

FACULTAD DE EMPRESA Y GESTIÓN PÚBLICA



GRADO EN GESTIÓN Y ADMINISTRACIÓN PÚBLICA

**IMPACTO DE LAS LEYES 39 Y 40/2015 EN LA
ADMINISTRACIÓN ELECTRÓNICA**

**IMPACT OF LAWS 39 AND 40/2015 ON THE SPANISH
E-GOVERNMENT**

Autor

Javier Casado Cadarso

Director

Fernando Mikelarena Peña

2016

“...en todas las oficinas del Estado, provinciales y municipales se admitan cuantas instancias y documentos se presenten hechos con máquinas de escribir, en los mismos términos y con iguales efectos de los escritos o copiados a mano”

— Real Orden de 12 de febrero de 1900, de Francisco Silvela , publicada en la Gaceta de Madrid del 19 de febrero de 1900

“La publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano o Entidad competente tendrá [...] los mismos efectos que los atribuidos a su edición impresa”

— art. 11, Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

SUMARIO

RESUMEN.....	5
SUMMARY.....	5
1. INTRODUCCIÓN.....	6
1.1 BREVE HISTORIA DE LA ADMINISTRACIÓN ELECTRÓNICA EN ESPAÑA.....	7
1.1.1 La Administración Pública en el ordenamiento jurídico español.....	7
1.2 LA ADMINISTRACIÓN ELECTRÓNICA EN LA LEY 30/1992.....	7
1.2.1 RD 263/1996, de 16 de febrero, de utilización de técnicas electrónicas, informáticas y telemáticas por la AGE.....	10
1.3 LEY 59/2003, DE 19 DE DICIEMBRE, DE FIRMA ELECTRÓNICA.....	10
1.4 LEY 11/2007 DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS.....	13
1.4.1 RD 1671/2009, de desarrollo parcial de la Ley 11/2007.....	17
1.5 ESQUEMAS DE INTEROPERABILIDAD Y SEGURIDAD.....	17
1.5.1 RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI).....	18
1.5.2 RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).....	21
1.6 LA COMISIÓN PARA LA REFORMA DE LAS ADMINISTRACIONES PÚBLICAS: EL INFORME CORA.....	23
1.6.1 Recomendaciones del informe CORA en e-administración.....	24
2 LEYES 39 Y 40/2015: ACTUALIZANDO LA ADMINISTRACIÓN ELECTRÓNICA.....	28
2.1 ÁMBITO DE APLICACIÓN.....	28

2.2 LA ADMINISTRACIÓN ELECTRÓNICA EN LA LPAC Y LA LRJSP.....	29
2.2.1 Del derecho de acceso a la obligación electrónica.....	30
2.2.2 Autenticación vs firma.....	31
2.2.3 Funcionarios Habilitados.....	33
2.2.4 Registro electrónico.....	33
2.2.5 Notificación electrónica.....	35
2.2.6 Documentos y Expedientes electrónicos.....	36
2.2.8 Sede electrónica.....	37
2.2.7 Relaciones interadministrativas.....	37
2.3 ENTRADA EN VIGOR.....	38
2.4 EL PAPEL DE LAS COMUNIDADES AUTÓNOMAS.....	38
3 LA ADMINISTRACIÓN ELECTRÓNICA EN ESPAÑA: FUNDAMENTOS TECNOLÓGICOS.....	39
3.1 LA FIRMA ELECTRÓNICA COMO GARANTE DEL DOCUMENTO ELECTRÓNICO.....	39
3.2 TIPOS DE CERTIFICADOS.....	42
3.2 EL DNI ELECTRÓNICO.....	46
3.3 EL DOCUMENTO ELECTRÓNICO.....	47
3.4 EL EXPEDIENTE ELECTRÓNICO.....	48
3.5 EL PORTAL DE ADMINISTRACIÓN ELECTRÓNICA (PAE).....	49
4 OBSTÁCULOS ACTUALES PARA LA IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA.....	53
5 FACILITANDO LA FIRMA: LA LEY 39/2015 Y CL@VE.....	56
6 CONCLUSIONES.....	59
BIBLIOGRAFÍA.....	64
NORMATIVA.....	66
RECURSOS WEB.....	68

RESUMEN

Este trabajo pretende analizar la situación de la administración electrónica en España y el impacto que en su implantación pueden suponer las nuevas Leyes 39 y 40 de 2015. Catorce meses después de su publicación y tras dos meses de su entrada en vigor, las Administraciones Públicas afrontan su cumplimiento con numerosas dificultades y grandes incertidumbres tanto jurídicas como tecnológicas.

Se analiza aquí el papel central que juega la firma electrónica y el importante intento en su simplificación que supone el sistema de claves concertadas [Cl@ve](#). Finalmente, tras identificar los obstáculos principales que se presentan en la adopción de la administración electrónica, se proponen algunas soluciones para superarlos.

“La burocracia destruye la iniciativa. Hay pocas cosas que los burócratas odien más que la innovación, especialmente la innovación que produce mejores resultados que las viejas rutinas. Las mejoras siempre hacen que aquellos que se hallan en la cúspide aparezcan como unos ineptos. ¿A quién le gusta aparecer como inepto?”

— Frank Herbert, *Una "Guía para el método de tanteo en el Gobierno"* de los Archivos Bene Gesserit, Dune (1965)

SUMMARY

This paper aims to analyze the situation of e-administration in Spain and the impact of the new Laws 39 and 40/2015 on its implementation. Fourteen months after its publication and after two months of its entry into force, Public Administrations face their compliance with numerous difficulties and great uncertainties, both legal and technological.

It analyzes the central role played by electronic signature and the important attempt in its simplification brought by the concerted keys system, Cl@ve. Finally, after identifying the main obstacles that arise in the adoption of e-government, some solutions are proposed to overcome them.

1. INTRODUCCIÓN

Las Administraciones Públicas están viviendo una auténtica revolución en nuestros días. El advenimiento de la administración electrónica está obligando a introducir numerosos cambios de gran calado en unas instituciones caracterizadas por su proverbial resistencia al cambio. Unas organizaciones cuyos métodos de trabajo han variado muy poco a lo largo de décadas, se ven ahora impelidas a modificar sus hábitos seculares y a revisar sus procedimientos por completo, ante la llegada de una modernización que está afectando a toda la sociedad y de la que sus administraciones no podían quedar al margen.

“¡Y pensar que algunos se asombran de que hayamos perdido las colonias! Lo que a mí me asombra es cómo no hayamos perdido, con esta burocracia, hasta los pantalones”

— Pío Baroja

El documento administrativo constituye el testimonio de la gestión administrativa y la garantía de los derechos, tanto de los ciudadanos como de la propia administración. De ahí la importancia de su conservación adecuada a efectos tanto probatorios como de testimonio histórico a largo plazo, en aquellos documentos que tengan dicho valor.

Los avances tecnológicos han afectado de lleno al documento administrativo, obligando a una puesta al día de este componente básico de la gestión diaria en las administraciones públicas. Tanto los documentos recibidos como los documentos generados por la propia administración, son en su mayor parte creados utilizando herramientas electrónicas y en ocasiones, nunca llegan a ser emitidos en soporte de papel.

La normativa obliga a las administraciones, ahora ya de forma imperativa, a la tramitación electrónica integral de los expedientes con la finalidad de que el ciudadano pueda presentar sus solicitudes por vía electrónica, así como recabar la información relativa al estado de tramitación de aquéllos asuntos en los que aparezca como interesado en cualquier momento y desde cualquier ubicación, haciendo uso de herramientas tecnológicas cotidianas como pueden ser un teléfono móvil, una tableta o un ordenador.

1.1 BREVE HISTORIA DE LA ADMINISTRACIÓN ELECTRÓNICA EN ESPAÑA

1.1.1 La Administración Pública en el ordenamiento jurídico español

La Administración Pública se considera en nuestro ordenamiento jurídico como un órgano más del Estado. El art. 97 de la Constitución Española de 1978 (CE1978) establece su dependencia directa del Gobierno, quien la dirige. No existe una relación de representación entre la ciudadanía y la Administración, sino que se trata de una estructura administrativa dependiente directamente del poder político.

“La burocracia es un mecanismo gigante operado por pigmeos”

— Honoré de Balzac

En la CE1978, la Administración se encuentra regulada principalmente en el art 103, donde se destaca el carácter de *servicio* que le es propio y su condición de *subordinada* a la Ley y al Derecho. Cabe destacar los principios de funcionamiento que en dicho artículo se enumeran: eficacia, jerarquía, descentralización, desconcentración y coordinación, todos ellos verdaderos impulsores de los avances tecnológicos que han de llevar a la Administración hacia el s. XXI.

1.2 LA ADMINISTRACIÓN ELECTRÓNICA EN LA LEY 30/1992

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP) fue la primera en regular la utilización de medios electrónicos en la tramitación administrativa. No hay que olvidar que cuando se elaboró esta Ley, la presencia social de dispositivos electrónicos era realmente baja; los ordenadores eran habituales en ámbitos empresariales y en grandes administraciones, pero la implantación en los hogares era mínima.

No obstante, la exposición de motivos de la LRJAP tenía a gala el reconocimiento de los procedimientos electrónicos incluidos en su articulado: *“la Ley se abre decididamente a la tecnificación y modernización de la*

actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas” o “Concluye el título IV con una abierta incorporación de las técnicas informáticas y telemáticas en la relación ciudadano-Administración”, son algunas de las afirmaciones que anuncian las novedades electrónicas recogidas en esta norma, las cuales se concentraban en dos artículos: un pequeño párrafo en el art 38.8, sobre registros y en el ya más extenso art. 45.

