BOLETIN

LVI (2006), NÚM. 4

CONFEDERACIÓN
DE ASOCIACIONES
DE ARCHIVEROS,
BIBLIOTECARIOS,
MUSEÓLOGOS
Y DOCUMENTALISTAS

BOLETÍN

de la

CONFEDERACIÓN
DE
ASOCIACIONES
DE
ARCHIVEROS
BIBLIOTECARIOS
MUSEÓLOGOS Y
DOCUMENTALISTAS

ANABAD

LVI (2006), NÚM. 4, OCTUBRE-DICIEMBRE. MADRID ISSN 0210-4164

ANABAD

Directora: M.ª del Pilar Gallego Cuadrado

Comisón de Publicaciones para este número:

Pedro González García
Luis-Daniel Fernández Ovalle
Angélica Zapatero Lourinho
Julio Cerdá Díaz
Julia M.ª Rodríguez Barredo

Editor: Confederación de Asociaciones de Archiveros, Bibliotecarios, Museólogos y Documentalistas

Dirección Postal: Boletín de la ANABAD.
c/Recoletos, 5
28001 Madrid. Tel.: 915 751 727
Fax: 915 781 615
c.e:anabad@anabad.org

Precio de suscripción: 93,60 Euros

Precio número suelto: 24,50 Euros

Canje: Sólo se mantendrá con las demás asociaciones profesionales o con aquellas publicaciones que se consideren de interés para la biblioteca de la ANABAD.

Periodicidad: Trimestral.

Impresión: Gráficas VARONA, S.A. (Salamanca)

Boletín de la ANABAD trata de ser un órgano de expresión y un medio de formación profesional permanente para todos sus asociados, al servicio de todos los archiveros, bibliotecarios, conservadores de museos y documentalistas de España.

Su campo son todos los problemas teóricos y prácticos que plantea la profesión de quien sirve a la difusión de la información científica de los bienes culturales y toda la información que pueda ser útil para el ejercicio de la misma y para que nos conozcan en otras latitudes.

Su responsable es la Confederación ANABAD. Cada colaborador lo es de sus propias ideas.

Este Boletín ha sido coordinado por D. Pedro González García, refleja el estudio sobre e-Administración y Documentación electrónica en España y se ha realizado con la ayuda concedida en 2006 por la Dirección General de Cooperación y Comunicación Cultural del Ministerio de Cultura.

SUMARIO

BOLETÍN DE LA ANABAD LVI (2006), NÚM. 4, OCTUBRE-DICIEMBRE. MADRID ISSN 0210-4164

EDITORIAL

El problema de los documentos electrónicos de archivo

El auténtico fogonazo que la aparición y extensión casi instantánea de las nuevas tecnologías ha supuesto en el momento histórico que estamos viviendo, ha removido parte de los cimientos de nuestra profesión y en algunos aspectos nos ha dejado bastante descolocados.

Concretamente en el mundo de la administración electrónica y de los documentos electrónicos de archivo, nos encontramos en un momento complejo en que incluso se pone en entredicho la viabilidad futura de nuestra profesión.

No nos referimos al trabajo relacionado con la documentación archivística convencional. Sin lugar a dudas las herramientas informáticas pueden sustituir muy favorablemente muchos de nuestros métodos tradicionales, pero son sólo herramientas que nos ayudan a desarrollar más eficientemente nuestro trabajo. Por eso las hemos adoptado con rapidez, tratando de sacarlas el mayor partido posible.

Nos referimos a la documentación que se genera originalmente en soporte electrónico (*born digital*, según la expresión inglesa). Para los productores de esta documentación lo que importa casi siempre son sólo los valores primarios, el uso inmediato, la seguridad y fácil recuperación, los costes que conlleva..., única y exclusivamente durante el tiempo reducido en que continúa vigente. Sólo los que estamos acostumbrados a tratar y entender los documentos en una perspectiva de ciclo vital y a largo plazo, y en el contexto de unos valores secundarios que hacen que muchos de ellos hayan de conservarse de forma permanente como testimonio de nuestra historia, podemos identificar el problema que esto puede generar.

¿Podrán las próximas generaciones disponer de los documentos electrónicos que ahora se están generando con suficientes garantías de integridad y

autenticidad?. ¿Cómo conservaremos para el futuro y con garantías razonables la documentación que hoy se produce?. ¿Cómo resolveremos los problemas planteados por la obsolescencia, para los documentos dotados de valor legal y validados con firma electrónica reconocida?. ¿Será preciso olvidarse de la firma digital al ingresar en los archivos la documentación electrónica de valor permanente?

Sin embargo no parece que los responsables de la Administración estén entendiendo toda la profundidad del problema, como queda claro en el Proyecto de Ley sobre Acceso Electrónico de los Ciudadanos a las Administraciones Públicas, inicialmente preparado como Borrador de Ley de Administración Electrónica. Este borrador dedica su artículo 31 al «archivo electrónico de documentos», pero ni siquiera se mencionan los temas que nos preocupan. En ningún momento se toman en consideración los aspectos temporales del documento, la evolución de sus valores primarios y secundarios... La Ley de Patrimonio no se cita ni una sola vez, ni se adjudica a ningún centro de archivos la responsabilidad de conservación, transferencia, valoración, eliminación en su caso y conservación definitiva.

En esta preocupante situación ANABAD presenta este número monográfico con la idea de contribuir a clarificar la situación aportando algunas informaciones para el debate profesional. El futuro de los documentos generados en la actualidad por la naciente administración electrónica está en juego. Incluso el futuro de los archivos, y tal vez también nuestro propio futuro profesional.

La Junta Directiva

INTRODUCCIÓN

Los Archivos en la encrucijada: el reto de los documentos electrónicos

PEDRO GONZÁLEZ*

RESUMEN: Se analizan en este artículo los principales problemas que los archivos y los documentos electrónicos plantean en la actualidad. El reto con el que se enfrentan los profesionales, los riesgos y problemas a los que hay que hacer frente (falta de normas, obsolescencia, falta de políticas adecuadas, falta de legislación, etc.). Se repasan asimismo algunas de de las herramientas que en la actualidad se están empleando, así como las estrategias que se están siguiendo en los países más avanzados. Y finalmente se plantean algunos interrogantes que afectan al futuro de la Administración, de los Archivos, y de los propios profesionales.

PALABRAS CLAVE: Administración electrónica, archivos electrónicos, documentos electrónicos, firma digital.

0. INTRODUCCIÓN

Cuando redactamos este texto, no sabemos aún cómo será definitivamente la prometida Ley de Administración Electrónica que en la actualidad se encuentra en marcha, al parecer reconvertida a una Ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas, ni cómo se aborda-

* Actualmente Asesor Técnico en el Archivo del Tribunal de Cuentas.

rá concretamente el tema del archivo de los documentos electrónicos. Pero lo que hasta la fecha hemos podido ver en el borrador de Anteproyecto que se ha hecho público por el MAP[1] es bastante descorazonador para los profesionales de los archivos.

Y eso que ya teníamos antecedentes para que el tema no nos cogiera por sorpresa, como la «medida 19» del Plan de Choque para el Impulso de la Administración Electrónica en España, que preveía que la Entidad Pública Empresarial *Red.es*, en colaboración con el MAP, se haría cargo de desarrollar «un servicio común de archivo de documentación» para ponerlo a disposición de los Ministerios[2]. Ninguna información actualizada hemos encontrado en la página web de Red.es sobre este asunto, aunque sabemos que se presentó en una reunión de profesionales de archivos por uno de sus responsables[3].

Y esto no parece haber sido reconducido en los planes posteriores. En el *plan Avanza*[4] sólo aparece una vez la palabra archivo para referirse a la «Creación de contenidos digitales por parte del sector público mediante la digitalización y difusión de fondos del patrimonio cultural, especialmente de bibliotecas y **archivos**». Y en las 25 páginas del *plan Moderniza*[5], según la presentación disponible en la web del MAP, la palabra Archivo no aparece ni una sola vez.

No deja de extrañarnos que en un país que fue pionero en la creación de archivos como soporte para la Administración (el Archivo de Simancas es el primer gran archivo de estado del mundo y el Reglamento que le otorga Felipe II en 1588 se considera el primer reglamento de archivos[6]), y que por ello

---

[1] http://www.060.es/informacion_060/noticias/proyecto_LAECAP/Proyecto_LAECAP-ides-idweb.jsp (consultado en diciembre de 2006)

[2] *Con el fin de poder contribuir en mayor medida a un mejor funcionamiento de los Departamentos Ministeriales, la Entidad Pública Empresarial Red.es en colaboración con el Ministerio de Administraciones Públicas desarrollará un servicio común de archivo de documentación que pondrá a disposición de los Ministerios que lo soliciten, proporcionando a su vez las correspondientes herramientas para su gestión.*

El servicio permitirá el archivado de documentos electrónicos de manera segura y a largo plazo, la salvaguarda de posibles pérdidas de información derivadas de ataques informáticos o fallos en los sistemas, así como el mantenimiento de aplicaciones, estándares y la realización de cualquier otra actividad que permita el acceso a la información almacenada.

[3] Gabriel Sánchez Dorronsoro, «El archivo telemático en las Administraciones públicas». En *Nuevos modelos para el tratamiento y gestión de los archivos públicos: sistemas, tecnologías y administración electrónica*, pp. 37-57. Junta de Comunidades de Castilla La Mancha, Consejería de Administraciones Públicas, 2005.

[4] Plan Avanza. Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas. Aprobado por Consejo de Ministros de 4 de noviembre de 2005. Es una de las actuaciones estratégicas del plan Ingenio 2010, presentado por el Presidente Zapatero el 23 de junio del mismo año. http://www.planavanza.es/pdf/plan_avanza.pdf

[5] Plan Moderniza. La Administración Ciudadana. Plan de medidas 2006-2008 para la mejora de la Administración. Aprobado en Consejo de Ministros de 9 de diciembre de 2005. http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/parrafo/00/document_es/Plan_Moderniza.pdf

[6] R.H. Bautier, «Les Archives», en *L'Histoire et ses méthodes*. Paris, 1972, p. 1128, citado por José Luis Rodríguez de Diego en su introducción para la *Instrucción para el Gobierno del Archivo de Simancas* (1588), publicado por el Ministerio de Cultura en 1989 con motivo del IV Centenario.

hoy dispone de uno de los más importantes patrimonios documentales, se despache en unas líneas bastante imprecisas y con poco fundamento la responsabilidad de conservar para el futuro la documentación que servirá de testimonio de nuestra historia presente.

La fractura que se ha producido es enorme si tenemos en cuenta que tanto en el «plan de choque» como en el borrador de Anteproyecto de Ley de Administración Electrónica o Ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas, se habla del «archivo de documentación» o del «archivo electrónico de documentos», pero sólo se presentan aspectos puramente informáticos de conservación y seguridad, ignorando por completo todo lo relativo a los aspectos legales, de tratamiento, organización, conservación y acceso a los documentos (excepto en lo que hace referencia a la legislación de protección de datos), ignorando en consecuencia a los responsables de los Archivos de la Administración, y obviando el carácter de patrimonio histórico que tienen los documentos producidos por la Administración, según la Ley 16/1985, de 25 de Junio, de Patrimonio Histórico Español. Ninguna referencia a la responsabilidad del Archivo General de la Administración o del Archivo Histórico Nacional, por ejemplo. Ninguna referencia a la consideración de los documentos como un todo, como testimonio de la gestión de la Administración, pero también como parte de nuestro patrimonio cultural, y por tanto como algo a conservar para el fututo.

Tal vez la culpa de este abandono sea de los profesionales que no hemos sabido hacer valer ante la sociedad la importancia del servicio que los archivos prestan o que no hemos sabido adaptarnos a las condiciones del mundo desarrollado, democrático y globalizado. Tal vez, encerrados en esos «arsenales para la historia» que se decía en nuestros textos, preocupados por describir hasta el último detalle de nuestros pergaminos medievales o de nuestros registros de cancillería, o por analizar y completar hasta el más mínimo elemento de descripción según la norma ISAD(G), no nos hayamos dado cuenta de por dónde iba la corriente de la historia y nos hayamos visto arrastrados por la marea conjunta del desarrollo económico y social del último medio siglo, del *boom* de las nuevas tecnologías y en última instancia de la llegada a la sociedad globalizada, con el crecimiento desbordado en la producción documental como consecuencia especialmente de la multiplicación de nuevos servicios al ciudadano y del incremento exponencial de las nuevas herramientas tecnológicas.

Hoy nuestros más importantes archivos están llenos de papeles en cantidades ingentes que no podemos manejar adecuadamente. En la Administración General del Estado la continuidad en la gestión correcta del ciclo de vida de los documentos está casi paralizada. El Archivo General de la Administración (AGA) apenas puede recibir documentos porque carece de espacio para ello, porque no se eliminan materiales sin valor (posiblemente más de la mitad de sus más de 150 kms. lineales de estantería) y porque tampoco tiene abierta una vía de salida hacia el Archivo Histórico Nacional (AHN). El AHN hace mucho tiempo que está paralizado en un edificio minúsculo, sin recursos y

perspectivas nuevas. Y la Administración, en lugar de poner los medios racionales para resolver el problema (personal cualificado en número suficiente, instrumentos legales adecuados, planes de trabajo para identificar y seleccionar lo que deba conservarse y a la vez eliminar todo lo inútil –que es mucho–...), opta por soluciones más fáciles y de rápida visibilidad, pero a veces mucho más costosas económicamente y menos eficaces a la larga.

Es posible que los Archiveros no nos hayamos dejado oír lo suficiente como para que los responsables de la Administración entendieran lo esencial de nuestra misión:

> «lograr los objetivos de salvaguardia y conservación de los documentos de valor permanente, y garantizar que sean accesibles e inteligibles»[7]

Sin embargo, aunque de forma excesivamente tímida y escasa los archiveros españoles hemos ido colaborando en algunos proyectos relacionados con los nuevos documentos electrónicos y hemos reclamado medidas para afrontar el problema que se estaba incubando[8]. Nos hemos planteado igualmente nuestra ubicación profesional en este nuevo mundo virtual aunque casi siempre bebiendo en las fuentes de los profesionales de otros países más avanzados, especialmente los anglosajones que nos llevan una importante ventaja.

Desde hace mucho tiempo, a nivel nacional e internacional, venimos anunciando el problema que se nos avecina: es posible que cuando los historiadores del futuro se pongan a analizar el momento que estamos viviendo, que por otra parte es el de mayor producción documental de la historia, se encuentren con determinadas lagunas que no sean capaces de rellenar porque no ha habido previsión suficiente para responder al reto planteado por las nuevas tecnologías para la conservación de los nuevos documentos. *Amnesia digital* se ha llegado a llamar a este problema. Son ya muchos los ejemplos que pueden ser traídos a cuenta, aunque para no ser tediosos nos limitaremos a recordar dos de distinto signo: el primero es internacional, el problema planteado en los Archivos Nacionales de Washington cuando se decidió la incorporación en 1976 del Censo de Población de 1960[9], cuyos materiales de tabulación fueron

[7] Consejo Internacional de Archivos. *Electronic Records: a Workbook for Archivists* (usamos la edición en castellano, *Documentos electrónicos. Manual para Archiveros.* Madrid: Ministerio de Cultura, 2006), p. 19, citando la *Guide for Managing Electronic Records from an Archival Perspective*, p. 25, publicada por el CIA en 1997.

[8] Yo mismo exponía ya en el año 1988 la urgencia en disponer de una legislación sobre los nuevos soportes en la ponencia presentada en las III Jornadas de Archivos. Cádiz, 1988: «Los documentos en nuevos soportes».

[9] Es este un caso muy conocido e incluso casi mitificado, pero transmitido erróneamente entre los profesionales de los Archivos. En marzo de 1985 un informe de un Committee on the Records of Government sacaba a la luz la pérdida de datos relacionados con el Censo americano de 1960. Cuando a mediados de los años 70 se decidió el ingreso de esta documentación en el NARA, se decía, sólo había dos equipos en el mundo capaces de leer las cintas, uno en el Smithsonian y otro en Japón. Aunque esta era una versión apócrifa, lo cierto es que el problema sólo se resolvió mediante el encargo a una empresa de la conver-

almacenados en cintas UNIVAC de un modelo hacía tiempo obsoleto, y el segundo es más cercano, el supuesto borrado de los discos de los ordenadores de la Presidencia del Gobierno en el último cambio de legislatura, del que la prensa nos informó y que se encuentra aún en manos de la justicia[10].

En este aspecto nuestro país tiene casi todo por hacer: se ha legislado sobre los documentos electrónicos y sobre su validez probatoria, se ha avanzado en los temas de la firma digital, hay organismos con sistemas muy avanzados de gestión electrónica de documentos (la AEAT por ejemplo), pero apenas se ha pensado en la conservación a largo plazo[11], no se ha tenido en cuenta «la variante tiempo» que afecta directamente al valor de los documentos (y en el mundo de las nuevas tecnologías es clave por la obsolescencia), no hay un centro que tenga claramente encomendada la función de «conservación permanente» de los documentos electrónicos, y sobre todo no se han realizado planes ni se han arbitrado recursos para buscar soluciones reales. Como suele suceder, las urgencias del momento, y más en la vida política, impiden pensar a largo plazo (y para los profesionales de los archivos el largo plazo es realmente largo¡).

Uno siente sana envidia cuando observa la actuación de un país como Australia. Se trata de un país con unos 20 millones de habitantes, aproximadamente la mitad que España, en una superficie 15 veces superior a la española. Por supuesto su patrimonio histórico y su tradición archivística nada tienen que ver con los nuestros. Pero con sólo entrar en la página web de los Archivos Nacionales de Australia[12] y especialmente su apartado de *e-Permanence*, es posible percatarse de la variedad de las alternativas exploradas en todo lo que se refiere a la gestión y a la conservación de documentos electrónicos (legislación, normalización, software...). En realidad se está creando un sistema com-

---

sión de aquellas cintas a formatos actualizados. Pueden verse los detalles de la Historia en «Preserving Digital Information». *Draft Report of the Task Force on Archiving of Digital Information*, Version 1.0, Aug. 24, 1995, p. 2. ftp://ftp.rlg.org/pub/archtf/final-report.pdf, y con más detalle en «Margaret O. Adams and Thomas E. Brown, "Myths and Realities About the 1960 Census». *Prologue*, Winter 2000, vol. 32, n.º 4 http://www.archives.gov/publications/prologue/2000/winter/1960-census.html

[10] El 13 de diciembre de 2004 desde diario El País se informó del borrado de los ordenadores de la Presidencia del Gobierno por parte del equipo saliente del Presidente Aznar, trabajo que había sido realizado por una empresa contratada para el caso por un total de 12.000 euros. Al conocerse los hechos, APEDANICA, Asociación para la Prevención y Estudios de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas, formuló una querella ante el Juzgado de Instrucción de Madrid. Está querella, que fue acompañada por otra presentada en 26 de julio de 2005, se encuentra en este siguiendo los procedimientos correspondientes.

[11] Como parte del proyecto de «Aplicaciones utilizadas para el ejercicio de potestades», del Consejo Superior de Informática, se incluyeron los «Criterios de conservación». Aunque estos criterios incluyen medidas sobre conservación a lo largo del ciclo de vida de los documentos electrónicos haciendo referencia de forma continuada al MoReq y al DLM Forum, el contenido es escaso y poco preciso y no se aborda el problema directamente y en profundidad.

[12] http://www.naa.gov.au/

pleto para la gestión y conservación permanente de documentos electrónicos, que evidentemente será discutible y mejorable pero que está realizado con racionalidad y a la vez atrevimiento en la innovación.

¿No sería posible plantear en nuestro país algo así, realizado con calma y sin sujeción a las urgencias políticas? Con la colaboración de las diferentes partes involucradas, fundamentalmente expertos en las nuevas tecnologías, juristas, administrativistas y archiveros. Entre todos podría tratar de buscarse una solución meditada para contribuir a encontrar alternativas a este gravísimo problema de la forma más racional posible. Eso es precisamente lo que nos gustaría que esta publicación pudiera impulsar, y por eso realizamos desde aquí una llamada de atención a los responsables de las Administraciones Públicas para que se busquen fórmulas abiertas para afrontar el problema. La Administración electrónica necesita de forma urgente herramientas y personal cualificado, necesita criterios y sistemas para la conservación de los nuevos documentos, si es queremos que dentro de unos cuantos siglos lo que hoy estamos produciendo en los inicios de esta nueva era pueda ser consultado igual que ahora consultamos los papeles y los pergaminos de la Edad Media.

1. Algunos conceptos

Para centrar el problema y para tratar de evitar confusiones por problemas terminológicos, conviene que comencemos por presentar algunas definiciones básicas. Esto es especialmente recomendable en un tema que se aborda desde distintas perspectivas en las que las palabras pueden tener significados muy distintos, incluso las más usadas. Es evidente que no es lo mismo un «archivo» o un «registro» para un informático que para un archivero. Especialmente nos interesa precisar «documento» y «documento electrónico», que incluso tienen significados muy diferentes en campos tan cercanos como el de los archivos y las bibliotecas o centros de documentación.

1.1. *Documento*

¿Qué entendemos aquí por documento? ¿A qué tipo de documentos nos referimos? Evidentemente no a cualquier documento meramente informativo, un libro o un artículo de revista por ejemplo, sino al documento de archivo, al que refleja y es producto de la actividad de una persona o una institución. El CIA en su texto «Documentos Electrónicos. Manual para Archiveros»[13], nos presenta esta definición que acepta de su antecedente (Guide for Managing Electronic Records from an Archival Pespective»[14]:

[13] Consejo Internacional de Archivos. *Documentos Electrónicos. Manual para Archiveros*, p. 19.

[14] Consejo Internacional de Archivos. *Guide for Managing Electronic Records from an Archival Perspective*, p. 25.

> «Información registrada producida o recibida durante la iniciación, desarrollo o terminación de una actividad personal o institucional y que incluye contenido, contexto y estructura suficientes para servir como testimonio de esa actividad»

Los documentos no son sólo portadores de información, son reflejo y evidencia de una actividad personal o institucional, son productos de una actividad administrativa, notarial, judicial... No importa el soporte en que se plasman, que lógicamente puede ser cualquiera (desde el pergamino a los actuales discos de almacenamiento masivo), ni el formato (texto, imagen, sonido...).

1.2. *Documento electrónico*

Siguiendo en esa línea el calificativo de electrónicos solamente completaría la definición anterior en el sentido de que nos referimos a documentos generados, conservados y transmitidos a través de medios electrónicos.

Ahora bien, la actual legislación ha optado por una definición más restrictiva y el artículo 3.5 de la Ley de Firma Electrónica[15] «considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente»[16].

El **documento electrónico**, por tanto, participa de todas las características del documento convencional, excepto en lo que queda afectado por el soporte o el sistema de creación, transmisión y conservación: puede tener el mismo valor legal, estar sometido a las mismas reglas de tratamiento archivístico a lo largo de su ciclo vital y formar parte del patrimonio histórico documental de la Nación. Sin embargo hay algunas diferencias muy importantes que desde el punto de vista archivístico conviene resaltar desde el primer momento porque afectan enormemente a todo el sistema de tratamiento y conservación.

1.3. *Posibilidad de separación entre contenido y soporte*

La primera de estas diferencias es la posibilidad de separación entre contenido y soporte. Mientras que en el documento tradicional el contenido estaba indisolublemente ligado al soporte hasta el punto de que la destrucción del soporte supondría la desaparición del propio documento, en el documento electrónico sí es posible esta separación, pudiéndose transferir el contenido a otro u otros soportes[17]. Electrónicamente el documento es un conjunto de

---

[15] LEY 59/2003, de 19 de diciembre, de firma Electrónica (BOE n. 304, de 20 de diciembre de 2003).

[16] Una discusión más completa sobre este tema puede verse en este mismo número en los artículos de Guillermo Ormazábal y de Margarita Vázquez de Parga.

[17] Seguimos en estos aspectos los estudios de Charles Dollar, auténtico pionero en estos estudios.

datos codificados en forma binaria, creados, organizados y manejados por un software específico y con unos comandos que dan el formato concreto al documento. El documento sólo adquiere realidad propiamente al presentarse en pantalla o papel.

1.4. *Diferenciación entre estructuras física y lógica*

Esta separación nos lleva a la diferenciación entre la estructura física y la estructura lógica del documento. De hecho la estructura física y la apariencia que presentaba el documento, reflejada en temas como el papel, las filigranas, la tinta, las firmas, los sellos... nos proporcionaba alguno de los más importantes criterios para la valorar la autenticidad y originalidad del documento. Pero en el documento electrónico la **estructura física** es dependiente del software y del hardware de creación, y por ello puede cambiar cuando por motivos de seguridad, de refresco de tecnología, de cambio de sistema... tiene que ser nuevamente grabado o migrado.

Puesto que la estructura física del documento electrónico es variable y no visible a simple vista, no puede tener la misma eficacia que tiene en el documento tradicional, en el que es pieza clave para conocer su autenticidad. Como alternativa puede atenderse a la conservación de la **estructura lógica** del documento, que incluye las relaciones entre distintos elementos internos (párrafos, márgenes, formatos...), que se conserva en forma de dígitos binarios (símbolos, comandos, formatos, software) pero que debe incluir información suficiente para que el usuario pueda de alguna forma representar en una pantalla o en un papel el documento con las características físicas con las que se creó.

1.5. *Forma de codificar el documento*

La forma de codificar el contenido del documento es otra de las importantes características diferenciadoras. Mientras un documento tradicional usaba unos símbolos visibles (el alfabeto, los números arábigos o romanos, los sellos o signos...), los sistemas electrónicos utilizan una codificación adicional más compleja (código binario, encriptación, sistemas de compresión, formatos de ficheros...), que exigen para poder visualizar el documento unas herramientas de hardware y de software que además están sometidas a abundantes problemas por la falta de normalización, la obsolescencia, etc.

En este sentido la **firma electrónica** es un elemento muy significativo: nada tiene que ver con una firma tradicional, realizada personalmente con su propia mano por el autor u otorgante del documento. Aunque se siga llamando firma, es en realidad un conjunto de datos asociados al documento, generados por un programa de software y codificado por un sistema de encriptación de clave pública.

1.6. *Una nueva diplomática*

Como consecuencia de estas variantes, algunos aspectos de la diplomática tradicional pierden fuerza a la vez que surgen nuevas herramientas que nos llevan a una nueva diplomática para el documento electrónico. Por ejemplo la «**tradición documental**»: original y copia son conceptos que cambian su significado, cuando el documento puede ser copiado múltiples veces manteniendo sus características y haciendo que todas las copias sean idénticas a la primera. Además los documentos electrónicos son «virtuales» y sólo adquieren realidad desde el punto de vista humano cuando se visualizan en una pantalla o en un papel, lo cual puede hacerse infinitas veces y en infinitos lugares.

En cambio la facilidad en la copia, borrado, modificación o manipulación del documento en el entorno electrónico sin dejar huellas (voluntaria o involuntariamente, con o sin mala intención), exige que se potencien otros criterios, especialmente los de Autenticidad, Integridad, Fiabilidad y Disponibilidad.

1.7. *Autenticidad*

El concepto de autenticidad[18] se convierte en el más importante. Es éste un criterio utilizado para la documentación tradicional en papel pero que aquí se vuelve aún más significativo. Según el Estándar ISO15489-1 (punto 7.2.2.), *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*[19]. Nada más y nada menos, he aquí el meollo de la cuestión: ¿cómo asegurase de la autenticidad de un documento electrónico? ¿cómo saber que un documento electrónico es auténtico? En última instancia este es el objetivo de los archivos: gestionar, conservar y tener accesibles documentos «auténticos», seleccionando aquellos que tengan valor de permanencia para el futuro. ¿Cómo realizar estas tareas adecuadamente con los documentos electrónicos?

1.8. *Integridad, fiabilidad y disponibilidad*

Complementarios de la autenticidad son los conceptos de fiabilidad e integridad. La **integridad** se refiere al hecho de que el documento esté completo

---

[18] El Consejo Internacional de Archivos elaboró para la UNESCO dos informes con el título de *Authenticity of Electronic Records*. El primero en 2002 fue elaborado por el Comité sobre Asuntos Legales presidido por el sueco Claes Gränström, y el segundo fue redactado en 2004 por Laura Millar, del Internacional Records Management Trust.

[19] International Organization for Standards. *ISO 14489-1, Information and Documentation-Records Management*. Geneva: international Organization for Standards, 15 September, 2001. Las citas se han tomado de la traducción española, edición de AENOR, 2006, p. 12.

y no haya sido alterado, en cuyo caso ya no sería auténtico, y la **fiabilidad** se refiere al hecho de que el contenido del documento pueda *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*[20], esto es que pueda ser utilizado como prueba.

La **disponibilidad** por su parte se refiere a la posibilidad de que el documento sea localizable, recuperable, presentable e inteligible, lo que en el entorno electrónico no es un asunto de menor importancia por los problemas de software propietario, de falta de estándares, de deterioro de los soportes y de obsolescencia.

1.9. *Contenido y Contexto*

Otros conceptos a tener en cuenta son los de Contexto y Contenido. El **contenido** del documento es aquello que el documento nos transmite, independientemente de su presentación: el mensaje o la información propiamente dicha. Más complejo es el concepto de contexto, que si tiene gran relevancia en el mundo de los documentos tradicionales tiene aún más en el mundo de los documentos electrónicos.

El **contexto** del documento hace referencia a todas las relaciones con su entorno jurídico, administrativo y archivístico (procedencia, funcionalidad, procesos, sistema de archivo, etc.), y si hablamos de documentos electrónicos también el sistema de creación, procesado, accesibilidad y almacenamiento.

2. Riesgos y problemas

Son muchos los riesgos que en la actualidad amenazan a la conservación de documentos electrónicos, especialmente de aquellos que tienen valor permanente y han de conservarse para generaciones futuras. La posibilidad de «amnesia digital» de que antes hablábamos para el período cronológico en que nos encontramos es real. El mundo de las nuevas tecnologías ha hecho explosión, está en crecimiento exponencial y todavía no se ha logrado asentar algunos conceptos y estrategias básicas. Veamos algunos de estos riesgos y problemas:

2.1. *La durabilidad del soporte*

La conservación del documento ha sido un problema constante para los responsables de los archivos. Las condiciones ambientales, los insectos bibliófagos..., han sido desde siempre objeto de preocupación ya desde la antigüedad,

[20] *Ibidem*, p. 13.

y en España tenemos algunos ejemplos históricos en Archivos como el de Simancas[21], el de Indias[22] y otros. Por eso no es de extrañar que en el momento que empiezan a llegar a los archivos las primeras cintas magnéticas surja la preocupación: si todavía podemos consultar documentos con muchos siglos de antigüedad, ¿qué ocurrirá con los documentos en nuevos soportes? ¿durarán siquiera tanto como los papeles o los pergaminos medievales que conservamos en nuestros archivos históricos?

Parece claro que no. En relación con la conservación de la información a lo largo de la historia podemos distinguir dos líneas contrapuestas. Una crece de manera exponencial, es la que corresponde a la cantidad de información que podemos guardar: desde unos cuantos caracteres en una tableta de arcilla a los miles de caracteres que aparecen en un fotograma de microfilm o los billones que nos proporcionan los formatos magnéticos y ópticos. La otra en cambio, la duración prevista del documento, disminuye a marchas forzadas: desde los varios miles de años de las tabletas de arcilla de las civilizaciones mesopotámicas o los papiros egipcios, a los pocos años que podemos esperar de la consulta de alguno de los papeles que hoy imprimimos. Y todavía la menor duración estimada de cintas, disquetes y discos.

Los fabricantes no garantizan una larga duración para los soportes electrónicos, a pesar de algunos anuncios que se hicieron en su momento, que hablaban de longevidades centenarias. Lo cierto es que la fragilidad del soporte, la tasa de error en la lectura, etc., se presentan como una seria amenaza para el futuro. A pesar de todo esto, tras los estudios pertinentes, en 1994 los Archivos Nacionales de Washington (NARA) publicaron un documento técnico por el que se comenzaba a admitir el ingreso de documentos en disco óptico, hasta entonces no aceptado como soporte de archivo[23].

Pero lo cierto es que hasta el momento no hay realmente ningún soporte al que por su prevista «durabilidad» le podamos aplicar el carácter de «archivístico». Por tanto, si los soportes tienen una longevidad tan reducida habrá que buscar estrategias para conservar al menos la información: copia (en el mundo digital «conservar es copiar», se ha dicho), migración, refresco de tecnología, etc.

---

[21] La *Instrucción para el Gobierno del Archivo de Simancas*, expedida por Felipe II en 1588, en su capítulo 14 establece como una de las obligaciones del Archivero, en relación con los documentos, que *tenga siempre cuidado de que no les falten cubiertas y las ataduras necesarias, y que esten limpios y sacudidos de poluo, y barridos los aposentos, procurando, en quanto fuere posible, que no aya polilla, humidad ni ratones...* (Véase el facsímil, trascripción y estudio de José Luis Rodríguez de Diego, en la edición de la Instrucción realizada por el Ministerio de Cultura en 1989, en conmemoración del IV Centenario de esta Instrucción)

[22] Está bien documentada la insistencia de los «padres» del Archivo General de Indias en algunos aspectos de la conservación de los documentos, que nos ha dejado como resultado la maravillosa estantería de caoba y cedro macho, obra de Blas de Molner en los últimos años del siglo XVIII. Los materiales estaban elegidos por su resistencia al ataque de los insectos.

[23] *Digital Imaging and Optical Digital Data Disk Storage Systems. Long term access strategies for Federal Agencies.* NARA Technical Information Paper Nº 12.

2.2. *La obsolescencia*

Sin embargo el problema de la duración de los soportes no es en realidad el problema más importante, lo que de verdad es un grave problema en la actualidad es la obsolescencia.

Define la Real Academia de la Lengua el término de obsolescencia, como la «cualidad de obsolescente», y éste a su vez como lo «que está volviéndose obsoleto, que está cayendo en desuso». Para obsoleto, en su segunda acepción, nos dice: «Anticuado, inadecuado a las circunstancias actuales», breves definiciones para unos conceptos que han adquirido una trascendencia enorme en el mundo actual de nuevas tecnologías. Se trata de la caída en desuso de equipos, soportes y sistemas, no por su deterioro o mal funcionamiento, sino como consecuencia de la aparición de nuevos medios que mejoran las prestaciones de los anteriores, y que inducen a un rápido abandono de lo antiguo en busca de las últimas novedades.

La importancia de la obsolescencia en el mundo actual se debe al rapidísimo desarrollo que se está produciendo en las últimas décadas, lo que va acompañado sin duda de un importante trasfondo económico. Es consecuencia de la importancia de la investigación y la innovación en el mundo actual (los equipos informáticos concretamente pueden multiplicar su capacidad de proceso o de almacenamiento en sólo unos meses), pero también consecuencia de la competencia en los mercados: para triunfar hay que presentar novedades antes de que lo hagan los demás. El triunfo de una línea de mercado puede obligar a abandonar otra, dejando multitud de productos obsoletos (recordemos la vieja lucha de los sistemas de video Beta y VHS, que se decantó por este último cuando era previsible la victoria del primero). Esto además puede completarse con estrategias empresariales como la de ofrecer productos incompletos y más baratos hasta asentar una línea de mercado, para presentar luego los productos más completos y caros. O la de vender productos que en la práctica tienen una fecha de caducidad, como sucede con los teléfonos móviles. O la de no ofrecer repuestos para sistemas antiguos u ofrecerlos a un precio muy elevado, para obligar a cambiar a los nuevos productos.

Se ha llegado a decir que la «obsolescencia es el motor de la economía de mercado». Pero en el mundo de los archivos puede ser tan peligrosa o más que la acidez del papel o los insectos bibliófagos. Por eso, la necesidad de establecer estrategias en los archivos para abordar el problema se viene afirmando desde hace ya bastantes años. Pero evidentemente el problema está ahí y presenta algunas características complejas, que pasan en general por el «refresco» de la tecnología, por la migración de equipos, soportes y sistemas, o por el copiado de la información y actualización de formatos y software... Ello supone siempre un esfuerzo económico muy importante. Estamos sometidos a una cadena permanente de actualización de productos informáticos, y aunque cada escalón conlleve mejores prestaciones, no siempre nos ofrece ventajas aplicables ni por supuesto siempre necesarias: nuevas compras y nuevos gastos.

La afirmación que suelen hacer los fabricantes de que las nuevas versiones de sus productos tienen «compatibilidad hacia atrás», esto es, que es posible utilizar los documentos, ficheros o bases de datos, no es cierta al 100%. Casi siempre se producen algunos cambios que hay que tener en cuenta, y por supuesto la compatibilidad entre productos de distintos fabricantes es menos habitual.

Si las nuevas versiones del software y hardware pueden modificar alguna de las características de los documentos, ¿cómo puede influir esto en la conservación a largo plazo que exigen los documentos de archivo?, ¿puede asegurarse la autenticidad, fiabilidad, integridad y disponibilidad de los documentos en el entorno electrónico?, ¿hasta qué punto condiciona esto nuestras funciones y operativas habituales, especialmente en la conservación a largo plazo?, ¿podrán consultarse en el siglo XXV los documentos generados hoy electrónicamente, igual que nosotros consultamos los documentos del siglo XV?

2.3. *Los problemas de seguridad*

Los problemas de la obsolescencia se hacen especialmente complejos en lo que respecta a la confidencialidad de las informaciones. Si la confidencialidad y el secreto han sido siempre un importante elemento en la gestión de documentos y en la función de archivo, estas características se hacen absolutamente imprescindibles en el mundo de la documentación electrónica en red. Sin confidencialidad desaparecería todo tipo de tramitación y comercio electrónico y la seguridad de las naciones sería imposible.

Para proteger la confidencialidad de las comunicaciones y la información electrónica, en los últimos tiempos ha crecido de forma exponencial el uso de sistemas criptográficos que permiten cifrar la información para impedir que pueda ser «entendida» por cualquier observador no autorizado. Es mucho lo que se ha avanzado en los últimos tiempos en este terreno, desde que la criptografía dejó de estar prácticamente confinada para usos de carácter militar, y especialmente desde que en 1976 Whitffield Diffie y Martin Hellman idearon los principios de la criptografía de clave pública (PKI) que sirve de base para la firma electrónica.

El problema es que los sistemas de encriptación avanzan a pasos agigantados, utilizando algoritmos cada vez más complejos y con claves más largas, pero a la vez que se desarrollan nuevos sistemas criptográficos avanzan las técnicas de análisis criptográfico que tratan de romper la seguridad de los sistemas. ¿Quién no ha oído hablar de los *hackers* que logran entrar en alguno de los secretos y «amurallados» centros de información de carácter militar o bancario?. Y es que muchas veces «los malos» son más rápidos y hábiles que «los buenos».

Esta continua carrera por la seguridad se está viendo en los últimos tiempos vigorizada por las perspectivas de la computación cuántica. Si el ordena-

dor cuántico termina por construirse, todos los sistemas de seguridad actuales perderán su valor, pues podrán ser fácilmente derribados por la capacidad de los nuevos procesadores. Es verdad que también podrá crearse una criptografía cuántica[24] supuestamente inviolable, pero todo esto no hace más que confirmar el problema del que venimos hablando, la obsolescencia, en este caso afectando a la seguridad de la información.

¿Cómo afectará todo esto a los documentos guardados en el Archivo electrónico? ¿Será preciso estar permanentemente involucrados en una carrera para «re-encriptar» cada muy poco tiempo la información confidencial con nuevas herramientas? ¿Cómo afecta todo esto al valor legal de los «documentos»?

2.4. *Problemas en la firma electrónica*

Hay un ejemplo extremo de la problemática de la obsolescencia en general y en los temas de seguridad en particular, el de la **firma electrónica**[25]. La firma electrónica se basa fundamentalmente en dos operaciones tecnológicas: la realización de un resumen (*hash*) del documento que se va a firmar, y la encriptación del mismo. El *hash* es en realidad una especie de huella que se realiza con complejos algoritmos matemáticos y cuyo resultado es diferente para cada documento. Cualquier mínima modificación en el documento, una simple coma o un acento o un espacio, daría un nuevo *hash*. Este resumen, codificado con un algoritmo de clave pública, constituye la firma digital del documento en cuestión. Pues bien, la obsolescencia puede hacer que la migración del documento, ante la llegada de nuevo software, produzca determinadas mutaciones en el documento original con lo que el *hash* sería distinto y la firma carecería de valor.

Por otra parte el sistema de cifrado, para evitar que el *hash* pueda ser descifrado con facilidad, también tendrá que evolucionar permanentemente hacia claves mas largas y algoritmos mas complejos, lo que igualmente incidirá en la pérdida de valor de la firma electrónica.

Estos problemas, unidos a otros derivados de la caducidad de los certificados y de las propias autoridades de certificación a lo largo de períodos relativamente cortos, hace, como veremos, que los archivos más avanzados estén desestimando la aceptación de documentos con firma electrónica, tratando de

[24] En la prensa de los últimos meses pueden verse entrevistas con Juan Ignacio Cirac, investigador español, premio Príncipe de Asturias, que dirige en Alemania uno de los grandes proyectos sobre este futuro ordenador y sus posibilidades con respecto a la criptografía.

[25] Puede consultarse sobre este tema el informe de Jean-Francois Blanchette para la Dirección de los Archivos de Francia, *La conservation de la signature electronique. Perspectives Archivistiques*, 2004 http://www.archivesdefrance.culture.gouv.fr/fr/circulaires/rapport_signature%E9lectronique_archivage1.pdf y también el artículo de Jordi Serra, «La firma electrónica y archivo digital». En *Primeres Jornades de Signatura Electrònica*. Agència Catalana de Certificació (CATCert). Barcelona, 10-11 de junio de 2004. http://eprints.rclis.org/archive/00002602/01/CATCERT_2004.pdf

garantizar la autenticidad del documento por otros medios, especialmente a través del propio sistema de gestión de documentos.

2.5. *El desconocimiento por parte de los profesionales*

Hay otro problema muy importante a tener en cuenta, y tiene que ver con los profesionales, tanto en los archiveros como en los expertos en nuevas tecnologías: el desconocimiento de las distintas vertientes del problema que se nos viene encima.

Los archiveros, aunque esto está cambiando con las nuevas generaciones, carecen a menudo de los conocimientos necesarios del mundo de la informática y las telecomunicaciones. Carecen de una visión general de lo que está sucediendo y de hacia dónde puede avanzarse en un próximo futuro. Evidentemente no se espera de ellos que sean técnicos informáticos, sino que dominen las técnicas de archivo. Pero de la misma forma que antes se estudiaba en profundidad la paleografía y la diplomática, sin tratar de ser los mejores expertos teóricos de estas disciplinas, y nos referíamos a ellas como «ciencias auxiliares» de la archivística por su interés práctico para nuestros trabajos, ahora tenemos que conocer con bastante profundidad las nuevas herramientas tecnológicas, que son ya imprescindibles para casi todo.

La escasez de estos conocimientos produce incapacidad para aportar criterios en el mundo de los nuevos documentos y para plantear correctamente los problemas ante la Administración por una parte y ante los técnicos encargados de buscar alternativas. Sólo conociendo en cierta profundidad lo que la tecnología nos puede aportar, podremos plantear correctamente nuestros requerimientos, cometeremos menos errores y no esperaremos soluciones milagrosas. La ignorancia induce además en los profesionales del archivo un cierto complejo de inferioridad que imposibilita para un buen trabajo.

Pero el problema no está sólo en los profesionales de los archivos. Las tecnologías están invadiendo todo el mundo de la información. Ofrecen herramientas muy potentes y ayudan a manejar grandes cantidades de datos de formas impensables hace sólo unos años. Pero sus profesionales, los técnicos en informática y comunicaciones, están involucrados en un acelerado proceso de cambio y carecen de algunos conocimientos y criterios necesarios para tratar la documentación de Archivo, que tiene unos valores diferentes de los puramente inmediatos o crematísticos, y que exigen un tratamiento más sosegado y con perspectiva a largo plazo, de carrera de fondo. Al informático que está en el filo de los nuevos avances, en las urgencias del día a día, atento a las novedades, le resulta muy lejano el mundo más reposado de los archivos, siempre pendiente de la conservación permanente como garantía de derechos y deberes y como información para la historia.

Esta doble debilidad en los profesionales provoca abundantes problemas, que en última instancia se plasman en la falta de un lenguaje común y en la falta de un buen entendimiento entre las partes.

¿Qué necesitamos por tanto? Buscar un punto de encuentro, las diferentes partes deben conocer más profundamente los intereses de las otra para poder dialogar de igual a igual y encontrar así las soluciones adecuadas. No es fácil el entendimiento. Y sin embargo es imprescindible.

2.6. *Las políticas de la Administración electrónica*

Los problemas de falta de entendimiento entre profesionales se complican a la hora de diseñar y poner en marcha la Administración electrónica. Los responsables de las administraciones están convencidos, con razón, de la importancia de las nuevas tecnologías. Aunque con resultados bastante desiguales, a lo largo de los últimos tiempos son muchos los proyectos que se han iniciado para impulsar la sociedad de la información, las nuevas tecnologías y la administración electrónica, tanto desde el punto de vista europeo como español.

