50 – 100%
	• Ayuda familiar	50 – 100%
	• Becas de estudio	50 – 100%
	• Reembolso de gastos médicos	50 – 100%
	• Matrícula universitaria	50 – 100%
	• Matrícula de vehículos	50 – 100%
	• Permisos y licencias medioambientales	50 – 100%
	• Citas médicas	50 – 100%
	• Registro de sociedades mercantiles	50 – 100%
<b>GRUPO 3</b>	• Permiso de construcción	Menos de 50%
	• Comunicación de traslados de domicilio	
	• Compras públicas por Internet	
	• Búsqueda de empleo	
	• Obtención de pasaporte	
	• Obtención de permiso de conducir	

De acuerdo con el informe, el 47% de los usuarios de Internet visitan páginas web de la administración y un 13% usan el correo electrónico para comunicarse con entidades del gobierno, mientras que un 17% envían formularios por Internet; en el 2003 existían 2608 portales web de las administraciones públicas y en varios de estos se incorporaron funcionalidades de acceso para discapacitados y en lenguas no oficiales.

Un tema pendiente en este escenario era la falta de un modelo general de coordinación y colaboración; las diferentes administraciones fueron creando servicios a la medida para sus propias necesidades que atendían problemas específicos, lo cual suponía una pérdida de recursos que podían haberse sumado para mejorar los beneficios para toda la administración. Por esta razón, se propuso un Plan de Choque para impulsar la administración electrónica en España, cuyos objetivos eran:<sup>5</sup>

<sup>5</sup> *Ibíd.* p. 63.

- Facilitar el acceso público a los usuarios.
- Impulsar el desarrollo de servicios para los usuarios.
- Facilitar el intercambio de información entre administraciones públicas.
- Apoyar la reorganización interna de la administración pública.

El Plan de Choque contemplaba 19 acciones estratégicas, articuladas al Plan de Acción e-Europa 2005, la última de las cuales se refiere específicamente al sistema de archivo y documentación electrónica. Al revisar detalladamente cada una de las acciones del plan de choque, se hace evidente la relación de la mayoría de estas con la gestión documental, tanto de manera explícita como implícita. El estudio igualmente remarca algunos sectores claves de la e-Administración en España, tales como el pago de obligaciones tributarias y el pago de cotizaciones laborales, su impacto para el ciudadano. Algunas de las conclusiones finales del estudio tienen que ver con aspectos que impactan directamente la gestión documental, tales como mejoras en la gestión pública y una transformación de los procesos y procedimientos del negocio, la integración tecnológica de los procedimientos administrativos en los que interactúan los ciudadanos y la reducción de la brecha digital, de modo que todos los ciudadanos tengan acceso a los beneficios de la administración electrónica.<sup>6</sup>

Complementan los anteriores lineamientos, el estudio realizado por la ONTSI de España en 2009,<sup>7</sup> relacionados con el acceso a documentos de las administraciones locales:

- La información que se ofrece desde las páginas Web de las administraciones, corresponde principalmente a tres categorías: 1) información general del municipio, 2) información y gestión del municipio y, 3) información destinada a empresas.
- La presentación de quejas y denuncias es uno de los servicios que utilizan mayoritariamente los ciudadanos, por encima de la posibilidad de consultar expedientes de la administración.

<sup>6</sup> *Ibíd.* p. 70.

<sup>7</sup> ONTSI. *Estado de las tecnologías de la información y las comunicaciones en la administración local*, Madrid, 2009. p 87-88.

- Casi todas las administraciones cuentan con servicios para realizar trámites electrónicos, aunque solo en la entrada de la información y no para todo el procedimiento.
- No se ha implementado de manera generalizada el uso del DNI electrónico y los certificados digitales.

Un tema relevante tiene que ver con la necesidad de definir un modelo general de coordinación y colaboración en el cual las diferentes áreas de la administración y las entidades creen servicios a la medida de sus propias necesidades, los cuales respondan a problemas específicos; lo anterior evitaría la pérdida de recursos que pueden invertirse para mejorar los beneficios del gobierno electrónico para toda la administración. Barroso propone trabajar en cuatro áreas para impulsar la administración electrónica:<sup>8</sup>

- Facilitar el acceso público a los usuarios.
- Impulsar el desarrollo de servicios para los usuarios.
- Facilitar el intercambio de información entre administraciones públicas.
- Apoyar la reorganización interna de la administración pública.

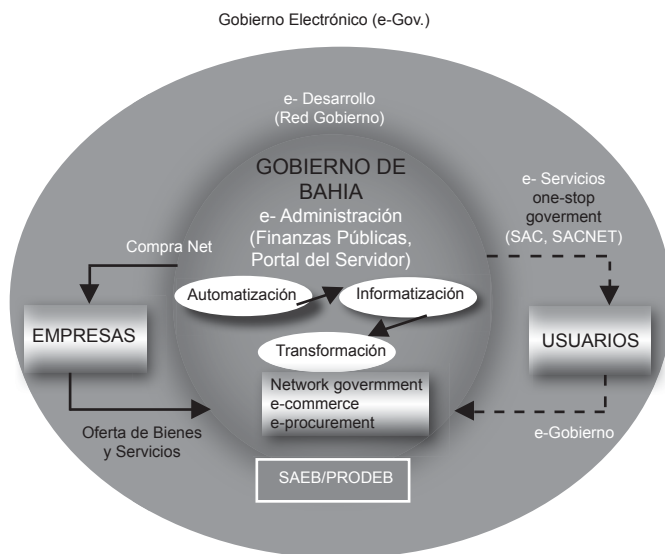
Mario Wohlers,<sup>9</sup> a partir del programa de gobierno electrónico de Bahía (Brasil), cuyo estudio fue realizado en 2003 por el Centro Latinoamericano de Estudios de Economía de las Telecomunicaciones - CELAET, identificó varios resultados de relevancia en las diferentes líneas estratégicas propuestas en aspectos como:

- Incremento del número de atenciones realizadas a los ciudadanos.
- Reducción de tiempo para tramitar documentos.
- Percepción positiva del ciudadano frente a los servicios prestados por la administración del Estado y de los municipios.
- Reducción de costos directos relacionados con la gestión interna de los asuntos de la administración.

<sup>8</sup> *Ibíd.* p. 63.

<sup>9</sup> WOHLERS, Mario. *Gobierno electrónico en Bahía: evolución y servicio de atención al ciudadano*. Salvador de Bahía, 2003, p. 1-2.

- Reducción de los niveles de exclusión digital, gracias a la implementación de servicios móviles.



Fuente: Wohlers a partir de Gordilho (2002)  
Figura 2. Gobierno Electrónico en Bahía (Brasil)

En el estudio de Wohlers se mencionan algunos aspectos que es necesario tener en cuenta en la implementación de la administración electrónica, si se desea asegurar su éxito en el mediano plazo:<sup>10</sup>

- La actualización e integración de las tecnologías y la modernización de las prácticas administrativas son indispensables para atender adecuadamente la creciente demanda de servicios por parte de los ciudadanos.
- Las mejoras en los canales de comunicación son indispensables para potenciar el uso de Internet en la prestación de los servicios para los ciudadanos.
- Las inversiones realizadas deben tener como objetivo central mejorar los servicios, la productividad y la eficiencia de la administración pública del Estado.

<sup>10</sup> *Ibid.*



- El modelo de gobierno electrónico seleccionado debe tomar en cuenta la dispersión geográfica de la comunidad, la concentración de la renta y el nivel educativo entre otros aspectos.
- Los resultados del gobierno electrónico serán mayores en la medida en que exista voluntad y compromiso político de la administración y de los gobernantes.
- Las alianzas estratégicas con el sector privado en la implementación del gobierno electrónico, son una opción que requiere y debe ampliarse, con el fin de lograr resultados satisfactorios en la prestación de los diferentes servicios públicos de la administración.

Visto de esta forma, el gobierno electrónico se refiere al uso de las tecnologías de la información para ampliar el acceso a los diferentes servicios que ofrece el gobierno a los ciudadanos, socios (y proveedores), a los empleados y a otros niveles gubernamentales; existen cuatro direcciones hacia las cuales se dirigen dichas prestaciones y servicios:<sup>11</sup> “el primer tipo (G2C) incluye la diseminación de información al público y de servicios básicos como trámites, impuestos, certificaciones, etc.; el segundo tipo (G2E) se refiere a servicios de información destinada a los empleados de las oficinas del gobierno, tales como planes de entrenamiento y capacitación, concursos, provisión de cargos, etc.; el tercer tipo comprende transacciones entre varios servicios del gobierno (G2B) para el desarrollo de las actividades propias del organismo frente a la comunidad; el último, (G2G) tiene lugar en dos niveles: local entre los diferentes niveles del gobierno e internacional entre gobiernos”.

Como complemento a lo anterior y en desarrollo del gobierno electrónico, han venido apareciendo diferentes prestaciones o servicios para facilitar la interacción entre el gobierno y los ciudadanos, acercando la gestión de la administración pública a los gobernados; algunas de estas prestaciones (e-servicios) pueden ser: trámites aduaneros, certificaciones, comercio electrónico, compras públicas, firma electrónica, impuestos, seguridad social, servicios a

<sup>11</sup> DELOITTE and Touche. *At the Dawn of e-Government: The Citizen as Customer*. Disponible en: <http://www.publicnet.co.uk/publicnet/e000620.htm>, consultado el 15 de enero de 2009.

empresas, voto electrónico, defensoría al cliente o consumidor, participación ciudadana, pagos en línea, matrículas escolares en línea, registro civil, notariado y registro; conforme se transformen y modernicen las entidades públicas, todos o la mayoría de los procesos y trámites de la administración se irán incorporando al modelo e-servicios. De acuerdo con la OUI, la administración electrónica incluye variadas aplicaciones de las TIC como por ejemplo: e-gobierno, e-servicios, e-transparencia, e-contratación, e-gestión, e-control, e-ciudadanía y e-democracia, las cuales pueden darse en el poder ejecutivo, legislativo y judicial; con relación a la jurisdicción territorial, comprende el nivel central, el regional o provincial y el local; respecto de los canales de prestación de los servicios, se incluyen la Web, Gobierno Móvil (m-Gobierno) y otras aplicaciones de las comunicaciones (telefonía móvil, televisión digital, etc.).<sup>12</sup>

Al ser los documentos resultado de las funciones, procesos y actividades que desarrolla una organización, independiente de la forma como estas se llevan a cabo, estos se encuentran en el *back office* de la administración electrónica y por lo tanto no se puede deslindar el ambiente en el cual tienen lugar las relaciones entre el gobierno, los ciudadanos, el negocio y otras instancias gubernamentales, con los procesos de la gestión documental, pues estos son inherentes o consustanciales a tales actividades.

Comprendido lo anterior, se puede afirmar que la gestión de documentos no puede ser vista como un simple conjunto de operaciones y técnicas documentales, por cuanto está articulada con el desarrollo de los procesos de negocio, teniendo un impacto mayor al que durante años se ha defendido; para responder a la complejidad que supone el giro de los negocios de las organizaciones de hoy, cuyo principal componente es el uso de las TIC, es necesario diseñar e implementar Sistemas de Gestión de Documentos (SGD)

<sup>12</sup> GOBERNANZA, GOBERNABILIDAD Y GOBIERNO DIGITAL. En línea: Boletín No.26, Julio 2007. e-Gobierno y Gobernabilidad. Foro e-Gobierno OEA. Consultado el 20 de febrero de 2009. Disponible en <http://www.educoas.org/RestrictedSites/Curso1/Newsletter26.html>. Citado por ZAPATA CÁRDENAS, Carlos. "Implicaciones del gobierno electrónico en la implementación de la gestión documental en la administración pública". En: *Memorias del XVIII Seminario del Sistema Nacional de Archivos* (noviembre 10 al 13 de 2009). Bogotá: Archivo General de la Nación. 2009. p. 4.

que respondan a las necesidades de las empresas de hoy y que contribuyan a resolver los problemas asociados al manejo de los documentos, en el cual el conjunto de elementos relacionados con la gestión documental que interactúen de manera sincronizada y controlada en la creación, conservación, uso y disposición de los documentos de una organización a partir de la aplicación de técnicas administrativas modernas dirigidas a aumentar la eficiencia administrativa, reducir costos y facilitar la gestión administrativa general, a partir de la integración de las diferentes tecnologías de la información y la comunicación, los sistemas de información y la aplicación de los principios básicos de la archivística.<sup>13</sup>

#### **IV. La Gestión de documentos electrónicos en Bogotá: relación con el programa de gobierno en línea (e-Gobierno)**

En 1997 el gobierno colombiano dio inicio a una ambiciosa política del gobierno en cuanto a la aplicación de las tecnologías de la información y la comunicación como estrategia para mejorar la eficiencia y la transparencia del Estado y ampliar el acceso ciudadano a los beneficios de las tecnologías de la información y la comunicación, a la cual denominó *Agenda de Conectividad*, dentro de la cual se formuló una propuesta de gobierno electrónico denominada el *Gobierno en Línea*, orientada a que los diferentes niveles del gobierno (nacional, departamental y local) aprovecharan las posibilidades de Internet para fortalecer y ampliar las relaciones con los ciudadanos, facilitando la realización de trámites, el acceso a la información pública, mejorar los espacios de discusión y asegurar el acceso al conocimiento necesario para el desarrollo de las comunidades.<sup>14</sup>

<sup>13</sup> ZAPATA CÁRDENAS, Carlos. "Implicaciones del gobierno electrónico en la implementación de la gestión documental en la administración pública". En: *Memorias del XVIII Seminario del Sistema Nacional de Archivos* (noviembre 10 al 13 de 2009). Bogotá: Archivo General de la Nación. 2009.

<sup>14</sup> ZAPATA CÁRDENAS, Carlos. *La gestión documental en el desarrollo de los proyectos de administración electrónica: estado de la cuestión en la administración distrital de Bogotá*. Salamanca: Universidad de Salamanca, 2010. [Trabajo de investigación presentado para optar al Grado de Salamanca]. p. 75.

Los ejes sobre los cuales se sustenta la estrategia del Gobierno en Línea son:<sup>15</sup> la eficiencia, eficacia y calidad de los servicios prestados; la publicidad de la información; la integración de los sistemas y la eficiencia de la gestión interna del Estado. Aunque la política pública de información se ha venido formando de manera progresiva en los últimos años, los avances mencionados se concentraban en las entidades del gobierno central, con incipientes resultados en el gobierno local. A su vez, el Decreto 1151 de 2008 definió los lineamientos y mecanismos necesarios para que todas las entidades del Estado pudieran lograr, a corto plazo, la implementación de la estrategia de Gobierno en Línea, para lo cual debían diseñar un plan de acción para este propósito.

De acuerdo con lo anterior, en el Distrito de Bogotá mediante el decreto distrital 619 de diciembre 28 de 2007 se estableció la Estrategia de Gobierno Electrónico para todas las entidades del distrito. Entre los elementos de dicha estrategia se definieron como principios la celeridad de las actuaciones de la administración distrital y la reducción de los costos de los trámites, procesos y procedimientos, elementos que hacen parte según los planteamientos de la UNESCO de una buena gestión documental. En esta norma se define que la estrategia de gobierno electrónico se debe llevar a cabo de manera coordinada entre diferentes organismos de la administración distrital, uno de los cuales es el Archivo de Bogotá, junto con la Comisión Distrital de Sistemas, la dirección Distrital de Servicio al Ciudadano y la Dirección Distrital de Desarrollo Institucional. Como complemento a lo anterior, la Comisión Distrital de Sistemas —CDS— expidió la Resolución 378 de diciembre 19 de 2008, mediante la cual se adoptó la *Guía para el diseño y desarrollo de sitios Web de las entidades y organismos del Distrito Capital*.<sup>16</sup>

El alcance fijado por el Distrito, contemplaba los siguientes ámbitos de aplicación de la estrategia de gobierno electrónico de la ciudad, así:<sup>17</sup>

<sup>15</sup> MINISTERIO DE COMUNICACIONES. *Manual para la implementación de la estrategia de gobierno en línea en la república de Colombia*. Bogotá; Ministerio de Comunicaciones, 2008. p. 9.

<sup>16</sup> ZAPATA CÁRDENAS, Carlos. *Op. cit.* p. 82.

<sup>17</sup> ALCALDÍA MAYOR DE BOGOTÁ. Decreto 619 de septiembre 18 de 2009. Artículo 2º.

- La visión, objetivos, alcance, etapas, acciones y plazos.
- El Plan de Acción que agrupará los diferentes planes sectoriales e intersectoriales en materia de automatización de trámites.
- Los estándares, las reglas técnicas, las condiciones de uso y la política de privacidad de los servicios al ciudadano, realizados a través de mensajes de datos, que suministren los organismos y las entidades de Bogotá, Distrito Capital.
- Los estándares, reglas y mecanismos para la producción, administración, almacenamiento y servicio de los documentos que son el registro de las actuaciones, actos y procedimientos administrativos.
- Las acciones y mecanismos para facilitar el acceso de los ciudadanos a los servicios y trámites electrónicos.
- Los mecanismos de coordinación sectorial e intersectorial en materia de automatización de trámites y servicios.
- Los mecanismos de seguimiento y actualización de los diversos componentes de la estrategia.

Estas disposiciones dieron solidez a lo establecido por el gobierno distrital en el artículo 5º del acuerdo 257 de 2006, según el cual “las actuaciones administrativas de todo el distrito deberán ser públicas y estar soportadas en tecnologías de información y comunicación, de manera que facilite el acceso a la información oportuna y confiable que permita el ejercicio del control ciudadano, político, fiscal, disciplinario y de gestión o administrativo”.

Con el fin de medir hasta donde la administración distrital había logrado articular el gobierno electrónico con la gestión de documentos, se llevó a cabo un proyecto de investigación<sup>18</sup> cuyos resultados ofrecen una visión general de la relación entre estos dos programas del gobierno distrital. Algunos de los resultados de la investigación

<sup>18</sup> Esta investigación fue desarrollada durante 2008 como parte de los estudios de *Doctorado en Metodologías y Líneas de Investigación en Biblioteconomía y Documentación* que el autor adelanta actualmente en la Universidad de Salamanca, la cual fue presentada en 2010 como trabajo de grado para obtener el Grado de Salamanca.

permitieron indagar sobre los diferentes subprogramas de gestión documental que se vienen implementando en el distrito, y muestran un nivel de desarrollo muy avanzado en tres aspectos: archivos de oficina, gestión de correspondencia y tablas de retención documental; un resultado interesante es la implementación de la gestión documental por procesos en la mayoría de las entidades analizadas; el estudio arrojó que los aspectos relacionados con documentos electrónicos presentan rezago frente a otros aspectos del Programa de Gestión de Documentos del Distrito. Esta conclusión está relacionada principalmente con la gestión de los sistemas de información de la ciudad, que según un estudio de la Contraloría de Bogotá, realizado en 2007 están desarticulados y no cuentan con un modelo de gestión de documentos e información uniforme, aumentando los problemas derivados del manejo del documento electrónico de la capital.

Las principales debilidades de la gestión de documentos electrónicos, según la investigación, se encuentran en las áreas de gestión de la reprografía, gestión del correo electrónico, gestión de documentos ofimáticos y gestión de archivos vitales o esenciales, aspectos que los responsables de la gestión documental en cada una de las entidades del distrito valoraron con un nivel de avance mínimo.

En relación con la participación de archivistas y responsables de gestión documental en el desarrollo de algunas de las prestaciones del gobierno electrónicos (gobierno en línea) del distrito, la investigación mostró que a pesar de que la mayoría de dichas prestaciones están asociadas al diseño y uso de documentos electrónicos (formas y formularios principalmente), ninguno ha colaborado en la implementación de estos servicios (e-servicios) desde el aspecto documental. En general, la investigación permitió corroborar que los directores de las áreas de informática (TI) y los administradores de los sitios web tienen una mayor participación en el desarrollo de las prestaciones y mecanismos del gobierno electrónico, frente a una participación muy reducida de los archivistas:

Lo anterior es un indicador de que los archivistas no se han insertado de manera apropiada en el desarrollo de los diferentes proyectos que se vienen llevando a cabo en cuanto al gobierno electrónico de la ciudad, situación que tiene implicaciones respecto de su papel

como gestores de información para el gobierno y para la ciudadanía, limitando su accionar a un ámbito meramente técnico en cuanto a la organización de la información y a su adecuada conservación, sin desconocer que desde el 2009 se han comenzado a vincular archivistas en este tipo de iniciativas. Adicionalmente, de acuerdo con los resultados de las encuestas realizadas, no todos los archivistas y responsables de la gestión documental del distrito están preparados adecuadamente para poder asumir el reto que significa su participación en el desarrollo de las diferentes prestaciones y proyectos relativos a la administración electrónica.

Finalmente, resulta muy significativo que a pesar de que existe un relativo grado de conocimiento sobre los objetivos del gobierno electrónico por parte de los funcionarios de gestión documental del distrito, los archivos están ausentes de tales objetivos. De acuerdo con la investigación, se observa que si bien un alto porcentaje de las entidades viene adelantando proyectos que permitan el acceso Web a los archivos, no se publican por ejemplo los cuadros de clasificación y mucho menos las tablas de retención documental en la página Web de la entidad. Adicionalmente, existen una serie de servicios como el acceso en línea a documentos públicos y la publicación de otras categorías de documentos acerca de las actuaciones de la administración distrital, que aunque, según los encuestados, se están adelantando en el momento, no tienen un claro horizonte para su implementación o desarrollo.

## **V. Avances logrados en la adaptación de la gestión de documentos al gobierno electrónico en Bogotá**

En el año 2001 se creó el Sistema Distrital de Información —SDI—, integrado por el conjunto de las “políticas, estrategias, metodologías, procedimientos, bases de datos, plataformas tecnológicas y sistemas de información que deben aportar todas las entidades de distrito”<sup>19</sup> con el objetivo de “facilitar el control político, contribuir a la participación

<sup>19</sup> CONTRALORÍA DE BOGOTÁ. *Los sistemas de información distrital*. Bogotá; Contraloría Distrital de Bogotá, 2007. p. 31.

ciudadana y ser una herramienta para consolidar el gobierno electrónico de la administración distrital”,<sup>20</sup> como complemento de lo cual el acuerdo 119 de 2004, determinó que el SDI debía garantizar a la administración y a la ciudadanía, la oportunidad y confiabilidad en los datos suministrados. En desarrollo de esta directriz, la administración distrital de Bogotá ha venido trabajando en diferentes iniciativas que permitan consolidar una gestión documental moderna, acorde con los niveles de desarrollo de las diferentes entidades del distrito, de forma que “los procesos, actividades y tareas de los sistemas de archivos, garanticen que los documentos producidos por una entidad y sus dependencias se acopien, procesen y conserven de tal forma que cuando sean requeridos se puedan buscar, localizar y poner al servicio de los usuarios en el menor tiempo posible”.<sup>21</sup> Una de estas iniciativas fue la creación, a instancias de la Ley 489 de 1998 (art. 30 y art. 37), de los Subsistemas Internos de Gestión Documental y Archivos – SIGA. El objetivo del SIGA es que los documentos producidos o recibidos cotidianamente en las oficinas de las diferentes entidades del distrito se puedan consultar por los funcionarios y ciudadanos para fines tales como la toma de decisiones, el control, la veeduría o como garantía de derechos; además de ser preservados como parte de la memoria de la ciudad.

De otro lado, el desarrollo de los programas y planes de gobierno electrónico y gestión documental, tienen un origen prácticamente simultáneo (2000 y 2001 respectivamente); en un principio las iniciativas que posteriormente derivaron en los programas de *gobierno electrónico y gestión documental* de la administración distrital no tenían relación alguna entre ambas; mientras que la responsabilidad sobre las aplicaciones de la estrategia de *Gobierno en Línea* recayó sobre la Comisión Distrital de Sistemas, lo relacionado con la *Gestión Documental* del Distrito quedó en cabeza del Archivo de Bogotá. La ausencia de articulación inicial entre ambos programas se debe a que para el año 2002, el Archivo de Bogotá no tenía relación con la Comisión Distrital de Sistemas en el año 2002, la cual

<sup>20</sup> *Ibíd.*

<sup>21</sup> ALCALDÍA MAYOR DE BOGOTÁ. *Guía de procedimientos de la gestión documental orientada a procesos*. Bogotá; Imprenta Distrital, 2007. p. 9.



estaba integrada por diferentes entidades o dependencias de la Alcaldía. En dicha estructura no figuraba el Archivo de Bogotá, entidad que para la fecha ya venía adelantando diferentes proyectos relativos a la gestión documental y que para entonces comenzaba a expresar su preocupación por el impacto que las TIC tenían sobre la gestión de documentos en el distrito; a pesar de lo anterior, la participación del Archivo de Bogotá en la Comisión Distrital de Sistemas era prácticamente inexistente; en adición a lo anterior en el año 2007, cinco años después de creada esta Comisión, la Contraloría de Bogotá adelantó un estudio sobre los Sistemas de Información del Distrito,<sup>22</sup> el cual evidenció la existencia de “problemáticas en los SI de las entidades del distrito”, dificultando los servicios a los ciudadanos y la garantía de que los gestores públicos cuentan con información adecuada para la toma de decisiones; aunque el estudio se centró en el análisis de los sistemas de información desde la perspectiva fiscal (utilización vs. Inversión), solo se hace mención en algunos apartados del mismo a la gestión de documentos, a pesar de la relación existente entre estos dos componentes de la gestión de información del Distrito.

En el año 2008, la administración distrital creó el *Comité para el Gobierno en Línea* coordinado por la Comisión Distrital de Sistemas e incorporó al mismo como un invitado permanente el Archivo de Bogotá, lo cual ha permitido un cambio de política en cuanto al papel que debe jugar este organismo y la importancia de la gestión de documentos en los lineamientos que deben regir la implementación del gobierno electrónico de la ciudad capital.

Aunque lo anterior supone un cambio de rumbo en el desarrollo del gobierno electrónico de la ciudad y la alineación de éste con la gestión documental y viceversa, los resultados de la investigación realizada permitieron identificar algunos aspectos que es preciso mejorar en el futuro:<sup>23</sup>

- I. Las diferentes entidades del distrito vienen trabajando de manera independiente en el desarrollo de la estrategia de gobierno en línea de Bogotá (gobierno electrónico), con resultados que se pueden calificar como incipientes. Aunque la Comisión

<sup>22</sup> CONTRALORÍA DE BOGOTÁ. *Op. cit.* p. 5.

<sup>23</sup> ZAPATA CÁRDENAS, Carlos. *Op. cit.* p. 115.

Distrital de Sistemas tiene como objetivo articular el desarrollo del Plan Maestro de Telecomunicaciones, dentro del cual se inserta la estrategia de gobierno electrónico, cada entidad parece tener prioridades diferentes en cuanto a su implementación, los servicios que se deben establecer y los objetivos que se persiguen.

2. Las entidades del distrito están avanzando de manera dispar en la implementación de los mecanismos y servicios del gobierno electrónico; solo hasta finales del 2009 se espera contar con un Plan de Gobierno Electrónico articulado con líneas de acción claramente definidas y con plazos sobre las metas a lograr.
3. Ante la falta de una hoja de ruta del gobierno electrónico para todo el distrito capital, cada entidad definió sus propios planes e itinerarios para el desarrollo de las prestaciones y servicios de la estrategia de gobierno en línea de acuerdo con sus propias necesidades, posibilidades técnicas y recurso humano.

Actualmente se está trabajando tanto en la formulación de un documento de Estrategia del Gobierno Electrónico de Bogotá como en las directrices para la automatización y la administración de los documentos basados en mensajes de datos que se generen en las actuaciones, actos y procedimientos administrativos que se adelanten ante las entidades distritales, a partir de cuyo momento se deberían alinear los objetivos del gobierno electrónico y los objetivos de la gestión documental en las aplicaciones y desarrollos que involucren la gestión de documentos electrónicos.

Aunque este plan de choque busca corregir el desfase entre los dos programas, el desarrollo del gobierno electrónico de Bogotá en cuanto a la gestión documental sigue siendo débil, no por ausencia de políticas en esta materia, sino por la ausencia de resultados en este aspecto. A pesar de que el decreto 619 de 2007 definió una serie de directrices respecto del manejo de los documentos, las normas se limitan a algunos de los ámbitos de aplicación de la gestión documental, dando mayor prioridad a los aspectos tecnológicos de la estrategia que a los aspectos de contenido, los cuales provienen de la interacción entre usuarios y entidad (solicitudes, trámites, debates y foros, preguntas, etc.); o de la gestión de

la propia institución (decisiones y actos administrativos, noticias, informes y eventos, etc.).<sup>24</sup>

En este sentido, algunas de las disposiciones que el distrito de Bogotá ha formulado dentro de la estrategia del gobierno en línea, tienen una relación directa con un programa de gestión de documentos electrónicos. Un ejemplo de lo anterior se encuentra en el decreto 619 de 2007, que explícitamente señala:

- Las entidades que automaticen sus actuaciones, actos y procedimientos (registradas casi en su totalidad en documentos) que gestionen en el ejercicio de sus funciones deberán asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la administración y la conservación de los datos e información.
- Los mensajes de datos utilizados en las actuaciones y actos administrativos que adelanten las Entidades Distritales en el marco del gobierno electrónico tendrán eficacia, validez y fuerza probatoria.
- Conforme a lo señalado en el artículo 6º de la Ley 962 de 2005, los actos y documentos administrativos que se realicen a través de mensajes de datos producirán todos los efectos jurídicos, siempre que se verifique la identidad del emisor del acto o documento, así como la fecha y hora de envío y recepción del mismo.
- La Secretaría General de la Alcaldía Mayor de Bogotá definirá las normas para emitir copias de actos administrativos basados en mensajes de datos y las reglas para permitir su acceso o remisión a otras dependencias públicas.
- Las Entidades Distritales emitirán los actos administrativos para habilitar o colocar a disposición de los ciudadanos los formularios basados en mensajes de datos, cuyo diligenciamiento se exija para adelantar los trámites y actuaciones administrativas o para presentar peticiones a la Administración.
- Las Entidades Distritales proveerán los medios a los ciudadanos para la presentación, registro, radicación y recepción de solicitudes, peticiones, escritos, quejas, comunicaciones y recursos en forma de mensajes de datos.

<sup>24</sup> ALCALDÍA MAYOR DE BOGOTÁ. Guía para sitios web del distrito capital. En línea. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34525#0>. Consultado el 20 de mayo de 2009.

- La información y documentos que presenten los ciudadanos en forma de mensajes de datos, estarán sujetas a reglas mínimas como:
  - o Presentación, contenido y estructura íntegra y sujeta a formatos estándar de presentación de la información.
  - o Suministrar los datos personales del remitente y del interesado.
  - o Registrar la fecha y la hora de envío y recepción de la solicitud, petición, comunicación o recurso.
- Para la notificación y publicación de los actos administrativos como resultado de las actuaciones y trámites administrativos adelantados por las entidades del Distrito Capital podrán utilizarse mensajes de datos, conforme a las siguientes reglas:
  - o Cuando el interesado acepte expresamente su utilización.
  - o En toda actuación administrativa se solicitará al interesado, al iniciar la gestión, una dirección de correo electrónico tanto para enviar notificaciones como para comprobar su identidad.
  - o La dirección de correo electrónico podrá ser revocada por el interesado en cualquier momento.
  - o Se utilizarán métodos de autenticación para la notificación de los mensajes de datos.
  - o Se debe contar con un mecanismo de acuse de recibo de los mensajes que envíen y reciban los ciudadanos.
  - o De toda notificación se dejará constancia a través de un mensaje de datos, el cual hará parte del expediente respectivo. El sistema de notificaciones deberá registrar la fecha y la hora en la que se coloque el acto notificado a disposición y acceso del interesado.
  - o El sistema de notificaciones debe incorporar en los documentos y actos a notificar, la información que sea obligatoria de acuerdo con la ley y observar en todo caso los plazos o términos que se establezcan en las normas procesales.
  - o El sistema de notificaciones debe observar las garantías definidas en las leyes procesales.

- Se fijan reglas para la computación de los plazos sobre las actuaciones, actos y procedimientos administrativos que se realicen a través de mensajes de datos:
- Cuando cualquier persona presente peticiones, quejas, reclamaciones o recursos basados en mensajes de datos se entenderán recibidos por la entidad en el momento en que el sistema de información de la entidad genere el acuse de recibo junto con el número de radicación consecutiva que genere automáticamente el sistema.
- Las entidades del distrito deberán llevar un estricto control y relación de los mensajes recibidos en su sistema de información.
- Conforme a lo expresado en la Ley 962 de 2005 la Secretaría General emitirá las directrices para desarrollar los siguientes aspectos de la automatización de las actuaciones, actos y procedimientos administrativos frente al ciudadano:
  - o Conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesado.
  - o Sistemas tecnológicos para otorgar las citas de atención de manera automática y oportuna sin necesidad de presentación personal.
  - o Medios de pago electrónico que apoyen los servicios y trámites.
- Las entidades de la Administración Distrital deberán disponer de los medios tecnológicos para el almacenamiento, conservación y servicio de los documentos basados en mensajes de datos.
- Las políticas y normas de administración y conservación de documentos basados en mensajes de datos se formularán conforme al Decreto Distrital 514 de 2006.




A pesar de que todas las disposiciones anteriores corresponden al alcance de un programa de documentos electrónicos, los resultados de la investigación mostraron que los aspectos relativos a los mensajes de datos (documentos electrónicos) están siendo trabajados principalmente desde el campo de actuación de las áreas de informática, sin una activa participación de los archivos del distrito.

Sin embargo, lo que resulta claro es que la actual administración del Archivo de

Bogotá está realizando ingentes esfuerzos para articular las políticas de gestión documental del distrito, con las decisiones en materia de sistemas y tecnologías de la información y la implementación de los diferentes servicios y prestaciones del gobierno electrónico de la ciudad; una de estas decisiones tiene que ver con la formulación de un marco normativo que asegure la concentración, organización y preservación del archivo digital del Distrito, proyecto que avanza rápidamente. En el corto plazo se podrán comenzar a ver algunos de los resultados en esta materia, de forma que se puedan mostrar acciones concretas frente a la gestión del documento electrónico de la administración distrital.





## VI. Recomendaciones para integrar la gestión de documentos electrónicos en la administración electrónica

A partir de los resultados de la investigación se presentan una serie de recomendaciones que podrían contribuir a potenciar los alcances de la administración y el gobierno electrónico:<sup>25</sup>

-  La implementación de las prestaciones y servicios de la administración electrónica, debe ser analizada desde una perspectiva interdisciplinaria y no exclusivamente tecnológica. El desarrollo del *e-gobierno* debe ser precedido de políticas coherentes, integrales, apoyadas en un marco legislativo acorde con la institucionalidad y las condiciones de cada país, ciudad o región.
-  En la conformación de los Comités para el *e-gov* se debe incluir a los archivistas o responsables de gestión documental de cada entidad, cuya participación es fundamental tanto en la planeación como en el desarrollo de las acciones de gobierno en línea.
-  Las exigencias que plantea el gobierno electrónico, unidas a los retos que se avecinan en el manejo de los documentos electrónicos y los riesgos propios de

<sup>25</sup> ZAPATA CÁRDENAS, Carlos. *Op. cit.* p. 163.

las tecnologías, hacen necesario adecuar el perfil de los archivistas en cuanto a los conocimientos, habilidades y competencias necesarias para apoyar esta transición hacia este nuevo modelo.

-  Las políticas sobre gobierno electrónico deben incluir el componente de gestión documental y gestión de archivos, y deben involucrar los principios de la teoría y la gestión documental moderna; dicho componente debe ser elaborado exclusivamente por los entes que regulan la política archivística (nacional, regional o local), en cabeza de los archivistas, por ser estos quienes pueden ofrecer una visión adecuada de la gestión de la información y los documentos.
-  El proceso de implementación del e-gobierno, debe armonizarse con el proceso de implementación del programa de gestión documental, de forma que cada fase del *e-gov*, cuente a la vez con su propia fase de gestión documental; de igual forma, es necesario que las dimensiones del e-gobierno (G2G, G2C, G2B y G2E) se armonicen entre si, en términos de los objetivos y aplicaciones de la gestión documental.
-  El desarrollo de Sistemas de Información de cualquier tipo en una organización debe contemplar la participación de archivistas, con el fin de asegurar una gestión documental que responda eficazmente a los objetivos del gobierno electrónico. La arquitectura de información y la plataforma tecnológica del gobierno electrónico, debe apoyarse en los conocimientos de los profesionales de la Archivística, para la construcción de taxonomías, clasificación del conocimiento, organización de la información, búsqueda y recuperación, análisis de información, descripción y metadatos, entre otros campos en los cuales dichos profesionales se desempeñan
-  El modelo de gobierno electrónico está conformado por dos capas denominadas *front office* y *back office*, la primera se refiere a las prestaciones que facilitan las relaciones del gobierno con el ciudadano y la población; el *back office* se refiere a los procesos internos que permiten que dicha interacción tenga lugar; sin embargo, del análisis realizado se desprende la necesidad de contar con una capa intermedia que integre las prestaciones del *front office* con los procesos realizados en el *back office*.