La referencia correspondiente al art. 38.4, es un párrafo donde se dice *“Mediante convenios de colaboración suscritos entre las Administraciones Públicas, se establecerán sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad informática y la transmisión telemática de los asientos”*. Se refiere a los registros de entrada y salida que las Administraciones deben mantener para registrar las solicitudes, escritos y comunicaciones que van dirigidos a las AA:PP. (registros de entrada) y para enumerar los documentos que la propia Administración remite a interesados o a otros entes administrativos (registros de salida).

La idea subyacente en lo referente a dichos registros, consistía en articular la interconexión entre las oficinas de registro de diferentes Administraciones para intercambiar información entre ellas y permitir la presentación de documentación destinada a una oficina específica en cualquiera de ellas, con la consiguiente facilidad y comodidad para los ciudadanos y usuarios. Era la entonces llamada *Ventanilla Única*. Pues bien, a día de hoy, este sigue siendo uno de los objetivos de la Ley 39/2015, lo cual da una idea clara del escaso éxito cosechado por lo dispuesto en la LRJAP y disposiciones posteriores.

En cuanto al art. 45 sobre la incorporación de medios técnicos, recogía en el apartado 1 que *“las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias [...]”,* una expresión ciertamente genérica en su redacción, pero que daba de esa forma soporte jurídico al incipiente uso que algunas administraciones venían ya haciendo de sistemas informáticos.

En el apartado 2, recogía que “[...] *los ciudadanos podrán relacionarse con ellas [las Administraciones] para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos con respecto de las garantías y requisitos previstos en cada procedimiento [...]*”, si bien esta posible relación quedaba sujeta a la compatibilidad con los medios técnicos disponibles en las Administraciones Públicas.

Por su parte, el apartado 4 exigía una aprobación previa por el órgano competente, sin mayor precisión, para “*los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus postestades*”. Este órgano competente quedaba a su vez obligado a “*difundir públicamente sus características [de los programas y aplicaciones]*”.

Y por último, dedicaba el apartado 5 a los *documentos electrónicos*:

“5. Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras Leyes”.

De una manera muy básica, la Ley 30/1992 permitía deducir que los documentos electrónicos eran simplemente, aquéllos que fueran elaborados utilizando medios electrónicos, concepto que, como iremos viendo más adelante, sobre todo a partir de la publicación del *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)*, contempla hoy en día una complejidad infinitamente mayor.

Ya entonces era fácil prever que una redacción tan genérica y ambiciosa al mismo tiempo, requeriría del correspondiente desarrollo reglamentario que habría de llegar casi cuatro años después a través del *RD 263/1996*.

1.2.1 RD 263/1996, de 16 de febrero, de utilización de técnicas electrónicas, informáticas y telemáticas por la AGE

El RD 263/1992 abordaba precisamente el desarrollo del art. 45 LRJAP, con la pretensión de delimitar las garantías, requisitos y supuestos de utilización de las técnicas electrónicas, informáticas y telemáticas en la AGE.

Pero de nuevo, tras un análisis detallado de su contenido, se puede afirmar que el RD no hacía sino abundar en las generalidades de las que ya pecaba el art 45 y no concretar ninguna de las materias que pretendía regular: soportes, medios, aplicaciones electrónicas, aspectos de seguridad, documentos electrónicos, garantías de seguridad (tanto técnica como jurídica), etc...

En realidad, y con la perspectiva que ofrece el tiempo transcurrido y la evolución que ha sufrido la materia a lo largo de este periodo, podría decirse que el Real Decreto proporcionaba a las Administraciones el marco reglamentario necesario para la introducción de las nuevas tecnologías en sus procedimientos de trabajo, pero sin señalar una dirección común para su desarrollo y posterior coordinación, sino dejando abiertas las posibilidades para que cada organismo decidiera como avanzar en su implantación. Se propiciaba así la aparición de “*islas tecnológicas*” en algunas organizaciones, mientras que en otras, no se producía avance alguno en esta materia.

1.3 LEY 59/2003, DE 19 DE DICIEMBRE, DE FIRMA ELECTRÓNICA

Se inició un periodo en el que pueden encontrarse aquí y allá referencias a la tramitación telemática en difentes normas de diverso rango, entre las que pueden enumerarse, sin ánimo de ser exhaustivos, las siguientes disposiciones:

- *Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado.*
- *Orden de 24 de abril de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre la Renta de las Personas Física*

- *Resolución de 3 de mayo de 2000, de la Agencia Estatal de Administración Tributaria, sobre expedición por medios telemáticos de certificaciones de estar al corriente en el cumplimiento de obligaciones tributarias u otras circunstancias de carácter tributario*
- *Resolución de 11 de abril de 2001, de la Agencia Estatal de Administración Tributaria, sobre asistencia a los contribuyentes y ciudadanos en su identificación telemática ante las entidades colaboradoras con ocasión de la tramitación de procedimientos tributarios*
- *Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos*
- *Resolución de 26 de mayo de 2003, de la Secretaría de Estado para la Administración Pública por el que se aprueban los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades*

Fue la regulación europea, a través de la Directiva 1999/93/CE, de 13 de diciembre de 1999, la que vino a establecer un marco comunitario común para la regulación de la firma electrónica basada en los servicios de certificación. Como toda Directiva, habría de transponerse al marco jurídico de cada uno de los estados miembros. Su objetivo principal era garantizar la interoperatividad de las transacciones comerciales que utilizaban la firma electrónica y definía los mecanismos de cooperación necesarios para facilitar el reconocimiento transfronterizo de las firmas, los certificados y las autoridades de certificación.

En tanto se produce la transposición de la Directiva a nuestro ordenamiento jurídico, se publican algunas otras disposiciones de gran trascendencia para la consecución de un marco de seguridad jurídica y garantía de derechos en el ámbito electrónico, como son:

- *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de*

Carácter Personal: regula tratamiento automatizado de los datos de carácter personal y los ficheros en los que se recoge dicha información. Es, a su vez, resultado de la transposición de la *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación*.

- *Directiva sobre el comercio electrónico*, que elimina las restricciones en el uso de contratos electrónicos y viene a complementar el marco establecido por la *Directiva 1999/93/CE*. Su denominación completa es *Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior*.
- *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, consecuencia de la *Directiva 2000/31/CE*. Esta Ley pretende eliminar las incertidumbres jurídicas derivadas del uso de los medios electrónicos en las relaciones comerciales.

Finalmente, la transposición de la *Directiva 1999/93/CE* tomó cuerpo en España en la *Ley 59/2003, de 19 de diciembre, de Firma Electrónica (LFE)*.

El principal avance de la LFE es el de conceder a la *firma electrónica reconocida* el mismo valor respecto de los datos consignados en forma electrónica, que a la firma manuscrita en relación con los consignados en papel (art. 3.4 LFE). Esta equiparación de garantías entre la firma electrónica y la firma manuscrita supone de hecho, la equivalencia en el sentido de validez y fehcencia, entre un documento firmado electrónicamente y un documento firmado en papel.

“La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel”

— art. 3.4, Ley 53/2003, de 19 de diciembre, de firma electrónica

La LFE vino a sentar las bases de los futuros documento y expediente

electrónicos, estructuras que suelen contener una o varias firmas electrónicas que les aportan las garantías de integridad e inalterabilidad del contenido y de identificación del (los) firmante(s). Posteriormente, esta LFE ha sido modificada en su artículo 3 por la propia LPAC.

En marzo de 2006 y aunque no se trata de una disposición normativa en sí misma, cabe destacar el comienzo de la implantación del DNI electrónico, un elemento cuyo propósito era extender y facilitar el uso de la firma electrónica entre toda la población, con una importante inversión económica en el desarrollo de la infraestructura tecnológica necesaria. Más adelante analizaremos en detalle el escaso resultado obtenido en cuanto a su uso en la relación electrónica administrativa y las causas para ello.

1.4 LEY 11/2007 DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS

La *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos* (LAESCP) fue la primera norma española centrada principalmente en la regulación de la administración electrónica. Ha estado vigente hasta su reciente derogación por la nueva *Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas* (LPAC) y su principal aportación fue sin duda, el reconocimiento del derecho de los ciudadanos a relacionarse electrónicamente con la Administración (art. 6). Esta relación electrónica abarcaba los derechos previstos en el artículo 45 de la LRJAP, que eran los vigentes en ese momento en la relación Administración - ciudadano y añadía también “*obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos*” (art. 6.1). Visto desde el lado de las Administraciones Públicas, este derecho se convierte en el deber de proveer los medios necesarios para garantizar el libre ejercicio de dicho derecho en el entorno de seguridad y garantías que la tramitación administrativa exige. El reconocimiento del ciudadano como portador de derechos a satisfacer de

forma efectiva por la Administración, supone la imposición del compromiso jurídico de incorporar las tecnologías de la información a la totalidad de las funciones administrativas.

Merecen ser destacados además, el reconocimiento de otros derechos propios de la naturaleza electrónica de la relación, como son la elección del canal de comunicación (servicios a través de internet, plataformas móviles u otros disponibles en cada momento), la obtención de copias electrónicas, la obligación de facilitar medios de identificación electrónica (certificados de identificación y firma) y otros que parecen inicialmente de menor calado, pero que suponen un gran reto en su provisión, como son:

- El derecho a conocer en cada momento, por medios electrónicos, el estado de tramitación de aquellos expedientes en los que una persona obre como interesado: en la práctica, esta disponibilidad supone la obligación de efectuar la tramitación electrónica de los expedientes y su conexión con las plataformas de acceso.
- A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información. Esta obligación requiere de la interconexión entre todas las Administraciones de cara a poder proporcionar cualesquiera de los documentos necesarios.
- A la conservación en formato electrónico, de los documentos que formen parte de un expediente.

