Preservando documentos digitales auténticos

Raquel Umaña Alpízar
raquel.umana@ucr.ac.cr
Universidad de Costa Rica
Tel: 2511-6453

Eje temático

Patrimonio documental: Conservación y preservación

Resumen

La preservación digital supone una serie de retos y desafíos, debido principalmente a la obsolescencia tecnológica por lo que es necesario un trabajo constante con el fin de garantizar los requisitos indispensables para la conservación y consulta de los documentos digitales. Es por esta razón que a nivel internacional se han desarrollado principios, directrices, normas y hasta modelos para la preservación digital como lo es el Modelo OAIS.

Debido a las características propias del documento digital, la preservación digital debe incluir un componente dedicado a la tarea de garantizar la autenticidad e integridad de los documentos, ya que tanto la gestión de los documentos electrónicos, como la conservación, y la migración de información, pueden implicar algún grado de pérdida o alteración del documento como tal.

Esta labor de aseguramiento supone un trabajo interdisciplinario que debe contar con un plan de actuación en el que se asegure la sostenibilidad económica, la idoneidad del recurso humano, un estricto control de los formatos, auditorías de evaluación de riesgos y una política de preservación, seguridad y continuidad digital.

Palabras claves:

Preservación digital, documentos electrónicos, autenticidad, archivo digital, repositorios digitales.

I. Introducción

El tiempo en que vivimos está fuertemente marcado por los avances científicos y tecnológicos, por la demanda del acceso a la información y por la producción masiva de esa información, sobre todo en nuevos y retadores formatos.

Así como el progreso que experimentamos en la actualidad se debe a la disponibilidad del conocimiento obtenido en siglos anteriores, la información que producimos hoy será el combustible que haga posible las revoluciones y los cambios del mañana.

La sociedad está a los albores de una revolución en el uso de la información, propulsada por la utilización de la tecnología, pero que abarca todos los ámbitos del quehacer humano sometiéndonos a constantes cambios económicos, políticos, sociales y culturales por lo que vivimos en una sociedad que ha recibido calificativos como "*sociedad de la información*" y "*sociedad del conocimiento*".

En esta sociedad, la eficiencia de los procesos productivos y de servicios, la eficacia en la gestión de los recursos, sean estos públicos o privados y la competitividad, tanto en el ámbito empresarial como estatal, están fundamentados en el acceso y la oportuna utilización de la información para la toma de decisiones.

El rol de los archivos en el siglo XXI no dista mucho entonces de lo que hasta ahora ha demandado esta "*sociedad del conocimiento*", excepto por la ineludible obligación de asumir la custodia y preservación de los documentos que se generan en los nuevos soportes digitales y que cada vez más dominarán el ámbito de la producción de los documentos.

II. Objetivos

- Brindar un acercamiento a los aspectos que implica el preservar documentos digitales para que sean auténticos, íntegros y accesibles.

- Concientizar a las instituciones para que cuenten con Archivos Digitales, con el fin de garantizar el acceso y la preservación de los documentos a través del tiempo.

III. Marco teórico-conceptual

3.1 Gestión de documentos

La Gestión de Documentos y los archivos han recorrido un largo camino desde Schellenberg a la familia ISO 30300, evolucionando para adaptarse a las necesidades de la sociedad que consume sus servicios. Este proceso de maduración busca la eficiencia, la eficacia y la calidad, mediante un trabajo interdisciplinario que permita simplificar la producción de los documentos, evitando la creación masiva e indiscriminada o la confección de documentos inútiles y aplicando una serie de procesos archivísticos, para facilitar y recuperar la información toda vez que sea necesario.

La "Gestión de Documentos", *como el área de la gestión administrativa general relativa a conseguir economía y eficacia en la creación, mantenimiento, uso y disposición de los documentos,* será entonces la que lleve el peso de ser garante de la información que el archivo tendrá en custodia.

Sin embargo, la incorporación de todas esas características y el entorno tecnológico que las facilita también conlleva retos y trabajo, la salvaguarda de la información de manera auténtica, íntegra y segura a través del tiempo implica la incorporación de técnicas y mecanismos específicos que pueden resolver el problema, pero la información y la solución misma comparten un obstáculo que debe vencerse, la obsolescencia tecnológica.

Pero ¿Cómo asumir el reto de los nuevos soportes electrónicos y a la vez garantizar las características de seguridad, autenticidad e integridad de los documentos a través del tiempo?.

3.2 Documentos tradicionales vs digitales

El documento de archivo es el vehículo por excelencia para la prueba de un hecho, así como en la diplomática están definidas las características necesarias para garantizar su valor como evidencia en los soportes tradicionales, la legislación vigente de cada país establece las características necesarias para que un documento digital revista también de carácter probatorio.

A diferencia de los documentos tradicionales en soporte papel, los documentos digitales requieren un medio electrónico de combinaciones de unos y ceros contenidos en un medio inaccesible por los sentidos, por esta razón se necesita de una combinación de tecnología especializada (hardware y software) para ser entendidos.

> La Diplomática es una ciencia antigua, que se ve fortalecida en el siglo XVI al darse un abuso de falsificaciones con los consiguientes reclamos políticos o religiosos, presentándose controversias, sin embargo, cuando los estudios comenzaron a mirar los documentos como evidencias históricas, la diplomática y la paleografía adquirieron un carácter científico y objetivo utilizado para analizar los documentos archivísticos con el fin de determinar sus caracteres internos y externos, establecer su tipología y determinar la autenticidad de los documentos (Duranti, L., 1996, pág. 25).

La diplomática estudia la forma y estructura de los documentos, su autenticidad y su valor probatorio, para ello establece una serie de caracteres internos y externos.

