Guía del curso

DOCUMENTOS Y FIRMA ELECTRÓNICOS

DIPUTACION PROVINCIAL DE HUESCA

Huesca, 2017

Dr. José Félix Muñoz Soro
Agencia Aragonesa para la Investigación y el Desarrollo (ARAID)
jfm@unizar.es

Contenido

Abreviaturas

- **ENI:** Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- **FNMT:** Fábrica Nacional de Moneda y Timbre.
- **LPAC:** Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- **LRISP:** Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- **LRJSP:** Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- **LSSI:** Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **LTBG:** Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- **LUTICAJ:** Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
- **NTI:** Normas técnicas de interoperabilidad.
- **PSC:** Prestador de servicios de confianza.
- **Reglamento eIDAS:** Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- **RRISP:** Real Decreto 1495/2011, de 24 de octubre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- **W3C:** *World Wide Web Consortium*. Entidad sin ánimo de lucro que establece los estándares de la web.

1 Contexto

1.1 Los documentos

1.1.1 Concepto

De acuerdo con el Diccionario de la Real Academia la palabra documento, procede del latín *documentum* y tiene, desde el punto de vista que aquí nos interesa, dos significados: 1) Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos, y 2) Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.

Estas dos definiciones reflejan las dos funciones principales de los documentos:

- La fijación y trasmisión de la información
- La prueba documental

En relación con este segundo significado distingue la Academia tres tipos de documentos, dentro del ámbito jurídico:

- Auténtico: el que está autorizado o legalizado.
- Privado: el que, autorizado por las partes interesadas, pero no por funcionario competente, prueba contra quien lo escribe o sus herederos.
- Público: el que, autorizado por funcionario para ello competente, acredita los hechos que refiere y su fecha.

Estas dos funciones se corresponderían con dos conceptos de documento, uno amplio, según el cual se considera que documento puede ser cualquier objeto material capaz de representar un hecho, y otro estricto, en el que el hecho representado debería tener trascendencia jurídica y el objeto constitutivo del documento tener características que le confieran valor probatorio [Pinochet 2002]. También se pueden distinguir dos conceptos de documento, en función de que utilicen o no un lenguaje simbólico para representar la información incorporada en el mismo. Estas diferencias podrían quedar reflejadas en la siguiente figura.

	Sin lenguaje simbólico	**Con lenguaje simbólico**
Sin carácter probatorio	Imágenes y videos	Documentos escritos
Con carácter probatorio	Imágenes o videos autenticados (por ej. video de una vista judicial)	Documentos escritos auténticos (por ej. escritura notarial)

Figura 1. Tipología de los documentos

Otra definición de documento es la contenida en la norma ISO 15489 que los define como "cualquier información creada, recibida y mantenida como evidencia e información por una organización o persona, en la consecución de sus obligaciones normativas o en las transacciones comerciales".

1.1.2 Definiciones legales

Por su parte, en Derecho español, la definición normativa más completa del término "documento" se halla recogida en el art. 2.3 del Decreto 242/1969, de 20 de febrero, de secretos oficiales, de acuerdo con el cual se entiende por documentos, cualquier constancia gráfica o de cualquier otra naturaleza y muy especialmente:

a) Los impresos, manuscritos, papeles mecanografiados o taquigrafiados y las copias de los mismos, cualesquiera sean los procedimientos empleados para su reproducción; los planos, proyectos, esquemas, esbozos, diseños, bocetos, diagramas, cartas, croquis y mapas de cualquier índole ya lo sean en su totalidad, ya las partes o fragmentos de las mismos.
b) Las fotografías y sus negativos, las diapositivas, los positivos y negativos de película, impresionable por medio de cámaras cinematográficas y sus reproducciones.
c) Las grabaciones sonoras de todas clases.
d) Las planchas, moldes, matrices, composiciones tipográficas, piedras litográficas, grabados en película cinematográfica, bandas escritas o perforadas, la memoria transistorizada de un cerebro electrónico y cualquier otro material usado para reproducir documentos.

Esta vieja definición supera, tanto en contenido como en precisión, a la más reciente recogida en el art. 2.2.b) del Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, según la cual "documento de archivo" es:

> el ejemplar en cualquier tipo de soporte, testimonio de las actividades y funciones de las personas físicas y jurídicas, públicas o privadas.

El artículo 317 de la Ley 1/2000, de 7 de enero, de enjuiciamiento civil, enumera las clases de documentos públicos.

> A efectos de prueba en el proceso, se consideran documentos públicos:
>
> 1º Las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Secretarios Judiciales.
>
> 2º Los autorizados por notario con arreglo a derecho.
>
> 3º Los intervenidos por Corredores de Comercio Colegiados y las certificaciones de las operaciones en que hubiesen intervenido, expedidas por ellos con referencia al Libro Registro que deben llevar conforme a Derecho.
>
> 4º Las certificaciones que expidan los Registradores de la Propiedad y Mercantiles de los asientos registrales.

> 5º Los expedidos por funcionarios públicos legalmente facultados para dar fe en lo que se refiere al ejercicio de sus funciones.
>
> 6º Los que, con referencia a archivos y registros de órganos del Estado, de las Administraciones públicas o de otras entidades de Derecho público, sean expedidos por funcionarios facultados para dar fe de disposiciones y actuaciones de aquellos órganos, Administraciones o entidades.

Por su parte, los documentos privados pueden definirse como aquellos documentos "que se formalizan entre los particulares, sin la intervención de notario o funcionario público que los autorice". De hecho, se trata de una categoría que la Ley delimita negativamente, por contraposición a la categoría de los documentos públicos que, como hemos visto, se delimita positivamente.

Dentro de los documentos públicos, el art. 26, 1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC), define como documentos públicos administrativos aquéllos que sean válidamente emitidos por los órganos de las Administraciones públicas. Así pues, es la procedencia (de un órgano de una Administración pública) la que califica como administrativo a un documento, debiendo estar a las reglas estatutarias aplicables para identificar, según la naturaleza administrativa o no del ente autor y emisor del documento, la naturaleza del mismo. Añade la norma que "las Administraciones públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia" por lo que la forma normal de los documentos administrativos pasa a ser el formato electrónico.

Finalmente, mencionar que el Código Penal castiga en sus arts. 390 a 394 la falsedad documental entendiendo por tal (i) la alteración de un documento en alguno de sus elementos o requisitos esenciales, (ii) la simulación total o parcial de un documento que induzca a error sobre su autenticidad, (iii) el reflejo en el mismo de la intervención de personas que no la han tenido, o la atribución a las que sí han intervenido declaraciones o manifestaciones diferentes de las que hubieran hecho, y (iv) la falta de correspondencia con la realidad en la narración de los hechos. De ello se deduce que el Derecho protege la integridad, autoría, veracidad y autenticidad de un documento, aunque no se especifican cuáles sean los "elementos o requisitos esenciales" de éste.

1.2 Evolución de los sistemas de información en las organizaciones

1.2.1 Introducción

J. Bing, un profesor de la Universidad de Oslo que fue pionero en el estudio de la Informática Jurídica, distingue tres generaciones de los sistemas de información en las administraciones:

- la primera orientada a los datos
- la segunda orientada a los documentos
- la tercera orientada al conocimiento

En la primera generación los ordenadores son capaces únicamente de manejar datos, es decir números y breves cadenas de caracteres. Los ordenadores de esta época son la base de los actuales grandes sistemas centrales, como pueden ser los de las sociedades de tarjetas de crédito, bancos y empresas de seguros, o los de Hacienda, la Tesorería de la Seguridad Social y la Policía. Son estas herramientas, suficientemente evolucionadas y probadas a lo largo de los últimos años, las que constituyen el núcleo de la automatización de las organizaciones. Esta se aplica ante todo a las administraciones financieras, las cuales a su vez determinan el funcionamiento de todas las demás administraciones, en la medida en la que controlan sus recursos económicos.

Actualmente los ordenadores nos permiten trabajar de forma similar a como venimos haciendo desde hace ya más de 5000 años con los documentos escritos, que están en la base de las burocracias y, en consecuencia, de la capacidad humana para crear organizaciones complejas. Es precisamente la migración de los documentos en papel a los documentos en formato electrónico lo que caracteriza a la segunda generación, en cuyos inicios nos encontramos. No dedicaremos ahora un apartado a esta generación, ya que en el curso se tratan a fondo los documentos electrónicos.

Finalmente, la tercera generación es el resultado de incorporar a los ordenadores no sólo información sino también "conocimiento", para lo que se utiliza un conjunto de técnicas que agrupamos bajo la denominación común de inteligencia artificial.

	Elementos físicos	**Elementos lógicos**	**Concepto jurídico**
1ª generación	Ordenadores centrales Redes jerárquicas	Bases de datos	Protección de datos de carácter personal
2ª generación	Ordenadores personales Internet	Bases documentales	Documento y firma electrónicos
3ª generación		Bases de conocimiento	Decisión automatizada

Figura 2.- Resumen de las características principales de las tres generaciones de los sistemas de información en las organizaciones

1.2.2 La primera generación

Aspectos físicos

Desde el punto de vista físico los sistemas de esta primera época se basan en grandes ordenadores que, de forma centralizada, dan servicio a toda una organización. La capacidad de cálculo y almacenamiento reside únicamente en este ordenador, que es capaz de atender a gran número de usuarios simultáneamente. A fin de unir a estos equipos con las sucursales remotas se establecieron redes telefónicas especiales para la transmisión de datos, que permitían que los miembros de las organizaciones pudieran acceder al sistema de forma permanente. En general, no se prevén las comunicaciones entre diferentes usuarios, ni la de documentos no formalizados. Los

ciudadanos no tienen acceso directo a los sistemas y siempre precisan de la intermediación de un miembro de la organización para actuar sobre estos.

La estructura de estos sistemas se denomina “de estrella”, ya que siempre existe un nodo central, del que podrán depender otros nodos, que a su vez podrán ser centro de su respectiva estrella. El esquema se corresponde con un árbol jerárquico, que arranca siempre de un único nodo superior. Por tanto, el paradigma jerárquico resulta totalmente adecuado para describir los sistemas de la primera generación. Y no sólo esto, sino que también cabe considerar que la rígida formalización impuesta a los miembros de la organización, y a los ciudadanos, en el modo de comunicarse con la organización acentúa el carácter jerárquico de las organizaciones. Debe considerarse que, como se ha dicho, la capacidad de cálculo se encuentra centralizada en mismo lugar, por lo que la delegación sufre una importante merma, ya que las decisiones que deban concordar con el sistema siempre dependerán de un único centro.

La autonomía de los miembros de la organización respecto a las decisiones decrece. En efecto, la comunicación de los usuarios con el sistema se reduce a la realización de las denominadas “transacciones” contra el ordenador central, algunos de cuyos datos pueden, según sus autorizaciones, consultar o modificar. Las transacciones se realizan mediante formularios, en los que los aspectos relevantes del caso y el modo en que deben expresarse quedan rígidamente definidos. A su vez, la estructura de los formularios guarda estrecha relación con el modo en que los datos son almacenados por el sistema. Los formularios no permiten la inclusión de datos no solicitados y, aun cuando el ciudadano o el miembro de la organización no respeten los límites que se le imponen, los procedimientos de trabajo no suelen estar preparados para considerar la información extra que pudiera haber sido aportada.

Aspectos lógicos

Desde el punto de vista de los programas, la herramienta básica utilizada por los sistemas de la primera generación son las llamadas “bases de datos”, en las que puede almacenarse gran cantidad de información. Inicialmente la estructura de estas bases fue la jerárquica, pero hace ya años que la mayoría de las bases de datos siguen el modelo relacional, llamado así porque se basa en la definición de entidades y de las relaciones entre éstas. Las entidades suelen tener uno o más atributos.

Por ejemplo, en un fichero de la Tesorería de la Seguridad Social las entidades pueden ser las personas y sus actos de cotización. La persona tendrá atributos como el nombre y la edad y los actos de cotización tendrán otros, como la fecha y la cuantía. La relación entre la entidad persona y la entidad actos de cotización es de uno a muchos, ya que a una persona pueden corresponder muchos actos de cotización y, por el contrario, cada acto de cotización sólo puede corresponder a una persona. De este modo la información contenida en el nivel de la base de datos se divide entre la inherente a su diseño (y es un acto de cotización perteneciente a x) y la contenida en los propios datos, es decir, los valores de los atributos de x e y.

En un tercer nivel el conocimiento se plasma en las sentencias del programa. Estos se crean mediante la llamada "programación condicional", que utiliza sentencias del tipo "si <condición> entonces <acción>". En estas sentencias debe incorporarse explícitamente el conocimiento de las relaciones entre los diferentes atributos de las entidades, así como el modo en que éstos participan en la decisión final. Posteriormente el programa en su ejecución sustituirá los datos genéricos (variables) de sus sentencias por los atributos concretos de una determinada entidad. Dicho de otro modo, en general, las bases de datos plasman el conocimiento fáctico de los casos, mientras que los programas incorporan el conocimiento normativo.

Las limitaciones inherentes a las herramientas de procesamiento automatizado de la información se deben, en primer lugar, a que la representación de los casos viene limitada por el tipo de datos que se pueden manejar. Estos sólo son, por una parte, los datos numéricos, sobre los que pueden realizarse gran número de operaciones matemáticas y lógicas, y por otra parte, la información textual que, básicamente, es manejada por los ordenadores en términos de coincidencia de cadenas, es decir, de correspondencia carácter a carácter de fragmentos de texto. La plasmación del conocimiento normativo se ve afectada por estas limitaciones que la ambigüedad inherente a las normas, que impide su plasmación mediante un lenguaje formal.