Si los documentos pueden ser electrónicos y su tramitación debería ser electrónica, lo natural es que su conservación también lo sea, es decir, el archivo administrativo deberá ser electrónico. Este extremo ha abierto el debate en torno a numerosas cuestiones de carácter técnico, como es el caso de los formatos de documentos de larga duración, los procesos de refirma y resellado de documentos que permitan garantizar su validez más allá del periodo de vigencia de los certificados electrónicos involucrados en su tramitación y firma y otras muchas.

La Ley plantea en su artículo 10 la necesidad de definir claramente el lugar electrónico en el que cada una de las Administraciones prestará sus servicios electrónicos, cuestión que resuelve definiendo el concepto de *sede electrónica*, que será de creación obligatoria para todas las Administraciones Públicas. Será en este espacio donde se establecerán las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad. Aunque la LAECSP no lo especificaba, se ha venido entendiendo esta sede como un espacio web convenientemente identificado y cifrado mediante navegación segura, basada en un certificado de servidor expedido expresamente para este fin. Actualmente, la LRJAP. ya concreta este extremo. La sede electrónica ofrece así, la misma garantía jurídica que una oficina física de la entidad.

La Ley define también en el anexo, algunos términos y conceptos que son de utilización habitual en su articulado; así sucede con la definición del expediente y documento electrónico, los registros electrónicos, las notificaciones electrónicas o el alcance y sistemas de sellado de tiempo.

Como no podría ser de otra manera, la LAECSP hace una mención especial a los sistemas de firma electrónica y prestadores de servicios de certificación reconocidos para ser utilizados en el ámbito de la administración electrónica. Dedicada a ello el art. 13 y ss, sobre formas de identificación y autenticación, siendo la *identificación* el método para conocer la identidad electrónica, tanto del ciudadano como de la propia Administración y la *autenticación* el mecanismo técnico que garantiza la integridad de un documento electrónico o de una comunicación electrónica. Ambos mecanismos están implícitos y se proporcionan mediante los sistemas de firma electrónica reconocida.

Añade además otros sistemas de firma electrónica adicionales a los ya recogidos en la LFE, como son:

- Sello de órgano: certificado electrónico utilizado para autenticar documentos y procedimientos en procesos automatizados. Equivale al sello identificativo de la entidad estampado en un documento en papel.
- Código seguro de verificación: permite la comprobación de la integridad

del documento mediante el acceso a la sede electrónica correspondiente, donde podrá consultarse el documento electrónico original y verificar la firma o firmas electrónicas que pudiera contener.

Otra novedad introducida por la LAECSP es la figura del *funcionario habilitado* para actuar en representación de los ciudadanos en la tramitación electrónica, cuando aquéllos no dispongan de identificación electrónica. Esta representación podrá ser válidamente realizada por funcionarios públicos mediante el uso del sistema de firma electrónica del que estén dotados.

Por último, debemos mencionar que la Ley obliga a las Administraciones a disponer del servicio de *registro electrónico* (por entonces también denominado *telemático*), donde los ciudadanos podrán presentar solicitudes y documentos ante la entidad titular del servicio con plenas garantías y regula el procedimiento de *notificación electrónica*, para el que exige que el interesado que vaya a ser notificado por la Administración, haya manifestado previamente su deseo de ser notificado por ese medio. Esta autorización podrá ser revocada en cualquier momento y eso obligaría a la Administración a volver a practicarle las notificaciones en papel.

Como queda reflejado en esta somera revisión del contenido de esta norma, la lista de novedades electrónicas que introduce en el mundo administrativo es ciertamente extensa y muchas de ellas, de una índole tan técnica que requieren ser definidas de forma exhaustiva. De esta forma, el art. 42 dispone la futura elaboración de dos normas, que serán publicadas en enero de 2010: el Esquema Nacional de Interoperabilidad (ENI) y el Esquema Nacional de Seguridad (ENS), los cuales más adelante revisaremos.

Finalmente, en lo concerniente a la entrada en vigor de los nuevos derechos que la ley reconoce y que obligan a las diferentes Administraciones, la Ley determina que, en el ámbito de la Administración General del Estado, los derechos reconocidos en el artículo 6, podrán ser ejercidos a partir del 31 de diciembre de 2009. En el caso de las administraciones autonómicas y locales, la fecha de ejercicio efectivo de derechos es también el 31 de diciembre de 2009, pero "*siempre que lo permitan sus disponibilidades presupuestarias*".

Pues bien, hemos llegado al 2 de octubre de 2016, fecha en que ha sido derogada la LAECSP tras 9 años de vigencia y 5 de obligatoriedad de su cumplimiento, y existen aún a día de hoy numerosas Administraciones que todavía no cumplen con lo dispuesto ella.

1.4.1 RD 1671/2009, de desarrollo parcial de la Ley 11/2007

El desarrollo reglamentario de la LAECSP se plasmó en el *RD 1671/2009*, el cual centró sus disposiciones principalmente en concretar algunos detalles acerca de la sede electrónica, una regulación específica destinada a hacer efectivo el derecho a no incorporar documentos que se encuentren en poder de las Administraciones públicas, la identificación y autenticación electrónica de personas físicas y jurídicas, los registros electrónicos, las comunicaciones y notificaciones y otros.

El apartado dedicado al documento electrónico y sus copias, contiene las primeras referencias a los *metadatos* que deberán asociarse a los documentos electrónicos, en el art 42. *“Se entiende como metadato [...] cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características”*. *“Los documentos electrónicos susceptibles de ser integrados en un expediente electrónico, deberán tener asociados metadatos que permitan su contextualización en el marco del órgano u organismo, la función y el procedimiento administrativo al que corresponde”*. Y remite al ENI a los efectos de definición de los que deberán considerarse metadatos mínimos.

De manera que, como ya sucedó con la propia LAECSP, además de sus propias disposiciones, el RD advierte de la necesidad de la elaboración de otros dos instrumentos de carácter técnico y complementario: el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad.

1.5 ESQUEMAS DE INTEROPERABILIDAD Y SEGURIDAD

Finalmente, las esperadas disposiciones normativas encargadas de

desarrollar los aspectos más técnicos que habrían de sentar las bases de la administración electrónica, vieron la luz en enero de 2011.

El avance de la administración electrónica en España no hubiera sido posible sin un completo marco legislativo, con especial mención a los aspectos técnicos, que ha incidido especialmente en la interoperabilidad entre las Administraciones Públicas y en la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

1.5.1 RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI)

La interoperabilidad es la técnica que habilita a los sistemas de información para compartir datos y posibilitar la comunicación y el intercambio de información entre ellos. Se trata de una capacidad imprescindible para poder cumplir con las obligaciones de la LAECSP, ya que ha de permitir la implantación de soluciones técnicas como las plataformas de intermediación para el intercambio de documentos y expedientes electrónicos, la interacción con plataformas de firma y validación electrónicas y el sistema de interconexión de registros para el intercambio de asientos registrales.

La interoperabilidad es un elemento indispensable para la cooperación y, en concreto, para la realización práctica de los servicios públicos europeos transfronterizos. Como dice el propio ENI en su preámbulo, *“La finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas”*.

La nueva LRJAP, contempla en su art. 156 la vigencia de los Esquemas Nacionales y respecto al ENI, afirma que *“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”*.

El ENI es una herramienta legislativa de fuerte contenido técnico que

contempla los principales referentes en materia de interoperabilidad provenientes de la Unión Europea y normalización nacional e internacional. Concretamente, su contenido se enmarca dentro de la Estrategia Europea de Interoperabilidad, del Marco Europeo de Interoperabilidad y del Programa ISA (Soluciones de Interoperabilidad para las AAPP) Tanto el ENI como sus normas técnicas de desarrollo contemplan de manera sistemática el enlace con instrumentos equivalentes del ámbito europeo.

Los grandes bloques que contempla este esquema incluyen:

- Los *estándares de interoperabilidad*, las infraestructuras y los servicios comunes, la reutilización de aplicaciones de las AAPP, de la firma electrónica y de los certificados y la conservación, que afecta de forma singular al documento y al expediente electrónico
- La *interoperabilidad organizativa*: incluye la publicación de servicios a través de la *Red de comunicaciones de las Administraciones Públicas* (Red SARA) con sus premisas de publicación; la utilización de nodos de interoperabilidad, como el *Servicio de Verificación y Consulta de Datos* (Plataforma de Intermediación); y el mantenimiento de inventarios de información administrativa, como el *Directorio Común de Unidades Orgánicas y Oficinas* (DIR3) y el *Sistema de Información Administrativa* (SIA) de la AGE. Las Administraciones Públicas conectarán sus redes y nodos de interoperabilidad aplicando el Plan de Direccionamiento de la Administración y la hora oficial.
- La *interoperabilidad semántica*: supone la publicación y aplicación de los modelos de datos de intercambio con la finalidad de compartir información entre las administraciones, así como los relativos a infraestructuras, servicios y herramientas comunes, a través del *Centro de Interoperabilidad Semántica de la Administración* (CISE).
- La *interoperabilidad técnica*: proporcionada por el uso de estándares destinados a garantizar la independencia en la elección, la adaptabilidad al progreso y la no discriminación de los ciudadanos por razón de su elección tecnológica.

- La *reutilización*: habilita las especificaciones necesarias para que las AAPP pongan a disposición de otras administraciones y de los ciudadanos los recursos tecnológicos de los que dispongan, a través del *Centro de Transferencia de Tecnología (CTT)*; aplicaciones reutilizables y soluciones disponibles para libre reutilización.
- La *interoperabilidad de la firma electrónica* y de los certificados: establece la política de firma electrónica de la AGE como referencia para otras AAPP y fija aspectos relativos a la validación de certificados y firmas electrónicas, listas de confianza, prestadores de servicios de certificación y plataformas de validación de certificados y firmas.
- El documento y el expediente electrónico: quedan claramente definidos en sus respectivas *Normas Técnicas de Interoperabilidad (NTI)*.