Esta capa intermedia sería el *middle office* del e-gobierno y estaría conformado por los procesos de gestión de la información (incluyendo la gestión documental) y las tecnologías necesarias para soportarlos, así como por la estructura encargada de su operación.





---

Raimon Nualart  
Miquel Serra

---

Transfiriendo **documentos electrónicos**  
auténticos hacia un repositorio digital seguro:  
el caso catalán (la plataforma IARXIU)



## Mercadé

Licenciado en Historia del arte por la Universidad Autónoma de Barcelona (2002).  
Graduado Superior en Archivística y Gestión de Documentos, con postgrado  
en Gestión de Documentos electrónicos por la misma Universidad.  
Responsable de la gestión documental y archivo en la Agencia  
Catalana de Certificación (CATCert) y responsable del  
Servicio iArxiu (Servicio de custodia y preservación  
de documentos electrónicos a largo plazo).



## Fernández

Es licenciado en historia por la Universidad de Girona (1999), con maestría en Gestión  
de Documentos y Archivística por la Universidad Autónoma de Barcelona y la  
Asociación de Archiveros de Cataluña (2002). Ha ocupado cargos como asis-  
tente técnico del Archivo Histórico Comarcal de Santa Coloma de Farnes,  
el Archivo Nacional de Cataluña y el Archivo Municipal de Vidreres y como  
gestor de documentos de los Archivos de la Universidad de Girona.  
Colabora en varios grupos de gestores de documentos y archivistas  
en Cataluña, España, así como en universidades. Pertenece al  
Consejo de la Asociación de Archiveros de Cataluña, y es  
director del TEAM Catalonia del Proyecto InterPARES

## I. Sumario

Este artículo se divide en dos partes, en la primera se exponen aquellas cuestiones relativas a la transferencia de documentos electrónicos auténticos y, especialmente, de aquellos que serán preservados a largo plazo. Estas cuestiones se enfocan desde dos puntos de vista, el teórico y el práctico. En el teórico, a partir del análisis de las normativas internacionales y nacionales y de los estándares, se definirá el concepto transferencia y también las directrices y recomendaciones en la transferencia de documentos electrónicos. En el práctico, se definirá el procedimiento de transferencia (*workflow*) y los metadatos asociados a la transferencia. En la segunda parte del artículo, se exponen aquellas cuestiones relativas a la plataforma iArxiu como solución funcional y tecnológica de archivo electrónico y preservación digital de documentación electrónica para las administraciones públicas en Cataluña (España), desarrollado por la *Agència Catalana de Certificació* (CATcert).

## II. El contexto

El contexto del presente artículo se centra en una de las diferentes necesidades —de las cuales se tiene que dar respuesta por parte de los profesionales archiveros/eras— por lo que respecta a la gestión de la documentación electrónica, en concreto, a la transferencia de documentación electrónica. El macro de fondo es que en Cataluña algunas organizaciones<sup>1</sup> poseen o están en vías de comprar un gestor de documentos y, entre otras preocupaciones en torno a la implantación de este producto informático, se deberán definir, planificar y ejecutar los procedimientos de transferencias de la documentación electrónica (híbrida o

<sup>1</sup> Por ejemplo, en el caso de las universidades públicas catalanas, durante el 2009 se iniciaron diferentes procedimientos de contratos administrativos para comprar un gestor documental. Este dato indica la preocupación de las organizaciones para la gestión de la documentación que poseen, sobretodo, a corto plazo de la documentación electrónica, pero, sin dejar de lado la gestión de documentos en soportes tradicionales o híbridos.

convencional inclusive) hacia repositorios digitales seguros (iArxiu)<sup>2</sup>. Los objetivos de este procedimiento son:

- Cumplir con la legislación española y catalana vigente sobre gestión de documentación electrónica (transferencia).<sup>3</sup>
- Cumplir con las normativas y estándares internacionales y nacionales por lo que respecta a la transferencia.
- Identificar y exponer las directrices, pautas y recomendaciones básicas a tener en cuenta en la transferencia de documentación electrónica (diseño, planificación, ejecución etc.).
- Definir un procedimiento de transferencia “estándar” de documentación electrónica hacia un repositorio digital seguro.
- Garantizar la preservación de la documentación electrónica auténtica a largo plazo.
- Definir las plantillas y esquemas de metadatos asociados al procedimiento de transferencia y a los documentos electrónicos.

### III. La transferencia: concepto y definición

A continuación se proponen algunas definiciones del concepto transferencia a través de las normativas internacionales y estándares nacionales:

<sup>2</sup> Como se comentará en la segunda parte de este artículo, en Cataluña la solución funcional y tecnológica de archivo electrónico seguro es iArxiu, proyecto desarrollado por el CATcert. Esto hace que aquellas organizaciones que quieran integrar sus gestores documentales a iArxiu tendrán que desarrollar procedimientos específicos.

<sup>3</sup> Legislación española: Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE número 150 de 23/6/2007), Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE núm. 304, de 20-12-2003, pp. 45329-45343), Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (BOE número 312 de 29/12/2007), y, Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE, núm. 25, de 29-01-2010).Y, Legislación catalana: *Decret 56/2009, de 7 d'abril, per a l'impuls i el desenvolupament dels mitjans electrònics a l'Administració de la Generalitat.* (DOGC núm. 5360 - 16/04/2009).

Tabla 1 – El concepto terminológico de la transferencia.

Fuentes	Definiciones <sup>4</sup>
ISO 15489 1 y 2: 2001 – versión en catalán, pp. 8	Transferència (transfer): <custòdia> Canvi de la custòdia, la propietat o la responsabilitat dels documents. Transferència (transfer) <moviment> Canvi d'emplaçament dels documents
OAIS model - CCSDS 650.0-B-1 (January 2002), pp. 1-11. <sup>5</sup>	Ingesta: The OAIS entity that contains the services and functions that accept Submission Information Packages from Producers, prepares Archival Information Packages for storage, and ensures that Archival Information Packages and their supporting Descriptive Information become established within the OAIS.
Principles and Functional Requirements for Records in Electronic Office Environments: Modules 1 - 3 (CIA ICA). <sup>6</sup>  Versión catalana pendiente de publicación por parte de la Associació d'Arxiviers de Catalunya (AAC).	Procés de disposició que consisteix en una exportació (amb confirmació) de documents d'arxiu electrònics i metadades associades i, si s'escau, d'agregacions de documents d'arxiu electrònic al qual segueix la seva destrucció al sistema corporatiu des d'on s'han exportat. Les transferències es produeixen d'una organització a una altra quan hi ha hagut canvis administratius, d'una organització a custòdia arxivística, d'una organització a un proveïdor de serveis, del govern al sector privat o entre governs. (Font: Adaptat a partir de The National Archives (Regne Unit), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, pàg. 6.)
International Records Management Trust: Training in electronic records management (Glossary), pp. 40. <sup>7</sup>	Transfer: In a records and archives environment, the act of changing the location or ownership of, and / or responsibility for, records. Transfer schedule. See Retention and disposal schedule.  Retention and disposal schedule: A document identifying the records of an organisation or administrative unit and specifying which records should be preserved permanently as archives and which can be destroyed after a certain period as obsolete or superseded. The retention and disposal schedule provides on going authorisation for the transfer of records from offices to records centres, along with the destruction of obsolete records and the preservation of archival materials. Also known as a disposal list, disposition schedule, records schedule, retention schedule or transfer schedule

<sup>4</sup> Se utilizan tres idiomas en las definiciones del concepto *transferencia* (catalán, castellano e inglés) según la fuente que se ha consultado, el motivo principal es que no haya ningún error de traducción que lleve a confusión / interpretación.

<sup>5</sup> Véase <http://public.ccsds.org/publications/archive/650x0b1.pdf> (2010/02/15).

<sup>6</sup> Véase: <http://www.ica.org/en/2008/02/26/principles-and-functional-requirements-records-electronic-office-environments-call-com> (2010/02/15).

<sup>7</sup> Véase [http://www.irmt.org/documents/educ\\_training/term%20modules/IRMT%20TERM%20Glossary%20of%20Terms.pdf](http://www.irmt.org/documents/educ_training/term%20modules/IRMT%20TERM%20Glossary%20of%20Terms.pdf) (2010/02/15).

MoReq 2 (Model Requeriments for the Management of Electronic Records 2). <sup>8</sup>	Transfer: Organisations may need to move records from their ERMS to other locations or systems for archival or other purposes. This is referred to here as "transfer".
Manual d'Arxivística i Gestió documental, pp. 295. <sup>9</sup>	S'entén per transferència l'operació física de traslladar la documentació des d'un arxiu de gestió als dipòsits d'un arxiu central. És una acció que implica alhora un traspàs de responsabilitats directes sobre els documents i la seva gestió, per la qual cosa s'ha de fer sempre de manera documentada.
Vocabularis de metadades, del grup d'Innovació Tecnològica, pp. 8 y 11. <sup>10</sup>	Paquet d'Informació de Transferència, PIT (Submission Information Package, SIP, segons terminologia OAIS): documents transferits pels productors de la documentació que inclouen els continguts a preservar i les metadades que faciliten la seva recuperació, tractament i preservació.
The society of American Archivists –SAA. (Glossary of Archival and Records Terminology). <sup>11</sup>	n. ~ Records · The process of moving records as part of their scheduled disposition, especially from an office to a records center, or from a records center to an archives. Notes Transfer may involve a change in custody without a change in title.

Del análisis de estas definiciones se derivan toda una serie de cuestiones claves que se deben tener en cuenta al diseñar, definir y ejecutar un procedimiento de transferencia de documentación electrónica hacia un repositorio digital seguro, lo cual implica: el traspaso legal y físico (movimiento) y de responsabilidades en la gestión de los documentos (establecer contratos/convenios/formulario de transferencia entre productores y preservadores), el cambio de custodia de la documentación transferida y también la verificación y la revisión del material digital transferido.

De otra parte, en Cataluña, el grupo de trabajo TEAM Catalonia, dentro del Proyecto

<sup>8</sup> Véase <http://www.moreq2.eu/> (2010/02/15).

<sup>9</sup> VVAA. *Manual d'Arxivística i Gestió Documental*. Barcelona, Ed. Associació d'Arxivers de Catalunya, 2009, página 295.

<sup>10</sup> Véase [http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425\\_vocabularis.pdf](http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425_vocabularis.pdf) (2010/02/15).

<sup>11</sup> Véase [http://www.archivists.org/glossary/term\\_details.asp?DefinitionKey=470](http://www.archivists.org/glossary/term_details.asp?DefinitionKey=470) (2010/02/15).

Internacional InterPARES 3, en el desarrollo del estudio general terminológico<sup>12</sup> está trabajando para poder ofrecer una propuesta de definición para el concepto de transferencia. Desde la dirección del grupo de trabajo se propuso, en la última reunión, como definición de transferencia (contextualizado en el marco profesional y archivístico catalán) *el traspaso legal y de custodia lógica de la documentación desde los productores hacia un archivo (preservador), como centro y servicio especializado en la custodia y preservación de la documentación electrónica.*

#### **IV. Directrices, pautas y recomendaciones sobre transferencia: fuentes y referentes metodológicos**

##### **a) Normas y estándares internacionales y nacionales**

La ISO 15489-1:2001<sup>13</sup> menciona que en la implementación de la disposición (apartado 9.9), las normas de disposición establecen la retirada de documentos fuera de los sistemas operativos que se han de aplicar a esos documentos, de manera sistemática y regular, y, éstas no se pueden aplicar si no se tiene la certeza que los documentos ya no son útiles, no tienen tareas pendientes o que no hay ningún litigio o investigación en curso. La acción de disposición puede comprender respecto a la transferencia: transferencia a un área o soporte de almacenamiento adecuados bajo el control de la organización, la transferencia a otra organización que haya asumido la responsabilidad de la actividad del negocio a través de la venta, reestructuración o privatización, la transferencia a otra organización gestionada por un proveedor independiente (a través de establecer acuerdos contractuales correspondientes), la transferencia de la responsabilidad de la gestión a una autoridad competente, inclusive si

<sup>12</sup> Entre los diferentes estudios generales y casos de estudio que realiza el TEAM Catalonia ([http://www.interpares.org/ip3/ip3\\_index.cfm?team=10](http://www.interpares.org/ip3/ip3_index.cfm?team=10)), como el resto de TEAMS de IP3, lleva a cabo el estudio terminológico que consiste en traducir al catalán los conceptos y definiciones de la base de datos terminológica de InterPARES 2 Project ([http://www.interpares.org/ip2/ip2\\_terminology\\_db.cfm](http://www.interpares.org/ip2/ip2_terminology_db.cfm)) (2010/02/15).

<sup>13</sup> UNE - ISO 15489 1 –Informació i documentació. Gestió documental. Part 1: Consideracions generals. p. 22.



todo el almacenamiento físico del documento es realizado por la organización que lo creó, la transferencia a un archivo histórico, la transferencia a una autoridad archivística externa.

La ISO 15489-2:2001<sup>14</sup> expone que en el procedimiento de transferencia (apartado 4.3.9.4) de documentación que una organización productora hace a otra organización (ya sea externa o subcontratada, a un archivo histórico, a un depósito de archivo, etc.) se transfiere la custodia o cesión de la propiedad de los documentos. En esta transferencia la ISO plantea toda una serie de cuestiones a tener en cuenta, relativas al cumplimiento de la legislación y normativa vigentes, sobre las necesidades administrativas y operativas, las consecuencias de la transferencia etc. Y por lo que respecta a la transferencia de documentos electrónicos, la ISO recomienda, que se han de valorar las cuestiones sobre la compatibilidad del hardware y software, los metadatos (control e información contextual), la documentación de los datos (información técnica sobre el tratamiento de los datos y la estructura de estos) y las normas y los contratos de licencias.

La ISO 14721:2003<sup>15</sup> define un modelo funcional de archivo electrónico y, entre diferentes funcionalidades, explica la ingesta de documentos electrónicos, es decir, los servicios y funciones: *Receive Submission, Quality Assurance, Generate AIP, Generate Descriptive Information and Coordinate Updates functions* de la transferencia de documentación electrónica del productor al preservador:

<sup>14</sup> UNE - ISO 15489 2 - *Informació i documentació. Gestió documental. Part 2: Directrius*. P. 30.

<sup>15</sup> ISO 14721:2003 - *Space and data information transfer systems -- Open archival information system -- Reference model*. Para ver con más detalle las funciones y explicaciones del modelo OAIS aplicado en un repositorio digital seguro ver la segunda parte del artículo donde se define detalladamente el proyecto iArxiu. Ver <http://public.ccsds.org/publications/archive/650x0b1.pdf>.

The functions of the Ingest entity are illustrated in figure 4-2.

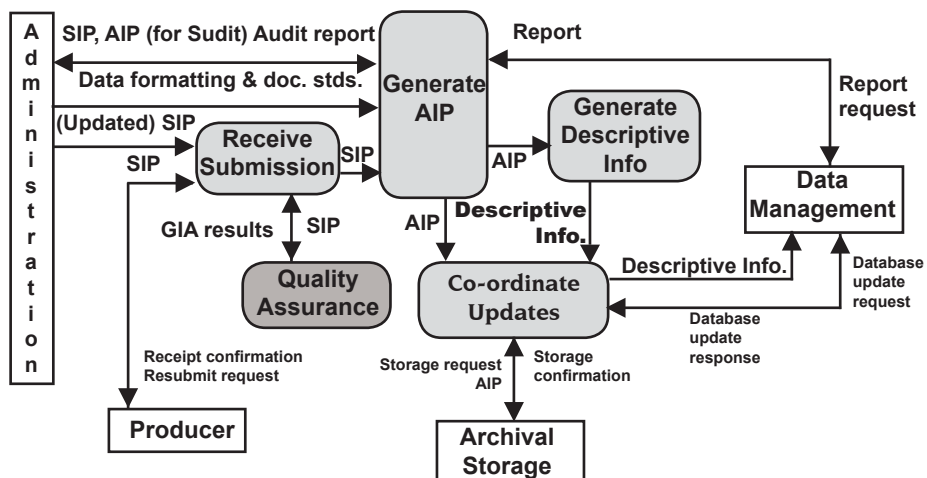


Fig. 1 – Funciones de la ingesta de documentación electrónica (modelo OAIS).

La ISO/TR 18492:2005<sup>16</sup> plantea que la transferencia y la custodia en el acceso a largo plazo de documentación electrónica constituyen puntos críticos. Entre otras cuestiones, recomienda como una buena estrategia de conservación la transferencia de la documentación electrónica por parte de los productores hacia un repositorio digital gestionado por un tercero (quien gestionará la documentación de acuerdo a unas políticas y prácticas documentadas).

La organización Internacional *Records Management Trust* en 2009 publicó una serie de módulos y materiales didácticos sobre gestión de documentos electrónicos titulados *Training in Electronic Records Management*.<sup>17</sup> En el módulo 3: *Managing the creation, Use and Disposal of Electronic Records*, hay toda una serie de recomendaciones interesantes a tener en cuenta cuando se planifica y desarrolla la transferencia de documentación electrónica:

<sup>16</sup> ISO/TR 14721:2005 Long-term preservation of electronic document-based information. P. 10.

<sup>17</sup> Véase <http://www.irmt.org/educationTrainMaterials.php> (2010/02/15).

identificar los documentos con valor histórico y transferirlos a instituciones archivísticas, determinar el formato en que se transferirán los documentos, copiar y, si es necesario, reformatear los documentos a transferir, preparar la documentación a transferir, transferir los documentos y la documentación a un centro de archivo, confirmar el éxito de la transferencia de los documentos y eliminar los documentos desde el sistema de origen. También se recomienda que la transferencia de documentación electrónica se haga en colaboración con personal técnico calificado (informáticos). En el módulo 4: *Preserving Electronic Records*, recomienda que en el momento de hacer una transferencia de documentos electrónicos auténticos hacia un repositorio digital seguro (ingesta) hay que tener en cuenta los siguientes procedimientos: asegurar que el objeto digital a transferir tenga un ID único, escaneado de virus de todos los objetos digitales, una vez transferidos los documentos electrónicos hacer copias de seguridad de ellos, verificar su integridad y almacenamiento, hacer un *checksum* e integrar todos los metadatos relevantes asociados a los documentos electrónicos preservadores.

Las MoReq 2<sup>18</sup> exponen que las razones de la transferencia pueden incluir la preservación permanente de los documentos de archivo por motivos legales, administrativos o de investigación y el uso de servicios propios o externos para la gestión de documentos a medio o largo plazo, y que el procedimiento de transferencia supone la exportación de una copia con todos los metadatos asociados y las pistas de auditoría, seguidas de la destrucción del original. De otra parte, MoReq2 recomienda que se implementen los metadatos relativos a transferencia: fecha de transferencia, código de clasificación completo, título, descripción, usuario responsable de transferencia, motivo de la transferencia y documentar cualquier referencia aportada por el sistema sobre los documentos que han sido transferidos. Finalmente, en Cataluña, en el caso de estándares nacionales de facto, a mi consideración se deben citar:

<sup>18</sup> Véase <http://www.moreq2.eu/> (2010/02/15).

- *Vocabularis de metadades del Grup Innovació Tecnològica de la Generalitat de Catalunya*.<sup>19</sup>
- *Arxiu: Estructura i creació de Paquets d'Informació de Transferència (PIT) utilitzant el model METS*.<sup>20</sup>

## b) El Proyecto Internacional InterPARES

De los diferentes modelos funcionales sobre transferencia de documentos electrónicos auténticos este artículo se centra y se basa en las directrices, pautas y recomendaciones del Proyecto Internacional InterPARES.<sup>21</sup> De una parte, las directrices y recomendaciones que se encuentran en los productos desarrollados durante la segunda fase del Proyecto InterPARES *Preserver Guidelines - Preserving Digital Records: Guidelines for Organizations*<sup>22</sup> y *Creator Guidelines - Making and Maintaining Digital Materials: Guidelines for Individuals*.<sup>23</sup>

InterPARES Project expone que la actividad en la adquisición de documentos electrónicos, con todas las acciones de la preservación que se derivan de este acto, tienen como objetivo la autenticidad continuada y la accesibilidad de los documentos electrónicos

<sup>19</sup> Véase: [http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425\\_vocabularis.pdf](http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425_vocabularis.pdf). Y también, el apartado 5 del presente artículo. (2010/02/15).

<sup>20</sup> Véase: [http://www.iarxiu.eocat.cat/documents/iArxiu%20v2%200%20-%20Estructura\\_PIT\\_%20METS\\_4.3\\_20090504.pdf](http://www.iarxiu.eocat.cat/documents/iArxiu%20v2%200%20-%20Estructura_PIT_%20METS_4.3_20090504.pdf) (2010/02/15).

<sup>21</sup> Véase <http://www.interpares.org>. Sobre todo las dos publicaciones de las dos primeras fases del proyecto: Luciana Duranti, ed., *La conservación a largo plazo de documentos electrónicos auténticos: Hallazgos del Proyecto InterPARES* (Cartegena, Spain: Concejalía de Cultura - 3000 Informática, 2005), 459 pp. (Spanish translation of the InterPARES I Project book.), y, Luciana Duranti, "Introduction," [electronic version] in *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Luciana Duranti and Randy Preston, eds. (Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008). ([http://www.interpares.org/display\\_file.cfm?doc=ip2\\_book\\_introduction.pdf](http://www.interpares.org/display_file.cfm?doc=ip2_book_introduction.pdf)).

<sup>22</sup> Este conjunto de directrices tiene como objetivo la producción, el mantenimiento y la preservación a largo plazo de documentos electrónicos y está dirigido para centros de archivos (preservadores). Véase - [http://www.interpares.org/ip2/display\\_file.cfm?doc=ip2\(pub\)preserver\\_guidelines\\_booklet.pdf](http://www.interpares.org/ip2/display_file.cfm?doc=ip2(pub)preserver_guidelines_booklet.pdf) (2010/02/15).

<sup>23</sup> Véase *Creator Guidelines - Making and Maintaining Digital Materials: Guidelines for Individuals* (2010/02/15).

seleccionados para su preservación permanente. Este movimiento de documentos desde la custodia del productor hacia un organismo preservador, es un punto crucial en la cadena de preservación, y se tiene que efectuar cautelosamente para asegurar que nada salga mal en el procedimiento de transferencia. A partir de este punto, InterPARES Project recomienda:

— Desarrollar un plan compartido para la transferencia.

InterPARES Project recomienda que los productores y preservadores de documentos electrónicos tienen que desarrollar conjunta y compartidamente sus planes de transferencia cuando hayan asumido la viabilidad técnica de la adquisición y la preservación de los documentos electrónicos (qué software y hardware se utiliza para producir documentos electrónicos, sus actualizaciones y mantenimiento etc.) y también tienen que consensuar los formatos lógicos y físicos (o virtuales) utilizados en la transferencia.

A diferencia de cómo se enfoca el contexto organizativo y archivístico del proyecto internacional InterPARES,<sup>24</sup> en el contexto español y catalán, dentro de cada organización, los órganos de gobierno y las unidades administrativas y técnicas (unidades productoras) son quienes desarrollarán conjuntamente sus planes de transferencia.

— Exigir procedimientos estándares.

Desde el gobierno catalán (*Departament de Cultura i Mitjans de Comunicació de la Generalitat de Catalunya*) y la Agencia Catalana de Certificación (CATcert) se ha desarrollado, como un estándar de facto, para todas las administraciones públicas que transferirán

<sup>24</sup> Lluís Esteve-Casellas en el prólogo de la traducción al catalán de las dos guías (directrices) de InterPARES 2 Project para productores y preservadores de documentos electrónicos, comenta que estas guías constituyen un modelo de referencia indiscutible para la gestión y preservación de documentos electrónicos; hay que tener presente que el contexto organizativo y profesional en el cual nacen es bastante diferente de la tradición archivística o del modelo profesional catalán. En este sentido, solamente se tiene que nombrar la distinción de las responsabilidades profesionales en la gestión documental según la documentación esté en fase activa o inactiva, funciones que en el contexto organizativo catalán se tienen que situar en la misma figura profesional como sería el archivero/a. Véase las dos guías traducidas al catalán en <http://www.arxivers.com/cat/publicacions.asp?IDCat=122> (2010/02/15).

documentación electrónica a iArxiu, un procedimiento para la creación del PIT (paquetes de información de transferencia según el modelo OAIS) utilizando el modelo METS.<sup>25</sup>

De otra parte, en Cataluña otra iniciativa en torno de la transferencia de documentación electrónica hacia un repositorio digital seguro (plataforma iArxiu) es el estudio que está desarrollando el TEAM Catalonia–InterPARES 3 *Project de la Associació d'Arxivers de Catalunya*.<sup>26</sup> Este grupo de trabajo actualmente —entre otras tareas, estudios e investigaciones— está desarrollando un procedimiento de transferencia desde una organización pública hacia el repositorio digital seguro iArxiu (pretende definir y explicar el *workflow* del procedimiento de transferencia y de sus metadatos asociados con el objetivo de servir de marco referencial para aquellas organizaciones usuarias de iArxiu).

—Conservar el formato lógico disponible más antiguo.

InterPARES Project recomienda, siempre que sea posible, que se conserve el formato original en que los documentos electrónicos fueron producidos cuando se transfieran a un repositorio digital seguro con el objetivo de que si las futuras estrategias de preservación (migraciones, conversiones, etc.) aplicadas a los documentos electrónicos fallasen, siempre se podría iniciar de nuevo el proceso de preservación desde los documentos electrónicos en formato original.<sup>27</sup>

— Evitar los duplicados.

<sup>25</sup> Este procedimiento, iArxiu: *Estructura i creació de Paquets d'Informació de Transferència (PIT) utilitzant el model METS* fue elaborado por el equipo técnico del proyecto iArxiu del CATcert y aprobado por el Grupo de Innovación Tecnológica de la Subdirección General de Archivos y Gestión de Documentos del gobierno catalán en el año 2008. Véase [http://www.catcert.cat/descarrega/iArxiu\\_v2\\_Estructura\\_PIT\\_METS\\_20080425\\_WEB.pdf](http://www.catcert.cat/descarrega/iArxiu_v2_Estructura_PIT_METS_20080425_WEB.pdf) (2010/02/15).

<sup>26</sup> El año 2008 la Associació d'Arxivers de Catalunya (<http://www.arxivers.com>) creó un grupo de trabajo (TEAM Catalonia) para participar y colaborar dentro de la fase del Proyecto Internacional InterPARES. Los dos autores de este artículo son investigadores de dicho grupo de trabajo. El procedimiento de transferencia de documentación electrónica auténtica hacia un repositorio digital seguro, desarrollado actualmente por el TEAM Catalonia está relacionado / vinculado con un caso de estudio de este grupo de trabajo titulado Preservación de los documentos vitales en la Universidad Pompeu Fabra de Barcelona.

<sup>27</sup> Esta recomendación la aplica iArxiu.

— Documentar todos los procesos:

InterPARES Project recomienda que los procesos iniciales aplicados e inmediatamente después de la transferencia pueden estar o no relacionados con la preservación *per se*. Comprobar la identidad de la documentación electrónica transferida, comprobar si tiene virus y evaluar la integridad de los documentos electrónicos, son operaciones que tienden a no provocar cambios en los documentos electrónicos. La conservación de documentos electrónicos, el cambio de nombres de las entidades digitales y la encapsulación de documentos electrónicos son actividades más intrusitas. En ambos casos, el preservador tiene que documentar todos los procesos aplicados a los documentos electrónicos, y sus efectos, mientras estén en su custodia.

También recomienda que si se hacen copias de los documentos electrónicos para que estos tengan la misma condición de original y por tanto de autenticidad, dichas copias se tienen que hacer siguiendo los requisitos relevantes de *InterPARES 1 Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records*.<sup>28</sup>

Y de otra parte, para la transferencia de documentación electrónica auténtica, se seguirá el modelo funcional COP model<sup>29</sup> (*Chain of Preservation Model*). En este modelo de la cadena de preservación de los documentos electrónicos entre otros procedimientos / *workflows* contiene:

1) Adquiriendo documentos electrónicos auténticos (A4-3)

<sup>28</sup> Véase [http://www.inter pares.org/book/inter pares\\_book\\_k\\_app02.pdf](http://www.inter pares.org/book/inter pares_book_k_app02.pdf).

<sup>29</sup> El modelo COP es un modelo funcional que representa las actividades de producción, conservación, evaluación y preservación de documentos electrónicos durante su ciclo vital. Este modelo de las actividades llevadas a cabo durante la gestión de los documentos al través de su ciclo de vida integrada proviene de tres modelos preexistentes: *Project UBC* (1994-97), de las actividades en la gestión corriente de los documentos y en dos modelos de las funciones de selección y preservación de los documentos electrónicos producidos durante la primera fase d'InterPARES Project (1998 – 2001).

— Diagrama:

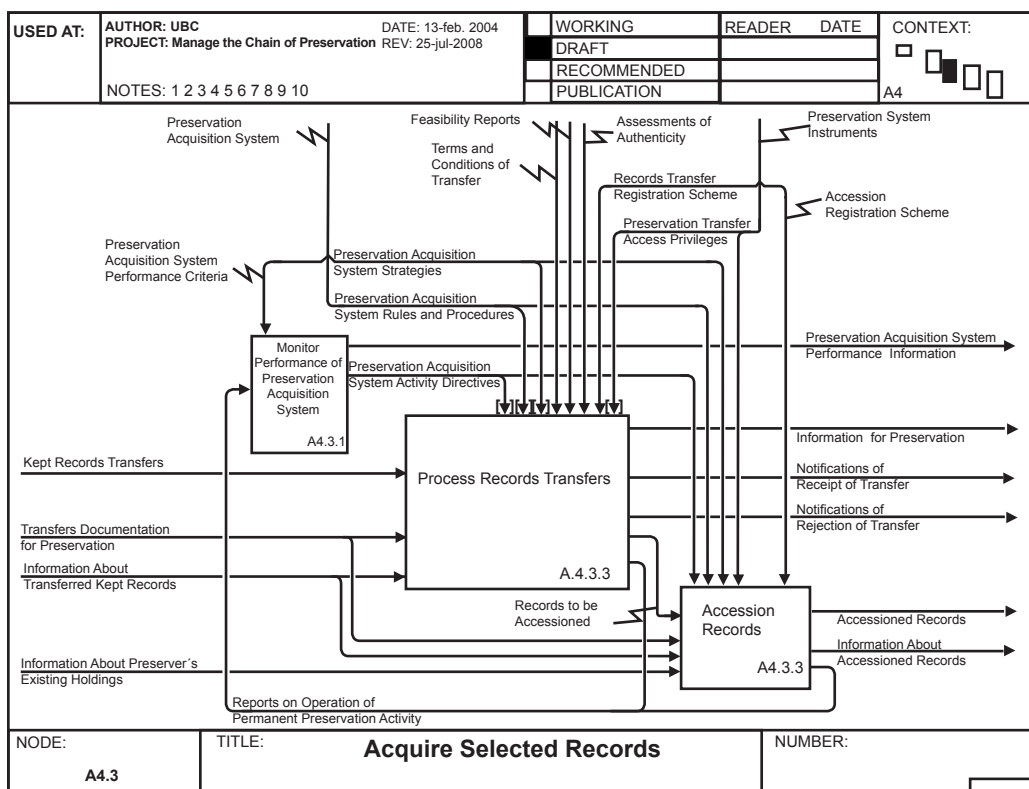


Fig. 2 - Adquiriendo documentos electrónicos auténticos (A4-3) – COP model InterPARES

— Explicación:

A través de este *workflow* se definen las acciones a realizar cuando se lleva a cabo la transferencia de documentos electrónicos hacia un repositorio digital seguro (verificación de la autoridad de transferencia, revisión de la documentación de la transferencia, el registro de la transferencia, etc.) estas acciones implican el traslado del modelo de custodia y el control de los documentos del productor hacia el preservador y el objetivo principal es continuar y



garantizar la accesibilidad y autenticidad de los documentos.

2) El proceso de transferencia de documentos electrónicos (A4.3.2).

— Diagrama:

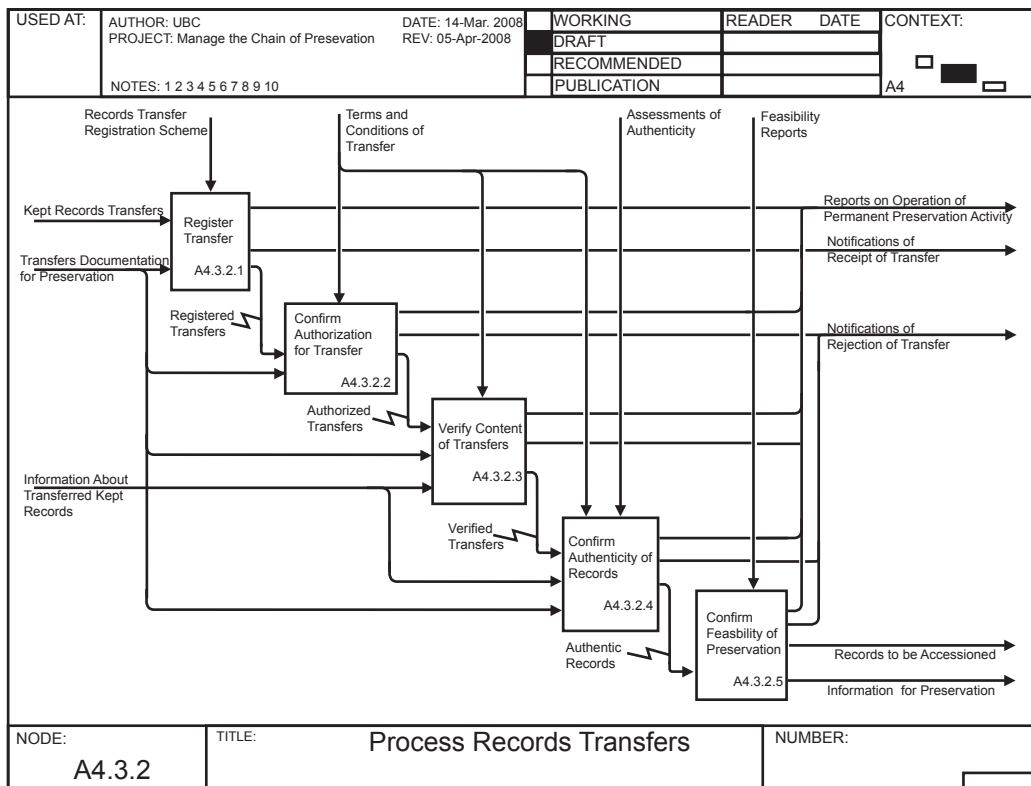


Fig. 3 - Proceso de transferencia de documentos electrónicos (A4.3.2) - COP model InterPARES Project.

— Explicación:

El modelo contempla 5 fases de procesamiento que incluyen las siguientes actividades:

1. Registrar la transferencia (A4.3.2): incluye registrar la información obtenida sobre la transferencia (implica solamente en este estadio el conocimiento de la recepción de la transferencia).

Metadatos (A4.3.2.1)
<ul style="list-style-type: none"><li>- Nombre de la persona responsable de la transferencia.</li><li>- Número de registro asignado al responsable de la transferencia.</li><li>- Fecha y hora de recepción de la transferencia.</li><li>- Nombre de la/s persona/s que registra la transferencia.</li><li>- Indicación del motivo/ autorización para la transferencia (p. ej. los términos y condiciones de la transferencia).</li><li>- Indicación de los documentos y otra documentación / información de transferencia recibida.</li><li>- Nombre de las personas a quienes se notifica la recepción de la transferencia.</li><li>- Nombre de la persona a quien se comunica la notificación, y,</li><li>- Fecha y hora en que la notificación fue enviada.</li></ul>

Tabla 2 – Metadatos registro de transferencia.

2. Confirmar la autorización de la transferencia (A4.3.2.2), incluye la confirmación de la persona autorizada a transferir los documentos electrónicos, y, en caso de personas no autorizadas, al transferir se incluyen las notificaciones de denegación de transferencia. El preservador tiene que poseer un listado de personas autorizadas a transferir. En caso negativo, se comunica mediante notificación de denegación.

Metadatos (A4.3.2.2)	
Aceptada	Denegada
<ul style="list-style-type: none"> <li>- Fecha y hora de aceptación de transferencia;</li> <li>- Nombre de la persona que confirma la autorización de la transferencia;</li> <li>- Número de autorización de transferencia (asignado por el archivo).</li> <li>- Términos y condiciones del número de transferencia.</li> </ul>	<ul style="list-style-type: none"> <li>- Fecha/hora de la transferencia denegada (no autorizada).</li> <li>- Nombre de la persona que deniega la transferencia;</li> <li>- Nombre de la/s persona/s quien/es notifica la denegación de transferencia;</li> <li>- Nombre de la persona que gestiona la notificación de denegación;</li> <li>- Fecha y hora de trámite de la notificación de negación.</li> <li>- Indicación del motivo de la denegación.</li> <li>- Número de denegación de la autorización de transferencia (asignado por el archivo).</li> <li>- Términos y condiciones del número de transferencia.</li> </ul>

Tabla 3 – Metadatos de confirmación de autorización de transferencia.

3. Verificar el contenido de la transferencia (A4.3.2.3), incluye determinar si los documentos electrónicos transferidos son correctamente enviados (por ejemplo que no hayan sido alterados durante la transmisión e incluyan todos los documentos y agregaciones). En caso negativo, se comunica mediante notificación de denegación.