Características generales

Pese a estas limitaciones, los sistemas de la primera generación adquirieron un protagonismo muy importante en las organizaciones. Ha de tenerse en cuenta la gran importancia que tienen en éstas el dinero y el medio para su control, la contabilidad. Esta última es la función primera y primordial que se asignó a los sistemas de información, que han demostrado una enorme capacidad para esta tarea. Además, muchas de las prestaciones del Estado del Bienestar han sido reguladas mediante términos concretos y definidos en relación con datos de carácter numérico, como la renta familiar o la edad, u otros fácilmente representables como, por ejemplo, el sexo o el estado civil.

Esta reducción de la ambigüedad no obedece sólo a una intencionalidad en cuanto a facilitar la automatización del proceso de formación de las decisiones, sino a una técnica legislativa que pretende la mayor equidad posible en el reparto de las prestaciones, condicionando éstas a la valoración de datos objetivos. Pero, tanto la sociedad contemporánea como las tecnologías de la información evolucionan con notable rapidez, aumentando por una parte la complejidad de las prestaciones comunicativas y por otra la intervención en éstas de la tecnología. Ello nos lleva a una segunda etapa en la que la intermediación en los actos comunicativos de los nuevos sistemas se convierte en el factor a destacar, quedando en un segundo plano la capacidad de proceso de la información. En efecto, el avance en las comunicaciones a lo largo del último decenio es el factor que en estos momentos influye de forma más intensa en el proceso de formación de las decisiones mientras, paralelamente, los sistemas de la primera generación continúan realizando sus funciones cada vez con mayor eficacia.

1.2.3 La tercera generación

La inteligencia artificial

La inteligencia artificial, cuyo origen se sitúa en torno a 1961, suele definirse como el estudio del modo en el que los ordenadores pueden realizar tareas que requieren del uso de la inteligencia, cuando son hechas por humanos. Esta definición es muy amplia e incluye acciones tan sencillas como sumar, por ello en la práctica se atiende también a las técnicas informáticas empleadas a la hora de calificar a una aplicación como propia de la inteligencia artificial.

La inteligencia artificial marca la frontera del conocimiento que es posible inculcar a los ordenadores a fin de obtener de ellos resultados equivalentes a los que lograría una actividad humana en la que se haga uso de la inteligencia. Para J. Bing es precisamente el uso masivo de las técnicas de la inteligencia artificial el fenómeno que caracterizará a la tercera generación de los sistemas de información en las organizaciones, aún por llegar. Ello implicará la extensión del acceso a un nuevo tipo de bases, las bases de conocimiento.

Hoy en día existen, básicamente, dos formas de "enseñar" a los sistemas informáticos: bien aportando conocimiento explícito en forma de reglas (sistemas basados en reglas), bien enseñándoles unas pautas al hacerles procesar casos ya resueltos (redes neuronales). La primera de estas técnicas es utilizada en los denominados "sistemas expertos", desarrollados desde los orígenes de la IA y que han sido aplicados a numerosos problemas jurídicos, entre ellos muchos relacionados con las administraciones.

Se considera que el Derecho constituye un excelente campo de investigación para los ingenieros del conocimiento, nombre que reciben quienes desarrollan sistemas expertos, ya que el razonamiento jurídico se basa en casos y reglas, plasmados generalmente en textos. Además, se utilizan distintas formas de razonamiento como el deductivo, el inductivo y la analogía. Por otra parte, el Derecho aporta un profundo estudio de la forma de razonar que le es propia, realizado a lo largo de los siglos por la Filosofía y la Teoría del Derecho. Estas teorías pueden aportar luz, por ejemplo, sobre los límites de los sistemas expertos, que dependen de en qué medida el conocimiento jurídico puede ser expresado en forma de reglas. Además, los estudios de aquellas corrientes que se dedican al análisis lógico y conceptual del Derecho son básicos en la construcción de sistemas de ayuda a la decisión jurídica basados en reglas.

Tras la extensión de uso de la inteligencia artificial, un segundo fenómeno que caracterizará a la tercera generación será la utilización, dentro de la técnica informática, de los denominados "métodos cooperativos", ya que, ante la complejidad creciente de los sistemas, cada vez con mayor frecuencia, los diseñadores y gestores recurren a los métodos cooperativos a fin de coordinar la intervención de los múltiples subsistemas en la resolución de las tareas de la organización. Los métodos cooperativos son ya utilizados en inteligencia artificial y en gestión de redes. Podríamos definir brevemente a estos métodos como aquellos que recurren a la colaboración entre varios agentes para la resolución de problemas. De hecho, se acepta hoy en día de forma generalizada que la resolución de problemas complejos

mediante inteligencia artificial pasa por la división de las tareas entre agentes especializados. Esta forma de actuar aumenta en un primer momento los trabajos a realizar, ya que al conocimiento propio del problema ha de añadirse aquél necesario para la coordinación entre los agentes, que se realiza gracias a un "diálogo" entre estos. Así, los protocolos que se desarrollan con estos fines prevén la existencia de negociaciones previas y la firma de contratos entre diferentes subsistemas.

Los sistemas expertos

La mayor parte de los sistemas informáticos basados en el conocimiento son "sistemas expertos", que han sido construidos para auxiliar a decisiones, normalmente de carácter técnico. Se trata de herramientas que "incorporan, de una manera práctica y operativa, el conocimiento que posee un experto en la materia de que se trate".

Suelen distinguirse en la inteligencia artificial dos clases de conocimiento: el sentido común, que concierne a tareas que cualquier adulto normal puede realizar sin ninguna formación especial, como hablar su lengua nativa, reconocer objetos, encontrar un camino, etc., y conocimiento experto, que presupone habilidades y saberes especiales, como es el caso del diagnóstico de enfermedades, el diseño de ordenadores, etc. Los sistemas incorporan habitualmente el conocimiento de carácter más especializado, aunque también se trabaja en sistemas que representen el sentido común. Entre el conocimiento a aportar a los sistemas expertos cobran especial importancia las reglas heurísticas, que pueden ser definidas como aquellas que usualmente contribuyen a la resolución de problemas, pero que no garantizan de ninguna manera que se alcance el resultado. Por ejemplo, una regla heurística en el juego del ajedrez sería dominar el centro del tablero, aunque en ningún modo es seguro que gane la partida el jugador que lo haga.

La herramienta utilizada para la construcción de los sistemas expertos son lenguajes basados en reglas. Estos lenguajes permiten actuar sobre tres componentes: una memoria de trabajo que contiene símbolos que representan hechos y aserciones utilizados para resolver un problema, reglas que contienen el "conocimiento del dominio" del problema y, por último, un motor de inferencia que selecciona una regla entre las que se adecuan a la configuración de datos y la ejecuta. El motor de inferencia funciona con un ciclo que llamamos de "reconocimiento/actuación", que consta de los siguientes pasos: reconocimiento, selección y ejecución. En la primera fase se determinan las reglas ejecutables, es decir, aquéllas cuya precondición coincide con el contenido de la memoria de trabajo, formándose el denominado "conjunto conflicto". De éste, en la segunda fase, se selecciona la regla más adecuada para posteriormente ejecutarla, ejecución que consiste en la modificación del contenido de la memoria de trabajo. En la selección de las reglas se utilizan los operadores lógicos. La lógica clásica he demostrado ser suficiente para muchas aplicaciones y tiene la ventaja de su simplicidad y claridad. También se utiliza la lógica multivaluada, en la cual se asigna a cada cláusula un valor de verdad, representado por un número comprendido entre el cero y el uno. Hay, además, autores que consideran que es preciso modificar las propias tablas de verdad de los operadores lógicos para su uso en el Derecho.

En la representación del conocimiento también se emplean frames y "redes semánticas". Los primeros pueden ser definidos como estructuras de datos diseñadas para representar una situación u objeto del mundo real. En cuanto a las segundas, establecen relaciones entre las palabras utilizadas en la representación. Normalmente estas relaciones son jerárquicas y establecen una clasificación de los términos que permite aplicar el mecanismo de la herencia, por el que las subclases asumen los atributos definidos para la clase en que se engloban. Tanto los frames como las redes semánticas pueden considerarse como una alternativa a la notación lógica, útiles para expresar de forma compacta contenidos complejos.

Tras la dificultad inicial que plantea la representación del conocimiento, aparece en segundo lugar la de su extensión. Así, los sistemas expertos para conseguir resultados apreciables deben incorporar un gran número de reglas. Por ello, su construcción debe atenerse a principios estrictos a fin de que el sistema permita ser validado, pueda ser actualizado y sea capaz de explicar sus razonamientos. El primero de los requisitos exige que la representación del conocimiento sea en su totalidad declarativa, el segundo que los elementos de la base de conocimiento puedan ser identificados en función de la fuente de la que provienen y, por último, el tercero exige que los elementos de la base estén correctamente definidos y, en particular, que puedan ser entendidos por las personas a las que se dirijan las explicaciones del razonamiento seguido.

Las redes neuronales

En los últimos años han cobrado gran auge en la inteligencia artificial unas nuevas herramientas, las redes neuronales, cuyas características son muy distintas de las del resto de lenguajes informáticos. Es así porque en programación todo el conocimiento debe hacerse explícito al ordenador mediante un análisis humano previo del problema y, por el contrario, las redes neuronales no son programadas sino entrenadas mediante la introducción de casos previamente resueltos de forma tradicional. Con este entrenamiento la red va ajustando sus valores internos, en un auténtico proceso de aprendizaje, de modo que finalmente será capaz de resolver casos similares según los criterios que regían los supuestos de entrenamiento, aunque estos criterios nunca hayan sido explicitados.

Un importante problema que plantea la utilización de redes neuronales en el ámbito jurídico es la imposibilidad de seguir su curso de razonamiento. De hecho, no puede hablarse con propiedad de razonamiento en sentido lógico, ya que lo que sí sabemos, es que la base del funcionamiento de estas redes son complicadas funciones estadísticas, cuya complejidad escapa a nuestra actual capacidad de análisis. En consecuencia, no es posible cumplir con estas redes el deber de justificación, que es propio de las decisiones jurídicas.

Las redes se componen de unos elementos, a los que se llama neuronas, que están interconectados entre sí. Cada una de estas neuronas recibe estímulos, que son un valor numérico, de dos o más vecinas y en función del valor de estas entradas y de sus propios pesos internos, la neurona calcula una señal de salida que a su vez alimenta a otra neurona. El proceso de aprendizaje consiste precisamente en el ajuste de los

pesos internos de cada neurona, de modo que se refuerzan unas conexiones y se debilitan e incluso desaparecen otras.

Desde una óptica informática, las redes neuronales presentan una gran ventaja que es su paralelismo intrínseco. De hecho, existe una gran correspondencia entre el esquema conceptual de las redes neuronales y su plasmación física. Ello significa que los cálculos pueden distribuirse con facilidad entre varios procesadores que trabajan de forma paralela sobre el problema, obteniéndose grandes capacidades de cálculo mediante la simple adición de elementos sencillos.

Por otra parte, las redes neuronales son paradigmáticas de la corriente llamada conexionismo, que defiende que pueden realizarse operaciones lógicas simulando el funcionamiento del cerebro a nivel neuronal. Ante algunas de las afirmaciones que en ocasiones se hacen al respecto es preciso recordar que el cerebro humano no sólo tiene un número muy grande de conexiones, sino que además la complejidad de los mecanismos de conexión es mucho mayor que la de los sistemas artificiales.

Entre las aplicaciones de las redes neuronales se encuentra la recuperación documental; así actualmente se investiga en redes neuronales que aprendan a buscar documentos examinando aquellos que el usuario ha seleccionado previamente. Pero es en el campo de la economía donde estos sistemas han encontrado múltiples aplicaciones como, por ejemplo, la concesión de créditos hipotecarios, la calificación de emisiones de bonos o la predicción de la quiebra financiera. El problema que subyace a las aplicaciones mencionadas es un problema de clasificación, que aparece también frecuentemente en el quehacer de las administraciones.

Las redes neuronales son herramientas particularmente adecuadas para el reconocimiento de patrones, por lo que resultan aptas para labores de vigilancia sobre las comunicaciones, identificando aquellas que se ajusten a determinados patrones considerados “sospechosos”. De hecho, ya son utilizadas por las sociedades de tarjetas de crédito para identificar secuencias de operaciones con tarjeta que se correspondan con los patrones observados en su utilización ilícita.

La actuación administrativa automatizada

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), contempla, en su art. 41, la actuación administrativa automatizada, que define como: “cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público”. Dentro de esta definición podríamos diferenciar dos clases de actuaciones:

- Actuaciones automatizadas de mero trámite o de comunicación de datos: son las que consisten únicamente en comunicar una información que está previamente almacenada en los sistemas de información de la entidad, o aquellas cuyo contenido está unívocamente definido por una norma, como, por ejemplo, la elaboración del acuse de recibo de un documento presentado en el registro electrónico.

- Actuaciones automatizadas que impliquen una clasificación o valoración: su contenido se elabora de forma automatizada utilizando herramientas informáticas que, sobre la base de conocimiento previamente aportado, realizan una tarea de clasificación o valoración, asignando una consecuencia jurídica en función de los datos de partida que les hayan sido aportados.

Para este segundo tipo de actuaciones se utilizan las técnicas de la inteligencia artificial. Son aún muy poco frecuentes, siendo un primer ejemplo en España la utilización de una red neuronal para elaborar las valoraciones de los bienes inmuebles a efectos tributarios.[1] Con la aparición de estos nuevos mecanismos se hace preciso establecer mecanismos de garantía y control, que contrarresten la opacidad de los sistemas informáticos cuando, cada vez en mayor medida, vayan siendo utilizados en la generación de decisiones automatizadas. El mencionado artículo 41 dispone que "En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación". El objetivo debería ser proporcionar información sobre la naturaleza del sistema empleado y la descripción del conocimiento aportado al mismo como base para su funcionamiento, en una medida suficientemente expresiva para la ciudadanía de los fundamentos de su actuación y de la adecuación de los mismos al Derecho.