Otros instrumentos y órganos destacados en la articulación y desarrollo de la interoperabilidad, establecidos por el ENI son:

- La Red SARA como Red de comunicaciones de las Administraciones públicas españolas
- CENATIC: Centro Nacional de Referencia de Aplicación de las Tecnologías de la Información y la Comunicación (TIC) basadas en fuentes abiertas.
- INTECO: Instituto Nacional de Tecnologías de la Comunicación.
- Plataformas de validación de certificados electrónicos y de firma electrónica, con *@firma* como solución de referencia en el ámbito de las administraciones públicas.

1.5.1.1 Normas técnicas de desarrollo

Como se ha visto, el ENI establece un marco general sobre el que desarrollar cada uno de los aspectos técnicos necesarios para hacer realidad la interoperabilidad de sistemas entre los diferentes niveles de la Administración, y en su Disposición Adicional primera enumera las normas técnicas de interoperabilidad a desarrollar, que serán de obligado cumplimiento por parte de las Administraciones públicas. Estas normas técnicas serán:

- Catálogo de estándares:
- Documento electrónico
- Digitalización de documentos
- Expediente electrónico
- Política de firma electrónica y de certificados de la Administración
- Protocolos de intermediación de datos
- Relación de modelos de datos
- Política de gestión de documentos electrónicos
- Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas (Red SARA).
- Procedimientos de copiado auténtico y conversión entre documentos
- Modelo de Datos para el intercambio de asientos

1.5.2 RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS)

El segundo de los Esquema Nacionales, centra sus disposiciones en lo referente a la seguridad en el ámbito de la administración electrónica. Este Reglamento, viene a cumplir lo dispuesto en el artículo 42.2 de la LAECSP y establece los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. Posteriormente, la *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP)*, hará mención al ENS en su artículo 156 apartado 2, en similares términos, corroborando de esta manera su vigencia.

La finalidad del ENS es crear las condiciones de confianza necesarias en el uso de los medios electrónicos a través de medidas orientadas a garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permitan la relación electrónica entre ciudadanos y administraciones públicas para el ejercicio de derechos y el cumplimiento de deberes en este ámbito (Ernst&Young, 2011).

Para la prestación de servicios administrativos electrónicos es

imprescindible que el usuario de los mismos, ciudadano, empresa u otra administración, perciba un ambiente de seguridad en su utilización, tanto jurídica como técnica. Hay que considerar que buena parte de la información depositada en los sistemas de las AAPP está protegida por la LOPD.

El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información y los servicios y será de aplicación en las AAPP para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos y servicios utilizados. En su articulado se determinan las dimensiones de seguridad y sus niveles, la categoría de los sistemas, las medidas de seguridad y la auditoría periódica de seguridad. Establece también la elaboración de un informe para conocer regularmente el estado de seguridad y trata la capacidad de respuesta ante incidentes de seguridad de la información del Centro Criptológico Nacional. Finalmente, en el Anexo IV y obedeciendo a un enfoque eminentemente técnico, incluye un glosario de términos relacionados con la materia.

El ENS y sus disposiciones será de aplicación a todos los sistemas empleados para la prestación de los servicios de la administración electrónica y soporte del procedimiento administrativo general. Estos sistemas se categorizan en el Anexo I según la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de dichos sistemas.

Para realizar la categorización, el ENS define las denominadas *dimensiones de la seguridad*, incluyendo entre ellas la disponibilidad, la autenticidad, la integridad, la confidencialidad y la trazabilidad. Cada una de estas dimensiones se adscribirá a uno de los siguientes niveles: bajo, medio o alto según el perjuicio que pudiera suponer sobre cada una de ellas un hipotético incidente de seguridad. Por último, los sistemas pueden encuadrarse en las categorías básica, media o alta, si alguna de sus dimensiones de seguridad alcanza el nivel correspondiente.

Por su parte, el Anexo 2 incluye las medidas de seguridad que permitirán el mantenimiento de un entorno controlado, minimizando los riesgos hasta

niveles aceptables y que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las propias medidas de seguridad

En 2015 se publicó una modificación del ENS plasmada en el *Real Decreto 951/2015*, de 23 de octubre, para adaptarlo a las regulaciones vigentes, en especial de la Unión Europea, en materia de las tecnologías de información y de la experiencia de la implantación previa del ENS.

1.5.2.1 Instrucciones técnicas de desarrollo

El ENS dispone que será el Centro Criptológico Nacional quien elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones, así como las instrucciones técnicas de seguridad, para cuya redacción se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.

1.6 LA COMISIÓN PARA LA REFORMA DE LAS ADMINISTRACIONES PÚBLICAS: EL INFORME CORA

La Comisión para la Reforma de las Administraciones Públicas (CORA) se crea a principios de 2012, dentro del proceso de reformas iniciado por el Gobierno para luchar contra la crisis económica.

El Consejo de Ministros en su reunión de 26 de octubre de 2012 aprueba el acuerdo por el que se crea la CORA y se le encomienda realizar un estudio integral de las Administraciones Públicas para identificar las áreas de mejora y las medidas a adoptar.

La CORA estructuró su análisis a través de cuatro subcomisiones:

- Duplicidades administrativas
- Simplificación administrativa
- Gestión de Servicios y Medios Comunes
- Administración Institucional

Sus resultados y propuestas se recogen en el Informe Ejecutivo, al que se

sumó otro grupo de medidas de carácter horizontal.

En los trabajos colaboró un Consejo Asesor con representación de organizaciones sociales empresariales y de empleados públicos y se abrió un buzón de participación ciudadana, que recibió 2.239 sugerencias.

El Informe Ejecutivo de la CORA fue presentado el 21 de junio de 2013 y detectó ineficiencias y redundancias en competencias que debían corregirse a través de un total de 217 medidas, agrupadas por cada una de las subcomisiones, además de una serie de medidas de carácter horizontal que afectan a todos los departamentos ministeriales.

El proyecto no finalizó con la presentación del Informe, sino que abrió un proceso de actuaciones a realizar para simplificar los procedimientos incorporando las nuevas tecnologías, reducir cargas administrativas y evitar solapamientos y duplicidades con otras Administraciones.

1.6.1 Recomendaciones del informe CORA en e-administración

La primera recomendación de la CORA con respecto a la administración electrónica es precisamente la que motiva el objeto de estudio de este trabajo: la de elaborar dos nuevas leyes que unifiquen la normativa dispersa que existía en ese momento en una ley de procedimiento administrativo y otra ley de régimen jurídico que regule los aspectos orgánicos de los entes administrativos. La finalidad era dotar a nuestro derecho público de un sistema administrativo sistemático, coherente y uniforme (MHAP, 2013). Esta recomendación se incluía entre las medidas de carácter general propuestas, mientras que algunas de las subcomisiones abordaban aspectos más concretos en lo referente a la e-administración.

La subcomisión de duplicidades administrativas detectó la existencia de dobles atribuciones en la elaboración de Listas de Prestadores de Certificación (TLS), situación que generaba trabas en el uso de los certificados electrónicos. La propuesta del informe consistió en la elaboración de una lista de prestadores de servicios de certificación de firma electrónica admitidos en las administraciones públicas y en los procedimientos administrativos asociados

para evitar duplicidades y facilitar la relación entre los Estados de la UE. Este papel normalizador fue asumido por Ministerio de Industria, Energía y Turismo, quien elabora y mantiene la Lista de confianza de prestadores de servicios de certificación (TsL). Esta recomendación se completaba con la recomendación de que se formalizaran convenios entre las 3 Comunidades Autónomas que tienen su propia autoridad de certificación (Cataluña, País Vasco y Valencia) para la plena admisión de certificados electrónicos por todas las AAPP

Por su parte, la subcomisión de gestión de servicios y medios comunes determinó la encomienda general a la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM) para la prestación de servicios de certificación electrónica a la AGE, con el objetivo de reducir el esfuerzo, tiempo y recursos de los Departamentos, organismos encomendantes y de la propia FNMT, además del coste total por los servicios de certificación.

La subcomisión de simplificación administrativa, por su parte, definió como uno de sus ejes básicos de actuación para conseguir la simplificación administrativa “*el impulso a la administración electrónica y a la sustitución de los medios administrativos tradicionales por medios electrónicos*”. Esta línea de trabajo quedó establecida como propuesta de carácter general u horizontal.

En este sentido, detectó falta de integración de las herramientas de administración electrónica desarrolladas hasta la fecha (Red SARA, @firma, Plataforma 060, Plataforma de intermediación de datos (PID), Registro Electrónico de Apoderamientos (REA),...) con las medidas implementadas en materia de simplificación administrativa.

Esta subcomisión dedicó un apartado completo de sus propuesta a la administración electrónica, algunas de ellas de carácter transversal, entre las que se encuentran:

1. La potenciación de la PID como medio para hacer efectivo el derecho de los ciudadanos a no presentar documentos que ya obren en poder de la Administración.
2. Puesta en funcionamiento del REA y potenciación de su uso por la AGE.
3. Creación del *Tablón Edictal Único* (TEU) de las Administraciones Públicas.

También se adjuntaba una relación de trámites administrativos de la AGE que debían pasar a disponer de su equivalente electrónico, relacionados con la Seguridad Social, Jefatura General de Tráfico, etc...

Esta subcomisión fue también la autora de las propuestas relativas al proceso de notificación electrónica, una de las áreas cuya revisión era más necesaria, tras el escaso resultado obtenido en este aspecto por la LAECSP.