Metadatos (A4.3.2.3)	
Aceptada	Denegada
<ul style="list-style-type: none"> <li>- Fecha/hora de aceptación y verificación de transferencia.</li> <li>- Nombre de la persona que verifica la transferencia.</li> <li>- Número de verificación del contenido de la transferencia (asignado por el archivo).</li> <li>- Términos y condiciones del número de transferencia.</li> </ul>	<ul style="list-style-type: none"> <li>- Fecha/hora de la transferencia denegada como contenido incorrecto.</li> <li>- Nombre de la persona que deniega la transferencia.</li> <li>- Nombre de la persona(es) a quien se notifica la denegación de transferencia.</li> <li>- Nombre de la persona que gestiona la notificación de denegación;</li> <li>- Fecha y hora de trámite de la notificación de denegación;</li> <li>- Indicación de las medidas empleadas por el acceso del contenido de la transferencia.</li> <li>- Indicación del motivo(s) de la denegación;</li> <li>- Número de denegación de contenido transferido (asignado por el archivo);</li> <li>- Términos y condiciones de número de transferencia.</li> </ul>

Tabla 4 – Metadatos de verificación de transferencia.

4. Confirmar la autenticidad de los documentos electrónicos en la transferencia (A4.3.2.4), incluye determinar si la valoración de la autenticidad del productor de los documentos electrónicos se ha transferido, la cual se llevó a cabo como parte del proceso de evaluación, y todavía al verificar que los atributos de la identidad y la integridad de los documentos se ha transmitido correctamente con los documentos electrónicos. En caso negativo, se comunica mediante notificación de denegación.

Metadatos (A4.3.2.4)	
Aceptada	Denegada
<ul style="list-style-type: none"> <li>- Fecha/hora de aceptación de la transferencia que contiene documentación auténtica;</li> <li>- Indicación de las medidas utilizadas para confirmar la autenticidad;</li> <li>- Número del informe de evaluación de la autenticidad (asignado por el archivo);</li> <li>- Número de verificación de la autenticidad de transferencia (asignado por el archivo);</li> <li>- Términos y condiciones del número de transferencia.</li> </ul>	<ul style="list-style-type: none"> <li>- Fecha/hora de transferencia cuando fue denegada por contener documentos de archivo que no se pudieron autenticar.</li> <li>- Nombre de la persona que deniega la transferencia;</li> <li>- Nombre de la/s persona/s quien/es gestiona la notificación de denegación de transferencia;</li> <li>- Fecha y hora de trámite de la notificación de denegación;</li> <li>- Indicación de las medidas empleadas para evaluar la autenticidad de los documentos de archivo en la transferencia;</li> <li>- Indicación del motivo/s de la denegación;</li> <li>- Número de verificación de autenticidad de transferencia (asignado por el archivo);</li> <li>- Términos y condiciones del número de transferencia</li> </ul>

Tabla 5 – Metadatos de confirmación de la autenticidad.

5. Confirmar la viabilidad de la preservación de la transferencia (A4.3.2.5), incluye verificar que la determinación de la viabilidad de la preservación era, durante el proceso de evaluación, todavía válida. En caso negativo, se comunica mediante notificación de denegación.

Metadatos (A4.3.2.5)	
Aceptada	Denegada
<ul style="list-style-type: none"> <li>- Fecha/hora de confirmación de la viabilidad de la preservación;</li> <li>- Nombre de la persona que confirma la viabilidad;</li> <li>- Número de informe de viabilidad (asignado por el archivo).</li> <li>- Número de verificación de viabilidad (asignado por el archivo);</li> <li>- Términos y condiciones del número de transferencia.</li> </ul>	<ul style="list-style-type: none"> <li>- Fecha/hora de denegación de transferencia por contener documentos de archivo que no pueden ser preservados;</li> <li>- Nombre de la persona que deniega la transferencia;</li> <li>- Nombre de la/s persona/s que gestiona/n la notificación de transferencia;</li> <li>- Fecha y hora de trámite de la notificación de denegación;</li> <li>- Indicación de las medidas empleadas para confirmar la viabilidad de la preservación;</li> <li>- Indicación del motivo/s de la denegación;</li> <li>- Número del informe de la viabilidad (asignado por el archivo);</li> <li>- Términos y condiciones del número de transferencia.</li> </ul>

Tabla 6 – Metadatos de confirmación de viabilidad de la preservación de transferencia.

## V. El procedimiento de transferencia

Como se ha comentado más adelante, el TEAM Catalonia – InterPARES 3 *Project de la Associació d'Arxivers de Catalunya* está trabajando en un estudio para definir un procedimiento de transferencia (*workflow* y metadatos asociados a éste) con una doble finalidad básica: desarrollar y aplicar este procedimiento al gestor documental corporativo<sup>30</sup>

<sup>30</sup> Algunos gestores documentales (ECM y RM) del mercado ofrecen de serie un *workflow* de transferencia pero a veces estos no se adaptan al contexto de cada organización, por esta razón, el TEAM Catalonia se ha fijado como objetivo la definición de un *workflow* de transferencia y sus metadatos asociados para que sirva como una referencia para administraciones públicas con gestores documentales e intención de hacer transferencias de documentos electrónicos a iArxiu.

y para poder facilitar la integración de éste con la plataforma iArxiu.

En la segunda parte de este artículo (punto 4.1 - Módulo de transferencia e ingreso) se comentarán las fases del procedimiento de transferencia desarrolladas por iArxiu:<sup>31</sup>

- Fase de preingreso.
- Fase de transferencia.
- Fase de ingreso.

## **VI. Los metadatos asociados al procedimiento de transferencia**

Los metadatos utilizados en el procedimiento de transferencia se dividen en dos grupos: los metadatos de gestión documental asociados / vinculados al procedimiento de transferencia y los metadatos de preservación digital.

Por lo que respecta a los metadatos de gestión documental<sup>32</sup> aplicables al procedimiento de transferencia de documentación electrónica y siguiendo exclusivamente las directrices, modelos y recomendaciones del Proyecto Internacional InterPARES, se identifican y definen los siguientes metadatos:<sup>33</sup>

<sup>31</sup> El módulo de transferencia de iArxiu toma como referencia: ISO 20652:2005. *Space data and information transfer systems – Open archival information systems – Producer-Archive interface methodology abstract standard y Business Requirements Specification (BRS), Record Exchange Standard* disponible en <http://www.ica.org/sites/default/files/Record%20Exchange%20Standard.pdf>. Véase el apartado “Módulo de transferencia e ingreso” de la segunda parte de este artículo. (2010/02/15).

<sup>32</sup> El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE, núm. 25, de 29-01-2010), en el glosario define como esquema de Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

<sup>33</sup> Este listado de metadatos está en fase de primera versión y su objetivo es servir de base/referencia para futuras investigaciones, estudios y trabajos en este ámbito con tal de mejorarlo y completarlo.

Metadatos	Fuente	Función / definición
Número de registro de transferencia	IP 2	Referenciar el número de transferencia efectuada por parte de las unidades administrativas hacia el Archivo. Se componen de dos numeraciones: general (es un ID contador global de transferencias efectuadas al archivo), específico (es un ID contador de las transferencias individualizadas que realiza cada unidad administrativa al archivo).
Unidad administrativa de transferencia (código y denominación) y responsable administrativo	IP 2	Referenciar el código y la denominación orgánica que transfiere y del responsable administrativo.
Responsable técnico de la transferencia	IP 2	Referenciar la persona que gestiona la transferencia (nombre, lugar de trabajo y denominación de la unidad orgánica)
Fecha y hora inicio de transferencia	IP 2	Referenciar la fecha y hora de inicio de transferencia
Fecha y hora finalización de transferencia	IP 2	Referenciar la fecha y hora de finalización de la transferencia
Volumen	IP 2	Referenciar e indicar la documentación electrónica transferida
Viabilidad	IP 2	Referenciar la información sobre la viabilidad del contenido, de la autenticidad y de la preservación de los documentos electrónicos transferidos.

Tabla 7 – Metadatos de gestión documental de transferencia

De otra parte, en Cataluña, como estándar de facto cuando se refiere a metadatos de preservación digital para la documentación electrónica que se preservará a largo plazo, hay los *Vocabularis de Metadades*.<sup>34</sup>

Este estándar nacional nació con la necesidad de trabajar en un modelo de intercambio de información entre los diferentes sistemas de gestión documental de los organismos de la *Generalitat de Catalunya*, esto llevó a que en el año 2005 el *Grup d'Innovació Tecnològica*<sup>35</sup>

<sup>34</sup> Véase [http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425\\_vocabularis.pdf](http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425_vocabularis.pdf) (2010/02/15).

<sup>35</sup> Véase: <http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.01121f9326561a075a2a63a7b0c0e1a0/?vgnextoid=aa9b3d70f2341210VgnVCM1000008d0c1e0aRCRD&vgnnextchannel=aa9b3d70f2341210VgnVCM1000008d0c1e0aRCRD&vgnnextfmt=default>. Actualmente los dos autores de este artículo forman parte de este grupo de trabajo de la *Generalitat de Catalunya*. (2010/02/15).



del gobierno catalán se propuso abordar la definición de un modelo de objeto digital a preservar que sirviera para el conjunto de las administraciones públicas catalanas. Coincidiendo en tiempo cuando se estaba desarrollando desde la *Agència Catalana de Certificació* (CATcert) el proyecto iArxiu, el servicio de archivo y preservación de documentos electrónicos a largo plazo que la agencia quería ofrecer a las administraciones públicas catalanas. Esta coincidencia en el tiempo hizo posible la vinculación del proyecto a desarrollar por el *Grup d'Innovació Tecnològica* —objeto digital— con los trabajos de CATcert lleva a cabo en este sentido. Después de un planteamiento inicial respecto a la necesidad de identificar el modelo conceptual y el objeto digital, se trató de definir las entidades y las representaciones asociadas, cogiendo la Norma de *Descripció Arxivística de Catalunya* (NODAC) como referente. Se hizo un primer planteamiento de cuestiones que se tendrían que abordar [terminología y definiciones, gestión de formatos, identificadores únicos, etc.] teniendo en cuenta los campos que recoge la NODAC y los elementos descriptivos que aparecen en *Model Requirements for the Management of Electronic Records*<sup>36</sup>, *MoReq*, actualizada el año 2008 como *MoReq2*.<sup>36</sup>

Los modelos / fuentes de que bebe los vocabularios de metadatos son de la NODAC, EAD, OAIS model, MoReq 1 y 2, ISO/TS 23081-1:2004, equivalencias entre Dublín Core 5 y normas de descripción, METS model, y —desde el CATcert— el estándar de preservación PREMIS6 (*Preservation Metafecha: Implementation Strategies*).<sup>37</sup>

Los vocabularios de metadatos de preservación digital engloban 4 plantillas / esquemas de metadatos genéricos: expediente, documento integrado a expediente, documento suelto y signatura electrónica. Así mismo, los vocabularios, identifican, definen y determinan la aplicabilidad de cada elemento de metadato a través de su ficha de control correspondiente.

<sup>36</sup> Vocabularios *Op. Cit.* Pp. 7 i 8.

<sup>37</sup> Vocabularios *Op. Cit.* P. 9.

La plantilla / esquema genérica/o de expediente: <sup>38</sup>	La plantilla / esquema genérica/o de documento integrado en un expediente: <sup>39</sup>	La plantilla / esquema genérica/o de documento suelto: <sup>40</sup>	La plantilla / esquema genérica de signature electrónica <sup>41</sup>
Código de referencia	Código de referencia	Código de referencia	Identificador signature
Número expediente	Número documento	Número documento	Identificador documento
Código de clasificación		Código de clasificación	Tipo de signature
Serie documental		Serie documental	Formato de la signature
Nivel de descripción	Nivel de descripción	Nivel de descripción	Fecha de la signature
Título	Título	Título	Fecha validación de la signature
Fecha de inicio			Evidencia de la validación
Fecha de finalización	Fecha de creación	Fecha de creación	Nombre de signatario
	Soporte	Soporte	Identificador de signatario
Nombre productor	Nombre productor	Nombre productor	Organización
Unidad productora	Unidad productora	Unidad productora	Unidad orgánica
Descripción	Descripción	Descripción	Política de signature
Descriptores	Descriptores	Descriptores	
Documentación relacionada			
Tipo relación	Tipo de documento	Tipo de documento	
Clasificación seguridad y acceso	Clasificación seguridad y acceso	Clasificación seguridad y acceso	
Sensibilidad datos LOPD (Ley Orgánica de Protección de Datos)	Sensibilidad datos LOPD	Sensibilidad datos LOPD	
	Nivel de clasificación evidencial	Nivel de clasificación evidencial	

<sup>38</sup> Vocabularios *Op. Cit.* pp.14 - 27.

<sup>39</sup> Vocabularios *Op. Cit.* pp. 40 - 52.

<sup>40</sup> Vocabularios *Op. Cit.* pp. 40 - 52.

<sup>41</sup> Vocabularios *Op. Cit.* pp. 53 - 63.

Tabla 8 – Plantillas genéricas – Vocabularios de Metadatos.

A partir de estos metadatos de preservación digital se definirán y aplicarán sobre la documentación electrónica que se transferirá al repositorio digital seguro (iArxiu) y por tanto se derivarán aquellas plantillas / esquemas específicos que se utilizarán para crear los paquetes de transferencia de documentación (PIT).<sup>42</sup>

## VII. Primeras conclusiones

A modo de conclusión de esta parte del artículo, se listarán las recomendaciones y consideraciones a tener en cuenta cuando desde las oficinas productoras de documentos electrónicos se planifica su transferencia hacia un repositorio digital seguro:

Desde el punto de vista legal:

- Establecer convenios / contratos entre productores y preservadores, que deben contener:
  - Traspaso de responsabilidades en la gestión de la documentación electrónica
  - Custodia de confianza continuada.
  - Privilegios de accesos.
- Cada organización tiene que diseñar e implantar:
  - Normativa de transferencias.
  - Formulario de transferencias.
  - Registro de transferencias.

Desde el punto de vista funcional y procedimental:

- Diseñar, planificar e implementar instrumentos de gestión documental que atañen al proceso de transferencia: calendario de conservación y eliminación, calendario de

<sup>42</sup> El paquete de información de transferencia (PIT), dentro de la terminología del modelo OAIS, son los documentos transferidos por los productores de la documentación que incluyen los contenidos a preservar y los metadatos que faciliten su recuperación, tratamiento y preservación. (Fuente: Vocabularis de metadades, grup Innovació Tecnològica pp 8). Para crear el PIT a transferir hacia un repositorio digital seguro (iArxiu) se seguirán las directrices y procedimiento incluidas a *iArxiu: Estructura i creació de Paquets d'Informació de Transferència (PIT) utilitzant el model METS* ([http://www.catcert.cat/descarrega/iArxiu/iArxiu%20v2%200%20-%20Estructura\\_PIT\\_%20METS\\_4.3\\_v1.pdf](http://www.catcert.cat/descarrega/iArxiu/iArxiu%20v2%200%20-%20Estructura_PIT_%20METS_4.3_v1.pdf)). (2010/02/15).

transferencias y cuadro de seguridad y acceso.

- Diseñar e implementar procedimientos de transferencias de documentos electrónicos estándares (objetivo si se utilizan diferentes plataformas de terceros para la preservación a largo plazo de los documentos que producen desde las organizaciones).
- Definir el régimen de acceso a la documentación electrónica transferida (permisos)
- Descripción (plantillas genéricas, específicas de metadatos y sus esquemas)
- En cada procedimiento de transferencia se tiene que documentar todo el procedimiento a través de la elaboración de un informe técnico.

Desde el punto de vista tecnológico:

- Asesoramiento y colaboración multidisciplinar e interdisciplinario (p. ej. Creación de los PIT, políticas de migración, conversiones futuras de la documentación transferida etc.)
- Utilizar servicios externos, especializados en la preservación digital y repositorios digitales (p. ej. iArxiu).
- Producir documentos electrónicos en formatos que puedan operar con repositorios digitales y que garanticen su preservación a medio y/o largo plazo.<sup>43</sup>

## VIII. El archivo electrónico, reto o necesidad

El despliegue de la sociedad de la información en estos últimos años ha provocado y sigue causando un sinfín de cambios de carácter económico, social, cultural y tecnológico impactando de lleno en el modo de prestar los servicios por parte de la administración. Dicha transformación o modernización implica un cambio en el modelo de gestión administrativa, una nueva forma de comunicación con el ciudadano conocida como *administración electrónica*. En especial, podemos destacar iniciativas y proyectos relacionados con la gestión electrónica de los procedimientos, procesos y servicios administrativos cuyo objetivo es desarrollar sistemas que posibiliten su gestión, tramitación y seguimiento de forma totalmente

<sup>43</sup> La plataforma iArxiu trabaja con una lista de formatos restringida, véase en la segunda parte de este artículo el apartado "Módulo de preservación".

electrónica. Eso sí, dentro de unos parámetros de racionalización, optimización, mejora y simplificación que permitan conseguir una gestión más eficaz, eficiente y transparente.

Además este avance en la simplificación y la digitalización administrativa, y mejora en la calidad y la transparencia de los servicios electrónicos, debe ir acompañado de una mejora en términos de seguridad: incorporar el uso de la firma digital como mecanismo de seguridad para garantizar la integridad, la autenticidad y la validez jurídica de los actos y los documentos y, en segundo lugar, establecer las medidas correspondientes para garantizar que dicha información sea accesible, disponible e interpretable, es decir, perdurable durante el período de tiempo que establezca la legislación vigente.

Con la digitalización de los procedimientos administrativos y el crecimiento de las transacciones electrónicas nos encontramos con que la documentación que se genera en estos sistemas sólo se encuentra en formatos y soportes electrónicos. Este sustrato documental electrónico, que testimonia dichos procedimientos, tiene la misma validez jurídica que su equivalente en papel, siempre y cuando se incorporen las medidas de seguridad convenientes. Además, hay que conservarlo durante periodos de tiempo que van más allá de su presencia en la fase de tramitación electrónica y, en muchos casos, más allá del propio ciclo de vida del entorno informático en que se produjo y gestionó esta documentación.

Ante este nuevo paradigma de gestión, la preservación y el archivo de los documentos electrónicos<sup>44</sup> se ha convertido en un reto, una necesidad y una obligación a la que tendrá que enfrentarse cualquier administración pública que pretenda conservar para futuros usuarios, ya sea por razones administrativas, legales, culturales o históricas, la documentación que genera o recibe en formato electrónico, en el ejercicio de sus funciones o actividades. En este sentido, se ha generado cierta inquietud en el seno de las administraciones públicas sobre cómo abordar la conservación de estos documentos. Preguntas como ¿qué hay que

<sup>44</sup> En la presente comunicación el concepto de archivo se entiende como un conjunto de personas y sistemas que han asumido el compromiso y la responsabilidad de conservar la información y hacerla accesible a una determinada comunidad de usuarios tal y como se establece en la norma ISO 14721:2003 - *Space data and information transfer systems. Open archival information systems. Reference model*.

preservar? ¿quién se responsabiliza de su custodia? o ¿existen herramientas o servicios al día de hoy para gestionar correctamente la preservación de los documentos electrónicos a largo plazo? están en boca de todos, especialmente desde la aprobación de la *Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos* (LAECSP).<sup>45</sup>

En este sentido, para evitar que los problemas de conservación supongan un problema para la modernización de las administraciones públicas catalanas, la Agencia Catalana de Certificación (CATCert), organismo dependiente del Consorcio Administración Abierta de Catalunya (Consorcio AOC) ha desarrollado un servicio de archivo electrónico, llamado iArxiu,<sup>46</sup> que representa una de las primeras experiencias en relación al archivo y preservación de documentos electrónicos a largo plazo en el ámbito de las administraciones públicas.

## IX. Definición y objetivos del servicio

Muchas veces se asocia un servicio de archivo/preservación a un repositorio digital o a una plataforma autorizada para custodiar los documentos electrónicos en un entorno seguro. Esta percepción es una verdad a medias ya que un servicio de preservación digital es mucho más que una solución puramente tecnológica.

En primer lugar, debemos considerar este servicio como un elemento integrado en el sistema de gestión documental de la institución. Esta dependencia funcional implica que su definición, diseño e implantación no se pueden abordar de una forma independiente, sino todo lo contrario, hay que establecer un único punto de vista, una estrategia corporativa en la gestión de los documentos electrónicos y afrontar la gestión del ciclo de vida de los documentos de una forma integrada, delimitando las atribuciones y responsabilidades de cada elemento o subsistema funcional.

En segundo lugar, la preservación se compone de un conjunto de actividades, procesos documentados y herramientas que tienen la finalidad de asegurar no sólo la accesibilidad

<sup>45</sup> Véase la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*.

<sup>46</sup> Para más información sobre el servicio véase: <http://www.iarxiu.eocat.cat>.

y disponibilidad de los documentos a largo plazo, sino también el mantenimiento de su autenticidad, integridad y fiabilidad en un entorno tecnológico presumiblemente distinto al original. Es verdad que el sistema fija su atención en la preservación de los documentos como una entidad autónoma, pero lo realmente importante es dotar al servicio, entendido como la suma de un repositorio digital más las actividades y los procesos de preservación, de unas medidas de seguridad y de calidad suficientes para transmitir confianza y garantía a los usuarios.

Una vez reconocido el problema de la obsolescencia tecnológica de los sistemas informáticos que generan o almacenan dicha información, así como la vida limitada de los soportes de almacenamiento, se hace palpable la necesidad de un servicio de archivo electrónico. Los grandes objetivos y responsabilidades del servicio iArxiu son los siguientes:

- Aceptar la **responsabilidad** del mantenimiento (**disponibilidad, preservación y evidencia**) de documentos electrónicos durante largos períodos de tiempo, más allá de la obsolescencia tecnológica.
- **Construir una plataforma tecnológica o repositorio digital** para almacenar los expedientes/documentos electrónicos durante su fase de vigencia y conservación permanente, bajo la forma de paquetes de información de archivo, y así garantizar, a lo largo del tiempo, su integridad, seguridad, recuperación y visualización. Este último punto es de especial interés, ya que lo realmente importante es garantizar que el contenido de la documentación sea accesible e interpretable por los usuarios de hoy y del mañana.
- **Prestar servicios** específicos relacionados con la **preservación digital** para tratar los problemas derivados de la fragilidad de los soportes y la obsolescencia tecnológica, ya sea del hardware, el software o de los formatos de los documentos.

En este contexto el CATCert, conjuntamente con otras administraciones catalanas, está colaborando en facilitar la transición a la custodia y al archivo del documento electrónico, considerando que no se trata sólo de un problema técnico o de seguridad, sino realmente de un problema jurídico y de una necesidad de gestión.

Las soluciones desarrolladas respetan el actual marco competencial en materia de

gestión documental y archivos<sup>47</sup> y actúan como elemento dinamizador para facilitar la normalización del documento electrónico en la gestión de los procedimientos y servicios públicos electrónicos. En este sentido, para alinearnos con los organismos competentes en materia de gestión documental y archivo hemos contado con la colaboración de la *Subdirecció General d'Arxius del Departament de Cultura de la Generalitat de Catalunya*<sup>48</sup> y del colectivo de archiveros a través del Grupo de Innovación Tecnológica<sup>49</sup> cuya misión es ofrecer pautas y criterios para la gestión de la documentación electrónica, asegurar su validez jurídica y conservación a largo plazo, en el marco de las políticas de *e-governance* que impulsa el gobierno de la *Generalitat de Catalunya*.

Asimismo, hay que señalar que el servicio iArxiu no está pensado para facilitar la tramitación y la gestión de los expedientes electrónicos en su fase de trámite, ni incluye herramientas de gestión de flujos de trabajo o funcionalidades propias de la gestión documental. A nuestro entender, hay que construir una visión global del concepto de gestión de la documentación electrónica que abarque desde su génesis hasta su disposición final. Este enfoque no implica que el sistema de gestión documental de una organización sea construido e implementado bajo una misma solución tecnológica, sino todo el contrario, debemos impulsar la integración e interoperabilidad entre las distintas piezas o servicios del sistema. Cada una de estas piezas da respuestas y soluciones a unas necesidades y funcionalidades muy específicas. Así, el servicio de archivo electrónico tiene la responsabilidad de custodiar, mantener y garantizar la perdurabilidad/accesibilidad, a largo plazo, de la documentación electrónica generada por los sistemas de información o de gestión documental de la organización.

<sup>47</sup> Véase la *Llei 10/2001, de 13 de juliol, d'arxius i documents*.

<sup>48</sup> Para más información véase: [http://www20.gencat.cat/portal/site/CulturaDepartament menuitem.01121f9326561a075a2a63a7b0c0e1a0/?vgnextoid=86efa3c922e31210VgnVCM1000008d0c1e0aRCRD&vgnnextchannel=86efa3c922e31210VgnVCM1000008d0c1e0aRCRD&vgnnextfmt=default](http://www20.gencat.cat/portal/site/CulturaDepartament%20menuitem.01121f9326561a075a2a63a7b0c0e1a0/?vgnextoid=86efa3c922e31210VgnVCM1000008d0c1e0aRCRD&vgnnextchannel=86efa3c922e31210VgnVCM1000008d0c1e0aRCRD&vgnnextfmt=default).

<sup>49</sup> Para más información véase: [http://www20.gencat.cat/portal/site/CulturaDepartament menuitem.01121f9326561a075a2a63a7b0c0e1a0/?vgnextoid=aa9b3d70f2341210VgnVCM1000008d0c1e0aRCRD&vgnnextchannel=aa9b3d70f2341210VgnVCM1000008d0c1e0aRCRD&vgnnextfmt=default](http://www20.gencat.cat/portal/site/CulturaDepartament%20menuitem.01121f9326561a075a2a63a7b0c0e1a0/?vgnextoid=aa9b3d70f2341210VgnVCM1000008d0c1e0aRCRD&vgnnextchannel=aa9b3d70f2341210VgnVCM1000008d0c1e0aRCRD&vgnnextfmt=default).



## X. Conceptos básicos

Para entender mejor el funcionamiento del servicio iArxiu y la gestión de la conservación de los documentos a lo largo del tiempo hay que explicar, aunque sea brevemente, qué entendemos por documentación electrónica. No pretendemos dar una definición específica, sino simplemente advertir que en el texto, cuando hablamos de documentación, nos estamos refiriendo tanto a un documento electrónico, ya sea estructurado o no, estático o dinámico (documentos ofimáticos, documentos transaccionales, correos electrónicos, evidencias documentales, bases de datos, documentos firmados, etc.) como a agrupaciones de documentos o expedientes electrónicos, conservados como información y prueba por una organización o un individuo en el desarrollo de sus actividades o en virtud de sus obligaciones legales.<sup>50</sup>

Además, otro elemento inseparable y esencial para el tratamiento y la preservación de los documentos electrónicos es el de los metadatos que nos describen el contexto, el contenido y la estructura de los documentos y nos permiten asegurar su autenticidad, fiabilidad, integridad y disponibilidad a lo largo de su ciclo de vida.<sup>51</sup> Por lo tanto, cuando hablamos de preservación de documentos nos referiremos tanto a los documentos, como objetos de información (contenido), como a los metadatos que nos ayudan a interpretarlos y gestionarlos correctamente.

Aunque debe abordarse la problemática de la conservación como un todo, el foco principal son los documentos. Por esta razón es imprescindible definir, modelar e implementar una forma de estructurar y agrupar todos los componentes que son objeto de conservación en un contenedor neutral, para que dejen de ser dependientes del código original y puedan ser almacenados en un formato de conservación. Si unimos, en un mismo contenedor los documentos u objetos digitales y sus metadatos, se crea una entidad que puede existir en cualquier entorno informático, ya que incluye toda la información necesaria para acceder y representar el documento. Nosotros

<sup>50</sup> Véase la definición de documento que propone la norma ISO 15489.

<sup>51</sup> Para más información sobre la gestión de los metadatos y su importancia en los procesos de gestión documental consultar: *ISO 23081-1:2006. Information and documentation - Records management processes - Metadata for records - Part 1: Principles y ISO/TS 23081-2:2007 Information and documentation - Records management processes - Metadata for records - Part 2: Conceptual and implementation issues.*

defendemos el uso del formato XML para representar y almacenar el documento y los metadatos. Siguiendo la terminología OAIS<sup>52</sup> existen tres tipos de entidades llamadas contenedores o paquetes de información (*package information*), dependiendo de la fase del ciclo de vida del documento.

En primer lugar, existen los documentos que son transferidos en su formato originario por los productores de la documentación siguiendo los protocolos de transferencia establecidos por los responsables de iArxiu.<sup>53</sup> Éstos deben incluir los contenidos a preservar y todos aquellos metadatos que faciliten su recuperación, tratamiento y preservación. Los conocemos como *paquetes de información de transferencia* (PIT).

Cuando estos PIT ingresan en la plataforma se les aplica un conjunto de controles para verificar su integridad, autenticidad e idoneidad con los requerimientos de conservación. Se les añaden otro tipo de metadatos como los relacionados con la información de representación y los de auditoría. Finalmente, para garantizar su integridad se incorpora una firma digital de archivo. A esta normalización del PIT se le llama *paquete de información de archivo* (PIA).

Cuando un usuario quiera consultar un documento almacenado en el repositorio, el sistema le permitirá descargarse una copia del PIA que se denomina *paquete de información de consulta* (PIC).

Ante la ausencia de un modelo normalizado de estructuración, empaquetado y encapsulación de documentos electrónicos, y después de analizar los distintos esquemas existentes (XFDU, FOXML...)<sup>54</sup> hemos decidido utilizar el esquema METS<sup>55</sup> por varios motivos:

<sup>52</sup> Véase ISO 14721:2003, *Ob. Cit.* (nota 1).

<sup>53</sup> Para más información sobre el protocolo de creación de paquetes de información consultar el documento *iArxiu: Estructura i creació de Paquets d'Informació de Transferència (PIT) utilitzant el model METS* accesible en: [http://www.iarxiu.eocat.cat/documents/iArxiu%20v2%200%20-%20Estructura\\_PIT\\_%20METS\\_4.3\\_20090504.pdf](http://www.iarxiu.eocat.cat/documents/iArxiu%20v2%200%20-%20Estructura_PIT_%20METS_4.3_20090504.pdf).

<sup>54</sup> Para más información sobre el formato XFDU véase: *XML Formatted Data Unit (XFDU) Structure and Construction Rules, The Consultative Committee for Space Data Systems*, 2004 disponible en: <http://sindbad.gsfc.nasa.gov/xfdu/pdf/docs/1prwbv2a.pdf> (consulta el 04/01/2010). FOXML, Fedora Digital Object Model XML es el formato nativo del sistema Fedora. Para más información véase: <http://www.fedora.info/download/2.0/userdocs/digitalobjects/introFOXML.html> (consulta el 04/01/2010).

<sup>55</sup> El esquema METS, acrónimo de *Metadata Encoding & Transmisión Standard* es una norma para codificar metadatos descriptivos, administrativos y estructurales en cuanto a los objetos dentro de un repositorio expresado con el XML. Véase <http://www.loc.gov/standards/mets/> (consulta el 04/01/2010).

- Permite estructurar los documentos de una forma flexible (arbórea) que se adapta a las distintas formas de agrupar la documentación (documento o expediente).
- Admite diferentes diccionarios o vocabularios de metadatos.
- Permite el “crecimiento” del paquete a medida que se aplican procesos de migración a los ficheros.
- Permite especificar los ficheros tanto de forma incrustada en base64 como vinculados externamente.
- Permite generar un paquete de información autónomo, autosuficiente y “auto-documentado”, en formato XML, independiente del sistema y desprovisto de las dependencias tecnológicas de la aplicación que lo generó. Incluye:
  - Los contenidos a preservar (fichero/s).
  - Metadatos descriptivos necesarios para facilitar su búsqueda y recuperación.
  - Metadatos administrativos o de preservación necesarios para la gestión de los documentos a largo plazo (almacenamiento y acceso).
  - Metadatos estructurales que definen la estructura interna del paquete y los elementos que lo forman.

## XI. Modelo funcional del servicio

Para la definición, la construcción y la puesta en marcha del servicio de iArxiu hemos utilizado como modelo de referencia el elaborado por el *Consultative Comité for Space Data Systems* de la NASA, conocido como modelo OAIS, que se convirtió posteriormente en la norma internacional ISO 14721:2003: *Open Archival Information System*. La razón es muy simple, es el modelo más utilizado y asumido por otras instituciones para crear repositorios de custodia y preservación de documentos electrónicos a largo plazo.

La plataforma tecnológica que sustenta el servicio iArxiu está formada por cinco módulos funcionales. El **módulo de ingreso** incluye todas las funcionalidades relacionadas con la preparación, transferencia e ingreso de los paquetes de información de transferencia

(PIT) generados por los productores de la documentación hacia la plataforma iArxiu siguiendo el protocolo de transferencia definido por CATCert.

Cuando estos PIT ingresan en el **módulo de archivo** se les aplica un conjunto de controles para verificar su integridad, autenticidad e idoneidad con los requerimientos de conservación. A la normalización del PIT se le llama PIA (paquete de información de archivo). El PIA será almacenado en el repositorio digital el tiempo que proceda y se le aplicará la política de preservación adecuada y pertinente para garantizar su conservación y acceso a largo plazo.

El **módulo de preservación** se encarga de gestionar el ciclo de vida de los documentos e implementar las estrategias de preservación más idóneas para garantizar la conservación de los PIA. En iArxiu se apuesta decididamente por la técnica de la migración de formatos por su aceptación e incorporación en el entorno legal y normativo de la administración electrónica como técnica de preservación y garantía de accesibilidad, véase el concepto de copia auténtica en la LAECSP<sup>56</sup> y, por la normalización y estandarización de formatos abiertos que está ayudando a su consolidación, como los formatos PDF/A y ODF.

Para atender a las peticiones de consulta y visualización de documentos se ha construido un **módulo de acceso**. Este módulo incluye el propio acceso a los PIA utilizando un motor de búsquedas por metadatos descriptivos, la consulta de metadatos, la descarga y visualización de los ficheros; la expedición de copias auténticas electrónicas y, sobretodo,

<sup>56</sup> *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*. Artículo 30: "Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento".

Artículo 31: "Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones."

un servicio de conversión de documentos en línea que permite visualizar los documentos en multitud de formatos y así facilitar su disponibilidad futura.

El último **módulo**, el de **administración** es el que permite gestionar correctamente el funcionamiento de la plataforma. Encontramos la gestión de los usuarios del sistema, de la jerarquía documental, de las políticas de disposición y de acceso, de los vocabularios y plantillas de metadatos, además de la administración del registro de auditoría y de las estadísticas de uso del sistema.

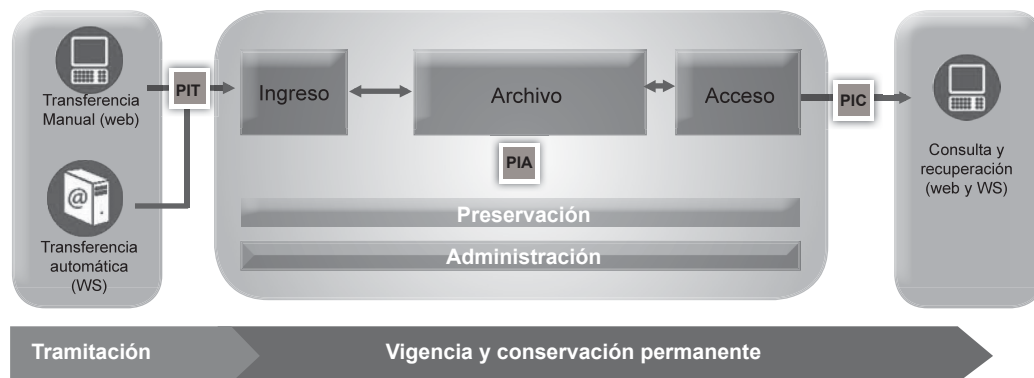


Fig. 1 – Esquema funcional del servicio iArxiu.

## XI.1 Módulo de transferencia e ingreso<sup>57</sup>

Este módulo es el encargado de recibir los PIT generados por las distintas aplicaciones o los sistemas de información de los productores de la documentación, además de validarlos y prepararlos para su almacenamiento y gestión dentro del archivo. En este contexto entendemos

<sup>57</sup> Para la definición de este módulo funcional los modelos de referencia han sido: ISO 20652:2005. *Space data and information transfer systems – Open archival information systems – Producer-Archive interface methodology abstract standard* y *Business Requirements Specification (BRS), Record Exchange Standard* disponible en <http://www.ica.org/sites/default/files/Record%20Exchange%20Standard.pdf> (consulta el 04/01/2010).

por transferencia todas las actividades implicadas en la transferencia de documentación de un sistema de información a otro, en este caso a la plataforma iArxiu:

- actividades administrativas incluyendo la negociación y definición del protocolo de transferencia entre el productor y iArxiu;
- el propio calendario de transferencias y;
- las operaciones concretas de transferencia.