Caracteres internos:

a) Elementos que comunican aspectos del contexto jurídico y administrativo: autor, destinatario (Protocolo)
b) Elementos que comunican la acción misma o asunto (contenido, motivación)
c) Elementos que comunican el contexto documental: Fecha (data tópica y cronológica), Validación (firma y sello). (Escatocolo)

Caracteres externos: Soporte, Clase, Tipología, Formato, Forma, Cantidad y Signos Especiales.

Los documentos de archivo son producto de las funciones de una institución, son instrumentos fehacientes, evidencias que dan testimonio, engendran derechos y obligaciones, es decir, tiene valor probatorio; por lo que una de las características más importante es la autenticidad de un documento, garantizar que es creado por la persona que afirma haberlo hecho, y que es íntegro, demostrar que no ha sido alterado.

Luciana Duranti señala que un documento es la representación de un hecho fijado a un soporte. De manera similar, en un entorno electrónico, la cadena de bits no puede perdurar durante ningún período de tiempo a menos que se fije a un soporte. Que el almacenamiento de una cadena de bits perdure, no es suficiente para conservar un documento. Asimismo, Duranti indica que el Grupo de Trabajo sobre Autenticidad observó que "estrictamente hablando, no es posible conservar un documento electrónico" (2005, pág. 35).

Es por esta razón que los documentos electrónicos no se pueden confinar en discos compactos ni en una computadora local, si no que deben almacenarse en un ambiente controlado, que le permita estar en constante revisión (análisis de características y funcionalidades) para asegurar que el formato en el que se ha ordenado la información conserva su capacidad para reproducir el documento y que la información es íntegra.

Como lo indica Jordi Serra, hay una clara separación entre el contenido que se debe conservar, la codificación que lo soporta (formatos informáticos) y el soporte físico en el que está almacenado, la *codificación* y el *soporte* pueden cambiar en el tiempo, mientras que el contenido debe ser inalterable, pero el *formato* y el *soporte de almacenamiento* también juegan un papel importante, porque pueden reforzar o debilitar el carácter auténtico del documento.

Esto se debe a que el formato define las características de presentación de un documento, según Voutssas y Barnard, el *formato* es la estructura y/o distribución de una entidad, y el *formato de archivo* (de cómputo) es la organización de los datos dentro de los objetos digitales, usualmente diseñada para facilitar el almacenamiento, recuperación, procesamiento, presentación y/o transmisión de esos datos por medio de algún programa [Informática]. No debe confundirse esta definición, que habla de "archivo" desde el punto de vista informático, con los archivos desde la archivística. (2014, págs. 173-121).

De acuerdo con la publicación "*Un marco de referencia para la preservación digital*" todo documento de archivo digital está conformado por uno o varios componentes digitales. Son objetos que pueden formar parte de uno o más documentos de archivo e incluyen a los metadatos necesarios para ordenar, estructurar o manifestar su contenido; y requieren de cierta acción de preservación. Por ejemplo, un correo electrónico que incluye una imagen y una firma digital tiene, al menos, cuatro compontes digitales: el encabezado, el texto en sí, la imagen y la firma digital. (2017, pág. 44).

3.3 Autenticidad de los documentos

Con el fin de asegurar el valor probatorio de los documentos digitales, para la ejecución de las actividades de la organización y la protección de los derechos de los ciudadanos, se deben producir y custodiar documentos que reúnan las características definidas en la Norma ISO 30300, a saber:

Autenticidad	Fiabilidad	Integridad
"Un documento auténtico es aquel del que se puede probar: a) que es lo que afirma ser; b) que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado; y c) que ha sido creado o enviado en el momento en que se afirma."	"Un documento fiable es aquél cuyo contenido puede ser considerado una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores operaciones o actividades."	"La integridad de un documento hace referencia a su carácter completo e inalterado.

Como lo indica Luciana Duranti "los documentos creados y mantenidos en forma electrónica están constantemente en riesgo de alteración inadvertida o intencionada, y tal alteración puede no ser rápidamente perceptible. La autenticidad de los documentos electrónicos se ve amenazada cada vez que los documentos se transmiten por el espacio… los requisitos para ponderar y mantener la autenticidad de los documentos electrónicos que se conservan a largo plazo son necesarios, por tanto, para apoyar la presunción de que un documento electrónico es, de hecho, y continuará siendo, lo que pretende ser, y que no ha sido modificado ni corrompido en aspectos esenciales." (2005, pág. 27).

A su vez Duranti define la "*forma documental*" como las reglas de representación de acuerdo con las cuales se comunican el contenido de un documento, su contexto administrativo y documental inmediato, y su autoridad. (2005, pág. 33).

Uno de los *caracteres internos* que analiza la diplomática para determinar la autenticidad y el valor probatorio de los documentos es la *validación* por medio de las firmas y sellos. Recíprocamente el estándar de aseguramiento de los documentos en soporte digital es la firma digital avanzada, un proceso criptográfico que permite determinar la autenticidad e integridad de un documento en formato digital, y que se realiza mediante una infraestructura de

certificados digitales con llaves públicas y privadas guardadas en un contenedor conocido como "*Certificado Digital*" y que debe provenir de una entidad certificadora autorizada.

En Costa Rica, con el objetivo de agilizar los trámites públicos y potenciar la interoperabilidad entre instituciones, en el año 2005 se publica la Ley No. 8454 denominada Ley de Firmas, Certificados Digitales y Documentos Electrónicos con el fin de equiparar la validez de una firma manuscrita con una digital.

Esta ley define firma digital como "*cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico." (pág. 7)*

Asimismo, en el año 2013 se publica la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente del MICITT, la cual establece los formatos oficiales para la firma digital, a saber: CAdES, XAdES y PAdES.