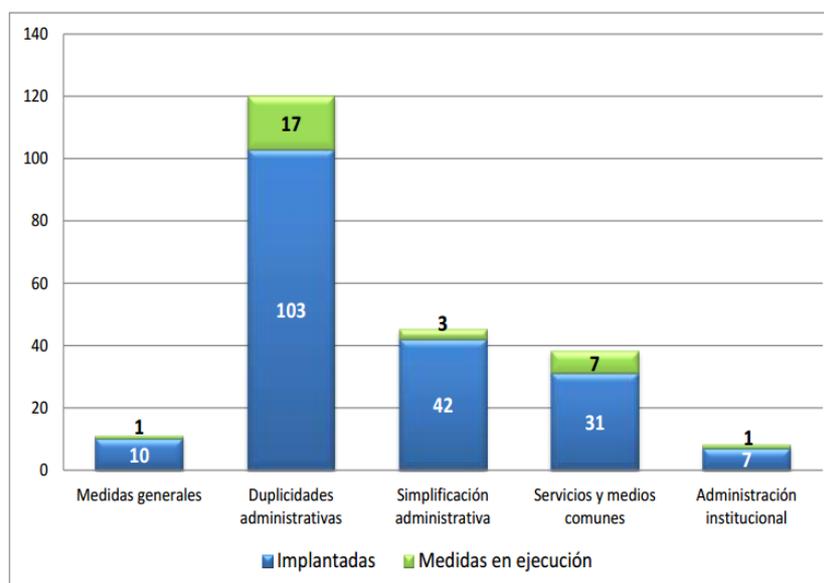
Se incluían también propuestas como la de extender la notificación electrónica obligatoria a los colectivos previstos en el artículo 27.6 de la LAECSP *“interesados que se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos”*. Este extremo se recoge hoy, incluso ampliado, en el art 14 de la LPAC, donde se reconoce a estos colectivos como *obligados electrónicos* en su relación con las AAPP.

Se propone también centralizar en un único punto las notificaciones de todas las AAPP y el uso para ello de una sola Dirección Electrónica Habilitada (DEH), misión esta que trata de cumplir la plataforma *Notific@*, que proporciona un único punto de acceso a las varias plataformas existentes en aquéllos organismos que habían avanzado más en este aspecto a partir de reglamentos propios, como es el caso de la AEAT o la TGSS. Incide el informe además, en la disminución de costes que supondría para las AAPP el uso masivo de la notificación electrónica y de los Centros de Impresión y Ensobrado (CIEs) para aquellas comunicaciones que deban ser remitidas en papel.

Tras la presentación del informe CORA, se creó la *Oficina para la ejecución de la reforma de la Administración*, OPERA, con el objetivo de velar por la ejecución de las medidas incluidas en el informe CORA, asumir su seguimiento, impulso, coordinación y proponer nuevas medidas. Como ya se ha mencionado muchas de las medidas propuestas en el informe ejecutivo ya se han llevado a cabo, otras están en proceso de adopción e incluso se sigue trabajando en nuevas propuestas dentro de la estrategia de reforma de las Administraciones Públicas iniciada por la Comisión. El último informe trimestral

de estado de ejecución de las medidas arroja un balance 193 medidas implantadas hasta mayo de 2016, con lo que se ha alcanzado un 86,94 % de ejecución sobre el total.

ESTADO DE EJECUCIÓN DE LAS PROPUESTAS DEL INFORME CORA POR SUBCOMISIONES



Fuente: [Informe trimestral de seguimiento de las medidas de la CORA](#)

A raíz del informe, se han puesto en marcha o potenciado, un conjunto de soluciones, infraestructuras y servicios comunes que facilitan la implantación de la administración electrónica, algunas de ellas, piezas clave recogidas en la LAECSP. Ejemplos especialmente representativos podrían ser:

- Red SARA para la interconexión de todas las AAPP.
- Plataforma *@firma* para la validación y firma electrónica y su extensión *Cl@ve*.
- Plataforma de intermediación de datos (PID) para la sustitución de los certificados en soporte papel. Hará posible el intercambio interadministrativo de documentos acreditativos que ya obren en poder de alguna administración.
- Registro Electrónico Común (Geiser y ORVE como herramientas más destacadas)
- Plataforma *Notific@* con conexión a la Carpeta Ciudadana y la Dirección Electrónica Habilitada (DEH).

2 LEYES 39 Y 40/2015: ACTUALIZANDO LA ADMINISTRACIÓN ELECTRÓNICA

Como se ha visto, las nuevas Leyes 39 y 40 de 2015, vienen a dar cumplimiento a la recomendación que en materia de regulación hacía el informe CORA en el ámbito de la administración electrónica: ordenar, estructurar y condensar la desperdigada normativa existente y a un tiempo, regular en una Ley las relaciones *ad extra* (el Procedimiento Administrativo en la 39/2015) y en otra las relaciones *ad intra* (el Régimen Jurídico de las Administraciones Públicas en la 40/2015, donde se incluyen las disposiciones que regulan el sector público institucional de las AAPP).

Esta disgregación en una doble norma tiene aspectos negativos evidentes, como la necesidad de recurrir a ambas de forma reiterada o el establecimiento de los criterios utilizados para delimitar algunos aspectos. No siempre resulta fácil delimitar la línea que separa el régimen jurídico del procedimiento administrativo y se producen distribuciones confusas en ciertas materias, como por ejemplo emplazar la regulación de los registros en la LPAC (art.16) y la de la sede electrónica en la LRJSP (art.38), o la correspondiente a los archivos repartida entre el art. 17 de la LPAC y el art. 46 de la LRJSP, o la regulación de la actuación administrativa automatizada, parte del procedimiento administrativo, en el art. 41 de la LRJSP (Gamero, 2015).

Resulta evidente que de haberse elaborado una única norma, este tipo de disfunciones podrían haberse soslayado fácilmente y se evitaría así cierto grado de inseguridad jurídica.

2.1 ÁMBITO DE APLICACIÓN

Para ambas leyes, con carácter de leyes básicas, su ámbito subjetivo de aplicación alcanza a todas las Administraciones Públicas territoriales y a su sector público institucional. Asimismo, serán de aplicación a las universidades públicas de forma supletoria, tal como recoge el art. 2.c en ambos casos.

2.2 LA ADMINISTRACIÓN ELECTRÓNICA EN LA LPAC Y LA LRJSP

En cuanto a las novedades introducidas en el ámbito electrónico, las nuevas Leyes vienen a impulsar de manera decidida su uso tanto en la tramitación interna como en las relaciones interadministrativas, estableciendo la vía electrónica como el medio único y obligatorio para estos fines.

Si la LAECSP se caracterizaba por reconocer el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, el gran aporte de las nuevas LPAC y LRJSP para la implantación de la administración electrónica y su adopción inexcusable por parte de todas las administraciones es, sin duda, el reconocimiento del procedimiento electrónico como el procedimiento habitual (art. 3.2) y la obligatoriedad del formato electrónico para los expedientes (art. 70).

“Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos [...]”.

— art. 3.2 **LRJSP**

“Los expedientes tendrán formato electrónico [...]”.

— art. 70.1 **LRJSP**

Así se manifiesta en la exposición de motivos de la LPAC cuando afirma que *“la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos sino que debe constituir la actuación habitual de las Administraciones”* o en la de la LRJSP al asegurar que *“un entorno en el que la utilización de los medios electrónicos ha de ser lo habitual”*.

Este nuevo enfoque en el que el electrónico deja de ser una versión especial del procedimiento para convertirse en el procedimiento habitual y, en muchos casos obligatorio, es el que Gamero denomina *principio de preferencia del medio electrónico* (Gamero, 2016) y se expresa de forma más clara en el art. 3.2 LRJSP, aunque puede deducirse de algunas disposiciones de la LPAC, principalmente de los arts. 16, sobre registros, 36.1 sobre el medio normal para dictar actos administrativos, 26 sobre documentos electrónicos, 70 sobre expedientes electrónicos o 43 sobre las notificaciones.

2.2.1 Del derecho de acceso a la obligación electrónica

Sobre el derecho a la relación electrónica con las AAPP que ya reconocía la LAECSP y que a su vez suponía para éstas la obligación de proveer los medios y servicios necesarios para satisfacerlo, la LPAC da un paso valiente (y porqué no, también controvertido) cuando en su art. 14.2 declara que “[...] *estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:*

- a) *Las personas jurídicas.*
- b) *Las entidades sin personalidad jurídica. [...]*”

Los apartados subsiguientes amplían este carácter de *obligados electrónicos* a otros colectivos, como quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria o a los empleados públicos, según regule cada Administración.

En todo caso, las personas físicas podrán elegir en todo momento si se comunican con las Administraciones públicas a través de medios electrónicos y el art. 12 determina la creación de un servicio de asistencia en el uso de medios electrónicos a los interesados, excluidos los obligados electrónicos, para lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas.

Este amplio universo de *obligados electrónicos* y su exclusión de los servicios de asistencia técnica, ha abierto algún debate debido a que abarca a muchos colectivos cuya capacitación técnica y material en materia electrónica no está garantizada por el simple hecho de pertenecer a ellos. Tal es el caso de pymes o profesionales liberales que pueden verse afectados por la llamada brecha digital y quienes no gozarían del derecho a la asistencia técnica. Se daría así la paradoja de que quienes resultan obligados a la relación electrónica, carecerían del soporte técnico necesario para poder cumplir con esa obligación.

2.2.2 Autenticación vs firma

La separación entre identificación y firma electrónica es una de la novedades que aporta la LPAC. Pretende con ello la simplificación de los procedimientos de modo que, con carácter general, sólo será necesaria la primera y se exigirá la segunda cuando deba acreditarse la voluntad y consentimiento del interesado, todo ello de acuerdo con lo dispuesto en el *Reglamento (UE) n.º 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 (eIDAS)*.