1.3 Interoperabilidad

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define interoperabilidad como la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada. Esta es precisa en todos y cada uno de los distintos niveles que forman los sistemas de información y que van desde el físico, que maneja las señales eléctricas, hasta el que gestiona la comunicación final con el usuario. También, como veremos, en el proceso de automatización de los procedimientos han de emplearse estándares para definir la forma de generar los documentos y de estructurar su contenido.

El legislador quiere que el desarrollo de la administración electrónica sirva para la modernización, racionalización y mejora de la actuación administrativa y ello exige de la interoperabilidad de los distintos sistemas utilizados. La cuestión presenta en España características especiales, porque actualmente podemos distinguir cuatro niveles administrativos, cada uno con sus propios ámbitos de competencias. Estos son la Unión Europea, el Estado, las comunidades autónomas y la administración municipal, dentro de la cual existen dos niveles, las diputaciones provinciales y los ayuntamientos, y aun, en Cataluña y Aragón, una figura intermedia; las comarcas.

El concepto de interoperabilidad se ha convertido, por tanto, en una de las claves en el desarrollo de la administración electrónica en nuestro país. Esta se plantea tanto a

[1] Puede verse en Gallego J.: La inteligencia artificial aplicada a la valoración de inmuebles. Un ejemplo para valorar Madrid. En: Catastro, abril, pp. 51-67 (2004).

nivel vertical, siguiendo la línea de las administraciones de mayor a menor, como a nivel horizontal, para que, por ejemplo, las aplicaciones utilizadas en las distintas comunidades autónomas sean interoperables.

Al respecto la LRJSP, establece en su artículo 156 que:

> 1. El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.
>
> 2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos contenía un mandato similar, que fue desarrollado por el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI). Además, se creaba un órgano específico con esta finalidad: el Comité Sectorial de Administración Electrónica, dependiente del Ministerio de Hacienda y Función Pública, que es responsable de desarrollo del Esquema Nacional de Interoperabilidad, a través de las denominadas normas técnicas de interoperabilidad (NTI) que establecen la normalización en los diferentes aspectos de los sistemas de administración electrónica. La Ley preveía asimismo el desarrollo de un esquema específico para la seguridad, en el que se establecen las distintas políticas de seguridad a seguir por las Administraciones y los niveles de seguridad mínimos exigibles en cada caso.

También la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (LUTICAJ) dedica a la interoperabilidad el capítulo II del título III, además de numerosas menciones a lo largo de su articulado. En forma equivalente a como lo hace la LRJSP en su artículo 42, ordena el desarrollo de un esquema judicial de interoperabilidad y seguridad.

La interoperabilidad es condición básica para la eficaz utilización de otros mecanismos instrumentales previstos por la LRJSP y que han de servir de base al desarrollo de la administración electrónica. Uno de los principales es la Red de comunicaciones de las Administraciones. Esta red se conoce como Red SARA y está a su vez interconectada con una red paneuropea denominada Red TESTA. Se prevé que a través de la SARA sea posible acceder a múltiples servicios como, por ejemplo, la verificación de los datos de identidad y residencia, y la plataforma de validación de firma electrónica (@Firma).[2]

[2] Al respecto es importante destacar que la LRJSP permite que los documentos intercambiados en entornos cerrados de comunicación sean considerados válidos a efectos de autenticación e identificación de los emisores y receptores, lo que dota de una gran virtualidad a la comunicación a través de estas redes.

Otros mecanismos instrumentales tienen como objetivo optimizar la utilización de los recursos públicos, fomentando la reutilización de aplicaciones. Para ello, se permite que cualquier Administración pública pueda poner a disposición de las demás, sin contraprestación ni convenio, las aplicaciones de cuyos derechos de propiedad intelectual sea titular. Además se ordena la creación de un directorio general de aplicaciones para su reutilización, que es gestionado por el Centro de Transferencia de Tecnología, dependiente del Ministerio de Hacienda y Función Pública. [3]

1.4 El derecho al libre acceso a la información publica

El derecho de acceso de los ciudadanos a la información pública es uno de las cuestiones principales a considerar en la gestión documental de cualquiera de estas Administraciones. Por ello, al diseñar los sistemas de información administrativos no pueden tenerse en cuenta únicamente las necesidades de los propios órganos de la Administración, sino también los requerimientos derivados de este derecho de los ciudadanos.

Cabe distinguir cuatro perspectivas normativas sobre el derecho de acceso a la información:

- El **acceso de los interesados** a los expedientes administrativos y judiciales, es la perspectiva que tradicionalmente ha formado parte de nuestro Ordenamiento. En el procedimiento administrativo se denomina derecho de acceso a archivos y registros. Su regulación básica se contiene en el artículo 53, 1, a) de la LPAC, que establece el derecho del interesado en el procedimiento administrativo "a conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados; … y los actos de trámite dictados. Asimismo, también tendrán derecho a acceder y a obtener copia de los documentos contenidos en los citados procedimientos".
- **El patrimonio documental** cuya norma básica es la Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español, desarrollada por el Real Decreto 111/1986, de 10 de enero, el cual ha sido modificado por el Real Decreto 64/1994, de 21 de enero. Existen además leyes sobre los archivos y el patrimonio histórico-documental en muchas comunidades autónomas. En estas leyes se contempla principalmente el acceso a la información con un interés histórico y académico, aunque no hay que olvidar la importancia que esta clase de acceso sigue teniendo para los derechos fundamentales de los ciudadanos.
- La **transparencia**, que se refiere a los aspectos políticos y aparece cuando nace la convicción de que la transparencia en la actuación de las Administraciones públicas es un bien jurídico de carácter colectivo, lo que lleva a que el 27 de noviembre de 2008 se adopte el Convenio del Consejo de Europa sobre Acceso a Documentos Públicos. La norma aplicable es la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTBG).

[3] Su sitio web es http://administracionelectronica.gob.es

- La **reutilización de la información del sector público** (RISP), que contempla los aspectos económicos y cuyo desarrollo comenzó en 1998 cuando la Comisión Europea elaboró un "libro verde" en el que destacaba la importancia de la información del sector público para el desarrollo económico de la Unión. Más tarde se publicó la Directiva 2003/98/CE, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público, cuya regulación España traspuso mediante la Ley 37/2007, de 16 de noviembre (LRISP). En 2011 se aprobó el Real Decreto 1495/2011, de 24 de octubre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal (RRISP)[4]. La Directiva de 2003 fue modificada por la Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013.[5] En este contexto, se ha popularizado el término "datos abiertos" (*open data*), para referirse a las acciones de las Administraciones públicas dirigidas a la puesta a disposición de sus datos.

Pero, en todos los casos, las normas que permiten el acceso a la información establecen limitaciones que se basan principalmente en dos razones: la seguridad pública o la necesidad de respetar los derechos de personas a las que se refiere la información. Dentro de la primera podemos incluir los preceptos de la Ley 9/1968, de 5 de abril, de secretos oficiales (modificada por la Ley 48/1978), y en la segunda destacan la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD)[6] y la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se trata de una de las cuestiones que más problemas plantea en el día a día a los responsables de la información pública ya que siendo su naturaleza jurídica la de un conflicto de valores (derecho a saber vs. seguridad pública e intimidad y honor), en el cual además la casuística es muy variada, no es posible establecer reglas precisas y queda por tanto un amplio margen para la interpretación.

[4] Hay también una norma específica para la información medioambiental, la Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente, que incorpora las Directivas 2003/4/CE y 2003/35/CE.

[5] Las modificaciones fueron incorporadas a nuestro ordenamiento por la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

[6] El 25 de mayo de 2018 entrará en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento general de protección de datos) que será directamente aplicable en los países miembros. El Ministerio de Justicia ha comenzado las tareas para adaptar el contenido de la LOPD al del Reglamento, si es posible, antes de dicha fecha.

2 Los documentos electrónicos

2.1 Introducción

Hemos visto que la circunstancia más característica del actual momento en la evolución de los sistemas de información en las organizaciones es precisamente la sustitución de los documentos en papel por sus equivalentes electrónicos. Este no es un mero cambio instrumental, sino que afecta de forma profunda a la forma en la que los procedimientos se sustancian y, con ello, a la forma en la que se desenvuelven las organizaciones y la sociedad en los aspectos jurídicamente ordenados.

La adecuada definición de los documentos electrónicos exige atender a diversos criterios: en primer lugar, a su naturaleza, en segundo lugar, al modo en que se plasma su contenido y en tercer lugar a su utilización en los procedimientos. En efecto, es preciso analizar la identidad de los documentos electrónicos porque, aunque en el mundo del soporte papel no hay problema para formar expedientes, integrados por documentos individuales, que podían desgajarse de los mismos y cumplir su función en lugares y casos muy diferentes, dicha virtualidad no surge por sí misma en el caso de los documentos electrónicos, sino muy al contrario, ya que éste no es, a diferencia del documento tradicional, un ente con existencia autónoma, sino un elemento más de un complejo sistema de información.

En segundo lugar, es preciso tener en cuenta que los documentos electrónicos pueden tener un contenido que va más allá de la mera transmisión de información, ya que el objetivo que se persigue es automatizar en la medida de lo posible, las operaciones a realizar con los mismos. Es así porque la administración electrónica forma parte de un proceso general de informatización de las tareas de las burocracias. Si la Revolución Industrial se caracterizó por la sustitución del trabajo manual por el realizado por máquinas, sobre todo en las tareas más repetitivas y pesadas, actualmente asistimos también a un proceso de automatización, pero en esta ocasión referido a tareas que consisten en el manejo e intercambio de información. Para ello se estructura el contenido de los documentos electrónicos, de forma que su potencialidad va mucho más allá de la mera transmisión de información entre personas, dado que que el objetivo que se persigue es automatizar en la medida de lo posible las operaciones a realizar con los mismos.

Otro aspecto a tener en cuenta es que en el desarrollo de los sistemas de administración electrónica los documentos aparecen generalmente vinculados a una entidad más compleja, como son los actos de comunicación. En cada uno de ellos es preciso conservar no sólo el documento o documentos que se comunican, con sus respectivas firma o firmas, sino también un sello de tiempo (*time-stamping*) acreditativo del momento en el que se efectuó la comunicación y las diligencias con el resultado de la verificación, hecha en ese momento, de la vigencia de cada uno de los certificados que respaldan las firmas.[7] Cabe prever que la progresiva automatización de

[7] Los sellos de tiempo son documentos electrónicos, firmados por una autoridad de sellado de tiempo, que vinculan un momento determinado con documento a través del resumen (hash) del mismo. Se incorporan a los acuses de recibo para garantizar el momento en el que se produjo la recepción de un

los procedimientos de lugar al incremento de los actos de comunicación que tendrán lugar directamente entre los sistemas de información. Aunque este hecho, por sí mismo, no tenga por qué suponer un aumento en la complejidad de las operatorias de administración electrónica sí que puede suponer una mayor desagregación de los documentos, que cada vez se parecerán menos a los que hoy los manejamos para la comunicación entre agentes humanos.

2.2 Definición legal de los documentos electrónicos

El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS), contiene en su artículo 3, 35 una definición amplia del documento electrónico.

> todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual;

De forma más concreta, el artículo 26,2 de la LPAC establece los requisitos que deben cumplir los documentos administrativos electrónicos, como: [8]

a) Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.
b) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.
c) Incorporar una referencia temporal del momento en que han sido emitidos.
d) Incorporar los metadatos mínimos exigidos.
e) Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable.

En el ámbito de la Administración de Justicia la LUTICAJ, en su artículo 27, define el documento judicial electrónico como:

1. Tendrán la consideración de documentos judiciales electrónicos las resoluciones y actuaciones que se generen en los sistemas de gestión procesal, así como toda información que tenga acceso de otra forma al expediente, cuando incorporen datos firmados electrónicamente en la forma prevista en la Sección 2.ª del Capítulo II del Título III de la presente Ley.

2. Las Administraciones competentes, en su relación de prestadores de servicios de certificación electrónica, especificarán aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

documento. Por su parte, las diligencias con el resultado de la verificación certifican el resultado obtenido al comprobar que un certificado no ha sido revocado.

[8] Otro tipo de documento electrónico es el documento público electrónico notarial, introducido por la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, que modifica la Ley de 28 de mayo de 1862, del Notariado. Sobre este puede verse: Giner, Javier. *La firma electrónica de notarios y registradores y el documento público electrónico*, Valencia: Tirant lo Blanch, 2007.

3. Tendrá la consideración de documento público el documento electrónico que incluya la fecha electrónica y que incorpore la firma electrónica reconocida del secretario judicial, siempre que actúe en el ámbito de sus competencias, conforme a lo dispuesto en las leyes procesales.

2.3 Los metadatos

2.3.1 Concepto

El prefijo "meta" procede de una palabra griega que significa "junto a, con, después, siguiente", de forma que cabe definir los metadatos, como *datos que tratan de (o se refieren a) otros datos*. Actualmente denominamos metadatos a la información que los bibliotecarios tradicionalmente habían puesto en los catálogos y, en general, a información descriptiva sobre recursos de la Web. Un registro de metadatos consiste en un conjunto de atributos, o elementos, necesario para describir la fuente en cuestión. Dicho de otro modo, los metadatos son información complementaria, independiente del documento, que permite clasificarlo y situar los contenidos del mismo dentro de su contexto facilitando así la localización y la comprensión del documento.

La relación entre un registro de metadatos y el recurso al que describe puede articularse de una de estas dos formas:

- los elementos pueden estar en un registro separado del documento, como en el caso del registro de un catálogo de bibliotecas; o
- los metadatos pueden estar incluidos [*embedded*] en el propio recurso.