Los costes de poner en marcha la nueva administración son sin duda elevados. Pero no suele ser un problema en general la realización de inversiones en estas materias. Las autoridades no ponen dificultades a la hora de invertir en la adquisición de equipamiento. ¡Cuántos equipos no se han comprado en diferentes centros para utilizar sólo una mínima porción de sus posibilidades o incluso para tenerlos arrumbados a la espera de que llegue otro que lo sustituya!. Tampoco a la hora de poner en marcha proyectos brillantes, que puedan tener resonancia pública, aunque muchas veces sean rápidamente abandonados al siguiente cambio político.

Pero es más difícil encontrar proyectos serenos, ambiciosos y madurados, estrategias coherentes y de largo alcance, libres de los avatares políticos y que puedan llevarse hasta el final con participación de todos los sectores implicados. El Consejo Superior de Informática ha ido poniendo en marcha algunos proyectos puntuales de interés[26], que podrían enmarcarse en una política más amplia de modernización al convertirse en el actual Consejo Superior de Administración Electrónica[27]. Ya hemos comentado antes que está en marcha el Anteproyecto de Ley de Administración Electrónica (ahora proyecto de Ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas), que será el paraguas en el que se enmarcarán todas estas actividades y proyectos. Pero desconocemos que haya hasta ahora una política global que incluya el proceso de archivo, con todas las implicaciones de conservación permanente y a largo plazo de los documentos, en la Administración electrónica.

Tal vez en esto influya también el viejo problema, tantas veces discutido entre los profesionales de los archivos, de la dependencia orgánica que los archivos tienen con el Ministerio de Cultura. Los aspectos puramente cultura-

[26] A destacar *Aplicaciones utilizadas para el ejercicio de potestades. Criterios de seguridad, normalización y conservación.* MAP, 2004.

[27] Regulado por Real Decreto 589/2005.

les de los Archivos, su pertenencia al patrimonio histórico del país son muy importantes. Pero no se pueden dejar de lado las otras funciones del Archivo, las funciones primarias. Si se primaran los aspectos jurídicos, administrativos, de eficacia en la gestión, de servicio al ciudadano..., así como el carácter «transversal» de los archivos en la Administración Pública, probablemente su dependencia orgánica debería pasar a Administraciones Públicas o a Presidencia del Gobierno.

3. Algunas herramientas

3.1. *Interoperabilidad, estándares y sistemas abiertos*

La interoperabilidad se ha definido como la condición mediante la cual sistemas heterogéneos pueden intercambiar procesos o datos. Es evidentemente una condición de suma importancia cuando se trata de acceso a información a través de sistemas informáticos y redes, y ha sido puesta sobre la mesa especialmente desde la llegada de Internet. La explosión de las nuevas tecnologías con el desconocimiento inicial del camino a seguir, así como la competencia brutal entre las distintas empresas y organismos del sector... condujo a la existencia prácticamente única de sistemas propietarios y a la dependencia tecnológica de determinados fabricantes. Había muchos formatos distintos y herramientas específicas para cada formato. En este entorno la obsolescencia tecnológica multiplicaba sus perjudiciales resultados.

Pero hoy está claro que éste no es el camino, sino que es preciso llegar a acuerdos consensuados para conseguir formatos únicos. Una de las más poderosas herramientas para enfrentarse a los problemas de la obsolescencia tecnológica y al software *propietario* es el uso de estándares generalmente admitidos. Si nuestros sistemas se sujetan a estándares, más fácil será en el futuro realizar migraciones a medida que vayan desarrollándose nuevos productos, nuevo software, nuevos soportes, etc. Los estándares abiertos, desarrollados por expertos de diferentes organizaciones con independencia y neutralidad, nos garantizan la libertad de elección, la independencia del fabricante, y el avance hacia la interoperabilidad.

El avance hacia la informática abierta, hacia el software libre, hacia los estándares abiertos, concita en la actualidad una opinión favorable generalizada por las diferentes ventajas que proporciona: flexibilidad, interoperabilidad, menor coste, facilidad para la evolución y el cambio, etc.[28] Por citar unos ejemplos significativo, recordemos el XML y sus desarrollos complementarios,

[28] Son muchos los ejemplos que podrían ponerse de la evolución hacia el uso de sistemas cada vez más abiertos. Por poner un ejemplo reciente, citamos la resolución del Parlamento de Dinamarca el pasado viernes 2 de junio del 2006, por la que ordena a su Gobierno el uso obligatorio de estándares abiertos en informática en la administración pública danesa a partir del 1 de enero del 2008.

impulsados por la W3C o el formato OpenDocument[29] del que se habla en profundidad en otro artículo de esta publicación, al exponer las actividades de los programas IDA e IDABC de la Unión Europea.

Aunque es evidente que, al menos hasta ahora los estándares sólo pueden ayudar a minimizar los riesgos de obsolescencia porque tienen también un periodo de vigencia relativamente reducido, de forma que ningún estándar puede considerarse definitivo porque ello impediría poder seguir evolucionando y avanzando.

3.2. *Los metadatos*

El mantenimiento a lo largo del tiempo de la estructura, el contenido y el contexto de los documentos en un entorno electrónico, con las condiciones de separación entre contenido y soporte y entre estructura física y lógica, exige conservar algunas informaciones complementarias relacionadas con el documento, que se conocen como metadatos, o datos sobre los datos. Aunque este concepto ha triunfado en los últimos años, no nos resulta lejano a los profesionales de la documentación, ya que buena parte de nuestro trabajo ha consistido desde siempre en describir, en inventariar, en catalogar... documentos, esto es en recoger datos sobre los documentos, en última instancia datos sobre los datos. Se trata por tanto de un concepto que ya existía, pero que ha hecho auténtica explosión en los últimos años, con la llegada de Internet y de la Web, como medio para ayudar en la realización de búsquedas más refinadas en los miles de millones de páginas. Las diferencias en la actualidad están en la mayor exigencia y precisión que se requiere, y en las herramientas automatizadas que facilitan el trabajo.

A través de los metadatos se puede recoger y conservar información sobre el contexto de creación y de tratamiento del documento (criterios de valoración, de selección, de acceso...), que nos ayudarán a gestionar los documentos electrónicos a lo largo de su ciclo vital, igual que hacemos con los documentos tradicionales.

¿Qué metadatos debemos conservar sobre nuestros documentos electrónicos? Está claro que en el momento globalizado actual no debemos ir por libre a la hora de seleccionarlos, sino que debemos atender a los estándares generalmente admitidos en el supuesto de que existan. Pero también en estos temas estamos en los comienzos, aunque hay algún punto de partida. El primer conjunto estándar de metadatos es el Dublin Core[30], un conjunto simple

[29] Véase en este número el artículo de Miguel A.Amutio «Acciones IDA de IDABD...». Información detallada sobre el tema en la página web de IDABD dedicada a la promoción del Open Document Exchange Format: http://ec.europa.eu/idabc/en/document/3439/5585#ODF

[30] El Dublin Core Data Element Set, creado por la Dublin Core Metadata Inicitative, puede descargarse en esta página http://es.dublincore.org/documents/dces/, y está for-

de 15 elementos pensado especialmente para los recursos presentes en la Web y que carece de elementos relacionados con las funciones archivísticas propiamente dichas (clasificación, valoración y selección, accesibilidad, etc.)

Más directamente preparado para la documentación de los Archivos, es el estándar de metadatos de los Archivos Australianos[31]. Se trata de un estándar completo, con toda la información necesaria (definiciones, relaciones entre elementos, condiciones de uso, ejemplos, etc.). Este estándar está compuesto por 20 elementos (8 de ellos obligatorios) y 66 subelementos[32].

También el MoReq ya citado incluye un amplio conjunto de metadatos específico para documentos electrónicos de Archivo. Y el Comité TC46/SC 11 de Archivos/Gestión de Documentos de la International Standard Organization (ISO) tiene en marcha un grupo de trabajo para llegar a una estándar internacional de metadatos[33]. Otro modelo es el METS o *Metadata Encoding and Transmission Standard (METS)*, mantenido por la Library of Congress, que utiliza esquemas XML[34].

3.3. *La migración*

La forma habitual de salvar los datos que corren riesgo de perderse por problemas de obsolescencia es la migración, o proceso de trasferencia de información desde la plataforma en riesgo a una plataforma nueva. Esta solución, que fue la primera en plantearse y utilizarse para la conservación de documentos de archivo, tiene un problema de coste (nuevos equipos, nuevo software, nuevo soportes, dedicación de personal, etc.). Pero tiene problemas mucho más importantes: el riesgo de pérdidas en el traspaso de la información, y las modificaciones en la funcionalidad y en la apariencia, lo que puede afectar a la estructura, al contenido y al contexto de los documentos.

La migración es un concepto que ha sido estudiado con cierta profundidad en algunos proyectos relacionados con la preservación de los documentos

mado por los siguientes elementos: Título, autor o creador, claves o materia, descripción, editor, otros colaboradores, fecha, tipo de recurso, formato, identificador, fuente, lengua, relación, cobertura y derechos.

[31] *Recordkeeping Metadata Standard for Commonwealth Agencies.* National Archives of Australia, 1999. Versión, 1.0. http://www.naa.gov.au/recordkeeping/control/rkms/rkms_pt1_2.pdf

[32] Los elementos son: agente (entidad o individuo responsable de alguna acción o uso del documento), gestión de derechos (regulación del acceso y uso del documento), título, materia, descripción, lengua, relación (entre el documento y otros, o entre conjuntos de documentos), cobertura (características jurisdiccionales, espaciales o temporales), función (función o actividades que se documentan), fecha, tipo, nivel (nivel de descripción o agregación), formato, identificador del documento, historia de la gestión, historia del uso, historia de la preservación, localización, información sobre cuestiones de selección y eliminación, y mandato (regulación y legislación correspondiente)

[33] http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4718

[34] http://www.loc.gov/standards/mets/

electrónicos. Análisis del tema pueden encontrarse Charles Dollar[35], en el Modelo de Referencia OAIS[36], o en el proyecto CAMiLEON[37].

La migración (y las herramientas cercanas como el refresco, la replicación, la recreación...) puede resolver alguno de problemas de obsolescencia en el día a día de los sistemas, pero por sí misma no resuelve los problemas de la permanencia de los documentos a largo plazo, además de ser costosa en tiempo y dinero, y exigir una cadena de migraciones permanentes para el futuro. Por eso se ha hecho precisa la búsqueda de otras herramientas estratégicas.

3.4. *La emulación*

Una de las alternativas que se han promocionado en los últimos años con objetivos de conservación de información digital es la **emulación,** entendida como «recreación en hardware actual del entorno técnico necesario para visualizar y usar objetos digitales de tiempos anteriores»[38].

Mientras la estrategia de migración se basa en la continua adaptación del documento original para que pueda ser usado por la nueva tecnología, la estrategia de emulación, se apoya en la idea de mantener el documento en su estructura original y a la vez emplear herramientas de software que permitan visualizar en el futuro el documento tal como era en el momento de su creación. En realidad la emulación se basa en la idea de que la única forma de mantener la autenticidad e integridad de un documento a lo largo del tiempo es continuar ofreciendo acceso en su entorno original (su sistema operativo y software original).

El término «emulación» se usa en informática para referirse al conjunto de técnicas que permiten usar un equipo o un programa en lugar de otro para conseguir los mismos efectos que con el equipo o programa original. «Emulación» no es «simulación», un simulador de vuelo no consigue los mismos efectos que un avión, no vuela, sólo representa o simula las condiciones del vuelo. Las empresas informáticas han vendido tradicionalmente «emuladores» de otros equipos o programas, propios o de otros fabricantes (lo que puede plantear problemas de derechos), por ejemplo emuladores de Apple Macintosh que corren bajo MS Windows. Estos emuladores no representan o fingen ser lo que no son, sino que logran producir, en un entorno distinto, los mismos efectos que el producto original.

---

[35] Charles Dollar. *Authentic Electronic Records: Strategies For Long-Term Access.* Chicago: Cohasset Associates, Cop. 2002

[36] http://public.ccsds.org/publications/archive/650x0b1.pdf

[37] Véase el documento de Paul Wheatley, *Migration - a CAMiLEON discussion paper.* http://www.ariadne.ac.uk/issue29/camileon/intro.html

[38] David Holsworth y Paul Wheatley. «Emulation, preservation and abstraction». *RGL Diginews,* August 15, 2001, vol. 5. N.º 4 http://www.rlg.org/preserv/diginews/diginews5-4.html#feature2

Jeff Rothenberg[39] ha sido el principal defensor teórico de la emulación casi como una panacea de cara a la permanencia futura de los documentos electrónicos. Incluso se han puesto en marcha algunos proyectos importantes para desarrollar la idea, como el proyecto UVC, o Universal Virtual Machine, promovido por IBM[40], o el CAMiLEON (Creative Archiving at Michigan & Leeds: Emulating the Old on the New)[41] desarrollado por las Universidades de Michigan y de Leeds.

Admitiendo como premisa que es imposible conservar para el futuro el hardware original de creación del documento, para que el proceso de emulación funcione es preciso conservar el documento original, sin modificación, juntamente con el software original y con todos los metadatos correspondientes, y desarrollar emuladores del hardware que sirvió para generar el documento. El reto por tanto será doble: por una parte crear emuladores del hardware en el momento en que el hardware está en uso, para poderlo comprobar (los promotores de la idea afirman que esto no es demasiado difícil), y a la vez mantener el emulador sin modificaciones una vez desarrollado[42]. Si un equipo puede emular siempre a su precedente, se podría disponer de una cadena en que cada equipo emulara a todos sus antepasados, con lo que el documento siempre se podría ver exactamente igual que fue creado.

Evidentemente queda mucho por resolver, pero para los teóricos de la emulación esta técnica es la única que permite mantener para el futuro la estructura, el contenido y el contexto de los documentos, incluyendo todas las informaciones correspondientes a los aspectos legales, procedimentales... tal como eran en su origen, de forma que dentro de 100 años, por ejemplo, un historiador del futuro pueda ver un documento de hoy en formato Word o una Hoja de Cálculo Excell tal como nosotros la vemos en nuestra versión actual. Además como estrategia para el usuario sería la mas simple y menos costosa de implementar.

---

[39] Jeff Rothenberg. *Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation.* CLIR, 1998
http://www.clir.org/pubs/reports/rothenberg/contents.html

[40] Raymond A. Lorie. «Project on Preservation of Digital Data». *RLG Diginews*, June 15, 2001. Vol. 5, n.º 3. http://www.rlg.org/legacy/preserv/diginews/diginews5-3.html#feature2

[41] http://www.si.umich.edu/CAMILEON/

[42] ¿Cómo se conseguiría esto? Se plantean varias estrategias: el «encadenamiento» de emuladores (si un ordenador –1– es emulado por su sucesor –2– y este a su vez por su propio sucesor –3–, el último emularía a todos los anteriores), el «rehosting» o realojamiento de los emuladores en las sucesivas plataformas, o la creación de una EVM (Emulation Virtual Machine), que sería una plataforma virtual en la que todos los emuladores que se desarrollen deberían funcionar. Esta EVM (que dicen podría desarrollarse sobre la base de algún proyecto ya existente como la JVM, Java Virtual Machine, o sobre la UVM, Universal Virtual Machine de IBM, por ejemplo), se iría instalando siempre en las nuevas generaciones de ordenadores que se adquieran.

3.5. *La* «canonicalización»

Es éste otro de los métodos que ha sido presentado como herramienta para la conservación de información digital a largo plazo. Se entiende por canonicalización el proceso de convertir datos que tienen varias posibles representaciones a la representación más estándar o «canónica», que en principio tiene más posibilidades de conservación futura. Un ejemplo simple sería la conversión a texto plano (ASCII) de un texto de un procesador cualquiera, a pesar de las pérdidas de formato, estilo, presentación...

Esta alternativa fue especialmente defendida por Clifford Lynch, Director de la Coalition for Nertwordked Information[43]. Ha sido desarrollada por la W3C, dentro de las operaciones de integración de la firma electrónica en el lenguaje XML, al incluir un «método de canonicalización» en el procedimiento de la *XML Signature*[44].

3.6. *El estándar OAIS, un modelo de referencia para archivos electrónicos*

Otra iniciativa a tener en cuenta por sus perspectivas futuras es el OAIS (Open Archival Information System), que ofrece un modelo de referencia para la preservación a largo plazo de la información, como garantía de accesibilidad en el futuro. Este modelo[45], que trata de conseguir el apoyo y la participación las más diferentes instituciones que conservan documentación digital (archivos, centros de documentación científica, bibliotecas digitales...), fue desarrollado por el CCSDS (Consultative Committee for Space Data Systems), y posteriormente aceptado como Norma ISO 14721:2003.

El OAIS ha sido aceptado e incorporado en importantes proyectos internacionales: el NARA entre los archivos, las Bibliotecas Nacionales de Holanda[46] y de Australia[47] entre las Bibliotecas, el National Space Science Data Center[48] de Estados Unidos, el proyecto CEDARS[49], el proyecto NEDLIB (Networked European Deposit Library), etc. También ha sido asumido como punto de partida por el proyecto InterPARES.

Se acepta generalmente que presenta un marco general conceptual, que al menos identifica los inicios de la hoja de ruta, incluyendo terminología y con-

---

[43] Clifford Lynch. «Canonicalization: A Fundamental Tool to Facilitate Preservation and Management of Digital Information». *D-Lib Magazine*, vol. 5, n.º 9, Sept 1999.

[44] *Guía Breve de seguridad*. W3C, World Wide Web Consortium http://www.w3c.es/Divulgacion/Guiasbreves/Seguridad

[45] http://public.ccsds.org/publications/archive/650x0b1.pdf

[46] http://www.kb.nl/site/sitemap-en.html, proyecto e-Depot

[47] http://pandora.nla.gov.au/overview.html

[48] Este centro de la NASA es quien en realidad inicia todo el proceso de creación del OAIS

[49] http://www.leeds.ac.uk/cedars/archive/archive.html

ceptos básicos, aunque evidentemente no ofrece aún las pautas detalladas que serían necesarias.

4. Las estrategias de los países más avanzados en gestión archivística de documentos electrónicos

Son pocos los países que han abordado con cierta profundidad el problema de la conservación archivística a largo plazo de los documentos electrónicos. Hagamos una pequeña revisión de alguno de sus planteamientos.

4.1. *Australia*

Australia dispone de un envidiable conjunto de herramientas de todo tipo (legislación, estándares, guías, software...) en el que quedan claramente definidas las obligaciones de las Agencias del Gobierno y de los Archivos Nacionales en lo que respecta a la producción y gestión de documentos. Y específicamente ha desarrollado un conjunto bastante completo de herramientas destinado a la gestión archivística de los documentos electrónicos a lo largo de su ciclo vital, incluyendo los aspectos de conservación permanente[50] (aproximadamente el 5% del total de los documentos generados por las Agencias del gobierno):

- Dispone en primer lugar de un amplio conjunto de leyes generales que afectan a los archivos y documentos, empezando por una Ley de Archivos[51].
- Además dispone de un completo marco de normas y buenas prácticas de gestión de documentos, sobre valoración, selección y eliminación, sobre conservación del papel, sobre instalaciones, etc., etc[52].
- Los documentos electrónicos están afectados lógicamente por todo este marco normativo. Pero además se ha desarrollado un conjunto de instrumentos legales, de normas, directrices, criterios... que atienden espe-

---

[50] La página web de los Archivos Nacionales de Australia contiene abundantísima información y permite conocer este tema con amplitud: http://www.naa.gov.au/

[51] *Archives Act 1983* (ley general sobre transferencias, selección y eliminación, custodia y acceso); *Freedom of Information Act 1982* (acceso); *Privacy Act 1988* (datos de carácter privado); *Evidence Act 1995* (criterios sobre la validez probatoria de los documentos); *Electronic Transactions Act 1999.*

[52] Citamos algunos de estos instrumentos: la norma *Australian Standard for Records Management,* AS ISO 14489, el Manual DIRKS: A Strategic Approach to Managing Business Information (2001), *el Recordkeeping Metadata Standard for Commonwealth Agencies (1999),* un thesaurus, *Keyword AAA: A Thesaurus of General Terms,* etc.

cíficamente a los aspectos «electrónicos» de los documentos: la autenticidad, la firma electrónica, la seguridad, la conservación permanente... Una información de carácter general sobre todo el proceso puede verse en el *Digital Recordkeeping Guidelines for Creating, Managing and Preserving Digital Records* (2004)[53]. Mas recientes son las *Functional Specifications for Electronic Records Management Systems Software (2006)*[54] que son completadas por *Guidelines for Implementing the Functional Specifications for Electronic Records Management Systems Software (2006)*[55].

- El proceso, que afecta a todo el ciclo de vida de los documentos en las diferentes agencias del gobierno, se completa con una detallada estrategia de conservación permanente en los Archivos Nacionales de los documentos electrónicos que cumplan los requisitos para su conservación a largo plazo por tener carácter histórico (Proyecto *e-Permanence*).

En la práctica esta estrategia se basa en la conversión de los documentos electrónicos a ficheros en formato abierto, basados en estándares y evitando todo tipo de software propietario. Para ponerlo en marcha han desarrollado herramientas de software que permiten realizar el proceso de conversión de los ficheros originales a formatos abiertos (XML) y que pueden también realizar la exportación de los ficheros ya convertidos para su presentación en el formato original.

Los productos de software desarrollados están a libre disposición para su descarga en la web de los Archivos Nacionales[56], especialmente el programa Xena (XML Electronic Normalising of Archives). El conjunto del proceso dispone de varias fases, con operación en redes independientes y espacios físicamente diferenciados: Cuarentena (control del estado de los documentos, integridad, virus...), Preservación (conversión a formatos abiertos con el software Xena) y Almacenamiento (conservación definitiva).

De la experiencia australiana queremos destacar algunas enseñanzas importantes:

- La normalización es la línea principal de trabajo. La solución buscada se basa en la conversión de los documentos electrónicos a un formato abierto antes de su conservación definitiva en el Archivo. El formato elegido es el formato XML, hoy generalmente aceptado como formato para conservación de las estructuras de los documentos.
- Para mantener la información de contexto se emplean los metadatos incluidos en su propio estándar.

[53] http://www.naa.gov.au/recordkeeping/er/guidelines.html
[54] http://www.naa.gov.au/recordkeeping/er/erms/ERMSspecifications.pdf
[55] http://www.naa.gov.au/recordkeeping/er/erms/guidelines.html
[56] http://xena.sourceforge.net/node/2

- No se aceptan documentos encriptados, lo que evidentemente lleva al olvido de la firma electrónica, al reconocer por una parte que en el momento de la transferencia de los documentos firmados al archivo las firmas electrónicas[57] habrán perdido normalmente por el paso del tiempo su funcionalidad, y por otra, que los elementos que la conforman no pueden ser mantenidos de forma permanente por el Archivo[58].
- La intervención de los archivos y de sus profesionales en todo el proceso de gestión documental desde el inicio del diseño de los propios sistemas, encuadrando así la gestión de documentos electrónicos en las mismas vías que los documentos convencionales, aunque atendiendo a las características propias del medio electrónico.

4.2. *Canadá*

Al igual que en Australia, los Archivos Nacionales de Canadá tienen un importante papel en todo lo relacionado con los documentos de la Administración Pública, apoyados en lo determinado por el artículo 12 (1) de la reciente *Library and Archives Canada Act* (2004)[59]: ningún documento bajo el control de una institución del gobierno puede ser destruido sin el consentimiento del *Librarian and Archivist of Canada*[60].

También dispone Canadá de una amplia legislación y de un importante conjunto de normas, guías, etc. sobre la gestión de archivos en general y sobre los documentos electrónicos en particular[61]. Uno de los principales movimientos teóricos para buscar solución a los problemas planteados por los nuevos documentos es el Proyecto InterPARES (The International Research on Permanent Authentic Records in Electronic Systems), desarrollado en la Universidad de British Columbia (Canadá), que ha proporcionado un abundante arsenal de información a los profesionales[62].

---

[57] El Gobierno Australiano puso en marcha en 1998 el Gatekeeper, estrategia y marco legal en el que se encuadra el uso de firma electrónica con infraestructura de clave pública.

[58] National Archives of Australia (2004) «RecordKeeping and Online Security Process: Guidelines for Managing Commonwealth Records Created or Received Using Authentication or Encryption» http://www.naa.gov.au/recordkeeping/er/Security/recordkeeping_online_security.pdf

[59] «No government or ministerial record, whether or not it is surplus property of a government institution, shall be disposed of, including by being destroyed, without the written consent of the Librarian and Archivist or of a person to whom the Librarian and Archivist has, in writing, delegated the power to give such consents».

[60] Otras importantes leyes relacionadas con los Archivos son *Privacy Act, Access to Information Act, Personal Information Protection and Electronic Documents Act, 2000.*

[61] Algunas herramientas canadienses para gestión de documentos en esta dirección: http://www.collectionscanada.ca/information-management/002/index-e.html

[62] La información más general del proyecto puede consultarse en la página web del mismo: http://www.interpares.org/

Los Archivos Nacionales de Canadá tampoco aceptan los documentos electrónicos encriptados y consecuentemente tampoco los acompañados de firma digital. La encriptación en los documentos transmitidos electrónicamente, dice una Guía sobre documentos cifrados y firmados digitalmente[63], es como el sobre de los documentos en papel: no forma parte integral del documento, sólo sirve para su envío confidencial.

Los Archivos Nacionales reconocen no tener capacidad para re-verificar la firma electrónica a lo largo del tiempo, por eso no pueden aceptarla al recibir documentos de las distintas instituciones del gobierno, aunque estén encriptadas de acuerdo con el sistema federal de PKI. En consecuencia la integridad y la autenticidad de los documentos se derivará de su ubicación dentro del sistema de gestión de documentos de la organización en cuestión, lo que otorga al Archivo y a sus profesionales una responsabilidad muy grande a lo largo de todo el proceso documental.

4.3. *USA*

El potencial tecnológico, económico y organizativo de los Estados Unidos también se refleja en los Archivos y en la gestión y conservación de los documentos electrónicos, con el NARA (National Archives and Records Administration) como punta de lanza. La legislación es amplia (partiendo de la Federal Records Act) y las competencias del NARA y del Archivero de los Estados Unidos muy precisas. Todo ello está incluido en las NARA Regulations[64], que forman parte del Code of Federal Regulations, y detallado en múltiples especificaciones y directrices, que reflejan además una larga tradición en el tratamiento y conservación de documentos electrónicos, ya que desde hace varias décadas se vienen incorporando documentos en soporte electrónico a los Archivos, como hemos visto con anterioridad. En esta regulación está claramente definida la responsabilidad de los Archivos (en sus distintos niveles) para ofrecer asistencia para la conservación de los documentos (incluyendo los electrónicos) de valor duradero.

Se distingue formalmente dentro del «paraguas» de la gestión de documentos (o Records Management), entre el ERM (Electronic Records Management) y el ERK (Electronic Records Keeping), refiriéndose el primero a la gestión automatizada o electrónica de documentos en soporte papel y el

---

[63] *Guidelines For Records Created Under a Public Key Infrastructure Using Encryption And Digital Signatures.* 2006. http://www.collectionscanada.ca/information-management/002/007002-3015-e.html

[64] *NARA Regulations.* Las normas que afectan a los documentos electrónicos están incluidas en el Subcapítulo 2 (*Records Management. Part 1234 Electronic Records Management*). Hay más información que afecta a los archivos en las partes del mismo Code of Federal Regulations que afectan al Federal Register y a la Information Security Oversight Office (ISOO) http://www.archives.gov/about/regulations/

segundo a la gestión propiamente dicha de documentos electrónicos. Estos sistemas deben asegurar la «autenticidad y la fiabilidad» de los documentos para cumplir las Leyes Federales o estatales relacionadas con la «evidencia»[65].

Los Archivos americanos siempre han tenido como una de sus principales líneas estratégicas el análisis teórico y la experimentación práctica de todo lo relacionado con las nuevas tecnologías y los documentos de archivo. Han hecho numerosas pruebas y redactado gran cantidad de textos profesionales. Asimismo han ido adaptando su estructura a las necesidades emergentes y en la actualidad están embarcados en un novedoso proyecto que se enmarca en el desarrollo de la E-Government Act: el proyecto ERA (Electronic Records Archives), que trata de construir un sistema completo, estructurado y dinámico de información que proporcione vías de conservación y acceso a los documentos electrónicos Federales y Presidenciales a través del tiempo. El esfuerzo económico, de coordinación, de participación de todo de colaboradores... es enorme. Pruebas en el San Diego Computer Center o en el US Army Research Laboratory están incluidas en el proyecto, que en 2006 se encuentra aún en desarrollo, aunque se esperan resultados importantes para 2007. Será muy importante estar al corriente de sus resultados[66].

La teoría americana asigna gran importancia al mantenimiento simultáneo del contenido, de la estructura y del contexto de los documentos, considerando vital mantener las tres características (lo que es más difícil que en el documento en papel) para que puedan mantener su valor probatorio. Si alguna de estas características se altera, la capacidad de los documentos para reflejar las actividades de una entidad disminuye.

Si esto se aplica a los documentos con firma electrónica, el mantenimiento de sus estructuras física y lógica implica la necesidad de conservar el equipo y el software que se han utilizado para realizar la firma, de forma que el documento pueda ser validado posteriormente[67]. El NARA, sin embargo no obliga a los organismos administrativos a conservar las estructuras física y lógica (manteniendo siempre el respeto al contenido y al contexto del documento). Pero en este caso deberán conservarse suficientes informaciones contextuales (metadatos) que documenten la existencia y la validez de la firma electrónica en el momento de la producción del documento (nombre del firmante, mecanismos de firma, etc.).

4.4. *La Unión Europea*

La Unión Europea viene trabajando también en el tema de los documentos electrónicos en diversos aspectos, aunque no parece que por el

[65] Federal Rules of Evidence: http://www.law.cornell.edu/rules/fre/

[66] Gran cantidad de informes técnicos sobre este proyecto pueden consultarse en l web del NARA http://www.archives.gov/era/research/research-publications.html

[67] National Archives and Records Administration. *Records Managament Guidance for Agencies Implementing Electronic Signature Technologies.* Washigton, D.C., 2000.

momento haya una estrategia completa que incorpore a todos los países que la forman.

En este mismo Boletín se presenta un artículo que expone detenidamente algunas de las líneas de trabajo, especialmente las referidas al avance hacia los documentos abiertos en los países miembros. También ha desarrollado algunos proyectos y producido algunas normas relacionadas con la firma digital[68] Estas iniciativas son difundidas en España a través del MAP y del Ministerio de Cultura.

Además la Unión Europea ha auspiciado el estudio de los problemas planteados por la llegada de los documentos electrónicos en el DLM Forum, que específicamente ha producido la importante Especificación MoReq, o Modelo de Requisitos para la Gestión de Documentos Electrónicos de Archivo[69].

Para su servicio interno la Comisión Europea dispone de una normativa sobre la gestión de documentos y especialmente los documentos electrónicos[70]. Y además ha producido un conjunto de herramientas informáticas válidas para la gestión de los documentos electrónicos (Adonis, Hermes, Ares, Nomcom...)[71].

5. Algunas preguntas

A lo largo de estas páginas (y esto quedará aún más claro en los artículos que siguen) hemos tratado de ofrecer una llamada de atención sobre el problema que los documentos electrónicos nos presentan, y la falta de una respuesta proporcionada por parte de las autoridades de la Administración. No hemos tratado de ofrecer soluciones sino de hacernos preguntas y de tratar de explicitar más claramente el problema.

¿Va o no va a haber continuidad entre los archivos con documentos en papel y los archivos con documentos electrónicos? ¿O va a quedar una tierra de nadie formada por un conjunto de años en los que la información se per-

---

[68] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica y Decisión de la Comisión de 14 de julio de 2003 relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo.

[69] La traducción española, realizada por un grupo de trabajo en el Ministerio de Cultura, puede verse en http://www.mcu.es/archivos/docs/moreq.pdf

[70] Decisión de la Comisión2002/47, de 23 de enero sobre gestión de documentos, completada con la Decisión 2004/563 sobre documentos electrónicos y digitalizados. Otros textos posteriores son las Implementing Rules on Registration (2003), Implementing Rules on Filing (2003), Implenting Rules on Preservation (2005) e Implementing Rules on electronic and digitised documentos (2005)

[71] Puede verse información en http://ec.europa.eu/transparency/edoc_management/informatic_en.htm

derá o se quedará sin alguna de las características fundamentales que garantizan su autenticidad?

¿Se van a asumir los riesgos que para la conservación permanente de los documentos electrónicos llevan consigo determinados aspectos como la obsolescencia tecnológica? ¿Se van a buscar soluciones, siguiendo los caminos ya iniciados en otros lugares? ¿Se van a tomar decisiones y a establecer estrategias sobre cómo han de crearse y conservarse los documentos electrónicos para mantener sus características básicas de integridad, autenticidad, etc.?

¿Afrontaremos los archiveros de verdad, sin miedos ni complejos, el reto que está en este momento planteado, o la conservación de los documentos electrónicos será tarea de otros profesionales diferentes, más cualificados en aspectos tecnológicos aunque tal vez sin asumir totalmente la visión histórica y cultural de los archivos?

¿Entenderán en algún momento las autoridades la doble vertiente que los archivos representan, la de herramienta en la gestión administrativa y la de institución cultural que conserva buena parte de las raíces de los pueblos? ¿Se reflejará esto en un cambio real en la administración archivística española en un futuro cercano?

¿Se contemplará en profundidad el papel de los archivos en la futura administración electrónica, comenzando por una redacción más acorde de la Ley en proyecto? ¿O seguiremos recibiendo en los archivos soportes informáticos sin orden ni concierto, con todo tipo de formatos, muchos de ellos ya obsoletos? ¿Se tendrá en cuenta la pertenencia de los documentos al Patrimonio Histórico de la nación y por tanto todas las responsabilidades sobre la correcta conservación, eliminación en su caso, derechos de acceso, etc.?

¿Se dispondrá algún día de una legislación archivística adecuada que precise las responsabilidades sobre la conservación de los documentos, incluyendo los nuevos documentos electrónicos? ¿Cuántos años más esperaremos una Ley de Archivos y su correspondiente desarrollo reglamentario? ¿Asumirá de verdad la proyectada Ley de Administración Electrónica (o de Acceso de los ciudadanos a la información electrónica) el ciclo vital de los documentos electrónicos y la necesidad de un sistema de archivos coherente? ¿Se encargará la tarea de control de la conservación permanente de los documentos electrónicos a una institución archivística de carácter nacional, como el AGA por ejemplo, tal vez dependiendo del Ministerio de la Presidencia o del de Administraciones Públicas, dotándole con toda la autoridad pertinente para llevar a cabo su tarea (y por supuesto con los medios legales, técnicos y presupuestarios necesarios), como sucede en los países más avanzados? ¿O por el contrario, en un país que tiene una de las mayores tradiciones archivísticas, iremos por libre y encargaremos el archivo de los documentos electrónicos a una «entidad pública empresarial», adscrita al Ministerio de Industria, Turismo y Comercio, como red.es?

¿Lograremos algún día tener una administración electrónica en la que el archivo forme parte integral del sistema desde el momento del inicio del pro-

cedimiento y de la producción de los documentos, y a lo largo de todo su ciclo vital, hasta el momento de la conservación definitiva de aquellos documentos que deban mantenerse de forma permanente por sus valores informativos, históricos y culturales?

El plazo para contestar a estas y otras preguntas se reduce cada vez más.

ARTÍCULOS

Acciones de IDA e IDABC en materia de promoción del uso de los formatos abiertos de documentos y de actualización MoReq y los criterios de conservación

MIGUEL A. AMUTIO GÓMEZ*

RESUMEN: El impulso de la Administración electrónica lleva aparejado la producción, manipulación, visualización, intercambio y almacenamiento de documentos en soporte electrónico a gran escala. Este hecho hace necesario afrontar cuestiones tales como la gestión de los archivos de documentos electrónicos, la utilización de formatos abiertos de documentos que favorezcan la interoperabilidad, la libertad de elección, así como la accesibilidad a lo largo del tiempo y las pautas para asegurar la gestión de los documentos y su conservación. Este artículo expone la acción de los programas comunitarios IDA e IDABC en materia de promoción del uso de los formatos abiertos para el intercambio de documentos; el estado de situación de la evolución de MoReq a MoReq2; así como los Criterios de conservación de la Administración General del Estado.

PALABRAS CLAVE: OpenDocument, IDA, ISO/IEC 26300, MoReq.

1. INTRODUCCIÓN

Se acepta ya de forma generalizada que la administración electrónica contribuye al desarrollo y aplicación de las políticas públicas, al desarrollo de la

* Jefe de Área de Planificación y Explotación, Ministerio de Administraciones Públicas
miguel.amutio@map.es

sociedad de la información, a la renovación de la Administración, a una mayor productividad y competitividad como dinamizador económico, social e incluso medioambiental y a una mayor inclusión, integración y participación de la ciudadanía en la democracia. Desde que el Consejo Europeo de Lisboa de marzo de 2000 lanzó el reto de convertir a la economía europea en la más dinámica y competitiva en 2010, se viene avanzando con gran esfuerzo en este campo en todos los niveles, sea comunitario, nacional, regional o local, en reformas, en simplificación y en desarrollo de servicios.

Este impulso de la Administración electrónica lleva aparejado la producción, manipulación, visualización, intercambio y almacenamiento de documentos en soporte electrónico a gran escala. Este hecho pone de manifiesto la necesidad afrontar una serie de cuestiones de alcance tales como, entre otras posibles, la gestión de los archivos de documentos electrónicos, la validez de los documentos en soporte electrónico en los ámbitos de la Administración y el comercio, la aplicación de la firma electrónica, el marco legal actual en relación con las cuestiones anteriores, la utilización de formatos de documentos que favorezcan la interoperabilidad, la libertad de elección en un escenario tecnológicamente heterogéneo, así como la accesibilidad a los mismos a lo largo del tiempo y, finalmente, las pautas para asegurar la gestión de los documentos y de su conservación.

El Plan de Acción sobre Administración electrónica i2010[1], que forma parte de la iniciativa i2010 a favor del crecimiento y el empleo en la sociedad de la información y con el objeto de contribuir de manera significativa al logro de los objetivos de los Estados miembros y de las políticas comunitarias, en particular las relativas a la estrategia de Lisboa, incluye la gestión de los documentos electrónicos entre las denominadas herramientas clave para el desarrollo de la administración electrónica. Expone que los documentos electrónicos serán esenciales para muchos servicios en áreas tales como la contratación pública, los servicios médicos y la educación. Contempla el establecimiento por parte de la Comisión Europea junto con los Estados miembros de un marco de referencia para los documentos electrónicos autenticados a través de la Unión Europea, así como el desarrollo e implantación de un programa de trabajo en materia de cooperación en la gestión y acceso a los documentos electrónicos y a los archivos en las administraciones públicas.

Ahora bien, en la prestación de servicios de administración electrónica, la relación entre los diversos actores por el medio electrónico, sean ciudadanos, empresas o administraciones, se produce en un entorno heterogéneo de soluciones tecnológicas que incluye muy especialmente, entre otras posibles interacciones, el intercambio de documentos en formato electrónico. En este contexto, la adhesión a estándares abiertos parece el camino adecuado para

[1] COMISIÓN EUROPEA. *Plan de acción sobre administración electrónica i2010: Acelerar la administración electrónica en Europa en beneficio de todos.* Disponible en Internet: http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/comm_pdf_com_2006_0173_f_es_acte.pdf

facilitar que los diversos actores puedan interactuar utilizando sus opciones tecnológicas preferidas, en condiciones de libertad de elección y de garantía de comunicación e interoperabilidad. La transcendencia de la interoperabilidad proviene entre otras cuestiones del hecho de que la cautividad en protocolos, especificaciones y formatos propietarios arrastra en cadena a unos y a otros actores.

En este sentido, la Comunicación de la Comisión sobre interoperabilidad (COM(2006) 45 final)[2] reconoce que los estándares, especificaciones e interfaces abiertos son cruciales para la interoperabilidad. Anteriormente, cuando el Plan de Acción eEurope 2005[3] encomendó a la Comisión Europea la elaboración del Marco Europeo de Interoperabilidad, instrumento que aborda las políticas y especificaciones técnicas recomendadas para lograr la interoperabilidad organizativa, semántica y técnica a fin de poder combinar los sistemas de información de las administraciones de la UE, señaló que éste se basaría en normas abiertas y fomentaría el uso de programas de fuente abierta. En este Marco Europeo de Interoperabilidad[4], cuya elaboración han abordado los programas IDA e IDABC, también se dice que los estándares abiertos son un elemento clave para lograr la interoperabilidad y se identifican aquellas características mínimas que debe reunir una especificación técnica para ser considerada un estándar abierto.

Estas actuaciones siguen la estela de las estrategias de sistemas abiertos que se desplegaron en su día a raíz de la Decisión del Consejo de 27 de diciembre de 1986 relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones (87/95/CEE)[5].

En una línea similar, la Unidad de Inspección Conjunta (*Joint Inspection Unit*) de Naciones Unidas[6], en el marco de los Objetivos del Milenio, considera que las administraciones deben velar por que todos los ciudadanos tengan igualdad de oportunidades en el acceso a la información disponible por el medio electrónico y que los ciudadanos no se vean forzados a la adquisición de determinadas soluciones para ejercer sus derechos. También considera que las administraciones debieran adoptar medidas consecuentes relativas a la exigencia de estándares abiertos y a políticas y prácticas de contratación que no conduzcan a la cautividad.

---

[2] COMISIÓN EUROPEA. *Comunicación de la Comisión sobre interoperabilidad (COM(2006) 45 final)*. Disponible en Internet: http://europa.eu.int/eur-lex/lex/LexUriServ/site/es/com/2006/com2006_0045es01.pdf

[3] COMISIÓN EUROPEA. *Plan de acción eEurope 2005*. Disponible en Internet: http://europa.eu/scadplus/leg/es/lvb/l24226.htm

[4] COMISIÓN EUROPEA. European Interoperability Framework. Disponible en Internet: http://europa.eu.int/idabc/en/document/3761

[5] Decisión del Consejo de 27 de diciembre de 1986 relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones. Disponible en Internet: http://europa.eu/scadplus/leg/es/lvb/l24106.htm

[6] OUEDRAOGO, L.D. *Free/open source software (foss) and the Millennium Development Goals*. Mérida, octubre de 2005. Disponible en Internet: http://www.unsystem.org/jiu

En el ámbito de la Administración General del Estado, los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades[7] y la Propuesta de recomendaciones a la Administración General del Estado sobre utilización de software libre y de fuentes abiertas[8], ya contemplan, entre otros aspectos, que los documentos deben ponerse en un formato tal que pueda ser accedido desde diversos productos alternativos. Este enfoque ofrece una mayor libertad a la ciudadanía para interactuar con la Administración, para el uso de las lenguas propias en las tecnologías de la información y una mejor adaptación a las necesidades del usuario.

A continuación, se exponen las acciones de los programas comunitarios IDA e IDABC en materia de promoción de los formatos abiertos para el intercambio de documentos; el estado de situación de la evolución de MoReq a MoReq2; así como los Criterios de conservación de la Administración General del Estado.

2. Promoción del uso de los formatos abiertos de documentos por los programas comunitarios IDA e IDABC

Los programas comunitarios IDA e IDABC vienen realizando una valiosa labor en materias tales como la promoción de los formatos abiertos para el intercambio de documentos y el modelo de requisitos para la gestión de documentos electrónicos de archivo (MoReq).

El Programa IDA (1999-2004)[9] cuya base legal fueron las Decisiones 1719/1999/CE y 1720/1999/CE, conocidas como Decisiones IDA (Intercambio de Datos entre Administraciones), y sus enmiendas 2045/2002/CE y 2046/2002/CE, todas ellas del Consejo y del Parlamento Europeo, persiguió el establecimiento, en primer lugar, de los servicios transeuropeos entre administraciones, para dar soporte a la aplicación de políticas y actos comunitarios, a la comunicación interinstitucional en la Unión Europea y al proceso de decisión comunitario; y, en segundo lugar, de las acciones y medidas horizontales necesarias para la interoperabilidad de infraestructuras, servicios y contenidos en apoyo del despliegue de los citados servicios. Fue gestionado por el Comité de Telemática entre Administraciones y contó con una dotación financiera de 145,6 millones de euros para el período 1999-2004.

En 2003 el Programa IDA emprendió una línea de acción encaminada a promocionar la utilización de los formatos abiertos para el intercambio de

[7] Ministerio de Administraciones Públicas. *Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades, versión 2.2 de junio de 2004.* Disponible en Internet: http://www.csi.map.es/csi/pg5c10.htm

[8] Ministerio de Administraciones Públicas. *Propuesta de recomendaciones a la Administración General del Estado sobre utilización de software libre y de fuentes abiertas.* Disponible en Internet: http://www.csi.map.es/csi/pg5s44.htm

[9] Conocido también como IDA II, pues daba continuidad al Programa IDA que se desarrolló en el período 1995-1999.

documentos. Esta acción vino motivada fundamentalmente por dos razones; se detectó, por un lado, una baja interoperabilidad entre aplicaciones ofimáticas con efecto insatisfactorio para el desarrollo de la administración electrónica; y, por otro, una falta de apoyo a formatos abiertos y estándar de documentos en soporte electrónico. Además, cuando los expertos del Programa IDA examinaron el estado de situación de la cuestión, se consideró que los documentos intercambiados entre las administraciones públicas y los ciudadanos deberían encontrarse en un formato tal que no obligara a éstos a la utilización de unos productos de software específicos y que asegurara también la accesibilidad permanente a los mismos.