Cabe destacar que a partir de la adopción de las tecnologías de información y evidentemente del respaldo normativo, las instituciones han empezado a implementar sistemas informáticos, para gestionar sus documentos y/o brindar servicios en línea. Los que al menos han dado ese paso, deberían tener claro que no basta con eso, es necesario implementar mecanismos de preservación de documentos a largo plazo, contar con estrategias de preservación y un repositorio diseñado para este fin específico.

En este sentido, también es importante señalar la diferencia entre los repositorios digitales que se han desarrollado para administrar información en línea, en plataformas de código abierto, pero que no aplican estrategias ni mecanismos de preservación, ni aplican un modelo estandarizado de ingesta, transformación y difusión de los objetos digitales en custodia.

3.4 Acceso y estrategias de Gobierno abierto

La Constitución Política de Costa Rica en su artículo 30, garantiza el libre acceso a la información sobre asuntos de interés público, la misma Carta Magna costarricense, garantiza el derecho a la intimidad, a la libertad y al

secreto de las comunicaciones, una iniciativa que se plasma con claridad mediante la Ley 8968 la protección de los datos personales.

En el año 2012 Costa Rica se incorporó a la iniciativa multilateral Alianza para el Gobierno Abierto (Open Government Partnership), la cual busca promover en los países miembros, un estilo de gobernanza basado en la transparencia, la participación ciudadana y el trabajo colaborativo interinstitucional y ciudadano.

Mediante el Decreto Ejecutivo número 39372-MP-MC del 7 diciembre de 2015, el Poder Ejecutivo declaró de interés público la Estrategia Nacional por un Gobierno Abierto. Asimismo, se unió a la Red de Transparencia y Acceso a la Información Pública (RTA), que es una red de intercambio entre organismos y/o entidades públicas que desarrollan supervisión en funciones en Transparencia y el Derecho de Acceso a la Información Pública en la región.

En el punto 2.4. Preservación digital, del Modelo Directrices G07/D02/O se indica que “Los documentos electrónicos deben conservarse, al igual que los documentos analógicos, como la evidencia de actos, a efectos de responsabilidad y memoria, manteniendo sus propiedades de autenticidad, fiabilidad, integridad y disponibilidad. Esta conservación debe implicar a especialistas en tecnologías de la información, gestores de documentos y archiveros.” Asimismo, menciona que “Si existen herramientas automatizadas, se debe considerar la opción de la migración de la información como una opción para abordar la obsolescencia de la tecnología, mediante la transferencia entre plataformas tecnológicas.”

Finalmente indica que “De igual manera que la preservación analógica, la preservación digital debe contemplar un plan que incluya: actores involucrados, objeto de protección y medidas implantadas, análisis de los riesgos y medidas preventivas.” (RTA, Modelo Directrices. Custodia y control de las instalaciones. Modelo de Gestión de Documentos y Administración de Archivos, pág. 16). Estos aspectos son elementales para lograr un Gobierno Abierto.

3.5 Preservación digital

La preservación digital es el conjunto de acciones estratégicas y concretas, destinadas a mantener la capacidad de presentar los elementos esenciales de objetos digitales auténticos y asegurar su acceso a mediano y largo plazo.

Juan Voutssas y Alicia Barnard en su Glosario de Preservación Archivística Digital definen "*Preservación digital*" como el proceso específico para mantener los materiales digitales durante y a través de las diferentes generaciones de la tecnología a lo largo del tiempo, con independencia de los soportes donde residan y "*Preservación de documentos de archivo*" como el conjunto de principios, políticas, reglas y estrategias que rigen la estabilización física y tecnológica así como la protección del contenido intelectual de documentos de archivo adquiridos, con objeto de lograr en ellos una secuencia de preservación continuada, inquebrantada, sin un final previsto. (2014, págs. 173-174).

Quizá la iniciativa más conocida sea el Modelo Open Archive Information System (OAIS), un modelo de referencia y conceptual para la creación de un Archivo para objetos digitales, nace como una iniciativa de la National Aeronautics and Space Administration (NASA) para crear un sistema de transferencia de datos e información espaciales. En el año 2003, el modelo se transforma en la Norma ISO: 14721 Space Data and Information Transfer Systems (OAIS).

OAIS se caracteriza por un entorno tridimensional compuesto por el productor de información, la dirección y el usuario; como eje central está el Archivo OAIS. Establece tres paquetes (contenedores) de información: Paquete de Transferencia de Información (*Submission Information Package* **SIP**), Paquete de Información de Archivo (*Archival Information Package* **AIP**) y el Paquete de Difusión de la Información (*Dissemination Information Package* **DIP**). El modelo funcional se detalla a continuación:

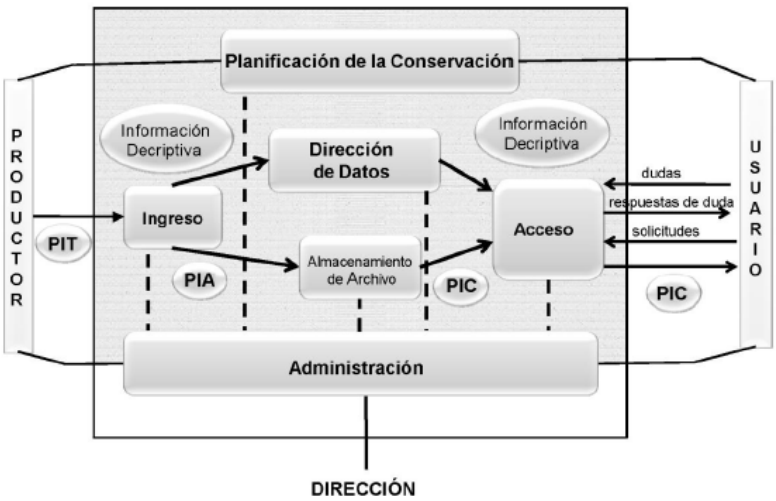

Imagen No. 1: Entidades Funcionales de OAIS. Tomado de la Norma ISO 14721:2015, pág. 41.