Según el eIDAS, “*identificación electrónica es el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica*”. Este proceso podría compararse al acto de mostrar un documento de identidad ante un funcionario, pero trasladado al ámbito electrónico. El proceso de identificación es uno de los componentes que conforman la firma electrónica, si bien en la firma, el firmante presta además su consentimiento al contenido del documento firmado.

El art. 9.2 LPAC detalla los sistemas de identificación válidos para las AAPP:

- Sistemas basados en certificados electrónicos reconocidos, como los de persona jurídica y de entidad sin personalidad jurídica.
- Sistemas basados en certificados de sello electrónico.
- Sistemas de clave concertada

Como esta diferenciación entre la identificación y la firma no estaba definida en la LFE y para ajustarse a lo dispuesto en el eIDAS, la DF segunda de la LPAC dispone la inclusión de un nuevo apartado en el art. 3 de la LFE con la siguiente redacción: “*11. Todos los sistemas de identificación y firma electrónica previstos en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley de Régimen Jurídico del Sector Público tendrán plenos efectos jurídicos.*”

Se da también cobertura a los *sistemas de clave concertada* que se habían

ido habilitando en la Agencia Tributaria a través de normas secundarias, como la Resolución de 17 de noviembre de 2011, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la AEAT.

Concretamente, se habían implantado los sistemas de firma con clave o número de referencia, de firma con información conocida por ambas partes y de firma con clave de acceso en un registro previo como usuario. La aceptación de estos sistemas suponía de facto, la posibilidad de realizar trámites con la AEAT si necesidad de utilizar firma electrónica, asunto muy cuestionable desde el punto de vista de la normativa entonces vigente y del tipo de trámites que podían (y pueden) realizarse. La presentación de una declaración de la renta de una persona física es un trámite que en su versión en papel y dado su carácter de declaración, requiere de forma inexcusable una firma. Sin embargo, al admitirse sistemas de identificación y *firma* basados en claves concertadas, como el uso de una simple referencia, se ha venido produciendo un incremento continuado del número de declaraciones presentadas por vía electrónica dada la gran facilidad que presenta así el procedimiento frente a la complejidad de la firma electrónica.

Los sistemas de claves concertadas, el pin24h o la clave pin de la Seguridad Social han obtenido excelentes resultados en el uso de los procedimientos electrónicos por parte de los interesados en los últimos años, así que la LPAC no hace sino autorizar el uso generalizado de estas prácticas.

Finalmente, en lo que respecta a la identificación, cabe mencionar que el art. 11 de la LPAC afirma que, con carácter general, la identificación será recurso suficiente para llevar a cabo una actuación administrativa, pero también enumera los trámites en los que será necesaria la firma electrónica, entre los que se encuentran

- a) Formular solicitudes.
- b) Presentar declaraciones responsables o comunicaciones.
- c) Interponer recursos.

- d) Desistir de acciones.
- e) Renunciar a derechos.

En esta relación se echa de menos la exigencia de la firma electrónica para la práctica de notificaciones, hecho que ha provocado uno de los grandes debates en torno a la práctica *fehaciente* de las notificaciones en la LPAC, pero hablaremos de ello un poco más tarde.

2.2.3 Funcionarios Habilitados

El art. 12 de la LPAC, sobre la ya mencionada asistencia en el uso de medios electrónicos a los interesados, dispone la existencia de funcionarios habilitados para llevar a cabo esa asistencia en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas. También se designarán funcionarios habilitados para actuar por vía electrónica en representación de aquéllos interesados que por alguna causa así lo soliciten. Estos funcionarios habilitados podrán serlo bien para realizar una de estas funciones o bien para ambas, y deberán constar en un *Registro de Funcionarios Habilitados*, cuya creación no será de obligado cumplimiento hasta el 2 de octubre de 2018, dos años después de la entrada en vigor de la Ley, según su DT séptima.

2.2.4 Registro electrónico

El art. 16 de la LPAC obliga a todas las Administraciones a disponer de un Registro Electrónico General en el que recibir la documentación presentada por vía electrónica, cuestión que es congruente con la existencia de obligados electrónicos que se relacionarán exclusivamente por esta vía. En cualquier caso, tampoco resulta una novedad de esta Ley, puesto que ya la LAECSP disponía la necesidad de crear este tipo de oficinas electrónicas en su art. 24. Más interesante resulta la exigida condición de interoperabilidad que les atribuye a estos Registros, de cara al intercambio de información entre las distintas oficinas que habrá de hacer posible en el futuro un verdadero Registro Administrativo Único.

En cuanto al Registro Electrónico, hay que hacer notar que la DT séptima pospone la entrada en vigor de las disposiciones relativas a algunos asuntos, entre los que se cuenta el Registro Electrónico, en dos años más desde la entrada en vigor de la propia LPAC, es decir, no sería obligatorio cumplir lo dispuesto sobre el Registro Electrónico hasta el 2 de octubre de 2018. Si los obligados electrónicos lo son desde el 2 de octubre de 2016 y una Administración decide no habilitar su Registro Electrónico hasta 2 años después, ¿Cómo podrán los obligados cumplir con su necesaria relación electrónica? En nuestra opinión, la inclusión del Registro Electrónico entre las materias susceptibles de ser demoradas es una incongruencia que debería ser corregida de manera inmediata para evitar la inseguridad jurídica de los afectados.

Otra de las novedades que suponen una clara apuesta por la tramitación electrónica plasmada en el momento mismo del inicio del procedimiento, es la obligación de digitalizar todos los documentos recibidos en papel en los registros de entrada de las AAPP. El mecanismo de digitalización que debería utilizarse, aunque no se explicita en la LPAC, deberá ser el recogido en la Norma Técnica de Interoperabilidad de Digitalización de Documentos, derivada del ENI y que contempla los procedimientos para realizar la digitalización certificada por parte de funcionarios habilitados para la realización de copias auténticas.

En cuanto a la potestad de las Administraciones Autonómicas y Locales para la prestación de los servicios materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico de la Administración, la DA segunda obliga a que estas Administraciones se incorporen a las correspondientes plataformas provistas por la AGE por cuestiones de eficiencia, aunque deja abierta la posibilidad de que las presten por sus propios medios, siempre que puedan demostrar que resultan más eficientes y que son plenamente interoperables.

2.2.5 Notificación electrónica

El procedimiento para realizar las notificaciones también se ha visto afectado por este nuevo ánimo electrónico general, de manera que la LPAC establece que *las notificaciones se practicarán preferentemente por medios electrónicos y, en todo caso, cuando el interesado resulte obligado a recibirlas por esta vía.*

Además, esta preferencia por lo electrónico se manifiesta en la obligación de que aquellas notificaciones que vayan a realizarse en papel, deban también ser puestas a disposición del interesado en la sede electrónica.

Hasta ahora era, comunmente aceptado que es necesaria la firma electrónica para que la notificación fuera fehaciente, pero con la nueva regulación de la LPAC, hay quien entiende que es suficiente con la simple identificación para entender practicada electrónicamente la notificación. Como vimos, el art. 11 no hace mención expresa a la notificación al enumerar los trámites en los que será necesaria la firma electrónica. Además, el art. 41.1 exige, para que las notificaciones sean válidas, la constancia de la identidad fidedigna del remitente y destinatario de la misma. Abundando en este enfoque, el art. 43.1, que regula las notificaciones electrónicas, dice que éstas se practicarán mediante comparecencia en la sede electrónica o a través de la dirección electrónica habilitada o mediante ambos sistemas, entendiendo por comparecencia en la sede, el acceso por el interesado o su representante debidamente identificado al contenido de la notificación.

Si, como parece, la LPAC considera suficiente la identificación para considerar practicada la notificación, se produciría un importante cambio en el planteamiento existente anteriormente de requerir para ello la firma del destinatario, extremo que ha venido lastrando la práctica de las notificaciones hasta ahora (Menéndez, 2016).

Para llevar a cabo estas notificaciones, se ha puesto en marcha la plataforma Notific@, de uso obligado para la AGE y a la que podrán adherirse otras AAPP. Notific@ integra, entre otras, la Dirección Electrónica Habilitada (DEH) y la recientemente creada Carpeta Ciudadana del Punto de Acceso General, e incluso pone a disposición de las entidades usuarias los servicios centralizados

de emisión de notificaciones en papel a través de los Centros de Impresión y Ensobrado (CIEs). No obstante, la Ley deja abierta la posibilidad de que una Administración decida habilitar un servicio de notificaciones en su propia sede electrónica, siempre que éste ofrezca las necesarias garantías que permitan tener constancia de su envío, de la recepción o acceso por el interesado, de sus fechas y horas, del contenido íntegro y de la identidad fidedigna del remitente y destinatario de la misma.

Según las propuestas incluidas en el informe CORA en cuanto a las notificaciones, el ahorro por notificación electrónica frente al papel se estimaba en 2,40€ por notificación y 0,22€ por comunicación. La implantación masiva de la notificación electrónica podría ascender fácilmente a varios millones de € de ahorro al año para las arcas públicas.

2.2.6 Documentos y Expedientes electrónicos

Si el documento administrativo constituye la base del acto administrativo, el art. 26 de la LPAC determina que *las AAPP emitirán los documentos administrativos por escrito, a través de medios electrónicos*, una muestra más de la decidida apuesta por lo electrónico de la nueva norma.

Pero el respaldo definitivo a este modelo electrónico lo encontramos en el art. 70, donde se afirma sin tapujos que *los expedientes tendrán formato electrónico*. Es decir, un expediente será electrónico necesariamente.

De esta forma, un expediente será siempre electrónico y estará compuesto por un conjunto de documentos electrónicos firmados o no, uno y otros con sus correspondientes metadatos, y todo ello precedido por un índice electrónico firmado, según lo dispuesto en el ENI. De esta forma, el archivo documental deberá también ser electrónico, como se recoge en el art. 17 de la LPAC.