La decisión de actuar en este campo por parte de IDA puso en marcha un proceso que, a lo largo de aproximadamente un año, dio lugar a los siguientes hitos:

— En mayo de 2003 se identificó una laguna en la disponibilidad de formatos abiertos de documentos, necesarios para el desarrollo de la administración electrónica y se acordó actuar en esta cuestión.

— En enero 2004 se aprobó el análisis comparativo, encargado por el Programa IDA, de los estándares de formatos de documentos disponibles y, en particular, de los estándares existentes o emergentes de formatos abiertos de documentos y de la posible evolución del mercado en este terreno. Este análisis, conocido como **Informe Valoris**[10], realiza valiosas aportaciones, entre las que figura, de forma destacada, la identificación de aquellas cualidades que sirven para examinar los formatos de documentos existentes y que, en su caso, determinan el formato de documento ideal. Tales cualidades son las ocho siguientes:

  • *Abierto:* se refiere a que la especificación del formato se encuentra accesible de forma pública, se puede distribuir libremente y el formato se puede implementar en programas y aplicaciones sin restricciones legales y libre de *royalties.*

  • *No-binario:* se refiere a que el contenido del documento, junto con sus etiquetas, se guarda como texto plano y no como una corriente binaria.

  • *Modificable:* se refiere al hecho de que el documento se puede editar, en contraste con los documentos que dan lugar a formatos de sólo lectura no editables.

  • *Fidelidad de la presentación:* se refiere a la capacidad del formato para asegurar la disposición original de los elementos en el documentos (por ejemplo, sangrados, espaciados, ubicación de logotipos, etc.) con independencia de plataformas hardware y entornos software.

[10] VALORIS. *Comparative Assessment of Open Documents Formats Market Overview.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/3439/5585#ODF

- *Interoperabilidad multiplataforma:* se refiere a que el formato puede ser explotado con plena garantía de sus cualidades en diversas plataformas hardware y software.
- *Soporta características de los procesadores de textos existentes:* se refiere a la capacidad del formato para soportar las funcionalidades comunes disponibles a la fecha en los procesadores de textos.
- *Soporta requisitos emergentes:* se refiere a la capacidad del formato para poder satisfacer posibles requisitos emergentes, tales como la firma electrónica.
- *Ampliamente adoptado:* se refiere a que el formato cuenta con una base de usuarios y de herramientas aplicables que aseguren la sostenibilidad y explotación del mismo; lo cual no significa necesariamente un dominio del mercado o que se trate del formato universalmente aceptado.

— En marzo de 2004 se convocó a los mayores actores del mercado (Microsoft y SUN), se les invitó a comentar el citado Informe Valoris, se les dio audiencia para que pudieran debatir con los expertos del Programa IDA, así como presentar y defender sus respectivos puntos de vista.

— El 25 de mayo de 2004, el Comité de Telemática entre Administraciones, de 25 Estados miembros, gestor del Programa IDA, respaldó las **recomendaciones relativas a la promoción de la utilización de los formatos abiertos de documentos**[11], elevadas por su grupo de expertos en la materia.

Al formular dichas recomendaciones, en primer lugar, se reconoció la especial responsabilidad del sector público europeo en cuanto a salvaguardar la accesibilidad de su información, la necesidad de mejorar las interacciones con los ciudadanos y las empresas así como el peso del sector público como comprador de productos y servicios.

En segundo lugar, y como resultado del proceso de análisis y estudio realizado, se identificaron los pasos dados por la industria, señalando la publicación de los formatos OpenOffice.org y WordML; se concluyó que no es necesario que todos los documentos sean editables y que en el caso de documentos que hayan de ser editados, XML ofrece el mejor escenario de separación de contenido, estructura, semántica y presentación; y que el sector público no debe forzar a la utilización de un producto determinado y que debe promocionarse un formato que pueda implementarse en diversas plataformas, que no sea discriminatorio de los actores del mercado y que ofrezca igualdad de

[11] EUROPEAN COMMISSION. *TAC approval on conclusions and recommendations on open document formats.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/3439/5585 #recommendations

oportunidades para su implementación; y, finalmente, se dio la bienvenida a la normalización del formato de OpenOffice.org por OASIS[12].

En tercer y último lugar, se formularon las recomendaciones propiamente dichas, a la luz de las limitaciones a la fecha de su emisión en cuanto a los formatos de documentos existentes y dirigidas a los actores con capacidad de influir en este campo.

De forma sintética, las recomendaciones se dirigieron a los diversos actores en los términos siguientes:

- *A la Industria:* que se involucre en la normalización de los formatos de documentos; que proporcione filtros de conversión entre formatos; que aporte herramientas y servicios para que el sector público pueda migrar sus documentos a formatos XML.
- *A Microsoft:* que se comprometa a publicar las especificaciones de Word XML; que eleve sus formatos a organismos de normalización; y que elimine los componentes no XML de WordML.
- *A OASIS:* que eleve el Formato Abierto de Documentos (ODF) a ISO/IEC.
- *Al Sector Público:* que utilice diversos formatos en la publicación de información.

Seguidamente a la emisión de estas recomendaciones, la Dirección General de Empresas (DG ENTR) de la Comisión Europea invitó a los principales productores de software a que trabajaran en pos de una mayor interoperabilidad en los formatos de documentos. En respuesta a esta llamada, IBM, Microsoft y SUN expresaron su compromiso de avanzar en la citada dirección[13].

El **Programa IDABC** (2005-2009)[14] [15], sucesor del Programa IDA, y cuya base legal es la Decisión 2004/387/CE del Parlamento Europeo y del Consejo de 21 de abril de 2004 relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC) persigue en un nuevo contexto que incluye a los ciudadanos y las empresas, la identificación, promoción y desarrollo de servicios que apoyan la aplicación de actos y políticas comunitarios, la comunicación interinstitucional en la UE y el proceso de decisión comunitario, así como de las medidas horizontales para el despliegue de los primeros. La base legal de IDABC establece de forma similar al caso de IDA una dotación financiera

---

[12] OASIS. *OASIS (Organization for the Advancement of Structured Information Standards).* Disponible en Internet: http://www.oasis-open.org/home/index.php

[13] EUROPEAN COMMISSION. *Responses from IBM, Microsoft and SUN to the TAC recommendations- Sept./Nov. 2004.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/3439/5585#responses

[14] EUROPEAN COMMISSION. *The Programme IDABC.* Disponible en Internet : http://europe.eu.int/idabc

[15] MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *La construcción de los servicios pan-europeos de Administración electrónica.* Disponible en Internet: http://www.csi.map.es/csi/pg3315.htm

de 148,7 millones de euros para el período 2005-2009; un mecanismo de gestión constituido por el Comité de Servicios Paneuropeos de Administración Electrónica; y, en sus anexos I y II, la relación exhaustiva de las áreas de actuación, tanto sectorial como horizontal.

El Programa IDABC también ha incluido en su Programa de Trabajo[16] la acción en materia de promoción de los formatos abiertos para el intercambio de documentos a fin de facilitar los intercambios de documentos en el nivel paneuropeo, pues si bien se han producido avances notables gracias al impulso del Programa IDA, los problemas de interoperabilidad siguen existiendo. Se persigue con esta acción que los Estados miembros y los actores de la industria se impliquen en el debate sobre la cuestión, en la identificación de soluciones, así como en la promoción de la concienciación del sector público en cuanto a la adopción de formatos abiertos de documentos. También se contempla continuar la exploración de posibles soluciones prácticas para la interoperabilidad de formatos de documentos. Así, IDABC viene trabajando en la elaboración de unas recomendaciones sobre la promoción de la utilización de los formatos abiertos para el intercambio de documentos que actualicen las emitidas en su día por el Programa IDA, en mayo de 2004, a la luz del estado de situación a la fecha.

3. El formato abierto de documentos OpenDocument

Como se ha visto más arriba, las citadas recomendaciones IDA llamaron a OASIS para que elevaran el Formato Abierto de Documentos a la normalización en el ámbito de la Organización Internacional de Normalización ISO/IEC.

Efectivamente, este Formato Abierto de Documentos, en inglés *Open Document Format*, fue adoptado como estándar ***OASIS Open Document Format for Office Applications (OpenDocument) v1.0***, el día 1 de mayo de 2005[17].

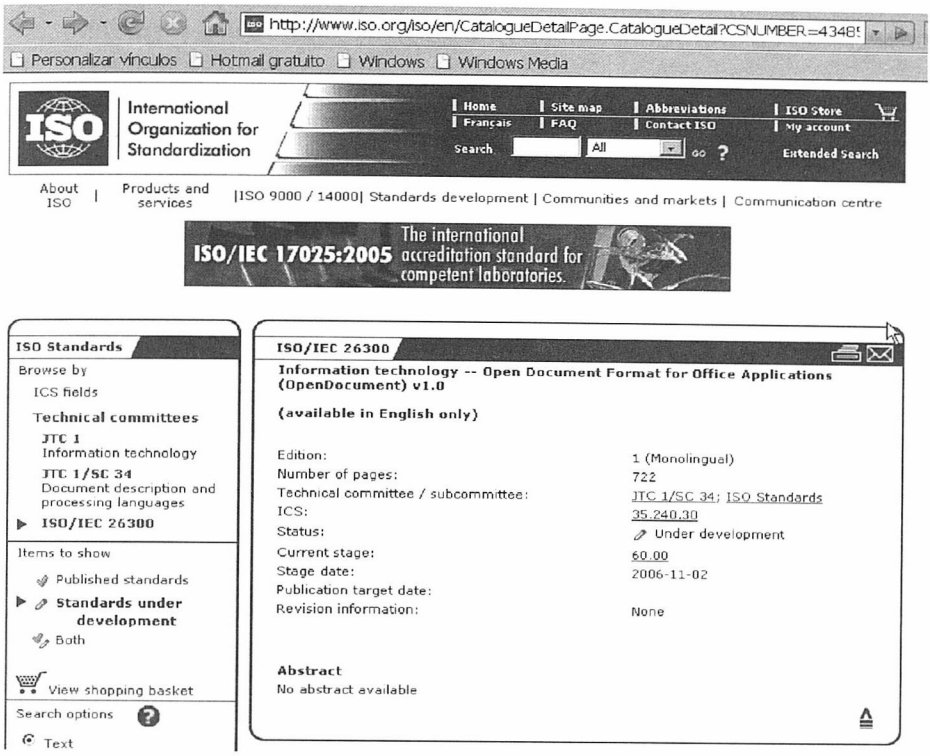
Tras su adopción como estándar OASIS, la especificación de OpenDocument se sometió a normalización en ISO/IEC, como habían solicitado las citadas recomendaciones, dando lugar al proyecto de normalización ***ISO/IEC 26300 Open Document Format for Office Applications (OpenDocument) v1.0***. En septiembre de 2005 se inició este proceso de normalización directamente en la fase DIS (*Draft International Standard*); a continuación, se sometió a un procedimiento de votación cuyo plazo venció con el final de abril de 2006, resultando aprobado con mayoría de votos positivos, con algunas abstenciones y ningún voto negativo. Este resultado de la votación permitió soslayar la fase FDIS (*Final Draft International Standard*) y avanzar el proyecto directamente a

[16] European Commission. *IDABC work programme 2005-2009*. Disponible en Internet: http://ec.europa.eu/idabc/en/document/5101/3

[17] Oasis. *OASIS Open Document Format for Office Applications (OpenDocument)*. Disponible en Internet: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office

la fase de publicación como norma internacional[18], situación en la que se encuentra a la fecha[19].

FIGURA 1.
Página de ISO/IEC correspondiente a la norma ISO/IEC 263000



El citado formato *OpenDocument* es un formato de fichero o conjunto de especificaciones basado en XML para los documentos en soporte electrónico, sean textos, hojas de cálculo, presentaciones o gráficos, entre otros posibles. El enfoque seguido por esta especificación se encamina a la reutilización de estándares abiertos XML existentes y, en su caso, a la creación de etiquetas nuevas cuando ninguno de los demás estándares abiertos disponibles ofrece la funcionalidad necesaria. Así, hace uso de Dublin Core XML para los metadatos, MathML para las fórmulas matemáticas, SVG para los gráficos vectoriales, SMIL para la multimedia, etc. OpenDocument separa el contenido, la disposición de

[18] ISO/IEC. ISO/IEC 26300 *Open Document Format for Office Applications (OpenDocument) v1.0.* Disponible en Internet: http://www.iso.org

[19] En concreto se encuentra en la etapa codificada como *'60.00 International Standard under publication'*. Véase: http://www.iso.org/iso/en/widepages/stagetable.html#60

éste en el documento y los metadatos. Su formato interno es un archivo comprimido ZIP que contiene a su vez una serie de ficheros y carpetas.

Uno de los aspectos más sobresalientes de OpenDocument es que puede ser soportado por múltiples aplicaciones ofimáticas que hayan implementado su especificación; así, a la fecha, lo soportan productos tales como OpenOffice.org[20], KOffice[21], Abiword[22], TextMaker, Writely, StarOffice, IBM Workplace, NeoOffice[23].

FIGURA 2.
Aplicaciones que soportan OpenDocument[24]

Text Documents [edit]

Word Processors [edit]

	Version	Operating systems	Office suite	Developer	License	Notes
AbiWord	2.4.2	Windows, Mac OS X, Linux, Unix-based systems	GNOME Office or standalone	AbiSource	GPL	
IBM Workplace Documents	2.5+	Any (Web-based)	IBM Workplace Collaboration Services	IBM	Proprietary	
KWord	1.4+	Linux, Unix-based systems	KOffice	KDE Project	LGPL	
NeoOffice Writer	1.2	Mac OS X	NeoOffice	Patrick Luby and Edward Peterlin	GPL	Import only
OpenOffice.org Writer	2.0	Windows, Linux, Unix-based systems	OpenOffice.org	OpenOffice.org	LGPL	
OpenOffice.org Writer	1.1.5	Windows, Linux, Unix-based systems	OpenOffice.org	OpenOffice.org	LGPL / SISSL	Import only
StarOffice Writer	8	Windows, Linux, Solaris	StarOffice	Sun Microsystems	Proprietary	
TextMaker	2006 (in beta as of 2006)	Windows	Beta is standalone	SoftMaker	Proprietary	Import only
Writely	2006 (now out of beta and called Google Documents)	Any (Web-based)	Standalone	Google	Proprietary	
Zoho Writer	2006	Any (Web-based)	Standalone	AdventNet	Proprietary	
	Version	Operating systems	Office suite	Developer	License	Notes

Other Applications [edit]

Besides word processors, other programs can and do support the OpenDocument text format. See the List of applications supporting OpenDocument for more.

Las razones por las que OpenDocument despierta tanto interés son diversas y tienen que ver con aspectos tales como los siguientes:

- El estado de situación de los formatos de documentos, en términos de la carencia de alternativas significativas en los formatos o de la vinculación con las herramientas que los procesan, de las insuficiencias en los formatos existentes y de las lagunas en materia de normalización de los mismos.

[20] Disponible en Internet: http://www.openoffice.org/

[21] Disponible en Internet: http://www.koffice.org/

[22] Disponible en Internet: http://www.abisource.com/

[23] WIKIPEDIA. Aplicaciones que soportan OpenDocument . Disponible en Internet: http://en.wikipedia.org/wiki/Comparison_of_applications_supporting_OpenDocument

[24] Aplicaciones que soportan OpenDocument. Fuente: http://en.wikipedia.org/wiki/Comparison_of_applications_supporting_OpenDocument

- Las cualidades de OpenDocument en cuanto a que ofrece un formato no-binario, multiplataforma (hardware y software), implementado e implementable por múltiples herramientas alternativas, aportando separación entre el formato y la herramienta que lo procesa, a la vez que soporta textos, hojas de cálculo, presentaciones, gráficos y otros posibles.
- OpenDocument cuenta con varias implementaciones de referencia que facilitan su extensión y un grado de adopción significativo, operables en múltiples plataformas hardware alternativas, por lo que no es un mero ejercicio teórico.
- La naturaleza de la especificación de OpenDocument es pública, abierta, desarrollada en un proceso abierto, público y visible, neutral, libre de royalties y abierto a la comunidad de usuarios, no controlada por un único actor, en manos de un grupo de trabajo abierto a nuevos miembros, sometido a un proceso formal de control de cambios y de adopción. Su especificación se encuentra libre de restricciones legales (por ejemplo de licencias o patentes) y es susceptible de ser implementado por cualquiera.

Y, en definitiva, por las consecuencias de todo la anterior, en particular, en los documentos de la administración electrónica y la conservación de la información:

- Las políticas tecnológicas en materia de administración electrónica conceden gran importancia a la libertad de elección y a la interoperabilidad.
- La conservación de documentos en soporte electrónico a largo plazo requiere la disponibilidad de estándares abiertos independientes de plataforma, que aporten independencia tecnológica, favorable a la conservación, frente a sucesivas oleadas tecnológicas y políticas comerciales particulares, así como la libertad de opción en el acceso y visualización de documentos y facilidad en el acceso a los mismos.

OpenDocument se extiende a través del uso de los productos que lo manejan, especialmente de OpenOffice.org.

En el ámbito internacional son conocidas, entre otras, las iniciativas de adopción de OpenDocument como formato para garantizar la conservación de la información en soporte electrónico por la administración de Massachussets[25] en septiembre de 2005 y por *Australia National Archives*[26] [27] en 2006.

[25] THE CONSORTIUMINFO.ORG. *Update: Massachusetts ODF Milestones, Due Dates and Schedule.* Disponible en Internet: http://www.consortiuminfo.org/standardsblog/article.php?story=20060407093016 79

[26] Disponible en Internet: http://www.naa.gov.au/

[27] THE CONSORTIUMINFO.ORG. *Case Study II: A National Archive Moves to ODF.* Disponible en Internet: http://www.consortiuminfo.org/standardsblog/article.php?story= 20060403090844 65

Movimientos similares se vienen produciendo en otros países como Francia[28] y Bélgica[29] [30]. También se ha lanzado el 3 de marzo de 2006 una iniciativa de apoyo denominada *Open Document Format Alliance*[31] con 35 miembros iniciales del sector público y del sector privado.

En el ámbito nacional, el Acuerdo de Consejo de Gobierno de 25 de julio de 2006 para la implantación de programas informáticos libres en los ordenadores personales de la Junta de Extremadura[32] contempla la utilización del citado OASIS OpenDocument para información en elaboración y proceso administrativo, junto con el formato de documento de intercambio PDF/A (*ISO/IEC 19005-1:2005 Portable Document Format*), para aquellas información para la cual se desea garantizar su inalterabilidad de visualización.

Merece la pena también reseñar que información reciente del sitio web de RedIRIS muestra que desde mitad de 2005 a mayo de 2006 se han producido 1.408.748 descargas de OpenOffice.org, más 133.737 descargas de distribuciones Linux que incluyen copias de OpenOffice.org.

La extensión de la utilización de Open Document en nuestro país mediante la utilización de OpenOffice.org viene también de la mano de la implantación de puestos GNU/Linux. Así a título orientativo, y sin ánimo de exhaustividad, se manejan las cifras siguientes: 70.000 puestos en Extremadura (con GNU/Linex), correspondientes a Sistema Educativo, Sistema Extremeño de Salud, Bibliotecas Públicas y Administración; 225.000 puestos en Andalucía (con GuadaLinex), correspondientes a Educación, Centros Guadalinfo, Bibliotecas Públicas y Centros de Día; 60.000 puestos en Cataluña con OpenOffice.org, correspondientes a las escuelas públicas.

4. MOREQ, MODELO DE REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO Y MOREQ2

El DLM-Forum[33] abordó por primera vez la necesidad de establecer una especificación exhaustiva de los requisitos de la gestión de los documentos electrónicos de archivo en 1996, en uno de los diez puntos de acción surgidos

[28] IDABC eGovernment Observatory. *FR: Official report recommends adoption of Open Document Format.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/6206/194

[29] PRESSCENTER.ORG. *Communiqué de presse du Conseil des Ministres Utilisation de standards ouverts pour l'échange de documents bureautiques* http://presscenter.org/archive/20060623/432d0130470a88df1105dda38d1282b0/?lang=nl&prLang=fr

[30] ODF ALLIANCE. *Newsletter 26 June 2006.* Disponible en Internet: http://www.odfalliance.org/press/Newsletter%2020060626.pdf

[31] Disponible en Internet: http://www.odfalliance.org/

[32] ODF ALLIANCE. JUNTA DE EXTREMADURA. *Acuerdo de Consejo de Gobierno de 25 de julio de 2006 para la implantación de programas informáticos libres en los ordenadores personales de la Junta de Extremadura.* Disponible en Internet: http://www.linex.org/mocion_consejo_gobierno. pdf

[33] DLM-Forum. Disponible en Internet: http://ec.europa.eu/transparency/archival_policy/dlm_forum/index_en.htm

de su reunión. DLM es un acrónimo de la expresión francesa *Données Lisibles par Machine*, en español «datos de lectura automática». El DLM-Forum tiene su base jurídica en las conclusiones del Consejo Europeo, de 17 de junio de 1994, sobre una mayor cooperación en el ámbito de los archivos (94/C 235/03).

MoReq, Modelo de Requisitos para la gestión de documentos electrónicos de archivo (SGDEA), es un modelo de requisitos funcionales para la gestión de documentos electrónicos de archivo que fue elaborado en 2001 través del Programa IDA[34] y con su financiación, con el fin de que pudiera ser utilizado en todos los países de la Unión Europea y por todos los interesados en el desarrollo y aplicación de sistemas de gestión de documentos electrónicos de archivo (archiveros, gestores, diseñadores de software, proveedores de servicios, instituciones académicas y de formación) o bien quisieran evaluar la capacidad del que ya poseen. Esta especificación se concibió partiendo de la premisa de que los usuarios del SGDEA no serían solamente los administradores y archiveros, sino también el personal de oficina y operativo, quienes utilizarían este sistema en su trabajo cotidiano para crear, recibir y recuperar documentos.

En España, el Grupo de Trabajo de Expertos en Documentos Electrónicos (CARMEN), coordinado por la Subdirección General de los Archivos Estatales realizó, a solicitud del en su momento Consejo Superior de Informática y para el Impulso de la Administración Electrónica, hoy Consejo Superior de Administración Electrónica, una revisión completa de la versión en lengua española[35], traducción de la versión original en lengua inglesa.

MoReq incide especialmente en los requisitos funcionales de la gestión de documentos electrónicos de archivo mediante la especificación de un sistema de gestión de documentos electrónicos de archivo. La especificación se centra en los requisitos funcionales, si bien también reconoce la importancia de los atributos no funcionales en la eficacia de un SGDEA. Así mismo, se abordan la gestión de documentos, así como la gestión electrónica de documentos de archivo tradicionales, por ejemplo, expedientes en papel o microfilm.

La especificación MoReq se ha concebido para que la utilicen:

- Los posibles usuarios del SGDEA como punto de partida en la preparación de una licitación.
- Los usuarios del SGDEA, en la auditoría o evaluación de un sistema ya existente.
- Las organizaciones dedicadas a la formación, como documento de referencia en la preparación de cursos de gestión de documentos de archivo o bien como material de trabajo en sus cursos.

[34] EUROPEAN COMMISSION. *MOREQ: Model Requirements for the Management of Electronic Records* http://ec.europa.eu/idabc/en/document/2303/5644

[35] COMISIÓN EUROPEA. *MoReq, Modelo de Requisitos para la gestión de documentos electrónicos de archivo.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/2631/5585 http://www.csi.map.es/csi/pg3315.htm#511

- Las instituciones académicas, como instrumento docente.
- Los proveedores y creadores de SGDEA, como directriz que guíe el desarrollo de sus productos, destacando las funcionalidades necesarias.
- Los proveedores de servicios de gestión de documentos de archivo, como orientación sobre la naturaleza de los servicios que prestan.
- Los posibles usuarios de servicios externos de gestión de documentos de archivo, como referencia a la hora de especificar los servicios qye va a contratar.

MoReq2 persigue actualizar y extender los requisitos funcionales para la gestión de documentos electrónicos de archivo, así como incluir las pruebas de conformidad. Las bases para la actualización de MoReq son el informe[36] que produjo el DLM-Forum tras realizar consultas con los principales actores e identificar tanto aquellas partes del modelo original que demandaban una actualización, como posibles nuevos contenidos requeridos y la Recomendación del Consejo de 14 de noviembre de 2005 relativa a las medidas prioritarias para aumentar la cooperación en el ámbito de los archivos en Europa (2005/835/CE)[37]. MoReq2 figura como uno de los instrumentos recogidos por el Plan de acción i2010 en relación con la gestión de los archivos de documentos electrónicos.

Los objetivos de MoReq2 son los siguientes:

- Actualizar los requisitos actuales para adaptarlos al estado del arte en materia de buenas prácticas
- Extender los requisitos funcionales para abarcar nuevas áreas que han ganado importancia en los últimos cinco años.
- Desarrollar orientaciones para las pruebas de conformidad. Así, los suministradores podrán demostrar su conformidad con el modelo. Para ello es necesario el desarrollo de instrumentos que faciliten estas pruebas de conformidad, así como su consistencia.
- Permitir mayor flexibilidad; debe ser posible implementar MoReq2 en diferentes entornos con diferente legislación y cultura en la gestión de documentos electrónicos de archivo.

Se contempla que MoReq2 sea una evolución del modelo existente, MoReq, sin dar lugar a un producto radicalmente diferente. La actualización

---

[36] EUROPEAN COMMISSION. *Report on archives in the enlarged European Union.* Disponible en Internet: http://ec.europa.eu/transparency/archival_policy/docs/arch/reportarchives. pdf

[37] *Recomendación del Consejo de 14 de noviembre de 2005 relativa a las medidas prioritarias para aumentar la cooperación en el ámbito de los archivos en Europa (2005/835/CE).* Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/site/es/oj/2005/l_312/l_31220051129es00550056.pdf

y extensión de MoReq, así como el desarrollo de las pruebas de conformidad se realizarán en línea con el citado informe realizado por el DLM-Forum en cooperación con la Comisión Europea. Durante la realización del proyecto la Comisión Europea ha previsto recabar asesoramiento del DLM-Forum. La actualización de MoReq se realizará con cargo a los fondos del Programa IDABC[38], mientras que el DLM-Forum se encargará del lanzamiento, publicación y difusión de MoReq2.

5. Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades

La elaboración de los Criterios de seguridad, normalización conservación de las aplicaciones utilizadas para el ejercicio de potestades es una encomienda al Consejo Superior de Administración Electrónica del Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, modificado por 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[39].

En particular, los **Criterios de conservación** se orientan a la conservación y protección de los documentos administrativos. Exponen los requisitos, criterios y recomendaciones para la conservación de la información en soporte electrónico en las aplicaciones cuyo resultado sea utilizado para el ejercicio por los órganos y entidades del ámbito de la Administración General del Estado de las potestades que tienen atribuidas; contemplan los requisitos de protección de los datos de carácter personal y van dirigidos a los responsables de la adquisición, diseño, desarrollo, implantación y explotación de las citadas aplicaciones.

Publicados por primera vez en diciembre de 2001, sus antecedentes se remontan al año 1996, época en la que difícilmente se encontraban modelos o referentes, salvo la suerte de que iniciara su andadura el DLM-Forum y constituyen, de forma pionera, la primera experiencia de la Administración en plasmar un documento de esta naturaleza.

Sus objetivos son:

- Facilitar la adopción generalizada por parte de la Administración General del Estado de medidas organizativas y técnicas que aseguren la conservación de la información en soporte electrónico.

---

[38] European Commission. *IDABC work programme 2005-2009.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/5101/3

[39] *Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.* Disponible en Internet: http://www.csi.map.es/csi/pg2001.htm

- Facilitar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa y asegurar a la vez el respeto de las garantías y derechos de los ciudadanos en sus relaciones con la Administración.
- Ser un documento vivo que ha de verse sometido a actualización con cierta regularidad.

Se estructuran en los siguientes capítulos:

- 1. Presentación
- 2. Conservación de la información en soporte electrónico. Trata los documentos administrativos y de los ciudadanos, el almacenamiento de la información en soporte electrónico y el análisis y gestión de riesgos.
- 3. Ciclo de vida de la información en soporte electrónico. Trata el ciclo de vida, el análisis del documento electrónico, el diseño de la estrategia de gestión, la creación de la información en soporte electrónico, la gestión de la información en soporte electrónico, el traspaso de la información al archivo, y el acceso y difusión a la información de soporte electrónico.
- 4. Formato de la información en soporte electrónico. Trata los tipos de formatos de ficheros y juego de caracteres.
- 5. Soportes. Incluye tipos de soportes de almacenamiento de la información.
- 6. Medidas de almacenamiento y conservación. Trata la reescritura de los archivos en soporte electrónico, la protección contra el deterioro físico, y la seguridad de la información.
- 7. Sistema de archivos. Trata el archivo de oficina, el archivo central, el archivo intermedio y el archivo histórico.

En cada uno de estos capítulos los contenidos se estructuran de la manera siguiente:

- Los requisitos de carácter normativo que obligan a aplicar distintas medidas para la conservación de la información.
- Los criterios a tener en cuenta en la aplicación de las distintas medidas de conservación para satisfacer los requisitos anteriores que indican qué medidas organizativas y técnicas se han de adoptar.
- Las recomendaciones complementan a los criterios expuestos y los desarrollan con descripciones de detalle de las medidas técnicas u organizativas.
- Los niveles de seguridad, que complementan los niveles de seguridad requeridos por el Real Decreto 994/1999.

- La ampliación técnica da referencias que permiten profundizar y ampliar los conceptos técnicos y organizativos en los que se fundamentan las distintas medidas de conservación.
- Adicionalmente, en ciertos capítulos se incluyen consideraciones que matizan el alcance o contenidos del capítulo, un apartado, denominado conceptos, con explicación o definición de aspectos clave y otro apartado, denominado ejemplo de solución, con algunas orientaciones más concretas de forma muy resumida.

Los Criterios de conservación parten del supuesto de que la información en soporte electrónico se debe poder conservar con independencia del soporte o de la tecnología. Además, la propia evolución constante de la tecnología, los factores agresivos de los soportes y la propia naturaleza de la información en soporte electrónico dan lugar a ciertos riesgos. Para abordar su conservación es necesario, por tanto, identificar los requisitos de plazo de conservación de la información, la información importante en soporte electrónico, las responsabilidades; definir reglas, formatos y estándares que aseguren la independencia de datos frente a soportes y plataformas tecnológicas para garantizar la durabilidad; la utilización de métodos y procedimientos para el diseño, la creación y la gestión de la información en soporte electrónico; la concienciación y la formación de los actores implicados; gestionar el plazo de conservación y el volumen de información almacenada, lo cual se traduce en la necesidad de convertir, regenerar, copiar o transferir la información de un soporte a otro, de un formato a otro, de una tecnología a otra a lo largo del tiempo.

A la vez, se deben mantener la autenticidad, la integridad, la confidencialidad y la disponibilidad de la información. Se trata de una tarea que exige la adopción de medidas organizativas y técnicas; la trazabilidad de las operaciones de creación, modificación y borrado; así como auditorías periódicas. Esto implica que los criterios para la conservación de los soportes, su custodia y su accesibilidad deben ser incluidos en los planes de seguridad y en los planes de contingencia; que los dispositivos y soportes informáticos de almacenamiento deben estar adecuadamente controlados y protegidos; que se deben establecer procedimientos operativos de seguridad para proteger de daño, robo o acceso no autorizado a soportes de almacenamiento, datos de entrada y de salida del sistema, documentación del sistema, etc.

Las medidas para la conservación de la información en soportes electrónico deben adoptarse de acuerdo con los especialistas en la gestión de archivos para diseñar soluciones prácticas a la medida de sus necesidades. Los Criterios de conservación persiguen recoger las buenas prácticas de gestión documental, ya establecidas y operativas, para trasladarlas al entorno electrónico, es decir a la gestión de documentos electrónicos procedentes de los archivos de oficina y a la conservación de documentación electrónica en archivos de carácter permanente. Esta estrategia se orienta a asegurar la participación de todos los actores implicados, recogiendo un enfoque de multidisciplinariedad, sean

archiveros, usuarios, responsables o técnicos de tecnologías de la información y contemplar la conservación, acceso y protección de la información, especialmente de los datos de carácter personal.

Para orientar en esta tarea, los Criterios de conservación se apoyan en pilares tales como el análisis y gestión de riesgos, el ciclo de vida de la información y los formatos de documentos.

La conservación de los documentos en soporte electrónico tiene lugar en un entorno complejo y no exento de riesgos. En primer lugar, la evolución continua de la tecnología hace que sea difícil la selección de soportes y formatos estables y duraderos, por los siguientes motivos:

- Aparición constante de nuevas versiones de plataformas, sistemas operativos, programas y formatos.
- Introducción de cambios en las características físicas de los soportes (características, tamaños, densidad de grabación y capacidad, etc.).
- Ciertos soportes pueden tener una mayor vida útil, como objeto físico, pero pueden estar sometidos a una rápida obsolescencia tecnológica.
- Generación de nuevas formas de documentos electrónicos, tales como los documentos compuestos, hipertexto o multimedia.
- Disponibilidad de una gran capacidad de procesamiento y de almacenamiento que no va acompañada de los procedimientos necesarios para el control adecuado de documentos.
- Desarrollo de sistemas de información orientados a la gestión de datos pero no tanto a la gestión de documentos.

En segundo lugar, existen amenazas tales como la acumulación incontrolada de documentos, la destrucción accidental o incontrolada de documentos, la manipulación no autorizada de los mismos (acceso, alteración, destrucción), la ausencia de documentación asociada y de metadatos, que da lugar a ineficiencias en el acceso, los factores agresivos que facilitan el deterioro de los soportes, tal es el caso de los campos magnéticos, de la oxidación o de la degradación de los materiales.

La adopción de medidas organizativas y técnicas para la conservación de la información se debe realizar de forma rigurosa y proporcionada a los riesgos detectados. Para ello, el análisis y gestión de riesgos aporta racionalidad, primero, en el conocimiento de los activos de tipo información, a qué amenazas están expuestos, cuáles son sus debilidades ante las mismas y cuál serían las consecuencias de la materialización de las citadas amenazas; y, segundo, en la introducción de las medidas que deben adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

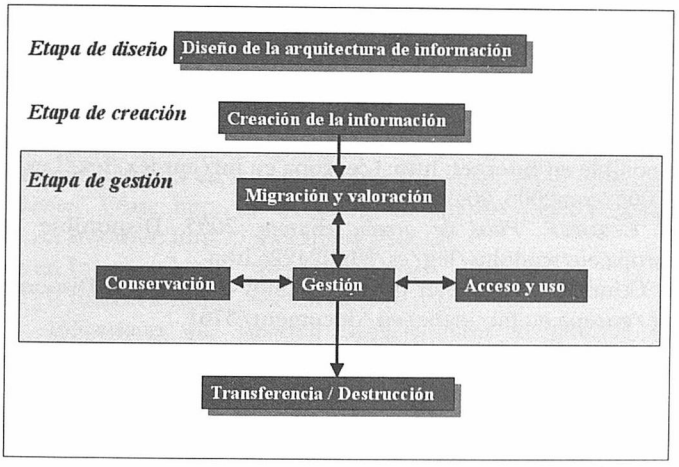
Es decir, el análisis y gestión de riesgos debiera ayudar a formular y responder preguntas como las siguientes: ¿Qué información se ha de conservar y

proteger?, ¿De qué tipo es?, ¿Cuáles son los plazos de conservación?, ¿En qué soportes y formatos está?, ¿Qué problemas de durabilidad, longevidad y degradación se plantean?, ¿Quién tiene acceso, a qué, para qué, cuándo y cómo?, ¿Qué amenazas afectan a la información?, ¿Cuáles son las consecuencias si se materializan?, ¿Qué medidas organizativas y técnicas se deben adoptar?

Para facilitar esta tarea, el Consejo Superior de Administración Electrónica ha elaborado MAGERIT versión 2, la Metodología de análisis y gestión de riesgos de los sistemas de información[40], un método formal para investigar los riesgos y para recomendar las medidas apropiadas que deberían adoptarse para controlar los mismos.

Los Criterios de conservación adoptan el ciclo de vida expuesto en la Guía de la información electrónica elaborada por el DLM Forum, la cual describe un enfoque de gestión de la información en soporte electrónico que contempla todo el ciclo de vida de la información en sus diversas etapas: diseño de la arquitectura de la información, creación de la información, gestión, acceso y uso, conservación y finalmente transferencia a archivo. Este enfoque de gestión de la información permite poner énfasis en el desarrollo de políticas y directrices en el ámbito de toda la organización; en el diseño de las aplicaciones que permiten la creación y la gestión de los documentos electrónicos; en el desarrollo de requisitos de implantación relativos a la configuración, gestión de datos, seguridad, acceso, responsabilidad del usuario, métodos de almacenamiento y recuperación; y en la promoción de estándares que permitan la gestión y migración de la información.

FIGURA 3.
El modelo de ciclo de vida de la información elaborado por el DLM-Forum



[40] MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *MAGERIT versión 2, Metodología de análisis y gestión de riesgos de los sistemas de información.* Disponible en Internet: http://www.csi.map.es/csi/pg5m20.htm

Los criterios y recomendaciones incluidos en los Criterios de conservación han tenido en cuenta términos de referencia tales como la Guía de la información electrónica elaborada por el DLM[41] Forum, el Manual de tratamiento de archivos administrativos[42], las Directrices de arquitectura IDA[43], entre otros. En todos los casos los criterios y recomendaciones se han seleccionado atendiendo a normas o estándares técnicos nacionales e internacionales de reconocida autoridad.

Durante el tiempo transcurrido desde la aprobación de la versión en vigor de los Criterios y su posterior publicación se han producido los lógicos avances que dan lugar a la necesidad de realizar su actualización. A la fecha, se suscita, por tanto, la necesidad de someterlos a una actualización de alcance que tenga presente el estado de situación de las siguientes cuestiones:

- La normalización en el ámbito del Comité Técnico de Normalización de Documentación (CTN/50) de AENOR.
- Los formatos de la información en soporte electrónico.
- La normalización de formatos de documentos (por ejemplo, ISO/IEC 26300 e ISO/IEC 19005).
- Las Recomendaciones IDA sobre la promoción de la utilización de los formatos abiertos para el intercambio de documentos.
- El estado de situación en materia de documentos electrónicos a la luz de lo previsto en el Plan de Acción i2010, MoReq2, entre otros posibles.

6. Referencias bibliográficas

1. Comisión Europea. *Plan de acción sobre administración electrónica i2010: Acelerar la administración electrónica en Europa en beneficio de todos.* Disponible en Internet: http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/comm_pdf_com_2006_0173_f_es_acte.pdf
2. Comisión Europea. *Comunicación de la Comisión sobre interoperabilidad (COM(2006) 45 final).* Disponible en Internet: http://europa.eu.int/eur-lex/lex/LexUriServ/site/es/com/2006/com2006_0045es01.pdf
3. Comisión Europea. *Plan de acción eEurope 2005.* Disponible en Internet: http://europa.eu/scadplus/leg/es/lvb/l24226.htm
4. European Comission. European Interoperability Framework. Disponible en Internet: http://europa.eu.int/idabc/en/document/3761

[41] DLM-FORUM. *Guidelines on best practices for using electronic information.* Disponible en Internet: http://europa.eu.int/ISPO/dlm/documents/guidelines.html

[42] Conde Villaverde, Mª Luisa. *Manual de tratamiento de archivos administrativos.* Ministerio de Cultura 1992.

[43] European Comission. *Architecture Guidelines.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/2317/5644

5. Decisión del Consejo de 27 de diciembre de 1986 relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones. Disponible en Internet: http://europa.eu/scadplus/leg/es/lvb/l24106.htm
6. OUEDRAOGO, LD. *Free/open source software (foss) and the Millennium Development Goals.* Mérida, octubre de 2005. Disponible en Internet: http://www.unsystem.org/jiu
7. MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades, versión 2.2 de junio de 2004.* Disponible en Internet: http://www.csi.map.es/csi/pg5c10.htm
8. MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *Propuesta de recomendaciones a la Administración General del Estado sobre utilización de software libre y de fuentes abiertas.* Disponible en Internet: http://www.csi.map.es/csi/pg5s44.htm
9. Conocido también como IDA II, pues daba continuidad al Programa IDA que se desarrolló en el período 1995-1999.
10. VALORIS. *Comparative Assessment of Open Documents Formats Market Overview.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/3439/5585#ODF
11. EUROPEAN COMISSION. *TAC approval on conclusions and recommendations on open document formats.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/3439/5585#recommendations
12. OASIS. *OASIS (Organization for the Advancement of Structured Information Standards).* Disponible en Internet: http://www.oasis-open.org/home/index.php
13. EUROPEAN COMISSION. *Responses from IBM, Microsoft and SUN to the TAC recommendations- Sept./Nov. 2004.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/3439/5585#responses
14. EUROPEAN COMISSION. *The Programme IDABC.* Disponible en Internet: http://europe.eu.int/idabc
15. MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *La construcción de los servicios pan-europeos de Administración electrónica.* Disponible en Internet: *http://www.csi. map.es/csi/pg3315.htm*
16. EUROPEAN COMISSION. *IDABC work programme 2005-2009.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/5101/3
17. OASIS. *OASIS Open Document Format for Office Applications (OpenDocument).* Disponible en Internet: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office
18. ISO/IEC. ISO/IEC 26300 *Open Document Format for Office Applications (OpenDocument) v1.0.* Disponible en Internet: http://www.iso.org
19. En concreto se encuentra en la etapa codificada como '*60.00 International Standard under publication*'. Véase: http://www.iso.org/iso/en/widepages/stagetable. html#60
20. Disponible en Internet: http://www.openoffice.org/
21. Disponible en Internet: http://www.koffice.org/
22. Disponible en Internet: http://www.abisource.com/
23. WIKIPEDIA. *Aplicaciones que soportan OpenDocument.* Disponible en Internet: http://en.wikipedia.org/wiki/Comparison_of_applications_supporting_OpenDocument
24. Aplicaciones que soportan OpenDocument. Fuente: http://en.wikipedia.org/wiki/Comparison_of_applications_supporting_OpenDocument
25. THE CONSORTIUMINFO.ORG. *Update: Massachusetts ODF Milestones, Due Dates and Schedule.* Disponible en Internet: http://www.consortiuminfo.org/standardsblog/article.php?story=2006040709301679
26. Australia National Archives. Disponible en Internet: http://www.naa.gov.au/

27. THE CONSORTIUMINFO.ORG. *Case Study II: A National Archive Moves to ODF.* Disponible en Internet: http://www.consortiuminfo.org/standardsblog/article.php?story=20060403090844 65
28. IDABC eGovernment Observatory. *FR: Official report recommends adoption of Open Document Format.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/6206/194
29. PRESSCENTER.ORG. *Communiqué de presse du Conseil des Ministres Utilisation de standards ouverts pour l'échange de documents bureautiques.* Disponible en Internet: http://presscenter.org/archive/20060623/432d0130470a88df1105dda38d1282b0/?lang=nl&prLang=fr
30. ODF ALLIANCE. *Newsletter 26 June 2006.* Disponible en Internet: http://www.odfalliance.org/press/Newsletter%2020060626.pdf
31. ODF ALLIANCE. Disponible en Internet: http://www.odfalliance.org/
32. JUNTA DE EXTREMADURA. *Acuerdo de Consejo de Gobierno de 25 de julio de 2006 para la implantación de programas informáticos libres en los ordenadores personales de la Junta de Extremadura.* Disponible en Internet: http://www.linex.org/mocion_consejo_ gobierno.pdf
33. DLM-Forum. Disponible en Internet: http://ec.europa.eu/transparency/archival_policy/dlm_forum/index_en.htm
34. EUROPEAN COMMISSION. *MOREQ: Model Requirements for the Management of Electronic Records* http://ec.europa.eu/idabc/en/document/2303/5644
35. COMISIÓN EUROPEA. *MoReq, Modelo de Requisitos para la gestión de documentos electrónicos de archivo.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/2631/5585 http://www.csi.map.es/csi/pg3315.htm#511
36. EUROPEAN COMMISSION. *Report on archives in the enlarged European Union.* Disponible en Internet: http://ec.europa.eu/transparency/archival_policy/docs/arch/reportarchives.pdf
37. *Recomendación del Consejo de 14 de noviembre de 2005 relativa a las medidas prioritarias para aumentar la cooperación en el ámbito de los archivos en Europa (2005/835/CE).* Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/site/es/oj/2005/l_312/l_31220051129es00550056.pdf
38. EUROPEAN COMMISSION. *IDABC work programme 2005-2009.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/5101/3
39. *Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.* Disponible en Internet: http://www.csi.map.es/csi/pg2001.htm
40. MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *MAGERIT versión 2, Metodología de análisis y gestión de riesgos de los sistemas de información.* Disponible en Internet: http://www.csi.map.es/csi/pg5m20.htm
41. DLM-FORUM. *Guidelines on best practices for using electronic information.* Disponible en Internet: http://europa.eu.int/ISPO/dlm/documents/guidelines.html
42. CONDE VILLAVERDE, Mª Luisa. *Manual de tratamiento de archivos administrativos.* Ministerio de Cultura 1992.
43. EUROPEAN COMMISSION. *Architecture Guidelines.* Disponible en Internet: http://ec.europa.eu/idabc/en/document/2317/5644

El documento electrónico como instrumento de prueba ante los Tribunales

GUILLERMO ORMAZÁBAL SÁNCHEZ*

RESUMEN: El artículo contiene un análisis de la problemática planteada por el uso del documento electrónico y especialmente la firma electrónica. Desde el punto de vista del derecho procesal, y en el marco de la antigua Ley de Enjuiciamiento Civil de 1881 y de la Nueva Ley de Enjuiciamiento Civil de 2000, así como del propio Código Civil, se cuestiona en primer lugar si el denominado documento electrónico es un verdadero documento a efectos probatorios o si es un medio de prueba «sui generis». Posteriormente se analiza en profundidad la última normativa sobre firma electrónica y el valor probatorio de los documentos firmados electrónicamente.