3.6 Metadatos

En el tema de la preservación de los documentos un aspecto fundamental es el empleo de metadatos, ya que es necesario garantizar su disponibilidad e integridad, manteniendo de manera permanente las relaciones entre el documento y su información contextual.

El modelo de referencia OAIS fue el adoptado por la OCLC y la RLG para definir los tipos de información que se deberían asociar a un objeto digital a efectos de preservación y que es el origen del PREMIS Data Dictionary. Este diccionario de datos implementa el modelo OAIS con unidades semánticas, bajo la forma de un esquema de metadatos específicos para preservación, que utiliza un repositorio para soportar el proceso de preservación digital, con entidades intelectuales, objetos, agentes, derechos y acontecimientos.

Por otra parte, METS es un esquema estándar para codificación y transmisión de metadatos. Está pensado principalmente para el envío de los ficheros, imágenes y objetos multimedia de o hacia un archivo digital. METS utiliza una estructura de etiquetas tipo XML, y está compuesto por 7 secciones principales (no todas deben implementarse de forma obligatoria).

3.7 Proyectos de preservación digital

3.7.1 Iniciativas internacionales

El Proyecto Internacional para la Investigación en Documentos de Archivo Auténticos y Permanentes en Sistemas Electrónicos (InterPares), es uno de los proyectos principales a nivel internacional. Está constituido de 4 etapas, la última es InterPARES-Trust, que se enfoca en los factores introducidos por la gestión de documentos de archivo y datos en-línea con el proyecto DAN.

Para este año 2017, el Consejo Internacional de Archivos y el Proyecto InterPARES, en con junto con el Archivo General de la Nación de México publican la serie “Temas fundamentales de preservación digital”, con el propósito de dar mayor difusión a los proyectos de preservación y dar confianza a los usuarios acerca de la autenticidad de los documentos en soporte digital.

Muchos de los estudios en el tema de la preservación digital son resultado de las diferentes experiencias en la implementación de sistemas elaborados específicamente para este fin. Asimismo, han surgido nuevos proyectos y diseño de sistemas que incluyen funcionalidades de preservación, a modo meramente ilustrativo se pueden mencionar algunas de las iniciativas internacionales que se han realizado, a saber: Archivemática, ERA (Electronic Records Archives), FEDORA (Flexibile Extensible Digital Object Repository Architecture), iARXIU, RODA (Repository of Authentic Digital Objects), entre otros.

Al mismo tiempo, se han desarrollado herramientas, programas o aplicaciones de conversión de formatos de fichero, servicios para la firma y sellado de tiempo que comprueban la integridad de los documentos, otros que brindan servicios de reconocimiento de formatos y extracción de metadatos y propiedades significativas como DROID, JSTOR, FIDO, FITS, LOCKSS, o proyectos como SPIRT, PLANETS, Plato o InSPECT que buscan soluciones al tema de la preservación digital con servicios para el análisis de los elementos o características esenciales (propiedades significativas) para la conservación de un objeto digital.

3.7.2 Iniciativas nacionales

Uno de los primeros intentos para desarrollar un Archivo Digital se dio en la Universidad de Costa Rica, cuando el Archivo Universitario Rafael Obregón Loria (AUROL), junto con la Sección de Archivística de la Escuela de Historia, en el año 2013 realizaron un proyecto basado en el modelo OAIS con la asesoría del Máster Jordi Serra Serra, profesor de la Facultad de Biblioteconomía y Documentación de la Universidad de Barcelona, miembro del grupo de investigación PRESERVA y reconocido consultor internacional en esta materia.

Sin embargo, la administración universitaria de ese momento no apoyó el proyecto, ni la iniciativa, por lo que el producto sólo ha podido ser utilizado como material de referencia en la parte académica, a través del curso de Licenciatura “Seminario de Temas Archivísticos” que imparte la Sección de Archivística, gracias a esta labor de difusión del conocimiento el modelo se ha empezado a utilizar como insumo en otras instituciones, de las cuales destaca la iniciativa del repositorio digital del Archivo Nacional de Costa Rica, debido al impacto que esta institución tiene a nivel nacional y la trascendencia de un proyecto de tal envergadura.

IV- Metodología

El presente trabajo se fundamenta en el paradigma cualitativo, puesto que las variables utilizadas en el estudio son de naturaleza meramente descriptiva, se busca el análisis y reflexión a partir de la información obtenida y se pretende señalar las características y requisitos imprescindibles para que los documentos sean auténticos a través del tiempo.

Es de tipo exploratorio, ya que busca la identificación de elementos, pautas y acciones estratégicas que garanticen la adecuada preservación de los documentos digitales.

Para ello, parte esencialmente del análisis y estudio de la bibliografía existente, se analizan textos relacionados con la preservación digital y la autenticidad de los documentos con el fin de obtener sus datos, y brindar una reflexión crítica sobre los conceptos planteados.

V- Análisis de resultados

La constante evolución de la tecnología hace necesario que se evalúen de forma constante las amenazas, los riesgos y las vulnerabilidades de la arquitectura informática, con el fin de establecer mecanismos de seguridad, para la protección de la información custodiada.