A nuestro entender, estas disposiciones constituyen la verdadera revolución electrónica incluida en esta reforma y vienen a irrumpir de forma drástica en el casi inmutable panorama de nuestras AAPP. Las implicaciones de su cumplimiento supondrán consecuencias que van a obligar a cambiar hábitos de trabajo largamente instaurados, van a obligar a la revisión de numerosos

procedimientos y a la adopción de nuevas herramientas de gestión documental y administrativa.

2.2.8 Sede electrónica

El Capítulo V de la LRJSP está íntegramente dedicado al funcionamiento electrónico del sector público y en su contenido cabe destacar, por su relevancia más que por su carácter innovador, el art. 38 sobre la sede electrónica. Este artículo es prácticamente idéntico al art. 10 de la LAECSP, con la única novedad del punto 6, donde se exige el uso de certificados de navegación segura en los sitios web dedicados a alojar sedes electrónicas administrativas. Este extremo, que no se explicitaba en la LAECSP pero podía deducirse de su contenido, dio lugar en su momento a la aparición de sedes cuyos servicios carecían de certificados de seguridad, cuestión que queda ahora zanjada de forma clara, incluso, como se verá en el punto 3.2, se ha definido un tipo de certificado específico destinado exclusivamente a este fin de identificación fehaciente de una sede electrónica administrativa y al cifrado de la comunicación establecida con ella.

En cuanto al resto del Capítulo V de la LRJSP, no existen novedades destacables frente a la regulación anterior.

2.2.7 Relaciones interadministrativas

El Capítulo IV de la LRJSP regula la relación electrónica entre Administraciones centrándose en la interconexión de las respectivas redes y dándole especial protagonismo al ENI y al ENS en ese cometido. Los artículos 157 y 158, que se corresponden en su contenido al 45 y 46 LAECSP, disponen la creación de directorios de aplicaciones para ser compartidas y reutilizadas total o parcialmente, en un intento de evitar gastos innecesarios por la adquisición de herramientas de las que ya las AAPP podrían disponer. En caso de que estas aplicaciones ya existan, las Administraciones Públicas estarán obligadas a su uso. El servicio de repositorio común de soluciones tecnológicas se presta desde el [Centro de Transferencia de Tecnología](#), integrado en el [Portal de](#)

[Administración Electrónica](#) del Ministerio de Hacienda y Administraciones Públicas.

2.3 ENTRADA EN VIGOR

Tanto la LPAC como la LRJAP se publicaron el 1 de octubre de 2015, pero establecían en sus disposiciones adicionales un año de vacatio legis en términos generales, es decir que la entrada en vigor de ambas se produjo el pasado 2 de octubre.

A esta demora hay que añadir la ya comentada disposición transitoria séptima de la LPAC, que incluye 2 años más de de vacatio legis en registros electrónicos (general y de apoderamientos), registro de empleados habilitados, punto de acceso general y archivo electrónico.

2.4 EL PAPEL DE LAS COMUNIDADES AUTÓNOMAS

En este punto y una vez revisado el marco jurídico actual en el que se encuentra la administración electrónica en España, queremos analizar el papel que están jugando las Administraciones Autonómicas, segundo nivel de nuestra estructura administrativa y que también ostenta potestad legislativa.

A fecha de hoy, tan solo cuatro Comunidades Autónomas han desarrollado normativa con rango de Ley en esta materia: Cataluña, Baleares, Castilla y León y La Rioja.

En el resto se han limitado a la aprobación de algún Plan de Administración Electrónica, como es el caso de la Comunidad Autónoma de Aragón, se ha elaborado algún Reglamento o decreto de aplicación interna o bien, no se ha regulado en absoluto.

El papel que están jugando las Comunidades Autónomas en general, no difiere en general del de las Corporaciones Locales, limitándose a tratar de adoptar las disposiciones de las normas estatales, pero sin ser actores protagonistas en el proceso. Solo algunas honrosas excepciones son las que han dado un paso al frente en este asunto y han tratado de liderarlo en su territorio, proporcionando medios normativos y materiales para su implantación.

3 LA ADMINISTRACIÓN ELECTRÓNICA EN ESPAÑA: FUNDAMENTOS TECNOLÓGICOS

3.1 LA FIRMA ELECTRÓNICA COMO GARANTE DEL DOCUMENTO ELECTRÓNICO

En una visión simplificada del procedimiento electrónico, podemos catalogar un documento administrativo como electrónico si éste está firmado electrónicamente e incluye los metadatos mínimos exigidos por el ENI. Por otra parte, el expediente electrónico definido en el ENI consiste en una agrupación de documentos electrónicos y un índice, similar al foliado en papel y todo el conjunto está a su vez firmado electrónicamente.

Un expediente electrónico típico se iniciará con la presentación de una solicitud por parte de un ciudadano en el registro electrónico de una administración cualquiera. Esta solicitud deberá ir firmada electrónicamente, tal como sucede con su equivalente en papel. Este expediente se tramitará por medios exclusivamente electrónicos y su resolución administrativa será certificada por el funcionario habilitado para ello dando fe electrónica del acuerdo o resolución. De este proceso simplificado, resulta fácil deducir que la herramienta común en todas sus fases es la firma electrónica. Toda la garantía jurídica y procedimental se basa en la firma electrónica y su condición de confiabilidad. La LFE concede a la *firma electrónica reconocida* el mismo valor respecto de los datos consignados en forma electrónica, que a la firma manuscrita en relación con los consignados en papel (art. 3.4 LFE).

La firma electrónica permite la identificación del firmante, la integridad del documento y el reconocimiento de autoría (el a menudo mal llamado *no repudio*) que son exigibles en un documento electrónico para que goce de plena validez jurídica, todos ellos garantizados mediante el uso de certificados electrónicos emitidos por un tercero de confianza. El uso de sistemas de infraestructura de clave pública (en inglés, PKI) proporciona las garantías asociadas a operaciones criptográficas como el cifrado, la integridad o el reconocimiento de autoría.

En este punto parece apropiado detallar algunos de estos conceptos clave, a fin de definir el papel que cada uno de ellos juega en la firma electrónica:

Identificación del firmante: es la garantía de que el firmante del documento electrónico es quien dice ser y que ninguna otra persona ha podido realizar la firma adjunta, puesto que los elementos necesarios para su consignación obran en poder exclusivo de dicha persona.

Integridad: garantiza que los datos firmados, en nuestro caso el documento administrativo electrónico, no han sido alterados o destruidos de forma no autorizada desde el mismo momento en que el firmante mostró su conformidad con el documento. Esta propiedad permite la detección de posibles cambios o alteraciones en el documento debidos a un ataque malicioso, a errores en la transmisión electrónica o a cualquier otra causa.

Reconocimiento de autoría: también conocido erróneamente como *no repudio de transacciones electrónicas*, consiste en la posibilidad de obtener evidencias de la realización de un acto electrónico que sirvan como prueba fehaciente en caso necesario, es decir, que resulte imposible negar la autoría del acto electrónico, en este caso la firma de un documento.

Estas propiedades de la firma electrónica avanzada se basan en la utilización de un certificado electrónico reconocido y en el uso de dispositivos seguros de creación de firma.

Los certificados electrónicos reconocidos constituyen una pieza fundamental de la llamada *firma electrónica reconocida*, que se define siguiendo las pautas marcadas por la Directiva 1999/93/CE como “*la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*”. Por otra parte, “*la LFE contiene las características que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida*” (exposición de motivos LFE).

En todo este entramado de requisitos exigidos para que las firmas o los certificados exhiban el necesario carácter de *reconocidos*, destaca el papel que juegan los *prestadores de servicios de certificación*. Estas son las entidades

encargadas de la expedición de los certificados electrónicos, elementos software que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito electrónico como firmante.

Los prestadores de servicios de certificación cumplen el papel de *tercero de confianza* o mediador de confianza, una institución ideada para el ámbito digital con origen en la figura del depositario. Esta figura ya se encontraba regulada en el artículo 25 de la ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

De forma concisa, el papel del prestador de servicios de certificación como mediador de confianza, consiste en ser el garante de que los certificados por él expedidos a nombre una persona, sea ésta física o jurídica, *obran en poder exclusivo de dicha persona y bajo su control y custodia*. De esta manera, aquellos prestadores que hayan sido reconocidos para ofrecer sus servicios a la administración pública española, definirán en las conocidas como *políticas de certificación* los procedimientos que una persona deberá seguir para obtener un certificado a su nombre y que incluirá algún mecanismo de identificación de dicha persona para evitar posibles suplantaciones de identidad.

En este sistema de confianza, juega un papel clave la obligación que contrae el titular del certificado, quien *“como firmante y custodio del certificado y sus claves, tiene la obligación de custodiar adecuadamente el certificado, los datos de creación de firma y, en su caso, la tarjeta o soporte del certificado, poniendo los medios necesarios para impedir su utilización por personas distintas a su titular o a su legítimo poseedor”* (RCM-FNMT, 2014).

A modo de ejemplo y para arrojar algo de luz que ayude a la comprensión de estos procesos, en el caso de los certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT), uno de los trámites que debe cumplir la persona solicitante de un certificado es el de la acreditación de su identidad, acudiendo personalmente a una de las más de 2400 oficinas de registro que en este momento existen en España. De esta forma, la FNMT puede garantizar que esa persona es quien dice ser y que es la poseedora única del certificado que

posteriormente descargará en su dispositivo electrónico. De la misma forma, se debe cumplir con este trámite si el solicitante del certificado es una persona jurídica, o bien si es un funcionario que solicita un certificado de empleado público, aunque en estos casos se debe aportar la documentación acreditativa pertinente.

