

La firma electrónica y el archivo digital

Jordi Serra Serra

Departament d'Universitats, Recerca i Societat de la Informació

Generalitat de Catalunya

jordiserra@gencat.net

Si en la década de los 90 el mundo de la informática evolucionaba influenciado principalmente por los conceptos de eficacia y eficiencia en la gestión, a partir del 2000 se ha incorporado con fuerza un concepto clave: la **seguridad**. Cada día crece el mercado de soluciones para garantizar la seguridad en las comunicaciones, para la protección de objetos digitales y para el archivo seguro, puesto que se considera que la seguridad es premisa imprescindible para generar confianza en las comunicaciones digitales, fomentando con ello el crecimiento de la administración y el comercio electrónicos. Sin embargo, ¿Puede existir seguridad sin conservación? ¿Podemos plantearnos seriamente el concepto de seguridad si omitimos la necesidad de conservar durante un tiempo determinado el entorno que fijamos mediante los sistemas de seguridad?

El artículo 45 de la Ley 30/1992, quizás el más citado de los últimos tiempos, establece con claridad los principios para la aceptación del valor administrativo de los documentos digitales: autenticidad, integridad y conservación.¹ Sin embargo, mientras los dos primeros conceptos han tenido en los últimos tiempos un desarrollo legislativo, reglamentario y tecnológico notable,² la conservación ha sido la gran olvidada, con soluciones tecnológicas insuficientes y un desarrollo legal prácticamente inexistente.³

Los documentos administrativos⁴ se caracterizan porque sirven de evidencia de determinados hechos, lo que los convierte en el soporte básico para la toma de decisiones y para la reconstrucción histórica. Este valor evidencial les confiere un carácter activo, siendo el vehículo para la creación de derechos y obligaciones, y justifica el uso de un conjunto de métodos y técnicas específicos para su gestión. Éstos

¹ Añadiendo el no repudio en el caso de documentos telemáticos.

² Tan sólo a nivel general podemos citar el Real Decreto 263/1996 de despliegue del mencionado artículo 45, la Ley 34/2002 de servicios de la sociedad de la información, el Real decreto 209/2003 sobre los registros y las notificaciones telemáticas, y la Ley 59/2003 de firma electrónica. En el aspecto tecnológico se constata un desarrollo notable de los sistemas basados en infraestructuras de clave pública (PKI), así como la creación de las correspondientes agencias reguladoras.

³ Ninguna norma regula de forma directa el procedimiento de conservación de los documentos digitales administrativos. Únicamente la legislación relativa a la protección del patrimonio cultural realiza de forma tímida menciones explícitas al respecto (p.e. la Llei 10/2001 d'arxius i documents de la Generalitat de Catalunya). La reciente resolución de la Agencia Estatal de Administración Tributaria, de 16 de abril de 2004, apunta una línea de trabajo al considerar el papel como soporte de sustitución válido para determinados documentos digitales. En lo relativo a los desarrollos tecnológicos, las soluciones comercializadas se basan en archivo seguro a corto o medio plazo. La conservación para plazos superiores a los 10-15 años tan sólo ha sido objeto de experiencias localizadas en el entorno universitario y en algunos archivos y bibliotecas nacionales.

⁴ La noción de documento administrativo no se limita al entorno de la Administración pública. Se entiende por documento administrativo el conjunto de información fijada sobre un determinado soporte, con independencia del medio utilizado, creada o recibida por un ente público, organización, empresa o particular como resultado de sus actividades, y conservada en cumplimiento de las obligaciones legales y como soporte a la toma de decisiones. Véase: *Dictionary of archival terminology*. Peter Walne (ed.). 2nd ed. München; New York; London; Paris: Saur, 1988.

métodos, que reciben el nombre de *sistemas de gestión de los documentos administrativos*, se orientan a dos objetivos:⁵

- Crear i mantener documentos íntegros y auténticos por sus valores primarios, es decir, por su interés, utilidad y valor de prueba para la organización que los produce o recibe.
- Conservar documentos íntegros por sus valores secundarios, es decir, por su capacidad informativa para personas no vinculadas a la organización productora o receptora, garantizando a los ciudadanos el derecho a la conservación de la memoria histórica.