El principal reto que enfrenta la preservación digital es la obsolescencia tecnológica, sin dejar de lado el deterioro del soporte de almacenamiento, para mitigar la segunda es necesario evitar el uso de soportes de almacenamiento “en frío” o desconectados, como lo son las unidades removibles o los discos ópticos, en el caso del principal reto, se debe hacer migraciones del objeto digital por medio de una transformación controlada, para que los usuarios puedan utilizar la información independientemente del constante cambio de la tecnología, considerando las propiedades del objeto digital, contenido, contexto, funcionamiento, estructura y apariencia, estableciendo las propiedades significativas que pudieran cambiar y la tolerancia al cambio entre los distintos procesos de conversión.

La seguridad informática debe velar por garantizar que los documentos sean legítimos a través del tiempo, Voutssas establece que “la permanencia depende del almacenamiento permanente seguro. Para asegurar este

almacenamiento de objetos digitales, –en este caso documentos de archivo– se requiere de estrategias, procedimientos y técnicas adecuadas para crear, operar y mantener archivos documentales a largo plazo. Tales estrategias deben permitir preservar la cadena de bits y sus formatos. Por lo mismo se deben diseñar y llevar a cabo meticulosamente esas técnicas y procedimientos para la conservación tanto de los soportes documentales como de sus contenidos digitales: la información del documento en sí misma y los metadatos asociados a él. La preservación del soporte, la cadena de bits, su estructura y su formato nos da la permanencia." (2010, pág. 133)

Como parte de las acciones de preservación del Archivo Digital se debe hacer mención a las funcionalidades que le permita la conversión de formatos de fichero, el reconocimiento de formatos y la extracción de sus propiedades significativas, añadir la firma digital avanzada y sellado de tiempo de documentos y el empleo de contenedores XML. En el proceso de conversión de formatos se debe garantizar que el contenido sea una representación completa del documento, asimismo, en todo momento es necesario que el documento esté protegido contra modificaciones no autorizadas.

No obstante, aunque se apliquen normas de seguridad que garanticen autenticidad e integridad hoy en día, estas normas no permanecerán inmutables ni vigentes por mucho tiempo antes de ser víctimas del mismo avance que las creó. La información misma, su contenido y sobre todo su formato y almacenamiento resultan especialmente vulnerables al paso del tiempo, que en las soluciones tecnológicas parece llevar un ritmo sustancialmente más acelerado que nuestro propio concepto del tiempo.

Para enfrentar este problema debemos dejar de ver el documento digital como un objeto acabado ya que debe evolucionar y cambiar con el tiempo, pero siempre en un marco de trabajo que de garantía de su autenticidad, integridad y seguridad y que permita conocer los atributos de seguridad originales, incluso a pesar de que éstos hayan sido superados por los procesos de transformación.

La mejor protección de la autenticidad se obtiene con medidas que garanticen la integridad de los datos y con documentos que conserven claramente la identidad de los objetos, por lo que las estrategias de preservación de documentos deben especificar qué adiciones o anotaciones autorizadas pueden realizarse en un documento, las cuales deben indicarse de forma explícita y dejar pistas de auditoría.

Incluso en el evento de una transformación masiva, siempre debe existir un mecanismo que permita retornar al objeto original para su verificación y otro que permita extraer la información de seguridad para consignarla en el valor de preservación del diccionario elegido, como ejemplo, suponiendo la migración de un documento digital de un formato descontinuado pero que incluía una firma digital a un formato sustituto de validez, aun cuando todos sus aspectos de forma se encuentren garantizados, el contenedor "AIP" debería conservar la forma original del documento y el diccionario de metadatos de preservación, supongamos que se trata de PREMIS debería contener un elemento con los datos de validación de la firma original, de manera que se pueda seguir conociendo la identidad del firmante original, la cadena de certificación, la validez del certificado firmante, el sello de tiempo, etc.

Las acciones de preservación pueden implicar modificaciones de los recursos originales o cambios en su modo de reproducción, pero éstas de ninguna manera deberían modificar el contenido de la información ni las condiciones de acceso. Por lo que se deben generar metadatos de evento, notificaciones, anotaciones en un registro de incidencias, y disponer de un sistema de seguridad y de un servicio de verificación de identidades (validación de firma y certificados electrónicos), así como de procesos automáticos de protección y resello para los objetos resultantes. Los metadatos pueden ayudar a soportar la autenticidad del recurso mediante la documentación de la procedencia digital de dicho recurso, su cadena de custodia y el historial de cambios autorizados.

Asimismo, para el ingreso de los documentos propiamente al Archivo Digital se deben establecer los formatos de fichero admitidos para el contenido, especificar los metadatos que deben coleccionarse y su estructura y la forma de recepción para el contenedor de información de ingreso (SIP). Deben existir mecanismos de control para verificar la exhaustividad de la captura automática, y validaciones de condiciones de seguridad e idoneidad, una de las validaciones debe ser la verificación de la firma del productor del documento y otro podría ser la revisión de un anti-virus.

Durante la creación del AIP por parte del Archivo Digital se ejecutan las acciones de normalización de formatos, existen procesos que incluyen la generación de metadatos del evento y se lleva a cabo la firma digital del archivo de contenedor, con la anotación de ingreso y notificación de resultado al productor o instancia que realiza la transferencia.

Solamente se deben aplicar modificaciones a cualquier representación tecnológica, únicamente con la finalidad de asegurar su acceso a lo largo del tiempo, siempre que se mantengan los valores y la significación de la entidad documental representada. Para ello, se deben establecer las propiedades significativas que podrán resultar modificadas. El órgano productor recibirá una notificación de afectación por obsolescencia cuando se inicie el proceso de migración y en una segunda notificación, los resultados cuando finalice el proceso.