A nuestro entender, la funcionalidad de la transferencia y su posterior ingreso es la más crítica de todo el sistema, pues debemos garantizar que en el propio proceso no se produzcan inconsistencias y que los paquetes de información se mantengan estables en su estructura, contenido y forma. Además, hay que encontrar el equilibrio entre los requisitos de iArxiu y los del productor. Por ejemplo, demasiada flexibilidad en el proceso de transferencia puede implicar que en el archivo se almacenen documentos de difícil gestión y preservación. Asimismo, si los requerimientos son demasiado complejos o implican elevados costes de integración los productores no utilizarán el servicio.

Para satisfacer estos requisitos hemos definido un proceso de transferencia e ingreso que incluye las siguientes fases:

- **Fase de preparación.** Incluye todas las actividades relacionadas con la gestión y la planificación adecuada de las transferencias. El objetivo es identificar qué tipo de documentación se debe preservar y su adecuación a los estándares de iArxiu, analizar la viabilidad y los costes del proyecto, diseñar los PIT, desarrollar la integración con iArxiu y firmar el convenio,<sup>58</sup> entre ambas partes, para regular la relación entre el productor y los responsables del servicio iArxiu.

<sup>58</sup> Para consultar el contenido del convenio acceder a: [http://www.iarxiu.eocat.cat/documents/Conveni%20iArxiu\\_2.0\\_20090625\\_pilots.pdf](http://www.iarxiu.eocat.cat/documents/Conveni%20iArxiu_2.0_20090625_pilots.pdf).

- **Fase de transferencia.** Una vez establecido el protocolo de transferencia hay que planificar su calendario y preparar el sistema para enviar la documentación:
  - Creación del PIT.
  - Preparación de la solicitud de transferencia.
  - Envío de la solicitud de ingreso del PIT.

Los usuarios tienen a su disposición dos formas para crear y transferir los PIT:

- De forma manual utilizando una interfaz web accesible con certificado digital: <https://www.iarxiu.eacat.cat/refweb>.
  - De forma automática utilizando los servicios web que ofrece la plataforma: <http://www.iarxiu.eacat.cat/core/soap/ingest.wsdl>.
  - Esta es la opción más idónea para los casos de integración entre una aplicación (por ejemplo, un gestor de expedientes o gestor documental) y la plataforma iArxiu.
- **Fase de ingreso.** Antes de proceder al ingreso de los documentos en el repositorio, iArxiu realiza una serie de tareas para verificar su integridad, autenticidad e idoneidad con los requerimientos de conservación:
    - Recepción de las solicitudes de transferencia, previa autenticación y autorización del envío.
    - Almacenamiento temporal de los PIT para proceder a su validación y completado. Los controles que se realizan son los siguientes:
      - Control de *checksum*, una medida muy simple para proteger la integridad de datos verificando que no hayan sido corrompidos.
      - Verificación de la existencia de virus en el PIT.
      - Introspección automática en los ficheros para extraer metadatos de carácter técnico útiles para garantizar su preservación.
      - Validación y, en el caso de utilizar el servicio de evidencia electrónica,

completado de las firmas digitales que forman parte del PIT.<sup>59</sup>

- Validación del contenido, de la estructura y la forma del PIT según lo establecido en el protocolo de transferencia.
- Incorporación de otros metadatos preestablecidos por el sistema o por las políticas de preservación con el fin de aumentar las garantías de preservación sobre el documento archivado.
- Generación del correspondiente registro de acciones o histórico de eventos con los datos del ingreso.
- Incorporación de un sello XAdES-A al paquete para garantizar su integridad.

<sup>59</sup> Cuando el productor de la documentación transfiere documentos a iArxiu puede que éstos tengan asociadas firmas digitales. A la vez, puede indicar si estas firmas deben ser preservadas o no. Si no se desea preservarlas simplemente se almacenarán y no se realizará ningún tratamiento sobre ellas. En esta situación, la validez jurídica de las firmas no se podrá garantizar con el paso del tiempo. En cambio, si se hace uso del servicio de evidencia electrónica, el sistema se encargará de realizar unos procesos de actualización, antes de ser almacenadas, para garantizar su validez a largo plazo.

El servicio de evidencia electrónica es útil y necesario para demostrar y testificar que un documento firmado es íntegro y auténtico y posee el valor indiscutible como evidencia electrónica. Para garantizarlo, iArxiu ejecutará las siguientes operaciones:

- Completado de la firma digital a la modalidad de archivo (AdES-A) con la incorporación de toda la información de contexto relacionado con la firma necesaria para ser validada en cualquier instante temporal (información sobre el certificado digital, incorporación del informe de validación que determina si en el momento de la firma el certificado era válido, etc.).
- Una vez validada y completada se almacena en un *stream* propio vinculado a la firma original.
- Extensión de la validez criptográfica de la evidencia electrónica mediante la actualización o refirmado periódico de las firmas cuando éstas pudieran ser susceptibles de ser modificadas o alteradas.
- La única limitación es que sólo se pueden preservar firmas en algún formato de firma avanzada AdES, como por ejemplo, CAdES y XAdES, ya que son las únicas que permiten su actualización periódica y el completado a la modalidad de archivo (AdES-A). Por este motivo es muy importante que en la fase de diseño de los trámites/sistemas que utilicen la firma digital se analice detalladamente el ciclo de vida de los documentos ya que en función del ciclo de vida habrá que escoger un tipo de firma u otro, atendiendo a las necesidades de preservación futuras.

Con independencia del mantenimiento y preservación de las firmas originales el sistema añade automáticamente un sello con la firma del archivo, del tipo XAdES-A, a todos los paquetes que ingresan en el archivo. La finalidad es garantizar que los documentos y sus metadatos sean auténticos e íntegros a partir del momento de la recepción y la validación de la transferencia.



- Generación del PIA, un objeto normalizado y apto para ser preservado en el repositorio digital en formato XML.
- Indexar la información de descripción para facilitar la búsqueda y la recuperación de los documentos.
- Enviar el PIA al repositorio para su almacenamiento y preservación.
- Creación del asiento correspondiente en el registro de transferencias.
- Notificación del éxito de la operación de transferencia al productor.

## **XI.2 Módulo de archivo: gestión del repositorio**

El sistema deberá custodiar y preservar los documentos, los PIA, durante largos períodos de tiempo. Como cualquier sistema de almacenamiento, iArxiu se basa en una doble estructura compuesta por un repositorio físico donde se registra la documentación y un sistema de ficheros que estructura de forma lógica la documentación contenida en el repositorio.

El almacenamiento de los documentos se realiza en el repositorio digital, el corazón mismo del sistema y, es el responsable de gestionar y mantener el archivo en condiciones de seguridad que den soporte a las operaciones de custodia, preservación y evidencia electrónica. En un primer momento, le corresponde recibir los PIA procedentes del módulo de ingreso y almacenarlos en el archivo durante el período de tiempo que establezca el calendario de disposición y retención.

Para mantener la información legible, interpretable y auténtica a largo plazo, es necesario que el sistema realice actuaciones planificadas y periódicas según lo establecido en la política de preservación. Este módulo es el responsable de ejecutar las medidas de preservación y restauración para hacer frente a la posible obsolescencia del hardware; mitigar las dependencias del software; solucionar el deterioro de los soportes de almacenamiento y minimizar el riesgo de pérdida de datos.

Las actividades principales que se realizan son:

- Gestión de la jerarquía de almacenamiento.
- Construcción del archivo según los niveles y los controles de seguridad que minimicen los riesgos comentados anteriormente lo que incluye un análisis de riesgo; un diseño seguro, una política de acceso físico, etc.
- Diseño de un sistema de protección y recuperación de datos que incluya la encriptación de datos, la política de copias de seguridad, la duplicación y la replicación de la información.
- Refresco de los soportes de almacenamiento, comprobación de su estado y mantenimiento en condiciones ambientales de funcionamiento estables.
- Implantación de mecanismos de control de la integridad de los datos.
- Provisión de toda la información necesaria para que se pueda acceder a los paquetes y así facilitar su difusión.
- Gestión y mantenimiento de la base de datos.

### **XI.3 Módulo de preservación**

La preservación digital intenta aportar soluciones para garantizar la conservación de los documentos electrónicos, sea cual sea su formato, el software, hardware o sistema que se utilizó para su creación, manteniendo así la información disponible pese a los rápidos cambios tecnológicos. Todos los documentos, independientemente de su formato y el medio de almacenamiento, están asociados a un ciclo de vida que determina el tiempo de retención en nuestros sistemas de información. A lo largo de su ciclo de vida debemos garantizar que su integridad, autenticidad, disponibilidad y fiabilidad no se vean comprometidas.

Las estrategias de preservación focalizan su atención en los dos aspectos más inherentes y esenciales de los documentos electrónicos: su contenido (el objeto digital o cadena de bits) y su significado (valor semántico).

El primer paso es preservar el documento en un soporte estable. Garantizar la integridad de su contenido y el mantenimiento de la secuencia de bits original a largo plazo es relativamente

sencillo, ya que sólo debemos aplicar una política planificada de renovación o refresco de los soportes de almacenamiento antes de que sean obsoletos o se hayan degradado e imposibiliten la recuperación de la información. De la misma forma, hay que establecer comprobaciones periódicas de su estado aplicando controles de integridad, para evitar riesgo de pérdidas de datos y mantenerlos en condiciones ambientales estables. La frecuencia de los refrescos dependerá de la política de preservación establecida y del tipo de soporte, así como de las limitaciones de rendimiento que establezcan los fabricantes de los soportes de almacenamiento. No obstante, el sólo preservar la integridad de los documentos no es suficiente para garantizar la disponibilidad y la accesibilidad a su contenido informativo a largo plazo.

El gran reto, y lo que realmente preocupa a los responsables de la gestión documental y a los productores de la documentación, es encontrar soluciones que permitan que el significado de los documentos sea accesible, interpretable y consultable a largo plazo. Actualmente ya existen varias técnicas de preservación digital como la emulación, la migración, la encapsulación o la virtualización que dan respuesta a estas necesidades. Escoger que técnica es la más adecuada debe determinarse en función del coste – beneficio que vayamos a obtener, los impedimentos legales y normativos, y los requerimientos de acceso que determinen los usuarios.<sup>60</sup>

En el servicio iArxiu apostamos decididamente por la estrategia de la migración. La migración se entiende como la transformación o conversión de un documento electrónico en un determinado formato a un formato más conocido o estable que pueda ser interpretado por los sistemas informáticos actuales, preservando la integridad del contenido del documento correspondiente y garantizando su correcta consulta y visualización en el futuro. Esta técnica se centra en adaptar el documento a las nuevas características del entorno tecnológico y se perfila como una de las estrategias a utilizar en el futuro por dos motivos:

<sup>60</sup> Para más información véase SERRA, J. 2001. "Gestión de los documentos digitales: estrategias para su conservación" en *El Profesional de la Información*, vol. 10, núm. 9 y LEE, K., SLATTERY, O., LU, R., TANG, X., MCCRARY, V. 2002. "The state of the art and practice in digital preservation" en *Journal of Research of the National Institute of Standards and Technology*.

- Por su aceptación e incorporación en el entorno legal y normativo de la administración electrónica como técnica de preservación y garantía de accesibilidad. Por ejemplo, la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos* incluye el concepto de copia electrónica y le otorga la misma validez que al documento original. Es decir, el objeto que se obtiene como consecuencia de aplicar la migración de un formato a otro más estandarizado tendrá la consideración de copia auténtica. Además, también regula la función de archivo y permite almacenar la información en otros formatos distintos al original siempre que se garantice su identidad, integridad y accesibilidad. Esta regulación y amparo legal nos va permitir estandarizar esta técnica y, seguramente impulsará la creación de herramientas de conversión de formatos.<sup>61</sup>
- La normalización y estandarización de formatos abiertos está ayudando a su consolidación, como los formatos PDF/A y ODF.<sup>62</sup> Es recomendable que las instituciones establezcan unos formatos normalizados para intentar reducir la cantidad de formatos existentes y, sobretodo, para facilitar las tareas de conservación ya que gestionar un reducido número de formatos permitirá a las organizaciones desarrollar procesos claros y coherentes de preservación alrededor de cada formato. También somos conscientes de que establecer estas listas de formatos “reconocidos” no es fácil porque muchas veces va a depender de la evolución del mercado y del contexto tecnológico.

Así, en el servicio iArxiu permitiremos la migración de los siguientes formatos, cuya decisión de aplicarlas dependerá de la estrategia de cada institución:

<sup>61</sup> Véase nota 13.

<sup>62</sup> Véase la *Norma ISO 19005-1:2005 Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)* y *ISO/IEC 26300:2006 Information technology - Open Document Format for Office Applications (Open Document) v1.0*.

Formato destino	application/msword	application/pdf	application/rtf	application/vnd.ms-excel	application/vnd.ms-powerpoint	application/vnd.oasis.opendocument.graphics	application/vnd.oasis.opendocument.presentation	application/vnd.oasis.opendocument.spreadsheet	application/vnd.oasis.opendocument.text	image/bmp	image/gif	image/jpeg	image/png	image/svg+xml	image/tiff	text/html	text/plain
application/msword		X	X						X							X	X
application/rtf	X	X		X				X	X							X	X
application/vnd.ms-excel		X						X								X	X
application/vnd.ms-powerpoint		X				X	X			X	X	X	X	X	X	X	
application/vnd.oasis.opendocument.graphics		X			X	X				X	X	X	X	X	X	X	
application/vnd.oasis.opendocument.presentation		X			X	X				X	X	X	X	X	X	X	
application/vnd.oasis.opendocument.spreadsheet		X		X												X	X
application/vnd.oasis.opendocument.text	X	X	X													X	X
application/vnd.openxmlformats-officedocument.presentationml.presentation		X			X	X	X			X	X	X	X	X	X	X	
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet		X		X				X								X	X
application/vnd.openxmlformats-officedocument.wordprocessingml.document	X	X	X						X							X	X
image/bmp		X				X				X	X	X	X	X	X	X	
image/gif		X				X				X		X	X	X	X	X	
image/jpeg		X				X				X	X		X	X	X	X	
image/png		X				X				X	X	X		X	X	X	
image/tiff		X				X				X	X	X	X	X		X	
image/vnd.dxf		X				X				X	X	X	X	X	X	X	
text/html	X	X	X	X				X	X								X
text/plain	X	X	X	X				X	X							X	

Fig. 2 – Relación formatos de migración.

El sistema dispone de un API que permite desarrollar *plugins* para conectarse a los motores de migración. Al día de hoy, la herramienta que utilizamos es *OpenOffice*.

Cuando se ejecute alguna operación de migración en un PIA para convertir algún documento a un formato más estandarizado, se procederá a actualizar el PIA. En primer lugar, el nuevo objeto pasará a tener la consideración de copia auténtica y será una nueva representación del documento originario. El documento resultante será firmado automáticamente por la plataforma y con un formato avanzado (XAdES-C detached), almacenando la firma resultante junto con el archivo migrado. Además, se añadirá al histórico de eventos del PIA un resumen de la operación de migración que se ha realizado y, finalmente, se añadirá una nueva firma del archivo para garantizar la integridad del PIA actualizado.

### **XI.3.1 Herramientas de análisis y registro de formatos**

Para facilitar la identificación de las características técnicas y el formato de los documentos electrónicos, entendiendo como formato la estructura interna y la codificación de un objeto digital, iArxiu dispone de una estructura basada en *plugins* que permite conectarse fácilmente con herramientas de introspección de formatos. Actualmente, se utiliza la herramienta de introspección tecnológica desarrollada por el departamento de preservación del Archivo Nacional del Reino Unido (TNA) llamada DROID<sup>63</sup> y la JHOVE.<sup>64</sup>

Estas herramientas automatizan al máximo los procesos relacionados con el tratamiento de los formatos: la identificación, la validación y la vinculación con la herramienta de gestión de los registros de formatos. Están diseñadas para satisfacer el requisito fundamental de cualquier repositorio digital: poder identificar y comprobar el formato exacto de todos los objetos digitales almacenados y vincularlo al registro de formatos.

<sup>63</sup> Para más información sobre DROID véase: <http://sourceforge.net/projects/droid://droid.sourceforge.net/wiki/index.php/Introduction> (consulta el 05/01/2010).

<sup>64</sup> Para más información sobre JHOVE véase: <http://hul.harvard.edu/jhove> (consulta el 05/01/2010).

La identificación y validación del formato en que el objeto digital está codificado es un requisito fundamental para facilitar su gestión posterior y permitir su consulta o descarga. Por este motivo se utiliza en la fase de ingreso de los documentos en el repositorio y facilita las tareas de identificación de los formatos a los productores de la documentación. Además la información que devuelve DROID y/o JHOVE se incorpora como metadatos de representación en el PIA, necesarios para poder solicitar, cuando se quiera acceder y recuperar el documento, el componente de visualización o visor correspondiente. También es una herramienta de control y nos permite denegar la petición de ingreso de un documento cuando el formato identificado no sea tratado por iArxiu porque el formato es propietario o no disponemos de la herramienta de visualización correspondiente.

Como se ha mencionado anteriormente es imprescindible conocer el formato del documento electrónico para garantizar su accesibilidad y permitir que su contenido sea interpretado correctamente por la herramienta de visualización de ficheros del sistema. Si no conocemos el formato, el documento solo es una colección de bits sin significado. De ahí, su relevancia. En consecuencia iArxiu dispone de un registro de formatos computacionales en el que se identifican de forma única e inequívoca los distintos formatos aplicados a ficheros, datos u objetos digitales en el que además se añade información completa del formato, incluyendo normas sintácticas y semánticas para codificarlos y descodificarlos correctamente. Para mantener la compatibilidad con la herramienta de análisis de formatos y evitar que iArxiu tenga que recoger y recopilar la información sobre los formatos ya existentes, hemos decidido utilizar como fuente el registro PRONOM, desarrollado también por el TNA.<sup>65</sup>

De la misma forma, iArxiu ofrece un servicio de visualización que permite presentar visualmente los documentos electrónicos en el formato de representación original o en el formato migrado. Sólo se incluyen visores *open-source*.

<sup>65</sup> Para más información sobre el registro PRONOM véase: <http://www.nationalarchives.gov.uk/pronom> (consulta el 05/01/2010).

## **XI.4 Módulo de administración**

Como cualquier plataforma, iArxiu incluye todas las funcionalidades necesarias para la configuración y la administración eficiente, segura y efectiva del sistema. Entre sus funcionalidades encontramos:

- La gestión de los usuarios y sus roles.
- La gestión de las aplicaciones de confianza que consumen los servicios web que ofrece la plataforma.
- La definición y gestión de las políticas de acceso al sistema.
- La definición, gestión y monitorización de las políticas de retención y disposición de los documentos cuyo objetivo es determinar el período de tiempo que los PIA deben permanecer en la plataforma (período de retención) en función de sus valores y asegurar su disposición correspondiente: eliminación, conservación permanente, conservación parcial y/o transferencia a otro repositorio.
- La definición y configuración de los vocabularios y las plantillas de metadatos que los usuarios utilizarán para describir los documentos.
- La gestión de la jerarquía documental (organismo, fondo documental y serie documental).
- Consulta del registro de acciones o historial de eventos y la consulta de las estadísticas de uso de la plataforma.

## **XI.5 Módulo de acceso**

Una de las funciones básicas de cualquier tipo de archivo es ofrecer algún tipo de herramienta a los usuarios para localizar la documentación que se halla en un archivo y, en el caso de un archivo digital, lo realmente interesante es garantizar la recuperación de los documentos y, especialmente, la visualización de éstos garantizando, en todo momento, el cumplimiento con la normativa vigente sobre acceso a los documentos por parte de los usuarios del servicio y a terceros.



Para facilitar el acceso a la documentación almacenada en el repositorio, iArxiu ofrece un motor de búsquedas a través de cualquier metadato descriptivo del PIA, ya sea vía interfaz web con certificado digital (<https://www.iarxiu.eocat.cat/refweb>) o a través de los servicios web que ofrece la plataforma (<http://www.iarxiu.eocat.cat/core/soap/dissemination.wsdl>).

Los usuarios podrán, si la política de acceso lo permite, acceder a los contenidos de los PIA y, optar entre los diferentes modos de visualización / recuperación:

- A. Consulta de los metadatos relacionados con el PIA.
- B. Consulta de los metadatos y visualización/descarga de los documentos (objetos digitales o ficheros) que forman parte del PIA.
  - En aquellos casos en que los documentos u objetos digitales se hubiesen migrado a un nuevo formato, el usuario podrá visualizar el documento original y la copia auténtica electrónica fruto de la migración, proporcionando el enlace al correspondiente visor.

En cuanto a la descarga de una copia del PIA, que se denomina *paquete de información de consulta* (PIC), el usuario puede escoger entre las siguientes modalidades:

- PIC en formato XML-METS que incluye sólo los metadatos.
- PIC en formato XML-METS que incluye metadatos más los contenidos u objetos digitales en B64.
- ZIP que incluye los metadatos en formato XML-METS y los objetos digitales.

Asimismo ofrece otras funcionalidades relacionadas con la consulta de los documentos:

- Consulta del historial de eventos.
- Conversión en línea de documentos. El usuario puede pedir descargar los ficheros en un formato distinto al original. A petición del usuario, iArxiu lo convertirá a uno de los formatos disponibles para que el usuario pueda visualizarlo sin problema. El nuevo binario será temporal y en ningún caso se almacenará para su preservación.
- Descarga de una copia auténtica en formato pdf.

## XII. Modalidades de uso y de prestación de servicio

Dada la heterogeneidad de necesidades y estructuras de las administraciones públicas catalanas y también del nivel de desarrollo y despliegue de la administración electrónica en el seno de éstas, existen dos formas de acceder a los servicios de la Plataforma iArxiu:

- Integración con aplicación corporativa (por ejemplo gestores documentales y/o gestores de expedientes) mediante los servicios web que ofrece la plataforma.
- Sin integración, utilizando las funcionalidades vía web:
  - Acceso con certificado digital en la web de referencia: <https://www.iarxiu.eacat.cat/refweb>.
  - Acceso a la web de referencia mediante la extranet de las administraciones públicas catalanas (eaCat): <https://www.eacat.cat/web/guest/Eacat>.

En relación al modelo de prestación del servicio existen dos posibles modalidades:

La primera de ellas, la modalidad de proveedor de servicios de aplicaciones, conocida por las siglas ASP (del inglés, *Application Service Provider*). En esta modalidad la administración usuaria o cliente utiliza la aplicación informática y los servicios de iArxiu a través de la red y además la infraestructura tecnológica que la sustenta y, en especial, el repositorio digital, reside en las instalaciones de un tercero, por ejemplo el mismo CATCert u otra administración pública. Es la mejor opción para administraciones pequeñas que no tienen los suficientes recursos, ni económicos ni personales, para asumir la construcción e instalación de la plataforma en sus instalaciones. Las responsabilidades se reparten de la siguiente forma:

- La administración cliente utiliza el software iArxiu para gestionar las transferencias; para definir las políticas del sistema; para gestionar la jerarquía documental y los usuarios; para la definición de las plantillas de metadatos; para la gestión de las consultas a los documentos y se encarga de la integración, si la hubiese, de su aplicación con iArxiu.
- El prestador del servicio (en este caso, CATCert) se encarga de la administración del

servicio de *hosting* o almacenamiento de los documentos; del mantenimiento de la infraestructura, de los servicios y de las aplicaciones relacionadas con la plataforma iArxiu y el propio mantenimiento correctivo y evolutivo de la plataforma. También incluye un servicio de soporte a los usuarios (formación y soporte técnico a los integradores).

En la modalidad de instalación cliente, la administración usuaria además de utilizar el software iArxiu, se encarga de la instalación, de la puesta en marcha y el mantenimiento de la infraestructura o hardware necesario para que funcione la aplicación. En este caso, CATCert se encarga de ceder bajo cesión el software y toda la documentación necesaria para que la administración cliente pueda desplegar la infraestructura, servicios y aplicaciones en sus instalaciones.<sup>66</sup> Es la mejor opción para organismos grandes, con presupuesto y los recursos suficientes. Las responsabilidades se reparten de la siguiente forma:

- La administración cliente utiliza el software iArxiu y además se encarga de la administración del servicio de *hosting* y de la plataforma.
- En este caso, CATCert da soporte técnico durante el despliegue de la aplicación y /o de nuevas versiones o *bugs* de la aplicación.

Escoger la modalidad de servicio dependerá de los recursos, del volumen de las transferencias y del modelo de relación y del modelo organizativo de cada administración.

<sup>66</sup> Aquellos que estén interesados en esta modalidad pueden consultar el siguiente documento donde encontrarán toda la información necesaria sobre los escenarios más representativos para desplegar e implementar la plataforma iArxiu en sus instalaciones: [http://www.iarxiu.eacat.cat/documents/iArxiu%20v2%20-%20Model\\_de\\_desplegament\\_v2.0.pdf](http://www.iarxiu.eacat.cat/documents/iArxiu%20v2%20-%20Model_de_desplegament_v2.0.pdf).

### XIII. Segundas conclusiones y futuro

El servicio iArxiu representa una de las primeras experiencias en relación a la preservación y almacenamiento de documentos electrónicos a largo plazo y, como tal espera aportar soluciones viables y tangibles para ayudar a la conservación y protección de la documentación electrónica. Como dice el *Manual de documentos electrónicos* elaborado por el Consejo Internacional de Archivos: “*la forma más segura de adquirir experiencia y especialización en este campo es actuar y no quedarse mirando*”.<sup>67</sup> Por eso sabemos que el servicio de iArxiu no finaliza aquí, sino todo lo contrario, tiene que mantenerse en permanente y continua evolución para adaptarse a las necesidades y requisitos del mañana.

En este sentido, las futuras líneas de actuación son:

- Abordar el tratamiento de la preservación y acceso de las bases de datos o información estructurada.
- Desarrollar más herramientas específicas de transformación o migración de documentos para dar cobertura a las necesidades de los usuarios y para facilitar la normalización del uso de formatos abiertos y estándares.
- Desarrollar un proceso de transferencia más flexible y que permita gestionar otras formas de estructuración de la documentación, además de METS, para facilitar la integración con el sistema.

En definitiva, se están llevando a cabo los pasos necesarios para que el compromiso respecto a la seguridad y conservación del documento público electrónico sea una realidad y así dar la confianza necesaria a todas las administraciones públicas catalanas para que puedan ir avanzando en esta digitalización de la administración, todo ello con las garantías técnicas y jurídicas de que los documentos electrónicos son, y continuarán siendo íntegros

<sup>67</sup> Véase el: CONSEJO INTERNACIONAL DE ARCHIVOS. COMITÉ DE ARCHIVOS DE GESTIÓN EN ENTORNO ELECTRÓNICO, 2006. *Documentos electrónicos: manual para archiveros*. Madrid: Ministerio de Cultura, Subdirección General de Publicaciones, Información y Documentación, 2006.

y, por tanto auténticos y sabiendo que se podrán recuperar siempre que sean requeridos, ya sea hoy o en el futuro.

---

Alicia Barnard

---

**La valoración documental**  
De los archivos en papel a los archivos digitales



## Amozorrutia

Consultora en archivos, con experiencia en la práctica archivística en archivos gubernamentales en México (1990-2008). Coinvestigadora del TEAM México del Proyecto InterPARES, y del Grupo de Reflexión sobre Evaluación Documental Latinoamericano FIED a partir de 2010, donde coordina el grupo de evaluación/valoración de documentos de archivo digitales. Fue representante ante el Comité Técnico Consultivo de Correspondencia y Archivo del Archivo General de la Nación. Ha publicado y presentado trabajos sobre archivística y documentos de archivo digitales tanto en México como en el extranjero.

## I. Resumen

La valoración documental,<sup>1</sup> como proceso para emitir un juicio de valor sobre el destino que se dará a los archivos una vez concluida su vida administrativa es, en esencia, una práctica similar tanto para los archivos en papel como para los archivos digitales; no obstante, en el ambiente digital se hace necesario incorporar nuevos elementos. En este trabajo se hace una revisión de las teorías sobre la valoración propuestas por Hilary Jenkinson y Teodoro Schellenberg, así como otro planteamiento de mayor actualidad relacionado con usos y usuarios; también se hace una revisión de las prácticas para valoración documental en archivos “leíbles en máquina” y se revisa la propuesta sobre macrovaloración, para finalizar, con el planteamiento del proyecto InterPARES respecto de la valoración documental de los documentos de archivo digitales.

## II. Teorías sobre la valoración

Respecto de la selección y destrucción de archivos, Hilary Jenkinson identifica rasgos comunes a considerar:

1. Las razones y justificación para la destrucción.
2. El método de seleccionar para la destrucción con las precauciones que se consideren necesarias.
3. Las personas a quienes se encarga la tarea de seleccionar.

Respecto de los archivos del futuro, en 1922 Jenkinson reconocía que el crecimiento de éstos se convertiría en una carga excesiva para el trabajo archivístico. Proponía que

<sup>1</sup> Para fines de este trabajo la definición del concepto *valoración* es el establecido por el proyecto InterPARES que significa: El proceso de evaluar los documentos de archivo con el propósito de determinar el período y condiciones de su preservación. Disponible en inglés en InterPARES 2 *Terminology Database*. [http://www.interpares.org/ip2/ip2\\_terminology\\_db.cfm](http://www.interpares.org/ip2/ip2_terminology_db.cfm) y en español en [http://www.interpares.org/ip3/ip3\\_documents.cfm](http://www.interpares.org/ip3/ip3_documents.cfm).



fuera el administrador (creador)<sup>2</sup> el responsable de realizar dicha selección y destrucción, antes de su transferencia a un archivo histórico. Sustentaba esta propuesta en los problemas encontrados por los archivistas de un archivo histórico en cuanto a determinar la forma o sistema de selección y destrucción con documentos. Señalaba también que al delegar esta actividad al creador, se aseguraba que en el futuro fuera posible contar con al menos un grupo de archivos del pasado, no censurables por un trabajo de selección y destrucción realizado por el archivista. No obstante, consideraba de suma importancia la intervención de éste a fin de evitar la destrucción irracional y procurar que la misma fuera suficiente.<sup>3</sup> Bajo esta óptica se percibe que esta actividad debería realizarse de manera conjunta entre el creador y el archivista. Más adelante, en 1956 Jenkinson reconocía “la necesidad de disminuir mediante la selección de cierto tipo la cantidad intolerable de documentos acumulados por la administración moderna...una necesidad desagradable.... Porque....no puede haber un criterio absolutamente seguro....”.<sup>4</sup> Con esto último coincide Terry Eastwood cuando dice que “ninguna teoría de valoración... ha sido aceptada de forma general como fundamento de metodología y práctica”.<sup>5</sup>

Por su parte, Teodoro Schellenberg también alrededor de los años cincuenta señalaba que el crecimiento de los archivos correspondía al crecimiento de la población desde el Siglo XVIII y comentaba que su reducción era necesaria, tanto para el gobierno como para el investigador, debido a que para los gobiernos era imposible mantener el alto volumen de

<sup>2</sup> La definición del concepto creador que será utilizado en este artículo corresponde a la que se define en el Glosario del Proyecto InterPARES, el mismo significa “*Persona física o jurídica que hace, recibe o acumula documentos de archivo por razones de su mandato, misión, función o actividades.* Disponible en [http://www.interpares.org/display\\_file.cfm?doc=ip3\\_mx\\_glosario\\_interpares\(20090318\).pdf](http://www.interpares.org/display_file.cfm?doc=ip3_mx_glosario_interpares(20090318).pdf)(consulta, Febrero, 2010).

<sup>3</sup> Hilary Jenkinson: (1922) *A manual of Archive Administration. Including problems of War archives and archives making.* Oxford at the Clarendon Press. London, Edinburgh, New York, Toronto, Melbourne and Bombay. HUMPHREY MILFORD, pp. 130-131.

<sup>4</sup> Elizabeth Shepherd y Geoffrey Yeo (2003). *Managing Records. A handbook of principles and practice.* Facet Publishing, Londres. Pp. 149-150.

<sup>5</sup> *Ibid.* 5, pp. 148.

documentos que producían las dependencias de ese entonces.<sup>6</sup>

Los conceptos y propuestas vertidas por Schellenberg, son conocidos por todos los que nos dedicamos a las tareas archivísticas aunque no está de más revisarlas. Éstas tenían como base un sistema de valores de documentos de archivo, un valor primario y uno secundario. El primero, de interés para las instituciones con propósitos administrativos, legales o fiscales; el segundo, es el que prevalece después de la conclusión de uso en oficinas, al que divide en dos:

1. la **evidencia** que contienen los archivos respecto de la organización y funcionamiento de las dependencias del gobierno, y
2. la **información** que contienen los archivos respecto de personas, organizaciones, cosas, problemas, condiciones con las cuales trata la dependencia de gobierno.

A estos valores los llamaré evidencial e informativo. Schellenberg se refería al carácter e importancia del asunto evidenciado, a diferencia de Jenkinson que reconocía como evidencia aquella que se deriva de “la custodia ininterrumpida” hasta su llegada al archivo histórico; agrega Schellenberg que estos dos valores podían coexistir en los documentos y propone que sea el archivista quien lleve a cabo una prueba de los valores evidenciales e informativos, contrario a la posición de Jenkinson quien pugnaba por no comprometer al archivista en el proceso de valoración. Para decidir cuales serían los archivos a preservar, el archivista debía tomar en consideración las siguientes preguntas:

1. ¿Cuáles unidades organizacionales en la oficina central de una dependencia tienen responsabilidad primaria para realizar decisiones respecto de su organización, programas, políticas y procedimientos? ¿cuáles oficinas realizan actividades auxiliares a esas decisiones? ¿cuáles series documentales son esenciales para reflejar tales decisiones?

<sup>6</sup> Theodore R. Schellenberg, “The Appraisal of Modern Public Records”. In. *A Modern Archives Reader: Basic Readings on Archival Theory and Practice*. Editors. M.F. Daniels y T. Walch. The National Archives and Records Service. 1984. Pp. 57-70.

2. ¿Con qué funciones de una dependencia se relacionan los archivos? ¿son funciones sustantivas? ¿cuáles series de archivos son esenciales para mostrar que cada función sustantiva fue realizada en cada nivel organizacional tanto en oficinas centrales como externas?
3. ¿Qué actividades de administración y supervisión están involucradas en cierta función? ¿cuáles archivos pertenecen a una función directiva, distinta de la función de ejecución? ¿en qué extensión se duplican tales archivos dentro de los niveles organizacionales? ¿cuáles archivos resumen las transacciones sucesivas realizadas bajo la función? ¿qué archivos deberían preservarse como una forma ejemplar para mostrar el proceso de trabajo en los niveles organizacionales más bajos?

Con el propósito de determinar el valor informativo de los documentos de archivo Schellenberg estableció tres conceptos:

- Ser único, es decir que no se encuentra en otros documentos en forma tan completa y accesible,
- La forma o grado en el cual la información es concentrada, y
- La importancia relacionada con asuntos imponderables que no pueden ser valorados con certeza, es decir, se asume una obligación de preservar archivos que contienen información para satisfacer las necesidades del Gobierno y que después puedan servir a los investigadores y al público en general.<sup>7</sup>

Mientras tanto, la tradición europea hacía énfasis en que la autenticidad de los archivos tenía su origen en las relaciones, por lo que se consideraba que cualquier selección artificial afectaba negativamente su imparcialidad como evidencia; se veía a cada documento de archivo como único en su contexto y de valor igual.<sup>8</sup> En esa época la visión de Jenkinson, en cuanto a que los administradores deberían ser los responsables de determinar el destino

<sup>7</sup> T.R. Schellenberg *Op. cit.* pp. 57-65.

<sup>8</sup> *Ibid.* 5 p. 149.

final de los documentos de archivo, se vio reflejada en el Comité Grigg en el Reino Unido (1952), donde se buscaba la mínima participación del personal de la *Public Record Office* en el proceso de valoración. Así, el Comité incluye procedimientos de transferencia al *Public Record Office* dividiendo los archivos en dos categorías: aquellos relacionados con asuntos de política, finanzas, legales y en otros asuntos generales y expedientes de casos (asuntos) o documentos muestra. El Comité recomendaba que:

- Los expedientes en la primera categoría deberían ser revisados por el personal de las oficinas cinco años después de cerrarse, utilizando el criterio de necesidad del propio departamento.
- Una siguiente revisión por el remanente debería llevarse a cabo 25 años después de la fecha de apertura utilizando ahora, criterios históricos.
- Los expedientes en la segunda categoría deberían normalmente programarse para destrucción en la primera oportunidad. Los expedientes de ambas categorías seleccionadas para la preservación en el largo plazo serían transferidos al *Public Record Office* antes de que llegaran a cierta edad (originalmente 50 años los cuales se han reducido recientemente a 30 años).<sup>9</sup>

Respecto de las propuestas de Jenkinson y Schellenberg, en torno a la valoración documental Ellen Shepherd and Geoffrey Yeo, en su excelente libro *El manejo de los archivos. Un manual de principios y prácticas* nos exponen sus limitaciones, las cuales resumo a continuación.