PALABRAS CLAVE: Documentos electrónicos. Firma electrónica. Medios de prueba en juicio. Valor probatorio del documento electrónico.

I. LA IRRUPCIÓN DEL DOCUMENTO ELECTRÓNICO EN EL MUNDO FORENSE

Uno de los numerosos ámbitos de la vida social donde se ha percibido el impacto y fuerza transformadora de las nuevas tecnologías de la información es el del tráfico documental. Y, por cierto, no en pequeña medida. La creación, reproducción, transmisión y conservación de los documentos ha experimentado mediante la informática un vuelco radical respecto de épocas anteriores. Los documentos en soportes electrónicos se confeccionan con mayor celeridad que antaño, cabe reproducirlos fácilmente y pueden ser remitidos y recibidos en pocos segundos cualquiera que sea el lugar del planeta donde se halle su destinatario.

Las repercusiones que esta evolución ha supuesto se han dejado sentir de modo muy particular en el campo de la actuación administrativa, en el del trá-

* Actualmente es Profesor de Derecho Procesal de la Universidad de Gerona.

fico comercial, y en el tráfico jurídico en general. La agilidad y la rapidez han pasado a resultar connaturales en ámbitos sociales otrora caracterizados por lo contrario.

La contrapartida de tan prometedora evolución es la aparición de ciertos riesgos, problemas y desafíos, tan novedosos como las propias tecnologías. La necesidad de garantizar la confidencialidad y de proteger la ingente masa de datos personales que circula por la red es uno de dichos retos. Pero en estas líneas voy a centrar mi atención en otro, tan poco desdeñable como el anterior: el de la fuerza probatoria de los documentos o soportes informáticos.

En efecto, la función primordial de todo documento es dejar constancia de ciertos eventos con el objeto evitar que alguien pueda cuestionarlos o negarlos. Tan relevante función probatoria resulta singularmente trascendente cuando se trata de acreditar ante un tribunal de justicia la autenticidad y veracidad de los hechos consignados en el documento.

En el transcurso de los siglos, el Derecho ha ido tejiendo una cuidadosa reglamentación en torno al valor y a la eficacia probatoria de los documentos tradicionales (o sea, los de celulosa, piel, pergamino, etc.), en la que cabe destacar la contundente fuerza que se concede al documento público. Suele decirse que, a diferencia del proceso penal, donde la prueba mediante testigos es con frecuencia la prueba más importante, en los procedimientos civiles la documental es la verdadera «reina de las pruebas» (*regina probatorum*), la prueba más segura, la más vigorosa, la que decanta el fallo a favor de uno u otro litigante.

El caso es que el documento electrónico (ya veremos que incluso esta misma denominación resulta jurídicamente problemática) ha irrumpido con fuerza en este reino. Si las relaciones jurídicas, tanto las privadas (compraventas, contratos con agencias de viajes, alquileres, etc.) como las de la administración con los administrados, van desarrollándose a través de redes telemáticas con mayor frecuencia, no debe sorprender que la presencia del documento electrónico resulte también cada vez más habitual en los litigios o pleitos antes los tribunales surgidos con ocasión de dichas relaciones jurídicas.

II. El problemático encuadramiento del documento electrónico en una legislación compleja. ¿Es el denominado documento electrónico un verdadero documento a efectos probatorios o un medio de prueba diferente?

1. *La situación legal durante la vigencia de la LEC 1881. La polémica entre el medio de prueba documental y el de reconocimiento judicial*

Hasta el siglo XXI el Derecho español ha mirado a la prueba mediante documentos o soportes informáticos con ojos del XIX. En efecto, los dos grandes cuerpos normativos que se ocupan de la fuerza probatoria de los documentos vieron la luz en dicha centuria: la Ley de Enjuiciamiento Civil de 1881 (en adelante, para abreviar LEC) que regula el proceso judicial ante los tribunales civiles; y el

Código Civil (en adelante, para abreviar CC), que data de 1889 y que contiene algunas normas sobre el documento. En este momento nos interesa sobre todo la ley procesal, pues es la que tiene por cometido regular el modo de practicarse la prueba ante los tribunales y su eficacia o valor.

Como el legislador procesal del siglo XIX no podía prever el imponente desarrollo que la tecnología iba a experimentar en los años posteriores, los primeros documentos electrónicos toparon con leyes que no se adecuaban a su naturaleza o peculiar modo de ser y con una judicatura que, en no pocas ocasiones, miraba la tecnología con el –en parte lógico– recelo y desconfianza propios del desconocimiento.

Surgió entonces una polémica que, si bien con perfiles y parámetros diferentes, no ha quedado en la actualidad, como veremos más adelante, totalmente apaciguada. Se discutía, efectivamente, sobre el encuadramiento del documento electrónico dentro del catálogo de medios probatorios previsto en el Código y en la Ley de Enjuiciamiento Civil (arts. 1215 CC y 578 LEC), y más en concreto, la procedencia de su introducción en el proceso como prueba documental o de reconocimiento judicial.

En efecto, las pruebas se introducen en el proceso mediante los denominados medios de prueba, previstos en la LEC (en la actualidad, los enumerados en el art. 299 de la LEC 2000). Se trata de una serie de cauces, de modos de proceder reglados, a través de los cuales han de practicarse o producirse en un juicio las pruebas destinadas a esclarecer los hechos controvertidos.

En concreto, los medios de prueba tradicionales, previstos por la LEC de 1881, eran: la prueba mediante peritos, cuando se tratase de aclarar cuestiones técnicas científicas, etc., discutidas en el proceso; la prueba mediante el interrogatorio de las partes litigantes (también denominada «confesión judicial»); la prueba mediante testigos; la prueba de reconocimiento o inspección judicial, cuando para el esclarecimiento de los hechos resulte útil que el propio juez tome contacto directo con estados de cosas, objetos, lugares, etc., para hacerse una idea de los hechos (reconocimiento de un inmueble ruinoso, por ejemplo); la prueba mediante documentos, públicos o privados.

El legislador decimonónico, como es lógico, no preveía un medio de prueba específico para los soportes informáticos. Pero incluso en el supuesto de que se acabase concluyendo que la prueba mediante documentos electrónicos no encontraba acomodo en ninguno de los medios probatorios referidos, parecía existir acuerdo entre los juristas y en la jurisprudencia acerca del carácter de *numerus apertus* de aquél catálogo de medios probatorios[1], lo que

[1] STS de 30 de Noviembre de 1992 (RAJ 9458). DE LA OLIVA, *Derecho Procesal Civil*, T-II, Madrid 1991, pp. 279 y ss; MONTERO AROCA consideraba que la discusión sobre el carácter de *numerus apertus* o *clausus* de la enumeración legal de medios probatorios es inútil: los medios de prueba serían los tasados en la ley, pero las fuentes de prueba, entendidas como elementos existentes en la realidad, podrían incorporarse al proceso mediante alguna de las actividades procesales en que consiste la noción de medio probatorio. En concreto, los documentos electrónicos, cintas de vídeo, etc., constituirían fuentes de prueba que habrían

permitiría su introducción en el proceso siguiendo analógicamente la regulación del medio con el que pudiese guardar una cierta semejanza.

Lo que sin lugar a dudas no cabía era rechazarlo. Toda limitación o restricción en el uso de pruebas –a menos que estuviese fundada en la necesidad de proteger otros derechos fundamentales como el del honor o la intimidad (y no puede decirse, al menos con carácter general, que sea éste nuestro caso)– resultaría difícilmente compatible con el derecho a la prueba constitucionalizado en el art.24.2 de la Constitución[2]. En efecto, nada más contrario al derecho de los ciudadanos a obtener la tutela que dispensan los órganos judiciales, que desdeñar medios de prueba que pueden aportar luz sobre la procedencia de sus reclamaciones, sólo porque el legislador haya descuidado establecer un medio de prueba *ad hoc*. Únicamente cabe rechazar pruebas cuando resulten ilícitas, impertinentes o inútiles, negativas propiedades que no cabe predicar, abstractamente, de los documentos electrónicos.

Parecía preciso, pues, encuadrar el documento electrónico en alguno de los medios de prueba ya existentes, con el fin de determinar de qué modo y en qué momento procesal había de aportarse y otras muchas cuestiones relevantes sobre su régimen jurídico, muy especialmente el valor o fuerza probatoria que cabía asignarle. Un sector muy amplio de la ciencia jurídica se decantó por la opción de asimilar la prueba mediante soportes informáticos a la prueba documental, en razón de las innegables analogías funcionales y conceptuales existentes entre el soporte electrónico y el tradicional. Otros, por el contrario, se decantaron por la opción de considerar que, a efectos de prueba, los documentos probatorios debían ser considerados como objeto de la prueba mediante reconocimiento judicial: se trata, sostenían, de que el juez entrase en contacto directo con una realidad determinada para formarse su propio juicio sobre los hechos controvertidos, en este caso visualizando el contenido del documento en una pantalla. Tanto si se trataba de una prueba de reconocimiento judicial como si se afirmaba el carácter documental, dichos medios probatorios podían practicarse simultáneamente con la prueba pericial, es decir, con la concurrencia de expertos informáticos que aportasen sus conocimientos técnico-científicos para ilustrar al juez sobre la fiabilidad, manipulabilidad, etc., de los instrumentos o soportes presentados.

Y por lo que a su eficacia o valor probatorio concierne, estaba de más cualquier otra observación que no consistiese en la pura remisión a las correspondientes normas de la LEC de 1881, que –con la salvedad de la confesión y

---

de ser incorporadas al proceso a través de alguna de las actividades que la ley denomina «medios». Cfr. *Derecho Jurisdiccional*, t. II, vol. 1º, Valencia 1991, pp. 225 y ss.; CORTÉS DOMÍNGUEZ (con GIMENO y MORENO), *Derecho procesal Civil*, 2ª edic., Valencia 1997, p. 205. Véase al respecto el trabajo de PICÓ I JUNOY, donde se abunda en esta idea con abundantes citas doctrinales y jurisprudenciales. Cfr. *El Derecho a la prueba en el proceso Civil*, Barcelona 1996, pp. 176 y ss.

[2] En este sentido véase PICÓ I JUNOY, *El Derecho a la prueba en el proceso Civil*...cit.p.178, quien cita la doctrina defensora de esta tesis y sostiene que el precepto constitucional consagra el «principio de libertad de prueba».

del documento público o del privado reconocido por la parte a quien haya de perjudicar– consagran el principio de libre apreciación de la prueba (cfr. arts.609, 632 y 659 LEC). Tanto si se acogía la opción documental como la del reconocimiento, sería, pues, el juzgador quien, en atención al bagaje probatorio acopiado y al resto de circunstancias concurrentes, resolviese libremente sobre el valor que quepa atribuir en cada caso al documento electrónico aportado en un proceso. En efecto, valoración libre de la prueba (contrapuesta a la denominada «valoración legal de la prueba») significa que el juez otorga a las pruebas practicadas la credibilidad, el valor de convicción que le sugiera su sentido común, su sano juicio o buen razonar (la ley procesal utiliza la expresión de «las reglas de la sana crítica»), sin que la ley le ordene atribuir a dichas pruebas un valor o fuerza de convicción concreta. Sólo existían reglas de valoración legal en el caso de la confesión en juicio (cuando un litigante reconocía hechos afirmados por su adversario que le resultaban completamente perjudiciales) y en el de los documentos públicos, es decir, los intervenidos o adverados por un fedatario público –sobre todo un notario– como es el caso de las escrituras públicas, etc. Singularmente en este último supuesto, la ley obliga al juez a tener por ciertos, sin posibilidad de cuestionamiento, todos aquellos extremos o aspectos que el notario haya comprobado personalmente mediante sus sentidos (la identidad de los personados, el tenor de sus declaraciones, la fecha, etc.). Se dice, en este caso, que el documento, «hace prueba plena».

En definitiva, sin pretender minusvalorar el valor teórico de dicha discusión y sin desconocer que existían motivos razonables para apoyar una u otra postura, personalmente siempre traté de argumentar que la opción entre prueba documental y reconocimiento judicial carecía de la relevancia que en ocasiones se le atribuía. O en otras palabras: el documento electrónico podía desplegar en el proceso su virtualidad probatoria con igual eficacia tanto si se admitía como prueba documental o de reconocimiento judicial. La valoración de cada uno de estos medios de prueba, como se vio, no está beneficiada por normas de valoración legal, lo que sólo sucede en el caso del documento público. Tanto en uno como en otro caso el juez decide sobre su fiabilidad o credibilidad conforme a su sano juicio.

2. *El documento electrónico en la LEC 2000: el documento electrónico como medio de prueba* sui generis

A mi parecer, en realidad el llamado documento electrónico no se adecuaba del todo a ninguno de ambos medios probatorios: ni era exactamente equiparable a un documento, aunque presentase múltiples semejanzas con él; ni el reconocimiento judicial era el cauce probatorio idóneo para traerlo al proceso.

Como la idoneidad y admisibilidad abstractas del documento electrónico como prueba parecían, como acabamos de ver, indudables durante la vigencia

de la LEC de 1881, no resultaba estrictamente necesaria una reforma legal que le confiriese valor probatorio expreso. Sin embargo, ausencia de estricta necesidad no significaba que una previsión legal explícita hubiese de dañar. Muy al contrario, dicha previsión podría resultar conveniente caso de advertirse una resistencia injustificada por parte de los tribunales a admitir la prueba mediante soportes informáticos o una tendencia a infravalorar o desdeñar su virtualidad probatoria, lo que efectivamente sucedió en la práctica en no pocas ocasiones.

El legislador, consciente de todo ello y de la progresiva importancia que va alcanzando el documento electrónico en el tráfico jurídico, ha decidido clarificar definitivamente esta cuestión en la Ley de Enjuiciamiento Civil de 2000, que vino a suplantar la tan anticuada e imperfecta LEC de 1881. Y lo ha hecho configurando un medio probatorio *ad hoc* (art. 299.2 LEC), sin tomar partido, pues, a favor de ninguna de las dos posturas antes expuestas. Queda, pues, claro que, en principio, los soportes electrónicos o –para seguir la terminología común– documentos electrónicos, no son documento por lo que atañe a la prueba, sin perjuicio de que su régimen probatorio siga al de los documentos en muchos aspectos.

En efecto, el art. 384 LEC regula la prueba mediante soportes o documentos informáticos y los denomina *instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso.* Su tenor literal es el siguiente:

> 1. Los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, que, por ser relevantes para el proceso, hayan sido admitidos como prueba, serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar y de modo que las demás partes del proceso puedan, con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga.
>
> 2. Será de aplicación a los instrumentos previstos en el apartado anterior lo dispuesto en el apartado tercero del artículo 382. La documentación en autos se hará del modo más apropiado a la naturaleza del instrumento, bajo la fe del Secretario, que, en su caso, adoptará también las medidas de custodia que resulten necesarias.
>
> 3. El tribunal valorará los instrumentos a que se refiere el apartado primero de este artículo conforme a las reglas de sana crítica aplicables a aquéllos según su naturaleza.

De la regulación de la prueba mediante instrumentos interesa destacar lo siguiente:

1. Régimen de aportación: En lo que atañe al régimen de aportación, la Ley los equipara al documento (arts. 265 y ss. LEC), es decir, han de aportarse junto con la demanda y su contestación o, por excepción, en otros momentos procesales posteriores (arts. 265.2, 3, 4; 270 y 271 LEC).

Es también oportuno advertir que el legislador ha preferido la expresión «instrumentos» a la de «soportes», señaladamente cuando se refiere a su apor-

tación al proceso (arts. 265 y ss. LEC). Creo que la dicción empleada por el legislador es acertada, pues el término «soporte» podría tal vez sugerir un «objeto» o materialidad que contiene cierta información, y resulta que estos medios de aportar certeza no tienen por qué ser traídos al proceso de dicho modo. No es que este término, estrictamente, sea incorrecto para referirse a la aportación por vías telemáticas, informáticas, etc. Me parece, sin embargo, que el de *medio* o *instrumento* es más abstracto y, por lo tanto, puede expresar mejor la posibilidad de presentar los documentos sin necesidad de aportar un objeto, materialidad o cosa. Cabe, en efecto, presentar ante el Tribunal estos instrumentos a través de medios telemáticos, informáticos, electrónicos, etc., diferentes a la entrega material de un objeto, señaladamente mediante el correo electrónico.

El art. 230.4 LOPJ dispone, en este sentido, que *las personas que demanden la tutela judicial de sus derechos e intereses podrán relacionarse con la Administración de Justicia a través de los medios técnicos a que se refiere el apartado primero* (cualesquiera medios técnicos, electrónicos, informáticos y telemáticos) *cuando sean compatibles con los que dispongan los Juzgados y Tribunales y se respeten las garantías y requisitos previstos en el procedimiento de que se trate.* Y, por su parte, el art. 135.5 LEC indica que *cuando los tribunales y los sujetos intervinientes en un proceso dispongan de medios técnicos que permitan el envío y la normal recepción de escritos y documentos, de forma tal que esté garantizada la autenticidad de la comunicación y quede constancia fehaciente de la remisión y recepción íntegras y de la fecha en que se hicieren, los escritos y documentos podrán enviarse por aquellos medios, acusándose recibo del mismo modo y se tendrán por presentados, a efectos de ejercicio de los derechos y de cumplimiento de deberes en el tiempo establecido conforme a la ley.* Si, por ejemplo, la demanda se interpone utilizando el correo electrónico, nada impide que se acompañe a la misma un archivo informático como fichero adjunto, sin necesidad de aportar materialmente el disquete donde se recoge el archivo que pretende hacerse valer como prueba según lo indicado en el art. 384 LEC. Puede ser que en la actualidad nuestros Tribunales no dispongan de la necesaria infraestructura, dotación de medios o cualificación para tramitar los procesos de esta manera, pero no cabe excluir –parece que se tiende a ello decididamente– que en el futuro cambie esta situación.

2. Regulación flexible y amplia: Es de notar, asimismo, que el legislador no regula de forma detallada o minuciosa lo relativo a estos instrumentos. A mi juicio no podía ser de otro modo. Téngase en cuenta que el precepto debe acoger múltiples sistemas, procedimientos o formas de recoger datos en soporte electrónico y que, además, el prodigioso avance de la ciencia y de la tecnología podría convertir en trasnochada una regulación más concreta o diseñada a la vista del estado de la técnica o de la ciencia en un momento histórico preciso[3].

[3] En este mismo sentido, véase SANCHÍS CRESPO, C., *La prueba por soportes informáticos*, Editorial Tirant lo Blanch, Valencia 1999, p. 157.

3. La práctica de la prueba: El legislador se conforma con asegurar que los litigantes se sitúen en una posición de igualdad y con establecer la posibilidad de que se sirvan de pruebas instrumentales (especialmente la pericial) para acreditar la autenticidad o exactitud de los datos, cifras, etc.

Por otra parte, no parece preciso que el examen del instrumento se lleve a cabo indefectiblemente en el acto del juicio o en la vista del juicio verbal. En efecto, si las partes han conocido el contenido del instrumento antes de la celebración del juicio o de la vista, no tiene porqué resultar necesario, por ejemplo, visualizar el disquete en aquellos momentos, limitándose las partes, en su caso, a hacer las alegaciones pertinentes o a proponer las pruebas que tengan por conveniente, sin perjuicio de que, por los motivos que sea (imposibilidad o extrema dificultad de trasladarles copia, mal estado del original, la necesidad o conveniencia de hacer observaciones o en su caso formular preguntas a peritos) dicho examen haya de hacerse en aquellos momentos procesales, en concurrencia del juzgador, las partes, sus defensores y, en su caso, peritos. En todo caso, el art. 431 LEC no incluye la prueba de instrumentos entre aquellas que deben practicarse en el juicio y el art. 289.2 LEC, al especificar las pruebas que inexcusablemente deben practicarse en presencia del juzgador se refiere a la de instrumentos precedida de la expresión *en su caso*, suficientemente expresiva de la falta de necesidad.

4. Valoración de la prueba: El art. 384 LEC no ha querido hacer a este medio de prueba objeto de una valoración tasada o legal, sino que deja su ponderación a la libre, aunque no por ello arbitraria, apreciación del juzgador (e*l tribunal valorará los instrumentos a que se refiere el apartado primero de este artículo conforme a las reglas de la sana crítica aplicables a aquéllos según su naturaleza.*).

En este punto se plantea un interrogante de gran trascendencia: ¿cabe aplicar a estos instrumentos la regla de valoración legal propia del documento privado (art. 326.1 LEC), conforme a la cual, cuando su autenticidad no sea cuestionada por el adversario, deben tenerse por ciertos el hecho, acto o estado de cosas que documenten, la fecha y la identidad de los intervinientes?.

La similitud, en este aspecto, de los instrumentos informáticos con el documento tradicional me parece total y, por ende, creo que esta norma de valoración legal habría de aplicarse también a los documentos informáticos cuya autenticidad no haya sido cuestionada por el adversario. Es cierto, como hemos visto, que el precepto se remite a las reglas de la sana crítica. Pero lo hace, concretamente, *a las reglas de sana crítica aplicables a aquéllos según su naturaleza*, una naturaleza, tratándose de instrumentos informáticos, muy afín a la de los documentos tradicionales, lo que permite trasplantar a aquéllos las máximas de experiencia o reglas de la sana crítica positivizadas aplicables a éstos, una de las cuales es la de la autenticidad del documento no cuestionado.

3. *La contrarreforma* «documentista»: *las leyes 59/2003, de 19 de diciembre, de Firma Electrónica (LFE), y 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)*

A. Equiparación de los soportes electrónicos firmados con el documento en sentido estricto

Dentro de los cambios introducidos por la Ley de Firma Electrónica (en adelante LFE) de 2003 cabe destacar el otorgamiento de la consideración de documento a los soportes electrónicos que incorporen datos firmados electrónicamente (art. 3.5 y 8, primero inciso, LFE).

Esta equiparación resulta, cuando menos, sorprendente, puesto que la LEC de 2000 ha creado, como se vio, un medio de prueba específico para introducir en el proceso los instrumentos o soportes informáticos de archivo (cfr. arts. 299.2, i 382 a 384 LEC), resolviendo de este modo la polémica que, con anterioridad a la promulgación de la nueva LEC, surgió en torno a la posibilidad de catalogar dichos instrumentos como documento.

Esta tendencia, por así denominarla «documentista», ha sido adoptada también en la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (en lo sucesivo, LSSI): su art. 24.2 dispone que *en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.*

Como puede comprobarse, aún hay quien persiste en sostener que la consideración de dichos soportes como documento constituye una fuente de ventajas probatorias favorecedoras de su uso procesal, opinión que personalmente no comparto. No porque dicha equiparación me parezca conceptualmente insostenible, pues al contrario, la considero en muy buena parte plausible (véase al respecto lo que escribí en mi monografía *La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos*, Madrid 2000), sino porque no reporta las ventajas y eficacia que algunos le atribuyen. Y además, sorprende que con pocas palabras el legislador haya querido introducir respecto de los contratos concluidos en soporte electrónico una excepción al régimen probatorio general de la LEC que, como se ha visto, cataloga los instrumentos que ahora nos ocupan como un medio probatorio particular o *sui generis*, diferente de los documentos.

Hay que volver a recordar que, con la excepción de los documentos públicos, tanto en el supuesto de los documentos privados como en el caso de los instrumentos del art. 384 LEC rige el principio de libre valoración de la prueba, con la excepción del no cuestionamiento de la autenticidad del documento privado, regla de valoración legal que también parece analógicamente aplicable a los instrumentos del art. 384 LEC. Por este camino, en definitiva, lejos de potenciarse la prueba mediante instrumentos, no se hace otra cosa que aplicar el mismo régimen jurídico a fuentes de prueba equivalentes parcialmente, con los inconvenientes que esto comporta respecto de los aspectos en que las características de estos medios probatorios sean diferentes.

Esta ignorancia o desviación consciente del régimen general de la LEC, se ha plasmado también en los apartados 5º, 6º, 7º y 8º de el art. 3 de la Ley de Firma Electrónica. En efecto, el redactado del apartado 5º del art. 3 LFE dispone que se considera documento electrónico el redactado en un soporte electrónico que incorpore datos firmados electrónicamente. Y el inciso primero del apartado 8º del art. 3 LFE indica que el soporte en que se encuentren los datos firmados electrónicamente será admisible como prueba documental en juicio. Más concretamente, el legislador aclara en el apartado 6º del mismo artículo que el denominado documento electrónico puede ser el soporte de documentos públicos, privados y administrativos. Por otra parte, el art. 6.1 lleva a cabo la misma equiparación al definir «certificado» como documento firmado electrónicamente por un prestador de servicios de certificación (...).

Con independencia de que se considere acertado o no atribuir la categoría de documento a los soportes informáticos en cuanto a su tratamiento probatorio, parece difícil encontrar una razón plausible que justifique calificar como documento los soportes informáticos electrónicamente firmados o aquellos que incorporan contratos celebrados en redes informáticas, como hacen los preceptos legales antes mencionados, y en cambio catalogar como instrumentos del art. 384 LEC el resto de soportes electrónicos. O si se prefiere, no resulta fácil fundamentar en aquellos dos supuestos una excepción al régimen general de la LEC, cuando probablemente, al elaborar el art. 384, el legislador tenía precisamente *in mente* los dos casos mencionados.

En todo caso, no constituye motivo alguno de alborozo que el legislador muestre semejante desprecio por un logro penosamente conquistado por la LEC de 2000, a saber, la unificación de las reglas de procedimiento civil, en este caso en materia probatoria, en un solo texto normativo a donde, por poner algún ejemplo, se han trasladado las normas sobre valoración de documentos públicos que otrora contuviese la legislación relativa a los préstamos usurarios. Con la nueva LFE el legislador vuelve a la denostable costumbre de sus predecesores de promulgar leyes procesales extravagantes a la LEC, lo que no sólo crea confusión, engorro, falta de claridad e inteligibilidad, sino que –lo que es peor y ha sucedido precisamente en la LFE– se pueden introducir reformas que rompen la sistemática o coherencia interna de la propia LEC. La complicada y, como se verá, inútil remisión del art. 3 LFE al art. 326 LEC no arregla en absoluto el referido desaguisado.

B. El documento electrónico firmado como «documento de documento»

La construcción jurídica con la que el legislador lleva a cabo la equiparación del soporte informático electrónicamente firmado al documento tradicional me parece, por otra parte, técnicamente desacertada e innecesariamente complicada. En efecto, el instrumento informático no es simplemente equiparado al documento privado, público o administrativo según la condición del firmante y la concurrencia de ciertos requisitos, cosa que hubiera simplificado

enormemente las cosas, sino que aquel instrumento es el soporte de un documento público, privado o administrativo. Pero como dicho soporte también es un documento (art. 3.5 LFE), resulta que estamos ante una suerte «de documento de documento» o documento que documenta otro documento.

En vez de establecer una construcción tan artificiosa, ¿no hubiera sido mucho más sencillo crear la categoría de documentos electrónicos privados, públicos o administrativos?. Efectivamente, sin necesidad de profundizar demasiado en esta cuestión, es inevitable que surja el siguiente interrogante: ¿Quedan ambos documentos tan indisociablemente vinculados que no se pueden valorar por separado o, contrariamente, son susceptibles de valoración independiente?. Los apartados 7º y 8º del art. 3 LFE podrían fácilmente sugerir la tesis de la valoración separable. En efecto, el apartado 7º del referido artículo indica que los documentos a que se refiere el apartado anterior (los privados públicos o administrativos a los que el documento electrónico sirve de soporte) tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable. El apartado 8º del art. 3 LFE, a su vez, dispone que el soporte en que se encuentren los datos firmados electrónicamente será admisible como prueba documental en juicio, y a continuación establece una serie de normas relativas a la impugnación de estos documentos electrónicos. Es decir: la valoración del documento electrónico firmado y de los documentos a los que aquél sirve de soporte aparece en dos apartados separados.

Más adelante nos ocuparemos de resolver este problema al tratar sobre el valor probatorio de la firma electrónica (véase *infra* apartado *IV.2)* de este trabajo).

III. La ley 59/2003, de 19 de diciembre, de firma electrónica. Explicación de sus nociones centrales

1. *Introducción. La firma electrónica como elemento necesario para dotar de seguridad y fiabilidad a la prueba por documentos electrónicos*

La Ley 59/2003 (en adelante LFE) se propone, como el Real Decreto-Ley 14/1999 que la precedió[4], regular la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación (art. 1 LFE).

[4] La promulgación de Real Decreto-Ley 14/1999, primer texto con rango legal que reguló en Derecho español la firma electrónica, suscitó en su día cierta sorpresa por dos clases de razones. Por una parte, se trata de una materia que ha de ser regulada por normas con rango de ley. El hecho de regularse mediante Decreto-Ley revela la urgencia con que el legislador deseaba hacer viable la firma digital en nuestro ordenamiento. La justificación de esta urgencia radicaba, como señala la Exposición de Motivos, en el hecho de que en España existía ya un sector empresarial que podía prestar un servicio de certificación de firma electrónica con suficiente solvencia, así como en el deseo de ofrecer a los usuarios de los nuevos servicios elementos de confianza en los sistemas, permitiendo su introducción y rápida difusión.

Como habrá observado el lector, se han promulgado nada menos que dos normas con rango legal y una directiva de la Unión Europea en un espacio temporal relativamente breve, hecho muy expresivo o revelador de la extraordinaria relevancia de la firma electrónica.

La implantación de sistemas de firma electrónica y su utilización en el tráfico jurídico constituye uno de los mayores desafíos mundiales en materia de comunicación. No es exagerado afirmar que la consecución de un elevado grado de seguridad en la transmisión de datos mediante la firma electrónica podría convertir los sistemas telemáticos en el cauce ordinario del tráfico jurídico entre particulares y entre éstos y los poderes públicos. De hecho, la expansión y consolidación del comercio electrónico, muy desarrollado en la actualidad, depende en buena parte del perfeccionamiento de este medio de autenticación, sobre todo por lo que se refiere a las operaciones o transacciones de un valor o entidad elevada. Sin un sistema de autenticación como la firma electrónica, la eficacia probatoria de los soportes informáticos, recogidos en los arts. 382 a 384 LEC, puede quedar considerablemente debilitada y resultar un cauce poco atractivo e inseguro para desarrollar el tráfico jurídico. Pensemos, por ejemplo, en un contrato recogido en un disquete o en el disco duro de un ordenador. Sin la utilización de algún procedimiento de autenticación podría resultar, en la práctica, de mucha menos utilidad probatoria que un documento privado y merecer al juzgador una credibilidad parecida a un fax o a una fotocopia: ciertamente no mucha, a no ser que se disponga de otros medios de prueba sobre los hechos.

2. *Los prestadores de servicios de certificación*

Uno de los elementos centrales del nuevo régimen de la firma electrónica es, precisamente, el de los prestadores de servicios de certificación, a los que la LFE dedica la mayor parte de sus preceptos. Por tales entiende el art. 2.2 LFE la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Como es sabido, la función principal de estos prestadores consiste en actuar como terceros de confianza, es decir, acreditar, mediante sus certificados, que una determinada clave pública pertenece a una persona concreta.

Por otra parte, el legislador se anticipó en algunos meses a la aprobación de la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de Diciembre de 1999, por la cual se establece un marco unitario para la firma electrónica.

Esta presurosa forma de proceder resultó finalmente del todo innecesaria, porque la aplicación efectiva de algunos preceptos esenciales del Decreto-Ley precisaba un desarrollo reglamentario que no tuvo lugar hasta la promulgación del Orden de 21 de Febrero de 2000, por la cual se aprobaba el Reglamento de acreditación de servicios de certificación y de certificación de determinados productos de firma electrónica (BOE núm. 45, de 22 de Febrero de 2000, 3514). Las previsiones de esta normativa, por lo demás, nunca llegaron a desplegarse efectivamente.

Por lo que respecta a su régimen jurídico, la LFE los somete a cierta disciplina administrativa que se concreta en el control que sobre ellos ejercen determinados organismos y en un régimen sancionador. Estos prestadores de servicios de certificación, de creación libre y que actúan en régimen de libre competencia, no precisan licencia o permiso administrativo de ninguna clase para desarrollar su actividad, sino sólo cumplir ciertas obligaciones, especificadas en el Capítulo Y del Título III de la LFE (arts. 17 a 21).

La ley actual suprime la obligación introducida por el Decreto-Ley 14/1999 que imponía a dichos prestadores inscribirse en un registro creado a tal efecto en el Ministerio de Justicia (art. 7 del Decreto-ley).

3. *La certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica*

La LFE prevé un sistema voluntario de certificación de prestadores de servicios de certificación (a) y de dispositivos de firma electrónica (b) en su Título IV, Capítulo II (arts. 26 a 28).

(a) A diferencia del Decreto-Ley 14/1999, la LFE no confía el monopolio de la certificación (que denominaba «acreditación») de prestadores de servicios de certificación ni la certificación de dispositivos de firma electrónica a un órgano público, sino que establece en su art.26.1 que la certificación de un prestador de servicios de certificación es el procedimiento voluntario mediante el cual una entidad cualificada, pública o privada, emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que ofrecen al público. En el apartado 2º, se contempla también la posibilidad de que los prestadores que lo deseen soliciten la certificación a entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con el que dispone la Ley 21/1992, de 16 de Julio, de industria y sus disposiciones de desarrollo. De todos modos, tampoco en este supuesto se trata de un acto administrativo certificador como sucedía con la acreditación, que la confería un órgano público incardinado en el Ministerio de Ciencia y Tecnología mediante el correspondiente acto administrativo.

A pesar de todo, la relevancia de la certificación de los prestadores de servicios de certificación ha experimentado un retroceso sustancial en relación con la fuerza probatoria que le atribuía el Decreto-Ley 14/1999, donde el legislador confería a la firma que hubiera obtenido el equivalente de la actual certificación de prestadores de servicios de certificación (entonces se denominaba «acreditación») una presunción fronteriza con una verdadera presunción *iuris tantum* de autenticidad de la firma. Más adelante habrá oportunidad de tratar sobre el acierto de la modificación legislativa.

(b) El art. 27.1 indica que la certificación de dispositivos de firma electrónica es el procedimiento mediante el cual se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para ser considerado como dis-

positivo seguro de creación de firma. Y el apartado 2º del mismo artículo incrementa la intervención pública para esta modalidad de certificación, que ha de llevarse a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con el previsto en la Ley 21/1992, de 16 de Julio, de Industria.

4. *Otras nociones contenidas en la LFE especialmente relevantes en cuanto al valor probatorio del documento firmado electrónicamente*

Pese a la aparente asepsia o neutralidad tecnológica que el legislador ha querido imprimir en el texto, quien lo lea detenidamente podrá constatar que la LFE, al referirse a la firma electrónica, está pensando sobre todo en la firma digital, es decir, en una clase concreta de firma electrónica, la basada en criptosistemas de doble clave o criptografía asimétrica, que es la que ofrece mayores garantías de seguridad. Más adelante habrá ocasión de corroborar esta afirmación con ejemplos concretos.

El texto de la LFE presenta notables dificultades de comprensión, puesto que regula cuestiones técnicas de cierta complejidad. Consciente de estas dificultades, la LFE ofrece a lo largo de su articulado algunas definiciones que contribuyen a clarificar su contenido y que se ajustan esencialmente a las que aparecen en el art. 2 de la Directiva 1999/93/CE. En este momento no parece conveniente comentarlas todas. Me limitaré a algunas especialmente importantes por su relevancia en cuanto al valor probatorio de la firma.

1) El art. 3.1 LFE define la **firma electrónica** como el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
2) Junto a este concepto general de firma electrónica, la LFE (art. 3.2) define una clase específica o cualificada a la cual denomina **firma electrónica avanzada**, que se caracteriza por reunir singulares exigencias de seguridad. Concretamente, es definida como la firma electrónica que permite identificar al signatario y detectar cualquiera modificación de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. Aquí se constata con claridad la afirmación hecha páginas atrás: pese a la buscada neutralidad o asepsia con que se expresan las palabras de la ley, parece claro que «firma electrónica avanzada» es una expresión que equivale prácticamente a la de firma digital, firma basada en la criptografía asimétrica, puesto que, de hecho, sólo esta clase de firma puede garantizar la vinculación única al firmante y la creación por medios que éste puede mantener bajo su exclusivo control.
3) **Firma electrónica reconocida**. El art. 3.3 LFE señala que se trata de una firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. En los números que

siguen explicaremos qué significan estas dos nociones (certificado reconocido y dispositivo seguro de creación de firma). El apartado 4º del mismo precepto dota a la firma electrónica reconocida de una singular eficacia jurídica consistente en la equiparación con la firma manuscrita tradicional.

4) En el art. 24.1 LFE, el legislador define el concepto de **datos de creación de firma** como los datos únicos, por ejemplo códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica. Se está haciendo, pues, referencia a lo que anteriormente definíamos como clave privada. El art. 25.1 LFE, por su parte, define como **datos de verificación de firma** los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica. En esta definición coincide perfectamente con lo que más arriba hemos denominado clave pública.

5) Tanto la aplicación de los datos de creación de firma como la aplicación de los datos de verificación de firma se realiza a través de un dispositivo, es decir, de un programa o sistema informático, que se denominan respectivamente, según el art. 24.2 y 25.2 LFE, **dispositivos de creación o verificación de firma**. Pues bien, el art. 24.3 introduce la noción de **dispositivo seguro de creación de firma**, que no es otra cosa que un dispositivo de creación de firma que cumple los requisitos establecidos en el propio art. 24.3 LFE, al que el legislador hace merecedor de un alto grado de fiabilidad[5].

Hay que advertir, no obstante, que el legislador, calculada o involuntariamente, ha generado cierta confusión, puesto que no todos los requisitos de este art. 24.3 LFE se refieren a los dispositivos utilizados para aplicar los datos de creación de firma o clave privada, sino también a los dispositivos para generar esta clave (por ejemplo, las letras a y b).

Como veremos más adelante, la certificación de estos dispositivos seguros de creación de firma se prevé en el art. 27 LFE. En la certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados y excepcionalmente las aprobadas por el Ministerio de Ciencia y Tecnología, que se publicarán en el directorio de internet de este Ministerio (art. 27.3 LFE). Este sello de calidad podría llegar a influir decisivamente en el ánimo de los jueces llamados a apreciar el valor probatorio del documento firmado electrónicamente. En todo caso, la certificación ya no sirve, como sucedía con la acreditación del Decreto-Ley 14/1999, para otorgar clase alguna de presunción de autenticidad.

---

[5] Los requisitos relacionados en este precepto son los siguientes.

a) *Que los datos utilizados para la generación de firma pueden producirse sólo una vez y se asegure razonablemente su secreto.*

b) *Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivadas de los de verificación de firma o de la propia firma, y que la firma está protegida contra la falsificación mediante la tecnología existente en cada momento.*

c) *Que los datos de creación de firma puedan ser protegidas de forma fiable por el firmante contra su utilización por terceros.*

d) *Que el dispositivo utilizado no altera los datos o el documento que haya de firmarse ni impida que éste se muestre al firmante antes del proceso de firma.*

6) El art. 6.1 LFE entiende por **certificado electrónico** «un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un signatario y confirma su identidad». Como se ha dicho, la actividad principal de los prestadores de servicios de certificación (también denominados corrientemente entidades o autoridades de certificación) consiste en expedir estos certificados. La LFE contiene relevantes novedades en la regulación de los certificados:
   a) El art. 7 LFE ha introducido la posibilidad que las personas jurídicas sean firmantes, es decir, la posibilidad de emitir certificados a favor de personas jurídicas, cosa que el Decreto-Ley 14/1999 reservaba a las personas físicas, aunque algunas normas tributarias lo permitían, singularmente con respecto al impuesto de sociedades. Aun cuando el titular del certificado sea la persona jurídica, ha de solicitarlo una persona física, concretamente su administrador, representante legal o voluntario con poder suficiente para hacerlo. Este solicitante persona física es a quien la ley hace responsable de la custodia de los datos de creación de firma asociadas al certificado, en el cual ha de constar su identificación. Los datos de creación de firma sólo pueden ser utilizadas en las relaciones que la persona jurídica mantenga con las administraciones públicas o en la contratación de bienes y servicios que sean propios o referentes a su giro o tráfico ordinario. Si lo desea, la persona jurídica puede también imponer otras limitaciones al uso de la firma en razón de la materia o de la cuantía de las operaciones, aspectos que deben hacerse constar en el certificado
   b) La ley grava con una serie de obligaciones la emisión de certificados electrónicos. Son las contenidas en los arts. 17, 18 y 19 LFE. El primero se refiere a obligaciones relacionadas con la protección de datos personales (consentimiento de los solicitantes para obtener datos personales, relativos a la utilización de pseudónimos por parte de los firmantes, etc.). El art. 18 LFE contiene una larguísima enumeración de obligaciones relativas, sobre todo, a cuestiones de seguridad o fiabilidad técnica (no almacenar datos de creación de firma, proporcionar cierta información al solicitante antes de la expedición del certificado, mantener un directorio actualizado de certificados expedidos especificando si son o no vigentes, garantizar la consulta al respecto, etc.). El art.19 LFE obliga los prestadores de servicios de certificación a formular una declaración de prácticas de certificación en la que han de detallar las obligaciones que se comprometen a cumplir, las condiciones aplicables al uso, expedición, suspensión y extinción de la vigencia de los certificados, medidas de seguridad que se comprometen a observar, etc.
7) Existe un tipo cualificado de certificado al que el art. 11 LFE denomina **certificado reconocido** y que se caracteriza por contener la información descrita en el segundo apartado del propio artículo y ser expedido por un prestador de servicios de certificación que cumple, además de los especifi-

cados en los arts.18 y 19, los requisitos u obligaciones enumeradas en los artículos 12, 13 y 20 LFE, cosa que le proporciona especiales garantías de seguridad. Como se verá, el hecho que el certificado reúna esta condición es también muy relevante a efectos probatorios[6].

En cuanto a las obligaciones, la ley contiene un amplísimo catálogo. Algunas de ellas son de carácter previo a la expedición de los certificados (art. 12 LFE), otras relativas a la comprobación de la identidad y circunstancias personales de los solicitantes (art. 13 LFE) y, finalmente, el art. 20 LFE prevé, además, otra serie de obligaciones de diferente tipo.

IV. Firma electrónica y prueba

1. *El art.3.4 LFE: una equiparación a la firma tradicional carente de eficacia probatoria*

El apartado 4º de su art.3 LFE dispone que si la firma electrónica cumple los requisitos necesarios para ser considerada como firma electrónica reconocida (véase la definición que dimos en el apartado anterior), tendrá, respecto a los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel. Esto significa, en definitiva, lo siguiente: cuando una norma jurídica requiera la constancia de

---

[6] La información a la que alude el precepto cuando se remite al art. 11.2 LFE es la siguiente:

a) La indicación de que se expiden con aquella cualidad (de certificados reconocidos, se entiende).
b) El código identificativo único del certificado.
c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad o a través de un pseudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su Código de Identificación Fiscal.
f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
g) El comienzo y el fin del periodo de validez del certificado.
h) Los límites de uso del certificado, si se establecen.
i) Los límites del valor de las transacciones para las cuales puede utilizarse el certificado, si se establecen.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo de acuerdo con la finalidad propia del certificado y siempre que aquel lo solicite. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la cual represente y, en caso de ser obligatoria la inscripción de los datos registrales, de conformidad con el apartado segundo del artículo 13.

una firma como presupuesto para la producción de ciertos efectos jurídicos (para tener por presentada una solicitud o como requisito de forma para los contratos, por ejemplo), tanto valdrá una firma manuscrita como una electrónica. La equiparación con la firma manuscrita, pues, no permite otorgar a los instrumentos informáticos firmados electrónicamente un especial valor probatorio. Hay que recordar una vez más que la firma tradicional no prueba nada por sí misma, sino que ha de ser objeto de prueba, salvo, claro está, que haya sido reconocida por el adversario procesal. Eso mismo es lo que sucede con la firma electrónica en virtud de la referida equiparación. Lo que en todo caso desplegaría plena eficacia probatoria sería la firma cuya autenticidad hubiera sido probada. Pero el art. 3.4 LFE equipara la firma electrónica a la firma manuscrita, sin más calificativos, no a la firma manuscrita auténtica.

2. *Valoración probatoria del documento electrónico firmado*

Dentro la valoración probatoria del documento firmado electrónicamente deben distinguirse dos aspectos:

— La valoración en cuanto a la autenticidad del documento una vez fijada la valoración de la firma electrónica.