En relación con el acceso, los usuarios accederán al archivo con la capacidad para realizar búsquedas y obtener copias de documentos, a través de los canales y con los medios de autentificación necesarios, para este propósito se puede establecer el uso de reprografías certificadas. Las reprografías descargadas como resultado de una consulta tendrán carácter de copia auténtica, se puede facilitar acceso entre sistemas en forma de contenedor de difusión de información (DIP), mediante un acuerdo previo que defina la estructura y formatos establecidos.

Como parte del proceso el Archivo Digital debe existir un protocolo que defina los derechos para realizar acciones de preservación sobre los documentos durante y después del ingreso, las notificaciones a la instancia cualquier cambio realizado en el contendor de información de archivo (AIP).

El *protocolo de ingreso y custodia* surge como herramienta de apoyo ante los problemas identificados en las experiencias de archivos digitales, en los cuales se analiza el aseguramiento que los registros y datos producidos por la organización; de tal manera que sean efectivas y periódicas al Archivo Digital en un contexto más adecuado para la Gobernanza que a la preservación digital pura y dura". (Serra-Serra, 2014, p. 5)

Una firma digital avanzada de alta longevidad, permite garantizar que los datos de autenticidad estarán disponibles en el futuro y que no se requiere de un tercero de confianza para validar la autenticidad del documento protegido, sino que se puede obtener la validación a partir de la información consignada en los componentes de la firma.

Esta información contiene elementos valiosos como por ejemplo la cadena de certificación, es decir la cadena de autoridad de los emisores que validan el certificado firmante, lo cual permite establecer la pertenencia y el valor de este último, también se incluye la información de la lista de revocación de certificados al momento de realizarse

la firma o al momento inmediato después de ésta, lo que nos da garantía de la validez del firmante en el momento en que se realizó la firma digital.

De los tres tipos de firma digital avanzada que existen, el más versátil es el estándar de XAdES que permite al mismo tiempo consignar y proteger metadatos correspondientes al activo de información protegido, así como el fichero mismo, y a su vez auto contener la información de validación, de manera que es fácilmente identificable su estado a partir del documento mismo.

El estándar de PAdES tiene la ventaja de estar altamente especializado para satisfacer las necesidades de autenticación, integridad y verificación de documentos de tipo textual, que constituyen el mayor porcentaje de la información en custodia de las organizaciones, cabe destacar que un documento protegido por PAdES puede estar a su vez contenido dentro de una estructura protegida por XAdES, como en el caso de una implementación típica del estándar METS, lo que proporciona un mayor nivel de aseguramiento y a su vez permite el acceso a funciones de mantenimiento sobre la preservación de la autenticidad, como son las funciones de resellado del estándar XAdES tipo A.

En cuanto al estándar CAdES su principal fortaleza consiste en su habilidad de no estar limitado a un tipo de archivo o de representación específicas, como sí sucede con PAdES que es exclusivo para el uso de ficheros en formato pdf o con XAdES que requiere que el archivo que se contenga dentro de él se exprese en forma de una cadena base 64, sin embargo, esta fortaleza también tiene un precio porque la firma digital es alojada en un fichero independiente almacenado sin una relación atómica con el fichero a partir del cual se obtuvo, lo que da como resultado la paradoja de tener que garantizar la autenticidad de dos archivos para dar garantía de uno de ellos.

Con todas las características señaladas es evidente que la firma digital se perfila como la herramienta más valiosa para garantizar la autenticidad de un documento en soporte digital. Sin embargo, existen escenarios en los que la aplicación de la firma digital es excesiva, o es un proceso demasiado largo y complejo que obliga a integrar métodos asincrónicos, o bien es simplemente imposible y obliga al uso de contenedores de información o del empleo de la firma digital como un elemento separado del objeto digital que deseamos asegurar, como ocurre con la firma de tipo CAdES.

Para ciertos propósitos una forma sencilla de firma digital podría ser más beneficiosa que una firma avanzada, por ejemplo, para garantizar la autenticidad de cada tupla en una tabla de registros, incluso podría optarse por otros mecanismos de criptografía para lograr el objetivo con mayor rapidez, siempre hay escenarios en los que el tiempo de respuesta es esencial y no se puede contar con el lapso requerido para acceder a servicios de terceros, como los servicios de TSA que se deben consumir para componer una firma digital avanzada, tal es el caso de las solicitudes de validación en la operación de las tarjetas de crédito, el intercambio de información para el pago de servicios externos, etc.

También existen en definitiva formatos de ficheros que es imposible firmar, a menos que se emplee CAdES, como es el caso de los ficheros audio visuales, sean estos fotografía estática o imágenes, audio o video, tres clases documentales que tienen cada vez más representación dentro de los documentos de archivo.

Otra consideración que se construye alrededor de la seguridad es la disponibilidad y continuidad del servicio, para lograr esto se debe mantener una redundancia completa, y copias con periodicidad incremental, en una ubicación externa. Hace pocos años era impensable la tecnología que permite tener los documentos en la nube, sin embargo, hoy en día es una estrategia que muchas instituciones han elegido, principalmente por las características de seguridad, precio y redundancia, al contar con sitio alternos en diferentes partes del mundo.

Debe considerarse que la capacidad y el tipo de los dispositivos de almacenamiento dependen de dos factores, el volumen de los datos y la cantidad de consultas, por lo que la infraestructura debe ajustarse a las necesidades de almacenamiento y de procesamiento de cada organización.

La evolución de la tecnología se percibe como un elemento de riesgo en la adopción del documento digital, y si bien es cierto nos obliga a repensar los procesos y analizar los diferentes escenarios, también es indiscutiblemente el motor que nos ha permitido alcanzar niveles de vida nunca antes vistos por la humanidad y sin duda nos llevará a la solución de los problemas que enfrentamos hoy, y también mostrará el camino a seguir para resolver sus retos a los que vienen detrás de nosotros, pero para que eso sea posible debemos garantizar que nuestros sucesores cuenten con información auténtica, íntegra y confiable acerca de lo que hacemos hoy y nuestras razones. De ahí proviene la obligación ineludible de implementar y perfeccionar los mecanismos necesarios para la correcta preservación del patrimonio documental que no es nuestro, sino que nos lo han dado a cuidar.