La visión de valoración de Jenkinson es ampliamente reconocida como intelectualmente coherente pero no práctica en el mundo moderno, como en el caso del Sistema Grigg-Jenkinson propuesto por el ya citado Comité Grigg, el cual tenía como base la valoración de expediente por expediente, estrategia factible cuando los archivos no representen al responsable de la valoración una carga excesiva por su volumen. Por otra parte, el sistema de valores de Schellenberg ha sido criticado con mayor frecuencia, por tener defectos y

<sup>9</sup> *Ibíd.* 5 pp. 149-150.

ser confuso. En particular, es rebatido por su enfoque en un contenido de hechos y en la presunta falla para reconocer la importancia de una evidencia auténtica que respalde las necesidades de la organización, la transparencia y la rendición de cuentas, aunque habría que considerar que a mediados de los 50's estos últimos dos factores no eran temas de relevancia en las instituciones. Otra crítica a su modelo ha sido la falta de visión en cuanto a la complejidad respecto del esquema de valores que propone, asume que las organizaciones solo tienen propósitos administrativos, legales y fiscales y que los usuarios externos solo tienen intereses culturales, i.e. de evidencia e información.<sup>10</sup>

Dentro de las propuestas más recientes para la valoración documental se encuentra la macrovaloración cuyo principal promotor es el archivista canadiense Terry Cook, (1992). Esta práctica se enfoca al proceso que da lugar al documento, en lugar de enfocarse al documento de archivo. Para ello se propone la elaboración de informes donde se describen los procedimientos para evaluar la importancia social de dichos procesos, a partir de los cuales se elaboran juicios acerca de la importancia de las relaciones de los documentos de archivo y las organizaciones. Respecto de la macrovaloración, Beaven<sup>11</sup> señala que ésta, en principio, pretende evaluar el alcance, contenido, naturaleza e importancia de un gran grupo de organizaciones y sus funciones. Según este enfoque, continúa Beaven, al determinar cuáles son las funciones más importantes socialmente, es posible establecer cuáles son los archivos que tienen mayor importancia archivística. Posteriormente, una vez identificados los archivos con alta importancia social, entonces la valoración cambia al creador en particular, enseguida se analiza la relación en su contexto estructural y funcional establecido por la actividad social y/o las características del creador. La macrovaloración es generalmente necesaria, pero como un ejercicio secundario y se utiliza para validar y refinar la hipótesis establecida acerca de la ubicación de las actividades funcionales más importantes de una organización y los creadores más significativos de documentos de archivo.<sup>12</sup>

<sup>10</sup> *Ibíd.* 5 pp. 160.

<sup>11</sup> Bryan P. N. Beaven (1999). *Macro-Appraisal: From Theory to Practice*. *Archivaria* 48:154-198.

<sup>12</sup> *Ibíd.* 12.

Una de las principales críticas a la macrovaloración es que la misma no prevé que los archivistas o gestores de documentos revisen los documentos de archivo ya que las decisiones se toman al evaluar el contexto de las actividades de su creación. Por otra parte, según Beaven este esquema puede olvidar las necesidades de los usuarios. Los métodos de macrovaloración dependen en evaluar y dar prioridad al valor aunque éste se encuentra disfrazado al usar los términos “importancia” o “significancia”.<sup>13</sup> La macrovaloración (también conocida como valoración funcional) ha sido adoptada por los archivos nacionales de Holanda, Australia y Canadá con el propósito de contar con medios prácticos para valorar grandes volúmenes, mientras que los Archivos Nacionales de Estados Unidos ha utilizado la valoración del documento de archivo en lugar de la función.<sup>14</sup>

La propuesta de valoración de los documentos de archivo de Shepherd y Geo se percibe como la integración de los planteamientos arriba comentados, la misma tiene como base las necesidades de los propósitos o fines de uso de los archivos, así como los costos y los riesgos en los que se incurren si los archivos no son preservados, la estrategia, que a continuación se resume, tiene como base un esquema de toma de decisiones de la cual se destaca lo siguiente:<sup>15</sup>

- La toma de decisiones sobre valoración documental debe realizarse en la etapa inicial de los documentos de archivo, cuando los sistemas de gestión son diseñados se tienen mayores ventajas.
- Es un prerrequisito conocer el ambiente de la organización y sus funciones y procesos.
- Es posible tomar una decisión al macro nivel de la función cuando los archivos están orientados a un propósito social, pero si existen requisitos especiales de una función particular, entonces es necesario llevar a cabo una valoración a un nivel más bajo.
- Los cuadros o esquemas de clasificación funcional son los más apropiados para la

<sup>13</sup> *Ibid.* 12.

<sup>14</sup> The *Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project (2005)*. Ed. Luciana Duranti. Appendix 3. *Appraisal of Electronic Records: A review of the Literature in English*, (Appraisal Task Force). Archilab. 2005 pp. 231-233. Disponible en <http://www.interpares.org/ip2/book.cfm> (consulta. Marzo, 2010).

<sup>15</sup> *Ibid.* 5. 153-155.

valoración documental pues proporcionan una firme conexión entre los documentos de archivo y el contexto de su creación.

- Debido a que las decisiones de retención pueden ser con frecuencia aplicadas a todos los documentos de archivo de una serie, éste será por lo general el nivel clave para el control de retención. Sin embargo a veces es apropiado tomar decisiones a un nivel menor.

Shepherd y Geo proponen para la evaluación de los documentos de archivo las siguientes necesidades de uso:

- Para propósitos de la función o negocio cuando sustentan aspectos de la administración, regulación, servicio profesional, actividades económicas o transacciones entre individuos y organizaciones.
- Para fines de rendición de cuentas y transparencia a la que están obligadas las organizaciones de acuerdo a disposiciones legales o reglamentarias.
- Con propósitos culturales cuando son utilizados como medio para conocer y entender una organización o aspectos de la sociedad.

Para esto establecen los valores que a continuación se describen y que pueden tener usos internos (en las organizaciones) y externos (por la ciudadanía):

1. **Evidencial.** Los documentos pueden servir de evidencia de una actividad mediante la cual se crearon y son usados cuando se requiere prueba de esa actividad.
2. **Informativo.** Los documentos se usan como fuentes de información, para la búsqueda de hechos o conocimiento, acerca de estructuras, operaciones, temas, personas o lugares.
3. **Estético.** Los documentos de archivo pueden usarse porque son obras de arte, cuando los usuarios están interesados en las cualidades estéticas, tangibles, forma física o valores asociados, este valor es raro en archivos nuevos y generalmente se guardan porque son inusuales, o agradables a la vista o, por razones simbólicas vinculadas a un evento en particular.

Por lo general, los archivos con valor evidencial tienen un alto uso para las actividades de las instituciones, así como para la rendición de cuentas y la transparencia por parte de los usuarios internos. Aquellos que tienen un valor informativo tienen también un alto uso dentro de las instituciones, en el caso del valor estético o artístico éste tiene una necesidad baja dentro de las instituciones. En cuanto a los valores que los usuarios externos buscan en los archivos, el evidencial es también altamente requerido para la transparencia y rendición de cuentas; el valor informativo tiene una alta utilidad cultural (académica, de investigación, etc.) por estos usuarios y el valor estético en los documentos de archivo es igualmente buscado por usuarios externos.

La valoración de los documentos “leíbles en máquina” ha sido una tarea que los Archivos Nacionales de Estados Unidos de Norteamérica han realizado desde 1969. Mediante este concepto se consideraba una amplia gama de medios de almacenamiento tales como las tarjetas perforadas, discos magnéticos, *cassettes*. Charles M. Dollar<sup>16</sup> hace una revisión interesante en cuanto a la valoración de este tipo de documentos de archivo, describe los procedimientos a seguir así como la documentación soporte, necesaria de acuerdo a los procesos establecidos por los Archivos Nacionales de Estados Unidos de Norteamérica. A continuación se resumen aspectos relevantes.

La primera decisión de valoración correspondía al creador o responsable de los archivos en las oficinas. En las tablas de disposición ya se disponía que los archivos maestros<sup>17</sup> serían valorados para su envío a los Archivos Nacionales, sin que esto fuera garantía de su recepción, los mismos debían acompañarse con documentación técnica, al menos aquella relacionada con formatos y códigos, así como la descripción de personas, lugares o cosas que cubrían los archivos. Esta información técnica era considerada como auxiliar en la consulta de las cintas. A continuación, si la cinta estaba intacta se checaba físicamente su legibilidad

<sup>16</sup> Charles M. Dollar: “Appraising Machine-Readable Records”. En *A Modern Archives Reader: Basic Readings on Archival Theory and Practices*. Ed. M. F. Daniels y T. Walch. National Archives and Records Service. Washington, D.C. 1984. Pp. 57-65.

<sup>17</sup> Se entendía a los “archivos maestros” como cintas de carrete que contenían archivos “originales” y no copias de los mismos .



en computadora, cuando ésta no podía leerse, se tomaban decisiones respecto del alcance y magnitud del daño, así como el valor básico del archivo.

En cuanto a los valores legales, evidenciales e informativos de los documentos de archivo, destaca Dollar la importancia de aquellos que por su valor legal se debían conservar de manera permanente como en el caso de registros de ventas de tierras. En cuanto al valor informativo éste era evaluado en proporción a su nivel de agregación y comenta que los datos a un micronivel no agregados tenían un mayor potencial para un procesamiento futuro. Además, se evaluaba el potencial del archivo para su procesamiento futuro y su vinculación. Dollar señala que la vinculación del archivo con otros datos era importante para el valor informativo; así, los archivos organizados a nivel de unidad (un individuo, una empresa) tenían un alto potencial de vinculación. También los atributos como lugar de residencia, ocupación, sexo, edad, permitían el vínculo con grupos con atributos similares.

Después de esta prueba de valor informativo, la validación de datos era un siguiente elemento a considerar, ésta involucraba una comparación manual de las especificaciones de código y formato mediante una impresión parcial. Cualquier inconsistencia no vista en el código o falta de datos eran considerados en el reporte de valoración. Esta validación también incluía la legibilidad y validez de los datos.

Si la cinta con archivos maestros satisfacía los criterios señalados, entonces el arreglo y accesibilidad de datos y los costos estimados de preservación debían sopesarse contra el valor documental antes de su ingreso a los Archivos Nacionales. Por arreglo se entendía la estructura interna de datos del archivo y la accesibilidad en cuanto a su dependencia o no dependencia en el software. Los archivos nacionales caracterizaban a un archivo “dependiente de software” cuando su acceso y procesamiento dependía de cualquier sistema o paquete. Al respecto, la política de los Archivos Nacionales era preservar los archivos independientes al software utilizado en su creación. Así, cuando los casos, lo ameritaban era necesario realizar una conversión, procedimiento que era costoso y largo.

Dollar, señalaba que los costos de ingresar y preservar y preparar para su divulgación un carrete de cinta magnética y su preparación para diseminación era de \$360.00 dólares

de la época, incluyendo tiempo del empleado, tiempo de computadora, entre otros. Esto siempre y cuando el carrete estuviera en un software no dependiente con código estándar y sin requerir de compactación de datos. Agrega que un estimado respecto de los 1,500 carretes de cinta que ya se encontraban en los acervos de los Archivos Nacionales representaba una inversión de aproximadamente un millón de dólares, la mitad correspondía a actividades de conversión y preservación en el largo plazo.

En su conclusión Dollar destaca dos factores asociados al crecimiento ineludible del almacenamiento de datos y archivos en computadoras:

- La imposibilidad de predecir, en ese entonces, el impacto en la valoración ante el desarrollo de minicomputadoras y el enorme crecimiento del procesamiento de palabras. Aunado a lo anterior, estaba el crecimiento desmedido de documentos de archivo que ya se creaban de forma descentralizada y de las dificultades existentes ante la ausencia de un control central. Esto debido a que la microcomputadora facilitaba su uso sin necesidad de especialistas para su manejo.
- Un problema más serio que Dollar ya visualizaba estaba relacionado con el incremento del manejo de sistemas de bases de datos, en particular en cuanto al ambiente de computadora en línea y la capacidad de acceso al azar que eliminaba la necesidad de almacenamiento secuencial o serial y la recuperación en común a través de cintas magnéticas de archivo, el usuario ya podía recuperar información de una variedad de áreas de almacenamiento instantáneamente sin conocer la ubicación física de los datos. Al respecto, Dollar reconocía que los elementos utilizados para la disposición de "archivos leíbles en máquina" basados en el paradigma de archivos en cintas magnéticas no serían viables en un ambiente de computadora en línea. Hacía finalmente énfasis en el incremento de los costos de preservación de este tipo de archivos en el futuro, mismos que además demandarían de la investigación que justificara su transferencia y recepción.

La investigación sobre los archivos digitales debido a factores como la falta de control en la creación de los mismos con la aparición de la microcomputadora o PC y el uso de información de diferentes fuentes, sin duda impactaron seriamente en la práctica archivística y en la valoración documental en particular, durante los últimos 30 años. Era necesario analizar si la archivística podía enfrentarse a la organización de archivos digitales, los cuales por primera vez adquirirían la característica de ser intangibles.

Harlod Naugler en un estudio RAMP<sup>18</sup> señalaba que la valoración de los documentos de archivo “leíbles en máquina” involucraba el análisis de contenido y el análisis tecnológico, el primero de acuerdo a los aspectos de valoración documental de archivos físicos y el segundo, lo consideraba como una actividad nueva pero de suma importancia en los documentos de archivo. Los elementos a considerar, que Naugler incluía para una evaluación técnica, eran la legibilidad de los documentos de archivo, la calidad de la documentación que acompañaba a los documentos de archivo electrónicos (al menos el diseño o diagrama o lista de los contenidos en un documento de archivo lógico que describe el ítem de información en cada campo, el largo de campo y la posición de cada campo en el documento de archivo), así como el catálogo de códigos (donde se localiza la explicación de los códigos utilizados para representar a la información en forma numérica). Como se verá estos elementos tecnológicos a considerar son semejantes a los considerados por los Archivos Nacionales de los Estados Unidos de Norteamérica. También, Naugler identificaba factores que tenían un impacto importante en la valoración de los documentos de archivo tales como:

- La legislación para inhibir o impedir a las instituciones archivísticas recibir o adquirir archivos electrónicos.
- Los datos localizados en una oficina podrían pertenecer a otra.
- Los datos que podían estar sujetos a acuerdos contractuales.

<sup>18</sup> Harold, Naugler. *The Archival Appraisal of Machine Readable Records: A RAMP Study with Guidelines* (París, Unesco, 1984). Disponible en: [http://unesdoc.unesco.org/ulis/cgi-bin/ulis.pl?req=0&mt=100&mt\\_p=%3C&by=2&sc1=1&look=default&sc2=1&lin=1&mode=e&utf8=1&gp=1&hist=1&text=Harold+Naugler&text\\_p=inc&submit=Search](http://unesdoc.unesco.org/ulis/cgi-bin/ulis.pl?req=0&mt=100&mt_p=%3C&by=2&sc1=1&look=default&sc2=1&lin=1&mode=e&utf8=1&gp=1&hist=1&text=Harold+Naugler&text_p=inc&submit=Search) (Consulta. Febrero, 2010).

- La existencia de programas de administración de datos dentro de las organizaciones.
- La dificultad para establecer vigencias después de que los sistemas han sido diseñados e instrumentados.
- La falta de capacitación de los archivistas en cuanto a valoración de archivos electrónicos.<sup>19</sup>

A finales de los años ochenta y ya en los noventa del siglo pasado, se hacía cada vez más claro que la aplicación de las técnicas de valoración documental desde la perspectiva de los “archivos leíbles en máquina” no estaba funcionando. Al respecto Margaret Hedstrom y Alan Kowlowitz concluyen:

- La preservación en el largo plazo depende de mejores programas de administración o gestión de documentos de archivo e información así como de una comunicación o disposición oficial acerca de la jurisdicción de los archivos.
- La necesidad de un sistema integrado para el manejo de archivos electrónicos y en papel basado en las necesidades de toda una organización.
- El establecimiento de vigencias al momento del diseño de los sistemas.
- La necesidad de mayores recursos para autoridad archivística a fin de enfrentar los problemas de los archivos electrónicos.
- El desarrollo de políticas y procedimientos para regular la elaboración y recepción de los documentos de archivo por funcionarios archivistas.<sup>20</sup>

De lo anterior, surgen inquietudes que dan lugar a los primeros documentos técnicos relacionados con el manejo de los archivos creados en un ambiente digital. Uno de los primeros estudios relacionados con la administración o gestión de archivos electrónicos en el entorno digital fue realizado por las Naciones Unidas en 1990 a través del Comité para la Coordinación de Sistemas de Información (ACCIS, por sus siglas en inglés) cuyo título fue la *Administración*

<sup>19</sup> *Ibíd.* 15.

<sup>20</sup> *Ibíd.* 21, pp. 225.

*de Documentos de Archivo: Temas y Lineamientos*, conocido como reporte ACCIS. Su propósito era impulsar programas de administración para uso en las organizaciones de las Naciones Unidas, tomando en consideración las prácticas tradicionales de los documentos de archivo y los archivos; se reconocía que las Naciones Unidas debían distinguir entre archivos y material no archivístico. También era necesario asegurar la autenticidad de los documentos de archivo; de acuerdo al reporte "...la legalidad de los archivos electrónicos dependerán de la evidencia que demuestre que éstos se crean dentro de un proceso normal de operación y que se ha instrumentado su cuidado y manejo adecuado durante el ciclo de vida del documento de archivo para asegurar su continuidad e inviolabilidad."

Por su parte, la *Guía para el Manejo de Documentos de Archivo Electrónicos desde la Perspectiva Archivística* (1997) elaborado por el Comité sobre Documentos de Archivo Electrónicos del Consejo Internacional de Archivos<sup>21</sup> hacía referencia al cambiante entorno de los documentos de archivo electrónicos dentro del cual se traslapaban tres fases en la evolución de las tecnologías de la información: la era de la computación central, la era de la computadora personal y la correspondiente a la era de la conexión de redes. En el manual también se habla de la influencia en los procesos de trabajo de las organizaciones y de cómo se veía afectada la procedencia, la propiedad y la ubicación física de los documentos de archivo. Asimismo, se hacía referencia a la obsolescencia tecnológica lo cual tenía como consecuencia implicaciones importantes para la valoración documental que requería de mayor estudio e investigación.

Lo anterior, así como aspectos legales y el desarrollo de sistemas de oficina que no eran fiables y el reconocimiento de la necesidad de identificar a los documentos de archivo de otro tipo de documentos electrónicos para manejarlos de tal forma que permitieran asegurar su confianza, llevó a académicos e investigadores de diferentes latitudes a intentar diferentes aproximaciones sobre los materiales digitales. Destaca el Proyecto de la Universidad de Columbia Británica (Proyecto UBC) el cual se orientó a revisar y estudiar de acuerdo con principios reconocidos y aceptados en ambiente tradicional como lo son las ciencias Archivística

<sup>21</sup> *Ibíd.* 15, pp. 236.

y Diplomática, (mientras la Archivística se encarga de estudiar a los documentos de archivo en agregaciones, la Diplomática estudia el documento de archivo de forma individual de tal forma que ambas disciplinas se integran en Diplomática Archivística para estudiar agregaciones de documentos de archivo digitales). Los hallazgos de este estudio dan lugar a las primeras aproximaciones sobre los componentes de un archivo electrónico, así como a la participación de este grupo de investigadores en la elaboración de uno de los primeros (sino es que el primero) estándares para archivos electrónicos la DOD 5015.2 "*Estandar para los criterios de diseño de aplicaciones de software para la gestión de archivos electrónicos*" de la Defensa de Estados Unidos de Norteamérica.<sup>22</sup> De igual manera, el Proyecto UBC viene a ser el detonante del Proyecto InterPARES (Proyecto Internacional de Investigación para el Estudio de la Preservación de Archivos Electrónicos Auténticos), mismo que ya tiene más de 10 años.

El Proyecto InterPARES ha dedicado especial atención a la valoración documental. En su primera fase las investigaciones realizadas tienen como resultado las siguientes conclusiones:

- Es mejor llevar a cabo la valoración de los archivos digitales cuando éstos están en etapa activa. Esto debido a que es posible tener acceso a la documentación acerca del rol operacional que juegan los documentos de archivo en la organización, de igual manera es posible tener acceso a la información técnica sobre la aplicación que genera y mantiene los documentos de archivo en etapas activa y semiactiva.
- El medio donde se localizan los documentos de archivo puede afectar el proceso de valoración pero no la tarea fundamental de asignar un valor. Hay nuevas tareas a desarrollar como la identificación de indicadores de autenticidad, la evaluación de estrategias de preservación.
- El monitoreo de la decisión de valoración para confirmar el valor archivístico de los documentos de archivo seleccionados es una actividad necesaria en el ambiente

<sup>22</sup> DoD 5015.2: *Electronic Records Management Software Applications Design Criteria Standard*, Department of Defense, United States of America, April 25, 2007. Disponible en <http://www.js.pentagon.mil/whs/directives/corres/pdf/501502std.pdf> (consulta febrero, 2010).

digital. Esto con el fin de ir al paso del cambio tecnológico.

- La información compilada durante la valoración deberá “empaquetarse” y tenerse a mano para apoyar en el monitoreo, transferencia, procesamiento, descripción preservación y acceso subsecuentes. La automatización de todos los aspectos del trabajo archivístico, incluyendo la valoración, facilitará el reuso constante, en fases subsecuentes, de la información integrada durante el proceso de valoración.<sup>23</sup>

Durante InterPARES 2, las investigaciones en cuanto a la valoración documental vienen a formar parte del Grupo Fuerza de Tarea de Valoración y Preservación y del Grupo Transversal de Modelaje.<sup>24</sup> Las investigaciones del Grupo de Valoración y Preservación dan lugar, entre otros documentos, a los *Lineamientos del Preservador. Preservación de Documentos de Archivo Digitales: Lineamientos para Organizaciones, así como los Requisitos de Referencia para sustentar la Presunción de Autenticidad de los documentos de Archivo Digitales*.<sup>25</sup> Por su parte en el Grupo de Modelaje se desarrollan dos modelos para los archivos electrónicos: el *Modelo de la Cadena de Preservación y el Modelo de Negocios*. El Modelo de la Cadena de Preservación representa las actividades para elaborar, mantener, valorar y preservar documentos de archivo electrónicos durante todo su ciclo de vida. En cuanto al Modelo de Negocios se orienta a la organización y su propio negocio o propósito dentro de contextos jurídicos, económicos y culturales y los documentos de archivo generados por ese negocio; comprende los documentos de archivo para uso cotidiano y aquellos que requieren retenerse y preservarse en el largo plazo para los intereses históricos de la sociedad.<sup>26</sup>

<sup>23</sup> Ivette Hackett (2007). *Methods of Appraisal and Preservation. Domain 3 Task Force Report*, pp. 2-3 versión electrónica disponible en [http://www.interpares.org/ip2/display\\_file.cfm?doc=ip2\\_book\\_part\\_4\\_domain3\\_task\\_force.pdf](http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_4_domain3_task_force.pdf) (consulta Febrero, 2010).

<sup>24</sup> Los reportes completos sobre los trabajos realizados por estos grupos se encuentran disponibles en <http://www.interpares.org/ip2/book.cfm> (Consulta. Febrero 2010).

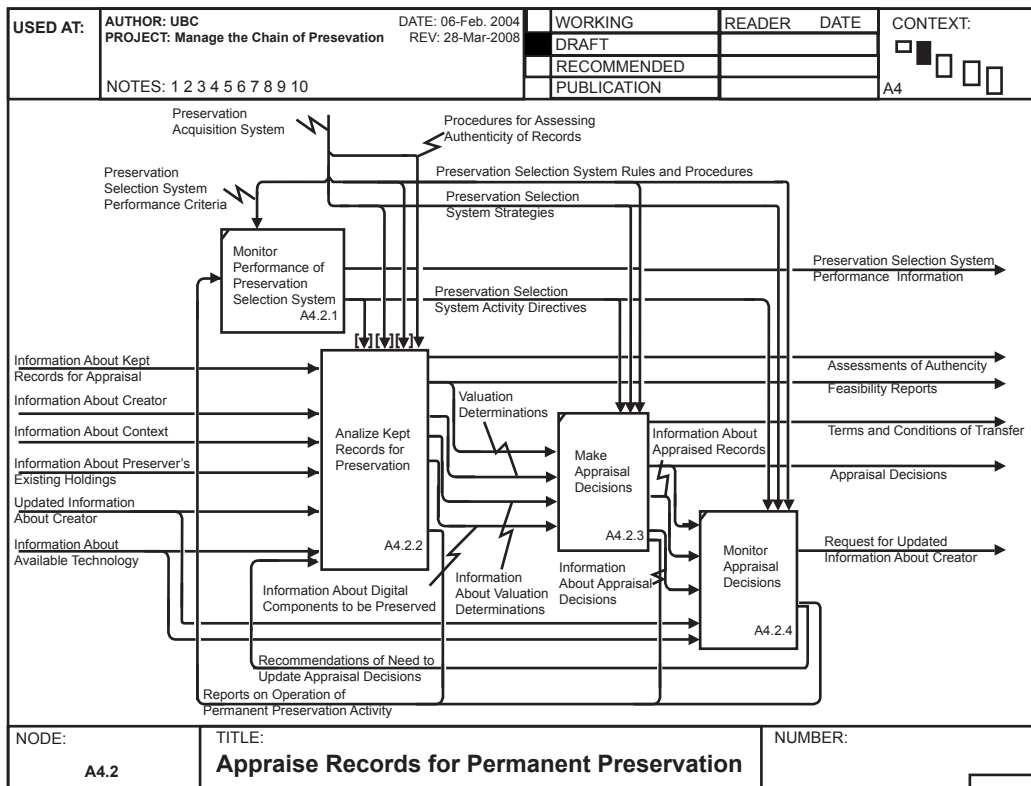
<sup>25</sup> Disponible en [http://www.interpares.org/ip2/display\\_file.cfm?doc=ip2\(pub\)preserver\\_guidelines\\_booklet.pdf](http://www.interpares.org/ip2/display_file.cfm?doc=ip2(pub)preserver_guidelines_booklet.pdf) (Consulta. Febrero 2010).

<sup>26</sup> Los modelos se encuentran disponibles en [http://www.interpares.org/ip2/ip2\\_models.cfm](http://www.interpares.org/ip2/ip2_models.cfm) (Consulta. Febrero, 2010).

Respecto del Modelo de la Cadena de Preservación, a continuación se incluye el esquema de actividades y flujos propuestos en cuanto a valoración documental, el cual se encuentra en inglés. Enseguida se resume la sección de valoración de los *Lineamientos del Preservador. Preservación de Archivos Digitales: Lineamientos para Organizaciones*.

### III. Modelo de la Cadena de Preservación

#### Valorar los documentos de archivo para su preservación permanente



<b>NODE:</b> A4.2	<b>TITLE:</b> Appraise Records for Permanent Preservation	<b>NUMBER:</b>
----------------------	--	----------------



## IV. Lineamientos para valoración de documentos de archivo para preservación permanente

**Valorar al inicio.** Debido a las dificultades técnicas en la preservación de archivos, es conveniente la identificación temprana de los documentos de archivo que serán preservados en el largo plazo. De igual manera, resulta apropiado que al momento de la valoración el preservador, junto con el creador, establezcan métodos e identifiquen estrategias de preservación.

**Ubicar dueños múltiples.** En casos donde los componentes intelectuales de una entidad digital tienen dueños múltiples, los mismos deben identificarse durante el proceso de valoración con el propósito de evaluar las ramificaciones que esta situación puede acarrear en la preservación en el largo plazo. Por ejemplo, en los sistemas donde se comparte información en diferentes niveles de gobierno pueden existir permisos para acceso sin que se hayan establecido políticas de preservación.

**Evaluar la autenticidad.** La evaluación de autenticidad ha sido parte de los procesos de valoración documental en archivos tradicionales, aunque en el ambiente digital se presentan dificultades y aún no se han establecido prácticas estandarizadas para evaluar la autenticidad en este medio. Esto debido a que las entidades digitales fácilmente se duplican, distribuyen, renombran, reformatean, o convierten, además pueden falsificarse fácilmente y sin dejar huella. Por ejemplo, la fecha de cualquier archivo digital puede ser modificado al ajustar el sistema de reloj; la introducción de redes de correos electrónicos permiten que los documentos de archivo viajen por nuevas rutas entre el personal en lugar de aquellas establecidas en los procedimientos de una oficina tradicional.

Por lo anterior, cuando se valoran documentos de archivo digitales, la evaluación de su autenticidad debe ser más abierta. La custodia ininterrumpida, el conocimiento de las prácticas de gestión documental y la verificación pueden ser aún elementos que permitan tener cierta certeza sobre la autenticidad de los documentos de archivo, sin embargo deben considerarse otros elementos como los que se indican en la siguiente sección.

**Documentar la evaluación de autenticidad.** Este reporte deberá documentar los controles que se establecieron para garantizar la identidad (que el documento es único) y la integridad (que está completo) del documento de archivo. Para ello y como ya se mencionó, se elaboraron *Requisitos de Referencia para sustentar la Presunción de Autenticidad de los documentos de Archivo Digitales*. Uno de los principios de InterPARES es el reconocer la autenticidad de los documentos de archivo mientras no se demuestre lo contrario. Así, para demostrar si los mismos son o no auténticos, a mayor cumplimiento de los requisitos mayor será la presunción de autenticidad de los documentos de archivo. A continuación se hace una descripción de los mismos.

**Requisito A.1.** Expresión de los atributos del documento de archivo y su enlace a éste. Los atributos están expresados explícitamente y vinculados inextricablemente a cada documento de archivo.

#### **Identidad del documento de archivo**

- Nombre de las personas que concurren en la formación del documento de archivo (autor, escritor, originador, cuando son diferentes al autor), nombre del destinatario.
- Nombre de la acción o materia,
- Fecha de creación (cronológica, de recepción, de archivo y de transmisión).
- Expresión de vínculo archivístico (código de clasificación).
- Indicación de anexos.

#### **Integridad del documento de archivo**

- Nombre de la oficina responsable.
- Nombre de la oficina de responsabilidad primaria (si es diferente a la anterior).
- Indicación de tipos de anotaciones agregados al documento de archivo posterior a su elaboración (fecha de recepción por ejemplo).
- Indicación de modificaciones técnicas. Comprende cambios en los componentes digitales e incluye cualquier cambio en la forma que cualquiera de los elementos

del documento de archivo están codificados digitalmente (software) y cambios en los métodos aplicados para su reproducción a partir de los componentes digitales almacenados; esto es, cualquier cambio que pueda hacer surgir preguntas sobre si el documento de archivo reproducido es el mismo antes de la modificación técnica. Estas modificaciones pueden estar referidas en documentos externos al sistema.

**Requisito A.2.** Privilegios de acceso, abarca la definición e instrumentación de privilegios de acceso en relación con la creación, modificación, anotación y destrucción de los documentos de archivo.

**Requisito A.3.** Procedimientos de protección: pérdida y alteración. Incluye el establecimiento e instrumentación de procedimientos para prevenir, detectar y corregir la pérdida o alteración de los documentos de archivo.

**Requisito A.4.** Procedimientos de protección: medios y tecnología. Comprende el establecimiento e instrumentación de procedimientos para garantizar la identidad e integridad continuada de los documentos de archivo en contra del deterioro de los medios y a través del cambio tecnológico.

**Requisito A.5** Establecimiento de formas documentales. El creador ha establecido las formas documentales de los documentos de archivo asociadas a cada procedimiento ya sea de acuerdo con los requisitos del sistema jurídico o por los propios del creador.

**Requisito A.6.** Autenticación. Cuando la autenticación es requerida por el sistema jurídico o por necesidades de la organización, el creador ha establecido reglas específicas respecto de cuales documentos de archivo van a ser autenticados, por quién y cuáles son los medios de autenticación.

**Requisito A.7.** Identificación del documento de archivo de autoridad. Se refiere al establecimiento de los procedimientos para identificar al documento de archivo de autoridad cuando existen múltiples copias del mismo documento de archivo.

**Requisito A.8.** Remoción y transferencia de documentación relevante. Si existe una transición de los documentos de archivo de su etapa activa a la semiactiva e inactiva

que involucra la remoción de documentos de archivo del sistema electrónico, se han establecido e implementado procedimientos para determinar qué documentación tiene que removerse y transferirse al preservador junto con los documentos de archivo.

## **V. Monitoreo de los documentos de archivo que han sido identificados para su preservación en el largo plazo**

El monitoreo de los archivos identificados para su preservación en el largo plazo debe llevarse a cabo en intervalos regulares hasta que los archivos son transferidos al archivo histórico. El monitoreo implica que el creador confirme que no hay cambios respecto de la creación y mantenimiento de los mismos; si los hubo, el creador confirmará que éstos no afectaron la naturaleza, atributos, valor, autenticidad y factibilidad de su preservación. Una actualización puede implicar un rediseño menor del sistema que podría remover la habilidad para separar documentos de archivo temporales de aquellos que serán preservados en el largo plazo. También los cambios dentro de la organización y de sus funciones pueden conducir a cambios en cuanto al uso de las aplicaciones de la computadora y la naturaleza y cantidad de datos que contienen. Los responsables de un rediseño del sistema podrían no darse cuenta de la existencia de un requerimiento para transferir los documentos de archivo al preservador designado antes de que el sistema sea modificado, esto podría dar lugar a la destrucción de los mismos. También, los discos duros pueden ser limpiados, las cuentas de los usuarios con todos sus archivos se pueden borrar, las cintas y discos reciclarse o destruirse sin entender el impacto de lo que tales acciones implican en la organización de los documentos de archivo o en las reglas o disposiciones de transferencia preexistentes.

**Actualizar la valoración.** Los cambios dentro de las organizaciones y de los sistemas de gestión documental son inevitables, de igual manera, las disposiciones organizacionales y responsabilidades cambian, también la forma en que estas responsabilidades se desarrollan y los datos acumulados en los sistemas existentes pueden tener nuevos usos, los cuales pueden incrementar su valor en el largo plazo. Lo anterior conlleva a actualizar la valoración

documental inicial durante las fases activa y semiactiva de los documentos de archivo digitales.

**Identificar los componentes digitales.** Los componentes digitales son entidades u objetos que forman parte de uno o más documentos digitales de archivo, incluyen, además, los metadatos necesarios para ordenar, estructurar o hacer manifiesto el contenido y requieren de una medida específica de preservación.<sup>27</sup> Por lo anterior, es necesario asegurar que todos los componentes digitales esenciales sean identificables y que las relaciones implícitas se hagan explícitas en los metadatos.

**Determinar la factibilidad de preservación.** Aunque no forma parte de la evaluación de los documentos de archivo el proceso de valoración debe concluir con una investigación cuidadosa de los requisitos técnicos para preservación. Las estrategias pueden variar en costo y pueden producir diferentes resultados. La determinación de la factibilidad es esencial para comprender el costo de recepción y preservación. No es una actividad nueva, se trata de una extensión al ámbito digital para identificar los recursos necesarios para la preservación. Los costos deben considerarse como recurrentes por ejemplo, recopiar acervos de un transportador físico (disco, *diskette*) a otro será una actividad tan frecuente como la obsolescencia del formato seleccionado, también la conversión de formatos será necesaria cuando la obsolescencia lógica pueda ser un riesgo para leer el contenido.

Para resumir, la **valoración al inicio** del ciclo de vida permite determinar si el documento de archivo debe conservarse para el largo plazo. Con lo anterior será posible establecer la disposición final del mismo (baja o preservación en el largo plazo); además, es necesario: **evaluar la autenticidad** de los documentos de archivo, determinar la **factibilidad** de preservación y **monitorear los documentos** de archivo seleccionados para preservación permanente. Al respecto Luciana Duranti, en cuanto a la esencia de la valoración documental comenta que la teoría no ha cambiado y comenta "...su propósito es aún el de preservar un documento de archivo concentrado y esencial del pasado que mantiene intactas todas sus características archivísticas en cuanto a su naturaleza, imparcialidad, interrelación, el ser

<sup>27</sup> En un documento de archivo es posible encontrar varios componentes digitales por ejemplo: un texto en procesador de palabras, una tabla en Excel, una firma electrónica.

único y lo más importante, la característica de autenticidad, sin la cual no se podría confiar en los documentos de archivo ya sea como evidencia o como fuentes de información.”<sup>28</sup>

## VI. A manera de conclusión

Además de InterPARES existe un número importante de iniciativas, documentos técnicos relacionados con la valoración; asimismo, los archivos nacionales de varios países han elaborado políticas o lineamientos destinados a este proceso. No sería posible en este documento hablar de los mismos, sin embargo está claro que la valoración de los documentos de archivo digitales se ha convertido en un tema relevante dentro de la comunidad archivística.