Como ejemplos de metadatos aparejados al propio recurso se pueden mencionar, los datos de la Catalogación en Publicación [*Cataloging In Publication* (CIP)] que van impresos en el reverso de la página del título de un libro, o la cabecera TEI [http://www.tei-c.org/] que se coloca al principio de un texto electrónico. Por otra parte, muchos estándares de metadatos utilizados hoy en día, incluido el Dublin Core, no prescriben ningún tipo de relación, y dejan la decisión a cada caso de implementación particular.

2.3.2 Clases

Dentro de los metadatos suelen distinguirse las siguientes categorías:

Metadatos descriptivos

Son los que describen el entorno del documento y aportan la información necesaria para su comprensión. En ellos se utilizan los estándares como Dublin Core y entre la información que contienen podemos encontrar la siguiente:

- identificación: título, identificador, fecha de creación, formato del fichero, tipo de contenido, clasificación, etc.

- localización: indica la pertenencia del fichero a una estructura de expediente, clases, archivos.
- descripción: autor, tipo de contenido, formato, relaciones con otros documentos, etc.
- seguridad: nivel de seguridad aplicable, permisos de accesos, etc.
- preservación: periodos de retención y disposición, componentes del documento previstos para eliminación.
- representación: referencias a los elementos necesarios para visualizar correctamente los contenidos del fichero y las presentaciones en las que se pueden mostrar.
- contenido: detalles, palabras clave, resúmenes, etc.
- índice: define el orden de los diferentes ficheros de contenidos que pueden aglutinarse en un expediente.

Metadatos administrativos

Tienen carácter más técnico y se utilizan para la gestión de los documentos. Contienen información como derechos de propiedad sobre el contenido, permisos de acceso, periodos de conservación, etc. Se corresponden con los denominados "metadatos de gestión de documentos" por el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, para el que son "información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan".

Metadatos estructurales

Se utilizan en los documentos electrónicos y establecen las relaciones internas entre los distintos elementos de los mismos, permitiendo que los usuarios los visualicen como una unidad. Se utilizan estándares como SGML y XML/RDF.

Hay además otros elementos, relacionados con la garantía del origen y de la integridad del documento, como la firma electrónica, que pueden llevar asociados sus propios metadatos.

Finalmente, cuando se trata de documentos electrónicos y estos son utilizados en una organización se utilizan nuevas categorías de metadatos principales que podemos clasificar en los siguientes grupos:

- metadatos del documento electrónico
- metadatos de trazabilidad
- metadatos de las firmas y evidencias
- metadatos del expediente electrónico

2.3.3 Estándares

Existen numerosos modelos y conjuntos de metadatos definidos por diferentes organizaciones, para distintas finalidades. También hay iniciativas, entre las que cabe destacar la iniciativa de archivos abiertos (*Open Archives Initiative OAI*), cuyo web puede verse en www.openarchive.org, y que establecen protocolos y estándares de interrogación universales que permitan acceder con un lenguaje común a la información conservada en todos los archivos que adopten sus estándares. En la siguiente tabla se incluye una relación de otros modelos y conjuntos de que, a nuestro juicio, gozan de mayor aceptación a nivel mundial.

Campo de aplicación	***Conjuntos de metadatos***
Recursos en general	DCMES DCMI metadata terms
Recursos bibliográficos	MODS (Metadata Object Description Schema) MARC21, UNIMARC, MARCXML TEI (Text Encoding Initiative) Headers
Objetos culturales y recursos visuales	CDWA (Categories for the Description of Works of Art) CDWA Lite VRA (Visual Resources Association) Core Categories
Archivos y preservación	EAD (The Encoded Archival Description) OAIS (Reference Model for an Open Archival Information System) PREMIS (Preservation Metadata: Implementation Strategies)
Recursos educativos	IMS LOM (Learning Object Metadata) CanCoreSCORM (Sharable Content Object Reference Model)
Publicación	ONIX (ONline Information Exchange)
Gestión de derechos de autor	copyrightMD DOI (Digital Object Identifier) ODRL (Open Digital Rights Language)
Recursos cientificos	CSDGM (Content Standard for Digital Geospatial Metadata) Darwin Core
Multimedia	MPEG-7 Multimedia Content Description Interface, PBCore, The Public Broadcasting Metadata Dictionary
Agentes	vCardFOF (Friend Of Friend)
Accesibilidad	IMS AccessForllMeta-data

Figura 3.- Estándares y modelos de metadatos

2.3.4 Dublín Core

Dublin Core es un modelo de metadatos elaborado por la DCMI (*Dublin Core Metadata Initiative*) y fue definido como la norma ISO 15836 en 2003. El nombre proviene de la ciudad de Dublín (Ohio, Estados Unidos), donde en 1995 se reunieron los especialistas a nivel mundial en metadatos y Web. Los elementos que componen Dublin core se definen en el documento *Dublin Core Metadata Element Set*. Todos los elementos son opcionales y pueden repetirse. Además, los elementos pueden aparecer en cualquier

orden. Las implementaciones de Dublin Core se realizan generalmente mediante XML y basándose en el *Resource Description Framework* (RDF).

Los elementos se clasifican en tres grupos que indican la clase o el ámbito de la información que se guarda en ellos:

- Elementos relacionados principalmente con el contenido del recurso
- Elementos relacionados principalmente con el recurso cuando es visto como una propiedad intelectual
- Elementos relacionados principalmente con la instanciación del recurso

Contenido	Propiedad Intelectual	Instanciación
Title	Creator	Date
Subject	Publisher	Type
Description	Contributor	Format
Source	Rights	Identifier
Language		
Relation		
Coverage		

Figura 4.- Elementos de Dublin Core

A continuación, se describen brevemente los elementos que forman Dublin Core.

Título (DC.Title)
El nombre dado a un recurso, usualmente por el autor.

Autor o Creador (DC.Creator)
La persona u organización responsable de la creación del contenido intelectual del recurso. Por ejemplo, los autores en el caso de documentos escritos, artistas, fotografos e ilustradores en el caso de recursos visuales.

Palabras clave (DC.Subject)
Los tópicos del recurso. Típicamente expresará las claves o frases que describen el título o el contenido del recurso. Se fomentará el uso de vocabularios controlados y de sistemas de clasificación formales.

Descripción (DC.Description)
Una descripción textual del recurso, tal como un resumen en el caso de un documento o una descripción del contenido en el caso de un documento visual.

Editor (DC.Publisher)
La entidad responsable de hacer que el recurso se encuentre disponible en la red en su formato actual, por ejemplo, la empresa editora, un departamento universitario u otro tipo de organización.

Otros Colaboradores (DC.Contributor)
Una persona u organización que haya tenido una contribución intelectual significativa en la creación del recurso, pero cuyas contribuciones son secundarias en comparación a las de las personas u organizaciones especificadas en el elemento Creator (por ejemplo, editor, ilustrador y traductor).

Fecha (DC.Date)
Una fecha en la que el recurso se puso a disposición del usuario en su forma actual. Esta fecha no ha de confundirse con la que pertenece al elemento Coverage, que sería asociada con el recurso sólo en la medida en que el contenido intelectual está de algún modo relacionado con esa fecha.

Se recomienda la utilización de uno de los formatos definidos en el documento "*Date and Time Formats*", http://www.w3.org/TR/NOTE-datetime basado en la norma ISO 8601 que incluye, entre otras, fechas en el formato AAAA y AAAA-MM-DD.

Tipo del Recurso (DC.Type)
La categoría del recurso, por ejemplo, página personal, romance, poema, minuta, diccionario. Para asegurar la interoperabilidad, Type debería ser seleccionado de entre una lista de valores que se encuentra bajo desarrollo en un grupo de trabajo.

Formato (DC.Format)
El formato de datos de un recurso, usado para identificar el software y posiblemente, el hardware que se necesitaría para mostrar el recurso.

Identificador del Recurso (DC.Identifier)
Secuencia de caracteres usados para identificar unívocamente un recurso. Ejemplos para recursos en línea pueden ser URLs y URNs (cuando estén implementados). Para otros recursos pueden ser usados otros formatos de identificadores, como por ejemplo ISBN (*International Standard Book Number*)

Fuente (DC.Source)
Secuencia de caracteres utilizado para identificar unívocamente un trabajo a partir del cual proviene el recurso actual.

Lengua (DC.Language)
Lengua/s del contenido intelectual del recurso. El contenido de este campo debería coincidir con los de la RFC 1766 (Tags para la identificación de lenguas, http://ds.internic.net/rfc/rfc1766.txt).

Relación (DC.Relation)
Un identificador de un segundo recurso y su relación con el recurso actual. Este elemento permite enlazar los recursos relacionados y las descripciones de los recursos. Por ejemplo:

IsVersionOf	Incluye la edición de un trabajo
IsBasedOn	La traducción de un trabajo
IsPartOf	Un capítulo de un libro
IsFormatOf	Un mecanismo de transformación de un conjunto de datos en una imagen

Cobertura (DC.Coverage)
La cobertura espacial y/o temporal del contenido intelectual del recurso.

La cobertura espacial se refiere a una región física (por ejemplo, sector celestial); uso de coordenadas (por ejemplo, longitud y latitud) o nombres de lugares extraídos de una lista controlada.

La cobertura temporal se refiere al contenido del recurso en vez de a cuando fue creado o puesto accesible ya que este último pertenece al elemento Date. Se usa el mismo formato basado en http://www.w3.org/TR/NOTE-datetime.

Derechos (DC.Rights)
Una referencia (URL, por ejemplo) para una nota sobre derechos de autor, para un servicio de gestión de derechos o para un servicio que dará información sobre términos y condiciones de acceso a un recurso.

2.3.5 La interoperabilidad semántica en el Esquema Nacional de Interoperabilidad

El ENI, dedica a la interoperabilidad semántica su capítulo IV, formado por un único artículo, con el número 10, que dice:

1. Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes, que serán de preferente aplicación para los intercambios de información en las Administraciones públicas, de acuerdo con el procedimiento establecido en disposición adicional primera.

2. Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes, establecerán y publicarán los correspondientes modelos de datos de intercambio que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

3. Los modelos de datos a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y se publicarán, junto con las definiciones y codificaciones asociadas, a través del Centro de Interoperabilidad Semántica de la Administración, según las condiciones de licenciamiento previstas en el artículo 16.

4. Las definiciones y codificaciones empleadas en los modelos de datos a los que se refieren los apartados anteriores tendrán en cuenta lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y el resto de disposiciones que regulan la función estadística.

2.4 El XML (*eXtensible Markup Language*)

Los documentos electrónicos permiten la transmisión de información entre las personas ya que estas pueden leer su contenido, pero la funcionalidad de los mismos va mucho más allá, ya que se diseñan de manera que los ordenadores pueden manejar su contenido y "comprender" partes del mismo. Ello permite realizar búsquedas con mayor facilidad y rapidez, pero además se abre el camino para realizar otras operaciones más complejas con los documentos. La base para todo ello es dotar a los documentos electrónicos de una estructura basada en el etiquetado de su contenido mediante lenguajes desarrollados utilizando XML.