V- Conclusiones y Recomendaciones

El incesante desarrollo tecnológico exige que los documentos en custodia se mantengan en un proceso de constante evolución, muy distante de los primeros intentos de almacenar los documentos digitales que consistían casi siempre en respaldos estáticos guardados en medios desconectados.

Que las instituciones implementen sistemas informáticos contribuye a agilizar la prestación de los servicios públicos, así como a incrementar la competitividad de las organizaciones, y hacer realidad las metas de la Ley de protección al ciudadano del exceso de requisitos y trámites administrativos, eliminando requisitos innecesarios y creando mecanismos de coordinación interinstitucional, de una manera ágil y transparente, pero a la vez, garantizando la intimidad y privacidad de los ciudadanos.

Es indispensable el empleo de la firma digital para asegurar la integridad y la autenticidad de la información, ya que nos provee de características y ventajas tan únicas como importantes en el manejo de los activos de información en soporte digital. Su principal atributo es contar con todo un marco legislativo que le atribuye su valor probatorio y que le confiere características de documento auténtico desde el punto de vista administrativo-legal, sin duda esta es la principal fortaleza de la firma digital y del uso de la infraestructura que acompaña esta tecnología.

Una firma digital avanzada apropiadamente construida, también nos proporciona certeza acerca del sujeto productor y de la organización a la que pertenece, nos permite conocer fuera de toda duda la autoría de un determinado documento y nos da garantía de esa autoría, pero adicionalmente también nos permite fijar una fecha y hora a partir de la cual se puede afirmar la existencia del documento, lo cual es parte fundamental en el ejercicio del valor probatorio legal de un activo de información.

La preservación digital sólo es posible si los documentos digitales siguen existiendo en un sistema de información, donde pueden ser accedidos y pueden evolucionar, migrar, a los nuevos formatos o versiones de los formatos dominantes, siempre dentro del marco de garantía de autenticidad e integridad que brinda un Archivo Digital.

El Archivo Digital es el responsable de almacenar, preservar, autenticar proteger y difundir los documentos digitales que custodia, mediante el cumplimiento de normativa específica y el uso de estándares internacionales de formato, debe aplicar las funcionalidades, estrategias y mecanismos de preservación a los documentos digitales para que estén disponibles y sean auténticos e íntegros. Las distintas implementaciones de Archivos Digitales que existan deben cumplir con las características mencionadas, sin embargo, los métodos específicos de custodia variarán de una implementación a otra.

En relación con la confidencialidad y seguridad, se deben aplicar las medidas necesarias para prevenir acciones no autorizadas. Al efectuarse una migración o conversión del formato, se debe garantizar que el documento continúa siendo auténtico, íntegro, por lo que se deben proteger los elementos que garanticen sus características en el nuevo formato y se aplique sobre el producto resultante la misma política de acceso que tenía el documento original.

La continuidad digital es la capacidad de utilizar la información en la forma que se necesite por el tiempo que sea necesario. Las estrategias de continuidad deben contemplar un plan de prevención de riesgos, de gestión de emergencias, de recuperación, formación, actualización y auditorías. La continuidad de los servicios debe realizarse con medidas preventivas que eviten la interrupción de los servicios. Las actividades de prevención y recuperación deben ofrecer las garantías necesarias, se debe medir la continuidad del negocio y la madurez digital.

Cuando se habla de garantizar la autenticidad y la integridad de la información digital, sea esta un documento textual, audiovisual o un registro de datos en una tabla, la herramienta por antonomasia será la firma digital, pero adicionalmente debe existir un mecanismo de trazabilidad que permita no sólo conocer el estado del acervo en custodia, sino también registrar sus operaciones, se deberá mantener un registro de todas las incidencias de seguridad que se produzcan, junto con la medida adoptada para resolverlas, el tiempo de resolución y las consecuencias, estos registros de auditoría también deberían contar con algún mecanismo de protección.

La infraestructura del Archivo Digital debe garantizar la integridad y la disponibilidad de todos los documentos, se debe realizar, como mínimo, muestreos de seguridad mediante recalcular periódicamente las identidades criptográficas de la información de archivo conservadas en el Archivo Digital. Si se detecta alguna incidencia, deberá notificarla inmediatamente al administrador del sistema.

La protección de los datos se basa en los mecanismos para garantizar la autenticidad e integridad de los documentos, así como de los principios de seguridad y redundancia de los sistemas. En los programas de preservación, la redundancia debe incluir copias de seguridad almacenadas de manera segura, destinadas a conservar los datos a largo plazo.

Las instituciones deben establecer normativa, planes y procedimientos necesarios para aplicar los mecanismos de preservación, control de accesos, verificaciones de integridad, protección contra ataques internos, y protección contra ataques eternos y desastres.

Finalmente se recomienda contar con un equipo interdisciplinario, competente y que esté en constante capacitación y actualización.