Al contrario que la firma manuscrita, la autenticidad de la firma digital no es disociable de la valoración de los datos cifrados. Puede, en efecto, suceder que la firma manuscrita de un documento tradicional sea auténtica pero que, ello no obstante, no lo sea el contenido del documento, puesto que su texto, una vez firmado, puede ser adulterado, falsificado o alterado[7]. En el caso de la firma electrónica, por el contrario, fijada la autenticidad de la firma queda excluida cualquiera duda sobre la autenticidad de la información documentada. Fijada la autenticidad de la firma, si el documento ha sido firmado por un fedatario público o por ciertos funcionarios o empleado públicos se aplicarán las normas de valoración legal de la prueba propias de los documentos públicos o administrativos, que hacen prueba plena (no desvirtuable) respecto de ciertos extremos[8].

[7] Tal sucedería cuando la declaración firmada en forma manuscrita haya sido posteriormente manipulada, adulterada o falsificada, al haberse añadido al texto aspectos que no figuraban en el momento de estampar la rúbrica, haberse suprimido otros que efectivamente constaban en aquel instante o, en general, haberse cambiado el contenido una vez rubricado. La autenticidad de la firma manuscrita, pues, no asegura absolutamente la autenticidad de la declaración. Y en Derecho español no hay una norma parecida a la del párrafo 440.2 de la Ley Procesal Civil alemana (ZPO): «Si consta la autenticidad de la firma o se advera notarialmente el signo manuscrito que figura al pie del documento, se presumirá que el escrito que aparece encima de estas firma o signo manuscrito es también auténtico».

[8] Véase art. 319.1 LEC: los documentos públicos hacen prueba plena del hecho, acto o estado de cosas que documentan, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y otras personas que, en su caso, hayan intervenido. Con respecto a los documentos administrativos Véase el apartado 2 de este mismo artículo.

El hecho de que la firma electrónica no haya sido fijada como auténtica, sin embargo, no implica necesariamente que el documento electrónico haya de ser tenido por inauténtico, puesto que, aún así, el interesado podría acreditar su autenticidad a través de otros medios de prueba.

— La valoración en cuanto a la autenticidad de la firma.

Este aspecto de la valoración del documento electrónico es disociable del anterior. Si la autenticidad de la firma electrónica es cuestionada por la parte contra la que se hace valer, ha de procederse conforme a lo que dispone el art. 3.8 LFE.

En efecto, como ya dije antes, soy partidario de una concepción unitaria del medio probatorio: se trata de un solo documento electrónico al cual, una vez establecida la autenticidad de la firma, se le aplican las normas de valoración de los documentos públicos, privados o administrativos (es decir, las contenidas en los arts. 319 y 326 LEC), según la condición de quien los haya firmado y la concurrencia de ciertos requisitos legales.

La diferencia con los documentos tradicionales radica, pues, en que la comprobación de que la firma electrónica es auténtica permite concluir con certeza que el contenido del documento es también auténtico, es decir, que no ha sufrido falsificación o alteración posterior a la firma. Precisamente lo relativo a la impugnación de la autenticidad de la firma es objeto de especial atención por parte de la LFE, concretamente en su art. 3.8. El precepto distingue dos casos:

(a) Si se impugna la autenticidad de la firma electrónica reconocida con la que se han firmado los datos incorporados al documento electrónico
(b) Si se impugna la autenticidad de la firma electrónica avanzada con la que se han firmado los datos incorporados al documento electrónico.

En el primero caso (a) el legislador se está refiriendo al cuestionamiento de la autenticidad de la firma cuando se alega la no concurrencia de los requisitos necesarios para otorgar a un certificado la consideración de reconocido, o cuando se discute la catalogación como seguro del dispositivo de creación de la firma o la consideración de avanzada de la firma. En el segundo caso (b), el legislador se estaría refiriendo a los casos en qué un litigante se limita a negar el carácter avanzado de una firma no reconocida. Analizamos ambos casos con más detalle:

A. Impugnación de la autenticidad de la firma electrónica reconocida con la que se han firmado los datos incorporados al documento electrónico

En este supuesto, la LFE dispone que se procederá a comprobar que el prestador de servicios de certificación, que expide los certificados electróni-

cos, cumple todos los requisitos establecidos en la Ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y especialmente, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes.

La expresión «se procederá» no significa que el Juez, ante la alegación de inautenticidad haya de iniciar una investigación sobre aquellos aspectos, sino que el aportante del documento electrónicamente firmado habrá de levantar la carga de proponer pruebas que demuestren la fiabilidad de los servicios del certificador. Y por lo que se refiere a la confidencialidad aludida en el precepto, es claro que no puede referirse a la confidencialidad, en el sentido de salvaguarda del secreto, reserva o no acceso de terceros al contenido de los mensajes cifrados. Este extremo no tiene, en principio, relevancia en materia probatoria. Puestos a atribuir un significado razonable a este término, lo más plausible parece ser traducirlo como equivalente a «inderivabilidad computacional» o «unidireccionalidad», es decir, la imposibilidad de derivar o extraer la clave privada de la clave pública. Así pues, la referida «confidencialidad» ha de interpretarse como una característica vinculada con la clave privada, es decir, con el aseguramiento de que nadie, ni el propio prestador de servicios de certificación ni ningún tercero, podrán tener conocimiento de la clave privada si su titular no la revela.

Por lo demás, considero del todo superflua la prolija atención que presta el legislador a los extremos sobre los que debe centrarse la prueba de quien presentó la firma electrónica cuya autenticidad se cuestiona. Para empezar, porque el carácter de «reconocida» de una firma no es un hecho que Juez haya de presuponer o del que deba partir, de manera que corresponda al adversario procesal la carga de acreditar que la firma no merece tal calificativo. El carácter «reconocido» de la firma, en efecto, es una calificación o adjetivo que el aportante de la firma atribuye unilateralmente a ésta y que descansa en una serie de presupuestos fácticos detallados en la ley, que, en caso de impugnación de la autenticidad, deben ser cumplidamente probados por dicho aportante. ¿A que viene entonces tan prolija enumeración de aspectos en los que debe recaer la prueba?. Bastaba decir simplemente que incumbe al aportante de la firma acreditar el carácter reconocido de la misma.

Además, lo que interesa propiamente no es tanto el carácter reconocido de la firma sino su autenticidad. Por lo tanto, eso es lo que habrá de probar quien aportó el documento firmado, en el caso de impugnación. Probablemente, si se acreditan los presupuestos fácticos sobre los que se basa el carácter reconocido de la firma[9], pocas dudas quedarán al Juez para, usando las reglas de la sana crítica, tener aquélla por auténtica. En todo caso –insisto– en caso de impugnación por parte del adversario procesal, lo que el aportante de la firma

[9] Para ser más exactos habríamos de decir: si se prueban los presupuestos de hecho que confieren a la firma el carácter de avanzada, al certificado la condición de reconocido y al dispositivo de creación de firma la consideración de seguro.

debe probar es su autenticidad, cosa que también podría hacer de un modo diferente a acreditar los requisitos necesarios para que la firma revista según la ley el carácter de «reconocida». Simplemente porque, según el art.3.9 LFE, no cabe negar efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida por el mero hecho de presentarse en forma electrónica. Y, aunque dicho precepto no existiese, también resultaría aberrante sostener que la autenticidad de una firma sólo puede probarse demostrando que merece la calificación legal de reconocida. Tal conclusión sería simplemente inconstitucional por contraria al art. 24.2 CE, al privar arbitrariamente de virtualidad probatoria a actos prueba no tachables de lícitos, inútiles o impertinentes.

En definitiva: si se impugna la autenticidad de una firma electrónica a la que su aportante atribuye el carácter de reconocida, será dicho litigante el gravado con la carga de probar su autenticidad, cosa que podrá hacer, o bien probando que efectivamente merece el calificativo legal de reconocida, al concurrir los presupuestos fácticos a los que dicha calificación legal se anuda; o bien de cualquier otro modo diferente previsto en Derecho. De donde se sigue que el texto del art. 3.8 LFE, con su enumeración o detalle, no hace otra cosa que oscurecer y complicar las cosas, o como mínimo, que resulta por completo superfluo. Bastaba, como máximo, con limitarse a recordar que la carga de probar la autenticidad de la firma (o su consideración legal de reconocida) grava al aportante del soporte informático firmado.

B. Impugnación de la autenticidad de la firma electrónica avanzada con la que se han firmado los datos incorporados al documento electrónico

En este caso, dice el apartado 8º del art.3 que se estará a lo establecido en el apartado 2 del artículo 326 LEC. La norma regula todo lo relativo a la impugnación de la autenticidad del documento cuando se cuestione el carácter avanzado de la firma que no tiene la condición de reconocida, es decir, cuando se discuta que el signatario pueda mantener los medios de creación de la firma bajo su exclusivo control, etc. (véase art. 3.2 LFE). El apartado segundo del art. 326 LEC regula la impugnación de la prueba por documentos privados. Establece, esencialmente, que el proponente de la prueba ha de solicitar el cotejo de letras o proponer otros medios de prueba que permitan demostrar la autenticidad del documento o, en nuestro caso, demostrar que el firmante del documento electrónico coincide con la persona a quien se atribuyó el documento. El cotejo de letras está exclusivamente pensado para los documentos manuscritos, de manera que quien aportó el documento electrónico deberá valerse de otros medios probatorios, singularmente la prueba pericial. Finalmente, aportadas o no aquellas pruebas adicionales, el Juez resolverá según las reglas de la sana crítica.

Pueden aplicarse aquí la mayoría de las consideraciones que hemos hecho respecto de la impugnación de la firma electrónica reconocida. La remisión,

concretamente al art. 326 LEC, carece de toda utilidad, fuera de resultar útil al legislador en su cruzada particular para recalcar que la prueba por soportes informáticos debe equipararse a la de documentos. En efecto, el cotejo de letras referido en el art. 326.2 LEC, como se ha dicho, es sólo aplicable a los documentos –llamémosles– tradicionales, de modo que a los documentos electrónicos firmados sólo cabría aplicarles la referencia a «cualquier otro medio de prueba que resulte útil y pertinente al efecto». Para lograr este resultado bastaba decirlo con muy pocas palabras, en vez de realizar una remisión a otro texto legal. De hecho, como se dijo, lo más adecuado hubiese sido que toda la regulación estuviese contenida en la LEC. Aunque la cuestión no reviste mayor trascendencia, cuando menos se hubiese evitado la complicada remisión introducida por la Disposición Adicional 10ª, que añade un nuevo apartado 3º a el art. 326 LEC, cuyo tenor literal es como sigue: *cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá de acuerdo con lo que establece el art. 3 LFE.* Es decir, el art. 326.3 LEC remite al art. 3 LFE, cuyo apartado 8º, a su vez, remite al 326.2 LEC.

3. *La relevancia probatoria de la acreditación de prestadores de servicios de certificación y de productos de firma electrónica. Consecuencias de la supresión de la presunción del art.3.1.II del Decreto-Ley de 1999*

El art.3.1.II del ahora derogado Decreto-Ley de 1999 establecía la presunción de que la firma electrónica avanzada reunía las condiciones necesarias para producir los efectos indicados en dicho apartado (equivalentes a los del actual 3.4 LFE), cuando el certificado reconocido en que se basase hubiese sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se hubiese producido estuviese certificado. Es decir, el Decreto-Ley de 1999 dotaba a la firma electrónica que ahora la LFE denomina «reconocida» de una muy enérgica presunción que potenciaba notablemente su valor probatorio. El requisito que había de añadirse al hecho de tratarse de una firma electrónica de las que la actual LFE denomina «reconocida» era que el prestador de servicios de certificación y el dispositivo de firma hubieran sido certificados, es decir, se hubieran sometido con éxito a cierto proceso dirigido a obtener un especial reconocimiento de fiabilidad, seguridad o solvencia técnica. Sin llegar propiamente a crear una verdadera presunción de autenticidad (por supuesto desvirtuable) se presumía que la firma electrónica reunía las condiciones para merecer la calificación de avanzada; que el certificado en qué se basaba cumplía los requisitos para tener la condición de reconocido y, por lo tanto, resultaba especialmente fiable o seguro; y que el dispositivo de creación de firma mediante el cual había sido producida reunía las condiciones para ser tenido por seguro. Como se puede comprobar, pues, el legislador, de manera indirecta, establecía una presunción prácticamente equivalente a la de autenticidad, que reportaba una inestimable utilidad a quien se sirviese en el proceso de este sistema de autenticación.

En efecto, la presunción del art. 3.1.II LFE eximía al proponente de la prueba de acreditar una serie de extremos, cuya demostración podría requerir una prueba pericial compleja y, quizás, considerablemente onerosa. Quien pretendía cuestionar la autenticidad de la firma había de hacer frente a la pesada carga de desvirtuar los hechos presumidos por el antiguo art. 3.1.II LFE (que la firma tiene la condición de avanzada, es decir, que permite la identificación material del signatario, etc.). Si el adversario no conseguía esta refutación –y es realmente difícil hacerlo– es poco probable que el Juez pudiera concluir, sin incurrir en arbitrariedad, que la firma y los datos firmados no eran auténticos. Sin la presunción del antiguo art. 3.1.II del Decreto-Ley de 1999, el uso de la firma electrónica como prueba pierde mucho atractivo. Una vez derogada en la actual LFE, cada vez que el adversario procesal cuestione la autenticidad, el proponente de la prueba de instrumentos firmados digitalmente habrá de hacer frente a aquella costosísima prueba. Sin una ayuda legal de aquella clase, el valor práctico de esta clase de prueba puede disminuir notablemente.

El modo de proceder del legislador alemán al transponer a su ordenamiento la directiva europea sobre firma electrónica contrasta con el cambio legislativo operado por el legislador español que acabamos de comentar. Efectivamente, en Alemania las consecuencias o efectos probatorios de la firma electrónica se han llevado a la norma procesal general, es decir, a la ZPO, concretamente a su § 371 a), que reza así:

> La apariencia de autenticidad que una declaración en forma electrónica genere como consecuencia de su verificación según lo dispuesto en la Ley de Firma Electrónica, sólo podrá ser arrumbada mediante hechos que permitan suscitar serias dudas de que dicha declaración haya sido realmente emitida por el titular de la clave de firma.

La verificación aludida en el precepto se refiere a la acreditación voluntaria de prestadores de servicios de certificación, prevista en el § 15.1 de la Ley alemana de Firma Electrónica (*Signaturgesetz*. Abreviadamente: SigG). Dicha acreditación corre a cargo de cierta autoridad pública y confiere una suerte de reconocimiento, marca o distintivo de calidad (*Gütezeichen*) de carácter oficial, que certifica un alto grado de seguridad técnica y administrativa en relación con los certificados reconocidos emitidos por el prestador de servicios.

Volviendo a la ley española, pese a no existir en la actualidad una presunción de las características descritas[10], el prestador de servicios de certificación puede, no obstante, haber superado un procedimiento de certificación, al que más arriba nos hemos referido, aunque no suponga un reconocimiento ofi-

[10] Como veremos en el epígrafe siguiente existe una presunción en el art. 28 LFE que puede incrementar considerablemente el valor probatorio del documento firmado electrónicamente. Como veremos, no se trata propiamente, sin embargo, de una presunción de autenticidad.

cial. Esta circunstancia, por sí misma, no implica ningún reforzamiento jurídico del valor probatorio de la firma electrónica, pero, indirectamente, su importancia puede resultar considerable, puesto que, de hecho, puede ejercer una notable influencia para persuadir al órgano judicial de la autenticidad de la firma. Efectivamente, si la actuación de las entidades de certificación, públicas o privadas, acaba distinguiéndose por su seriedad y alto grado de solvencia técnica, es posible que acaben ganándose un prestigio y reconocimiento generalizados que lleven a los juzgadores que han de valorar la prueba a no vacilar respecto de la autenticidad de la firma.

A no dudar, este modo de sucederse las cosas sería el ideal. La confianza de los tribunales en la firma electrónica no sería consecuencia de una imposición *ope legis* sino el reflejo lógico y normal del desarrollo de la ciencia y de la tecnología en el razonamiento probatorio de los órganos judiciales. Para que las cosas discurran de una manera tan afortunada hace falta, sin embargo, que exista un alto grado de permeabilidad, interacción o comunicación entre el mundo forense y el mundo de la tecnología y la industria. Como se sabe, no siempre ha existido la mejor sintonía entre estos ámbitos. No cabe descartar, por esta razón, un cierto grado, cuando menos inicial, de perplejidad o desconcierto en los tribunales ante la valoración probatoria de los soportes informáticos firmados electrónicamente. El medio para desvanecer aquella situación de duda será habitualmente la proposición de prueba pericial, cuando el adversario niega la autenticidad de la firma. Como decíamos, puede resultar una prueba compleja y onerosa y si los litigantes se ven frecuentemente precisados a recurrir a ella es probable que la utilización de la firma en el tráfico jurídico se resienta considerablemente.

En definitiva, será la práctica la que habrá de demostrar si la reputación y la solvencia técnica de los prestadores de servicios de certificación corren paralelas a la valoración que hacen de la firma electrónica los tribunales de justicia. O si se prefiere: será preciso esperar unos años para comprobar si el público confía en la firma electrónica como medio para autenticar transacciones para las que antes utilizaba la celulosa y la firma tradicional; o si, contrariamente, se retrae de dicho uso al comprobar la exigua confianza que los tribunales muestran frente a la firma electrónica o, en todo caso, de la necesidad de aportar pruebas periciales más o menos onerosas cada vez que el adversario procesal cuestiona su autenticidad. Así pues, la clave del éxito del nuevo sistema en materia probatoria radica en la confianza hacia la certificación de prestadores de servicios de certificación y de dispositivos de creación de firma.

Hay que resaltar aquí la novedad introducida por la LFE previendo la posibilidad de que esta actividad sea llevada a cabo por entidades privadas. Este hecho, en mi opinión, no constituye obstáculo o factor de inseguridad alguno. Al menos no por principio, sin perjuicio de que la práctica demuestre lo contrario. Ahora bien: no parece plausible que la justificación de esta novedad sea predominantemente la de asegurar la autorregulación de la industria, como parece razonar la Exposición de Motivos de la LFE:

> Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación. El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público.

Lo que no parece tener en cuenta el legislador al hacer estas afirmaciones es que no se trata tanto de que la industria diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación, sino de velar por las necesidades de toda clase de usuarios. Que los intereses de la industria y los de los usuarios pueden en algunos casos no converger armónicamente parece poco discutible, como lo parece también que alguna clase de intervención pública puede resultar muy saludable e incluso necesaria para corregir las disfuncionalidades de un mercado que, abandonado a su espontaneidad y dinámica, no siempre es capaz de satisfacer ciertos intereses esenciales.

4. *La presunción del art. 28 LFE*

Una novedad importante de la nueva LFE es la presunción introducida por su art. 28.1, cuyo tenor literal reza así:

> Se presumirá que los productos de firma electrónica aludidos en el párrafo d) del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el «Diario Oficial de la Unión Europea».

Lo que está en juego, si se demuestra la conformidad de los productos de firma electrónica con las normas técnicas, no es poca cosa, pues la presunción abarca nada menos los siguientes aspectos:

a) Que el prestador de servicios de certificación que expide certificados reconocidos utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte (cfr.art.20.1.d LFE)

b) Que el dispositivo de creación de firma ofrece las siguientes garantías (cfr. art.24.3 LFE):

   a Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

   b Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de

firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Como se ve, quien acredita la conformidad o ajuste de los productos de firma empleados con las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el «Diario Oficial de la Unión Europea» tiene muy fundados motivos para confiar en que su firma será considerada como auténtica por el Juez.

Dicha declaración de ajuste o conformidad la deben llevar a cabo, si se trata de dispositivos de creación de firma, entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo (cfr. art. 27.2 LFE). Si se trata de otros «productos» de firma electrónica (dispositivos de verificación de firma, por ejemplo), la LFE no especifica quien deba o pueda llevar a cabo dicha verificación. Recuérdese que los productos de firma electrónica sobre los que recae la presunción no son sólo los dispositivos de creación de firma, a los que se refiere el art. 24.3 ahora trascrito, sino cualesquiera otros, aludidos en el art. 20.1.d LFE, asimismo arriba trascrito.

Tal acreditación, realizada por la entidad correspondiente, habría de introducirse en el proceso por la vía de la prueba pericial, método mediante el que ingresan en el proceso las máximas de experiencia y los conocimientos científicos, tecnológicos, etc., necesarios para esclarecer los hechos controvertidos. Es el único modo, en concreto, de salvaguardar el derecho de defensa del adversario procesal, que podrá, además de aportar su dictamen o solicitar del Juez la designación de perito, solicitar la comparecencia en el juicio del perito de la parte contraria con el objeto de formularle preguntas y pedirle las aclaraciones que crea precisas.

De lo dicho se infiere que, a efectos probatorios, tanto o más valor que la acreditación voluntaria de los prestadores de servicios de certificación, posee la certificación de que los productos de firma electrónica se ajustan a ciertas normas técnicas. De la solvencia y fiabilidad de las entidades que emiten dichas certificaciones o declaraciones de ajuste o conformidad depende, pues, en muy considerable medida, la eficacia probatoria que pueda desplegar la firma electrónica.

5. *Tres problemas adicionales que pueden comprometer el valor probatorio del documento informático electrónicamente firmado*

Interesa dejar constancia en este momento que la firma electrónica resulta útil para acreditar la autenticidad del documento electrónico, es decir la

identidad de su autor aparente con su autor real. No es éste, sin embargo, el de la autenticidad, el único problema que puede comprometer el valor probatorio de la firma electrónica. Existen además, entre otros, tres importantes escollos a superar de los que voy a dar cuenta en las líneas que siguen.

A) La constancia temporal de la firma. El sellado temporal de los instrumentos informáticos

La LFE sólo exige que quede constancia temporal o cronológica respecto a la emisión y revocación del certificado, pero no respecto al momento de la firma, de manera que el adversario procesal podrá alegar que el instrumento fue firmado con posterioridad al momento de extinción del certificado. O en todo caso, presupuesta la vigencia del certificado, la misma fecha de la firma del documento puede resultar de vital importancia, por ejemplo para acreditar que la aceptación del contrato se realizó en el plazo que se había estipulado. En estos supuestos, salvo el improbable caso de que se disponga de otros medios probatorios, la eficacia probatoria quedaría disminuida, al no resultar probado el elemento cronológico. Para evitar este inconveniente, se pueden utilizar ciertos procedimientos de sellado temporal de los documentos, algunos de los cuales ofrecen garantías considerables de fiabilidad.

Este inconveniente ha sido detectado por el legislador en relación con la contratación electrónica con condiciones generales, concretamente en el artículo 5.2.II del Real Decreto 1906/1999, de 17 de septiembre, donde se exige acompañar el documento electrónico de una consignación de fecha y hora de emisión y recepción, si procede. En el mismo sentido que este Real Decreto, el artículo 25.I LSSI prevé la intervención de terceros de confianza para la consignación de fecha y hora en el ámbito general de la contratación electrónica:

> Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar.

Y con respecto a otros ámbitos, en relación con los asientos de presentación practicados en virtud de títulos presentados por vía telemática en los registros de la propiedad, mercantiles o de bienes muebles, el artículo 112.4 de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social (LMFAS), establece lo siguiente:

> [...] reglamentariamente se establecerán los criterios y el procedimiento para que los asientos de presentación que traigan causa de títulos presentados por vía telemática, dentro o fuera de las horas de oficina, se practiquen de modo correlativo a la hora de su recepción teniendo en cuenta a su vez la hora de presentación de los demás títulos que tengan acceso al Registro, tanto los presentados en papel como los presentados por vía telemática.

Y el artículo 4.1.II LFE, una vez establecida la posibilidad de que el uso de la firma en el seno de las administraciones públicas se supedite a condiciones adicionales fijadas por ley, especifica que una de estas condiciones adicionales puede ser, precisamente:

> [...] la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo.

Y especifica que:

> [...] se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

B) La falta de implementación del sistema de certificación voluntaria

Como hemos visto, al faltar una presunción como la del artículo 3.1.II del Decreto-Ley 14/1999, la fuerza probatoria de la firma electrónica depende en gran medida del «sello» de confianza que pueda otorgar la certificación de prestadores de servicios de certificación y de dispositivos de firma. Así pues, mientras no empiecen a funcionar estos certificadores, la firma electrónica se verá privada de buena parte de su potencial vigor probatorio.

Una mirada retrospectiva al precedente del Decreto-Ley 14/1999 no permite tejer grandes esperanzas: el sistema de acreditación no se puso nunca en marcha ni funcionaron nunca las entidades de evaluación ni el resto de los aspectos previstos en la ya analizada Orden del Ministerio de Fomento, de 21 de febrero de 2000, por la cual se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. Hay que confiar en que al menos los certificadores privados de la LFE actúen con una celeridad superior.

C) Registro y conservación de los certificados con el objeto de verificar *pro futuro* la autenticidad de los documentos

Sin duda un problema de considerable importancia que afecta a los documentos electrónicos, firmados o no, es el de su conservación o perdurabilidad en el tiempo, problema que no se presenta (no, al menos, de modo tan agudo) en el caso de los documentos tradicionales, muchos de los cuales han desafiado exitosamente al transcurso de los siglos e incluso de los milenios. En el caso de la firma electrónica, a dicho problema se añade otro: no basta con conservar el documento o soporte físico y los dispositivos que permitan su lectura. Es necesario, además, poder acreditar para la posteridad (es decir, para un tiempo futuro indeterminado y potencialmente infinito) la clave pública y

el certificado del prestador de servicios de certificación. En definitiva, ¿como podremos fiarnos de aquí a cuarenta, sesenta años, un siglo, si interesa a los efectos que sea, de la correspondencia de la clave pública que permite desencriptar el documento, con la persona que aparece como firmante del mismo?. ¿Como se va a acreditar en el futuro dicha correspondencia? ¿Deben conservar los prestadores de servicios de certificación los certificados ya extinguidos hasta el final de los tiempos? Y aunque así fuera ¿qué sucede si desaparece el propios prestador?

La LFE trata de resolver este problema del modo siguiente:

El art. 18 LFE, que establece las obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos, señala sólo que los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones: (...) *c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.* Mantener un directorio actualizado, ¿hasta cuándo, con qué alcance temporal?.

La concreción no es mucho mayor en el caso de los prestadores de servicios de certificación que emitan certificados reconocidos, a los que el art. 20. 1. f) LFE sólo obliga a *conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.*

El legislador es más explícito en lo que respecta a la desaparición o cese de la actividad del prestador de servicios de certificación. En este supuesto, el art. 21.3 LFE dispone que *los prestadores de servicios de certificación remitirán al Ministerio de Ciencia y Tecnología con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f). Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo.*

El legislador también parece haber detectado el problema al introducir en el art. 115 LMFAS[11] una disposición transitoria undécima a la referida Ley de Notariado mediante la que se excluye el uso del soporte electrónico para las matrices de las escrituras y de las actas hasta que los avances tecnológicos hagan posible su autorización o intervención y conservación en aquel soporte, y precisa, en consecuencia, que la regulación del documento electrónico del artículo 17 bis LN se refiere tan sólo a las copias de la matriz y, en su caso, a la reproducción de las pólizas intervenidas.

[11] Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social. Al respecto, véase apartado siguiente.

6. *La Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social (LMFAS): la firma electrónica en las funciones notarial y registral y, en particular, el documento público notarial en soporte electrónico*

Siguiendo un procedimiento legislativo que no merece ser alabado precisamente por su transparencia ni por su corrección técnica pero que desgraciadamente ya se ha empezado a convertir en habitual, el legislador aprovechó la denominada Ley de Acompañamiento de los Presupuestos Generales del Estado (Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, en lo sucesivo, para abreviar, LMFAS) para introducir en el Derecho español el uso de técnicas electrónicas, informáticas, telemáticas, etc. en el desarrollo de las funciones notariales y de registro y, especialmente, para incorporar a nuestro ordenamiento jurídico el documento público electrónico notarial.

La regulación a la cual nos referimos se encuentra en los artículos 106 a 115 LMFAS, agrupados en una sección octava (capítulo XI, título V), que lleva como rúbrica *Incorporación de técnicas electrónicas, informáticas y telemáticas a la seguridad jurídica preventiva*, y afecta a los notarios y los registradores de la propiedad, mercantiles y de bienes muebles. Concretamente, el artículo 106 LMFAS indica lo siguiente:

> [...] esta sección tiene por objeto regular la atribución, y uso de la firma electrónica por parte de notarios y registradores de la propiedad, mercantiles y de bienes muebles, en el ejercicio de sus funciones públicas.

El objeto de la regulación que nos ocupa se centra en estos aspectos:

A) *Necesidad de que los notarios y registradores sean titulares de una firma electrónica avanzada.* El artículo 107.1 LMFAS establece que los notarios y los registradores tienen que disponer, obligatoriamente, de sistemas telemáticos para la emisión, transmisión, comunicación y recepción de información. La Dirección General de los Registros y del Notariado es el órgano encargado de velar, mediante las instrucciones oportunas, para que aquellos sistemas se actualicen periódicamente, reúnan la solvencia técnica necesaria y garanticen la ruptura del nexo de comunicación, de manera que se impida el televaciado y la manipulación del núcleo central de sus respectivos sistemas de almacenamiento de la información.

El hecho de obligar a los notarios a disponer de aquellos sistemas telemáticos busca precisamente posibilitar la emisión, transmisión, comunicación y recepción de información digitalmente firmada, de conformidad con lo que disponen los artículos subsiguientes 108 a 115 LMFAS.

Según el artículo 109 LMFAS, los notarios y los registradores tendrán que obtener, tan pronto como tomen posesión de una plaza, una firma electrónica avanzada, basada en un certificado reconocido y producida por un dispositivo seguro de creación de firma. Además, el certificado reconocido tiene que

haber sido expedido por un prestador de servicios de certificación acreditado. El legislador, en efecto, quiere reservar la posibilidad de que los dispositivos de creación de firma de los notarios y registradores se sometan a condiciones y requisitos distintos (en principio, entendemos, más exigentes y rigurosos) de los que permitirían con carácter general la certificación, según lo previsto en el antiguo Decreto-Ley 14/1999. Como veremos a continuación, el artículo 108 LMFAS incluye entre los aspectos que deben ser objeto de un posterior desarrollo reglamentario *los requisitos a los cuales se tienen que someter los dispositivos de creación y verificación de la firma.*

El artículo 108 LMFAS remite al Decreto-Ley 14/1999 (ahora se tendrá que entender en la LFE) todo lo que se refiere a los certificados electrónicos de los notarios y registradores, que deberán vincular unos datos de verificación de firma a la identidad, calidad profesional, situación administrativa de los notarios y registradores en activo y también a la plaza de destino que tengan asignada. El desarrollo del resto de los aspectos relativos a los certificados (requisitos a los cuales deben someterse los dispositivos de creación y verificación de la firma, la forma en la que se tengan que generar y entregar a los titulares, menciones que debe contener el certificado, procedimiento y publicidad de su vigencia y suspensión y revocación) se llevó a cabo mediante los reglamentos oportunos. El artículo 109.1.c) LMFAS concreta más el contenido del certificado al señalar que tendrá que expresar que el uso de la firma electrónica se limita exclusivamente a la suscripción de documentos públicos u oficiales propios del oficio del signatario.

La ley no establece la necesidad de que los certificados en los que se basa la firma electrónica de los notarios hayan de ser emitidos por un prestador de servicios de certificación determinado. Según el artículo 109.3 LMFAS la generación de los datos de verificación de firma se llevará a cabo en el momento de tomar posesión de la plaza de destino, con intervención personal del signatario, en presencia de la autoridad corporativa competente y auxiliado por los mecanismos técnicos correspondientes. En todo caso, el prestador de servicios de certificación correspondiente, que no podrá almacenar ni copiar los datos de creación de firma, no emitirá el certificado antes de recibir la notificación electrónica, firmada por el titular del órgano corporativo competente, expresiva de los datos de creación de firma y acreditativa de la condición de notario o registrador del signatario, de su situación de servicio activo, plaza de destino y de haberse cumplido los requisitos de asunción de la firma reglamentariamente establecidos.

B) *Remisión de documentos entre notarios y registradores y entre éstos y los particulares (artículo 110 LMFAS).* En virtud del artículo 110 LMFAS, la firma electrónica adecuada a lo que disponen los artículos 108 y 109 LMFAS confiere eficacia jurídica a la remisión telemática de documentos públicos notariales, comunicaciones, declaraciones y autoliquidaciones tributarias, solicitudes y certificaciones. El precepto dota también de eficacia jurídica a la comunicación practicada de esta manera tanto entre los registradores y notarios entre

sí como de éstos con las administraciones públicas o cualquier órgano jurisdiccional, dentro de su respectiva competencia y en razón de su oficio, y también al envío de copias simples y notas simples informativas en soporte electrónico a entidades y personas interesadas, cuando consten al notario su identidad y el interés legítimo.

Con respecto a la remisión no ya de copias y notas simples sino de documentos e informaciones a los particulares, el apartado tercero del artículo 110 la prevé expresamente, pero reserva la concreción del valor y régimen jurídico de este tipo de comunicaciones a un futuro desarrollo reglamentario.

C) *Presentación de títulos en los registros mediante vías telemáticas (art. 112 LMFAS).* Entre los documentos objeto de comunicación o remisión entre notarios y registradores, destacan por su relevancia los que pueden dar lugar a la práctica de un asiento registral o, con otras palabras, los que sean susceptibles de calificación e inscripción registral. El notario que lleve a cabo la remisión de esta manera debe dejar constancia de la misma en la matriz o, si es el caso, en el libro indicador. El registrador, a su vez, tiene que comunicar al notario por vía electrónica la práctica del asiento de presentación o su denegación, y también la nota de calificación y realización de la inscripción, anotación preventiva, cancelación o nota marginal que corresponda según la legislación notarial. El notario deberá dejar constancia de haber recibido esta comunicación mediante testigo, bajo su fe, en la matriz y en la copia que expida.

D) *Formalización de negocios jurídicos a distancia con intervención notarial (artículo 111 LMFAS).* Uno de los aspectos de más trascendencia de la normativa que nos ocupa es la posibilidad de concluir negocios jurídicos en los que deba emitirse más de una declaración de voluntad sin necesidad de que los sujetos que intervienen se reúnan físicamente y concurran en presencia de un solo notario. Se trata, en definitiva, de abrir la posibilidad de que distintas personas puedan celebrar negocios jurídicos sin necesidad de desplazarse. El artículo 111 LMFAS, en efecto, dice lo siguiente:

> Por conducto electrónico podrán dos o más notarios remitirse, bajo su respectiva firma electrónica avanzada, el contenido de los documentos públicos autorizados por cada uno de ellos que incorporen las declaraciones de voluntad dirigidas a conformar un único negocio jurídico.

Las condiciones y procedimientos para la integración de las declaraciones de voluntad en un negocio unitario y la plasmación de éste en un solo documento público tendrán que ser desarrolladas reglamentariamente.

E) *Testimonios y certificaciones de los documentos electrónicos en soporte papel (artículo 113 LMFAS).* Las comunicaciones o notificaciones notariales realizadas por los notarios en soporte electrónico pueden ser testimoniadas en soporte papel. Y, a su vez, los registradores también podrán certificar en soporte de

papel las comunicaciones electrónicas que reciban o envíen conforme a la legislación hipotecaria.

F) *El documento electrónico público notarial (artículo 115 LMFAS).* Aparte de la trascendental novedad que implica el hecho mismo de permitir la utilización de instrumentos telemáticos para la realización de las tareas notariales y registrales, el artículo 115 LMFAS contiene la innovación sin duda más importante operada por la ley mencionada. Se trata de la introducción de un artículo 17 bis LN que crea la categoría del documento o instrumento público electrónico notarial. Dice, efectivamente, el artículo 17 bis. 1 LN lo siguiente:

> [...] los instrumentos públicos a que se refiere el artículo 17 de esta Ley no perderán dicho carácter por el sólo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquél de conformidad con la Ley reguladora del uso de firma electrónica por parte de notarios y demás normas complementarias.

Este precepto no despliega inmediatamente toda su efectividad, ya que se reserva al desarrollo reglamentario correspondiente lo que concierne a la regulación de los requisitos indispensables para la autorización o intervención y conservación del instrumento público electrónico (art. 117 bis 2.I LN). Consciente de las dificultades técnicas que en el estado actual de la ciencia y de la tecnología implica el almacenamiento de soportes electrónicos, el legislador ha introducido mediante el mismo artículo 115 LMFAS una disposición transitoria undécima a la referida Ley de Notariado. En esta disposición excluye el uso del soporte electrónico para las matrices de las escrituras y de las actas hasta que los avances tecnológicos hagan posible su autorización o intervención y conservación en aquel soporte, y precisa, en consecuencia, que la regulación del documento electrónico del artículo 17 bis LN se refiere tan sólo a las copias de la matriz y, en su caso, a la reproducción de las pólizas intervenidas. Al referirse, pues, al documento público electrónico, el legislador quiere aludir más precisamente a sus copias.

Continuando con el análisis del precepto, la Ley establece que las copias autorizadas de las matrices se podrán expedir en soporte digital con la firma electrónica del notario (art. 17 bis 3 LN), obtenida de conformidad con lo que disponen los artículos 108 y 109 LMFAS, ya examinados antes. Los diferentes apartados del artículo (concretamente del tercero al séptimo) hacen ciertas precisiones, entre las cuales parece conveniente destacar un par:

— Las copias sólo se podrán expedir para remitirlas a otro notario, a un registrador o a cualquier otro órgano de las administraciones públicas o jurisdiccional, siempre en el ámbito de su competencia y en razón de su oficio. También se pueden expedir copias, si son simples, para remitirlas a cualquier interesado cuando consten de manera fehaciente al notario su identidad e interés legítimo (art. 17 bis 3 LN).

— Las copias electrónicas tan sólo serán válidas para la concreta finalidad para la que se solicitaron, lo cual deberá hacerse constar expresamente en cada copia, de modo que en cada una de las mismas habrá que expresar aquella finalidad (art. 17 bis 7 LN).

En los términos ahora mismo referidos, el documento público en soporte electrónico se equipara al que consta en papel, lo cual, si no quedaba ya lo bastante claro con la dicción del apartado 1 del artículo 117 bis LN (los instrumentos públicos a los que se refiere el artículo 17 de esta ley no perderán este carácter por el hecho de estar redactados en soporte electrónico), resulta aún más explícito en el tenor literal del apartado 2.II del mismo precepto. En este apartado se indica que la autorización o intervención notarial del documento público tiene que estar sujeta a las mismas garantías y requisitos que los de todo documento notarial y, sobre todo, producirá los *mismos efectos*. Esto, como precisa a continuación el legislador, supone dos consecuencias:

— Con independencia del soporte electrónico, informático o digital en el que se contenga el documento público notarial, el notario deberá dar fe de la identidad de los otorgantes, de que según su opinión tienen capacidad y legitimación, de que el consentimiento ha sido libremente prestado y de que el otorgamiento se adecua a la legalidad y a la voluntad debidamente informada de los otorgantes e intervinientes (art. 17 bis 2.II.a LN).

— Los documentos públicos electrónicos, como los que constan en soporte papel, gozan de fe pública y su contenido se presume veraz e íntegro de acuerdo con lo que se dispone en ésta y en otras leyes (art. 17 bis 2.II.b LN).

En virtud de la equiparación de los instrumentos notariales electrónicos con el documento público tradicional, la valoración probatoria de aquellos es de carácter legal, es decir hacen prueba plena en los términos especificados en el artículo 319 LEC. Al igual que sucede con los documentos públicos en soporte de papel, parece que si el adversario procesal cuestiona la autenticidad del documento público electrónico, la manera subsiguiente de proceder deberá ser exactamente la misma que en el caso de los documentos públicos tradicionales; es decir, dar lugar al careo (*cotejo*) o comprobación que se prevé en el artículo 320 LEC, ya que la matriz u original del denominado documento público notarial, como hemos visto, no puede constar todavía en soporte electrónico (disposición transitoria undécima a la referida ley de notariado, introducida por el artículo 115.2 LMFAS).

Producción y gestión de documentos electrónicos de Archivo. Estado de la cuestión en España

MARGARITA VÁZQUEZ DE PARGA*

RESUMEN: Después de recorrer los principales pasos de implantación de la administración electrónica en España, se analiza en profundidad la situación actual de la producción y de la gestión de documentos electrónicos de archivo en las distintas administraciones públicas, incluyendo el actual proyecto de Ley de acceso electrónico de los ciudadanos a la Administración.

PALABRAS CLAVE: Administración electrónica. Archivos electrónicos. Documentos electrónicos de archivo. Firma electrónica.

INTRODUCCIÓN

A pesar de la tantas veces anunciada desaparición del papel como soporte para la plasmación de las transacciones administrativas, parecía que no iba a llegar nunca. Sin embargo, ante el imparable avance de la Sociedad de la Información, y el decidido empeño de las Administraciones en implantar la administración electrónica, y eliminar el papel, su sustitución como soporte de los documentos administrativos por el soporte electrónico, con pleno valor administrativo y legal, empieza a ser una realidad[1]. A pesar de ello, no debemos pensar que va a dejar de utilizarse el papel, aunque esperemos que se reduzca[2].

* Ex-Subdirectora General de los Archivos Estatales.

[1] VÁZQUEZ DE PARGA, Margarita: «Documentos electrónicos: Estándares para su creación», Boletín de la Confederación de Asociaciones de Archiveros, Bibliotecarios, Museólogos y Documentalistas, LIII (2003), nº 4, en el que se describe el grado de implantación de la e-administración en España a la fecha.

[2] Existe una cultura tan arraigada de su utilización y la tecnología ofrece tantas facilidades para imprimir y pasar a soporte papel los documentos producidos electrónicamente, que no se debe esperar su desaparición al menos en un plazo de tiempo corto.

Si bien han pasado dieciséis largos años desde que se inició la puesta en marcha de la administración electrónica, con la aprobación de la Ley 30/1992, de las Administraciones Públicas y del Procedimiento Administrativo Común[3], Ley que debe considerarse como la partida de nacimiento de la administración electrónica en nuestro país, y que se recibió con gran incredulidad por amplios sectores de la administración, y aún más por el sector de los archivos, es cierto que un cambio de cultura administrativa tan radical no puede llevarse a cabo en un período de tiempo corto, ya que exige el desarrollo legal y normativo que adecue el procedimiento administrativo a la tecnología de forma que se garantice el necesario valor legal y seguridad a las transacciones administrativas realizadas por medios informáticos, electrónicos y telemáticos[4], el desarrollo de las infraestructuras tecnológicas y de comunicación y el de soluciones y aplicaciones tecnológicas que faciliten la gestión y permitan mantener y mejorar el nivel de servicios ofrecidos a los ciudadanos.

En este sentido, el *Proyecto de Ley de Acceso electrónico de los ciudadanos a las administraciones Públicas*, aprobado en Consejo de Ministros el 1 de Diciembre

---

[3] *Ley 30/1992 de Régimen de las Administraciones Públicas y del Procedimientos Administrativo Común*, BOE nº 285, de 27 de Noviembre, 1992, (modificada por *Ley 4/1999 14 enero 1999*). Cabe destacar el Artº 45.5 en el que se establece que «los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, ... o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia del documento original, siempre que quede garantizada su autenticidad, integridad y conservación, y en su caso, la recepción por el interesado...»

[4] A partir de la Ley 30/1992, se aprueba toda una serie de normas legales que profundizan en distintos aspectos con el objetivo de dar legalidad a las transacciones administrativas y la emisión de documentos por medios informáticos, electrónicos y telemáticos, de entre las que destacamos las siguientes, de aplicación general:

Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas para la Administración General del Estado. BOE nº 52, de 29 de Febrero de 1996.

Real Decreto 209/2003 de 11 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. BOE nº 51, de 28 de febrero de 2003,

Ley 24/2001 de 27 de Diciembre, por la que se regula la: Notificación electrónica, Consulta de expedientes, Sistema de certificación Seguridad en la tramitación telemática, Real Decreto Ley 14/1999 sobre firma electrónica, Ley Orgánica 15/1999 de Protección de datos de carácter personal, Ley 34/, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico Real Decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, *Orden PRE/1551/2003, de 10 de Junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan....*BOE nº 141, de 13 de junio de 2003, *Orden PRE/1551/2003, de 10 de Junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan....*BOE nº 141, de 13 de junio de 2003, *Ley 59/2003, de 19 de diciembre, de firma electrónica, Ley General Tributaria de 2003*

Ver además: VÁZQUEZ DE PARGA, Margarita: *op. cit.* en donde se recoge la normativa legal con mayor amplitud, con especial referencia al articulado que supone cambios fundamentales en cuanto a la equiparación legal de los documentos independientemente de que se produzcan en soporte electrónico o soporte papel.

de 2006[5], viene a dar un paso más para la implantación real de la administración electrónica, con el objetivo de lograr una mayor eficacia y eficiencia de las Administraciones públicas, y facilitar la comunicación de los ciudadanos con éstas por medio de las tecnologías de la información y la comunicación, sin que tengan necesidad de desplazarse hasta las dependencias administrativas. Es también objetivo de la Ley cambiar el concepto que los ciudadanos tienen de la Administración, tal y como se explicita en su preámbulo: *En esas condiciones permiten también a los ciudadanos ver a la Administración como una entidad a su servicio y no como una burocracia pesada que empieza por exigir, siempre y para empezar, el sacrificio del tiempo y del desplazamiento que impone el espacio que separa el domicilio de los ciudadanos y empresas de las oficinas públicas..... Se da así un paso trascendental para facilitar, en igualdad de condiciones, la plena integración de estas personas en la vida pública, social, laboral y cultural.*

No menos importante es llevar a cabo la necesaria gestión del cambio que permita asimilar un cambio tan radical, y generar la confianza necesaria, tanto en los gestores administrativos como en los ciudadanos.