Esta gestión sistemática de los documentos administrativos está condicionada por la problemática de los documentos digitales. Además de la problemática tecnológica, relativa a la preservación de la integridad, la autenticidad y la legibilidad a lo largo del tiempo, se plantea otra problemática de tipo metodológico, relativa a la identificación y captura de los documentos a partir de los sistemas informáticos operacionales, a la forma de aplicarles los criterios de selección y eliminación, y a la posibilidad de conservar los documentos a largo plazo de forma externa a los sistemas de gestión. Esto obliga a las organizaciones a diseñar políticas específicas para la gestión y preservación de los documentos administrativos digitales.

1. La definición de una política de preservación

La definición de políticas de preservación digital se enmarca en el ámbito competencial de los sistemas de gestión de la documentación administrativa. Desde el año 2001 se dispone de un estándar para la definición de sistemas de gestión documental, la norma ISO 15489.⁶ La secuencia de pasos que establece esta norma permite definir una política de preservación digital, agrupándolos en tres grandes fases:

- La primera fase consiste en la definición del **ciclo de vida** de los documentos generados por cada proceso o trámite. Esta fase comprende el determinar los documentos que es necesario capturar a partir de los sistemas de gestión (9.1). Para este conjunto de documentos es necesario establecer el período de conservación (9.2), la forma de captura (9.3), el sistema de registro y descripción (9.4), y finalmente el sistema de clasificación o categorización (9.5).
- La segunda fase consiste en la creación de un **archivo digital** seguro, organizado y gestionado según criterios documentales. Esto implica habilitar un sistema de almacenamiento (9.6), un sistema de acceso controlado (9.7), y un sistema de *tracking/logging* (9.8).
- La tercera fase consiste en la definición de las **estrategias tecnológicas** para garantizar la legibilidad a largo plazo de los documentos (9.9).

Este planteamiento puede suponer un esfuerzo excesivo para determinadas organizaciones. Desde una perspectiva pragmática, se ha sugerido la conveniencia de realizar la definición de la política en sentido inverso, con el objetivo de ajustarla a las

⁵ Véase *The Preservation of the Integrity of Electronic Records*. Vancouver: University of British Columbia, 1997.

⁶ La norma ISO 15489 tiene por objetivo normalizar las mejores prácticas internacionales en materia de gestión documental, utilizando como punto de partida el estándar australiano AS 4390.

posibilidades de cada organización. Esto significa que, en primer lugar, se analizarán los recursos de la organización, así como sus responsabilidades con relación a la conservación de los documentos más allá de la caducidad de sus valores primarios. Tan sólo en el caso de que exista esta obligación, y en función de las estrategias tecnológicas de conservación a largo plazo que se esté en condiciones de aplicar, se definirán los requisitos de conservabilidad de los documentos (formatos admitidos, niveles de descripción, etc.). El siguiente paso será la definición del ciclo de vida, identificando previamente qué informaciones se deben capturar de los sistemas de gestión y de qué forma. Finalmente, se deberán modificar dichos sistemas de gestión con el fin de introducir las funcionalidades necesarias para crear y capturar documentos de forma controlada y de acuerdo con el modelo definido en la política de preservación. El objetivo de la política de preservación es, pues, habilitar los sistemas operacionales para producir, a partir de un determinado momento del ciclo de vida, objetos digitales conservables de acuerdo con una determinada capacidad tecnológica.

En su aplicación, la definición de una política de preservación adquiere tres matices:

- La conservación de los documentos con valores primarios dentro de los sistemas informáticos de gestión. Se incluyen los sistemas de archivo seguro y los procedimientos de copia de seguridad.
- La conservación de los documentos con valores primarios fuera de los sistemas informáticos de gestión (conservación a largo plazo).
- La conservación de los documentos con valores secundarios, en este caso recibiendo un tratamiento externo por motivos económicos y funcionales (conservación permanente).⁷

El principal reto de una política de preservación es la identificación de los documentos digitales administrativos para hacer posible su captura. Esto implica la conversión de una estructura tecnológica en una estructura documental, gestionable e inteligible de forma independiente a su contexto tecnológico. En este sentido se han formulado dos modelos de identificación y captura.⁸