VI- Bibliografía

1. Archivo General de la Nación (2017) Un marco de referencia para la preservación digital. Módulo 1. Serie: Temas fundamentales de preservación digital. Cuadernos Digitales de Archivística. Desarrollado conjuntamente por el Consejo Internacional de Archivos (ICA), el proyecto InterPARES y el Archivo General de la Nación. Trad. Alicia Barnard, Alejandro Delgado y Juan Voutssas. México. [en-línea]. Disponible en: http://iibi.unam.mx/archivistica/InterPARES_1_020617.pdf

2. Asamblea Legislativa de la República de Costa Rica (2005) Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454 [en línea] Disponible en: http://www.firmadigital.go.cr/documentos/ley%208454.pdf

3. Asamblea Legislativa de la República de Costa Rica (2011) Ley de Protección a la Persona frente al tratamiento de sus datos personales N° 8968. [En línea] Disponible en: http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf

4. Asociación Española de Normalización y Certificación. (2015). Norma UNE-ISO 14721. Sistema de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia. España: AENOR.

5. Asociación Española de Normalización y Certificación. (2016). Norma UNE-ISO 15489-1 Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios. España: AENOR.

6. Asociación Española de Normalización y Certificación. (2011). Norma UNE-ISO 30300: Sistemas de gestión para documentos, fundamentos y vocabulario. España: AENOR.

7. Asociación Española de Normalización y Certificación. (2011). Norma UNE-ISO 30301: Sistemas de gestión para documentos y requisitos. España: AENOR.

8. Asociación Española de Normalización y Certificación. (2015). Norma UNE-ISO 30302: Información y documentación. Sistemas de gestión para los documentos. Guía de implantación. España: AENOR.

9. Casellas i Serra, L. (2016) “A la preservación de datos… !y más allá! En: Legajos 9 Boletín del AGN, 8ª época, 3. [en-línea]. Disponible en: http://189.206.27.87/Legajos/pdf/Legajos09/ALaPreservacionDeDatos.pdf

10. Duranti, L. (1996) Diplomática usos nuevos para una antigua ciencia. Trad. Manuel Vázquez. Sevilla: S&S ediciones Carmona.

11. Duranti, Lucuana (2004) Definición de documentos archivísticos electrónicos en el sector público y su fiabilidad y autenticidad. Traducción Alejandro Delgado Gómez. Conferencia SARBICA, Hanoi.

12. Duranti, L. (2005) La conservación a largo plazo de documentos electrónicos auténticos. Hallazgos del Proyectos InterPARES. Trad. Alejandro Delgado Gómez. Cartagena: Compobell S.L.

13. Forero Duarte, Johana Catalina (2016) Digitalización certificada con fines probatorios: herramienta de gestión en la toma de decisiones en la administración pública. Universidad Militar Nueva Granada: Bogotá. [En línea]

Disponible en: http://repository.unimilitar.edu.co/bitstream/10654/15951/1/ForeroDuarteJohanaCatalina2016.pdf.pdf

14. International Council on Archives (2016) Records in Contexts. A Conceptual Model for Archival Description. Consultation Draft v0.1

15. InterPARES – The Internacional Research on Permanent Authentic Records in Electronic Systems (2004). Business Driven Recordkeeping (BDR) Model. Disponible en: http://www.interpares.org/ip2/ip2_models.cfm

16. Ministerio de Ciencia y Tecnología (2013). Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente. [En línea] Disponible en: http://www.mifirmadigital.go.cr/wp-content/uploads/2016/03/DCFD-Poli%CC%81tica-de-Formato-Oficial-v1.0.pdf

17. Ministerio de Cultura y Juventud. (2015). *Implementación y uso de sistemas informáticos para la gestión documental y administrativa con firma digital en el Ministerio de Cultura y Juventud y sus Órganos desconcentrados.* [En línea] Disponible en: https://www.imprentanacional.go.cr/pub/2015/10/22/COMP_22_10_2015.pdf.

18. Ministerio de Hacienda y Administraciones Públicas (2016) Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE) Versión 2.0 Documentación complementaria a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos. [en-línea]. Disponible en: http://administracionelectronica.gob.es/

19. National Archives (2015) NARA 2015-04: Appendix A, Minimum Metadata Elements and Terms. [en-línea]. Disponible en: https://www.archives.gov/records-mgmt/bulletins/2015/2015-04-appendix-a.html

20. Red de Transparencia y Acceso a la Información (RTA) (2014) Modelo de Gestión de Documentos y Administración de Archivos (MGD) [En línea] Disponible en: http://mgd.redrta.org/modelo-de-gestion-de-documentos-y-administracion-dearchivos-para-la-red-de-transparencia-y-acceso-a-la-informacion/mgd/2015-01-23/093820.html

21. RLG-NARA Digital Repository Certification Task Force (2007) "Trustworthy repositories audit & certification: Criteria and checklist". [En línea] Disponible en: http://www.crl.edu/PDF/trac.pdf

22. RLG-OCLC Working Group on Digital Archive Attributes (2002) "Trusted digital repositories: Attributes and responsibilities". Mountain View, CA: Research Libraries Group (RLG). [En línea] Disponible en: http://www.oclc.org/research/activities/past/rlg/trustedrep/repositories.pdf

23. Serra Serra, Jordi (2014) Desarrollo de una Política de preservación digital como oportunidad de negocio para consultores y archiveros. Girona: Arxius i Indústries Culturals.

24. Térmens, M. (2013). Preservación digital. España Barcelona. Ed: UOC.

25. Voutssas, Juan y Barnard Alicia. (2014) "Glosario de Preservación Archivística Digital". Versión 4.0. México: Instituto de Investigaciones Bibliotecológicas y de la Información, UNAM.

26. Voutssas. (2010). *Preservación digital y seguridad informática.* [En línea] Disponible en: https://www.google.com/search?q=Preservaci%C3%B3n+digital+y+seguridad+inform%C3%A1tica&rlz=1C1GGGE_esCR502CR502&oq=Preservaci%C3%B3n+digital+y+seguridad+inform%C3%A1tica&aqs=chrome..69i57j69i61l2.334103j0j7&sourceid=chrome&ie=UTF-8.