Tanto el desarrollo legal y normativo como las infraestructuras y soluciones tecnológicas han venido desarrollándose durante estos dieciséis años hasta llegar a un punto de madurez en el que se puede considerar que las administraciones pueden basarse en las TIC para la gestión y tramitación de sus relaciones con los ciudadanos.

Y como consecuencia inmediata de su implantación empieza a producirse, aunque lentamente, la tan anunciada sustitución del soporte papel por el soporte electrónico, que aún cuando todavía es muy incipiente, supone uno de los mayores retos archivísticos de los últimos años a los que deben hacer frente tanto las administraciones, en general, como las empresas y, por supuesto, los profesionales de los archivos.

Los esfuerzos de las distintas Administraciones para lograr el objetivo se hacen patentes en los proyectos que vienen desarrollando, entre los que cabe destacar:

- La intranet de la Administración General del Estado, que facilita el acceso y el intercambio seguro de información entre las distintas administraciones españolas así como con la Unión Europea.
- El Sistema de Aplicaciones y Redes para las Administraciones (SARA), que supone una disponibilidad de los servicios de la administración las 24 horas al día los 7 días de la semana, por medio del cual al menos doce Comunidades Autónomas pueden intercambiar información con la Administración central: Andalucía, Asturias, Baleares, Canarias, Cantabria, Castilla-León, Cataluña, Extremadura, Madrid, Murcia, País Vasco y

[5] *Proyecto de Ley de Acceso electrónico de los ciudadanos a las administraciones Públicas*, aprobado en Consejo de Ministros el 1 de Diciembre de 2006. disponible en internet [fecha de acceso dic. 2006] www.map.es

Valencia, así como otros organismos de la administración, como el Tribunal de Cuentas, el Consejo de Seguridad Nuclear o la Agencia de Protección de Datos y se empieza a desplegar en la administración local. Además del ahorro en tiempo y dinero que supone este proyecto, se estima que se ahorrarán 100.000 kilos de papel.

- El plan de Modernización, en el que la eliminación de papel ocupa un lugar importante: supresión de papel en las ventanillas de atención al ciudadano, facilitando la presentación telemática o en soporte informático de los documentos necesarios en un conjunto de trámites, y el que es fundamental para el tema que nos ocupa, el Sistema de tramitación telemática para ministros y altos cargos que dispondrán de firma electrónica,
- El plan Avanza[6], cuyas áreas de actuación prioritaria para los próximos años son el sector empresarial, especialmente las PYMES, la administración electrónica[7] y educación y ciudadanos, aspecto este último fundamental, ya que sin su participación toda la inversión en tecnología y medios para su funcionamiento quedaría infrautilizada.
- El documento de identidad electrónico, que es una pieza esencial para que los ciudadanos utilicen los medios que pone a su alcance el nuevo modelo de administración, sin necesidad de obtener el certificado de firma electrónica[8], y que, sin duda, repercutirá en una mayor producción de documentos electrónicos.

  La primera experiencia de emisión de eDNI se ha llevado a cabo en Burgos, en la que se han registrado, hasta el 5 de junio de 2006, 11.067 consultas de ciudadanos, centradas en los servicios digitales que ofrecen la Seguridad Social y el Ministerio de Administraciones Públicas a través de sus oficinas virtuales. Se prevé que en el año 2008

---

[6] El Plan cuenta con un presupuesto de 1.539,9 M?. 2007, de los que 329,9 M? se destinan a nuevas iniciativas. Ver www.planavanza.es (consultado en Febrero 2007)

[7] En el sector de las Administraciones Públicas se trata de impulsar una serie de servicios entre los que destacamos, por afectar a la producción de documentos electrónicos, los siguientes:

A.2.1.- Sanidad en línea

A.2.4.- DNI electrónico

A.2.5.- AGE: Administración electrónica

A.2.6.- Ciudades Digitales

A.2.7.- Ciudades Singulares

A.2.8.- Avanza Local: Impulso de la Administración electrónica en las Entidades Locales

[8] Proyecto de Ley.... Sección Segunda. Identificación de los ciudadanos y autenticación de su actuación. Artículo 13. Utilización del Documento Nacional de Identidad. Las personas físicas podrán, en todo caso, utilizar los sistemas de firma electrónica incorporados al Documento Nacional de Identidad en su relación por medios electrónicos con las Administraciones Públicas. El régimen de utilización y efectos de dicho documento se regirá por su normativa reguladora.

la totalidad de la población cuente con el eDNI, lo que sin duda favorecerá la utilización de los servicios digitales de las administraciones Públicas.

- Los proyectos promovidos por Red.es, en colaboración con las distintas administraciones.
- Los proyectos de desarrollo de una plataforma para la administración electrónica que se están llevando a cabo en las Comunidades Autónomas, entre las que destacan, en orden alfabético, Andalucía, con su proyecto W@nda, Asturias, con SPIGA, Soporte a la Producción, Información, Gestión administrativa y Archivo, Cataluña, y el País Vasco, por citar sólo a las Comunidades más avanzadas en su implantación.

El proyecto de Ley de acceso electrónico de los ciudadanos a las Administraciones Públicas

Pero como se ha mencionado anteriormente el proyecto de Ley de acceso electrónico de los ciudadanos a las Administraciones Públicas, se presenta como el impulso definitivo del Ministerio de las Administraciones Públicas para la implantación real de la administración electrónica. Por ello, no podemos pasar por alto determinados aspectos del Proyecto de Ley por la repercusión directa que tienen en la producción, gestión e identificación de los documentos electrónicos resultantes de las transacciones administrativas, esto es, en los documentos electrónicos de archivo.

En primer lugar, señalaremos algunas definiciones que se incluyen en el glosario que se incorpora en el Proyecto de Ley, que nos producen una cierta sorpresa e inquietud:

a) Actuación administrativa automatizada*: Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.* Esta definición parece un tanto optimista en su afirmación de que *no es necesaria la intervención de una persona física en cada acto singular,* pues la intervención de las personas físicas sigue siendo necesaria, al menos por el momento, aunque la tramitación se sustente sobre aplicaciones informáticas, electrónicas y telemáticas.

j) Documento electrónico: *Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.*

¿Se puede identificar en esta definición a los documentos resultantes de las transacciones administrativas, tal y como los define cualquier manual de procedimiento administrativo? Llama poderosamente la atención esta definición de documento electrónico, excesivamente general y omnicompren-

siva de cualquier tipo de información producida electrónicamente, ya que al no especificar las características que definen a los documentos administrativos considerados soporte legal de las actuaciones, tanto de las administraciones como de los administrados, esto es, su originalidad: identificación del firmante del documento; integridad: que el texto y los datos incluidos en el documento estén completos, sin que se haya suprimido ninguno; y autenticidad: que ninguno de los datos haya sido modificado o alterado, cabe cualquier tipo de información siempre que esté archivada en soporte informático.

A esta definición del glosario hay que añadir el concepto de Documento electrónico que se establece en el articulado del Proyecto de Ley[9], en el que se aprecia una cierta contradicción con la definición que se da en el glosario.

Así mismo, la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (art. 46.6,) precisa el concepto de documento administrativo, declarando que *tienen la consideración de documento público administrativo los documentos válidamente emitidos por los órganos de las Administraciones Públicas, cuyas características fundamentales son:*

- *Que siempre producen efectos frente a terceros o en la propia organización administrativa.*
- *Son válidos cuando cumplen una serie de requisitos formales y sustantivos, exigidos por las normas que regulan la actividad administrativa.*

Tampoco coincide la definición de documento con las que se hacen tanto en la Norma ISO 15489: *Información creada o recibida, conservada como información y prueba, por una organización o un individuo en el desarrollo de sus actividades o en virtud de sus obligaciones legales*[10] como en el Modelo de Requisitos para los Sistemas de Gestión de Documentos Electrónicos de Archivo, MoReq[11]: *Información creada o recibida, conservada como información y prueba, por una orga-*

---

[9] Artículo 26. Documento electrónico.

1. Las Administraciones Públicas podrán emitir validamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas tal como se establecen en la ley 59/2003, de 19 de diciembre, de Firma Electrónica.

2. Los certificados electrónicos previstos en los apartados c y d del artículo 12.1 podrán utilizarse para realizar firma electrónica de documentos administrativos.

3. Los documentos administrativos podrán incluir referencia temporal autenticada con sujeción a medidas de seguridad que lo garanticen.

[10] Norma ISO-UNE 15489. Documentación e Información. Sistemas de Gestión de documentos. 2006.

[11] Modelo de Requerimientos para los sistemas de gestión de documentos electrónicos de Archivos. Programa IDA. Comisión Europea, Luxemburgo, 2001.

nización o un individuo en el desarrollo de sus actividades o en virtud de sus obligaciones legales.

A mayor abundamiento, esta definición, digamos «tan Light» de documento electrónico, no parece coherente con la que se da en el Documento «Criterios de Seguridad» del Consejo Superior de Informática[12]: *Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente. El documento electrónico será soporte de:*

a. *Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.*
b. *Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.*
c. *Documentos privados.*

Tampoco concuerda con las definiciones de firma electrónica y sistema de firma electrónica que incluye el Proyecto de Ley, en las que se especifican las distintas formas de firma electrónica posibles, y que son esenciales para dar validez a los documentos administrativos en soporte electrónico[13].

Producción de documentos electrónicos de archivo

A partir de aquí vamos a tratar de analizar hasta qué punto se están produciendo en nuestro país documentos electrónicos de archivo en sustitución

[12] «Criterios de Seguridad de las aplicaciones para el ejercicio de las potestades. Consejo Superior de Informática, Ministerio de Administración Pública, Madrid 2004, www.map.es

[13] k) Firma electrónica: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, «conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante» l) Firma electrónica avanzada: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, «firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control». m) Firma electrónica reconocida: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, «firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma». q) Sistema de firma electrónica: conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

de los tradicionales documentos en soporte físico. Nos centraremos únicamente en el entorno de las Administraciones Públicas, sin entrar en el del sector privado.

Ante todo debemos aclarar qué entendemos y a qué nos referimos realmente cuando decimos «documentos electrónicos de Archivo».

¿Se pueden considerar documentos electrónicos de Archivo los documentos en soporte informático que no estén validados por una de las formas admitidas de firma electrónica? Desde nuestro punto de vista, no. Los documentos no validados son simplemente información en soporte electrónico, pero sin que tengan la categoría de documento de archivo ya que carecen de valor legal y probatorio. Y, en función de esta premisa debemos preguntarnos si en nuestro país se están produciendo documentos electrónicos de archivo y en que cantidad.

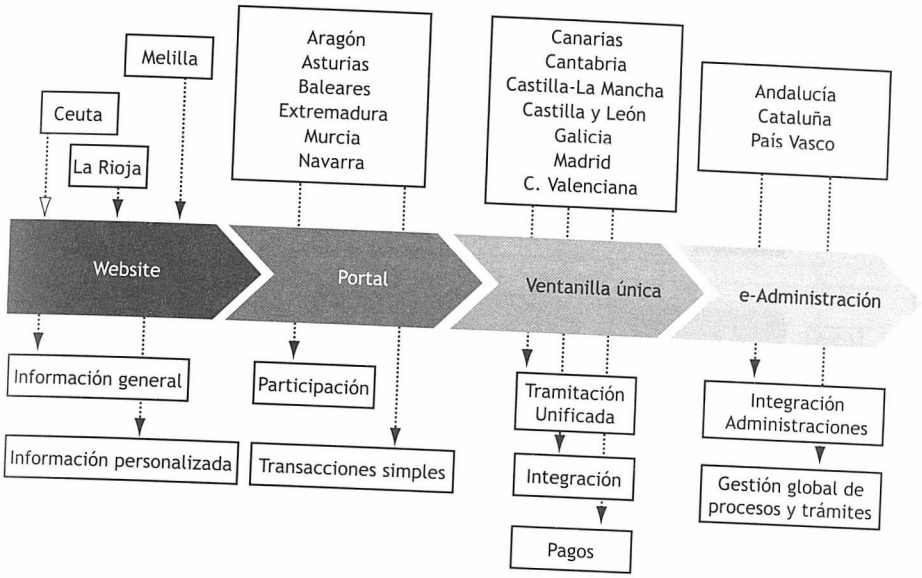
Para obtener una idea del volumen y tipo de documentos electrónicos de archivo que se producen, analizaremos los servicios de administración electrónica que ofrecen las administraciones actualmente a través de sus Portales de información.

Estos servicios están categorizados en cinco niveles en función del tipo de servicio y del grado de automatización y de tramitación telemática que ofrecen, tal y como se refleja en el cuadro siguiente:

Nivel 0	No existe información
Nivel 1	Facilita información acerca de la forma y requisitos para iniciar un trámite
Nivel 2	Además de la información da la posibilidad de descargarse formularios, que se deben imprimir, cumplimentar, firmar y presentar en una ventanilla
Nivel 3	Posibilidad de obtener la descarga de formularios electrónicos y reenviarlos cumplimentados, dando inicio al procedimiento. Exige autenticación por parte del ciudadano
Nivel 4	Posibilidad de realizar un trámite en su totalidad telemáticamente a través de la Web, con certificado electrónico de identificación

Si revisamos la oferta de servicios digitales que ofrecen las distintas administraciones, encontramos un variado panorama en el que todas ellas ofrecen en sus Portales servicios de administración electrónica en los cuatro niveles descritos, prácticamente ya no queda ninguna de nivel 0, que van desde servicios de información hasta servicios de teletramitación, para acceder a los cuales se exige al ciudadano disponer de certificado de firma electrónica en alguna de sus modalidades, o DNI electrónico, en función de la criticidad de los trámites a realizar.

GRÁFICO 16.6.
Evolución y fases de desarrollo de la eAdministración Autonómica. 2004



Fuente: eEspaña 2005

Informe de la Sociedad de la Información en España 2005. Fundación Auna[14].

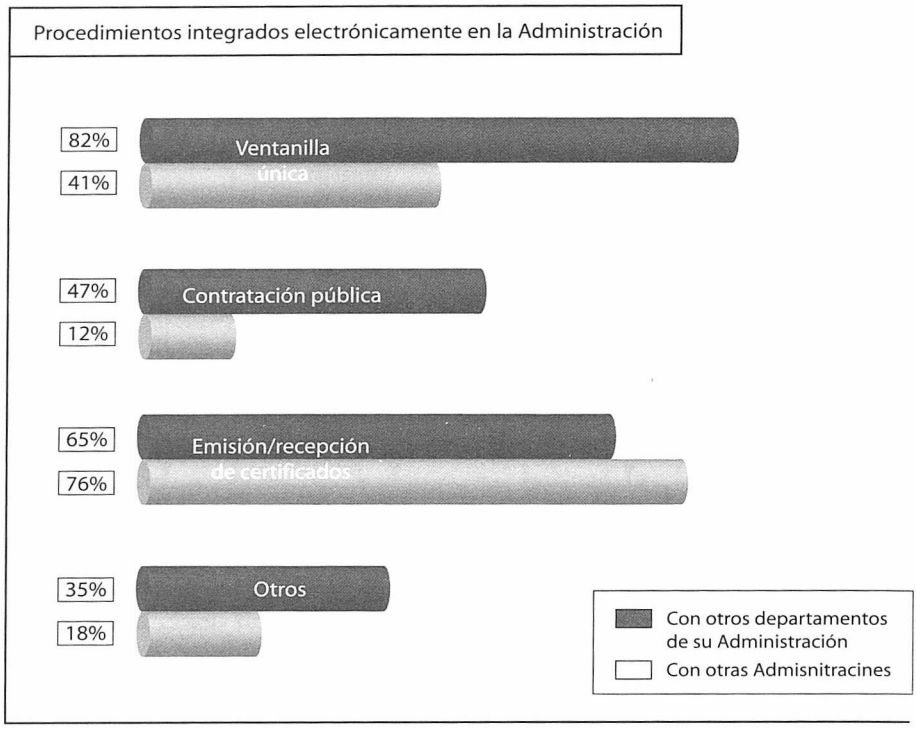
RESULTADOS DEL CUESTIONARIO DE ADMINISTRACIÓN ELECTRÓNICA[15]

Porcentaje de CCAA con procedimientos integrados electrónicamente en su Administración

	No tiene	Dentro de la Admón.	Con otras Admones.	Dentro y con otras Admones.	Total
Ventanilla única	17,65%	41,18%	0%	41,18%	100%
Contratación pública	47,06%	41,18%	5,88%	5,88%	100%
Emisión/rec. certificados	17,65%	5,88%	17,65%	58,82%	100%

[14] A pesar de que en el gráfico Asturias no aparece como una de las Comunidades Autónomas en la que está implantada la administración electrónica, nos consta que su nivel de desarrollo y de integración de servicios, permite incluirla en esta categoría.

[15] Cuestionario de Administración Electrónica 2006. Observatorio de la Administración Electrónica. Consejo de la Administración Electrónica www.map.es (visitado marzo 2007)



Base: contestan 17 Comunidades Autónomas

Como se puede apreciar en los gráficos anteriores, tomados del informe de evolución del año 2006 del Observatorio de la Administración Electrónica (OAE), elaborado por el Consejo de la Administración Electrónica, se presenta el porcentaje de los distintos tipos de servicios de administración electrónica ofrecidos por las Comunidades Autónomas, en función de los cuales se puede deducir que ya se está produciendo un importante número de documentos electrónicos de archivo.

Todas ofrecen la posibilidad de realizar trámites y gestiones por medios electrónicos. Las Comunidades que ofrecen un mayor avance de administración electrónica, con integración de los organismos de la administración y disponibilidad de un número importante de trámites y procedimientos son el País Vasco, (www.ej-gv.net), Cataluña, a través del portal www.gencat.net, donde se puede acceder a 80 trámites de la Generalitat y a otra serie de trámites de otras Administraciones, tanto catalanas como de la Administración General del Estado. Andalucía www.andaluciajunta.es, que con su lema «la administración cerca de ti» ha desarrollado el conjunto de plataformas básicas para la administración electrónica y Asturias www.asturias.es, que ofrece igualmente un importante número de trámites que pueden gestionarse totalmente de forma telemática a través de su plataforma SPIGA.

En el caso de la administración local, la situación reflejada en el Cuestionario de la administración electrónica 2006, es el que se representa en las tablas reproducidas a continuación:

TABLA 15.1.
Principales iniciativas de los Ayuntamientos en materia de SI

Ayuntamiento	Plan específico SI	Acciones		
		Sociedad	Empresa	eAdministración
Albacete		X	X	X
Alcalá de Henares		X	X	X
Alicante		X	X	X
Almería		X	X	X
Ávila		X	X	X
Badajoz		X	X	X
Badalona	No ha sido posible obtener información			
Barcelona	X	X	X	X
Bilbao	Plan estratégico	X	X	X
Burgos*		X	X	X
Cáceres	Plan estratégico	X	X	X
Cádiz	No ha sido posible obtener información			
Cartagena		X	X	
Castellón de la Plana		X		X
Ciudad Real		X		X
Córdoba		X	X	X
(A) Coruña*		X	X	X
Cuenca*	X	X	X	X
Dosnostia-San Sebastián*	MICT	X	X	X
Elche	Plan estratégico	X	X	X
Fuenlabrada		X	X	X
Getafe		X		
Gijón		X	X	X
Girona	X	X	X	X
Granada		X		X
Guadalajara		X	X	
Hospitalet de Llobregat		X		X
Huelva		X	X	X
Huesca	X		X	X
Jaén		X		
Jerez de la Frontera*	No ha sido posible obtener información			
Las Palmas de Gran Canaria	Plan estratégico	X	X	X
Leganés*			X	
León	MICT	X	X	X
Lleida	MICT	X	X	X
Logroño	X	X	X	X
Lugo		X		X
Madrid		X	X	X
Málaga		X	X	X
Móstoles	Plan estratégico	X	X	X
Murcia		X	X	X
Ourense		X	X	X
Oviedo		X		X
Palencia		X	X	X
Palma de Mallorca		X	X	X
Pamplona-Iruña		X		
Pontevedra		X	X	X
Sabadell		X	X	X
Salamanca*	X	X	X	X
Santa Cruz de Tenerife	X	X		
Santander		X		X
Segovia		X	X	X
Sevilla		X	X	X
Soria		X	X	X
Tarragona		X	X	X
Terrassa		X		X
Teruel*	X	X	X	X
Toledo*	MICT	X	X	X
Valencia	MICT			X
Valladolid	X	X	X	X
Vigo		X		X
Vitoria-Gasteiz		X	X	X
Zamora		X	X	X
Zaragoza		X		
Total	X	X	X	X
Variación Año 2003-2004	20	58	46	53
Variación Año 2002-2004	▲4	▲7	▲4	▲1
	▲7	▲8	▲16	▲14

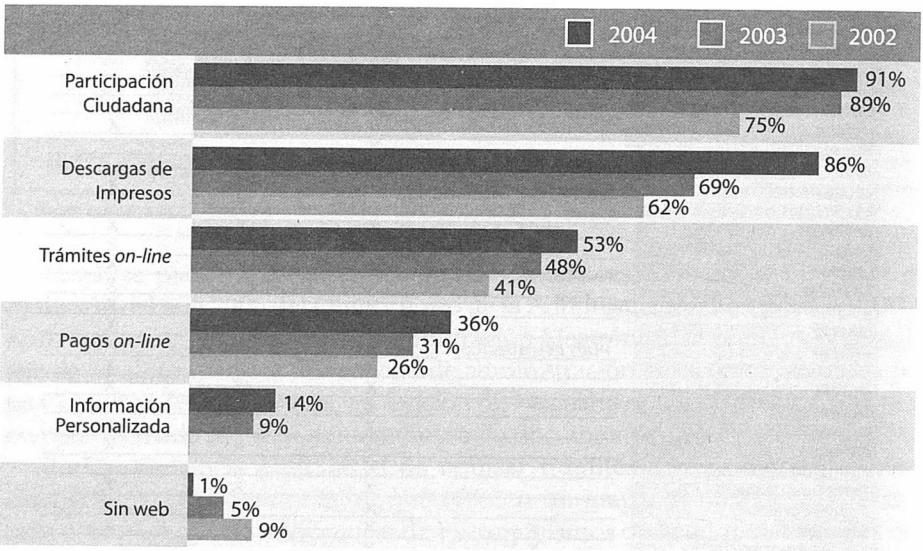
*Nota: Pendiente de aplicación

Fuente: eEspaña 2005

Llama la atención, que sólo un número reducido de los Ayuntamientos reflejados en la tabla anterior tienen un plan estratégico de Sociedad de la Información, lo que sin duda trata de subsanar el proyecto SIGEM, Sistema Integrado de Gestión Municipal, que están desarrollando conjuntamente el Ministerio de Industria, Turismo y Comercio, a través de Red.es, el Ministerio para las Administraciones Públicas, y la Federación de Municipios y Provincias, cuyo objetivo es el desarrollo de una plataforma integrada de gestión municipal[16].

En cuanto al porcentaje que representan los servicios ofrecidos por los ayuntamientos y el crecimiento que han experimentado desde el año 2002 al 2004, son los siguientes:

GRÁFICO 15.3.
Servicios Municipales on-line. En % de los Ayuntamientos



Fuente: eEspaña 2005

El ámbito de servicios que ha tenido un mayor crecimiento es el de servicios de administración electrónica, seguido de los servicios a empresas, y de las actuaciones para la sociedad, siendo todavía muy reducido el porcentaje de Ayuntamientos que ofrecen información personalizada al tiempo que se puede considerar residual el porcentaje de Ayuntamientos que no disponen de web.

[16] El proyecto de desarrollo de la plataforma SIGEM, se presentó a concurso público, resultando adjudicataria para su desarrollo Informática El Corte Inglés.

En la tabla siguiente podemos ver en detalle el tipo de servicios que ofrecen los Ayuntamientos.

TABLA 15.3.
Servicios Municipales on-line

Ayuntamiento	Información personalizada	Descarga de Impresos	Trámites *on-line*	Pagos *on-line*	Participación ciudadana
Albacete		X	X		X
Alcalá de Henares	X	X	X	X	X
Alicante		X	X	X	X
Almería		X			X
Ávila		X			
Badajoz		X	X		X
Badalona		X	X	X	X
Barcelona	X	X	X	X	X
Bilbao		X	X		X
Burgos		X	X		X
Cáceres		X			X
Cádiz					X
Cartagena		X	X		X
Castellón de la Plana		X			X
Ciudad Real		X			X
Córdoba	X	X	X	X	X
(A) Coruña	X	X	X	X	X
Cuenca		X			X
Dosnostia-San Sebastián		X	X	X	X
Elche		X			X
Fuenlabrada		No dispone de página web			
Getafe		X			X
Gijón		X	X	X	X
Girona		X	X	X	X
Granada	X	X	X	X	X
Guadalajara		En construcción			
Hospitalet de Llobregat		X	X	X	X
Huelva		X			X
Huesca		X			X
Jaén		En construcción			
Jerez de la Frontera	X				
Las Palmas de Gran Canaria		X	X	X	X
Leganés	X	X			X
León		X			X
Lleida		X	X		X
Logroño		X	X		X
Lugo		X			X
Madrid		X	X	X	X
Málaga		X	X	X	X
Móstoles		X			X
Murcia		X	X	X	X
Ourense					X
Oviedo		X			X
Palencia		X	X		X
Palma de Mallorca		X	X		X
Pamplona-Iruña		X	X	X	X
Pontevedra		X			X
Sabadell		X	X	X	X
Salamanca		X			X
Santa Cruz de Tenerife		X			X
Santander		X			X
Segovia		X	X	X	X
Sevilla		X			X
Soria		X	X		X
Tarragona		X			X
Terrassa		X	X	X	X
Teruel		X			X
Toledo		X	X	X	X
Valencia	X	X			X
Valladolid		X	X	X	X
Vigo	X	X	X	X	X
Vitoria-Gasteiz		X	X	X	X
Zamora		X			X
Zaragoza		X	X	X	X
Total	9	54	34	23	58
Variación 2003-2004	▲4	▲10	▲3	▲3	▲1
Variación Año 2002-2004	▲7	▲14	▲8	▲7	▲10

Nueva página web

Fuente: eEspaña 2005

Otro elemento a tener en cuenta para deducir el volumen de documentos electrónicos producidos, es el número de gestores que disponen de firma electrónica para validar las decisiones y resoluciones que emiten, que de acuerdo con el Informe IRIA 2006[17] en la AGE varía enormemente entre unos Ministerios y otros, destacando por el número de empleados que disponen de ella los Ministerios de Economía y Hacienda y de Industria, Turismo y Comercio, a los que sigue, con gran distancia, el Ministerio de Sanidad y Consumo. Aunque los 12.109 empleados que disponen de firma electrónica representan únicamente el 2% de los empleados públicos, al ser los altos cargos los que disponen de ella, el número de documentos electrónicos de archivo que se están produciendo, puede ser importante.

FIRMA ELECTRÓNICA

Tabla 3-44 1-1-2006

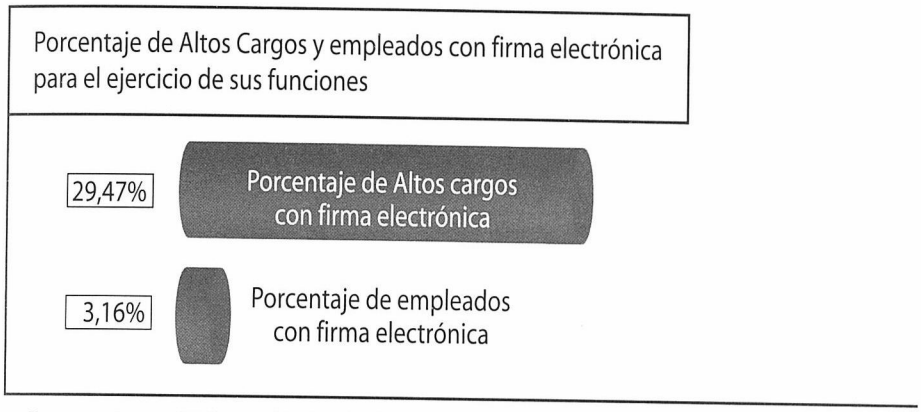
Ministerios	Nº Empleados con firma elect.	% sobre el total de Empleados Públicos
Industria, Turismo y Comercio	4.294	62%
Sanidad y Consumo	780	17%
Vivienda	70	14%
Economía y Hacienda	5.674	12%
Presidencia	170	5%
Agricultura, Pesca y Alimentación	55	2%
Administraciones Públicas	129	1%
Justicia	206	1%
Trabajo y Asuntos Sociales	317	1%
Fomento	112	0%
Interior	271	0%
Educación y Ciencia	9	0%
Asuntos Exteriores y Cooperación	2	0%
Defensa	20	0%
Medio Ambiente	-	-
Cultura	-	-
Total	12.109	2%

- Datos no disponibles

[17] Informe IRIA 2006, Las tecnologías de la información y la Comunicación en las administraciones Públicas. MAP, 2006, www.map.es, (visitado marzo 2007)

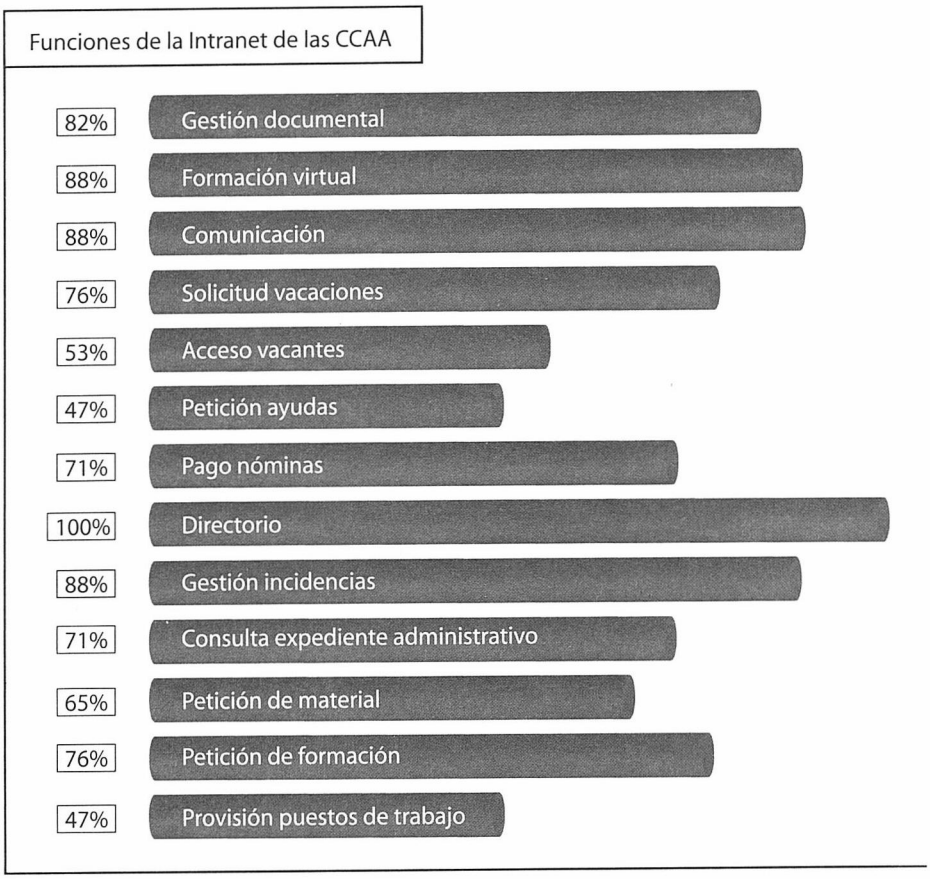
En cuanto a la situación en la Comunidades Autónomas, según el Cuestionario del OAE, de las Comunidades Autónomas que ofrecen servicios de teletramitación en mayor o menor grado, el 29,4% de los altos cargos disponen de firma electrónica, llegando algunas de ellas al 50% de altos cargos, como es el caso de Andalucía, Asturias, Cataluña y País Vasco.

En el caso de los empleados el número desciende al 3,16%, lo que no es muy significativo para el caso que nos ocupa, ya que la toma de decisiones y la firma de resoluciones corresponde a los altos cargos.



Base: contestan 12 Comunidades Autónomas a Altos Cargos y 15 a empleados

De la misma forma, el número de servicios a los empleados que pueden tramitarse telemática o informáticamente, a través de las respectivas intranets de las instituciones y organismos de las administraciones, es muy elevado, destacando con un 100% los servicios de información, seguidos con un 88% los servicios de formación virtual, comunicación y gestión de incidencias, y con un 82%, la Gestión documental. También se puede observar cómo la mayor parte de servicios de gestión interna, se resuelven de forma telemática.



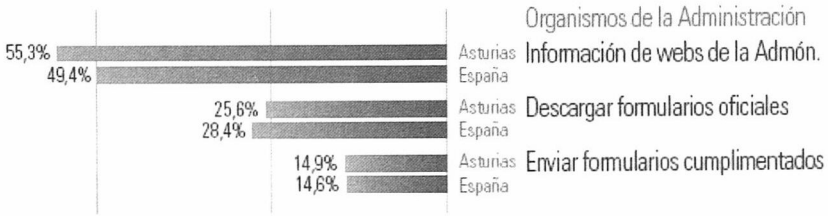
Base: contestan 17 Comunidades Autónomas

En cuanto a los servicios ofrecidos a los ciudadanos, de acuerdo con los informes y webs consultados, varía enormemente entre las distintas Administraciones.

A modo de ejemplo, veamos la situación que presentan dos Comunidades Autónomas, una de las más desarrolladas, Asturias, y otra de las menos desarrolladas, Galicia.

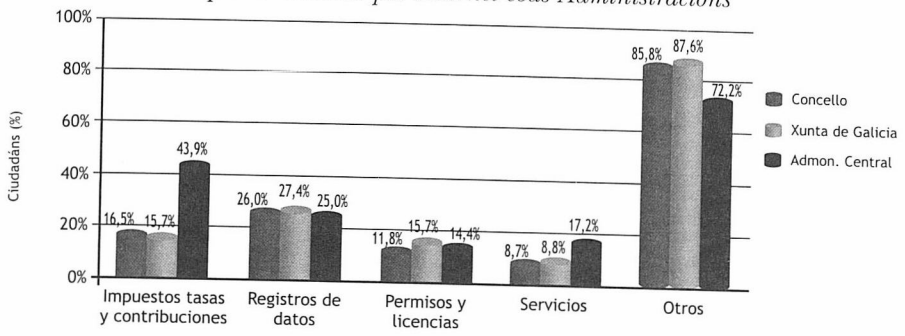
ASTURIAS —RESTO DE ESPAÑA— INFORME DE LA SOCIEDAD DE LA INFORMACIÓN 2006

Principio del formulario



En cuanto a Galicia, reproducimos el tipo de trámites y porcentajes que se gestionaron por los ciudadanos por este medio en las distintas administraciones de Galicia, en el año 2004.

FIGURA 7.19.
Tipos de trámites por Internet coas Administracións



Base: Ciudadáns que usaron Internet coa Administración
Fonte: © Observatorio TIC, Xuño 2005

Para dar una idea del tipo y número de trámites disponibles recogemos, a modo de ejemplo, el listado de los que están disponibles en el Principado de Asturias, a través de su Portal, www.asturias.es, reunidos por familias de procedimientos, y que son los habitualmente ofrecidos por las administraciones más avanzadas:

- Acreditaciones y homologaciones (50)
- Asesoramiento (4)
- Autorizaciones y permisos (359)
- Ayudas y subvenciones (399)
- Becas (18)
- Campañas (8)
- Carnés (19)
- Certificados (28)
- Concesiones de dominio público (9)
- Declaraciones de interés público (6)
- Derechos económicos (4)
- Expropiaciones (4)
- Indemnizaciones, devoluciones y compensaciones (20)
- Infracciones y sanciones (81)
- Información general (19)
- Inspección y control (27)
- Licencias (25)
- Matrículas y títulos académicos (28)
- Pensiones (2)
- Premios y distinciones (31)
- Registros (88)

- Selección de personal (2)
- Situaciones administrativas del personal (39)
- Suscripciones (1)

Además es posible realizar los siguiente tramites

- Interposición de recursos administrativos
- Aportar documentación a un expediente ya iniciado
- Verificar un certificado digital
- Consultar una notificación

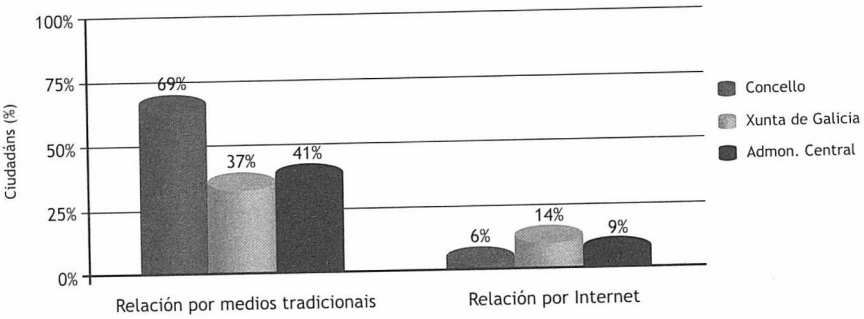
Ahora bien, a pesar de que las administraciones ofrecen todos estos servicios, el uso que hacen los ciudadanos de ellos es todavía relativamente bajo, como se obtiene del Informe elaborado por el Observatorio de la Sociedad de la Información de la Xunta de Galicia, para el año 2004, en el que se puede constatar el alto predominio de la comunicación presencial con las administraciones, frente a la comunicación telemática. Esta misma observación la hizo el Director General de Modernización del Principado de Asturias, durante la celebración de las Jornadas E-DOCPA, celebradas en Oviedo en noviembre pasado. A pesar del elevado número de procedimientos disponibles el porcentaje de utilización por los ciudadanos es mínimo.

Sin duda, a medida que los ciudadanos dispongan del DNI electrónico y se familiaricen y adquieran la confianza necesaria con la tecnología, el número de ciudadanos que interactúen con las administraciones por este medio crecerá de forma exponencial.

Igualmente, se puede observar que el nivel de transacción telemática es todavía muy reducido, tanto en la AGE, 12,18%, como en la Xunta y los Ayuntamientos de Galicia, en cuyo caso se reduce a un 5,5%[18].

FIGURA 7.18.

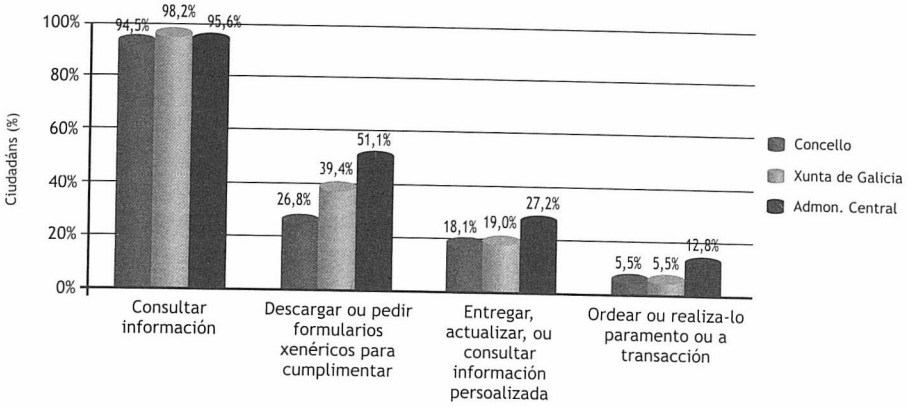
Ciudadáns que se relacionaron coas Administracións Públicas no último ano



Base: Todolos ciudadáns
Fonte: © Observatorio TIC, Xuño 2005

[18] Observatorio http://pdxcapp.xunta.es/consellarias/observatorio/node/464

FIGURA 7.20.
Nivel de interacción por Internet coas Administracións



Base: Ciudadáns que usaron Internet coa Administración
Fonte: © Observatorio TIC, Xuño 2005

Información obtenida del Observatorio de la Sociedad de la Información de Galicia[19].

Del análisis hecho hasta aquí, podemos concluir que el número de documentos electrónicos de archivo que se producen actualmente en España es todavía relativamente bajo, pero que puede producirse un crecimiento exponencial, a medida que se van incorporando más medios técnicos, especialmente la extensión y generalización del DNI electrónico como medio de firma electrónica autorizada.

LA GESTIÓN DE LOS DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

El grupo de Archiveros Nacionales reunidos en torno a la Comisión Europea, en el año 1995, conscientes del problema que se avecinaba, de cómo gestionar y conservar los documentos electrónicos que empezaban a producirse en las administraciones, convocó una reunión de la que se esperaba obtener directrices para su producción, gestión y conservación a largo plazo, dando lugar al DLM Forum, (Foro de los documentos legibles por máquina) cuya primera reunión tuvo lugar en Noviembre de 1996, y como resultado del cual se publicó la Guía de Información Electrónica[20].

Al mismo tiempo, a partir de la publicación de la Ley 30/1992, se desarrolla toda una serie de normativa dirigida a regular la utilización de los medios

[19] Observatorio para la sociedad de la Información de Galicia. http://pdxcapp.xunta.es/consellarias/observatorio/node/464 (visitado marzo 2007)

[20] http://europa.eu.int/historical_archives/dlm_forum/index_en.htlm

informáticos, electrónicos y telemáticos para la gestión de los servicios de las administraciones públicas[21], concretamente, el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, modificado por 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, encomienda al Consejo Superior de Informática y para el impulso de la Administración Electrónica la aprobación y difusión de criterios de conservación de la información producida por medios informáticos, electrónicos y telemáticos y criterios de seguridad y de normalización de las aplicaciones, que efectúen tratamientos de información cuyo resultado sea utilizado por los órganos y entidades del ámbito de la Administración General del Estado para el ejercicio de las potestades que tienen atribuidas.

Fruto de esta encomienda son los documentos *Aplicaciones Utilizadas para el ejercicio de las potestades. Criterios de Conservación*[22], *Criterios de seguridad*[23] y *Criterios de Normalización*[24].

El documento de *Criterios de Conservación* proclama perseguir los siguientes objetivos:

- *Proporcionar el conjunto de medidas organizativas y técnicas de seguridad que garanticen el cumplimiento de los requisitos legales para la conservación de la información en soporte electrónico relativa a los procedimientos administrativos de la Administración General del Estado que utilicen los medios electrónicos, informáticos y telemáticos en el ejercicio de sus potestades.*
- *Facilitar la adopción generalizada por parte de la Administración General del Estado de las medidas organizativas y técnicas que aseguren la conservación de la información manejada por las aplicaciones utilizadas para el ejercicio de potestades.*
- *Promover el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa y asegurar a la vez el respeto de las garantías y derechos de los ciudadanos en sus relaciones con la Administración.*

---

[21] Ver nota 4, en la que se reseña un conjunto de normas legales para la administración electrónica

[22] Aplicaciones Utilizadas para el ejercicio de las potestades. Criterios de Conservación, Ministerio de las administraciones Públicas, Madrid, 2003,www.map.es/csi/criterios_conservacion.htm

[23] Aplicaciones Utilizadas para el ejercicio de las potestades. Criterios de Seguridad, Ministerio de las administraciones Públicas, Madrid, 2004, www.map.es/csi/criterios_conservacion.htm

[24] Aplicaciones Utilizadas para el ejercicio de las potestades. Criterios de Normalización, Ministerio de las administraciones Públicas, Madrid, 2004 www.map.es/csi/criterios_conservacion.htm

Ante esta declaración de intenciones nos llama la atención el que cuando se expresa la necesidad de *garantizar el cumplimiento de los requisitos legales para la conservación de los documentos electrónicos* únicamente se hace referencia a la normativa legal derivada de la Ley 30/1992, y sólo se hace referencia a la Ley del Patrimonio Histórico Español, cuando se entiende que, ya finalizada la fase activa, deben ser transferidos a los archivos, manteniendo el concepto tradicional de fases de archivos, central, intermedio e histórico, dudosamente aplicable en el contexto electrónico, obviando que esta Ley debe ser tenida en cuenta, también, durante las fases de tramitación en lo que afecta al tratamiento de los documentos administrativos, independientemente de su fecha de producción, si se quiere garantizar su cumplimiento[25].

A pesar de que cuando se plantea la necesidad de *adoptar medidas organizativas y técnicas*, que no tecnológicas, se piense en la posibilidad de contar con los especialistas en el tratamiento y gestión de los documentos, los archiveros, parece que su aportación se ha centrado exclusivamente en la fase estrictamente de archivo de los documentos y con una visión anclada en el pasado, lo que en nuestra opinión es un error, ya que en el contexto en que nos movemos nos parece esencial la actuación de los especialistas desde el mismo momento de la creación de los documentos, esto es, cuando se diseñan y parametrizan las aplicaciones y se diseñan los documentos, y por tanto aún antes de que pasen a la fase de producción durante la tramitación administrativa, hasta cerrar su ciclo de vida.