El primero es el **modelo datacéntrico**, o identificación orientada a procesos. Este modelo no realiza distinción alguna entre la estructura tecnológica y la estructura documental, de manera que todo el sistema informático se considera en conjunto un mismo documento. Este modelo parte de la premisa de que cada sistema automatiza una o un grupo de funciones de la organización de forma completa, razón por la cual puede recibir un tratamiento documental homogéneo. Esto es frecuente en las aplicaciones informáticas corporativas, o en las aplicaciones con un desarrollo “ex profeso”. Así, una aplicación de gestión de personal, o una que automatice la tramitación de un conjunto de subvenciones, pueden recibir esta consideración sin problema. No así los sistemas informáticos sin vinculación concreta a ninguna tramitación, como un sistema de mensajería, un sistema de trabajo en grupo, o un *Data warehouse*, donde no tendrá sentido la aplicación de este modelo. Sin embargo, en ciertos casos es la complejidad tecnológica, o la imposibilidad de segregar los elementos de un sistema, lo que va a recomendar su tratamiento en conjunto.

⁷ El perfil tecnológico de un archivo digital histórico será siempre mucho más bajo que el de un archivo seguro en fase administrativa, pero también mucho más económico y, por lo tanto, sostenible.

⁸ Para una definición más completa de estos modelos véase Serra, Jordi. “L’administració electrònica i la gestió de documents”, en *BiD*, núm. 11, 2003.

El segundo modelo recibe el nombre de **modelo docucéntrico**, o identificación orientada a objetos. Este modelo se aplica cuando la estructura tecnológica no se considera relevante o representativa para adquirir y preservar los valores documentales, de manera que el sistema se considera únicamente un generador de documentos. El esfuerzo se centra en este caso a conseguir que el sistema genere objetos digitales con valor evidencial, y con unas características que les permitan ser conservados. Es vital el análisis de las funciones y los procesos, junto con la determinación de la forma válida del substrato documental de estos procesos, lo que en el ámbito de la gestión documental recibe el nombre de evaluación o valoración. La captura, en este caso, implica a menudo algún tipo de transformación en el documento, habitualmente la conversión a un formato digital conservable. Están ya disponibles registros públicos de formatos con indicación de su nivel de fiabilidad para la conservación a medio y largo plazo.⁹

2. Modelos de archivo digital

Las experiencias en archivos históricos de carácter público han configurado un modelo de archivo digital, basado en la custodia de soportes, que en su mayor parte replica los planteamientos y procedimientos de los archivos de soportes tradicionales.¹⁰ Así, el ingreso de los documentos se realiza mediante una transferencia física de soportes digitales, junto con su posterior almacenamiento y conservación. Habitualmente se determina un formato inicial de conservación permanente, que condiciona la admisibilidad de los documentos, y que no se modifica a lo largo del período de conservación.¹¹ La documentación sobre el contexto tecnológico y documental se transfiere de forma desvinculada de los documentos.

Sin embargo, el estándar OAIS (*Open Archival Information System*) ha normalizado un nuevo modelo de archivo digital, basado en la gestión de depósitos, que permite la creación de un archivo digital de forma distribuida y sin la custodia directa de la información, utilizando la transferencia telemática y la conservación en sistemas de archivo que permitan el acceso en línea. La desvinculación de un soporte físico concreto obliga a generar objetos digitales conservables, autosuficientes y fácilmente gestionables, combinando el uso de la metadescripción endógena,¹² la encapsulación de

⁹ Véase el proyecto *PRONOM* de los archivos nacionales del Reino Unido (<http://www.nationalarchives.gov.uk/pronom/>). Véase también *Global Digital Format Registry Project*, impulsado por la Digital Library Federation (<http://hul.harvard.edu/gdfr/>).

¹⁰ Para las experiencias europeas véase Schürer, Kevin. *Better access to electronic information for the citizen: the relationship between public administration and archives services concerning electronic documents and records management*. Luxembourg: Office for Official Publications of the European Communities, 2001. Para una comparativa de este modelo véase Serra, Jordi. "Estrategias de preservación de documentos electrónicos: el National Archives and Records Administration y el Public Record Office". En: *Actas de las V Jornadas de Archivos Electrónicos*. Priego de Córdoba: Archivo Municipal, 2002.

¹¹ Los formatos más habituales son texto plano, SGML o XML para los documentos textuales, texto delimitado para los ficheros de datos, y TIFF para las imágenes. Son formatos estandarizados y, a ser posible, humanamente legibles.

¹² Véase Méndez, Eva. "Tratamiento de los objetos de información en los archivos: retos y estándares para la descripción basada en metadatos". En: *La administración electrónica y los archivos: amenazas y oportunidades para la archivística*. Toledo, 2003.

los documentos por agrupaciones documentales, y el uso opcional de la firma electrónica de archivo.