El XML (*eXtensible Markup Language*), definido por el *World Wide Web Consortium* (W3C), es el estándar más empleado para estructurar el contenido de los documentos electrónicos de forma que los programas puedan manejar la información que contienen. Se trata de un metalenguaje que establece las reglas sintácticas que permiten crear dialectos para aplicaciones específicas como, por ejemplo, la contabilidad o los historiales médicos. Estos dialectos son "lenguajes de etiquetas" con los que se da al contenido de los documentos una estructura que permite que algunos aspectos puedan ser interpretados por programas informáticos. Ello permite automatizar algunas de las operaciones a realizar con los documentos, ya que pueden ser creados y modificados por programas informáticos. Los avances en esta línea están estrechamente relacionados con los que se realizan en el ámbito de la inteligencia artificial.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <cotizacion>
    <nombre>Autentia</nombre>
    <mercado>Madrid</mercado>
    <precio>12</precio>
  - <fecha>
      <dia>24</dia>
      <mes>04</mes>
      <anio>2003</anio>
    </fecha>
  </cotizacion>
```

Figura 5.- Ejemplo de texto estructurado con XML

El primer dialecto del XML que ha conseguido aceptación mundial ha sido el XBRL (*extensible Business Reporting Language*), utilizado para el intercambio de información financiera. Otros esquemas XML han sido estandarizados a través de normas ISO como, por ejemplo, la norma ISO 20022, que define el *Universal financial industry message scheme*, o la norma ISO/TS 19139, para información geográfica. Como organismo especializado en el desarrollo de estándares XML puede destacarse la *Organization for the Advancement of Structured Information Standards* (OASIS).

En el ámbito jurídico hay distintos proyectos, como la red LEXML, que comenzó en el año 2000 y agrupa varias iniciativas para la elaboración de diccionarios comunes, y en

Estados Unidos el proyecto LegalXML. Hay también iniciativas en el campo de los tribunales, aunque son más incipientes. Entre estas puede mencionarse como ejemplo el Global Justice XML Data Model (Global JXDM), del Departamento de Justicia de los Estados Unidos de América.

Entre las iniciativas surgidas dentro de la administración electrónica española se encuentra el portal de la Administración General del Estado (AGE), 060.es, que tiene un sistema de gestión documental basado en XML, ximDEX. Por su parte, el Ministerio de Hacienda ha desarrollado dos esquemas XML, PENLOC para el presupuesto de las administraciones locales y PENLOC para la liquidación de cuentas, que permite que las entidades locales le remitan esta información al propio Ministerio, la Tribunal de Cuentas y a otras Administraciones competentes. Dentro de las comunidades autónomas, el País Vasco, Cataluña y Andalucía desarrollan para sus sedes proyectos de web semántica basados en XML.

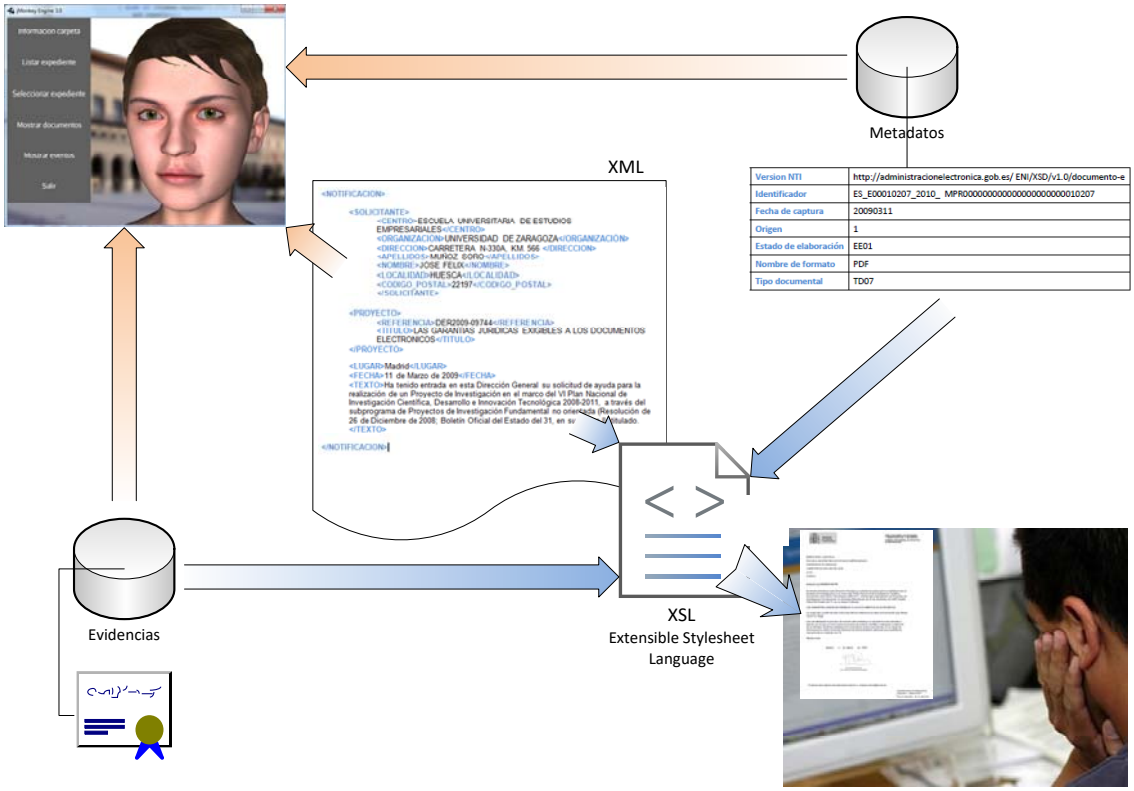

Figura 6.- Estructura de los documentos electrónicos

2.5 La web semántica

La Web Semántica, idea formulada por Tim Berners-Lee en 1998 y 2001, es hoy una iniciativa liderada por el W3C cuyos dos objetivos principales son la estandarización y la automatización. En efecto, la Web Semántica persigue, por una parte, crear una estructura de datos global y compartida entre todos los sitios web que forman Internet y, por otra, hacerlo de forma que esta estructura pueda ser tratada por agentes automáticos, además de por usuarios humanos. Para ello se vinculan, etiquetándolos,

los contenidos de la web con categorías definidas en ontologías, tarea que se realiza mediante el ciclo modelado/publicación-etiquetado/consulta. El modelado consiste en definir las categorías y determinadas relaciones entre las mismas para un ámbito de conocimiento dado. Una vez desarrollado nuestro modelo procederemos a etiquetar los contenidos del web con las categorías definidas en el mismo y publicaremos el resultado, lo que permitirá a los usuarios (humanos o automatizados) realizar consultas semánticas sobre nuestro web.

Podemos agrupar los estándares especialmente relevantes para la gestión de documentos electrónicos en seis niveles o capas:

1. el formato de codificación de bajo nivel de los documentos,
2. las direcciones permanentes que permiten localizar un documento en Internet de forma estable y duradera,
3. lenguajes basados en XML, que facilitan la descripción, la estructuración lógica y el formateo de los documentos, y proporciona herramientas para la extracción de datos y la generación automática de nuevos documentos a partir de datos existentes,
4. el lenguaje RDF, que permite formular relaciones entre los elementos codificados en los documentos dentro del espacio global de Internet, y, que por tanto, permite soportar operaciones sobre los conjuntos de datos que contienen los documentos y los mismos documentos, como, por ejemplo, la recuperación de información a través de la definición de conjuntos de metadatos,
5. los estándares de descripción de ontologías, cuyo objetivo es ligar los metadatos con descripciones sistemáticas de los dominios para permitir la inferencia, esto es, la comprobación sistemática de modelos y la ejecución de razonamientos automáticos, y
6. los medios de autentificación de los documentos, las personas, las instituciones y los procesos.

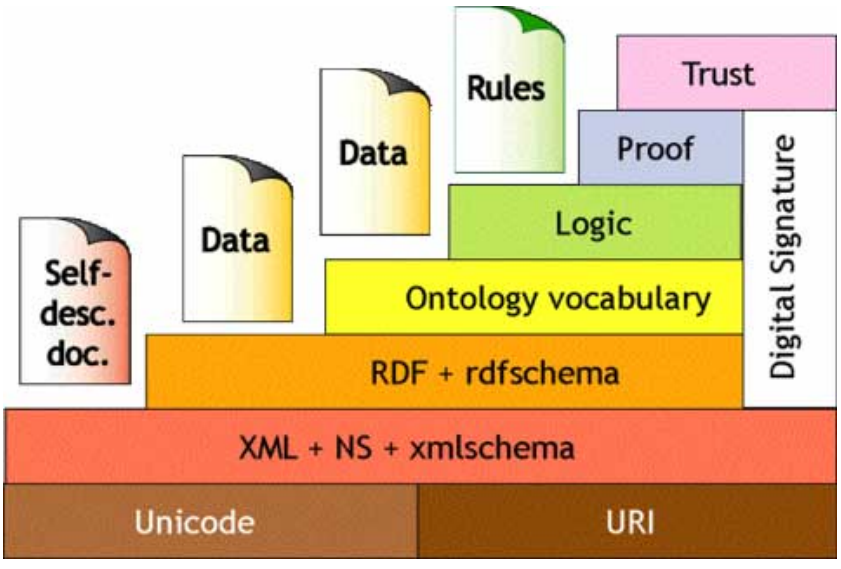

Figura 7.- Diseño de la Web Semántica según Tim Berners-Lee y colaboradores (2001)

Dentro de los niveles anteriores, hay distintos estándares definidos por el W3C para la Web Semántica y la utilización de uno u otro dependerá del nivel de expresividad lógica que queramos alcanzar en nuestro modelo. En el nivel 3, el XML, al que ya nos hemos referido, es la herramienta básica. En el nivel 4, la base es el estándar *Resource Description Framework* (RDF), lenguaje que permite construir grafos basándose en el uso de tripletas. Tiene como unidad básica el recurso, que es cualquier cosa que puede ser identificada por una URI, y permite establecer relaciones entre recursos mediante las tripletas. Dichas tripletas responden al formato sujeto-propiedad-objeto, de manera que el recurso sujeto queda relacionado con el recurso objeto a través de la propiedad especificada. Una extensión de este estándar, denominada *RDF Schema* (RDF-S) añade funcionalidades que permiten, básicamente, definir clases (taxonomías) y establecer relaciones is_a, de pertenencia a las mismas y entre las mismas (relaciones de jerarquía).

El nivel 5 son los estándares de descripción de ontologías, que aportan el vocabulario para la descripción de los documentos, de su contenido y de los procedimientos. Ello exige una identificación precisa de los términos que, a su vez, precisa de la utilización subyacente de un vocabulario estructurado para la recuperación de la información (ISO/DIS 25964-1, ISO/DIS 25964-2). De esta forma, es posible reducir sinónimos y ambigüedades, así como precisar y ampliar conceptos, o preguntar por conceptos relacionados y ofrecer información sobre ellos. Para asegurar la interoperabilidad con otros sistemas internos del organismo y, sobre todo, con otras administraciones, resulta fundamental expresar la arquitectura temática de la información con estándares semánticos, fundamentalmente RDF y OWL. El *Ontology Web Language* (OWL) “añade más vocabulario para describir propiedades y clases: entre otros, relaciones entre clases (por ejemplo, desunión), cardinalidad (por ejemplo, "uno exacto"), igualdad, más tipos de propiedades, características de propiedades (por ejemplo, simetría), y clases enumeradas” (W3C 2004). Por otro lado, OWL ahora ya está en su versión 2.0 y dispone de tres perfiles EL, QL y RL. Estos perfiles se definen según la tarea para la que se quiera usar la ontología. Las versiones reducidas OWL Lite y DL pueden ser vistos como otros perfiles adicionales de OWL2.

Por su parte, el *Simple Knowledge Organization System* (SKOS) no es una herramienta para ontologías propiamente dichas, sin para organizaciones de conocimiento. La principal diferencia es sutil: mientras que en OWL se modela el mundo mediante conceptos per sé, en SKOS se modelan temas, inclusiones por significado (*broaderThan, narrowerThan*). Es decir, para organizar unos documentos, en OWL tendríamos un concepto Documento con su propiedad vaSobreTema, mientras que podríamos usar SKOS para decir Biología que es broaderThan FisiologíaAnimal, FisiologíaHumana. SKOS por tanto no está pensado para modelar el mundo, sino para ser traducción directa de sistemas de categorización. Por último, como herramienta para el acceso a la información estructurada semánticamente ha de destacarse el *Protocol and RDF Query Language* (SPARQL), un lenguaje de consulta cuyo modelo de datos son grafos y en el que las respuestas se forman por reconocimiento de patrones (*pattern matching*).

La elaboración de modelos es una tarea que precisa de importantes recursos por lo que la reutilización se convierte en algo imprescindible. Actualmente hay diferentes entidades e iniciativas cuyo objetivo es crear modelos que puedan ser utilizados ampliamente. Algunas tienen propósito general, como es el caso de la antes mencionada *Organization for the Advancement of Structured Information Standards* (www.oasis-open.org), de EuroVoc, tesauro multilingüe de la Unión Europea (eurovoc.europa.eu) y de wiki.dbpedia.org, cuyo objetivo es extraer información estructurada del contenido de la Wikipedia. Otras iniciativas se centran preferentemente en un ámbito; el del comercio electrónico en el caso de schema.org, cuyos sponsors son Google, Yahoo y Microsoft; o el de la administración electrónica, en el caso de www.oegov.org o del *Semantic Interoperability Centre Europe* (semic.eu), auspiciado por el organismo de estandarización de la Comisión Europea, *Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens* (IDABC).

Los ejemplos de uso de la web semántica por las Administraciones son aun escasos, pero cabe mencionar al Ayuntamiento de Zaragoza, que publica su perfil del contratante utilizando la ontología PPROC (http://pproc.unizar.es/def/sector-publico/pproc.html) desarrollada en un proyecto conjunto con la empresa iASoft, la Agencia Aragonesa para la Investigación y el Desarrollo (ARAID) y la Universidad de Zaragoza.

3 La autenticación de los documentos

3.1 La firma electrónica

3.1.1 ¿Cómo funciona?

Para que los documentos electrónicos puedan sustituir a sus homólogos en papel en las funciones relacionadas con la prueba documental es preciso garantizar que cumplen con dos requerimientos básicos: la autenticidad de origen y la garantía de integridad. El primero significa que debemos ser capaces de conocer con seguridad cual o cuales son la persona o personas que crearon un determinado documento. El segundo consiste en que, una vez creado el documento, su contenido no pueda ser modificado sin que lo detectemos. Nos referimos con el término autentificación al método que permite a los documentos electrónicos satisfacer estos dos requisitos.[9]

La firma electrónica es el mecanismo técnico/jurídico que utilizamos para autenticar los documentos. Desde el punto de vista técnico, el problema consiste en que, a diferencia de los documentos en papel, que son objetos del mundo físico y por tanto únicos, los documentos electrónicos se materializan mediante codificaciones informáticas que no son sino larguísimos números, representados en una base binaria, formada por ceros y unos. Por tanto, la existencia de los documentos electrónicos es abstracta y carecen de identidad única. ¿Cómo es posible, entonces, conocer con exactitud cuál es el origen de un documento?

El problema se resuelve mediante la denominada criptografía moderna en la que se utiliza una pareja de claves, tales que lo que se cifra con una de ellas solo puede descifrarse con la otra. En su uso práctico, hay una que denominamos “clave privada”, ya que solo debe poseerla el firmante, y otra que denominamos “clave pública”, porque se da a conocer de forma pública. Por ello la criptografía moderna se denomina también de "claves asimétricas" o "criptografía de clave pública". Su origen teórico es un célebre artículo de W. Diffie y M. E. Hellman. En 1978, R. Rivest, A. Shamir y L. Adleman desarrollaron los algoritmos RSA en los que se basa la utilización práctica de este método criptográfico.

Para garantizar la autenticidad de origen del documento el emisor añade al documento una firma cifrada con su clave privada y el destinatario utiliza la clave pública del emisor para comprobarla. En consecuencia, decimos que la clave privada es el "mecanismo de creación firma" y la clave pública el "mecanismo de reconocimiento de firma". El elemento que el firmante cifra con su clave privada para crear una firma electrónica no es el mismo documento, sino que utilizamos unas funciones