Las medidas de conservación, organizativas y técnicas que recomienda, se basan en gran medida en las recomendaciones de la *Guía de la Información electrónica* ya citada, teniendo siempre en cuenta la normativa legal referida a la administración electrónica[26], y los riesgos y amenazas a los que se ven sometidos los documentos electrónicos, entre los que se reseñan:

- La obsolescencia de la tecnología con la aparición de nuevas versiones de plataformas, sistemas operativos y programas cada vez más potentes y eficientes y la inestabilidad de los soportes y formatos,

[25] Ley 16/1985, del Patrimonio Histórico Español, Artº 49.2, Forman parte del Patrimonio Documental los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado u otras entidades públicas y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos en lo relacionado con la gestión de dichos servicios.

Artº 55, 1. La exclusión o eliminación de bienes del Patrimonio Documental y Bibliográfico contemplados en el artículo 49.2 y de los demás de titularidad pública deberá ser autorizada por la Administración competente. 2. En ningún caso se podrán destruir tales documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos..... y El Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de los documentos administrativos en soporte distinto al original.

[26] Ver nota nº 4.

- Nuevas formas de documentos electrónicos, tales como los documentos compuestos, hipertexto o multimedia.
- Disponibilidad de una gran capacidad de procesamiento y de almacenamiento que no va acompañada de los procedimientos necesarios para el control adecuado de documentos.
- Desarrollo de sistemas de información orientados a la gestión de datos pero no tanto a la gestión de documentos.
- Acumulación incontrolada de documentos.
- Destrucción accidental o incontrolada de documentos.
- Manipulación no autorizada de los mismos (acceso, alteración, destrucción).
- Ausencia de documentación asociada y de metadatos, que dificulta su acceso.
- Factores físicos externos que pueden dar lugar a su deterioro, como es el caso de los campos magnéticos, la oxidación o la degradación de los materiales.
- Sobrecostes debidos a la mala dimensión del sistema de almacenamiento.

De entre estos riesgos y amenazas, nos parece especialmente interesante el que se refiere a la orientación de los sistemas de información a la gestión de datos, y no de documentos, problema que subsiste en la mayoría de los sistemas de gestión de documentos electrónicos de los que tenemos noticia, posiblemente porque han sido planificados por tecnólogos, poco sensibles a los aspectos de los valores administrativo, jurídico e histórico de los documentos.

Como medidas organizativas y técnicas se incorpora el concepto de análisis y gestión de riesgos, lo que permitirá conocer de manera rigurosa el estado de seguridad, determinar la valoración del riesgo y establecer las medidas preventivas. Los elementos que se recomienda analizar son:

- Qué documentos se tienen que conservar y proteger en función de su valor y de los plazos de conservación establecidos.
- Tipos de soportes y formatos y sus características y posibles problemas de durabilidad.
- Derechos y tipo de acceso.
- Amenazas que afectan a los documentos y consecuencias de su destrucción.
- Vulnerabilidad de las instalaciones físicas, y carencias de apoyo logístico (suministros, repuestos y consumibles).
- Características de la instalación ofimática, aplicaciones y equipos y sistema de tratamiento de la información.
- Existencia de documentos en soporte electrónico y en otros soportes (papel, microfilm, etc.).

- Características de la Organización: gestores y usuarios.
- Elementos asociados a la credibilidad, intimidad e imagen de las personas físicas o jurídicas.
- Posibilidad de incidentes que puedan dar lugar a daños materiales e inmateriales.
- Detección del riesgo de pérdida de autenticidad, integridad, confidencialidad y disponibilidad de la información.

En función de la necesidad de conservar los documentos producidos electrónica, informática o telemáticamente, y contenida en soportes del mismo tipo, que puedan afectar a los derechos e intereses de los ciudadanos, se recomienda adoptar las siguientes medidas:

- Estructurar los datos en forma de documentos y bases de datos, para almacenar la información, adoptando un criterio coherente de clasificación de los mismos.
- Agrupar los documentos (correspondencia, expedientes y registros), que describen una actividad, en un solo fichero o unidad coherente de información.
- En cada unidad de información clasificar los documentos por orden cronológico y temático o por palabras clave para facilitar la búsqueda y recuperación de la información.
- Conservar las bases de datos copiando los datos a un formato de bajo nivel (texto plano o en modo de acceso secuencial indexado) o si son bases de datos propietarias, considerar la posibilidad de exportarlas a una base de datos de software libre, de forma automática o semiautomática.

Como metadatos para la identificación y recuperación de los documentos se recomiendan los siguientes:

- Código, número de expediente.
- Título, denominación dada a los documentos electrónicos.
- Número de versión.
- Creador o Autor, persona/s responsable/s del contenido del documento.
- Destinatario, número de copias.
- Tema, palabras claves que describen el contenido, utilizadas en vocabularios o descriptores.
- Descripción, del contenido del documento.
- Editor, entidad responsable y que da acceso a la información.
- Colaboradores, persona/s u organismo/s además del creador que aportaron una contribución importante.

- Fecha, expresada en forma de número de ocho cifras: (D) día; (M) mes y (A) año, tipo: DDMMAAAA.
- Tipo, categoría de la información elegida de entre una lista de tipos: borrador; trabajo, informe técnico. Estos tipos y categorías no responden al concepto de documento administrativo de archivo.
- Formato, representación de los datos de la información: elegidos de entre los de una lista, que pueda aportar información sobre las aplicaciones, programas y equipos necesarios para poder visualizarlos o ejecutarlos.
- Identificador, número utilizado para identificar la información.
- Fuente, obra impresa o electrónica de donde procede la información, por ejemplo la versión papel del documento que sirvió para su transcripción a versión electrónica.
- Lenguaje, lengua del contenido de la información, puede coincidir con los códigos de caracteres para los lenguajes escritos.
- Información relacionada, por ejemplo, imágenes de un documento, partes o capítulos o de un libro.
- Alcance, características espaciales o temporales de la información.
- Derechos de autor.
- Condiciones de acceso.
- Niveles de seguridad y medidas aplicables.
- Palabras clave.

Con respecto a cómo gestionar la información establece las siguientes recomendaciones:

- Hacer planteamientos a corto, medio y largo plazo de acuerdo con las necesidades reales de conservación.
- Establecer la política de gestión de documentos de la Organización y la asignación de responsabilidades.
- Determinar la estructura de los ficheros con los datos de carácter personal y la descripción del sistema de información que los trata. Establecer el sistema de identificación de usuarios e interesados, en la creación y eliminación de la información, y de protección y acceso a la misma por personal autorizado, junto con las medidas de seguridad aplicadas a la información que contiene datos personales.
- Elección de formatos de fichero normalizados y perdurables para asegurar la independencia de los datos de sus soportes.
- Establecer los plazos de conservación, archivo y traspaso de la información.
- La traducción de la información a formatos normalizados e independientes del equipo físico.
- La política de realización de copias de respaldo y de recuperación de los datos.

- Las condiciones de la renovación de sistemas y sustitución de soportes.
- Mantener un registro o historial, sistema de auditoria, de las operaciones de tratamiento de la información en soporte electrónico.
- Hacer auditorias periódicas de seguimiento de la utilización de los procedimientos establecidos.

Con respecto a la gestión de los documentos, se hacen las siguientes recomendaciones, teniendo en cuenta la necesidad de mantener el principio de unidad del expediente, cuyo inicio y resolución se lleva a cabo en el organismo que tiene asignada la competencia de su tramitación, y siempre bajo la perspectiva de que se debe conservar y preservar la fiabilidad, autenticidad, integridad de la información electrónica durante toda la vida del documento:

- Mantener un archivo de oficina para la gestión de la información en soporte electrónico.
- Registrar, y transferir, la información de los expedientes en un soporte único, papel o electrónico, pero no en ambos a la vez (preferentemente electrónico).
- Transferir la responsabilidad de la gestión de la información a otro archivo (Archivo Central) al final de la parte activa de su ciclo de vida, en función de la frecuencia de utilización y los plazos de prescripción.

En relación con la transferencia y selección de documentos, a la que se da el nombre de «compactación de la información», establece los siguientes criterios:

- Cuando el servidor de la aplicación no pueda mantener los datos de gestión activamente, aplicar un proceso de compactación periódica, que deberá permitir eliminar del soporte de almacenamiento, los datos que no sean utilizados para el ejercicio de potestades.
- En el caso de que los datos compactados se transfieran, a otro soporte de almacenamiento, y se eliminen del soporte de gestión, existirá un proceso que permita reincorporar los datos compactados de forma que sean legibles por la aplicación de origen o por otra aplicación sustitutiva, y en todo caso deberán ser accesibles a los gestores en tanto mantengan su valor administrativo.
- En ningún caso podrán compactarse documentos activos.

En el proceso de transferencia de los documentos se deberán realizar los siguientes pasos:

- Eliminar la información que carece de valor administrativo de acuerdo con los criterios de valoración establecidos por el archivo.

- Hacer copias de los ficheros y de las bases de datos, verificar la consistencia de la información, documentar los errores de los ficheros y de los documentos.
- Abrir los documentos poseedores de una firma electrónica o cifrados, para acceso público antes de transferirlos al Archivo central.
- Comprobar que toda la información, y su contexto, está completa, documentada, y es conforme a los procedimientos y requisitos de conservación establecidos por el Archivo al que se transfiere.
- No preservar la operatividad de las firmas electrónicas, ya que la documentación y los procedimientos de transferencia al Archivo central garantizan la autenticidad de los datos.
- Asegurarse de que se almacena en un formato normalizado internacional libre de patentes y royalties.

En lo relativo al acceso y difusión de la información, se limita a prever la posibilidad de dar acceso presencial, o bien por medio de Internet, sin entrar en aspectos fundamentales como el de la identificación del interesado mediante certificado electrónico, en garantía del cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal, y a recomendar los protocolos, soportes y formatos para facilitar el acceso y difusión de la información:

— Soportes magnéticos para distribución de información:
  - Disquete de 3 1/2".
  - CD-ROM y DVD.

— Protocolos Internet para comunicación e intercambio de documentos:
  - HTTP para páginas hipertexto.
  - FTP para ficheros.

— Formatos de documentos:
  - XML para definir documentos independientes de la plataforma.
  - HTML para páginas Web y documentos breves.
  - PDF para visualización de documentos.

— Formatos de bases de datos:
  - SQL2 para consulta de bases de datos relacionales.
  - ISAM para almacenamiento de ficheros secuenciales indexados.

Con respecto a los formatos de ficheros y dispositivos de almacenamiento recomendados, no vamos a entrar a reseñarlos aquí, ya que quedan recogidos en otro Artículo de esta misma publicación dedicado a las Normas para la creación de Documentos electrónicos[27].

[27] Ver *op. cit.* nota 1.

Como medidas de conservación adicionales recomienda la copia de la información a nuevos soportes, debiendo seleccionarse aquellos que sean normalizados y no propietarios, siempre con garantía de preservar su autenticidad, originalidad, integridad y accesibilidad, y la conservación física de los soportes, de acuerdo con los criterios habituales de conservación establecidos para los archivos, de los que cabe destacar:

- La necesidad de determinar la frecuencia de tiempo con que se realizarán copias de respaldo y recuperación.
- Determinar la migración de soportes en función de su vida útil.
- Definir la manera de inventariar periódicamente los contenidos de la biblioteca de soportes y mantener y verificar el inventario de los soportes.
- Especificar los plazos de tiempo de conservación de los soportes, su puesta fuera de servicio y el borrado de ficheros.

En cuanto a la identificación y control de soportes, las recomendaciones son las habituales en el control de los fondos de los archivos, teniendo en cuenta la necesidad de:

- Identificar los soportes por su nombre, fecha de creación, durabilidad y período de retención.
- Identificar y controlar la duración de los equipos y soportes
- Impedir cualquier recuperación de la información almacenada en los soportes posterior a su baja en el inventario o a consecuencia de su salida fuera de los locales en que están ubicados.
- Control de los cambios, documentando y justificando la necesidad del cambio y evaluando sus consecuencias.
- Proteger los soportes de cambios no autorizados.
- Aprobar, implantar y verificar la realización de los cambios.
- Seguir la evolución y los cambios que puedan afectar a la aplicación y la plataforma.

En lo relativo a la seguridad de la información se hacen una serie de recomendaciones de las que destacaremos las siguientes:

Gestión de soportes removibles:

- Documentar todos los procedimientos y niveles de autorización: quién tiene acceso y a qué soportes.
- Retirar los soportes con autorización escrita y mantener su registro y trazabilidad: registro de salida.
- Evitar identificar los datos almacenados a partir de la etiqueta del soporte.
- Reutilizar y retirar los soportes eliminando sus contenidos con diferentes patrones de borrado.

- Realizar *in situ* reparaciones de medios, equipos y sistemas, para evitar el riesgo de fuga de datos.

Manipulación de datos de carácter personal:

- Documentar la manipulación y esquema de etiquetado de todos los soportes.
- Mantener un registro actualizado con la lista de personas autorizadas.
- Controlar los datos, acusar recibo y marcar las copias remitidas a los receptores autorizados.
- Registrar las operaciones de creación, modificación y borrado, para su trazabilidad.
- Realizar auditorías periódicas para determinar el grado de cumplimiento de los procedimientos.
- Cifrar la información de carácter sensible, requisito de confidencialidad.
- Firmar y fechar digitalmente la información sensible, requisito de autenticidad.
- Ubicar de forma segura los soportes; disponer de una caja de seguridad para el almacenamiento de los soportes.

Documentación del sistema de conservación:

- Establecer controles para proteger al sistema de accesos no autorizados.
- Ubicar físicamente la documentación en armarios robustos.
- Almacenar la documentación separada de los ficheros de aplicaciones y programas.
- Proteger la documentación asignándole el adecuado nivel de acceso.
- Eliminación de soportes:
- Eliminar los soportes que contengan información de carácter sensible, o borrar los datos para su reutilización. Destruir mediante trituradoras o medios similares los impresos y el papel.
- Identificar los soportes que deban destruirse de forma segura, tales como fax, telex, papel carbón, cintas, discos removibles, casetes, listados de programas, datos de prueba y documentos del sistema.
- Encomendar la destrucción de soportes a organizaciones especializadas, seleccionándolas por su experiencia y condiciones de control de seguridad.
- Llevar un registro de la destrucción de soportes con información sensible, a efectos de auditoría.
- Evitar la acumulación de gran cantidad de información sensible para su destrucción.
- Realizar el seguimiento del estado de la tecnología.

Por último dedica un capítulo al Sistema de Archivo de los documentos electrónicos, en el que se reproducen las recomendaciones vigentes para los archivos de documentos físicos, como ya hemos dicho anteriormente, con un concepto de archivo excesivamente tradicional, y sin entrar en algunos de los problemas fundamentales, como son, si los documentos electrónicos se van a custodiar en los Archivos, o en los órganos productores, qué política se debe seguir con las firmas electrónicas, o cómo definir la política de transferencias y conservación a largo plazo, y de acceso a los documentos desde el Archivo.

Uno de los aspectos fundamentales del tratamiento y gestión de los documentos electrónicos es el de la seguridad, al que el Consejo Superior de Informática y para el impulso de la Administración electrónica, dedicó un documento independiente, orientado a la seguridad de los datos de carácter personal y dar cumplimiento a la Ley 15/99 y al Real Decreto 994/1999[28], y en el que se establecen los criterios que se deben seguir en el diseño, desarrollo, implantación y explotación de las aplicaciones utilizadas por la Administración General del Estado para el ejercicio de la de las potestades que tienen atribuidas, así como los aspectos relativos a la protección de los datos de carácter personal.

Los objetivos fundamentales del documento son:

- Proporcionar el conjunto de medidas organizativas y técnicas de seguridad que garanticen el cumplimiento de los requisitos legales para la validez y eficacia de los procedimientos administrativos de la Administración General del Estado, que utilicen los medios electrónicos, informáticos y telemáticos en el ejercicio de sus potestades
- Facilitar la adopción generalizada por parte de la Administración General del Estado de medidas organizativas y técnicas que aseguren la protección proporcionada a los riesgos de los sistemas y aplicaciones que la manejan.

La finalidad última de la seguridad es proteger la autenticidad, confidencialidad, integridad y disponibilidad de la información, desde una perspectiva del conjunto de requisitos legales, técnicos y tecnológicos que garanticen el acceso a través de redes, la seguridad en el acceso mediante firma electrónica, la disponibilidad mediante la protección de soportes de información y copias de respaldo, y el desarrollo y explotación de sistemas y gestión y registro de incidencias, por lo que debe plantearse dentro de la política global de seguridad de la información de la Organización.

La política de seguridad deberá atender a los siguientes aspectos:

En relación con las aplicaciones para el ejercicio de potestades:

— Adoptar medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información garantizando la restricción de utilización, la prevención de alteraciones y la protección a procesos informáticos. (RD 263/1996, arts. 4.2 y 4.3)

[28] Ley Orgánica 15/1999 de Protección de datos de carácter personal, y Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

En relación con la protección de los datos de carácter personal:

— Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. (LO 15/1999, art. 9.1), para lo que se establecerán los procedimientos a seguir con los ficheros que contengan datos de este tipo, con los siguientes puntos:

- Objeto del documento.
- Ámbito de aplicación de la política de seguridad.
- Recursos protegidos.
- Funciones y obligaciones del personal.
- Normas, procedimientos, reglas, estándares y medidas para garantizar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.
- Identificación, autenticación y control de accesos.
- Gestión de incidencias de seguridad.
- Gestión de soportes y copias de respaldo.
- Acceso a través de redes.
- Contingencias y continuidad del servicio.
- Controles periódicos de verificación del cumplimiento.

Contará además con los siguientes Anexos:

- Documentos de notificación y normas de creación de ficheros o de la aplicación para el ejercicio de potestades.
- Descripción de la aplicación y del sistema informático.
- Descripción de la estructura de ficheros o bases de datos.
- Entorno del sistema operativo y de comunicaciones.
- Descripción de locales y equipamientos.
- Análisis y gestión de riesgos.
- Descripción de las funciones y obligaciones del personal.
- Personal autorizado para acceder al fichero/aplicación.
- Procedimientos de control de accesos y perfiles de usuarios.
- Gestión de soportes de información.
- Gestión de copias de respaldo y recuperación.
- Procedimientos de notificación y gestión de incidencias.
- Plan de contingencias.
- Auditorias y controles periódicos.

A la información que se debe proteger, se le asigna el nivel de protección en función de los valores de sensibilidad que establece la Ley 12/99, que se reflejan en la siguiente tabla:

Tipo de datos	Nivel	Autenticación	Confidencialidad	Integridad
Según función / Datos de carácter NO personal	N/A	Baja	Libre	Baja
Según función / Datos de carácter personal: • Todos los ficheros que contengan datos de carácter personal.	Básico	Normal	Restringida	Normal
Según función / Datos de carácter personal; o Infracciones administrativas o penales. o Hacienda Pública. o Servicios financieros. o Ficheros que se rijan por el artículo 29 de la Ley Orgánica 15/1999.	Medio	Alta	Protegida	Alta
o Datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.				
Según función / Datos de carácter personal; o Datos de ideología, religión, creencias, origen racial, salud o vida sexual. o Datos recabados para fines policiales sin consentimiento de las personas afectadas.	Alto	Crítica	Confidencial	Crítica

En cuanto al los mecanismos de protección se describen en detalle las funciones y responsabilidades que deben asumir los distintos actores implicados en la política de seguridad de la Organización y las medidas preventivas a aplicar frente a éstos, las medidas de protección física, la autenticación de los usuarios de la aplicación, en función de la criticidad de los datos, desde la simple autenticación hasta sistemas de identificación criptográfica, y la política de asignación y mantenimiento de claves de acceso.

Para la conservación de la integridad se recomiendan:

- las copias de seguridad,
- la asignación de resumen o hash, firma electrónica, fechado electrónico,
- medidas de seguridad en las aplicaciones que garanticen la posibilidad de completar las transacciones,
- seguimiento de las actuaciones mediante sistemas de auditoria y trazabilidad,
- comprobación de la integridad del software, especialmente en los ordenadores cliente, dada su vulnerabilidad

Para la conservación de la disponibilidad, se definen los criterios en función de la criticidad de los datos, y en cualquier caso, se deben adoptar medidas de seguridad instalando:

- sistemas redundantes de hardware, de suministro de electricidad,
- instalación de firewals contra posibles ataques,
- y se debe diseñar un plan de contingencias para el caso de que ocurriera un desastre.

En relación con el acceso se regirá por la política de gestión de usuarios y asignación de privilegios de acceso y de actuación sobre los datos, revisándolos periódicamente para su actualización, y medidas especiales para los casos de acceso por personas ajenas a la Organización, y especialmente en el caso de acceso a través de redes, en que se deben instalar cortafuegos que impidan accesos indeseados y ataques al sistema de información. Especial protección se debe dar a los datos de carácter personal, y analiza las distintas formas y sistemas de firma electrónica aplicables, igualmente en función del nivel de seguridad que requieran los datos gestionados, así mismo se recomienda que las aplicaciones dispongan de un sistema de auditoría que permita hacer el seguimiento de todas las actuaciones sobre la aplicación.

El tercer documento, dedicado a los Criterios de Normalización tiene por objetivo facilitar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa en condiciones de racionalidad y economía, mediante la adopción de normas para asegurar la interoperabilidad de los sistemas informáticos y telemáticos, para lo que define

los protocolos de intercambio recomendables para la operación de la Intranet Administrativa, que es la infraestructura básica de comunicaciones y de servicios telemáticos comunes, para el intercambio electrónico seguro de información entre departamentos de la Administración General del Estado, y entre ésta y las Administraciones de Comunidades Autónomas, Corporaciones locales y Unión Europea, y que es la base para el desarrollo de la Administración electrónica debido a la racionalización de las comunicaciones que conlleva.

Así mismo se definen los criterios de normalización a seguir para garantizar el acceso a la web a personas con los distintos tipos de discapacidad que se presentan en la sociedad[29].

La Gestión y conservación de documentos en el Proyecto de Ley de Acceso de los ciudadanos a las administraciones Públicas

Volvamos al Proyecto de Ley de acceso de los ciudadanos a las Administraciones Públicas, para ver que atención dedica a la gestión y conservación de los documentos que van a ser soporte legal y evidencia de sus actuaciones y de las de los de los ciudadanos en sus relaciones con éstas.

Y de nuevo nos llama la atención el hecho de que el legislador, a juzgar por la poca atención que dedica a este aspecto, parece más preocupado, en aras de la modernidad, por la eliminación del papel, que por la forma de gestionar y conservar, durante el tiempo que sea necesario por su valor testimonial, los documentos resultantes de las transacciones administrativas.

Y llama aún más la atención en un momento en el que otras administraciones, como la americana, sensibilizadas por la eliminación de documentos que se han visto necesarios para dilucidar escándalos de índole política y económica, ha emitido regulaciones y normas para la gestión y conservación de los documentos electrónicos, estableciendo penalizaciones importantes, tanto a la administración federal como al sector privado por su eliminación inadecuada.

Así el Proyecto de Ley, establece la posibilidad de hacer copias electrónicas de documentos analógicos, a las que se les reconoce como copias auténticas y con valor probatorio, y la eliminación de los documentos físicos originales, siempre que e cumplan los requisitos establecidos[30]. A medida que se impon-

[29] Para ver en detalle estos criterios ver el documento «Criterios de Normalización», citado.

[30] Artículo 29. Copias electrónicas.

1. 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 inicial 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 el documento original.

ga esta norma y se generalice la conversión de documentos físicos a documentos analógicos, crecerá enormemente el número de imágenes digitales con valor probatorio. A ésta se añade la normativa sobre la compulsa electrónica de las imágenes digitales[31], que si bien de momento se limita a ser una norma del Ministerio de Industria, Turismo y Comercio, no tardará mucho tiempo en extenderse a otros ámbitos.

Como consecuencia de estas normas, habrá que aplicar las mismas normas de gestión y conservación a las imágenes de los documentos, que a los documentos originales.

En cuanto al Archivo de los documentos establece la posibilidad de almacenarlos electrónicamente, bien en el formato original o en cualquier otro, siempre que asegure la identidad e integridad de la información necesaria para reproducirlo, así como la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos[32]. En este aspecto se rompe con el concepto tradicional de documento, en el que los datos y el soporte debían de permanecer unidos para garantizar la originalidad y autenticidad, concepto difícil de mantener en el contexto electrónico.

En la definición de expediente electrónico incorpora, junto al sistema de foliado de los documentos mediante un registro electrónico, un concepto

---

2. Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por los interesados o consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

4. En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, podrá procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.

5. Las copias realizadas en soporte papel de originales emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar Administración Pública, órgano o entidad emisora.

[31] Orden ITC/1475/2006, de 11 de mayo, sobre utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria,Turismo y Comercio.

[32] Artículo 30. Archivo electrónico de documentos.

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares podrán 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.

nuevo, como es el que un mismo documento pueda formar parte de dos expedientes distintos, sin necesidad de hacer una copia[33]. Y poco más dice con respecto a este tema, lo que nos parece insuficiente para garantizar la gestión correcta del ciclo de vida de los documentos en su totalidad.

Balance del Estado de la Cuestión

Hasta aquí hemos tratado de analizar como debe regirse la producción, gestión y archivo de los documentos electrónicos a la luz de la normativa en nuestro país, así como de evaluar el volumen de documentos electrónicos de archivo que se producen actualmente, y nos preguntamos ¿se está cumpliendo la Normativa, que como hemos podido ver es amplia y detallada?, ¿tenemos la garantía de que los documentos que se están produciendo se conserven, al menos, en tanto se mantiene sus valores administrativos y probatorios, por no decir ya su valor informativo?

Lamentablemente, creemos que el panorama no es para inducir al optimismo. Si bien, como hemos visto, tanto la Administración General del Estado como las Comunidades Autónomas, y los Ayuntamientos ofrecen en un número importante la posibilidad de realizar los trámites administrativos telemáticamente, son pocas las organizaciones que han definido y diseñado una plataforma informática que permita gestionar correctamente el ciclo de vida de los documentos en su totalidad, incluyendo la fase de archivo y que han adoptado las medidas organizativas necesarias para lograrlo.

De los datos que hemos podido obtener, en el momento actual sólo dos Comunidades Autónomas, Andalucía y Asturias cuentan con una plataforma que cubra el ciclo en su totalidad de forma integrada.

La plataforma de Andalucía está compuesta por una serie de plataformas básicas:

- @ries: Aplicación de Registro E/S. Normativa SICRES y adaptación de módulos para integración con aplicaciones de ventanilla única virtual
- @firma:Plataforma de certificación electrónica
- Not@rio: Sellos de tiempo y acuses de recibo
- Notific@: Notificación telemática: envío y seguimiento de recepción por el interesado

[33] Artículo 31. Expediente electrónico.

1. El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

2. El foliado de los expedientes electrónicos podrá llevarse a cabo mediante un índice electrónico, firmado por la Administración u órgano actuante, según proceda. Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

- Sond@: Chequeo de servicios y de operatividad de las aplicaciones
- Incidenci@s: Sistema de gestión de incidencias técnicas de las distintas plataformas y servicios
- @PLOPD: Soporte al cumplimiento de la LOPD,
- @rchiva: Plataforma para el sistema de archivo corporativo de la Administración
- W@rda: Sistema de archivo de documentos electrónicos

La plataforma del Principado de Asturias SPIGA, está compuesta por las plataformas de:

- Registro de Entrada y salida de documentos en sus tres modalidades, presencial, web y telemático,
- Tramitación administrativa, electrónica y telemática,
- Archivo unificado para la gestión de documentos físicos y electrónicos
- Sistema de atención a ciudadanos a través de un sistema de CRM.

En cuanto a las otras Comunidades Autónomas calificadas de avanzadas en la implantación de la administración electrónica en el Informe Auna[34], el País Vasco está en la fase de definir su modelo de gestión documental, incluida lógicamente la gestión del Archivo de documentos electrónicos, basado en la plataforma Documentum, y Cataluña está en la fase de seleccionar una nueva plataforma para la gestión de la administración electrónica y de definir el modelo de gestión de los documentos electrónicos.

Entre las restantes Comunidades Autónomas se dan distintos casos: Comunidades Autónomas que han seleccionado una plataforma para su gestión, sin tener en cuenta por el momento la fase de archivo, como es el caso de Castilla-La Mancha y Castilla y León, y que están empezando a plantearse la necesidad de definir cómo gestionar sus documentos electrónicos de archivo; de Navarra, que está iniciando la implantación de una plataforma de tramitación electrónica de un lado y de otra la implantación de una aplicación de gestión unificada de Archivo, con la intención de integrarlas; Canarias, que ha adoptado la plataforma de tramitación electrónica, que se está implantando poco a poco, y la aplicación de gestión unificada de archivo, que se encuentra en fase de implantación, y, al igual que en el caso de Navarra, con la perspectiva de integración de ambas plataformas.

Otras Comunidades, están empezando a desarrollar su plataforma basada en software libre, como es el caso de Extremadura, pasando por las que van acometiendo proyectos de administración electrónica con el único objetivo de poner servicios a disposición de los ciudadanos, pero sin una idea integral e integradora de las distintas fases y módulos que la componen.

[34] Ver *op. cit.*

Y en cuanto a la Administración General del Estado, puede decirse que no hay uniformidad, cada Ministerio ha optado por un modelo de plataforma distinto, y en ningún caso se integra con la fase de Archivo.

En lo relativo a la Administración Local, ya hemos comentado el Proyecto SIGEM, Sistema Integrado para la Gestión Municipal, en el que se ha definido un modelo integrado del ciclo documental en su totalidad.

El panorama es, como puede verse, diverso y en la mayoría de los casos no se tiene en cuenta la fase final, la del archivo de los documentos electrónicos, que si es importante en el caso de los documentos físicos, lo es aún más en el de los documentos electrónicos. Quizá el olvido se deba a que, por lo general, los modelos de plataforma se diseñan por tecnólogos sin el concurso de los especialistas de gestión de los archivos.

Esperemos que todavía estemos a tiempo de corregir la situación.

Intencionadamente no hemos hecho mención de cual es la situación y cómo se están gestionando la enorme cantidad de imágenes digitalizadas de documentos electrónicos, que deben gestionarse con los mismos criterios de conservación que los documentos electrónicos, y que sin embargo, en muchos casos no se gestionan de acuerdo con ellos, tema que merecería un inventario de recursos digitalizados y el análisis de la gestión y garantía de su conservación a largo plazo.

ANEXO I

Aspectos prácticos de la firma electrónica

1. Algunas nociones

¿Qué es la firma electrónica?

Según el Art. 3 de la Ley 59/2003, de 19 de diciembre, de **Firma Electrónica**, es *el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*

Se denomina **firma electrónica avanzada** a la *que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.*

Y por fin, se considera **firma electrónica reconocida** a *la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.*

¿Qué requisitos debe cumplir la firma electrónica reconocida?

- Que identifique al firmante del documento: garantizar la **identidad del autor**.
- Que el documento se conserve íntegramente sin ser modificado con posterioridad: **integridad**.
- Que el firmante de un documento no pueda negar posteriormente haberlo firmado: **no repudio**.

¿Cómo se consiguen estos objetivos?

A través de:

- Sistemas tecnológicos avanzados que combinan técnicas criptográficas (especialmente mediante clave asimétrica o clave pública) y funciones matemáticas como el resumen *hash.*
- Certificados digitales emitidos por *Terceras partes de confianza* (Prestadores de servicios de certificación)

2. Las bases tecnológicas de la firma electrónica

La criptografía

La criptografía (del griego κρυπτός, oculto, y γράφειν, escribir) es la disciplina que incluye los principios, medios y métodos para transformar los datos con intención de ocultar la información y prevenir la modificación y los usos no autorizados de la misma.

Las técnicas criptográficas se han usado a lo largo de la historia, especialmente con fines militares (ya los egipcios la empleaban, hay un método criptográfico conocido como César porque Julio César lo empleaba en sus comunicaciones). Pero las tecnologías informáticas han desarrollado enormemente los criptosistemas para conseguir la confidencialidad y secreto de las comunicaciones.

Lo que importa aquí especialmente es la distinción entre dos tipos de claves que utilizan los sistemas criptográficos:

— **Criptosistemas de clave simétrica o secreta**: una misma clave secreta es compartida por el emisor del mensaje cifrado y por el receptor del mismo. Es un sistema sencillo, pero exige un intercambio previo de la clave. La seguridad del sistema reside en la dificultad que plantee el algoritmo de codificación, pero además en la necesidad ineludible de mantenerla en secreto.
Los algoritmos más extendidos para el cifrado con clave secreta son Data Encription Standard (DES), Triple DES, Rivest Cipher 4 y 5 (RC4 y RC5).

— **Criptosistemas de clave asimétrica o pública**. Se trata de sistemas muy avanzados, que aparecen a partir de los años 70 con las nuevas tecnologías y que utilizan algoritmos de codificación muy complejos, que los hacen prácticamente irrompibles.
En este caso cada miembro de la red dispone de dos claves distintas, la pública (puede ser conocida y utilizada por todos) y la privada (sólo la conoce su propietario). Una de las dos claves se emplea para cifrar y la otra para descifrar, pero el algoritmo de cifrado es tan complejo que es prácticamente imposible, aunque se conozca una clave, averiguar la otra.

Lo que se cifra con la clave privada sólo puede descifrarse con la clave pública y lo que se cifra con la clave pública sólo puede descifrarse con la clave privada. Así por ejemplo:

- Si se desea enviar a alguien un mensaje que nadie pueda descifrar, se utiliza la clave pública del destinatario. Nadie podrá descifrarlo, excepto el destinatario que utilizará para ello su clave privada.
- Por el contrario si alguien desea dar a conocer un mensaje que todos puedan interpretar y que además sepan que ha sido enviado necesariamente por él, utilizará su clave privada. Todos los que dispongan de la clave pública del emisor podrán descifrar el mensaje e identificarán con certeza al remitente.

Los algoritmos más usados para el cifrado con clave pública o asimétrica son Rivest-Shamir-Adleman (RSA) y Diffie-Hellman (DH).

En resumen, la criptografía ofrece herramientas para mantener **el secreto y la confidencialidad de las comunicaciones**. Pero no garantiza la identidad del emisor (autenticidad), la integridad del mensaje ni la recepción por el destinatario.

Para conseguir esto y para conseguir la firma digital, se ha de mezclar la criptografía de clave asimétrica con el resumen *hash*.

Función de resumen (HASH)

La función *hash* permite realizar una operación matemática sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales:

- El resultado de la función *hash* es una especie de resumen del documento.
- Este resumen es de tamaño fijo e independiente del original.
- Está ligado unívocamente el original: el mismo mensaje dará siempre el mismo resumen, por lo que se acepta como su «huella electrónica».
- A partir de un texto base, es fácil y rápido calcular su resumen.
- Es de una sola vía: es imposible reconstruir el texto base a partir de su resumen.
- Es imposible que dos textos base diferentes tengan el mismo resumen (algunos expertos dicen que no es tan imposible).

Para realizar la función *hash* se utilizan diversos algoritmos. Los más extendidos son SHA, SHA-1 y MD5.

¿Cuáles son los pasos básicos en la firma digital de un documento?

1. El autor de un documento en formato electrónico aplica la función *hash* a su documento, con lo que obtiene su «resumen» o «huella digital».
2. Cifra con su clave privada (cifrado asimétrico) el resumen *hash.*
3. Envía al destinatario el documento y su resumen *hash.*
4. Para comprobar la validez de la firma el receptor descifra el resumen *hash,* aplicando la clave pública del firmante.
5. A continuación aplica la función *hash* al texto original y obtiene también su «resumen» o «huella digital»
6. Se comparan ambos resúmenes.

Si los dos resúmenes son iguales es que el documento ha sido enviado por quien afirma haberlo enviado y además no ha sido modificado (en caso contrario los resúmenes no coincidirían):

- El sistema nos garantiza **la identidad del firmante y la integridad de documento.**
- También garantiza el «**no repudio**». Su autoría no puede ser negada por el remitente, ya que el resumen lo cifró con su clave privada, que nadie, excepto él mismo, conoce.

Por tanto, una firma digital es un **conjunto de datos asociados a un mensaje, que permite asegurar la identidad del firmante y la integridad del mensaje**.

Tener en cuenta que «firmar digitalmente» no es lo mismo que cifrar o encriptar. La firma digital sólo exige necesariamente cifrar el resumen *hash* que sirve como firma. El documento puede estar «en claro», o puede también cifrarse.

3. Autoridades de certificación y certificados digitales

¿Cómo se consigue que una firma digital se convierta en una *firma electrónica reconocida* de acuerdo con la Ley?

Que se genere en un «dispositivo seguro de creación de firma», cumpliendo algunos requisitos:

- Garantía de que la clave privada sólo la conoce su propietario (es posible almacenarla en un fichero accesible con PIN, pero la mayor seguridad es la que proporcionan las tarjetas inteligentes, que no pueden ser duplicadas).
- Garantía de que la clave pública la pueden conocer los demás usuarios.
- Garantía de que no puede existir confusión o duplicidad entre unas claves públicas y otras.

Esto se realiza a través de los **Certificados Digitales**, que son certificados electrónicos que garantizan que una clave pública pertenece a un usuario concreto. Son expedidos por las **Autoridades de Certificación** o **Prestadores de Servicios de Certificación**, que actúan como **Terceras Partes de Confianza.**

El certificado vincula una clave pública al nombre del titular de la clave y al uso previsto de la clave durante un período de tiempo. Lo emite una Autoridad de Certificación reconocida, utilizando para ello su propia clave privada como entidad, y garantiza que una clave pública concreta pertenece realmente al titular que figura como propietario.

El Certificado debe incluir:

- Información sobre la identidad del usuario.
- Su clave pública.
- Un número de serie único.
- El periodo de validez.
- La identidad del emisor del certificado.
- La firma digital, con la clave privada, de la autoridad de certificación emisora.

El protocolo utilizado actualmente para la generación de certificados digitales es el X509v3, que es una recomendación de la ITU (International Telecomunication Union)

El algoritmo usado habitualmente para la firma, para la realización del proceso de *hash*, es el SHA-1 (Secure Hash Standard-1)y el de cifrado de clave pública es el RSA (Rivest-Shamir-Adleman)

Es interesante tener en cuenta algunos aspectos adicionales:

- La Ley 59/2003, de 19 de diciembre de firma electrónica, en su artículo 7 regula la **firma electrónica de las personas jurídicas**, a través de sus administradores y representantes, y siempre dentro del respeto a la legislación civil y mercantil vigente.
- El artículo 8 de la citada Ley regula la **extinción de la vigencia de los certificados electrónicos**, por expiración del plazo de validez para el que fue expedido o por otras diversas causas como la revocación por parte del firmante, por violación del secreto de los datos de creación de firma, por cese de las actividades de la Autoridad de certificación, etc.
- Los certificados digitales pueden renovarse antes de la fecha de su caducidad (los certificados para personas físicas de la FNMT tienen una validez de 3 años).
- Las Autoridades de Certificación, igual que tienen a disposición de los usuarios la información de los certificados vigentes, han de tener **listas de certificados revocados**.

4. Mayor seguridad para la firma electrónica. Las tarjetas inteligentes. El DNI electrónico

El usuario de un certificado es responsable de la correcta custodia del mismo y de sus claves de acceso, para evitar cualquier uso fraudulento (recordemos aquí el rigor que se empleaba hace siglos para conservar las matrices de los sellos usados en la documentación solemne).

Sin embargo los sistemas de copias de seguridad en ficheros almacenados en discos o disquetes no reúne las mejores condiciones. Para resolver estas deficiencias en la actualidad la mejor solución está en las llamadas «tarjetas inteligentes».

Una tarjeta inteligente físicamente es una tarjeta de plástico parecida a las tarjetas de crédito, pero que en lugar de la banda magnética dispone de un chip que en realidad es un microprocesador capaz de almacenar información, de realizar complejas funciones criptográficas e impedir intentos de acceso no autorizados, así como impedir la duplicación de la misma.

El DNI electrónico, regulado por Real Decreto 1553/2005, de 23 de diciembre y ya en marcha, además de la función habitual de DNI cumple las funciones de tarjeta inteligente, válida para la acreditación y firma electrónica, ya que dispone de un microchip con todos los certificados y funciones criptográficas necesarios. Incluye dos certificados, uno válido para autenticación o acreditación de identidad con objetivo de establecimiento de conexiones telemáticas seguras y otro de firma electrónica que incluye el «no repudio» por parte del firmante de un documento.

Aunque casi todo son ventajas a favor de las tarjetas inteligentes frente a la utilización de ficheros tradicionales para la conservación de los certificados digitales, las tarjetas inteligentes exigen algunos elementos de software y hardware que hacen que sean más caras y menos usadas, aunque por motivos de seguridad parece claro que terminarán por imponerse en un plazo corto.

5. Fechado digital (sellado de tiempo o *time stamping*)

Estamos acostumbrados a incluir nuestra firma detrás de la fecha en los documentos en papel. Pero ¿qué pasa con los documentos firmados electrónicamente? ¿Cómo podemos estar seguros de que un documento ha sido firmado en el momento en que se nos indica? En muchas ocasiones puede ser necesario tener la certeza de que un documento electrónico ha sido firmado en un momento determinado, en una fecha y en una hora concreta. ¿Cómo tener garantía técnica y legal de ello?

El mecanismo que puede ayudarnos a resolver este problema es el fechado digital, también llamado sellado de tiempo y en inglés *time stamping*. Igual que la firma digital se basa en la existencia de un «tercero de confianza» que actúa como Autoridad de Fechado o prestador de servicio de fechado digital (en inglés, Time Stamping Authority o TSA).

La Autoridad de Fechado, que es normalmente al misma Autoridad de Certificación, utiliza como apoyo una fuente fiable de fecha y hora, un sistema informático con GPS que permite disponer de la fecha y hora reales, en tiempo universal coordinado. Esta fuente fiable está sincronizada con el Real Instituto y Observatorio de la Armada, que de acuerdo con lo previsto en el Real Decreto 1308/1992, de 23 de octubre, sobre la hora legal, es el depositario del Patrón Nacional de Tiempo.

Para fechar un documento con su firma, los pasos básicos son los siguientes:

- Generar el documento en uno de los formatos habituales.
- Producir el resumen *hash* del documento.
- Solicitar a la Autoridad de Fechado que incorpore el sello de tiempo *(token).*
- El sello de tiempo que se obtiene como respuesta de la Autoridad de Fechado (avalado por el certificado de esta Autoridad), se incrustará en el documento, proporcionando una garantía adicional.

6. ¿Cómo se obtiene un certificado digital de usuario para realizar firma electrónica reconocida?

1. *Solicitud de certificado*

El primer paso es dirigirse a través de Internet a la entidad prestadora de servicio de certificación. Elegimos la FNMT-RCM (Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda) para el ejemplo, pero adjuntamos posteriormente la lista de AC en España.

http://www.cert.fnmt.es/clase2/solicitud/mainpeti.htm

Téngase en cuenta que todos los pasos de este proceso deben hacerse a través del mismo ordenador, que además no podrá ser formateado durante el periodo que dure la obtención del certificado, y a través del mismo navegador (Explorer, Netscape...).

Introduciendo el NIF del interesado el sistema devuelve un código que habrá que presentar cuando se acredite la identidad.

2. *Acreditación de identidad en la Oficina de Registro*

Con el código que ha sido proporcionado en el caso anterior y con documento acreditativo (DNI, NIE...), es preciso acudir físicamente a una Oficina de Registro, como única forma de garantizar la identidad del solicitante. Estas oficinas, también reguladas por la Ley de Firma Electrónica, realizarán las ges-

tiones oportunas para que en un plazo máximo de 48 horas se pueda descargar el certificado.

3. *Descarga del Certificado*

Con el número de NIF del titular y el código de la solicitud de certificado, se vuelve a entrar en la web de la FNMT y se descarga el certificado. Durante el proceso se generan las claves privada y pública del interesado. La privada se le entrega directamente al peticionario, que será responsable de su conservación cuidadosa, y la pública se pone a disposición de todos a través de la red. Para el cifrado asimétrio se utiliza el algoritmo RSA y para la generación de funciones hash se utiliza el algoritmo SHA-1

4. *Copias de seguridad y exportación del certificado*

Una vez recibido el certificado es recomendable obtener una copia seguridad del certificado y su correspondiente clave privada por dos motivos principales:

- para evitar quedarnos sin el certificado y sin la clave en el caso de que el ordenador donde se haya generado el certificado tenga algún problema,
- para poder instalar y utilizar el certificado en otro ordenador.

Para realizar estas operaciones los navegadores proporcionan las herramientas adecuadas.

5. *Envío y recepción de mensajes firmados*

A partir de ahora podremos enviar y recibir mensajes firmados electrónicamente, utilizando para ello las herramientas que nos proporcionan los distintos sistemas de correo electrónico o diferentes paquetes de software. Por poner un ejemplo, los clientes de correo electrónico convencionales disponen de herramientas fáciles de utilizar, tanto para la firma de nuestros mensajes con nuestro certificado de usuario como la comprobación de la validez de los mensajes recibidos utilizando la clave pública del remitente.