Al respecto conviene puntualizar lo siguiente:

- En países de Latinoamérica los temas relacionados con la gestión de archivos digitales han venido adquiriendo relevancia en un lapso muy corto, no obstante, el conocimiento sobre la valoración de estos materiales aún es escaso. Por fortuna, dentro del Proyecto con “Grupo de Reflexión sobre Evaluación/Valoración de Documentos en Iberoamérica”, financiado parcialmente por el Consejo Internacional de Archivos, recientemente se ha conformado el Grupo de Evaluación/Valoración de Archivos Electrónicos. En el proyecto participan expertos archivistas de Argentina, Brasil, Colombia, Costa Rica, España, México, Perú y Uruguay. En el grupo de valoración/evaluación de archivos electrónicos se pretende llevar a cabo un análisis exhaustivo con el propósito de elaborar un documento técnico de carácter general útil a la Región de Latinoamérica.
- El crecimiento exponencial de datos que se localizan en servidores de las instituciones, dentro de los cuales con seguridad existe una cantidad importante de documentos de

<sup>28</sup> Luciana Duranti. November 16, 2007 – Closing overview speaker. "Rethinking Appraisal - Conference Overview," DELOS International Conference, "Appraisal in the Digital World," in association with Digital Preservation Europe and InterPARES, 15-16 November 2007. Accademia Nazionale Dei Lincei, Rome, Italy. Disponible en [http://www.interpares.org/ip2/ip2\\_dissemination.cfm?proj=ip2&cat=pl-conf](http://www.interpares.org/ip2/ip2_dissemination.cfm?proj=ip2&cat=pl-conf).

los cuales un gran número reúne características de documento de archivo, trae como consecuencia costos elevados en los sistemas, el almacenaje y el software (se calcula que entre el 60% y 80% de los datos que se localizan en servidores son inactivos y los porcentajes siguen creciendo).<sup>29</sup> Esto obliga a considerar seriamente a la valoración como una práctica necesaria para los archivos digitales.

- La valoración documental por si sola no es una solución a la problemática que se enfrenta en el entorno de los archivos digitales, como también sucede en archivos en papel. Se requiere de la existencia de un sistema sólido de gestión, que incluya procesos e instrumentos técnicos útiles a la creación, organización, uso, mantenimiento y preservación de archivos digitales en el largo plazo.
- A fin de crear conciencia en cuanto al valor de los archivos como activos de las instituciones, se hace necesario iniciar trabajos sobre los riesgos a los que se enfrenta una organización privada o gubernamental ante la falta de archivos valorados para su preservación en el largo plazo que puedan presumirse auténticos. La opacidad de las instituciones, la invasión a la privacidad de las personas, la falta de prueba ante la ley o la carencia de información para ejercer un derecho ciudadano que en apariencia tendría tan solo un costo social, puede traducirse en costos económicos. Por ejemplo, ante la falta de transparencia en la aplicación de recursos de los gobiernos, hay mayores posibilidades de que la inversión de otros sectores se reduzca. De igual manera, existen costos económicos ante la falta de pruebas en juicios y controversias, tanto para las instituciones privadas como gubernamentales. Sin duda la historia de las instituciones y de la sociedad se encuentran también dentro de los factores de riesgos que se corren ante la falta de archivos organizados y valorados para su preservación en el largo plazo. En esto de la carencia de una identidad en un entorno, existen costos sociales y económicos necesarios de sopesar.

<sup>29</sup> Jack Olson (2009). *Data Archiving Basics. A new Function for Improving Data Management*. Disponible en [http://www.information-management.com/specialreports/2009\\_164/databases\\_data\\_management\\_storage\\_information\\_lifecycle\\_management-10016143-1.html](http://www.information-management.com/specialreports/2009_164/databases_data_management_storage_information_lifecycle_management-10016143-1.html) (Consulta. Febrero 2010).

---

Juan Voutssás

---

**La cadena de preservación en**  
archivos digitales



---

## Márquez

Es Ingeniero en tecnologías de la información con maestría y doctorado en bibliotecología y ciencias de la información. Investigador del Centro de Investigaciones Bibliotecológicas de la Universidad Nacional Autónoma de México. Ha sido consejero y consultor sobre tecnologías de la información y en sistemas para diferentes organizaciones. En los años recientes se ha enfocado en proyectos de preservación digital dentro de bibliotecas y ahora también en proyectos de preservación en archivos digitales. Es director del TEAM México del Proyecto InterPARES.

## I. Introducción

Entre los muchos sorprendentes hechos del advenimiento de las “Tecnologías de Información y Comunicaciones” —TIC— se encuentra la continua mejora y crecimiento en capacidad de los dispositivos para almacenamiento de información al mismo tiempo que sus costos se han reducido en la misma proporción. Los variados dispositivos y medios para almacenamiento ponen hoy en día al alcance de personas y organizaciones la capacidad de almacenar millones y millones de *bytes* de información de todo tipo: textos, imágenes, música, video, etcétera.

Durante los últimos cincuenta años el almacenamiento de datos, tanto magnético como óptico ha logrado maravillas en su relación costo/beneficio de una manera sorprendente; tanto que no se trata simplemente de un fenómeno de “*comodidad*” tecnológica o simple “*mejora de una capacidad*”. Debemos reflexionar acerca del hecho de que pocas cosas en la historia reciente del género humano han tenido un crecimiento y un abaratamiento tan espectacular como el almacenamiento opto-magnético. Es tan relevante este fenómeno, que ha cambiado en unos pocos años radicalmente el concepto social de lo que, —en lo tocante a información— es almacenable y lo que no.

Consideremos el primer dispositivo de *disco duro* comercial que existió: la unidad de disco “*disk drive*” IBM 350, que comenzó a comercializarse en septiembre de 1956 con la —entonces asombrosa— capacidad de 4.4 Megabytes.<sup>1</sup> El dispositivo no era exactamente un disco duro; en realidad era un “paquete” o conjunto de 50 discos de 24 pulgadas de diámetro cada uno; esto es 61 centímetros, 100 superficies en total. El gabinete que contenía los discos medía 1.73 mts. de altura, 1.52 mts. de frente y 74 cms. de fondo; prácticamente dos metros cúbicos. En la época en que apareció se rentaba, no se vendía, por 3,200 dólares mensuales —dólares de 1956—. Para tener una referencia, en ese entonces el *Ford Fairline Sunliner Convertible Coupé*, el modelo más caro de esa línea de autos familiares, se vendía por 2,359 dólares; el lujoso *Ford “Thunderbird”* se vendía ese año por 3,408

<sup>1</sup> 1 *Megabyte* = 1'000,000 = 10<sup>6</sup> “*bytes*” o caracteres.

dólares. Para tener un valor de compra de esa unidad de disco, si amortizáramos su renta a tres años tenemos un costo total de poco más de 115,000 dólares: aproximadamente 26,000 dólares por cada *Megabyte* de almacenamiento.

Ya para 1980 la empresa “*Morrow Systems*” vendía un disco duro de 26 *Megabytes* de capacidad por “sólo” 5,000 dólares: 193 dólares por *Megabyte*. En esa misma época aparecieron los primeros discos duros para PC, conocidos como “*Winchester*”: el ST-506, que tenía una capacidad de cinco *Megabytes* se vendía aproximadamente por 1750 dólares. Medía 8 x 15 x 20 centímetros; algo así como 2.4 litros de volumen. El costo unitario era por tanto de aproximadamente 350 dólares por cada *Megabyte* de almacenamiento.

Diez años después, a principio de la década de los noventa, se compraba un disco duro de “*Western Digital*” de 40 *Megabytes* por 1,200 dólares. El costo unitario se abatía entonces a 30 dólares por megabyte de almacenamiento. Para el año 2000 se podían comprar ya *Gigabytes*<sup>2</sup> —mil *Megabytes*— a un costo unitario de aproximadamente 1.80 de dólar por *Megabyte*. Hoy en día podemos comprar un *Terabyte* —mil *Gigabytes* o un millón de *Megabytes*— a un costo unitario aproximado de 0.005 dólares por *Megabyte*. Esto significa que podemos comprar por el mismo dinero más de cinco millones de veces lo que se podía comprar hace 50 años. Aun quitando la depreciación inflacionaria ocurrida en estas cinco décadas —1 dólar de 1956 = 7.84 dólares de 2009— por el mismo dinero en valor real podemos comprar 668,000 veces más almacenamiento. Esa es la proporción en la que ha crecido en medio siglo la capacidad de almacenamiento a un cierto costo, sin mencionar la reducción de espacio.

Siguiendo con las tendencias actuales, esto significa que dentro de unos siete u ocho años más estaremos comprando un *Petabyte*<sup>3</sup> —mil *Terabytes* o un millón de *Gigabytes* o mil millones de *Megabytes* o  $10^{15}$  *bytes* o un uno seguido por quince ceros de *bytes*— por

<sup>2</sup> 1 *Gigabyte* = 1000 *Megabytes* = 1'000,000,000 =  $10^9$  “bytes” o caracteres.

1 *Terabyte* = 1000 *Gigabytes* = 1'000,000 *Megabytes* = 1'000,000,000,000 =  $10^{12}$  “bytes” o caracteres.

<sup>3</sup> 1 *Petabyte* = 1,000 *Terabytes* = 1'000,000 *Gigabytes* = 1'000,000,000 *Megabytes* =  $10^{15}$  “bytes” o caracteres.

algo así como 500 dólares. En un *Petabyte* pueden almacenarse más de 300 millones de canciones de 3 minutos cada una en formato mp3 o 30 millones de canciones en calidad CD, o 300,000 películas de 90 minutos cada una, en máxima calidad, o 500 millones de fotografías de buena resolución de una cámara actual. Otro ejemplo son los dispositivos portables: a principios de los setenta, se guardaban cien *kilobytes* —un décimo de *Megabyte*— en un disquete de tres dólares. Diez años después, se almacenaba un *Megabyte* en un disquete por esa cantidad. En los noventa, se almacenaban seiscientos cincuenta *Megabytes* en un cd-rom de treinta centavos de dólar y a la fecha se almacenan cuatro *Gigabytes* en un DVD de treinta centavos de dólar. Cuarenta mil veces en treinta y cinco años por un cierto precio. Proporciones parecidas existen en las cintas y otros dispositivos; y la tendencia se mantiene.

Actualmente, el mercado de discos magnéticos vende discos cuya capacidad de almacenamiento oscila alrededor de treinta y dos *Gigabytes* por pulgada cuadrada —en un disco que además sólo pesa cien gramos y ocupa menos de cien centímetros cúbicos—. Como dato adicional y curioso, esto nos da la medida actual de un *bit*: 20 x 80 nm —nanómetros<sup>4</sup>— en los discos magnéticos más recientes. El almacenamiento magnético actual cae ya totalmente en el campo de la nanotecnología, es decir, partículas menores a 100 nm. El límite actual del almacenamiento magnético está ya determinado en la práctica por una frontera física fundamental, el límite en el que la energía térmica de los materiales excede a la energía magnética almacenada en cada pequeño grano del material sensible; si el tamaño del grano magnético disminuye a cierto tamaño, el calor creado y almacenado por el dispositivo en sí mismo puede desmagnetizarlo. Sin embargo, ya se vislumbran desde luego algunas innovaciones en puerta que permitirán evadir los efectos nocivos de este límite, no sólo con nuevos materiales sino con nuevas maneras de estructurarlos, algunos de ellos provenientes del campo de la biología [Bandit, Litvinov, Rooks. 2008].

Por todo lo anterior, y dados los enormes volúmenes de almacenamiento que se pueden comprar fácilmente hoy en día, observamos el fenómeno de grandes cantidades de información

<sup>4</sup> Un nanómetro (nm) = 10<sup>-9</sup> metros; esto es la milmillonésima parte de un metro, o la millonésima parte de un milímetro.

almacenada hoy por parte de personas y organizaciones. Como se puede constatar, tal abundancia de almacenamiento aunado al mínimo espacio que ocupa y a su bajo precio han causado un cambio radical en la forma en que en la actualidad percibimos el almacenamiento de información; todo tipo de información: textos, imágenes, música, videos, bases de datos, etcétera, pueden ser almacenados hoy en día en cantidades y a costos que eran imposibles de concebir hace una o dos décadas. Pero de la misma manera que se ha incrementado la facilidad para almacenar información ha crecido el problema de preservarla en la misma medida que crece el riesgo de dañarla o perderla. Almacenar no es lo mismo que preservar.

Junto con esta facilidad para adquirir dispositivos para almacenamiento de información se han diversificado notoriamente las tecnologías para crear, capturar, transmitir, administrar y reproducir todo tipo de información; dispositivos, programas, estándares, formatos, metodologías, estrategias, personal entrenado, etcétera. Por lo mismo, en la actualidad se producen y almacenan ya muchos *Exabytes*<sup>5</sup> de información cada año. Ya he mencionado en otras obras los estudios de Lymann y Varian al respecto. Y todavía más; un reciente estudio de John Ganz pronostica que para fines del año 2010, y como resultado sólo de lo generado en ese año, el mundo producirá ya un *Zettabyte* de información.<sup>6</sup> (Ganz, 2007). Desgraciadamente, desde la perspectiva de la preservación a largo plazo no se han producido avances tecnológicos ni de experiencia acumulada en el tema al mismo ritmo que la producción y el almacenamiento de información.

<sup>5</sup> 1 Exabyte = 1000 Petabytes = 1'000,000 Terabytes = 1'000,000,000 Gigabytes = 1'000,000,000,000 Megabytes =  $10^{18}$  "bytes" o caracteres.

<sup>6</sup> 1 Zettabyte = 1000 Exabytes = 1'000,000 Petabytes = 1'000,000,000 Terabytes = 1'000,000,000,000 Gigabytes = 1'000,000,000,000,000 Megabytes =  $10^{21}$  "bytes" o caracteres.

## II. La problemática de la preservación documental digital

Los requerimientos para la preservación a largo plazo llevan al límite a las tecnologías actuales de información y administración de información. Preservar información digital a largo plazo requiere de sistemas, instituciones, modelos técnicos y de organización, personal calificado y experimentado lo suficientemente robustos para sortear fallos tecnológicos, cambios sucesivos de plataformas de cómputo, obsolescencia de medios y formatos de almacenamiento, errores humanos, negligencia y ataques malintencionados, cambios a la misión institucional de las organizaciones, fallas e interrupciones en su dirección y financiamiento, por mencionar algunas amenazas.

En la obra "*Preservación del Patrimonio Documental Digital en México*"<sup>7</sup> se establecieron las bases y definiciones de la preservación documental digital, así como sus premisas básicas. Se establecieron también los seis factores que inciden -positiva o negativamente- en el proceso de preservación documental digital. Se establecieron propuestas para ayuda en la toma de decisiones y en la elaboración de proyectos estratégicos en ese aspecto. Cabe destacar que aunque en ese trabajo se introdujeron algunas consideraciones y elementos desde el punto de la archivística, se enfocó mayormente a bibliotecas digitales y sus correspondientes colecciones de materiales.

Es necesario continuar este esfuerzo en una segunda fase pero ahora con un punto de vista primordialmente archivístico. Si bien los principios y metodologías fundamentales de ambas disciplinas son muy semejantes, es necesario enfocarse a los problemas y técnicas propios de ese tipo de materiales y su tratamiento especial, de forma tal que podamos lograr una visión integral de la preservación digital archivística acorde con ese tipo de acervos. Así tendremos ambas visiones: la bibliotecológica y la archivística.

Poniendo aparte entonces a las bibliotecas y a sus colecciones y herramientas y

<sup>7</sup> Voutssás M, Juan. 2009. *Preservación del Patrimonio Documental Digital en México*. México: UNAM: Centro Universitario de Investigaciones Bibliotecológicas. 207 pp. ISBN: 978-607-02-0583-5.

pensando bajo un enfoque archivístico, ¿cuáles son los principales elementos a considerar?

- Cada día son más las empresas y organizaciones que crean y guardan sus archivos documentales en formatos digitales: bancos, compañías de seguros, financieras, bursátiles, universidades y escuelas, hospitales, almacenes, librerías, etcétera, en donde se encuentra toda una variedad enorme de información almacenada acerca de sus usuarios y crean cada vez más acervos documentales de: cuentas bancarias y de inversiones, préstamos y pagos, pólizas, expedientes estudiantiles y médicos, compras y ventas —tanto presenciales como en-línea—, perfiles de usuarios, catálogos y manuales de productos y servicios, además de su propia información interna. Hoy en día la factura electrónica, el pago o transferencias electrónicas, la compra de bienes y servicios en-línea, la firma de documentos electrónicamente, etcétera, son cada día *más* cotidianos y tienden a incrementarse cada vez más, dejando huellas y registros digitalmente.
- Los servicios gubernamentales registran cada vez más trámites oficiales que guardan información digital acerca de sus usuarios y sus transacciones: actas de registro civil y otros jueces de paz; sentencias y resoluciones de juzgados y cortes; pagos de impuestos y otros hacendarios, actas de calificaciones y exámenes, certificados de estudios, oficios, correos, memorandos, reportes, contratos, patentes, convenios, trámites vehiculares, pasaportes, visas, tratados internacionales, etcétera. Esto puede verse a nivel de los tres poderes y de los diversos servicios de gobierno, federal, estatal o local. Y su presencia tiende a incrementarse; también, estas transacciones tienden a incrementarse cada vez más, dejando huellas y registros digitalmente.
- La falta de conciencia del valor histórico de los acervos documentales archivísticos y de su fragilidad.
- Los factores tecnológicos que inciden en la preservación de material digital a mediano y largo plazo: soporte, formatos, equipo de cómputo y programas asociados para su visualización, así como las correspondientes obsolescencias tecnológicas.
- Seguridad de la información, ya que ésta es un activo muy valioso para casi todas las organizaciones; para algunas, es el más valioso. Cada vez más, la información

se encuentra depositada en formas digitales ya que debe ser operada, distribuida y consultada por muchos y en forma remota. Por sus condiciones de ser digital y operada en red, la información contenida en archivos de este tipo se enfrenta a riesgos de daño o pérdida. Las organizaciones —en especial sus sistemas de información—, se enfrentan cada vez más con riesgos procedentes de una amplia variedad de fuentes: pérdida, alteración, copia o consultas no autorizadas de su información debido a negligencia, sabotaje o vandalismo. Pérdida de información por desastres naturales: incendios, inundaciones, terremotos, etc. espionaje y fraudes informáticos. El sabotaje y/o vandalismo se presenta en muy variadas formas: *spam*, virus informáticos, ataques de intrusión o de negación de servicio, robo de identidades, etc., son cada vez más comunes, ambiciosos y sofisticados

- Restricciones y consideraciones legales con respecto a derechos de propiedad intelectual y de acceso a ciertos documentos, las cuales se oponen a las consideraciones legales con respecto a la transparencia y acceso a la información; finalmente, las consideraciones legales relativas al derecho a la privacidad de las personas.
- Diseño e inclusión de metadatos adecuados y pertinentes para la recuperación adecuada de la información, sobre todo en acervos grandes.
- Integración de los elementos principales de la cadena de preservación: evaluación, adquisición, preservación y distribución en-línea.
- Mecanismos que permitan garantizar el acceso futuro a la información por el público. Cierre de la *brecha digital* en este aspecto.
- Y obviamente, los costos asociados a la preservación de este material digital, aparte de los generados por la producción del mismo.
- Mantener en los documentos de esos acervos los elementos necesarios para su uso permanente: permanencia, disponibilidad, accesibilidad, confidencialidad (privacidad), integridad (autenticidad), aceptabilidad (no repudio).
- Poder preservarlos en estas condiciones por eones.



No estamos considerando aquí la enorme cantidad de material archivístico susceptible de digitalizarse retrospectivamente a partir de soportes “tradicionales”: millones y millones de piezas documentales que ya se encuentran en archivos de todo tipo, públicos y privados; solamente de los creados digitalmente de origen. Como puede observarse, el problema es complejo; sus fuentes son variadas y sus soluciones requieren de múltiples enfoques. Los planes y/o proyectos de este tipo requieren de un análisis desde varios puntos de vista y aproximaciones para tratar de ir respondiendo a las consideraciones que aquí se han ido planteando.

### **III. Los seis factores de la preservación digital**

Hemos mencionado que existen múltiples factores que inciden en la preservación a largo plazo. Tales factores pueden agruparse de varias formas para su estudio. En lo personal, yo los he agrupado en seis categorías: Factores tecnológicos, legales, documentales, culturales, económicos y sociales. Los factores son válidos también para el entorno de archivos digitales.

Estos seis factores han sido ya explicados en detalle en la obra “*Preservación del Patrimonio Documental Digital en México*” por lo que simplemente, se presenta un resumen de ellos: estos seis factores cubren tres enfoques fundamentales en este tipo de proyectos: en primer lugar, los factores culturales y sociales nos brindan el enfoque humanista, mismo que nos ayuda a poder ubicar los objetivos dentro del contexto social adecuado, la accesibilidad futura, los usuarios, la reducción de la brecha digital, etcétera. En segundo lugar, los factores tecnológicos y documentales nos ayudan a enfocar, por un lado los aspectos alrededor de la tecnología de cómputo y telecomunicaciones del proyecto y por el otro lado la metodología archivística necesaria para la creación, conservación, preservación y recuperación documental. En tercer lugar, los factores legales y económicos nos permiten concluir la contextualización de los proyectos ayudándonos a enfocarlos alrededor de estos aspectos jurídicos y financieros del proyecto, tomando en consideración los intereses de creadores, autores y preservadores acerca del financiamiento, costos, presupuestos actuales y viabilidades futuras, etcétera.

Entrando un poco más en detalle, los factores tecnológicos tienen que ver con el cambio rápido y constante de los dispositivos y aspectos tecnológicos relacionados a la información electrónica. Dentro del concepto de “*obsolescencia tecnológica*” se afirma hoy en día que el problema ya no es conservar los bits, sino cómo hacer que sean legibles en un futuro, dados esos cambios tecnológicos ajenos a la información documental en sí, pero indispensables para hacerla legible. Estos son los factores relacionados con el entorno de esa información digital, tales como el equipo y los programas que se requieren para reproducirlos. Mencione aparte requieren los sistemas operativos y múltiples formatos que se han creado para la representación de diversos documentos digitales en todos sus tipos: texto, audio, imagen estática y en movimiento, etcétera, y que surgen y desaparecen con rapidez cada vez mayor. Dentro de los factores tecnológicos se encuentran además los factores de seguridad de la información; ¿cómo se evitará que se pierdan por accidente, error o mala intención documentos en los acervos de preservación? ¿cómo se garantiza su integridad mientras se evita que manos no autorizadas sustraigan, destruyan o alteren esos documentos?

A continuación tenemos los factores de tipo legal alrededor de la preservación de documentos de archivo; una vez que se ha seleccionado una estrategia de preservación, deben revisarse sus implicaciones legales. Por ejemplo, la conversión de formatos de documentos fuera de sus ambientes propietarios puede ser ilegal de acuerdo con ciertas legislaciones en el mundo. Dentro de los factores legales deben revisarse las disposiciones de derechos de acceso a la información, transparencia y rendición de cuentas de archivos públicos para que estén en correcto balance con el derecho a la privacidad de las personas y las disposiciones legales al efecto. ¿hasta dónde puede distribuirse la información sin lesionar la privacidad de alguien? ¿hay legislación vigente en el entorno de nuestros archivos al efecto? ya se observan fenómenos muy complejos y realmente preocupantes, desde el caso del *spam* en la red hasta el acoso y la divulgación de información personal. Transparencia y privacidad de la información se contraponen y deben balancearse.

Los factores documentales —o metodológicos— se discuten ampliamente hoy en

día dada su enorme importancia y tienen que ver en primer lugar, con la valoración de los documentos de archivo con el fin de tasar o establecer oficialmente el valor de los mismos con propósito de determinar el periodo y condiciones de su preservación. No todos los documentos generados digitalmente y mucho menos todas sus copias, deben ser preservados. En segundo lugar, tiene que ver con los procedimientos para el registro de los documentos y los metadatos que deben ser agregados a estos acervos; de nada sirve preservar millones y millones de documentos digitales si luego no van a poder ser encontrados. ¿Cuáles son los metadatos adecuados para cierto tipo de documento de archivo? ¿cómo se buscará en conjuntos no homogéneos de colecciones con metadatos distintos? ¿cuáles son los metadatos mínimos? ¿cuáles los óptimos? ¿cómo debe ser la interoperabilidad actual de datos, formatos y sistemas para que todo interopere en el futuro? todo esto debe ser establecido junto con los proyectos de preservación; de otro modo el esfuerzo será estéril.

Los factores culturales tienen que ver con la falta de sensibilidad de ciertas sociedades en ciertas épocas respecto al valor histórico de partes de su patrimonio documental lo cual lleva a excluir la necesidad de preservar ese patrimonio, y que a la larga deriva en la pérdida de ese acervo documental. Nuestros tiempos, a pesar de que se afirma que vivimos en la “*sociedad de la información*” tienen en forma general un enorme problema de tipo cultural con respecto a la preservación de la información electrónica, una especie de oxímoron cultural.

Respecto a los factores sociales, debemos pensar en cómo vamos a poder garantizar el acceso y la usabilidad documental. Es necesario establecer los mecanismos para que en un futuro se pueda tener acceso efectivo y masivo a esa información por parte del público. De nada sirve preservar por preservar si nadie tendrá acceso a ella. Salvados los derechos, propiedades, privacidades y restricciones correspondientes, el reto futuro será cómo hacer llegar esa información digital a un número mayor de personas en el mundo sin crear nuevas brechas segregacionistas. Recuérdese todo lo que se ha debatido ya en este momento acerca de la “brecha digital” y sus consecuencias a futuro. Debemos crear las infraestructuras para que sea posible que las personas tengan acceso a esa información y que la brecha tienda a

cerrarse y no al contrario. Adolfo Rodríguez ha abundado en su obra al respecto <sup>8</sup>.

Finalmente, un proyecto de estos alcances debe reflexionar insoslayablemente en materia de costos. ¿Cuánto cuesta preservar un acervo? ¿quién tiene la responsabilidad de costear la preservación de acervos documentales? ¿pueden lograrse economías sin menoscabo de la calidad? ¿existen modelos económicos sustentables? Estos no son nunca proyectos baratos ni de corto plazo; por ello deben establecerse minuciosamente los elementos económicos que deben verse involucrados en el desarrollo de los mismos para hacerlos y mantenerlos viables desde el punto de vista económico. Y por caros que sean, debe recordarse siempre también a la hora de costear, que no preservar sale a la larga todavía más caro.

Como ya mencioné, puede abundarse más en la lectura de los seis factores en la obra *Preservación del Patrimonio Documental Digital en México*.

#### IV. Iniciativas y modelos

En la actualidad no existe un modelo único que establezca o defina los atributos y características ideales de los documentos de archivos digitales y sus procedimientos asociados con miras a su preservación a largo plazo. En los últimos quince años se han ido estableciendo una serie de iniciativas planteando “*modelos*” y “*marcos de referencia*” para tratar de definir o establecer los atributos de documentos, procedimientos, sistemas, organizaciones, etcétera que se encuentren involucradas en la gestión y/o la preservación digital. Cada uno de ellos hace énfasis en elementos o atributos que considera importantes para el establecimiento del modelo en cuestión.

La base de todas estas iniciativas es la norma ISO 15489:2001 “*Information and Documentation: Records Management: Part 1. General*”. Consiste en una guía para la gestión de documentos de archivo de una organización, sea cual sea su soporte. Esta norma

<sup>8</sup> Rodríguez G., Adolfo. 2006. *La Brecha Digital y Sus Determinantes*. México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas. 254 pp. ISBN: 970-32-3853-X.

establece 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”.

Entre las principales iniciativas podemos destacar las siguientes: El modelo de referencia conocido como OAIS — *The Open Archival Information System*— el cual provee un modelo de alto nivel acerca de la identificación de atributos de archivos y cuyo propósito es asegurar la permanencia de cierta información digital generada por una comunidad dada.<sup>9</sup> Observamos también el reporte acerca de “*Repositorios Digitales Confiables*” de RLG-OCLC en el cual se establecieron los atributos y recomendaciones para los mismos, entre las cuales destacan el desarrollo de marcos de trabajo y procesos tendientes a apoyar la certificación de repositorios digitales.<sup>10</sup> Derivado de estos esfuerzos, surgió la lista de verificación del “*Digital Repository Certification Task Force*”<sup>11</sup> la cual se enfoca a establecer los criterios necesarios para construir la “confianza” en los documentos de archivo. La “*Administración Nacional de Archivos y Registros*” de la unión americana —*National Archives and Records Administration*— adoptó como estándar para el manejo de archivos gubernamentales el denominado DoD.5015.2 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.

En el continente europeo, distinguimos las especificaciones establecidas por el proyecto de los Archivos Nacionales —*National Archives*— del Reino Unido, uno de los más ambiciosos y avanzados al momento, el cual consiste principalmente en un conjunto estandarizado de requerimientos funcionales para archivos electrónicos. Son notables

<sup>9</sup> *Consultative Committee for Space Data Systems*. 2002. “Reference model for an open archival information system (OAIS).” Washington, D.C.: CCSDS Secretariat.

<sup>10</sup> RLG-OCLC *Working Group on Digital Archive Attributes*. 2002. “Trusted digital repositories: Attributes and responsibilities”. Mountain View, CA: Research Libraries Group (RLG). Disponible en: <http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf>.

<sup>11</sup> RLG-NARA *Digital Repository Certification Task Force*. 2007. “Trustworthy repositories audit & certification: Criteria and checklist.” Disponible en: <http://www.crl.edu/PDF/trac.pdf>.

también las especificaciones denominadas MoReq —Modelo de requisitos para la gestión de documentos de archivo— muy difundidas en ese continente. Este no es un modelo de preservación en sí; consiste en un modelo de requisitos funcionales para la gestión de documentos electrónicos de archivo elaborado por la Comisión Europea a través de su programa IDABC —*Interoperable Delivery of European e-Government Services to Public Administrations, Business and Citizens*— con objeto de ir estandarizando la gestión de archivos digitales 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, etcétera—. Sin ser un modelo de preservación, es interesante ya que abarca aspectos que son útiles para la misma.

En ese continente existen también las especificaciones del *Digital Curation Center*, *Digital Preservation Europe*, etcétera. Son notables también las especificaciones establecidas por DRAMBORA,<sup>12</sup> —“*Digital Repository Audit Method Based On Risk Assessment*”—. Esta es una herramienta de auto-diagnóstico para una aproximación sistemática para evaluación de riesgos inherentes a un repositorio digital.

En Australia se creó un modelo conocido como el “*Records Continuum*” —“*Continuo de los documentos de archivo*”— el cual ha sido trabajado por el “*Records Continuum Research Group*”<sup>13</sup> de ese país afiliado con el “*Center for Information as Evidence at UCLA, California*”. Este modelo se opone al más utilizado, basado en el concepto del “*ciclo de vida*” de los documentos de archivo. El modelo del *records continuum* está construido sobre la afirmación de que la gestión del documento es un proceso continuo desde el momento de su creación; los conceptos relativos a dicha gestión pertenecen a cuatro “dimensiones”

<sup>12</sup> *Digital Curation Centre, and Digital Preservation Europe*. 2008. “DRAMBORA Interactive: Digital repository audit method based on risk assessment”. Disponible en: <http://www.repositoryaudit.eu/>.

<sup>13</sup> Records Continuum Research Group. Monash University. ABN. Australia. Disponible en: <http://www.infotech.monash.edu.au/research/groups/rcrg/>.

o “puntos de vista del observador”.<sup>14</sup> Este modelo también es conocido como “*Modelo de gestión de documentos de archivo orientado a organizaciones*” —*Business-Driven Recordkeeping Model*— o simplemente *BDR Model*. En una temática relacionada con el tema, los Archivos Nacionales de ese país publicaron las “Especificaciones funcionales para software de sistemas de administración de documentos de archivo electrónicos” y las “Guías asociadas para su implementación”.<sup>15</sup>

El *ciclo de vida* de un documento es un modelo o concepto clásico de la archivística moderna. Se refiere a las distintas fases o etapas por las que pasan los documentos y a las transformaciones en sus valores legales, informativos, etcétera, desde su creación como coproductos de la actividad humana hasta su eliminación o selección para su custodia permanente, generalmente por su valor histórico. Estas etapas son ocho: creación, clasificación, mantenimiento para el uso, disposición, descripción de las ayudas o auxiliares de consulta, preservación, referencia y consulta.

En la Universidad de la Columbia Británica del Canadá se creó desde 1999 un proyecto denominado InterPARES —*The International Research on Permanent Authentic Records in Electronic Systems*—. Este es un proyecto de investigación teórica y desarrollo de tecnología alrededor de la preservación de documentos de archivo electrónicos. Este proyecto perfeccionó un modelo de aproximación a la preservación digital denominado “*Cadena de Preservación*” —*Chain of Preservation*— o simplemente “COP”.<sup>16</sup> Este modelo establece que los documentos de archivo digitales deben ser cuidadosamente manejados a lo largo de toda su existencia para asegurar que sean accesibles y legibles a lo largo del tiempo

<sup>14</sup> InterPARES. 2008. “InterPARES 2 : Experiential, Interactive and Dinamic Records. Appendix 16. Overview of the Records Continuum Concept”. Extracted and adapted from “Xiami An. An Integrated approach to Records Management”. *Information Management Journal*. July/August (2003): 24-30. Disponible en: [http://www.inter pares.org/ip2/display\\_file.cfm?doc=ip2\\_book\\_appendix\\_16.pdf](http://www.inter pares.org/ip2/display_file.cfm?doc=ip2_book_appendix_16.pdf).

<sup>15</sup> National Archives of Australia. 2007. “Functional Specifications for Electronic Records Management Systems Software (ERMS)” and “Guidelines for Implementing the Functional Specifications for ERMS”. Disponibles en: <http://www.naa.gov.au/records-management/publications/ERMS-specs.aspx>.

<sup>16</sup> *InterPARES -The International Research on Permanent Authentic Records in Electronic Systems*. 2004. “Business-Driven Recordkeeping (BDR) Model”. Disponible marzo 1, 2010 en: [http://www.interpares.org/ip2/ip2\\_models.cfm](http://www.interpares.org/ip2/ip2_models.cfm).

dejando su forma, contenido y relaciones intactas hasta el punto necesario para lograr su continua confianza como documentos de archivo. El manejo de los documentos de archivo digitales debe emanar de un entendimiento integral de todas las fases o etapas de la existencia de los documentos de archivo, desde el momento en que son generados, a través de su conservación por parte de su creador, durante la evaluación, disposición y preservación a largo plazo como comprobantes auténticos de las acciones y asuntos de los cuales son parte. Desde la perspectiva de la preservación a largo plazo, todas las actividades tendientes a administrar documentos de archivo a lo largo de su existencia están interrelacionadas, como en una cadena, y son interdependientes entre sí. Si un eslabón de esa cadena llega a fallar, la cadena no puede cumplir su cometido. Si ciertas actividades y acciones no son realizadas sobre esos documentos de archivo, su confianza —esto es, su fiabilidad, autenticidad o exactitud— se vuelve cuestionable.

El modelo de la “*Cadena de Preservación*” es ampliamente aceptado en norteamérica —incluyendo a México—, en la mayor parte de Europa y mayormente en muchas otras partes del mundo: Sudamérica, África, Lejano Oriente. Es más utilizado y aceptado que el modelo del “*continuo*” de los documentos de archivo. En particular, la terminología y conceptos utilizados en este documento se apegan a este modelo de la “*Cadena de Preservación*”.<sup>17</sup>

## V. La “Cadena de Preservación”

¿En qué consiste este modelo de la “Cadena de Preservación”? En términos generales, es una secuencia de actividades y enfoques agrupados en varias etapas que conforman los “eslabones” de la cadena. De todas y cada una de estas actividades y elementos se han ido haciendo investigaciones y especificaciones detalladas y su conocimiento profundo implica un estudio a fondo de ellas. Haciendo un resumen de las mismas, la “Cadena de Preservación” consta de cinco etapas:

<sup>17</sup> InterPARES 2. 2008. “Preserver Guidelines - Preserving Digital records : Guidelines for Organizations”. Disponible en: [http://www.interpares.org/display\\_file.cfm?doc=ip2%28pub%29preserver\\_guidelines\\_booklet.pdf](http://www.interpares.org/display_file.cfm?doc=ip2%28pub%29preserver_guidelines_booklet.pdf).



- I. Establecer el marco de referencia del fondo archivístico. No todos los fondos archivísticos a preservar tienen el mismo propósito. Es necesario definir de entrada el “objeto de preservación”.

- I.1 **Establecer alcance y objetivos**

Definir el propósito y objetos del fondo documental a preservar. En acervos documentales científicos, puede desearse guardar sólo los reportes o documentos finales de los proyectos; o también incluir los datos primarios. En artes, puede desearse preservar sólo grabaciones o imágenes de las obras; o puede desearse guardar los elementos individuales que las conforman. Las bases de datos no pueden preservarse; es necesario definir “instantes” periódicos de las bases de datos en una forma adecuada y pertinente para la preservación.

- I.2 **Allegarse los recursos**

Los proyectos de preservación requieren de recursos económicos, tecnológicos y humanos. Es necesario al inicio de un proyecto de preservación definir la forma, alcances y dimensiones de estos recursos. Tiempos de adquisición, de capacitación, etcétera. Con respecto a la forma, es conveniente tener en mente que pueden conseguirse nuevos recursos, o reubicarse recursos ya existentes.

- I.3 **Enfocarse en los documentos de archivo digitales**

En los proyectos de preservación digital, es conveniente enfocarse principalmente en aquellos documentos que sólo existen en versión digital, y en segundo plano en aquellos de los que se guarda copia en soporte tradicional.

- I.4 **Ofrecer asesoría**

Los preservadores deben asesorar a los creadores, operadores y usuarios de los documentos acerca de procedimientos, especificaciones y características de los buenos acervos digitales.

- I.5 **Desarrollar procedimientos**

Los preservadores deben establecer controles sobre la transferencia, conservación y reproducción de los documentos de archivo, y en especial en procedimientos y

sistemas usados para la gestión documental al interior de la organización.