El *Reference model for an open archival information system (OAIS)*¹³ ofrece el marco para definir un sistema de archivo digital orientado a la conservación a largo plazo, proporcionando la conceptualización y la terminología para establecer los elementos, las fases y el funcionamiento de este archivo. Un OAIS se define como un conjunto de personas y sistemas que han aceptado la responsabilidad de conservar información y hacerla accesible a una determinada comunidad. El modelo OAIS estructura su funcionamiento en tres etapas:

- **Adquisición** (*ingest*). Sea a través de un proceso previo de valoración y selección, sea a partir de la adquisición directa, los documentos se reciben en su formato original. En esta fase se realiza la transformación de los documentos originales en objetos digitales conservables, lo que implica la verificación de sus requisitos de conservabilidad (validación de la sintaxis, cumplimiento de reglas de integridad en bases de datos, y ausencia de virus, contraseñas y compresiones), la migración a un formato más estable y la encapsulación por agrupaciones documentales. A continuación se completa su descripción, opcionalmente se firman, y se copian al dispositivo de almacenamiento.
- **Conservación** (*archival storage*). Se lleva a cabo en un repositorio digital seguro, y en el formato de conservación a largo plazo. Periódicamente se aplican los mecanismos necesarios para chequear los errores y garantizar la legibilidad.¹⁴ En función de la transformación que estos mecanismos realicen sobre el código del documento original, hablaremos de conservación del entorno tecnológico original cuando no se realice ningún tipo de transformación, de migración cuando se modifique el código fuente del documento, y de emulación cuando se modifique el código del entorno tecnológico del documento. La migración puede realizarse dentro del entorno tecnológico original (compatibilidad retroactiva e interoperabilidad), a un entorno neutro (conversión a estándar), a un entorno predefinido (conversión a formato de emulación) o, simplemente, a otro entorno (cambio de medio o soporte físico).
- **Acceso** (*access*). La recuperación de los documentos se lleva a cabo en tres etapas. En primer lugar se consulta el inventario o catálogo de documentos, construido a partir de los metadatos. Una vez localizado, el documento se convierte a un formato que facilite su difusión. Finalmente el documento se transfiere a una área donde sea accesible para sus usuarios durante un tiempo determinado.

El modelo OAIS identifica diferentes estadios en la información que gestiona. Así, en la fase de adquisición se reciben objetos digitales originales (*Submission information*

¹³ El *Reference model for an open archival information system (OAIS)* es producto de la colaboración entre el *Consultative Committee for Space Data Systems (CCSDS)* y la *International Organization for Standardization (ISO)*. Iniciado en 1995, su desarrollo se completó en enero de 2002 con su aprobación como estándar internacional ISO 14721.

¹⁴ Para una revisión de las estrategias tecnológicas de preservación digital, véase: Serra, Jordi. "Gestión de los documentos digitales: estrategias para su conservación". *El profesional de la información*, vol. 10, núm. 9 (septiembre 2001). Véase también: *Cedars guide to digital preservation strategies*. Version 3. Leeds: Cedars project, april 2002. Disponible en <http://www.leeds.ac.uk/cedars/>.

package, o SIP), que se transforman en objetos conservables (*Archival information package*, o AIP). Estos objetos se componen de una información de contenido (*content information*), que incluye el documento original (*content data object*) y la información de representación (*representation information*), más una información descriptiva sobre la preservación (*preservation description information*, o PDI). En la fase de acceso, los AIP se transforman en objetos digitales accesibles (*Dissemination information package*, o DIS).

3. La firma electrónica de archivo

En un horizonte de archivos virtuales, con repositorios distribuidos y sistemas de acceso centralizados, se hace imprescindible la securización a nivel de objeto. La firma electrónica cobra así un papel primordial, como medio básico para fijar el valor evidencial de un documento digital, de forma independiente de su contexto de creación y utilización. A menudo, sin embargo, la tecnología de la firma electrónica ha sido considerada para la conservación a largo plazo más una amenaza que un beneficio, presentando una problemática que afecta a todas las fases del ciclo de vida:

- En la fase administrativa, el principal problema es la caducidad de la firma. La actualización de la firma original sólo es posible cuando se tiene acceso al documento y al sistema utilizado para firmarlo. Desde el momento en que la transferencia al archivo significa una desvinculación del entorno tecnológico original, se dificulta la actualización de la firma.
- En la fase de conservación a largo plazo, la firma electrónica se convierte en un factor de riesgo para mantener la legibilidad de los documentos digitales, puesto que constituye una capa tecnológica, añadida a los documentos, que mantiene vinculaciones externas determinantes para su validez (software de firma y cifrado, lista de certificados revocados, etc.). El uso de técnicas de encriptación puede dificultar posteriores migraciones, del mismo modo que la obsolescencia tecnológica puede afectar al software de firma y cifrado. Se añade que, para mantener la vigencia de la firma por un período de tiempo prolongado, es necesario conservar los elementos básicos de la infraestructura de firma (PKI).

Sin embargo, estas objeciones no invalidan el uso de la firma electrónica en archivos digitales. El uso combinado de la tecnología de firma electrónica y sello de tiempo tiene un potencial enorme en la concepción de archivo digital derivada del modelo OAIS, especialmente en los casos siguientes:¹⁵

- El disponer de una firma electrónica corporativa permite al archivo la sustitución de la firma personal, distinta para cada documento y con un plazo de caducidad pocas veces superior a los cinco años, por una firma de archivo. Esta firma, única y con un plazo de caducidad mucho mayor, facilita la tarea de refirmar

¹⁵ Véase Waugh, Andrew. "On the use of digital signatures in the preservation of electronic objects". Véase también Dumortier, Jos & Van den Eynde, Sofie. "Electronic signatures and trusted archival services". Ambos en: European Commission. *Proceedings of the DLM-Forum 2002: Access and preservation of electronic information*. Luxembourg: Office for Official Publications of the European Communities, 2002.

periódicamente los documentos, manteniendo intacto su valor evidencial y su potencial utilización legal, incluso después de la caducidad de su firma original. El archivo actúa en este caso de fedatario público.

- Un segundo factor de simplificación proviene de la aplicación del paradigma archivístico a la gestión de los documentos digitales. La gestión de los documentos como evidencia de actividades no tiene sentido de forma individualizada: la unidad mínima de gestión es siempre la unidad documental compuesta (el tradicional expediente), e incluso en determinados casos el nivel superior (la serie documental).¹⁶ En este caso podemos pasar de gestionar documentos a gestionar, agrupados en bloques significativos, los substratos documentales de las actividades, reduciendo aproximadamente a un 5%-10% el número total de objetos a gestionar. La firma electrónica de archivo se aplicará únicamente a nivel de agrupación documental, sustituyendo de éste modo la firma individual de documentos.
- A lo largo del ciclo de vida de cada tramitación tienen lugar una serie de eventos que precisan de una constancia fechada. Estos eventos son la finalización de la actividad (el cierre del expediente), la generación de la versión de archivo y la constancia de la transferencia de la responsabilidad de la custodia. En estos casos, el uso del sello de tiempo permite fijar los eventos al bloque firmado de forma indisoluble.
- El mantener legibles los documentos implica, como hemos comentado, una serie de operaciones técnicas que a menudo exigen su transformación o conversión a formatos vigentes. Cada modificación que se realiza sobre un documento original debe ser documentada, y exige la constancia de su autoría y fecha. Nuevamente se pueden utilizar la firma electrónica y el sello de tiempo para la validación de modificaciones con fines de preservación. Así, el documento digital conservable a largo plazo se convierte en un bloque, correspondiente a una agrupación documental, autenticado por el responsable de la custodia, y periódicamente modificado, actualizado y refirmado mediante una serie de capas de información acumulativas.

La utilización de la firma electrónica de archivo no excluye la necesidad de conservar la infraestructura de clave pública. Sin embargo, mediante una estructura cooperativa de archivo digital es posible la conservación de documentos digitales por un período de tiempo considerable y a un coste asequible para la mayoría de organizaciones. Aunque no se pueda hablar de soluciones definitivas, la necesidad urgente de conservar el patrimonio digital actual exige éxitos a corto plazo, el primero de los cuales puede ser la puesta en marcha de soluciones económicas que permitan ganar el tiempo suficiente para el desarrollo de tecnologías más estables.

Barcelona, 30 de julio de 2004

¹⁶ Para la definición de los elementos de la jerarquía de agrupaciones documentales véase *ISAD(G): General International Standard Archival Description*. 2nd ed. Adopted by the Committee on Descriptive Standards Stockholm, Sweden, 19-22 September 1999.