[9] Debe distinguirse la identificación, que se refiere a las personas y procesos, de la autentificación, que se refiere a los documentos. El término autenticación sería en principio sinónimo de autentificación, pero se crea cierta confusión porque en contextos técnicos suele utilizarse para referirse a la identificación. Por su parte el Reglamento eIDAS le asigna ambos significados (identificación y autentificación) ya que lo define como “un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico”.

denominadas hash, que permiten obtener de un fichero de cualquier longitud —el documento— un número de longitud fija, que es un resumen único del documento. Este resumen, o hash, tiene la propiedad de que su valor varía ante la más mínima modificación del conjunto de datos inicial, propiedad que permite garantizar la integridad del documento. Existe, por tanto, una relación totalmente univoca entre cada documento y su resumen. Por tanto, una firma electrónica puede definirse como el resumen de un documento, cifrado con la clave privada del firmante.

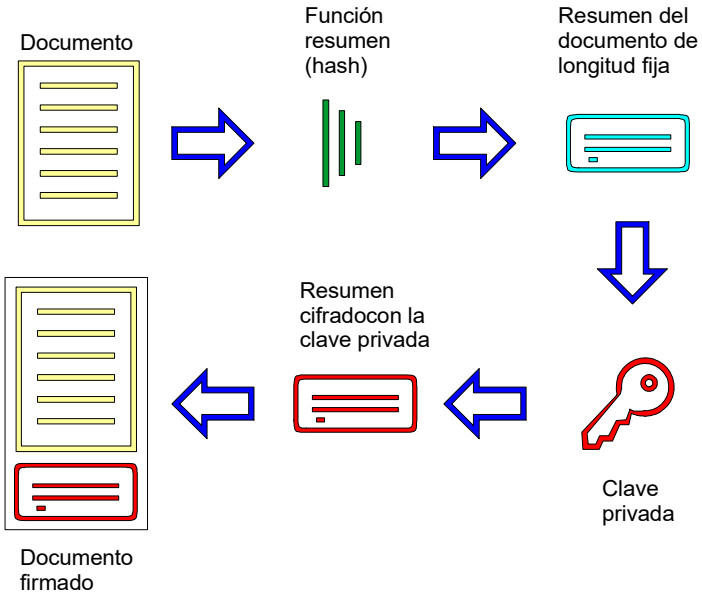

Figura 8.-Firma de un documento

Para comprobar la firma se realizan dos operaciones. Por una parte, se calcula de nuevo el resumen del documento con la misma función que se empleó al firmarlo, por otra se descifra la firma utilizando la clave pública del firmante, de forma que extraemos el resumen contenido en la firma. Esta última será correcta si el valor de ambos resúmenes coincide, ya que así sabremos con seguridad que el resumen de la firma fue cifrado con la clave privada del firmante, así como que el documento no ha sido modificado.

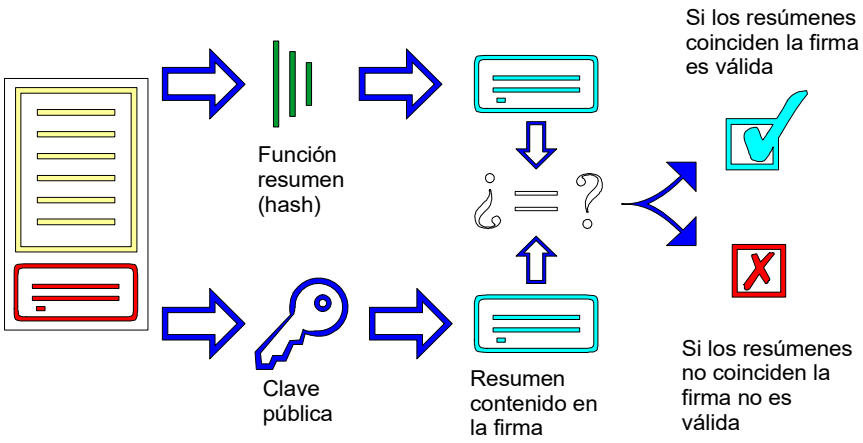

Figura 9.- Comprobación de la firma

La firma electrónica tal como la hemos explicado hasta ahora se denomina firma avanzada. Pero esta modalidad no es la única que existe, ya que el Reglamento eIDAS define la firma electrónica como “los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar”. Dentro de esta definición se engloban otros medios de firma, que podemos denominar como firma no avanzada, y se corresponden con las contraseñas y mecanismos equivalentes. Por ejemplo, en una banca electrónica la primera clave que se nos pide es una clave de identificación, pero luego cuando realizamos una operación, como puede ser ordenar una transferencia se nos solicita una segunda clave y esta es una firma electrónica no avanzada. En la práctica se utilizan, por ejemplo, claves de ocho posiciones de las que se solicitan 4 cada vez o tarjetas de coordenadas.

En estos medios de firma no avanzada se basan la práctica totalidad de los sistemas de banca y comercio electrónico existentes en la actualidad y la experiencia ha demostrado que ofrecen un nivel de seguridad suficiente para estas aplicaciones. La gran ventaja que presenta es su bajo coste y su facilidad de implementación y uso. Sin embargo, tienen dos inconvenientes muy graves: el primero es que los datos de creación de la firma nos lo da la otra parte (por ejemplo, el banco) y que, por tanto, es inevitable que los conozca; el segundo es que la firma no está vinculada de forma indisociable con los datos firmados, sino que solo existe lo que la Ley denomina "una asociación funcional". Esto quiere decir que son los programas los que se encargan de vincular el momento en el que introducimos la clave de firma con la operación que estamos autorizando y que no queda luego constancia permanente de que fue lo que firmamos. Como puede comprenderse en estas condiciones la firma no avanzada solo puede utilizarse en contextos donde la confianza en la otra parte sea muy elevada. Por el contrario, como hemos visto, la firma electrónica avanzada es única para cada documento y está relacionada con este de forma totalmente univoca.

3.1.2 Los certificados electrónicos

La clave pública es, como hemos visto, el mecanismo de comprobación de las firmas electrónicas. Pero, ¿cómo podemos saber con seguridad que una clave pública pertenece a una persona dada? En grupos pequeños puede ser suficiente con que las personas intercambien sus claves públicas de forma presencial, pero cuando el ámbito es mayor se hace preciso el concurso de unas nuevas entidades suelen denominarse “autoridades de certificación”,[10] aunque el término que emplea el Reglamento eIDAS es el de Prestadores de Servicios de Confianza (PSC).

Estos servicios emiten certificados electrónicos, que no son sino unos documentos electrónicos, firmados por la entidad de certificación, en los que se vincula a una persona con una clave pública. De esta forma podemos distribuir con seguridad las claves públicas, ya que las recibimos en un pequeño documento en el que se acredita quien es su titular.

[10] Del ingles *Certification Authorities* (CA).

¿Quién certifica a los certificadores?
Para comprobar la autenticidad de un certificado necesitamos conocer la clave pública del servicio de certificación que lo ha emitido. Estas claves se incorporan en los certificados que denominamos "autofirmados" o "certificados raíz". Los fabricantes de sistemas operativos, como Microsoft, incluyen en el sistema los certificados raíz de los servicios de certificación más importantes, lo que permite la comprobación de la validez de los certificados emitidos por los mismos de forma "transparente para el usuario".

Antes de emitir un certificado hay que realizar alguna comprobación sobre la identidad del poseedor de la clave y este debe manifestar de forma fehaciente ser el poseedor de la clave privada y su compromiso en el futuro con las firmas que sean generadas mediante la misma, a fin de que quede vinculado por estas. La seguridad con que se realiza dicho trámite, que se denomina de inscripción o registro, es el principal factor a la hora de distinguir el nivel de confianza de los certificados. El mínimo exigido por el Reglamento eIDAS para los certificados cualificados es la identificación presencial del suscriptor del certificado o la utilización de un medio de identificación en cuyo origen se haya realizado una identificación presencial.

Otro requisito importante que deben cumplir los servicios de certificación es mantener un directorio, accesible por Internet, en el que pueda consultarse que certificados han sido revocados de forma que, para dar por válida una firma se verifica que el certificado no esté revocado. Esta medida permite que en caso de pérdida o compromiso de la clave privada los titulares de los certificados puedan invalidarlos y, con ello, las firmas posteriores al momento de la revocación.

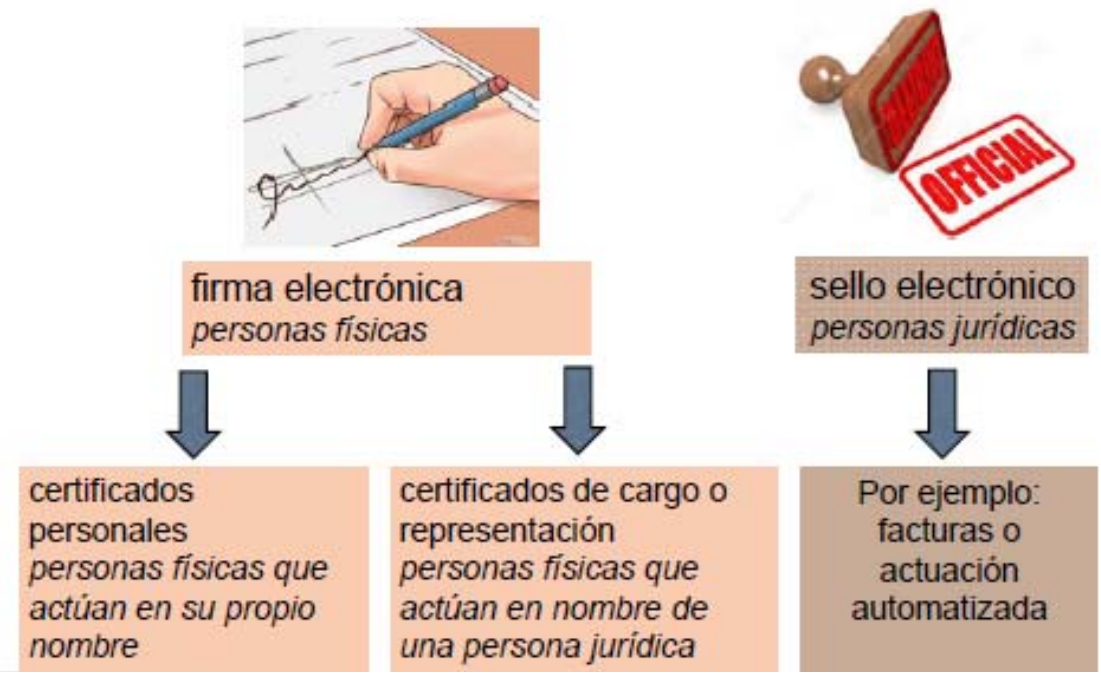

Figura 10.- Clases de certificados

La primera norma española sobre firma electrónica
El derogado Real Decreto Ley 14/1999, de 17 de septiembre, fue la primera norma española sobre firma electrónica. En su artículo 2, establecía que los signatarios únicamente podían ser personas físicas. Y ello pese a que la experiencia de la única administración que en aquellos momentos había desarrollado operatorias de administración electrónica, la AEAT, ya le había llevado a utilizar certificados de persona jurídica, lo que hizo que la misma norma añadiera una excepción al respecto en el sentido de que el Ministro de Economía y Hacienda, podría determinar "respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica".

Los certificados se emiten, en primer lugar, para personas físicas, las cuales disponen gracias a ellos de firma electrónica. Estos certificados se denominan personales cuando se emiten para usos propios del suscriptor y solo contienen información del mismo como, por ejemplo, el DNI electrónico.

Para las personas jurídicas se emiten sellos electrónicos. Desde un punto de vista práctico puede ser útil el criterio de que equivalen al tradicional sello en tinta y de que, por tanto, podrán utilizarse en los mismos casos que este. Desde la óptica de las nuevas formas de proceder asociadas a los sistemas de información, los sellos están asociados a los procesos automatizados, que conllevan la emisión de determinados documentos de forma masiva, sin la intervención directa ni la supervisión individualizada del contenido por una persona física. Son ejemplo de lo anterior la emisión de las facturas electrónicas, en el caso de las empresas, o de los acuses de recibo en los registros de entrada, en el caso de las Administraciones públicas.

Pero las personas jurídicas también actúan a través de sus representantes. Para este supuesto se emiten certificados de cargo o representación, que son certificados de firma, porque su titular es una persona física, pero además acreditan que esta puede actuar en nombre de una persona jurídica. Los certificados de cargo o representación pertenecen a un tipo de certificados denominados "de atributos", que son aquellos en los que, además de la identidad del titular, se hace constar alguna información sobre el mismo como, por ejemplo, su condición de profesional en ejercicio o, en el caso que nos ocupa, el hecho de que ocupa un cargo en una organización o de que es apoderado de la misma. Desde el punto de vista técnico el concepto de certificados de atributos se refiere más bien a certificados vinculados a un certificado principal, que es el que contiene la clave pública, y que permitirían crear alrededor del mismo una estructura —variable— de atributos. Estos certificados serian emitidos por "autoridades de atributos" como, por ejemplo, un colegio profesional que acreditaría la condición de profesional en ejercicio.

El uso de estos certificados es preciso porque de muchas de las actuaciones de las personas jurídicas, tanto públicas como privadas, pueden derivarse responsabilidades de las personas físicas que actúan con agentes de las mismas y, por tanto, en estos actos la firma electrónica deberá aportarnos una doble información: la de la persona física que suscribe el documento y la de su carácter de representante de una determinada organización. De hecho, una posibilidad que planteó en alguna ocasión era utilizar en las Administraciones públicas una doble firma: la de la persona que suscribe el documento y un sello de la entidad que es la firma de la persona jurídica, ya

que, como decía la Exposición de Motivos de la Ley 59/2003, de 19 de diciembre, de firma electrónica, la única incorporación de la firma de persona jurídica, sin que quede constancia de la persona física que incorporó la firma al documento puede dar lugar "a la aparición de obligaciones incontrolables frente a terceros".

3.1.3 La Declaración de prácticas y las Políticas

Una cuestión que añade mucha complejidad al uso de la firma electrónica es que las firmas electrónicas, según el certificado por el que están respaldadas, tienen un valor muy diferente. Así, por ejemplo, hay servicios de certificación que emiten certificados de prueba, sin ningún valor legal, de forma que las firmas electrónicas respaldadas por los mismos carecen de cualquier carácter vinculante. En el otro extremo, las firmas respaldadas por un Certificado Notarial Personal, certificados emitidos por la Autoridad Notarial de Certificación (ANCERT), en los cuales el acto de registro se realiza ante un notario, tienen pleno valor legal, sin limitación en la naturaleza o cuantía del negocio jurídico en el que se utilicen.

Por ello, desde el punto de vista jurídico, otro elemento básico de los servicios de certificación son los documentos en los que se establece, entre otras cuestiones, el valor que podemos otorgar a una firma respaldada por una determinada clase de certificados. El primero de estos documentos es único para cada PSC y se denomina "Declaración de prácticas". Este documento es obligatorio y en él se establece el modo en el que el PSC gestiona las claves y certificados, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, y los mecanismos de información sobre la vigencia de los certificados. En particular, enumera las distintas clases de certificados que emite el PSC con sus características básicas, el procedimiento para la emisión de los certificados de esa clase, su contenido, los usos posibles y el alcance y limitaciones de las firmas respaldadas por los mismos.

Además, es práctica frecuente disponer también de unos documentos más breves, denominados Políticas de certificación, que para cada clase de certificados establecen estos últimos extremos. Tanto la Declaración de prácticas de certificación como las Políticas deben estar disponibles al público de manera fácilmente accesible, al menos por vía electrónica, y de forma gratuita. De acuerdo con los estándares técnicos, los certificados indican en uno de sus campos la dirección de Internet donde pueden verse estos documentos.

El DNI electrónico
El RD 1553/2005, de 23 de diciembre, regula la expedición del DNI y sus certificados de firma electrónica. El art. 11, 4 dice que el DNI contendrá "Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora...". Por motivos de seguridad, se considera conveniente utilizar distintas claves para la identificación y la autenticación y el DNI electrónico, contiene dos claves privadas con sus correspondientes certificados, una para identificación (se utiliza el término autenticación para denominar esta clave) y otra para firma.