## 1.6 Implementar estrategias de conservación documental

En general se invierte mucho esfuerzo en el desarrollo de las estrategias para la preservación, pero poco se hace con respecto a las estrategias para la conservación, salvaguarda y seguridad informática de los documentos. Preservación, conservación y seguridad informática no son sinónimos.<sup>18</sup> Preservación documental digital se define como “*la totalidad de principios, políticas y estrategias que controlan las actividades destinadas a asegurar la estabilización física y tecnológica, así como la protección del contenido intelectual de materiales (datos, documentos o archivos) y cuyo fin ulterior y a largo plazo, es el de asegurar la permanencia y acceso del contenido de documentos digitales a lo largo del tiempo y las tecnologías, independientemente de su soporte, formato o sistema*”. Seguridad informática es “*el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos*”. Conservación documental digital: “*acciones tomadas para anticipar, prevenir, detener o retardar el deterioro del soporte de obras digitales con objeto de tenerlas permanentemente en condiciones de usabilidad, así como la estabilización tecnológica, la reconversión a nuevos soportes, sistemas y formatos digitales para garantizar la trascendencia de los contenidos*”.

2. Evaluar los documentos de archivo para preservación permanente.

### 2.1 Evaluar lo más pronto posible

Debido a las dificultades técnicas propias de la preservación digital, la determinación de cuáles registros deben ser sujetos de preservación debe hacerse

<sup>18</sup> Voutsás M., Juan. 2010. “Preservación Documental Digital y Seguridad Informática” En: *Investigación Bibliotecológica*. Centro Universitario de Investigaciones Bibliotecológicas, UNAM. Vol 24, no. 49.

lo más pronto posible, ya que esto incide en retroalimentación de procedimientos y/o características al creador de los registros, a la transferencia y a las estrategias de conservación y preservación, lo cual mejora las probabilidades de éxito del proyecto.

## 2.2 Localizar múltiples propietarios

Existen casos donde los contenidos y/o usuarios de un fondo documental pertenecen a diversas organizaciones, inclusive de distintos subsistemas. Aunque por lo general existen acuerdos para el uso y explotación de la gestión documental, rara vez se contemplan acuerdos de largo plazo, y donde las responsabilidades, derechos, etcétera, deberán quedar perfectamente establecidos.

## 2.3 Valorar la autenticidad y documentarla

Como parte del proceso inicial de evaluación, es necesario establecer la autenticidad de los documentos de archivo ya existentes. Luciana Duranti establece:

El original de un documento —esto es, la primera instanciación completa de una entidad documental que alcanzó sus propósitos— desaparece en el ambiente digital la primera vez que es salvado. Lo que nosotros recuperamos siempre es una copia. No podemos preservar documentos —entidades— digitales: sólo podemos preservar la capacidad de reproducirlos una y otra vez. En este contexto, una entidad digital preservada es considerada auténtica si puede considerarse que es —o aun mejor— declararse que es una copia auténtica por el custodio quien de fe de su identidad y de su integridad a lo largo del tiempo partiendo desde el momento en que lo ingresó a su acervo y ese custodio puede documentar además correctamente el proceso de conservación —inclusive cualquier migración posterior y sus consecuencias tanto en forma como en contenido—. Ello significa que, en lo relativo a documentos en medios tradicionales, la autenticidad fue establecida siempre a través del objeto mismo, del documento, así que el custodio sólo necesitó preocuparse de que el usuario analizase el objeto y sacara sus propias conclusiones acerca de su autenticidad. Con medios digitales, lo que el usuario necesita para analizar y

concluir es conocer la autoridad y la capacidad —competencia— del custodio, así como la calidad de la documentación del proceso de conservación.<sup>19</sup>

Es necesario documentar los elementos que permitieron declarar la autenticidad, documentación que por lo general contiene los siguientes elementos:

- a) Expresión de los atributos de los documentos de archivo y vínculos a otros documentos (metadatos de integridad e identidad).
- b) Privilegios de acceso.
- c) Procedimientos de protección contra pérdida o corrupción de documentos.
- d) Procedimientos de protección contra deterioro de medios y cambios tecnológicos.
- e) Establecimiento de las formas documentales; es decir, las reglas de representación según las cuales el contenido de un documento de archivo, su contexto administrativo, documental y su autoridad son comunicados.
- f) Autenticación de los documentos de archivo.
- g) Identificación del documento de archivo autorizado u oficial.
- h) Remoción y transferencia de documentación relevante.

#### **2.4 Monitorear documentos de archivo seleccionados para preservación a largo plazo**

Una vez que se ha establecido cuáles documentos formarán parte a la larga de la preservación, es necesario supervisar periódicamente muestreando esos documentos para verificar que nada ha cambiado en sus características y procedimientos ya establecidos, y que conservan sus especificaciones tal como el día que fueron definidos.

#### **2.5 Actualizar la valoración**

De tiempo en tiempo, es necesario revisar los criterios de valoración para certificar

<sup>19</sup> Duranti, Luciana, and Thibodeau, Kenneth, "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.

que esta sigue vigente y que los contextos no han cambiado y, en su caso, hacer las adaptaciones correspondientes.

### **2.6 Identificar todos los componentes digitales**

A diferencia del papel, el cual siempre es un componente identificable como un todo, los registros de documentos digitales pueden estar formados por varias “capas”, componentes, o elementos que deben ser integrados para reproducir el documento original. Debe verificarse que se han identificado todos los elementos que componen un documento de archivo digital y que son transferidos integralmente.

### **2.7 Determinar la viabilidad de la preservación**

Durante la evaluación es necesario establecer los límites y características de la usabilidad y aceptabilidad de los documentos de archivo para poder mantener a lo largo del tiempo las características de “calidad intrínseca” que son indispensables de preservar para mantener ese nivel de calidad en el documento. Deben contemplarse también los procedimientos y costos recurrentes derivados de migración, transformación, emulación, reformateo, etcétera.

3. Ganar, obtener o conseguir posesión o control sobre los fondos archivísticos seleccionados o agregar a los fondos ya poseídos con fines de preservación permanente.

#### **3.1 Desarrollar plan para transferencias documentales**

La transferencia exitosa de documentos de archivo desde su creador o sucesor hacia el preservador de largo plazo, requiere de un plan previamente establecido, el cual debe contemplar plazos, formatos, etcétera.

#### **3.2 Aplicar procedimientos estandarizados**

Los controles para la transferencia de documentos de archivo de un creador hacia el preservador deben establecer, implementar y monitorear procedimientos para el apropiado registro de los documentos transferidos,

verificando que en efecto sean los que deben transferirse, su completitud, su pertinencia, su autenticidad, etcétera.

### **3.3 Mantener el formato más antiguo que sea utilizable**

Debe tratar de mantenerse el formato lógico más antiguo que todavía sea posible utilizar en el cual los documentos fueron creados o mantenidos y sólo cambiarse cuando su uso ponga en riesgo su accesibilidad.

### **3.4 Evitar duplicados**

Es fácil que en los procesos de transferencia se de el fenómeno de duplicación de documentos. Es necesario tomar previamente las medidas para detectar oportunamente y descartar estos documentos.

### **3.5 Documentar todos los procesos**

Todos los procesos adicionales que son realizados de manera rutinaria o eventual sobre los documentos deben ser documentados; por ejemplo, procesos de antivirus, integridad de la base de datos, compactación, transferencia, cambio de versión, etcétera, desde su razón de ser aplicados, a cuáles registros se les aplicó el proceso, fechas de realización, personas involucradas, impacto a integridad e identidad de los documentos, problemas detectados, etcétera.

4. Preservar los documentos de archivo cuya autenticidad y viabilidad de preservación han sido confirmados y han sido recibidos e ingresados a un archivo histórico por el preservador.

#### **4.1 Describir/catalogar/registrar los documentos de archivo**

Es necesario describir de alguna forma normalizada a cada documento del archivo. Además de la descripción básica, el acervo debe tener descripciones detalladas de sus contextos administrativo, documental, jurídico-administrativo, procedimental, de procedencia y tecnológico.

#### **4.2 Identificar aspectos legales de la preservación**

Es necesario identificar y establecer previamente las implicaciones legales del almacenamiento y distribución de la información. Definir restricciones al acceso y cambio de la misma, transparencia, privacidad, seguridad, etcétera.

#### **4.3 Confirmar la eficacia de la estrategia de preservación elegida**

Periódicamente debe ser revisada y evaluada la eficacia de la estrategia de preservación, sus costos / beneficios, etcétera y, en su caso, replanteada.

#### **4.4 Almacenar adecuadamente**

Las condiciones de almacenamiento de los soportes digitales deben ser establecidas previamente y vigiladas periódicamente: seguridad física, temperatura, humedad, respaldos, múltiples copias, refrescados, etcétera.

### **5. Distribuir los documentos de archivo.**

#### **5.1 Documentar cómo se hicieron las copias preservadas**

Es necesario documentar cuidadosamente las similitudes y/o diferencias entre las copias del autor y las usadas para preservación, así como las medidas utilizadas para garantizar forma documental y contenidos.

#### **5.2 Documentar los requerimientos para acceso**

Es necesario establecer y documentar los requerimientos para el acceso a los documentos, tanto tecnológicos, como de autorización, tiempos, alcances, etcétera.

## **VI. Conclusiones**

Como ha podido observarse, el fenómeno de la preservación documental digital, aunque es un problema eminentemente derivado del uso de las tecnologías de almacenamiento electrónico, no se limita a ser un simple problema de tecnología y su obsolescencia. Su solución por tanto tampoco radica en el simple almacenamiento y/o recopia de documentos

digitales. Es toda una escuela de pensamiento cuyo objetivo central pretende llevar los materiales documentales existentes en archivos digitales hacia el largo plazo, muy largo plazo; idealmente a perpetuidad, además de mantenerlos confiables, auténticos.

Como ha podido apreciarse también su eje central implica el desarrollo y observancia meticulosa de procedimientos que comienzan con la gestión documental, involucran a todo el ciclo de vida del documento y desembocan finalmente en la preservación adecuada. Espero haber podido mostrar a pesar de lo breve de este documento, que existen ya toda una serie de conocimientos y habilidades alrededor de la preservación que las organizaciones con acervos archivísticos deben ir cultivando y desarrollando para poder preservar sus fondos digitales adecuadamente y a largo plazo. “...*un poco de instrucción es peligrosa. Bebe copiosamente, o no pruebes del manantial de la sabiduría*”.<sup>20</sup>

Como puede apreciarse también, la preservación documental digital no es un simple método para mantener cadenas de *bits* legibles y utilizables mañana; tiene una fuerte connotación cultural y de utilidad social. La preservación del patrimonio cultural es un elemento crucial de las identidades institucionales, regionales y nacionales y son a su vez enlace de una comunidad con su pasado. Las sociedades actuales, supuestamente “de la información y el conocimiento” de la información deben aprovechar y preservar el patrimonio cultural para el futuro. A pesar de la dificultad y los costos de preservar, no es conveniente ni recomendable soslayar el problema. Todos los conglomerados humanos, todas las regiones y países poseen riquezas documentales que necesariamente hay que preservar y distribuir. Forman en esencia su patrimonio cultural. Nosotros, como parte de ese conglomerado humano tenemos gran parte de la responsabilidad de hacerlo. Debe recordarse siempre que, a la larga, —socialmente hablando—, no preservar resulta más caro.

<sup>20</sup> Diálogo entre los bomberos Beatty y Montag, en “*Fahrenheit 451*”, de Ray Bradbury.





---

Alejandro Delgado

---

**El archivero electrónico**  
en el país de nunca jamás



# Gómez

Licenciado en Filosofía y doctorado en Razón, discurso e historia en la filosofía contemporánea. Técnico de archivos del Ayuntamiento de Cartagena (España).

Consultor Senior de 3000 Informática (España). Investigador afiliado del Center for Information as Evidence (Universidad de California-Los Angeles). Investigador asociado del Centre for Organisational and Social Informatics (Universidad de Monash). Colaborador del TEAM Catalonia de InterPARES 3 (Universidad de British Columbia). Miembro del Observatorio Infoscopos (Universidad de Zaragoza). Miembro de los comités científicos de las revistas Tabula y Scire.

## I. Introducción

El presente artículo explora la complejidad de los actuales entornos digitales de producción de información registrada y de documentos, y la consiguiente complejidad de la gestión y la conservación de tal información y documentos, a partir de la descripción de un proyecto de administración electrónica emprendido por el Ayuntamiento de Cartagena, y cuya integración con los procesos de gestión de documentos y archivo es necesaria, si es que se quiere disponer de información y documentos como evidencia a lo largo del tiempo. Puesto que el equipo interdisciplinar de trabajo del Ayuntamiento se encuentra altamente implicado en el diseño de las herramientas de la fase de producción, la herramienta de gestión de documentos y de archivo del proyecto que se describe en el presente artículo ha sido elaborada por la compañía externa 3000 Informática, que ha integrado en su propio desarrollo tecnológico los requisitos que le han sido dados por los responsables del proyecto.

En lo que sigue, se describe en primer lugar el escenario del entorno de producción actual o en fase de desarrollo en el Ayuntamiento. En segundo lugar, se describe la solución de gestión de documentos y de archivo propuesta, así como los mecanismos de integración con el entorno de producción. Por último, se delinearán algunas conclusiones.

El autor desea agradecer a los equipos de trabajo del Servicio de Informática del Ayuntamiento de Cartagena y de la compañía 3000 Informática su incondicional apoyo, sin el cual la finalización del proyecto que se describe en el presente artículo no hubiera resultado posible.

## II. Las necesidades derivadas del nuevo marco legislativo

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos,<sup>1</sup> y su normativa de desarrollo (a nivel nacional, el Real Decreto 1671/2009, de

<sup>1</sup> Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. URL: [http://www.boe.es/aeboe/consultas/bases\\_datos/doc.php?id=BOE-A-2007-12352](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2007-12352) (Consulta: 25-2-2010).

6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos;<sup>2</sup> y los recientemente aprobados Esquema Nacional de Interoperabilidad<sup>3</sup> y Esquema Nacional de Seguridad),<sup>4</sup> han marcado sin duda un antes y un después en el imparable proceso de implantación de las tecnologías de la información y de las tecnologías de convergencia universal en todos los ámbitos de la vida pública y privada, en este caso en el contexto de la Administración Pública y de las interacciones entre ésta y la ciudadanía. El texto legal de origen, por lo demás, reconoce la necesidad de conservar los documentos generados de manera electrónica en sistemas de archivo, también electrónicos, con las debidas garantías, a saber:

- identidad e integridad
- traslación segura de datos
- autenticidad
- confidencialidad
- calidad
- protección y conservación
- identificación de los usuarios y control de accesos
- protección de datos.

No obstante, los actuales sistemas que generan documentos electrónicos son maquinarias extremadamente complejas que requieren un minucioso análisis antes de su diseño, un cuidadoso seguimiento durante el mismo y una exhaustiva documentación de los procesos de creación tanto de los sistemas como de la información y documentos

<sup>2</sup> Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. URL: [http://www.boe.es/aeboe/consultas/bases\\_datos/doc.php?id=BOE-A-2009-18358](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2009-18358) (Consulta: 25-2-2010).

<sup>3</sup> Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. URL: [http://www.boe.es/aeboe/consultas/bases\\_datos/search.php](http://www.boe.es/aeboe/consultas/bases_datos/search.php) (Consulta: 25-2-2010).

<sup>4</sup> Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. URL: [http://www.boe.es/aeboe/consultas/bases\\_datos/search.php](http://www.boe.es/aeboe/consultas/bases_datos/search.php) (Consulta: 25-2-2010).

que generan, si es que se pretende cumplir con las citadas garantías. Por ello, como ha venido indicando de manera profusa desde los años noventa del siglo veinte la investigación archivística,<sup>5</sup> es evidente que los sistemas de gestión de documentos y de archivo deben intervenir desde las primeras fases de diseño de los sistemas de gestión y de información, y conectar con ellos tan pronto como sea posible, con el fin de insertar en los mismos mecanismos que garanticen los requisitos mencionados por la Ley.

### III. El entorno de producción de documentos electrónicos en el Ayuntamiento de Cartagena

Las distintas herramientas, proporcionadas tanto por las propias administraciones como por la empresa privada, sugieren un escenario en el que distintos sistemas o subsistemas interactúan de diferentes maneras, con los riesgos para los requisitos documentales que toda transmisión en el tiempo y el espacio implica. En el caso que nos ocupa, el escenario es el siguiente:<sup>6</sup> el ciudadano, desde su hogar, inicia un expediente en el sitio web del Ayuntamiento,

<sup>5</sup> Quizá el defensor más acendrado de este punto de vista haya sido David Bearman. Confróntese, por ejemplo, Bearman, David A.: "Archival Principles and the Electronic Office". En: *Electronic Evidence: Strategies for Managing Records in Contemporary Organizations*. Pittsburgh: Archives & Museums Informatics, 1994; "Documenting Documentation". En: *Archivaria*. N. 34 (Summer 1992). P. 33-49; *Electronic Evidence: Strategies for Managing Records in Contemporary Organizations*. Pittsburgh: Archives & Museums Informatics, 1994; *Functional Requirements for Evidence in Recordkeeping*. University of Pittsburgh, School of Information Sciences. URL: <http://web.archive.org/web/20000818163633/www.sis.pitt.edu/~nhprc/> (Consulta: 25-2-2010); "Item Level Control and Electronic Recordkeeping". En: *Archives & Museum Informatics*, vol.10, n. 3 (1996). P.195-245. URL: <http://www.archimuse.com/papers/nhprc/item-lvl.html> (Consulta: 25-2-2010); "Record-Keeping Systems". En: *Archivaria*. N. 36 (Autumn 1993). P. 16-36.

<sup>6</sup> Pueden encontrarse referencias parciales al sistema descrito en, por ejemplo, Delgado Gómez, Alejandro, Rodríguez Gutiérrez, Miguel, Tornel Cobacho, Cayetano: "El desarrollo de un sistema de gestión de expedientes mediante estrategias interdisciplinarias: el caso del Ayuntamiento de Cartagena". En *Fesabid'09: X Jornadas Españolas de Documentación*. Zaragoza, 20-22 mayo 2009. URL: <http://www.fesabid.org/zaragoza2009/actas-fesabid-2009/307-314.pdf> (Consulta: 25-2-2010); Ketelaar, Eric, Alejandro Delgado Gómez: "El reto de los archivos intangibles". En: *Tábula*. N. 12. P. 63-84.

rellenando un formulario HTML y enviándolo junto con su firma electrónica al Ayuntamiento, donde los datos quedan almacenados en un cierto modelo de base de datos. Éste conecta con otro modelo de base de datos que asigna automáticamente la clasificación funcional, el tipo documental y el calendario de retención, a partir del identificador de formulario enviado por el ciudadano. El sitio web ha sido diseñado de manera independiente por parte del Servicio de Informática del Ayuntamiento, y tiene que conectar adecuadamente con un sistema de registro que también ha sido diseñado de manera independiente de conformidad con la última versión admitida del módulo SICRES. Este sistema de registro, por otra parte, ha tenido que asumir los datos de sistemas antiguos, con el peligro de incoherencias o pérdidas que todo proceso de migración implica. Además, el sistema debe lanzar una consulta a un sistema externo, el de validación de la firma electrónica del ciudadano, que tiene que verificar extremos del estilo de “esta firma es reconocida por el sistema”, “esta firma se corresponde con la persona de la que se presume que ha firmado” o “el certificado asociado a esta firma no ha sido revocado”. Una vez devuelto el visto bueno por parte del sistema externo de concesión y verificación de firmas, el sistema de registro tiene que conectar con otras bases de datos existentes en el Ayuntamiento, como el padrón de habitantes o los padrones de impuestos, para verificar a su vez que los datos proporcionados por el ciudadano son correctos y, en su caso, extraer datos adicionales pertinentes. Una vez realizadas estas verificaciones previas, el sistema de registro tiene que enviar los datos procedentes del formulario web o, en su caso, de consultas adicionales a otras bases de datos, a uno o varios sistemas de gestión de expedientes. Téngase en cuenta que, habida cuenta de que el Ayuntamiento es una organización antigua, grande y compleja, dispone de un recién estrenado sistema moderno de flujo de tareas desarrollado con tecnología web avanzada; pero, dependiendo de las áreas, también dispone de sistemas relativamente recientes que todavía son útiles, o sistemas obsoletos o *legacy* que en algún momento será preciso migrar al nuevo sistema. Algunos de tales sistemas, además, conectan en algún punto unos con otros, bien porque se precise cierta información a modo de antecedente, bien porque una transacción en un sistema no puede iniciarse si antes no se ha completado otra transacción en otro sistema. Tales sistemas, además, contienen numerosos componentes

de diversa naturaleza, pero todos imprescindibles para que funcionen: herramientas de flujos de tareas, formularios para la introducción de datos por parte del personal, distintos tipos de bases de datos, herramientas de control de versiones o de conversión a PDF y de inserción de metadatos, directorios LDAP o diferentes sistemas de autenticación que deben conectarse para evitar molestias al usuario... Por otra parte, el hecho de que la Ley impulse la utilización de medios electrónicos no significa que el soporte papel quede excluido, por ejemplo para una masa crítica de ciudadanos no habituados a las nuevas tecnologías, como sugeriría el primer informe del Plan Avanza, en el que ya se explicaba que en España las transacciones electrónicas aún inspiraban un cierto grado de desconfianza.<sup>7</sup> Finalmente, obsérvese que en la descripción de este escenario se ha utilizado con profusión el término “datos”, pero escasamente el término “documento”. Como hemos explicado en otros lugares, ello se debe al hecho de que, en sentido estricto, en el entorno digital el documento no existe: existen secuencias de bits en la capa más alta de abstracción, datos y reglas en una segunda capa, y representaciones o instanciaciones de esos datos, manifestados de manera legible para el humano, de conformidad con esas reglas.<sup>8</sup>

Nuestra disciplina, al menos tal y como la conocemos en su estado actual, es relativamente reciente. Con anterioridad siempre existieron, bajo una u otra denominación, custodios de documentos como garantes de evidencia.<sup>9</sup> Tales custodios o garantes utilizaban

<sup>7</sup> Ministerio de Industria Turismo y Comercio. Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información: Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas. Madrid: Mytic, 2008.

<sup>8</sup> Confróntese, por ejemplo, Delgado Gómez, Alejandro: *El documento electrónico en la sociedad de la información*. México D.F.: Archivo General de la Nación, 2009.

<sup>9</sup> Confróntense, por ejemplo, Cook, Terry: “What is Past is Prologue: A History of Archival Ideas Since 1898, and the Future Paradigm Shift”. En: *Archivaria*. N. 43 (Spring 1997). P. 17-63. Gilliland-Swetland, Anne: *Enduring Paradigm, New Opportunities: The Value of the Archival Perspective in the Digital Environment*. Washington D.C.: Council on Library and Information Resources, 2000. URL: <http://www.clir.org/pubs/reports/pub89/pub89.pdf> (Consulta: 25-2-2010). Thomassen, Theo: “The development of archival science and its European dimension”. En: *Arkivarien och Arkivvetenskapen. Seminarium för Anna Christina Ullsparre/ The Archivist and the Archival Science. Seminar for Anna Christina Ullsparre*. Lund: Swedish National Archives, 1999. P. 75-83. URL: <http://www.archiefschool.nl/docs/thomdeve.pdf> (Consulta: 25-2-2010).



ciertos métodos que no coinciden necesariamente con los que ha construido nuestra disciplina durante aproximadamente ciento cincuenta años para gestionar documentos en papel. Tales métodos se apoyaban, entre otros principios subyacentes, en la asunción de que los documentos ocupaban un espacio físico, “estaban” en un lugar identificable,<sup>10</sup> asunción que, como demuestra el escenario descrito en el párrafo anterior, han venido a tirar por tierra las actuales tecnologías de la información y de convergencia universal. Los documentos ya no están en un lugar, sino en un conjunto de sistemas distribuidos, complejos e interconectados. En último extremo, los documentos ni siquiera “son”.<sup>11</sup> Por tanto, si es que los gestores de documentos o los archiveros quieren seguir jugando el rol de custodios, de garantes de evidencia, tienen que salir del lugar en el que anteriormente dormitaba su objeto y viajar a ese País de Nunca Jamás en el que los objetos no existen, sino que más bien continuamente se procesan.<sup>12</sup> El gestor de documentos, el archivero, ha perdido la sombra que sólidamente le sostuvo durante un siglo y medio, la sombra de la estabilidad, de la neutralidad, y embarcarse en la aventura de, sin sombra, comenzar a gestionar el sistema, ya nunca maduro, ya nunca estable, sino, muy al contrario, infantilmente en perpetuo movimiento.

<sup>10</sup> Puede encontrarse una impecable defensa de este principio en Duranti, Luciana: “Archives as a Place”. En: *Archives & Manuscripts*. Vol. 24, n. 2 (1996). P. 242-255.

<sup>11</sup> Confróntese, Ketelaar, Delgado Gómez, *op. cit.*; también, Ketelaar, Eric: “Writing on Archiving Machines”. En: Neef, Sonja, van Dijck, José, Ketelaar, Eric (eds.), *Sign here! Handwriting in the Age of New Media*. Amsterdam University Press, Amsterdam, 2006. P. 183-195.

<sup>12</sup> Confróntese, por ejemplo, Cook, Terry: “Electronic Records, Paper Minds: The Revolution in Information Management and Archives in the Post-Custodial and Post-Modernist Era”. En: *Archives and Social Studies: A Journal of Interdisciplinary Research*. Vol. 1, n. 0. URL: [http://socialstudies.cartagena.es/images/PDF/no0/cook\\_electronic.pdf](http://socialstudies.cartagena.es/images/PDF/no0/cook_electronic.pdf) (Consulta: 25-2-2010); “From Information to Knowledge: An Intellectual Paradigm for Archives”. En: Nesmith, Tom, ed.: *Canadian Archival Studies and the Rediscovery of Provenance*. Society of American Archivists and Association of Canadian Archivists, in association with The Scarecrow Press, 1993. P. 201-226.

### III.1 La gestión de documentos en el Ayuntamiento de Cartagena

Para que la organización no sufra un colapso ni quiebre su funcionamiento cotidiano, es evidente que todo el complejo entramado más arriba descrito debe fundirse, integrarse, conectarse de manera muy meticulosa; pero también es evidente, como se anticipó, que este constante flujo de datos que generan documentos supone un riesgo permanente, espacial y temporal, para tales datos y para el cumplimiento de los requisitos documentales exigidos por la Ley.<sup>13</sup> Por ello es necesario que los controles y procesos archivísticos y documentales que garantizan tales requisitos no se ejecuten al final del proceso, sino que estén incluidos al comienzo del mismo, en el momento del diseño o de la integración. Como ya indican normas de reconocido prestigio, como *ISO 15489 – Gestión de documentos*,<sup>14</sup> y la práctica jurídica y archivística desde hace siglos, si los documentos han de ser evidencia de acciones, deben generarse en el momento mismo en que se producen esas acciones, o tan pronto como sea posible después de la acción. Cuanto más tiempo pasa entre la acción y el documento que la refleja, más débil es la evidencia y el cumplimiento de los requisitos documentales. En el entorno electrónico, en el que no dejan de ejecutarse acciones, esta convención centenaria deviene una necesidad crítica. Además, y como ya vienen indicando proyectos pioneros, por ejemplo *Clever Recordkeeping Metadata*<sup>15</sup> y sus derivados, en entornos electrónicos costosos en dinero, tiempo, equipamiento y personal, la reutilización de datos en distintos

<sup>13</sup> La exposición al riesgo en sistemas en movimiento ha sido detalladamente descrita, así como sus alternativas, en Duranti, Luciana (ed.): *La conservación a largo plazo de documentos electrónicos auténticos: hallazgos del Proyecto InterPARES*. Cartagena: Ayuntamiento: 3000 Informática, 2005.

<sup>14</sup> ISO 15489-1: *Información y documentación – Gestión de documentos. Parte 1: Generalidades*. Ginebra: International Organization for Standardization, 2001.

<sup>15</sup> *Clever Recordkeeping Metadata* –URL: <http://www.sims.monash.edu.au/research/rcrg/research/crm/index.html> (Consulta: 25-2-2010). Una descripción del mismo puede encontrarse en: Evans, Joanne, McKemmish, Sue y Bhoday, Karuna: "Create Once, Use Many Times: The Clever Use of Recordkeeping Metadata for Multiple Archival Purposes". En: *Archival Science*. N. 5 (2005). P. 17-42.

puntos del rango de vida documental supone, no sólo garantía de evidencia, sino también economía de costes. Por ejemplo, si el sistema de archivo conecta con el sistema de registro para capturar los datos existentes en el mismo, en lugar de reescribirlos al final del proceso, no sólo dispondrá de mejor evidencia, sino que además ahorrará tiempo, dinero y personal.

Para conseguir que esta compleja integración funcione, no obstante, resulta imprescindible la habilitación de ciertos componentes facilitadores, tanto conceptuales como físicos:

- En primer lugar, es necesaria la actitud positiva y colaboradora de los distintos agentes que intervienen en el entorno de producción y en los sistemas de información y de documentos: archiveros, informáticos, juristas, responsables de calidad, etc.<sup>16</sup>
- En segundo lugar, es necesario que se comprenda que ya no existen sistemas de gestión, sistemas de gestión de información y sistemas de gestión de documentos por separado, sino que, muy al contrario, todos se encuentran conectados en algún punto y todos deben integrar de manera coherente sus diferentes requisitos.<sup>17</sup>
- Por último, se precisa de un sistema físico y lógico que permita, por una parte, esta integración permanente, y, por otra, el dejar traza de la misma con objeto de cumplir los requisitos de evidencia exigidos por la Ley.

El proyecto expuesto en el presente texto, por tanto, aborda el reto de diseñar un sistema de gestión de documentos y archivo, que, sin dejar de satisfacer los controles y procesos archivísticos que permiten garantizar los requisitos establecidos en la Ley, sea capaz de conectar estos controles y procesos con los distintos sistemas y subsistemas de gestión y de gestión de la información en una organización, y no a posteriori, sino desde el mismo momento en que se diseñan o integran tales sistemas y subsistemas, de tal manera que las garantías documentales queden establecidas desde el principio y durante tanto tiempo como se requiera.

<sup>16</sup> El International Records Management Trust, por ejemplo, ha dedicado una buena parte de sus módulos formativos a explicar "cómo vender" la gestión de documentos a la organización: International Records Management Trust: *Training in Electronic Records Management*, particularmente en sus dos primeros módulos. London: IRMT, 2009.

<sup>17</sup> Confróntese, por ejemplo, Delgado Gómez, Alejandro: *El centro y la equis: una introducción a la descripción archivística contemporánea*. Cartagena: Ayuntamiento; 3000 Informática, 2007.

Para conseguir este fin se precisa un sistema que permita:

- Cumplir los requisitos de confiabilidad establecidos tanto por ley (Ley 11/2007, art. 31.2 y .3: integridad, autenticidad, confidencialidad, calidad, protección, conservación, identificación de los usuarios, control de accesos, protección de datos, posibilidad de trasladar los datos a otros formatos y soportes) como por normas técnicas (ISO 15489: autenticidad, fiabilidad, integridad, disponibilidad; Consejo Internacional de Archivos: autenticidad, completitud, accesibilidad, comprensibilidad, procesabilidad, reutilización;<sup>18</sup> ISO 23081;<sup>19</sup> MoReq2)<sup>20</sup> y buenas prácticas reconocidas (InterPARES: fiabilidad, completitud, control sobre el procedimiento de creación, autenticidad, integridad, identidad, exactitud, precisión, corrección, verdad y pertinencia);<sup>21</sup>
- Garantizar que tales requisitos queden establecidos en el comienzo de los procesos de diseño o integración, y en distintos sistemas y subsistemas, haciendo uso por tanto de las tecnologías más interoperables y con mejores posibilidades de interconexión sin pérdida de integridad existentes en cada momento; y
- Garantizar que tales requisitos se pueden seguir manteniendo a lo largo del tiempo, reutilizando en fases posteriores o simultáneas aquellos componentes que permitan sostener a coste razonable una mejor evidencia.

<sup>18</sup> Consejo Internacional de Archivos: *Documentos electrónicos: manual para archiveros*. Madrid: Ministerio de Cultura, 2006.

<sup>19</sup> ISO 23081-1:2006: *Information and documentation - Records management processes - Metadata for records - Part 1: Principles*. Geneva: International Organization for Standardization, 2006.

<sup>20</sup> MoReq2 Specification: *Model Requirements for the Management of Electronic Records: Update and Extension 2008*. Bruxelles, Luxembourg: CECA-CEE-CEEA, 2008. URL: <http://www.moreq2.eu/downloads.htm> (Consulta: 25-2-2010).

<sup>21</sup> InterPARES Project: *Ontology C: Trustworthiness of a Record*. URL: [http://www.interpares.org/ip2/ip2\\_terminology\\_db.cfm](http://www.interpares.org/ip2/ip2_terminology_db.cfm) (Consulta: 25-2-2010).

## IV. Alcance del proyecto

De conformidad con lo expuesto en la sección anterior, el proyecto descrito en el presente artículo aborda el desarrollo de un sistema de gestión de documentos y archivo integrable desde el comienzo con los distintos sistemas y subsistemas de gestión y de gestión de la información derivados de la creciente implantación de modelos de administración electrónica. Este sistema, de conformidad con la legislación, debe permitir, no sólo satisfacer los principios que rigen la mera administración o el gobierno electrónicos, sino particularmente lo que se ha venido a conocer como gobernanza electrónica, una necesidad crítica en un momento de crisis global derivada de un mal gobierno generalizado tanto a nivel internacional, como a todos los niveles gubernamentales dentro de la nación. Ahora bien, puesto que los escenarios en los que la administración, el gobierno y la gobernanza electrónicos tienen lugar, son o pueden ser, como se ha sugerido en la sección anterior, múltiples, imprevisibles, complejos y dispersos, el mencionado sistema debe disponer de unas determinadas características que lo pongan en disposición de afrontar diversas realidades, a saber:

- Debe estar desarrollado, como se ha dicho, con la tecnología con mejores posibilidades de interconexión, integración e interoperabilidad existente en cada momento; en el actual estado de conocimiento de la ingeniería informática estas tecnologías son aquellas de fuente abierta y de software libre, por ejemplo J2EE, XML, Linux, etc. No podemos olvidar, sin embargo, la emergente reutilización o combinación de tecnologías preexistentes conocida como *Cloud Computing*. Aunque la nube se encuentra en fase de euforia y pendiente de refinamiento y contraste, ciertamente es económica, ecológica, permite redistribuir el conocimiento de nuevas maneras, y se alinea con un reforzamiento de la noción de sociedad de la información como vía de

escape de una de las peores crisis conocidas en el último siglo.<sup>22</sup>

- Además, debe tratarse de una tecnología que admita rápidos desarrollos para configurar, parametrizar y personalizar el sistema, dependiendo de las diferentes necesidades de esas diversas realidades. Una vez más, la nube parece flotar en torno a este requisito.
- Por último, debe ser un sistema altamente modular, con el objeto de implantar aquellos subsistemas que cada realidad demande y no otros, sin dejar de satisfacer los controles y procesos documentales. Y una vez más, asoma la nube, ese País de Nunca Jamás por encima de aquel País de Nunca Jamás que ahora comienza a parecer provincia.

En lo que concierne a las dos primeras características, las soluciones estrictamente tecnológicas no son el enfoque del presente artículo, que se concentra más bien en los controles y procesos documentales. En lo que concierne a los módulos que deben componer el sistema, éstos se describen a continuación. Téngase en cuenta que para la definición de tales módulos se han tomado en consideración, tanto los controles y procesos archivísticos convencionales, como los requisitos funcionales expuestos en dos modelos de diferente naturaleza, pero cuya certificación contribuirá a garantizar la calidad en años venideros: por una parte, la ya mencionada especificación europea MoReq2; por otras, los requisitos funcionales del Consejo Internacional de Archivos, que están en la base de un futuro informe técnico ISO.<sup>23</sup> Además, se ha tenido en mente el cambio de orientación del propio SC I I ISO,

<sup>22</sup> Acerca del fenómeno del *Cloud Computing*, confróntense, por ejemplo, Dikaiakos, Marios D., Pallis, George, Katsaros, Dimitrios, Mehra, Pankaj, Vakali, Athena: *Cloud Computing: Distributed Internet Computing for IT and Scientific Research*. Buyya, Rajkumar, Chee, Shin Yeo, Venugopal, Srikumar: *Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities*. Particularmente, el monográfico "Cloud Computing: IT's Day in the Sun?# En: *The Journal of Information Technology Management*. Vol. 22, No. 6-7 (June-July 2009).

<sup>23</sup> International Council on Archives and Australasian Digital Records Initiative, *Principles and Functional Requirements for Records in Electronic Office Environments – Module 1: Overview and Statement of Principles*, 2008, published at [www.ica.org](http://www.ica.org); International Council on Archives, *Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems*, 2008, published at [www.ica.org](http://www.ica.org); International Council on Archives, *Principles and Functional Requirements for Records in Electronic Office Environments – Module 3: Guidelines and Functional Requirements for Records in Business Systems*, 2008, published at [www.ica.org](http://www.ica.org) (Consulta: 25-2-2010).

que está modificando ISO 15489 para convertirla en un modelo orientado a sistemas bajo controles y procesos; y, por supuesto, tanto la Ley 11/2007 como el cuerpo legal, anterior o posterior, del que se constituye en eje vertebrador: la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información; el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica; el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos; la Ley 59/2003, de 19 de diciembre, de firma electrónica; la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento que desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; etc.