7. Autoridades de certificación

La primera autoridad de certificación reconocida y la más extendida en nuestro país, especialmente en lo que a las Administraciones Públicas se refiere es la Fábrica Nacional de Moneda y Timbre. Real Casa de la Moneda, que

a través de su proyecto CERES (Certificación Española) ofrece certificados de usuario (incluyendo las opciones de tarjetas inteligentes) tanto para personas físicas como jurídicas. Pero además de ella existen otras opciones.

Presentamos a continuación la lista de los prestadores reconocidos, que según la página web del Ministerio de Industria, Comercio y Turismo han realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 (las direcciones URL fueron comprobadas el día 2 de agosto de 2006):

AC ABOGACÍA
http://www.acabogacia.org/acaPublico/publica/index.htm

ANCERT – Agencia Notarial de Certificación
http://www.ancert.com/

ANF AC.- Asociación Nacional de Fabricantes, Autoridad de Certificación
http://www.anf.es/security/cont.html?lang=es

Autoridad de Certificación de la Comunidad Valenciana (ACCV)
http://www.accv.es/default_default.htm

BANESTO CA
http://ca.banesto.es/

CAMERFIRMA
http://www.camerfirma.com/

CATcert (Agencia Catalana de Certificación)
http://www.catcert.net/web/cas/inici/home.jsp

FABRICA NACIONAL DE MONEDA Y TIMBRE (Ceres)
http://www.cert.fnmt.es/

CICCIP (Colegio de Ingenieros de Caminos, Canales y Puertos)
http://pki.ciccp.es/

FIRMAPROFESIONAL
http://www.firmaprofesional.com/bienvenida.htm

IZEMPE, S.A.
http://www.izenpe.com/s15-5218/es/

ANEXO II

Legislación

1. España

Leyes y decretos

- LEY 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (BOE n. 285 de 27 de noviembre) (Artículo 45).
- REAL Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado (BOE n. 52 de 29 de febrero).
- LEY 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos (BOE n. 57 de 7 de marzo).
- REAL DECRETO 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (BOE n. 151 de 25 de junio).
- LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE n. 298 de 14 de diciembre).
- REAL DECRETO 111/2000, de 28 de enero, por el que se modifican determinados artículos del Reglamento General de Recaudación, aprobado por Real Decreto 1684/1990, de 20 de diciembre, en materia de ingresos correspondientes a declaraciones presentadas por vía telemática. (BOE n. 25 de 29 de enero).

- REAL DECRETO 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11de junio (BOE n. 49 de 26 de febrero).
- LEY 24/2001, de 27 de diciembre, de medidas fiscales, administrativas y del orden social (BOE n. 313 de 31 de diciembre).
- LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE n. 166 de 12 de julio).
- REAL DECRETO 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original (BOE n. 274 de 15 de noviembre).
- REAL DECRETO 1377/2002, de 20 de diciembre, por el que se desarrolla la colaboración social en la gestión de los tributos para la presentación telemática de declaraciones, comunicaciones y otros documentos tributarios. (BOE N. 205 de 15 de noviembre).
- 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 (BOE n. 51 de 28 de febrero).
- LEY 7/2003, de 1 de abril, de la Sociedad Limitada Nueva empresa por la que se modifica la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada (BOE n.79 de 2 de abril).
- REAL DECRETO 682/2003, de 7 de junio, por el que se regula el sistema de tramitación telemática a que se refiere el artículo 134 y la disposición adicional octava de la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada (BOE n. 138 de 10 de junio).
- LEY 59/2003, de 19 de diciembre, de firma Electrónica (BOE n. 304, de 20 de diciembre de 2003).
- 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 (BOE n. 307 de 24 de diciembre de 2005).

Órdenes, resoluciones, instrucciones

1999

- ORDEN de 21 de diciembre de 1999 por la que se fijan los umbrales estadísticos de asimilación definidos en el artículo 28 del Reglamento (CEE) 3330/91 del Consejo y se autoriza la presentación de declaraciones Intrastat por vía telemática. (BOE n. 310 de 28 de diciembre).

- ORDEN de 22 de diciembre de 1999 por la que se establece el procedimiento para la presentación telemática de las declaraciones-liquidaciones que generen deudas o créditos que deban anotarse en la cuenta corriente en materia tributaria. (BOE n. 311 de 29 de diciembre).

2000

- ORDEN de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica (BOE n. 45 de 22 de febrero).
- ORDEN de 24 de abril de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre la Renta de las Personas Físicas. (BOE n. 103 de 29 de abril).
- ORDEN de 28 de abril de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre el Patrimonio. (BOE n. 103 de 29 de abril).
- ORDEN de 28 de junio de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes, en pesetas y en euros, para los períodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 1999 y de los modelos para efectuar los pagos fraccionados, en pesetas y en euros, a cuenta de los citados impuestos durante 2000. (BOE n. 156 de 30 de junio).
- INSTRUCCIÓN de 19 de octubre de 2000, de la Dirección General de los Registros y del Notariado, sobre el uso de la firma electrónica de los fedatarios públicos (BOE n. 269 de 9 de noviembre).
- CORRECCIÓN de errores de la Orden de 20 de noviembre de 2000 por la que se aprueban los modelos 115, en pesetas y en euros, de declaración-documento de ingreso; los modelos 180, en pesetas y en euros, del resumen anual de retenciones e ingresos a cuenta sobre determinadas rentas o rendimientos procedentes del arrendamiento o subarrendamiento de inmuebles urbanos del Impuesto sobre la Renta de las Personas Físicas, del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes, correspondiente a establecimientos permanentes, así como los diseños físicos y lógicos para la sustitución de las hojas interiores del citado modelo 180 por soportes directamente legibles por ordenador y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 304 de 20 de diciembre).

- ORDEN de 24 de noviembre de 2000 por la que se aprueban los modelos 347, en pesetas y en euros, de declaración anual de operaciones con terceras personas, así como los diseños físicos y lógicos para la sustitución de sus hojas interiores por soportes directamente legibles por ordenador y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 286 de 29 de noviembre).
- ORDEN de 21 de diciembre de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática por internet de las declaraciones correspondientes a los modelos 117, 123, 124, 126, 128, 216, 131, 310, 311, 193, 198, 296 y 345. (BOE n. 311 de 28 de diciembre).
- ORDEN de 21 de diciembre de 2000 por la que se establece el procedimiento para la presentación telemática por teleproceso de las declaraciones correspondientes a los modelos 187, 188, 190, 193, 194, 196, 198, 296, 345 y 347. (BOE n. 311 de 28 de diciembre).
- CORRECCIÓN de errores de la Orden de 21 de diciembre de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática por internet de las declaraciones correspondientes a los modelos 117, 123, 124, 126, 128, 216, 131, 310, 311, 193, 198, 296 y 345. (BOE n. 5 de 5 de enero).
- ORDEN de 28 de diciembre de 2000 por la que se fijan los umbrales estadísticos de asimilación definidos en el artículo 28 del Reglamento (CEE) 3330/91 del Consejo y se autorizan nuevas formas de presentación de declaraciones Intrastat por vía telemática. (BOE n. 313 de 30 de diciembre).

2001

- ORDEN de 15 de marzo de 2001 por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes, en pesetas y en euros, para los períodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 2000, se dictan instrucciones relativas al procedimiento de declaración e ingreso y se aprueban los modelos para efectuar los pagos fraccionados, en pesetas y en euros, a cuenta de los citados impuestos que deben realizarse durante 2001 y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 68 de 20 de marzo).
- CORRECCIÓN de errores de la Orden de 15 de marzo de 2001 por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes, en pesetas y en euros, para los períodos impositivos iniciados entre el 1 de enero y el 31

de diciembre de 2000, se dictan instrucciones relativas al procedimiento de declaración e ingreso y se aprueban los modelos para efectuar los pagos fraccionados, en pesetas y en euros, a cuenta de los citados impuestos que deben realizarse durante 2001 y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 168 de 14 de julio).

- ORDEN de 10 de abril de 2001 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre la Renta de las Personas Físicas y del Impuesto sobre el Patrimonio para el ejercicio 2000. (BOE n. 92 de 17 de abril).
- RESOLUCIÓN de 11 de abril de 2001, de la Agencia Estatal de Administración Tributaria, sobre asistencia a los contribuyentes y ciudadanos en su identificación telemática ante las entidades colaboradoras con ocasión de la tramitación de procedimientos tributarios. (BOE n. 98 de 24 de abril).
- CORRECCIÓN de errores de la Orden de 7 de agosto de 2001 por la que se aprueba el modelo 346 en euros, de declaración informativa anual de subvenciones e indemnizaciones satisfechas o abonadas por entidades públicas o privadas a agricultores o ganaderos, así como los diseños físicos y lógicos para la sustitución de las hojas interiores de dicho modelo por soportes directamente legibles por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 222 de 15 de septiembre).
- ORDEN de 8 de agosto de 2001 por la que se aprueba el modelo 346 en euros, de declaración informativa anual de subvenciones e indemnizaciones satisfechas o abonadas por entidades públicas o privadas a agricultores o ganaderos, así como los diseños físicos y lógicos para la sustitución de las hojas interiores de dicho modelo por soportes directamente legibles por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 190 de 9 de agosto).
- ORDEN de 4 de octubre de 2001 por la que se aprueba el modelo 192 de declaración informativa anual de operaciones con Letras del Tesoro, así como los diseños físicos y lógicos para su presentación por soporte directamente legible por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso y se modifica la Orden de 22 de diciembre de 1999, por la que se aprueban los modelos 198 de declaración anual de operaciones con activos financieros y otros valores mobiliarios. (BOE n. 240 de 6 de octubre).
- ORDEN de 12 de noviembre de 2001 por la que se autoriza el pago en metálico del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados que grava la emisión de documentos que realicen función de giro o suplan a las Letras de Cambio, se amplía la autoriza-

ción del pago en metálico del impuesto correspondiente a determinados documentos negociados por Entidades Colaboradoras, se aprueban los modelos 610, 611, 615 y 616 en euros del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados, así como los diseños físicos y lógicos para la presentación de los modelos 611 y 616 de declaración informativa anual en soporte directamente legible por ordenador y se establece el procedimiento para su presentación telemática por teleproceso. (BOE 275 de 16 de noviembre).

- RESOLUCIÓN de 11 de diciembre de 2001, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se regula la presentación por vía telemática de recursos de reposición y otras solicitudes de carácter tributario. (BOE n. 311 de 28 de diciembre).
- ORDEN de 21 de diciembre de 2001 por la que se aprueba el modelo 195 de declaración trimestral en euros de cuentas u operaciones cuyos titulares no hayan facilitado el número de identificación fiscal a las entidades de crédito en el plazo establecido, y el modelo 199 de declaración anual en euros de identificación de las operaciones con cheques de las entidades de crédito, así como los diseños físicos y lógicos para la presentación de los citados modelos por soporte directamente legible por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 312 de 29 de diciembre).
- RESOLUCIÓN de 21 de diciembre de 2001, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se delegan competencias en el Director general en materia de Convenios de colaboración para la presentación telemática de declaraciones, comunicaciones y otros documentos tributarios. (BOE n. 28 de 1 de febrero).
- ORDEN de 28 de diciembre de 2001 por la que se aprueba el modelo de declaración para el desglose por establecimientos de cuotas centralizadas de impuestos especiales de fabricación; se establece la presentación telemática por Internet de declaraciones-liquidaciones por los conceptos de impuestos especiales de fabricación y del impuesto sobre el valor añadido en operaciones asimiladas a las importaciones; y la obligación de declarar el numero de albarán con cargo al cual se expiden las notas de entrega en el procedimiento de ventas en ruta. (BOE n. 5 de 05/01/2002).
- CORRECCIÓN de errores de la Orden de 28 de diciembre de 2001 por la que se aprueba el modelo de declaración para el desglose por establecimientos de cuotas centralizadas de impuestos especiales de fabricación; se establece la presentación telemática por internet de declaraciones-liquidaciones por los conceptos de impuestos especiales de fabricación y del impuesto sobre el valor añadido en operaciones asimiladas a las importaciones, y la obligación de declarar el número de albarán con cargo al cual se expiden las notas de entrega en el procedimiento de ventas en ruta. (BOE n. 31 de 5 de febrero).

2002

- RESOLUCIÓN de 8 de enero de 2002, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueba el modelo de solicitud de devolución y el modelo de comunicación de datos adicionales por el Impuesto sobre la Renta de las Personas Físicas, ejercicio 2001, que podrán utilizar los contribuyentes no obligados a declarar por dicho Impuesto que soliciten la correspondiente devolución, y se determinan el lugar, plazo y forma de presentación de los mismos, así como las condiciones para su presentación telemática. (BOE n.13 de 15 de enero).
- ORDEN HAC/360/2002, de 19 de febrero, por la que se aprueba el modelo 349, de declaración recapitulativa de operaciones intracomunitarias, se establecen las condiciones generales y el procedimiento para su presentación telemática y se regula la colaboración social en la presentación telemática de la declaración anual de operaciones con terceras personas, modelo 347. (BOE n. 46 de 22 de febrero).
- CORRECCIÓN de errores de la Orden HAC/401/2002, de 26 de febrero, por la que se aprueban los modelos 202, 218 y 222 para efectuar los pagos fraccionados a cuenta del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes y se establecen las condiciones generales y el procedimiento para su presentación telemática, y se regula la colaboración social en la presentación telemática de las declaraciones-liquidaciones correspondientes a los modelos 115, 117, 123, 124, 126 y 128 y de las declaraciones correspondientes a los resúmenes anuales de retenciones, modelos 180 y 193. (BOE n. 100 de 26 de abril).
- ORDEN HAC/536/2002, de 7 de marzo, por la que se aprueban los modelos de declaración del Impuesto sobre la Renta de las Personas Físicas y del Impuesto sobre el Patrimonio para el ejercicio 2001, se determinan el lugar, forma y plazos de presentación de los mismos y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 62 de 13 de marzo).
- CORRECCIÓN de errores de la Orden HAC/536/2002, de 7 de marzo, por la que se aprueban los modelos de declaración del Impuesto sobre la Renta de las Personas Físicas y del Impuesto sobre el Patrimonio para el ejercicio 2001, se determinan el lugar, forma y plazos de presentación de los mismos y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 94 de 19 de abril y 100 de 26 de abril).
- ORDEN HAC/593/2002, de 12 de marzo, por la que se aprueba el modelo 183 de declaración informativa de determinados premios exentos del Impuesto sobre la Renta de las Personas Físicas, así como los

diseños físicos y lógicos para su presentación por soporte directamente legible por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 67 de 19 de marzo).

- ORDEN HAC/639/2002, de 21 de marzo, por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes para los períodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 2001, se dictan instrucciones relativas al procedimiento de declaración e ingreso y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 73 de 26 de marzo).
- ORDEN HAC/921/2002, de 24 de abril, por la que se aprueba el modelo 291 de declaración informativa en relación con los rendimientos de cuentas de no residentes obtenidos por contribuyentes, sin mediación de establecimiento permanente, del Impuesto sobre la Renta de no Residentes, así como los diseños físicos y lógicos para su presentación por soporte directamente legible por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 101 de 27 de abril).
- ORDEN HAC/998/2002, de 3 de mayo, por la que se establecen las condiciones generales y el procedimiento para la presentación telemática del modelo 361 de solicitud de devolución del Impuesto sobre el Valor Añadido soportado por determinados empresarios o profesionales no establecidos en el territorio de aplicación del Impuesto y por la que se modifica el anexo VII de la Orden de 15 de junio de 1995. (BOE n. 110 de 8 de mayo).
- CORRECCIÓN de errores de la Orden HAC/1025/2002, de 7 de mayo, por la que se aprueban nuevos modelos de declaración censal de comienzo, modificación o cese de la actividad que han de presentar a efectos fiscales los empresarios, los profesionales y otros obligados tributarios y se establece el ámbito, condiciones generales y procedimiento para su presentación telemática. (BOE n. 115 de 14 de mayo)
- ORDEN ECO/1101/2002, de 13 mayo, por la que se regula la presentación por vía telemática de determinadas solicitudes en materia de Comercio Exterior. (BOE n. 118 de 17 de mayo).
- RESOLUCIÓN 5/2002, de 17 de mayo, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se regula la participación por vía telemática en procedimientos de enajenación de bienes desarrollados por los órganos de recaudación. (BOE n. 124 de 24 de mayo).
- ORDEN ECO/1758/2002, de 9 de julio, por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos en materia de personal. (BOE n. 166 de 12 de julio).

- ORDEN HAC/1927/2002, de 24 de julio, por la que se modifica la Orden de 4 de julio de 2001 por la que se aprueban los modelos 600, 620 y 630, en pesetas y en euros, de declaración-liquidación del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados y se determinan el lugar y plazos de presentación de los mismos y la Orden de 12 de noviembre de 2001 por la que se autoriza el pago en metálico del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados que grava la emisión de los documentos que realicen función de giro o suplan a las letras de cambio, se amplía la autorización del pago en metálico del impuesto correspondiente a determinados documentos negociados por entidades colaboradoras, se aprueban los modelos 610, 611, 615 y 616 en euros del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados, así como los diseños físicos y lógicos para la presentación de los modelos 611 y 616 de declaración informativa anual en soporte directamente legible por ordenador y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 181 de 30 de julio).
- RESOLUCIÓN de 25 de julio de 2002, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se regula la presentación por vía telemática de instancias, solicitudes, escritos y comunicaciones en procedimientos internos de gestión de recursos humanos. (BOE n. 208 de 30 de agosto).
- ORDEN HAC/2894/2002, de 8 de noviembre, por la que se establecen las condiciones generales y el procedimiento para la presentación telemática por Internet de la declaración ajustada al modelo 111 a presentar por las Administraciones públicas, incluida la Seguridad Social. (BOE n. 275 de 16 de noviembre).
- INSTRUCCIÓN de 3 de diciembre de 2002, de la Dirección General de los Registros y del Notariado, desarrollando la de 23 de octubre de 2001 que aprueba la cláusula autorizatoria para la presentación telemática de contratos en el Registro de Bienes Muebles y resolviendo otras cuestiones con relación al mismo. (BOE N. 302 de 18 de diciembre).
- ORDEN HAC/3134/2002, de 5 de diciembre, sobre un nuevo desarrollo del régimen de facturación telemática previsto en el artículo 88 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido, y en el artículo 9 bis del Real Decreto 2402/1985, de 18 de diciembre. (BOE n. 298 de 13 de diciembre).

2003

- RESOLUCIÓN de 16 de enero de 2003, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueba el modelo de solicitud de devolución y el modelo de comunicación de datos adi-

cionales por el Impuesto sobre la Renta de las Personas Físicas, ejercicio 2002, que podrán utilizar los contribuyentes no obligados a declarar por dicho Impuesto que soliciten la correspondiente devolución, y se determinan el lugar, plazo y forma de presentación de los mismos, así como las condiciones para su presentación telemática. (BOE n. 17 de 20 de enero 2003).

- RESOLUCIÓN 1/2003, de 20 de enero, de la Dirección General de la Agencia Estatal de Administración Tributaria, sobre asistencia a los contribuyentes en su identificación telemática ante las entidades colaboradoras, para el pago de deudas correspondientes a autoliquidaciones y liquidaciones practicadas por la Administración contra cuentas mediante el uso de tarjetas de crédito o débito asociadas a estas cuentas. (BOE n. 27 de 31 de enero 2003).
- RESOLUCIÓN de 20 de enero de 2003, de la Intervención General de la Administración del Estado, por la que se aprueba el modelo normalizado para la solicitud y se regula la participación por vía telemática en el procedimiento de solicitud de representante de la Intervención General de la Administración del Estado para los actos de comprobación material de la inversión. (BOE n. 55 de 5 de marzo).
- ORDEN ECO/97/2003, de 22 de enero, por la que se establecen los criterios generales de tramitación telemática de solicitudes de participación en procedimientos de provisión de puestos de trabajo. (BOE n. 26 de 30 de enero 2003).
- ORDEN HAC/96/2003, de 28 de enero, por la que se aprueban los diseños físicos y lógicos, modelo 185, a los que debe ajustarse la información mensual que los órganos y entidades gestores de la Seguridad Social y las Mutualidades están obligadas a suministrar de sus afiliados o mutualistas, para su presentación por soporte directamente legible por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 26 de 30 de enero 2003).
- RESOLUCIÓN 2/2003, de 14 de febrero, de la Dirección General de la Agencia Estatal de Administración Tributaria, sobre determinados aspectos relacionados con la facturación telemática. (BOE n. 51 de 28 de febrero).
- RESOLUCIÓN de 27 de febrero de 2003, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se modifica la Resolución de 16 de enero de 2003, por la que se aprueba el modelo de solicitud de devolución y el modelo de comunicación de datos adicionales por el Impuesto sobre la Renta de las Personas Físicas, ejercicio 2002, que podrán utilizar los contribuyentes no obligados a declarar por dicho Impuesto que soliciten la correspondiente devolución, y se determinan el lugar, plazo y forma de presentación de los mismos, así como las condiciones para su presentación telemática. (BOE n. 51 de 28 de febrero).

- ORDEN HAC/539/2003, de 10 de marzo, por la que se aprueban los diseños físicos y lógicos, modelo 186, a los que debe ajustarse la información mensual a suministrar a la Agencia Estatal de Administración Tributaria acerca de determinados datos obrantes en el Registro Civil relativos a nacimientos y defunciones, para su presentación por soporte directamente legible por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 63 de 14 de marzo).
- ORDEN HAC/540/2003, de 10 de marzo, por la que se aprueban los modelos 202, 218 y 222 para efectuar los pagos fraccionados a cuenta del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes y entidades en régimen de atribución de rentas constituidas en el extranjero con presencia en territorio español, y se establecen las condiciones generales y el procedimiento para su presentación telemática, y se modifica la regulación de la colaboración social en la presentación telemática de las declaraciones-liquidaciones correspondientes a los modelos 115, 117, 123, 124, 126 y 128 y de las declaraciones correspondientes a los resúmenes anuales de retenciones, modelos 180 y 193. (BOE n. 63 de 14 de marzo).
- RESOLUCIÓN de 12 de marzo de 2003, de la Subsecretaría del Ministerio de Economía, por la que se incluyen determinados procedimientos internos en materia de personal en el ámbito de aplicación de la Orden de 26 de diciembre de 2001 para posibilitar su tramitación telemática a través del Registro Telemático del Departamento. (BOE N. 66 de 18 de marzo).
- ORDEN HAC/573/2003, de 13 de marzo, por la que se aprueban los modelos de declaración del Impuesto sobre la Renta de las Personas Físicas y del Impuesto sobre el Patrimonio, para el ejercicio 2002, se determinan el lugar, forma y plazos de presentación de los mismos y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 67 de 19 de marzo) INSTRUCCIÓN de 18 de marzo de 2003, de la Dirección General de los Registros y del Notariado, con relación al Artículo 107 de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social (BOE n. 85 de 9 de abril).
- ORDEN ECO/755/2003, de 20 de marzo, por la que se regula la presentación por vía telemática de las declaraciones posteriores a través de intermediarios financieros relativas a operaciones de inversión en valores negociables. (BOE n. 81 de 4 de abril).
- RESOLUCIÓN de 26 de marzo de 2003, de la Dirección General de Comercio e Inversiones, por la que se especifican los modelos normalizados y las instrucciones que deben utilizar los intermediarios financieros para la presentación por vía telemática, prevista en el anexo I, I.2.3

y en el anexo II, I.2.3 de la Resolución de 31 de mayo de 2001, de la Dirección General de Comercio e Inversiones, de las declaraciones de inversiones extranjeras en valores negociables cotizados en mercados españoles y de inversiones españolas en valores negociables cotizados en mercados extranjeros. (BOE N. 82 de 5 de abril).

- ORDEN HAC/729/2003, de 28 de marzo, por la que se establecen los supuestos y las condiciones generales para el pago por vía telemática de las tasas que constituyen recursos de la Administración General del Estado y sus Organismos Públicos. (BOE n. 79 de 2 de abril).
- RESOLUCIÓN de 9 de abril de 2003, del Instituto de Contabilidad y Auditoría de Cuentas, por la que se establece la aplicación del procedimiento para la presentación de la autoliquidación y las condiciones para el pago por vía telemática de la tasa prevista en el artículo 23 de la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas. (BOE N. 86 de 10 de abril).
- ORDEN PRE/829/2003, de 4 de abril, por la que se modifica la Orden de 27 de junio de 1989, para establecer un sistema de presentación telemática de las solicitudes de adjudicación de plaza en las pruebas selectivas para el acceso a plazas de formación sanitaria especializada. (BOE n. 86 de 10 de abril).
- ORDEN HAC/958/2003, de 10 de abril, por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes para los períodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 2002, se dictan instrucciones relativas al procedimiento de declaración e ingreso y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 97 de 23 de abril).
- CORRECCIÓN de errores de la Orden HAC/958/2003, de 10 de abril, por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no residentes correspondiente a establecimientos permanentes para los periodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 2002, se dictan instrucciones relativas al procedimiento de declaración e ingreso y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 101 de 28 de abril).
- ORDEN HAC/1149/2003, de 5 de mayo, por la que se establecen las condiciones generales y el procedimiento para la presentación telemática por Internet de los documentos utilizados en la gestión de Impuestos Especiales y se modifica la Orden de 22 de marzo de 2000, por la que se aprueban los nuevos modelos de relaciones recapitulativas y los soportes magnéticos de documentos de acompañamiento expedidos y de documentos de acompañamiento recibidos en tráfico intracomunitario, incluidos los simplificados. (BOE n. 114 de 13 de mayo).

- ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria (BOE n. 116 de 15 de mayo).
- ORDEN HAC/1398/2003, de 27 de mayo, por la que se establecen los supuestos y condiciones en que podrá hacerse efectiva la colaboración social en la gestión de los tributos, y se extiende ésta expresamente a la presentación telemática de determinados modelos de declaración y otros documentos tributarios. (BOE n. 132 de 3 de junio).
- INSTRUCCIÓN de 30 de mayo de 2003, de la Dirección General de los Registros y del Notariado, en relación a la entrada en vigor de la Ley 7/2003, de 1 de abril, de la Sociedad Limitada Nueva Empresa.(BOE n. 140 de 12 de junio).
- ORDEN ECO/1371/2003, de 30 de mayo, por la que se regula el procedimiento de asignación del Código ID-CIRCE que permite la identificación de la Sociedad Limitada Nueva Empresa y su solicitud en los procesos de tramitación telemática.(BOE n. 130 de 31 de mayo).
- ORDEN JUS/1445/2003, de 4 de junio, por la que se aprueban los estatutos orientativos de la Sociedad Limitada Nueva Empresa. (BOE n. 134 de 5 de junio).
- RESOLUCIÓN de 24 de junio de 2003, del Comisionado para el Mercado de Tabacos, por la que se establece el procedimiento para la solicitud de autorizaciones de venta con recargo mediante la presentación telemática de las autoliquidaciones y las condiciones para el pago por vía telemática de la tasa devengada por el ejercicio de la venta de labores de tabaco con recargo. (BOE n. 157 de 2 de julio).
- ORDEN ECO/1864/2003, de 30 de junio, por la que se amplía el ámbito de aplicación de la Orden ECO/97/2003, de 22 de enero, por la que se establecen los criterios generales de tramitación telemática de solicitudes de participación en procedimientos de provisión de puestos de trabajo. (BOE n. 161 de 7 de julio).
- ORDEN ECO/2087/2003, de 9 de julio, por la que se regula la presentación por vía telemática de las solicitudes de autorización de los regímenes aduaneros económicos de perfeccionamiento activo y perfeccionamiento pasivo que concede la Secretaría General de Comercio Exterior. (BOE n. 176 de 24 de julio).
- CORRECCIÓN de errores de la Orden HAC/2116/2003, de 22 de julio, por la que se aprueban el modelo 190 para el resumen anual de retenciones e ingresos a cuenta del Impuesto sobre la Renta de las Personas Físicas sobre Rendimientos del Trabajo, de determinadas actividades económicas, premios y determinadas imputaciones de renta, los diseños físicos y lógicos para la sustitución de las hojas interiores de

dicho modelo por soportes directamente legibles por ordenador, se establecen las condiciones generales y el procedimiento para su presentación telemática por internet y se modifican las normas de presentación de determinados modelos de declaración anual. (BOE n. 247 de 15 de octubre).

- RESOLUCIÓN de 24 de julio de 2003, de la Subsecretaría del Ministerio de Economia, por la que se extienden a los Servicios Periféricos determinados procedimientos internos en materia de personal en el ámbito de aplicación de la Orden de 26 de diciembre de 2001 para posibilitar su tramitación telemática a través del Registro Telemático del Departamento. (BOE n. 188 de 7 de agosto).
- RESOLUCIÓN de 30 de julio de 2003, de la Subsecretaría del Ministerio de Economía, por la que se establece la aplicación del procedimiento para la presentación de la autoliquidación y las condiciones para el pago por vía telemática de la tasa prevista en el artículo 57 de la Ley 16/1989, de 17 de julio, de Defensa de la Competencia. (BOE N. 188 de 7 de agosto).
- ORDEN HAC/2572/2003, de 10 de septiembre, por la que se aprueba el modelo 840 de Declaración del Impuesto sobre Actividades Económicas y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 224de 18 de septiembre).
- ORDEN HAC/3219/2003, de 14 de noviembre, por la que se aprueba el modelo 182 de declaración informativa de donativos, donaciones y aportaciones recibidas, así como los diseños físicos y lógicos para la sustitución de las hojas interiores de dicho modelo por soportes directamente legibles por ordenador, y se establecen las condiciones y el procedimiento para su presentación telemática a través de Internet. (BOE N. 279 de 21 de noviembre).
- RESOLUCIÓN de 18 de noviembre de 2003, de la Comisión Nacional del Mercado de Valores, por la que se establece el procedimiento y las condiciones para el pago a través de entidad colaboradora en la gestión recaudatoria y por vía telemática de las tasas aplicables por las actividades y servicios prestados por la Comisión Nacional del Mercado de Valores. (BOE n. 284 de 27 de noviembre).
- ORDEN HAC/3580/2003, de 17 diciembre, por la que se aprueba el modelo 156 de declaración informativa anual de las cotizaciones de afiliados y mutualistas a efectos de la deducción por maternidad, así como los diseños físicos y lógicos para su presentación por soporte directamente legible por ordenador, y se establece el procedimiento para su presentación telemática por teleproceso. (BOE n. 306 de 23 de diciembre).
- RESOLUCIÓN de 18 de diciembre de 2003, de la Comisión Nacional de Energía, por la que se establecen los criterios generales de tramita-

ción telemática de determinados procedimientos y se crea un registro telemático para la presentación de escritos y solicitudes cuya resolución compete a la Comisión Nacional de Energía. (BOE n. 8 de 9 de enero 2004).

- ORDEN HAC/3626/2003, de 23 de diciembre, por la que se aprueban los modelos de declaración 210, 215, 212, 211 y 213 del Impuesto sobre la Renta de no Residentes, que deben utilizarse para declarar las rentas obtenidas sin mediación de establecimiento permanente, la retención practicada en la adquisición de bienes inmuebles a no residentes sin establecimiento permanente y el gravamen especial sobre bienes inmuebles de entidades no residentes, así como el modelo de declaración 214, declaración simplificada de no residentes de los Impuestos sobre el Patrimonio y sobre la Renta de no Residentes; se establecen las condiciones generales y el procedimiento para la presentación telemática por internet de dichas declaraciones y otras normas referentes a la tributación de no residentes. (BOE n. 312 de 30 de diciembre).

2004

- ORDEN APU/203/2004, de 29 de enero, por la que se crea un Registro Telemático en el Ministerio de Administraciones Públicas para la presentación de escritos y solicitudes y se establecen los criterios generales de tramitación telemática de determinados procedimientos. (BOE n. 33 de 7 de febrero 2004).
- ORDEN HAC/171/2004, de 30 de enero, por la que se aprueba el modelo 184 de declaración informativa anual a presentar por las entidades en régimen de atribución de rentas y los diseños físicos y lógicos para la sustitución de las hojas de declaración de rentas de la entidad y las hojas de relación de socios, herederos, comuneros o partícipes de dicho modelo por soportes directamente legibles por ordenador, y se establecen las condiciones generales y el procedimiento para su presentación telemática por internet. (BOE n. 30 de 4 de febrero 2004).
- ORDEN HAC/1163/2004, de 14 de abril, por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes y a entidades en régimen de atribución de rentas constituidas en el extranjero con presencia en territorio español, para los períodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 2003, se dictan instrucciones relativas al procedimiento de declaración e ingreso y se establecen las condiciones generales y el procedimiento para su presentación telemática. (BOE n. 109 de 5 de mayo 2004).

- ORDEN PRE/989/2004, de 15 de abril, por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos por el Ministerio de la Presidencia y los organismos públicos adscritos al departamento y se crea un registro telemático para la presentación de escritos y solicitudes. (BOE n. 92 de 16 de abril 2004).
- RESOLUCIÓN de 31 de mayo de 2004, del Consorcio de Compensación de Seguros, por la que se aprueban los modelos en los que deberán realizarse las declaraciones-liquidaciones de recargos recaudados por su cuenta a través de la vía telemática. (BOE n. 141 de 11 de junio 2004).
- ORDEN TAS/2839/2004, de 29 de julio, por la que se implanta el proceso normalizado para la tramitación de modificaciones de crédito por vía telemática, e-MOPRES, en el Sistema de la Seguridad Social. (BOE n. 204 de 24 de agosto 2004).
- ORDEN EHA/3212/2004, de 30 de septiembre, por la que se establecen las condiciones generales y el procedimiento para la presentación telemática por internet de las declaraciones correspondientes a los modelos 308, 309, 341, 370, 371, 430 y 480. (BOE n. 243 de 8 de octubre 2004).
- ORDEN EHA/3433/2004, de 19 de octubre, por la que se aprueba el modelo 191 de declaración informativa anual de personas autorizadas en cuentas bancarias y por la que se aprueban las condiciones generales y el procedimiento para su presentación en soporte directamente legible por ordenador y por vía telemática por teleproceso. (BOE n. 258 de 26 de octubre 2004).
- CORRECCIÓN de errores de la Orden EHA/3433/2004, de 19 de octubre, por la que se aprueba el modelo 191 de declaración informativa anual de personas autorizadas en cuentas bancarias y por la que se aprueban las condiciones generales y el procedimiento para su presentación en soporte directamente legible por ordenador y por vía telemática por teleproceso. (BOE n. 21 de 25 de enero 2005).
- ORDEN EHA/3492/2004, de 25 de octubre, por la que se modifica la Orden HAC/2116/2003, de 22 de julio, por la que se aprueban el modelo 190 para el resumen anual de retenciones e ingresos a cuenta del Impuesto sobre la Renta de las Personas Físicas sobre rendimientos del trabajo, de determinadas actividades económicas, premios y determinadas imputaciones de renta, los diseños físicos y lógicos para la sustitución de las hojas interiores de dicho modelo por soportes directamente legibles por ordenador, se establecen las condiciones generales y el procedimiento para su presentación telemática por internet y se modifican las normas de presentación de determinados modelos de declaración anual. (BOE n. 261 de 29 de octubre 2004).
- Orden EHA/3895/2004, de 23 de noviembre, por la que se aprueba el modelo 198, de declaración anual de operaciones con activos financie-

ros y otros valores mobiliarios, así como los diseños físicos y lógicos para la sustitución de sus hojas interiores por soporte directamente legible por ordenador y se establecen las condiciones y el procedimiento para su presentación telemática a través de Internet y por teleproceso y se modifican las Órdenes de aprobación de los modelos de declaración 193, 296 y 347. (BOE n. 287 de 29 de noviembre 2004).

- CORRECCIÓN de errores de la Orden EHA/3895/2004, de 23 de noviembre, por la que se aprueba el modelo 198, de declaración anual de operaciones con activos financieros y otros valores mobiliarios, así como los diseños físicos y lógicos para la sustitución de sus hojas interiores por soporte directamente legible por ordenador y se establecen las condiciones y el procedimiento para su presentación telemática a través de internet y por teleproceso y se modifican las Órdenes de aprobación de los modelos de declaración 193, 296 y 347. (BOE n. 12 de 14 de enero 2005).

2005

- ORDEN ECI/23/2005, de 9 de enero, por la que se crea un registro telemático en el Ministerio de Educación y Ciencia para la presentación de escritos y solicitudes y se establecen los criterios generales de tramitación telemática de determinados procedimientos. (BOE n. 16 de 19/01/2005).
- RESOLUCIÓN de 21 de febrero de 2005, de la Subsecretaría del Ministerio de Administraciones Públicas, por la que se establece la aplicación del procedimiento para la presentación de la autoliquidación y las condiciones para el pago por vía telemática de la tasa de derechos de examen prevista en el artículo 18 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social respecto de pruebas selectivas de los cuerpos adscritos al Ministerio de Administraciones Públicas. (BOE n. 60 de 11 de marzo 2005).
- ORDEN EHA/748/2005, de 21 de marzo, por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes y a entidades en régimen de atribución de rentas constituidas en el extranjero con presencia en territorio español, para los períodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 2004, se dictan instrucciones relativas al procedimiento de declaración e ingreso, se establecen la condiciones generales y el procedimiento para su presentación telemática y se dictan determinadas instrucciones relativas al pago fraccionado de los citados impuestos. (BOE n.75 de 29 de marzo 2005).

- CORRECCION de errores de la Orden EHA/748/2005, de 21 de marzo, por la que se aprueban los modelos de declaración-liquidación del Impuesto sobre Sociedades y del Impuesto sobre la Renta de no Residentes correspondiente a establecimientos permanentes y a entidades en régimen de atribución de rentas constituidas en el extranjero con presencia en territorio español, para los períodos impositivos iniciados entre el 1 de enero y el 31 de diciembre de 2004, se dictan instrucciones relativas al procedimiento de declaración e ingreso, se establecen las condiciones generales y el procedimiento para su presentación telemática y se dictan determinadas instrucciones relativas al pago fraccionado de los citados impuestos. (BOE n. 90 de 15 de abril 2005).
- RESOLUCIÓN de 14 de abril de 2005, de la Subsecretaría del Ministerio de Industria, Turismo y Comercio, por la que se establece la aplicación del procedimiento para la presentación de la autoliquidación y las condiciones para el pago por vía telemática de la tasa de derechos de examen prevista en el artículo 18 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, respecto de pruebas selectivas de acceso a cuerpos especiales convocadas por el Ministerio de Industria, Turismo y Comercio. (BOE n. 96 de 22 de abril 2005).
- RESOLUCIÓN de 16 de mayo de 2005, de la Dirección General del Patrimonio del Estado, por la que se aprueba la aplicación Conecta-Patrimonio para la presentación telemática de proposiciones a los concursos de adopción de tipo de bienes y servicios de adquisición centralizada, así como de peticiones de suministros y servicios derivados de dichos concursos. (BOE n. 128 de 30 de mayo 2005).
- ORDEN EHA/1744/2005, de 3 de junio, por la que se establecen las condiciones generales, formularios y modelos para la presentación y tramitación telemáticas de solicitudes de clasificación de empresas, y se aprueba la aplicación telemática para su tratamiento. (BOE n. 140 de 13 de junio 2005).
- RESOLUCIÓN de 16 de junio de 2005, de la Subsecretaría del Ministerio de Fomento, por la que se establece el procedimiento para la presentación de la autoliquidación y las condiciones para el pago por vía telemática de diversas tasas correspondientes al Ministerio de Fomento. (BOE n. 151 de 25 de junio 2005).
- ORDEN EHA/1981/2005, de 21 de junio, por la que se aprueba el modelo 576 de declaración-liquidación del Impuesto Especial sobre Determinados Medios de Transporte, el modelo 6 de declaración del Impuesto Especial sobre Determinados Medios de Transporte, exenciones y no sujeciones sin reconocimiento previo, se establecen las condiciones generales y el procedimiento para la presentación tele-

mática por Internet de las declaraciones correspondientes al modelo 576 y se modifica la Orden de 30 de septiembre de 1999, por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de las declaraciones-liquidaciones correspondientes a los modelos 110, 130, 300 y 330. (BOE n. 153 de 28 de junio 2005).

- ORDEN EHA/2102/2005, de 29 de junio, por la que se modifican la Orden de 12 de julio de 1993, por la que se establecen diversas normas de gestión en relación con los impuestos especiales de fabricación, y la Orden de 2 de febrero de 1999, por la que se aprueban los modelos en euros para la gestión de los impuestos especiales de fabricación y la presentación por vía telemática de las declaraciones-liquidaciones para las grandes empresas. (BOE n. 157 de 2 de julio 2005).
- ORDEN EHA/2339/2005, de 13 de julio, por la que se aprueba el modelo 299, de declaración anual de determinadas rentas obtenidas por personas físicas residentes en otros Estados miembros de la Unión Europea y en otros países y territorios con los que se haya establecido un intercambio de información, los diseños físicos y lógicos para la presentación por soporte directamente legible por ordenador, se establecen las condiciones y el procedimiento para su presentación telemática a través de Internet y por teleproceso y se modifican la Orden de 21 de diciembre de 2000, por la que se establece el procedimiento para la presentación por teleproceso de las declaraciones correspondientes a los modelos 187, 188, 190, 193, 194, 196, 198, 296, 345 y 347 y otras normas relativas a la expedición de certificados de residencia fiscal. (BOE n. 171 de 19 de julio 2005).
- ORDEN DEF/2416/2005, de 18 de julio, por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos por el Ministerio de Defensa y los organismos públicos adscritos al departamento y se crea un registro telemático para la presentación de escritos y solicitudes. (BOE n. 177 de 26 de julio 2005).
- RESOLUCIÓN de 23 de agosto de 2005, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se regula la presentación de determinados documentos electrónicos en el registro telemático general de la Agencia Estatal de Administración Tributaria (BOE n. 219 de 13 de septiembre).
- ORDEN EHA/3061/2005, de 3 de octubre, por la que se establecen las condiciones y el procedimiento para la presentación telemática por Internet de las declaraciones correspondientes al modelo 038 y el procedimiento para la presentación telemática por teleproceso de las declaraciones correspondientes al modelo 180, se regula el lugar, plazo y forma de presentación de la declaración-resumen anual correspon-

diente al modelo 392 y se modifican determinadas normas de presentación de los modelos de declaración 180, 193, 345, 347 y 349, y otras normas tributarias. (BOE n. 239 de 6 de octubre 2005).

- RESOLUCIÓN de 19 de octubre de 2005, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se extiende la colaboración social a la presentación por vía telemática del recurso de reposición y se aprueba el documento normalizado para acreditar la representación para su presentación por vía telemática en nombre de terceros. (BOE n. 256 de 26 de octubre 2005).
- ORDEN CUL/4229/2005, de 28 de diciembre, por la que se crea un registro telemático en el Ministerio de Cultura para la presentación de escritos, solicitudes y comunicaciones y se establecen los criterios generales de tramitación telemática de determinados procedimientos. (BOE n. 11 de 13/1/2006).

2006

- RESOLUCIÓN de 10 de febrero de 2006, de la Secretaría de Estado de Justicia, por la que se publica el Acuerdo de encomienda de gestión del Ministerio de Justicia a la Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda para la prestación de servicios de certificación de firma electrónica y otros servicios relativos a la administración electrónica (BOE n. 56 de 7 de marzo)
- ORDEN ITC/352/2006, de 14 de febrero, por la que se aprueban medidas para la transparencia, innovación y gestión telemática de las ayudas del Ministerio de Industria, Turismo y Comercio. (BOE N. 39 de 15 de febrero 2006)
- RESOLUCIÓN de 22 de febrero de 2006, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se aprueba el modelo de impreso de solicitud de admisión a pruebas selectivas convocadas por la citada Agencia y liquidación de la tasa de derechos de examen, se dictan instrucciones complementarias sobre su aplicación y se establece el procedimiento para la presentación por vía telemática. (BOE n. 63 de 15 de marzo 2006)
- ORDEN FOM/660/2006, de 1 de marzo, por la que se crea el Registro Telemático del Ministerio de Fomento y se establecen los criterios generales para la tramitación telemática de determinados procedimientos. (BOE n. 59 de 10/3/2006)
- ORDEN PRE/1563/2006, de 19 de mayo, por la que se regula el procedimiento para la remisión telemática de las disposiciones y actos administrativos de los departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado» (BOE n. 123 de 24 de mayo)

2. Unión Europea

Firma electrónica

- DIRECTIVA 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica.
- DECISIÓN 2000/709/CE DE LA COMISIÓN de 6 de noviembre de 2000 relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica.
- DECISIÓN DE LA COMISIÓN de 14 de julio de 2003 relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo.

Documentos electrónicos de archivo para los archivos de la Comisión

- DECISION DE LA COMISIÓN 2002/47, de 23 de enero, por la que se modifica su Reglamento Interno, incorporando un Anexo titulado «Disposiciones sobre gestión de documentos». (DOUE, n. L 21, de 24 de enero).
- DECISION DE LA COMISIÓN 2004/563 de 7 de julio de 2004 por la que se modifica su Reglamento interno, con un Anexo titulado «Disposiciones de la Comisión relativas a los documentos electrónicos y digitalizados». (DOUE, n. L 251, de 27de julio).

CONFEDERACIÓN
DE ASOCIACIONES
DE ARCHIVEROS,
BIBLIOTECARIOS,
MUSEÓLOGOS Y
DOCUMENTALISTAS