El Reglamento eIDAS establece que cualquier entidad pública o privada puede constituirse como organismo emisor de certificados, sin que sea necesaria ninguna autorización previa (Reglamento eIDAS, art. 4). El principio de libre prestación de los servicios de la sociedad de la información que inspira toda la normativa europea sobre la materia y que, en particular, introduce en nuestro ordenamiento el art. 7 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), se traduce en materia de firma electrónica en este principio de libre creación de prestadores de servicios de certificación. Pero en la práctica son pocas las entidades que han constituido servicios de certificación. En nuestro país los principales son la Fábrica Nacional de Moneda y Timbre, la Autoridad Notarial de Certificación (ANCERT), el Servicio de Certificación de los Registradores (SCR) y Camerfirma, constituido por las Cámaras de Comercio, además de alguna empresa.

El Reglamento también crea un mecanismo que permiten alcanzar un nivel "reforzado" de seguridad en los servicios prestados; los certificados cualificados. Los servicios de certificación que expidan estos certificados, así como los propios certificados, deben cumplir un conjunto de requisitos establecidos por el mismo Reglamento. Por imperativo legal, la firma electrónica avanzada basada en un certificado cualificado tiene un valor equivalente al de la firma manuscrita (Reglamento eIDAS, art. 25, 2).

Pero, pese a esta afirmación de la Ley es preciso tener en cuenta que, por su distinta naturaleza, la firma electrónica no es directamente asimilable a la manual, ya que esta última es una acción consciente, con un resultado que es característico de cada individuo. Si en materia de medidas de seguridad se distinguen tres niveles —algo que se sabe, algo que se tiene y algo que se es— podríamos afirmar que la firma manuscrita corresponde a un cuarto nivel, algo que se hace. Además, hay otra diferencia muy importante, y es que la firma manual y las reglas para su utilización están profundamente arraigadas en nuestra cultura. Por el contrario, la firma electrónica se genera mediante un dispositivo y sólo la correcta conservación y utilización del mismo garantiza que tengamos el control de todas las firmas de las que somos titulares. Y esta cultura para la gestión de los mecanismos de creación de firma y, en general, para el uso de la firma electrónica está aún por desarrollarse.

Estándares

Los principales estándares técnicos sobre firma electrónica provienen de la Unión Internacional de Telecomunicaciones (UIT), como el X-509 v.3 que establece el formato de los certificados, por el ETSI (*European Telecommunications Standards Institute*), y por el IETF (*Internet Engineering Task Force*). Este último elabora los estándares de Internet mediante los *Request for Comments* (RFC) que se denominan así porque, una vez aprobados inicialmente se someten a los comentarios de la comunidad científica, hasta que finalmente son aprobados.

Para la publicación de certificados revocados el primer estándar definido se basa en listas que contienen todos los certificados revocados, son las denominadas CRL's (*Certificate Revocation List*). Este método ha sido prácticamente sustituido por un nuevo estándar que permite consultar directamente el estado de un certificado concreto y que se llama OCSP (*On-line Certificate Status Protocol*).

Finalmente, es preciso distinguir el uso de las claves privadas y de los certificados para la identificación de personas y para la autentificación de documentos. En el primer caso únicamente utilizamos la clave para resolver lo que en criptografía se denomina un reto, que permite comprobar que poseemos la clave privada. Podríamos decir que esta forma de operar equivale a que nos entreguen una tarjeta en blanco para firmar en ella y viendo nuestra firma poder comprobar nuestra identidad. Una vez realizada esta operación la "tarjeta" se desecha. Por el contrario, cuando generamos una firma electrónica para autentificar un documento, nuestra intención es que la firma se incorpore al documento, de forma que garantiza el origen y la integridad del mismo. En este caso la firma que generamos tiene ánimo de permanencia y de servir como prueba del compromiso del firmante con el contenido del documento.

3.2 La autenticación de los documentos administrativos electrónicos

3.2.1 Introducción

La firma electrónica es un elemento imprescindible para la realización de trámites utilizando medios electrónicos, ya que las Administraciones públicas deben garantizar la seguridad de sus operatorias y ello exige tanto poder identificar a las personas, físicas o jurídicas, que actúan en un determinado momento, como poder garantizar la autenticidad e integridad de los documentos electrónicos generados por las mismas.

La prestación de servicios de certificación para firma electrónica comenzó en España en el año 1997. Los pioneros fueron la Fábrica Nacional de Moneda y Timbre (FNMT), con el proyecto CERES, y la Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE) formada, entre otros, por los Consejos Generales del Notariado y de la Abogacía, y la Universidad de Zaragoza. La FNMT es el PSC para la Administración General del Estado, según el art. 81 de la Ley 66/1997, de 30 de diciembre, de acompañamiento a los presupuestos para 1998.[11] También presta estos servicios a otras administraciones, como es el caso de la Diputación General de Aragón y las entidades locales de la Comunidad Autónoma, según convenio de 21 de noviembre de 2005. Otras comunidades han creado sus propios servicios de certificación como CatCert, en Cataluña, e Izempe, en el País Vasco.

La experiencia de estos años ha demostrado que la adopción de la firma resulta mucho más lenta y difícil de lo esperado. De hecho, vemos que el comercio electrónico, incluida la banca, ha alcanzado un alto nivel de penetración basándose en la firma electrónica no avanzada, mientras que la administración electrónica pone una barrera que la mayoría de ciudadanos no supera, al exigir la utilización de firma electrónica avanzada. Al comenzar los primeros desarrollos de administración electrónica se consideró que la firma electrónica no avanzada no era suficiente para la realización de trámites administrativos, ya que no quedaba una prueba fehaciente, y que acreditara su momento y contenido, de los trámites realizados. Sin embargo, la lentitud de la introducción de la firma electrónica avanzada se convirtió en una barrera para la evolución del gobierno electrónico.

[11] Desarrollado por el RD 1317/2001, de 30 noviembre.

Un ejemplo de lo anterior es la presentación del Impuesto de la Renta de las Personas Físicas (IRPF) a través de Internet. En las primeras campañas del IRPF en las que se incorporó esta posibilidad, el procedimiento se basaba en que el contribuyente obtuviera un certificado de la FNMT que le permitía presentar su declaración y el número de declaraciones presentadas por Internet era muy bajo, del orden de 20.000. Ante la baja utilización de este canal, la Agencia Tributaria (AEAT) creó una figura, denominada "colaboración social", en base a la cual se emiten unos certificados específicos para despachos profesionales como gestorías, abogados, etc. y para los bancos. Estos certificados permiten presentar la declaración de cualquier contribuyente. A partir de este momento el número de declaraciones presentadas por Internet aumentó hasta llegar a ser de varios millones, pero el sistema sacrificó buena parte de su seguridad, ya que la AEAT no tiene ninguna constancia de que el contribuyente ha autorizado al presentante a que presente su declaración.

La Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos allanó estas dificultades al establecer un marco más flexible para garantizar la autenticidad de origen y la integridad de los documentos. Cabe pensar que la forma en la que la Ley reguló esta obligación era reflejo de su clara visión práctica, derivada de la experiencia anterior en el desarrollo de sistemas de administración electrónica y de las dificultades observadas. En efecto, entre estas dificultades, una de las más destacadas era la exigencia a los sistemas, por parte de las Administraciones usuarias, de niveles de seguridad muy superiores a los existentes previamente y que no resultaban necesarios en muchos de los casos. Frente a esta tendencia, la Ley hizo suyo un principio básico de la seguridad informática: el de proporcionalidad, estableciendo que "sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones", con un límite inferior ya que también dice que se exigirá como mínimo un nivel de seguridad equivalente al de las operatorias no electrónicas. Aunque hoy haya sido derogada, las leyes posteriores han mantenido en lo sustancial esta misma regulación.

La evolución de la entrega de la declaración del IRPF sirve como ejemplo de las ventajas de esta regulación más flexible. Así, desde que se promulgó la mencionada Ley 11/2007, se da a los contribuyentes que han recibido el borrador de la declaración la posibilidad de presentar su declaración simplemente aceptando el borrador con el envío de un SMS con un código alfanumérico que se incluye en el borrador. Una vez recibido este, la AEAT envía otro SMS con un código de verificación que sirve al contribuyente como acuse de recibo. Se trata, de una operatoria ejemplar por su sencillez y por la comodidad que supone para el presentante.

3.2.2 Los medios de identificación y autenticación de los administrados

La LRJSP establece los medios de identificación y autenticación que podrán utilizarse en la administración electrónica, comenzando por los ciudadanos (LPAC art. 9,2). Se establece que los certificados cualificados serán el medio de identificación y autenticación universalmente aceptado por las Administraciones públicas. Cada entidad deberá establecer una "política de firma" en la que detalle los certificados que acepta en sus operatorias de administración electrónica.

También admite la LPAC la utilización de sistemas de firma electrónica no avanzada en términos muy amplios, al referirse a "cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan". Un ejemplo sería el supuesto anteriormente mencionado de presentación de la declaración del IRPF a través del envío de un SMS.

Por último, la LPAC contempla el supuesto de aquellos ciudadanos que carecen de los medios electrónicos de identificación necesarios para una determinada operación. En estos casos habrá funcionarios, expresamente habilitados para ello, que podrán sustituir con sus propios medios de identificación y autenticación al ciudadano. Para ello este último deberá identificarse y dar su consentimiento expreso, del que deberá quedar constancia. Se trata de una disposición de marcado sentido práctico, útil tanto para evitar que quienes no disponen de medios de identificación electrónicos se vean imposibilitados de acceder a algunos servicios como para solucionar problemas concretos que puedan darse en el día a día del funcionamiento de las operatorias de administración electrónica.

3.2.3 La identificación y autenticación de las Administraciones públicas

Los medios de identificación de los que es titular la propia Administración son, de acuerdo con lo visto anteriormente, certificados de persona jurídica. Entre ellos cabe mencionar en primer lugar los certificados utilizados para la identificación de las sedes electrónicas, debiendo las Administraciones “para identificarse y garantizar una comunicación segura con las mismas”, disponer de “certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente” (LRJSP art. 38,6).

Los certificados de servidor
Los "certificados de servidor" tienen una doble función: por una parte, acreditan que un servidor pertenece a una organización o persona y, por otra, garantizan la confidencialidad de la información que se intercambia entre el servidor y el ordenador del usuario (cliente). Su activación se indica al usuario mediante la aparición de la imagen de un candado cerrado de color amarillo en el navegador web. Estos certificados utilizan el protocolo SSL (*Secure Socket Layer*) que permite identificar de forma segura al sitio web y activa el cifrado de confidencialidad entre servidor y cliente durante toda la sesión. Para ello cuando el cliente inicia una conexión con el servidor éste le envía su certificado con la clave pública. A continuación, el cliente envía al servidor una clave de sesión para cifrado simétrico cifrada con la clave pública del servidor. Este último al descifrar la clave de sesión demuestra que posee la clave privada correspondiente al certificado y prueba, por tanto, su identidad. A partir de ese momento la clave de sesión se utiliza para cifrar todos los datos que se intercambien entre ambos ordenadores, con lo que se consigue también la confidencialidad de la comunicación.