#### **IV. 1 Una solución propuesta**

En lo que sigue, se describe una solución que, tras dos años de experimentación, ha resultado viable y satisfactoria. Por supuesto no es la única, pero creemos que puede resultar sugerente y aportar ideas para aquellos gestores de documentos y archiveros que quieren viajar al País de Nunca Jamás, y que quizá aún no conocen con exactitud su hoja de ruta. La descripción utiliza una estructuración a partir de los convencionales procesos archivísticos, a efectos de comodidad de lectura.

#### **IV.2 La descripción archivística**

En la medida en la que, como reconocen tanto normas técnicas (por ejemplo *ISO 23081–Metadatos para la gestión de documentos*), como buenas prácticas y proyectos de reconocido prestigio (*Clever Recordkeeping Metadata*, *Recordkeeping Metadata Standard*,<sup>24</sup> InterPARES), y líderes de la disciplina a nivel internacional, en el entorno electrónico los metadatos, tanto

<sup>24</sup> Recordkeeping Metadata Project. URL: <http://www.sims.monash.edu.au/research/rcrg/research/spirt/index.html> (Consulta: 25-2-2010).

en el punto de captura como posteriores al mismo, son componentes fundamentales para garantizar los requisitos de confiabilidad del documento y de la información registrada, un módulo de introducción de datos deviene central al sistema. La introducción de datos, y de sus metadatos asociados, debe estar automatizada hasta donde sea posible; es decir, este módulo debe conectar con las bases de datos de otros sistemas para obtener de ellas la información que resulte relevante a efectos de garantizar la confiabilidad, y esto con un doble fin: por una parte, minimizar la intervención humana, que puede conducir a errores o a acciones maliciosas; por otra, garantizar una mejor evidencia, por cuanto los datos no se introducen a posteriori, sino que se capturan en el mismo momento en el que entran en el sistema de origen.

No obstante, los metadatos no sólo cumplen la función de garantizar evidencia, sino que, convencionalmente, se usan también para incorporar al documento información de valor añadido, con el objeto de contribuir a encontrarlo y recuperarlo. Por este motivo, el proyecto ha añadido al módulo de introducción de datos una funcionalidad de descripción que permite, esta vez sí a posteriori, insertar metadatos contextuales a efectos de descubrimiento y recuperación.

Una segunda circunstancia que debe tenerse en cuenta al diseñar el módulo de introducción de datos es el hecho de que debe conectarse a sistemas distintos, con diferentes modelos y estructuras de datos, y diversos esquemas de metadatos, e incluso el hecho de que estos modelos, estructuras y esquemas son a veces contradictorios entre sí o se solapan en algunos aspectos. Además, en la actualidad existen múltiples esquemas de metadatos, como mostraría por ejemplo el registro MADRAS,<sup>25</sup> y es probable que, para obtener una alta garantía de mejor evidencia, varios de ellos tengan que interoperar, en un esquema de diseño propio. Por ello, un módulo de introducción de datos debe tener una estructura muy amplia y flexible, para que, mediante un interfaz amigable, puedan definirse multitud de campos de origen y destino, así como sus propiedades, para acoger, sin pérdida de identidad e integridad, datos y metadatos de diversa naturaleza.

<sup>25</sup> Evans, Joanne, Lindberg, Lori: "Describing and analyzing the recordkeeping capabilities of metadata sets". URL: [http://www.nl.go.kr/dcpapers/pdf/2004/Paper\\_27.pdf](http://www.nl.go.kr/dcpapers/pdf/2004/Paper_27.pdf) (Consulta: 25-2-2010).



Otra circunstancia que debe tenerse en cuenta, al hilo de la amplitud de la estructura de datos, es el hecho de que el sistema debe ser utilizado por usuarios que no tienen por qué tener destrezas en el uso de grandes modelos poco manejables cotidianamente. Por ello, el módulo de introducción de datos tiene que contemplar la inserción de una funcionalidad de diseño de plantillas o formularios que permita presentar, y trabajar con, sólo aquellas porciones de la estructura que resulten relevantes para diferentes usuarios, así como asignar atributos que faciliten este trabajo.

Estas plantillas o formularios deben cumplir además una segunda funcionalidad. Recuérdese que en el escenario dibujado no todos los documentos serán electrónicos, sino que durante un margen de tiempo previsiblemente amplio también se gestionarán documentos en papel. Para un sistema híbrido, las plantillas se utilizarán para la gestión de expedientes analógicos, de tal manera que los datos de los mismos también queden incorporados al sistema de gestión de documentos y de archivo desde el inicio, no a posteriori.

Además, al hilo de la necesidad de una amplia estructura de datos, debe preverse el hecho de que éstos pueden representarse de diferente manera, por ejemplo en aplicación de diferentes esquemas de metadatos; o incluso puede que no sea conveniente, por ética o reglamentación, que determinados datos sean representados a determinados usuarios. Por este motivo, deben implantarse funcionalidades que permitan el diseño de distintas representaciones, en pantalla o impresas, dependiendo de los diferentes tipos de datos y usuarios.

Por otra parte, debe tenerse en cuenta que, tradicionalmente, y esta tradición ha sido recogida por normas de reconocido prestigio como ISO 15489 o *Recordkeeping Metadata Standard*, un medio fundamental para garantizar mejor evidencia es disponer de sistemas de clasificación de distinto tipo —funcional, de conservación, de acceso, de indización—, que se asignan en forma de metadatos. Estos sistemas de clasificación tienen que estar integrados en el módulo de introducción de datos y, de manera más importante, tienen que venir asignados automáticamente en los sistemas de origen, de tal modo que la conexión deviene bidireccional: no sólo es preciso que el sistema recupere datos de otros sistemas,

sino que además tiene que insertar en estos otros sistemas de origen los metadatos de sistema de clasificación, de manera no intrusiva.

Por último, debe tenerse también en cuenta que estos datos y metadatos no constituyen por sí mismos el documento que tiene que custodiar el sistema de gestión de documentos y de archivo. Con toda probabilidad, los diferentes sistemas de gestión y de gestión de la información dispondrán de distintos mecanismos, como por ejemplo la combinación de datos con una plantilla, para generar representaciones de documentos, por ejemplo un PDF. Estos ficheros que representan documentos también pasan a la custodia del sistema de gestión de documentos y de archivo, de tal manera que debe existir una funcionalidad que permita vincular de manera inextricable los datos y metadatos obtenidos con los ficheros a los que hacen referencia, así como a las reglas de negocio y cualquier otra documentación que ayude a interpretar a largo plazo cómo funcionaba el sistema de origen.

### **IV.3 Los usuarios del sistema**

Una de las características distintivas de los documentos generados por las administraciones y organismos públicos es el hecho de que frecuentemente contienen información sensible y sujeta a medidas de protección de datos. El que se puedan producir violaciones a tales medidas de protección es, en escenarios electrónicos distribuidos como el que se ha descrito en sección anterior, un riesgo evidente, que debe minimizarse mediante una adecuada definición de usuarios, grupos y roles, así como de los accesos a datos y funcionalidades a que tiene derecho cada uno de ellos. En este sentido, el sistema de gestión de documentos y archivo objeto del proyecto que se describe en el presente artículo plantea los siguientes requisitos:

En primer lugar, el módulo que nos ocupa debe disponer de funcionalidades de restricción, no sólo de usuarios, sino también de datos. Téngase en cuenta que en entornos distribuidos e interconectados existirán probablemente diferentes unidades organizativas, cada una de ellas generadora de distintos tipos documentales, y no siempre será conveniente,

por ética o reglamentación, que los documentos generados por una unidad sean accesibles a otra. Así, el módulo de gestión de usuarios debe disponer de una funcionalidad para la configuración de diferentes depósitos de datos a los que sólo puedan acceder aquellos usuarios a los que el administrador les confiera tal derecho, con independencia de que los administradores tengan acceso a todos los depósitos. Esta funcionalidad debe venir complementada por otra que evite, dado el uso de tecnología web, el que un usuario, mediante navegación por hipervínculos, pueda llegar a acceder a información a la que no tiene derecho. En este sentido, la ya descrita funcionalidad de configuración de representaciones en pantalla o impresas constituirá también una ayuda inapreciable. No puede perderse de vista el hecho de que, en entornos distribuidos, el acceso se producirá en muchas ocasiones vía intranet o extranet, con los riesgos adicionales que esto implica. De hecho, las nuevas aplicaciones diseñadas para diferentes propósitos por el Servicio de Informática del Ayuntamiento de Cartagena se distribuyen vía intranet, pero no para todos los trabajadores: cada uno de ellos tiene acceso únicamente a aquellas que son necesarias para la ejecución de sus tareas.

En lo que concierne a los privilegios y restricciones, ya no por datos, sino por usuarios, el módulo de gestión de usuarios debe disponer de dos funcionalidades: una de ellas debe permitir definir grupos o roles de usuarios, por unidades organizativas o cualquier otro criterio que se considere relevante; y la otra debe permitir definir usuarios individuales. El motivo de separar grupos y usuarios es el hecho de que muchos usuarios tendrán idénticos derechos de acceso o idénticas restricciones. Si éstos se definen en un grupo, es posible que los usuarios individuales hereden los permisos del grupo, de tal modo que se minimice el trabajo de gestión de permisos. Por lo demás, en un escenario como el descrito también es muy probable que otros sistemas tengan otros modelos de permisos de usuario: un directorio LDAP para toda la organización, un sistema de usuario y contraseña para acceder a la intranet, un sistema de pin para acceder a las aplicaciones web, etc. Con el objeto de evitar el que un usuario tenga que autenticarse en múltiples aplicaciones, el módulo de gestión de usuarios debe conectar también con los sistemas de autenticación

del Ayuntamiento, y los metadatos de usuario asociados en estos sistemas también deben pasar a formar parte de los metadatos de usuario del módulo de gestión de usuarios. Por ejemplo, el Ayuntamiento dispone de un sistema LDAP por el que pasan todos sus demás sistemas. En este caso, la conexión se llevará a cabo con este mecanismo de autenticación centralizado, y los metadatos de éste pasan a ser automáticamente también metadatos del módulo de gestión de usuarios.

No obstante, puede que esto no sea suficiente. El sistema de gestión de documentos y archivo objeto del proyecto descrito en el presente artículo dispone de funcionalidades de configuración complejas y sofisticadas que no deberían estar al alcance de todos los usuarios, para no producir incoherencias ni quiebras en el sistema. Por ello, se incorporará una funcionalidad para restringir y personalizar las opciones de menú a que puede tener acceso cada usuario o grupo de usuarios. Como complemento de esta funcionalidad, se añadirá una funcionalidad de parametrización de restricciones adicionales por grupos de usuarios.

A pesar de todas las precauciones que se tomen, el riesgo de violación de privilegios por error o de manera maliciosa siempre seguirá existiendo. Por este motivo, todas las normas y buenas prácticas reconocen la necesidad de disponer de una pista de auditoría inalterable y no eliminable, en la que queden reflejadas todas las acciones llevadas a cabo por los usuarios del sistema, incluidos los intentos de violación. Esta pista de auditoría almacenará la acción llevada a cabo, el usuario que la realizó y la fecha y hora de la misma.

Con todo, debe tenerse en cuenta que al proyecto descrito en el presente artículo le concierne un sistema de gestión de documentos y archivo destinado a custodiar documentos a largo plazo y no sólo con fines administrativos, sino también de investigación, históricos, culturales, etc. Así, además de las restricciones de acceso deben preverse los derechos de acceso de la ciudadanía y de los investigadores. Dado que tales derechos de acceso y los plazos en que los documentos son accesibles y para quién vienen dados por ley (por ejemplo la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español; la Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por

el Real Decreto Legislativo 1/1996, de 12 de abril; o la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común), los mecanismos de restricción serán los ya mencionados con fines administrativos. Sin embargo, se incorporará al módulo de gestión de usuarios una funcionalidad de gestión de usuarios externos que, al igual que en el caso del nivel administrativo, permitirá tanto la definición de perfiles, grupos y usuarios individuales, como la visualización de datos y documentos con valor histórico o para la investigación. En condiciones ideales, siempre que pudiera garantizarse que no se producirán brechas de seguridad, el módulo de acceso a la investigación debería conectar con los sitios web externos del organismo. Sin embargo, asegurar que no se producirán brechas de seguridad es extremadamente difícil, de tal manera que en la mayoría de los casos, y con el objeto de facilitar el acceso de la ciudadanía a través de Internet, será necesario replicar las porciones accesibles de la base de datos de manera independiente, y proceder a la conexión con el sistema, a efectos por ejemplo estadísticos o de control, mediante pasarelas que garanticen mayor seguridad.

#### **IV.4 La conservación de los documentos**

Una de las funciones esenciales de un sistema de gestión de documentos y archivo, impuesta además por ley, es la adecuada conservación y custodia de los documentos, en tanto tercera parte fiable, durante tanto tiempo como resulte preciso, que puede ser durante toda la vida del documento, es decir, siglos, o al menos, de manera más realista, durante toda la vida del responsable de los documentos, dado que el largo plazo deviene cada vez más difuso e inseguro, y sustituirlo por un prudente “a lo largo del tiempo” resultaría más adecuado. Téngase en cuenta, no obstante, que la conservación no es un proceso único, sino un compuesto de diferentes procesos de disposición —valoración, transferencia, eliminación reglada, conservación permanente—, y que, en entornos electrónicos, particularmente si conviven con sistemas en papel, las circunstancias de conservación pueden ser extremadamente variadas. Por poner sólo unos ejemplos: puede que tengan que valorarse

documentos en papel y que estas decisiones de valoración deban quedar documentadas en el sistema; puede que tengan que valorarse documentos electrónicos que no están aislados, sino en interacción con otros muchos componentes de los sistemas del organismo, de tal manera que su eliminación conduzca a un mal funcionamiento de otro sistema o subsistema; puede que se produzca una transferencia física de documentos electrónicos a un servidor diferente al de origen, y sus metadatos pueden pasar a otro servidor, de tal manera que también habrá que extremar las precauciones para que no se pierdan los vínculos; puede que no se transfieran físicamente porque, por ejemplo, siguen estando en mejores condiciones de seguridad en el servidor de origen, pero sí se transfiera la responsabilidad sobre los documentos, de modo que habrá que modificar cuidadosamente los roles de los usuarios; puede que se transfieran documentos en papel, pero sus metadatos se transfieran de un sistema *legacy* y haya que convertirlos, con las debidas garantías de autenticidad, a un formato actualizado; puede que se prevea un cambio de tecnología y para seguir conservando de manera auténtica los documentos haya que proceder a una cuidadosa conversión de datos, metadatos y documentos; etc. Esta extrema diversidad de circunstancias ha convertido el proceso, o los procesos, de conservación en una interminable tarea de documentar todas las acciones que tienen lugar sobre los documentos y sus componentes. Esto obliga, aún más si cabe, al sistema de gestión de documentos y de archivo que es objeto del proyecto descrito en el presente artículo, a extremar las precauciones en un triple sentido: en primer lugar, la estructura de datos debe ser lo suficientemente amplia como para admitir todos los metadatos de conservación que serán necesarios para garantizar a lo largo del tiempo los requisitos exigidos por ley; en segundo lugar, las tecnologías a utilizar deben ser aquellas que mejor garanticen que pueden realizarse movimientos como migraciones, conversiones o exportaciones de datos a lo largo del tiempo y sin pérdida de integridad; en tercer lugar, y teniendo en cuenta que, bien por mala gestión de la conservación, bien por decisiones regladas de eliminación, se pueden perder, y de hecho se perderán, datos, información o documentos, las decisiones de conservación deben configurarse al inicio, en los sistemas de origen, el módulo de conservación tiene que estar conectado con ellos de manera

no intrusiva, y los procesos deben automatizarse, aun sin perder el control por parte de humanos, por ejemplo administradores o auditores.

Teniendo en cuenta esta enorme complejidad, el módulo de conservación dispondrá, en primer lugar, de una funcionalidad de definición de calendario de conservación, en el que, por tipos documentales y atendiendo a lo que disponga la legislación y otras regulaciones en cada momento, se configurarán, previo análisis de los valores administrativos, jurídicos, legales, financieros, informativos, culturales, etc., y debidamente contextualizados en sus sistemas de origen y en sus relaciones con otros tipos documentales, los plazos de las acciones de disposición (transferencia, eliminación, conservación permanente) sobre cada tipo documental y sus componentes. De igual modo, se definirá el método de disposición (transferencia de responsabilidad, transferencia total, transferencia de metadatos pero no de documentos, conversión de formato...). Para que este análisis y esta configuración tengan éxito, no obstante, se precisan dos tipos de conexión. En primer lugar, se precisa una conexión interna con el módulo de introducción de datos, en el que deben incorporarse automáticamente todos los datos relativos a conservación, incluido el esquema de metadatos de conservación más exhaustivo existente en cada momento, y que a los efectos del presente proyecto será PREMIS.<sup>26</sup> Además, como se anticipó, se precisa una segunda conexión, o conexiones, con los sistemas que generan esos tipos documentales, con un doble fin: por una parte, incorporar, también en forma de metadatos, las acciones de disposición que deben tener lugar sobre ellos y sus plazos; por otra, extraer de forma automática tantos metadatos PREMIS como sea posible, minimizando de esta manera la posibilidad de fallo humano. Un ejemplo del primer fin es la adición de un campo "Fecha de transferencia" a la estructura de datos del sistema de origen. Un ejemplo del segundo es la llamada al formato de fichero en el que se almacena el documento para que automáticamente se rellene en el esquema de metadatos PREMIS.

<sup>26</sup> PREMIS Editorial Committee : PREMIS Data Dictionary for Preservation Metadata. Version 2.0. The Library of Congress, 2008. URL: <http://www.loc.gov/standards/premis/>(Consulta: 25-2-2010).

El módulo de conservación debe disponer de dos funcionalidades, una de transferencia y otra de eliminación, que admitan todo el abanico de posibilidades que se ha explicado más arriba: transferencia de documentos electrónicos y en papel, de responsabilidad, de documentos y datos y metadatos por separado, eliminación reglada en distintas fases, etc. Para ello, estas funcionalidades deben ser configurables de conformidad con los criterios expuestos en la funcionalidad acerca de calendario, siendo tal configuración accesible sólo para los administradores. La funcionalidad de eliminación sólo debe ser accesible a administradores o usuarios a los que se les asigne formalmente tal responsabilidad. La funcionalidad de transferencia, sin embargo, debe ser susceptible de configuración de un doble interfaz: el primero de ellos debe mostrar a los usuarios del sistema de origen aquellas fases del proceso de transferencia que sean de su interés, para proceder a su validación; el segundo debe mostrar a los usuarios del sistema de destino, sean o no los usuarios del sistema de gestión de documentos y archivo, los datos, información o documentos que reciben y en qué circunstancias, para proceder a una segunda validación. Por lo demás, previendo la posibilidad de que determinados sistemas, dentro del Ayuntamiento, gestionen documentos en papel o datos en formatos obsoletos o con escasas posibilidades de duración, se incluirá una funcionalidad de importación de datos a formatos normalizados desde sistemas *legacy*.

Evidentemente, el módulo de conservación constará de una funcionalidad de conservación a lo largo del tiempo, que, en el caso del proyecto que nos ocupa, adoptará la forma de depósito seguro OAI.<sup>27</sup> Aunque el modelo OAI, en su representación original y en aquella que queda reflejada en la norma ISO 14721<sup>28</sup> que establece sus especificaciones, no se corresponde con el escenario complejo y distribuido que se ha diseñado en la sección anterior, en realidad esta representación es traducible a entornos complejos en los que participa más de un sistema del organismo, o incluso sistemas de diferentes organismos. Por una parte, los requisitos tanto funcionales como de información de un OAI tienen un alto

<sup>27</sup> *Archival Information System (OAI): CCSDS 650.0-B-1: Blue Book: January 2002*. CCSDS, 2002.

<sup>28</sup> ISO 14721:2003: *Space data and information transfer systems —Open archival information system —Reference model*. Geneva: International Organization for Standardization, 2003.



grado de detalle, lo cual permite establecer garantías de que las transmisiones hacia, dentro de y desde el depósito, se realizarán bajo estrictas condiciones; y, por otra, básicamente un OAIS simplemente asevera que debe existir un depósito seguro de objetos digitales junto con sus metadatos, adoptando la severa pero segura herramienta de encapsulación, que también ha sido adoptada por exitosos proyectos como *Victorian Records Electronic Strategy* (VERS);<sup>29</sup> así como que deben existir tres tipos de agentes, aquellos que envían información al depósito, aquellos que administran o gestionan el depósito y aquellos que solicitan paquetes de información al depósito. En ningún caso se requiere que deba existir un solo depósito ni en una sola ubicación física. Por tanto, el modelo es aplicable en entornos distribuidos y complejos, como el que nos ocupa.

No obstante, y como ha venido sucediendo en los módulos descritos más arriba, si han de convivir durante un cierto período documentos electrónicos y en papel, el módulo de conservación contemplará la funcionalidad de gestión de depósitos físicos, complementaria de la anterior, y de gestión de expedientes híbridos, que, tal y como recomiendan tanto MoReq2 como el Consejo Internacional de Archivos, se gestionarán mediante metadatos utilizados como marcadores, insertos de manera no intrusiva en los sistemas de origen, y extraídos automáticamente para ser controlados desde el módulo de introducción de datos.

#### **IV.5 El acceso a los documentos**

Como ya se ha adelantado, la finalidad última de un sistema de gestión de documentos y archivo no es por defecto restringir, sino facilitar el acceso a los documentos y a la información, con los controles legales y reglamentarios que sean del caso, y con las debidas medidas de seguridad. Con el objeto de facilitar el acceso a usuarios tanto internos como externos, sin dejar de garantizar la seguridad de aquellos datos que no deban ser vistos por determinados segmentos de usuarios, el proyecto que se describe en el presente artículo propone un módulo de acceso con las siguientes funcionalidades:

<sup>29</sup> VERS: *Forever Digital*. URL: <http://www.prov.vic.gov.au/vers/vers/default.htm> (Consulta: 25-2-2010).

En primer lugar, debe incluirse una funcionalidad que permita determinar cómo deben realizarse las consultas al sistema y qué consultas pueden realizarse, dependiendo del tipo de usuarios y de datos, puesto que, como se ha descrito en secciones precedentes, no todos los usuarios deberían tener acceso a todos los datos. Esta funcionalidad facilitará, pues, a los administradores la posibilidad de determinar las condiciones de búsqueda, de construir la sintaxis de los criterios de consulta y de diseñar los interfaces de consulta para diferentes tipos de usuarios. Los resultados de esta configuración estarán inmediatamente vinculados al módulo de gestión de usuarios y de privilegios de acceso de los mismos.

En segundo lugar, y como contrapartida de la funcionalidad de configuración de consulta, debe existir una funcionalidad de interfaz o interfaces de búsqueda, determinadas desde esa primera funcionalidad. Este interfaz de búsqueda, dependiendo del tipo de documento y de los privilegios de usuario, debe permitir realizar al usuario, interno o externo, distintos tipos de operaciones: consulta sólo de los datos, solicitud de acceso de sólo lectura al fichero que constituye la representación del documento, solicitud de copia simple o autenticada, o solicitud de préstamo, si se trata de un documento en papel. Siempre que la seguridad quede garantizada, esta funcionalidad promoverá el acceso mediante tecnología web: intranet, extranet, Internet, SMS o TDT; así como la navegación segura mediante hipervínculo.

En tercer lugar, no debe olvidarse, como se ha indicado anteriormente, que el sistema no sólo ha sido concebido con fines administrativos, sino también con fines culturales y de investigación, de tal modo que, siempre que se permita el acceso externo mediante tecnología web y con las debidas medidas de seguridad, se conectará la funcionalidad de consulta con herramientas inclusivas y sociales tipo Web 2.0 que permitan recuperar información de valor añadido. Esto significa, por ejemplo, que, bajo las debidas garantías, la ciudadanía debería poder recuperar, no sólo los registros existentes en el sistema a los que tenga derecho, sino, digamos, registros de un instrumento wiki existente en el organismo,

como es el caso de la herramienta, también desarrollada por el Ayuntamiento, CTpedia,<sup>30</sup> a efectos de contextualización; o debería poder insertar, sin perjudicar el funcionamiento del sistema, etiquetas que contribuyeran a enriquecer el registro y recuperarlo desde distintos puntos de vista, tal y como vienen haciendo las aplicaciones de gestión bibliotecaria de uso común en el Ayuntamiento, y desarrolladas por la misma compañía que colabora en el proyecto. Con ello no se pretende disminuir el valor de evidencia del documento a favor de su valor informativo. Muy al contrario, se pretenden incluir en el documento interpretaciones y significados paralelos a las interpretaciones y significados que le proporciona el archivo, contribuyendo con ello a su democratización.<sup>31</sup>

## V. Otras funcionalidades

Como se ha indicado en sección precedente, la tecnología a utilizar debe ser lo suficientemente flexible como para permitir desarrollar de manera rápida y eficaz módulos complementarios de estos módulos centrales, a medida que se vaya mostrando su necesidad. Ejemplos de tales módulos incluyen:

- Estadísticas e indicadores de rendimiento
- Administración y configuración avanzadas
- Construcción de tesauros temáticos o funcionales, o
- Posibilidad de realizar operaciones masivas sin pérdida de integridad

<sup>30</sup> CTpedia. URL: <http://www.ctpedia.es/w/index.php/Portada> (Consulta: 25-2-2010).

<sup>31</sup> Ketelaar, Eric: "Archival temples, archival prisons: Modes of power and protection". En: *Archival Science*. Vol. 2, n- 3-4 (September 2002). P. 221-238; "Gestión de registros y poder social". En McKemmish, Sue, Piggott, Michael, Reed, Barbara, Upward, Frank (eds.): *Archivos: gestión de registros en sociedad*. Cartagena: Ayuntamiento: 3000 Informática, 2007.

## VI. Fase de análisis del proyecto

En cualquier caso, el proyecto que se describe en el presente texto se compone de dos fases genéricas, una de análisis, y otra de desarrollo —en pruebas, en preproducción y en producción—. Por lo que nos preocupa, en el marco del presente artículo, la fase de análisis se describe a continuación. La finalidad de esta fase es conocer con detalle los distintos sistemas de gestión y de gestión de la información existentes en la organización, así como las conexiones entre los mismos y con sistemas externos, desde una triple perspectiva, legal, técnica y archivística, con el objeto de dimensionar y configurar adecuadamente el sistema de gestión de documentos y archivo, y de establecer mecanismos correctos y seguros de conexión con aquellos otros sistemas y subsistemas.

Desde la perspectiva legal, la finalidad primaria es cumplir con los ya mencionados requisitos de archivo de la Ley 11/2007: integridad, autenticidad, confidencialidad, calidad, protección, conservación, identificación de los usuarios, control de accesos, protección de datos, y posibilidad de trasladar los datos a otros formatos y soportes. Para ello, y aunque constituye la herramienta primaria, no resulta suficiente el enfoque exclusivo sobre la Ley 11/2007, sino que deben tomarse en consideración, como mínimo, los siguientes instrumentos:

- la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información;
- el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica;
- el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos;
- la Ley 59/2003, de 19 de diciembre, de firma electrónica;
- la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; y

- el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento que desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Del análisis desde la perspectiva legal se esperaba, y se ha conseguido, obtener información suficiente acerca de los requisitos de confidencialidad, protección, identificación de los usuarios, control de accesos y protección de datos. Estos aspectos quedan documentados en el análisis preliminar y sirven para configurar los metadatos del sistema relativos a privilegios y restricciones de usuarios y roles, o a control de acceso a los registros y a los datos vinculados. De igual modo, sirven para elaborar un sistema de clasificación de seguridad conforme con buenas prácticas, como las establecidas en MoReq2, para proceder a la desclasificación de registros a medida que se cumplan plazos legales. Un aspecto fundamental que se deriva del análisis desde la perspectiva legal es la determinación de aquellos datos que tienen valor histórico, estadístico, científico y, en general, para la investigación; y aquellos otros que están sujetos con carácter general al régimen de protección de datos establecidos por ley. Esta determinación permite, por una parte, establecer las oportunas relaciones con la Agencia de Protección de Datos y, por otra, sentar las bases para el posterior desarrollo de un calendario de conservación.

Desde la perspectiva técnica, la finalidad primaria es conocer con detalle los componentes de hardware, software y comunicaciones en uso actualmente en los sistemas y subsistemas de gestión y de gestión de la información del Ayuntamiento, con el objeto de determinar su adecuación e idoneidad, su esperanza de vida, su capacidad para facilitar o inhibir la implantación del sistema, la necesidad de remodelar sus estructuras de datos, interfaces, conexiones, etc.; la necesidad de desarrollar mecanismos de conexión intermedios con el objeto de no obstruir el funcionamiento de sistemas en uso; o la necesidad de reemplazar y migrar sistemas abiertamente obsoletos. De igual modo, es una finalidad esencial verificar que se están respetando estándares consolidados, herramientas de software

libre y fuente abierta, e instrumentos que faciliten en general la interoperabilidad, y, en los puntos en los que así no suceda, analizar las posibilidades de modificar la situación o, al menos, de minimizar su potencial carácter inhibitorio.

Desde la perspectiva archivística, la finalidad primaria es conocer hasta qué punto en los sistemas y subsistemas en uso se encuentran ya insertos los controles y procesos que permiten satisfacer los requisitos establecidos por ley, y hasta qué punto debe procederse a su remodelación para insertar tales controles y procesos, de común acuerdo con los responsables del análisis desde la perspectiva técnica.

## VII. Conclusiones

En un entorno crecientemente digital, la percepción de que sea un documento de archivo tiene que cambiar radicalmente, de manera particular porque, como se dijo, el documento ya no existe, o ya no existe en el consolador estilo en el que existía en un entorno analógico. El documento es intangible y distribuido, de lo que se deriva que la evidencia que comporta también lo es. Es probable que la propia noción de evidencia cambie. No obstante, es misión del archivero el gestionar, mantener, conservar y poner a disposición documentos que constituyan evidencia de acciones, con independencia del soporte en el que tales documentos se inscriban. Para ser eficaz en este empeño, el archivero tiene que dejar de pensar en el documento y comenzar a pensar en su intangibilidad y su dispersión; en los sistemas que lo crean y contienen; en las nuevas reglas de construcción del mismo. Adoptando esta perspectiva liberadora, somos de la opinión de que el diseño de nuestros propios sistemas también experimentará una liberación que, lejos de equivaler a una renuncia de nuestros convencionales controles y procesos archivísticos, contribuirá a una integración reforzada de los mismos en un mundo que, por definición, se escapa de las manos; en un País de Nunca Jamás en el que no podremos acomodarnos, pero en el que conoceremos una existencia enriquecida y despojada de nuestros tradicionales lechos de Procusto. A nuestro juicio, cualquier otro planteamiento de nuestro futuro profesional está condenado al fracaso y a la extinción.



# Índice

Presentación.....	5
La autenticidad del documento electrónico en los ámbitos jurídico y diplomático	
I. Introducción.....	11
II. ¿Qué es la autenticidad?.....	12
III. El acto administrativo.....	13
III. 1 El acto jurídico administrativo y la autenticidad.....	14
III. 2 La formación del e-expediente en la administración pública: su autenticidad.....	18
IV. El documento electrónico de archivo.....	20
A. Reconocimiento jurídico.....	21
B. La determinación de la autenticidad por la diplomática.....	24
V. La autenticidad elemento jurídico fundamental.....	28
VI. Confluencia de la autenticidad jurídica y diplomática en el documento electrónico de archivo.....	31
VI. 1 Comprobación de la autenticidad.....	32
VI.2 Comprobación de la autenticidad por InterPARES.....	34
VII. Conclusiones.....	35



El documento electrónico en la e-administración: análisis de caso	
I. Introducción.....	39
II. La gestión de documentos electrónicos frente a la modernización de la administración pública.....	41
III. La Administración electrónica y la gestión documental.....	43
IV. La Gestión de documentos electrónicos en Bogotá: relación con el programa de gobierno en línea (e-Gobierno).....	50
V. Avances logrados en la adaptación de la gestión de documentos al gobierno electrónico en Bogotá.....	54
VI. Recomendaciones para integrar la gestión de documentos electrónicos en la administración electrónica.....	61

## Transfiriendo documentos electrónicos auténticos hacia un repositorio digital seguro: el caso catalán (la plataforma IARXIU)

I. Sumario.....	67
II. El contexto.....	67
III. La transferencia: concepto y definición.....	68
IV. Directrices, pautas y recomendaciones sobre transferencia: fuentes y referentes metodológicos	
a) Normas y estándares internacionales y nacionales.....	71
b) El Proyecto Internacional InterPARES.....	75
V. El procedimiento de transferencia.....	85
VI. Los metadatos asociados al procedimiento de transferencia.....	86
VII. Primeras conclusiones.....	90
VIII. El archivo electrónico, reto o necesidad.....	91
IX. Definición y objetivos del servicio.....	93
X. Conceptos básicos.....	96
XI. Modelo funcional del servicio.....	98

XI.1 Módulo de transferencia e ingreso.....	100
XI.2 Módulo de archivo: gestión del repositorio.....	104
XI.3 Módulo de preservación.....	105
XI.3.1 Herramientas de análisis y registro de formatos.....	109
XI.4 Módulo de administración.....	111
XI.5 Módulo de acceso.....	111
XII. Modalidades de uso y de prestación de servicio.....	113
XIII. Segundas conclusiones y futuro.....	115

## La valoración documental.

### De los archivos en papel a los archivos digitales

I. Resumen.....	119
II. Teorías sobre la valoración.....	119
III. Modelo de la Cadena de Preservación	
Valorar los documentos de archivo para su preservación permanente.....	135
IV. Lineamientos para valoración de documentos	
de archivo para preservación permanente.....	136
V. Monitoreo de los documentos de archivo que han sido	
identificados para su preservación en el largo plazo.....	139
VI. A manera de conclusión.....	141

### La cadena de preservación en archivos digitales

I. Introducción.....	145
II. La problemática de la preservación documental digital.....	149
III. Los seis factores de la preservación digital.....	152
IV. Iniciativas y modelos.....	155
V. La “Cadena de Preservación” .....	159

VI. Conclusiones.....	166
El archivero electrónico en el país de nunca jamás	
I. Introducción.....	171
II. Las necesidades derivadas del nuevo marco legislativo.....	171
III. El entorno de producción de documentos electrónicos en el Ayuntamiento de Cartagena.....	173
III.1 La gestión de documentos en el Ayuntamiento de Cartagena.....	177
IV. Alcance del proyecto.....	180
IV.1 Una solución propuesta.....	182
IV.2 La descripción archivística.....	182
IV.3 Los usuarios del sistema.....	185
IV.4 La conservación de los documentos.....	188
IV.5 El acceso a los documentos.....	192
V. Otras funcionalidades.....	194
VI. Fase de análisis del proyecto.....	195
VII. Conclusiones.....	197
Índice.....	199



*Archivos Electrónicos. Textos y Contextos*  
se terminó de imprimir el 30 de marzo de 2011.  
Impreso en Editorial Siete Días.  
Cerrada Porfirio Díaz no. 28 La Joya, Puebla. Pue.  
El tiraje fue de mil ejemplares,  
impreso en papel couché de 115 gr.  
encuadernación rústica.

En el entorno de los países hispanoparlantes los temas sobre archivos electrónicos o digitales aún causan inquietud e incertidumbre, inclusive hasta resistencia por parte de archivistas y otros profesionales que tienen bajo su responsabilidad coordinar e instrumentar procesos para la organización y conservación de archivos.

Ante ello y con el propósito de abordar desde diferentes perspectivas aspectos relacionados con los archivos electrónicos o digitales, es que se presentan los textos que integran el número VII de Formación Archivística *Archivos Electrónicos. Textos y Contextos* coordinado por Alicia Barnard, especialista mexicana en el tema. Todos los autores, latinoamericanos y de España, por primera vez en México nos ofrecen sus experiencias y conocimientos sobre este tema.

Aida Luz Mendoza, reconocida investigadora de archivos del Perú; Juan Voutssás, investigador del CUIB de la UNAM; Ramón Nualart, responsable del servicio iArxiu de Cataluña y Miquel Serra, archivista de la Universidad de Girona; Carlos Alberto Zapata, investigador de la Universidad de la Salle en Colombia, y Alicia Barnard, participante del TEAM del Proyecto InterPARES en México -al igual que los demás en sus respectivos países- son los autores de los textos en los cuales el lector podrá apreciar principios teóricos y prácticos acerca de este tema tan actual.

Es así como la Benemérita Universidad Autónoma de Puebla, a través de su Archivo Universitario en colaboración con la Red Nacional de Archivos de Instituciones de Educación Superior, contribuye al desarrollo de la cultura archivística en nuestro país.

Esperamos que “*Archivos Electrónicos. Textos y Contextos*” no sea la única publicación sobre el tema sino que sirva de arranque a otras más.

---

Renales