Entre los sistemas de firma electrónica para la actuación administrativa automatizada la LRJSP incluye un mecanismo basado en la firma electrónica avanzada, que son los sellos electrónicos, y otro de firma electrónica no avanzada, los códigos de verificación. En cuanto a los sellos cabe hacer una precisión de tipo técnico y es que mientras los

certificados de servidor son únicamente un medio de identificación —ya que su función es garantizar la identidad de un sitio web— los sistemas de firma electrónica para la actuación administrativa automatizada (sellos) se utilizan principalmente como medio de autenticación de documentos, ya que no se emplean para identificar al órgano administrativo, sino para que éste pueda autenticar documentos que genera de forma automatizada, como los acuses de recibo de un registro electrónico o los certificados emitidos en base a información obrante en las bases de datos de la Administración correspondiente, de los que un buen ejemplo es el certificado de vida laboral, que emite la Tesorería General de la Seguridad Social (TGSS). Por otra parte y de acuerdo con lo dispuesto en la LRJSP cada Administración deberá publicar en su sede electrónica la relación de los sellos electrónicos que utilice, con sus características y los prestadores de servicios de certificación que los emiten.

Los códigos de verificación son cadenas alfanuméricas, generadas de forma que puede establecerse su vinculación con el órgano que las emite. Además, la principal garantía que establece la LAE es que, en todo caso se permitirá su cotejo con el original electrónico obrante en el archivo de la Administración pública de que se trate. Este cotejo deberá poder realizarse a través de la sede electrónica. Los códigos seguros de verificación son utilizados desde los principios de la Administración electrónica ya que son un método sencillo de implementar y que no exige ningún esfuerzo ni requisito adicional por parte del ciudadano. Además, cuando el objetivo es generar copias en papel que puedan ser aportadas en cualquier procedimiento son, hoy por hoy, el único procedimiento utilizable. Con el mecanismo de cotejo en la sede se convierten en un medio robusto de autentificación de documentos, sin perder nada de su sencillez.

REFERENCIAS ELECTRÓNICAS

Id. CEA:	Fecha:	Código CEA:	Página:
9F9TWY4945GQ	15/05/2017	32H5V-FI4N6-HZEHD-QKIAK-L57KW-IUFCD	1

Este documento no será válido sin la referencia electrónica. La autenticidad de este documento puede ser comprobada hasta la fecha 11/11/2017 mediante el Código Electrónico de Autenticidad en la Sede Electrónica de la Seguridad Social, a través del Servicio de Verificación de Integridad de Documentos.

Figura 11.- Código seguro de verificación de la vida laboral (TGSS)

3.2.4 La autenticación de documentos por los empleados de las Administraciones públicas

La LRJSP establece, en primer lugar, que el modo común de actuación de las Administraciones públicas cuando actúen por medios electrónicos será a través de la firma electrónica de sus empleados, de forma que los medios vistos en el apartado anterior se utilizarán únicamente en los casos específicos para los que se han previsto. Como dijimos anteriormente es una opción lógica ya que la mayor parte de las decisiones de las organizaciones han de venir respaldadas por una persona física que, en virtud de su función o cargo, pueda responder de las mismas.

El artículo 43,2 de la LRJSP establece que “cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios”. La Ley no obliga a ello, pero parece preferirle la utilización certificados de empleado, que son certificados de

persona física, pero que también identifican a la organización y pueden contener el puesto o cargo que el titular ocupa dentro de la misma.

Hay varias razones para preferir la utilización de certificados específicos, frente a certificados personales como, por ejemplo, el DNI electrónico. Desde el punto de vista de los titulares, los empleados, se manifiesta con frecuencia la reticencia a tener que utilizar en el ejercicio de sus funciones públicas los mismos mecanismos de creación de firma que en sus actividades privadas. Aunque suele objetarse que es lo mismo que ocurre actualmente con la firma manual, lo cierto es que dada la gran diferencia entre la naturaleza de ambas clases de firma la percepción de las personas sobre las mismas es muy distinta y la firma electrónica se considera, con acierto, como un mecanismo técnico que debería proporcionarnos la organización, cuando va a utilizarse en funciones relacionadas con la misma.

Desde el punto de vista de la Administración los certificados de atributos son un medio muy potente para el control de los permisos dentro de sus sistemas de información. Explicándolo de forma sencilla, existen dos paradigmas técnicos para la gestión de los permisos que un empleado tiene dentro del sistema. El primero y más utilizado actualmente consiste en identificar al empleado —normalmente mediante su nombre de usuario y su contraseña— y posteriormente consultar una base de datos donde se contienen los permisos que tiene respecto a una determinada operatoria. El segundo paradigma es la gestión de los permisos a través de certificados, de forma que al identificarse el empleado mediante un certificado ya no sabemos sólo quien es, sino que también sabemos con certeza cuál es su puesto en la organización, tanto a nivel jerárquico como funcional, y en virtud de ello podemos autorizarle a acceder o no a una determinada operatoria del sistema. Esta segunda solución facilita lo que técnicamente se denomina una gestión de permisos "distribuida".

Además, en las grandes organizaciones, los certificados de empleado suelen incorporarse a tarjetas que ya vienen utilizándose para la identificación en accesos físicos a la sede, normalmente para control de horarios, y que en algunos casos ya se utilizan también como medio de identificación para el acceso a los sistemas informáticos, en sustitución del nombre de usuario y la contraseña. En estos casos parece natural la evolución en el sentido de sustituir las tarjetas por tarjetas criptográficas e incorporar en las mismas los certificados de identificación y firma.

Por último, desde el punto de vista del ciudadano, el uso de certificados de empleado público es el que en mayor medida garantiza sus derechos ya que, cuando recibe un documento firmado por una Administración pública, tiene información completa y fehaciente sobre el órgano del que proviene el documento, la personas o personas físicas que lo emitieron y el puesto que estas ocupan en la Administración, en virtud del cual han suscrito el correspondiente documento.

La FNMT ha creado en 2009 una autoridad de certificación destinada a las Administraciones públicas. La nueva autoridad de certificación se denomina CA APE y emite tres clases de certificados: de personal al servicio de las Administraciones públicas o funcionario, de sede electrónica y para la actuación administrativa automatizada (sello electrónico). También emiten certificados para los empleados públicos la Autoridad Notarial de Certificación (ANCERT) bajo la denominación de

"certificados para corporaciones de Derecho público" y el Servicio de Certificación de los Registradores (SCR), bajo la denominación de "certificado de cargo administrativo". Cabe mencionar una carencia en este esquema y es que, al implementar sistemas de firma electrónica por ejemplo en las Administraciones locales, se echan de menos certificados específicos para los cargos electos, como alcaldes y concejales, que se encuentran entre los principales usuarios de la firma electrónica, y que no parece adecuado asimilar a los empleados de la Administración, única opción actualmente existente.

El último mecanismo de identificación y autenticación que contempla la LRJSP tiene también un marcado carácter práctico, al establecerse que los documentos intercambiados en entornos cerrados de comunicación sean considerados válidos a efectos de autenticación e identificación de los emisores y receptores. El término que utiliza la Ley —entornos cerrados de comunicación— se corresponde con lo que habitualmente conocemos como intranet, recurso técnico que cada vez es más utilizado en todas las organizaciones, tanto del sector público como del privado.

4 Los procedimientos

4.1 La optimización de los procedimientos

El legislador de la repetida Ley 11/2007 no quería que la migración de los procedimientos al universo electrónico fuera un mero cambio instrumental, sino que se pretendía aprovechar la ocasión para realizar una profunda reforma de la actuación administrativa. Por ello, la norma exigía un paso previo a la implementación de la tramitación electrónica de los procedimientos, que era una fase de rediseño funcional y simplificación, en la que el conjunto de los procedimientos de una determinada Administración debía ser examinado para reducir el número de trámites, evitar redundancias y suprimir documentos innecesarios. Entre las mejoras que debían conseguirse la Ley también mencionaba la reducción de plazos y la racionalización del trabajo, distribuyendo mejor las cargas entre las diferentes secciones y unidades administrativas. Aunque esta norma haya sido derogada, lo establecido en la misma no debería dejar de ser tenido en cuenta siempre que se automatice un procedimiento administrativo.

En la práctica un reflejo de lo anterior es que los proyectos de implantación de la administración electrónica deberían siempre comenzar con la elaboración de un "catalogo unificado de procedimientos", en el que se sistematizan la totalidad de los trámites de la Administración correspondiente. Esta información se modeliza con metodologías adecuadas, de forma que pueda ser fácilmente implementada en el tramitador (*workflow*) utilizado en la entidad.

4.2 Modelización

La modelización de un procedimiento consiste en la representación del mismo de forma que pueda ser luego traducida a lenguajes específicos para su implementación en herramientas de flujo de trabajo como, por ejemplo, las plataformas de tramitación. Uno de los estándares más utilizados es el BPMN (*Business Process Modeling Notation*). Dicho lenguaje tiene distintas representaciones en XML, como pueden ser el *Business Process Modeling Language* (BPML) o el *XML Process Definition Language* (XPDL), estandarizado por la *Workflow Management Coalition* (WfMC), que permite especificar la parte declarativa de proceso. Existen diversas herramientas para el trabajo con estos estándares, algunas propietarias, como IBM FileNet y Oracle BPM Studio 10g, y otras dentro del software libre. Como ya se ha dicho, la aplicación típica de los modelos en BPMN es la implementación del modelo en una herramienta de flujo de trabajo (*workflow*), a fin de automatizar la tramitación de los procedimientos. Pero, para ello es preciso migrar previamente el modelo a un lenguaje interpretable por la herramienta de flujo de trabajo, como es, por ejemplo, el estándar abierto XPDL (*XML Process Definition Language*). Además de está función del BPML hay otra muy importante, que es la optimización de los procedimientos a partir del modelo de los mismos. Existen herramientas informáticas diseñadas para este fin, que realizan simulaciones y, en base a estas, hacen el análisis, diagnóstico y rediseño de los procedimientos.

Desde hace algunos años se ha realizado algunas aproximaciones a la aplicación del BMPN para la modelización de procedimientos administrativos. En cuanto a las herramientas, en nuestro país pueden destacarse dos, que son software libre. Una es Model@, herramienta desarrollada íntegramente en Java que permite crear gráficamente, gestionar y mantener diagramas de definición de procedimientos, mediante el estándar XPDL. Model@ ha sido desarrollado por la Junta de Andalucía, dentro del proyecto W@nda. Otra, Opencities, está destinada específicamente al ámbito local.

Hay ya diversas experiencias de aplicación del BPM en las Administraciones públicas españolas incluyendo el modelado de los procedimientos mediante XPDL, como, por ejemplo, el sistema GEN (Gestor de Expedientes Normalizado) de la Secretaria General de Energía del Ministerio de Industria, Turismo y Comercio. En cuanto a la optimización y el rediseño, el MAP puso a disposición de las Administraciones públicas la aplicación ARIS, dentro de su acción Herramienta de Rediseño y Simulación (HARPA). Está fue utilizada por el Ministerio de Educación y Ciencia para el rediseño del procedimiento de Homologación de Títulos Extranjeros de Educación Superior a Títulos Universitarios y Grados Académicos Españoles.

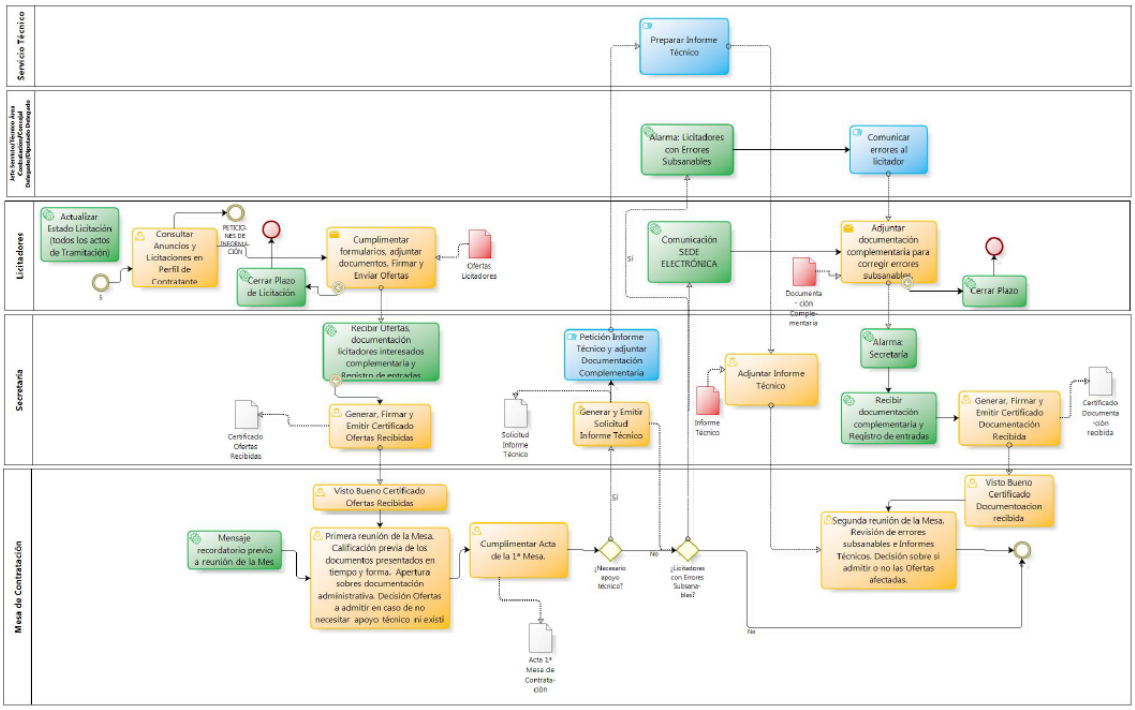

Figura 12.- Diagrama BPMN de una fase de un procedimiento de contratación