Otro ejemplo aún más garantista es el de los certificados emitidos por la Dirección General de la Policía (DGP) en el momento de expedición de un DNI electrónico (DNle). Los certificados que alberga la tarjeta criptográfica incluida en el propio DNle se generan en el momento de la expedición y con la presencia del interesado ante el funcionario responsable de ello.

Desde ese momento, el uso del certificado ante una administración pública española a través de un medio electrónico garantizará la identidad de la persona en base a una cadena de confianza con origen en ese acto de identificación y en la relación de confianza que la administración pública española tiene con los prestadores de servicios de certificación incluidos en la *lista de confianza de prestadores de servicios de certificación* (TsL) establecidos en España, publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo (TsL, 2016).

3.2 TIPOS DE CERTIFICADOS

Recientemente, el *Reglamento (UE) n.º 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 (eIDAS)*, que entraba en vigor el pasado 1 de julio de 2016, venía a ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso. El eIDAS establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica (certificados) de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica de otro Estado miembro, así como las normas para los servicios de confianza y un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo

electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

De esta forma, en función del destinatario de los mismos, los prestadores de servicios de certificación emiten diferentes tipos de certificados orientados a uno u otro uso. Para analizar la relación de certificados existente, tomaremos como ejemplo los emitidos por la FNMT-RCM:

1.- Certificado de Persona Física

El Certificado de Persona Física es la certificación electrónica que vincula a su suscriptor con unos datos de verificación de firma (clave pública) y confirma su identidad personal. Este certificado permite identificarse de forma telemática y firmar o cifrar documentos electrónicos.

2.- Certificado de Representante

2.a- Representante para Administradores únicos y solidarios

En este caso, el titular actúa en representación de una persona jurídica en calidad de representante legal con su cargo de administrador único o solidario inscrito en el Registro Mercantil.

2.b- Representante de Persona Jurídica

Este certificado sustituye al tradicionalmente utilizado por las Administraciones Públicas para el ámbito tributario y que, posteriormente, se extendió para otros usos. Por tanto, este certificado se expide a las personas jurídicas para su uso en sus relaciones con aquellas AAPP, Entidades y Organismos Públicos, vinculados o dependientes de las mismas.

2.c- Representante de Entidad sin Personalidad Jurídica

Este certificado electrónico se expide a una Entidad sin personalidad jurídica y vincula un firmante a unos datos de verificación de firma y confirma su identidad en los trámites tributarios y otros ámbitos admitidos por la legislación vigente.

3.- Administración Pública

Para dar soporte a los nuevos certificados correspondientes a la Administración Pública, la FNMT-RCM creó una nueva Autoridad de Certificación derivada de la ya existente, denominada AC Administración Pública. Los certificados emitidos para las AAPP pueden ser de tres tipos:

3.a- Certificado de personal adscrito a la administración o funcionario

Este certificado es válido para la realización de firma electrónica por parte del personal al servicio de las administraciones públicas y vincula la identidad de su titular (número de identificación personal, cargo y puesto de trabajo...) al órgano, organismo o entidad de la Administración Pública donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad. El uso de este tipo de certificados abarca las diferentes competencias y funciones propias de los titulares de acuerdo con su cargo o empleo.

3.b- Certificado de sede electrónica

Son certificados emitidos con el fin exclusivo de identificar los sitios web creados por las AAPP para establecerse como sede electrónica de una entidad y proporcionan además servicios de navegación segura (<https://>).

3.c- Certificado de sello electrónico

Estos certificados identifican a una unidad organizativa, que es la que realiza la actuación administrativa automatizada: área, sección, departamento, etc. de una entidad de la Administración Pública. Se utilizan para la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada de la unidad organizativa.

4.- Certificados de Componente

Dentro de esta categoría pueden catalogarse los certificados para componentes informáticos genéricos o de firma de código.

4.a- Certificados de firma de código

Estos certificados electrónicos se utilizan para la identificación de

aplicaciones informáticas descargadas a través de internet. Pueden ser componentes software necesarios para el funcionamiento adecuado de los servicios, aplicaciones, librerías, instalables, ActiveX y otros componentes. Garantizan la identidad del autor y la integridad del contenido para realizar distribuciones de software seguras a través de Internet.

4.b- Certificados SSL/TLS

Estos certificados electrónicos se utilizan para la identificación fehaciente de servidores web que no sean sedes electrónicas. Dentro de esta categoría pueden catalogarse los certificados de servidor SSL/TLS, certificados SAN y certificados wildcard.

4.c- Certificados de sello de Entidad

El certificado de sello de entidad permite a una persona jurídica identificarse telemáticamente y realizar firmas electrónicas para garantizar la autenticidad e integridad de los documentos electrónicos a los que están vinculados, la autenticación de componentes informáticos y otras infraestructuras tecnológicas de la entidad, el intercambio de mensajes o datos cifrados con garantías de confidencialidad, autenticación e integridad o la firma de la comunicación con la plataforma FACe para la Factura electrónica.

TIPOS DE FIRMA PARA DOCUMENTOS ELECTRÓNICOS

TIPO DE FIRMA	DESCRIPCIÓN
XAdES internally detached signature	Contenido firmado y firma comparten una misma estructura XML como nodos independientes y del mismo nivel.
XAdES enveloped signature	Contenido firmado y firma comparten una misma estructura XML necesaria para la validación de la firma. La firma se ubica justo después del contenido firmado.
CAdES detached / explicit signature	Contenido firmado y firma constituyen ficheros independientes
CAdES attached/implicit signature.	El fichero de firma envuelve el propio contenido firmado de forma que, para acceder al contenido, es necesario interpretar la firma.
PAdES	Contenido firmado y firma se incluyen bajo un único fichero PDF que permite el acceso a ambos componentes de forma independiente.

Fuente: [NTI de Política de firma electrónica y de certificados de la Administración](#)

3.2 EL DNI ELECTRÓNICO

En marzo de 2006 comenzó a expedirse en España el DNI electrónico (DNle), una puesta al día del documento de identidad obligatorio emitido por la Dirección General de la Policía. Se trata de un documento que utiliza como soporte una tarjeta criptográfica en la que se insertan dos certificados electrónicos asociados al titular del documento, uno para identificación electrónica (autenticación) y otro para firma electrónica (firma).

En octubre de 2015 se cifraban en más de 44 millones el número de documentos emitidos en este formato que ha ido sufriendo mejoras a lo largo de este tiempo y alcanza en la actualidad su versión 3.

Este proyecto estaba sin duda llamado a ser el gran impulsor de la administración electrónica en España. Debido a su carácter universal, todo español está en posesión del soporte tecnológico necesario para poder relacionarse electrónicamente con las AAPP. Tan solo se requiere un lector de tarjetas criptográficas para empezar a utilizarlo y durante unos años, se distribuyeron miles de dispositivos en diversas iniciativas institucionales orientada a hacer del uso del DNle un hábito normalizado.

Pero a día de hoy, su uso continúa siendo muy reducido: la necesidad de adquirir un lector adicional para poder hacer uso de los certificados incluidos y la rígida política de certificación establecida por la autoridad de certificación de la D. G. de Policía, centrada exclusivamente en la seguridad frente a la usabilidad, son dos dificultades añadidas al ya de por sí complejo uso de la firma electrónica. En la implantación y uso de los servicios electrónicos de identificación y firma proporcionados por el DNle, deberían haber jugado un papel importante las empresas privadas, como bancos y comercio online, claros beneficiarios de las garantías de seguridad que supone el uso del DNle, pero son muy pocas las que han implementado su uso y sus clientes prefieren sin dudar el sistema de identificación basado en usuario y contraseña, menos seguro pero mucho más sencillo y sin complejidades técnicas.

3.3 EL DOCUMENTO ELECTRÓNICO

En un primero momento, la LFE lo definió en su art 3.5 al señalar “*se considera documento de este carácter al redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente*”.

La Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información, introdujo una modificación en la LFE, dejando el texto como sigue: “*Se considera documento electrónico la información de cualquier naturaleza en forma electrónica archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*”

Además, clasificaba el documento electrónico en documentos públicos, por estar firmados electrónicamente por funcionarios y documentos privados. (art 3.6 LFE).

Posteriormente, la LAESCP describe el documento administrativo electrónico y lo dota de validez jurídica: “*Las Administraciones Públicas podrán emitir validamente por medios electrónicos los documentos administrativos [...], siempre que incorporen una o varias firmas electrónicas*” (art. 29).

Sin embargo, la definición del documento electrónico recogida en su anexo, es de nuevo mucho más laxa: “*Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*”.

De conformidad con el artículo 26.2 de la LPAC, los documentos electrónicos administrativos deberán contener información archivada en un soporte electrónico según un formato determinado, disponer de los datos de identificación que permitan su individualización, incorporar una referencia temporal del momento en que han sido emitidos, además de los metadatos mínimos exigidos y las firmas electrónicas que correspondan.

Finalmente, es en la Norma Técnica de Interoperabilidad relativa al documento electrónico, donde se hace una descripción más detallada de su contenido y estructura. Según esta NTI, “*un documento administrativo*

electrónico es, por tanto, el objeto digital administrativo que contiene la información objeto (datos y firma) y los datos asociados a ésta (metadatos)."

Y en este punto es donde debe considerarse la importancia de los metadatos en la documentación electrónica.

Los metadatos, en lo relativo a la gestión de documentos, son unidades de información estructurada que informan sobre la creación, gestión y uso de los documentos y del contexto al que pertenecen a lo largo de su ciclo de vida. Los metadatos sirven para identificar, validar y contextualizar documentos, así como a las personas que los utilizan y los procesos y dispositivos en los que se realiza su gestión y tramitación.

Los metadatos que deberán utilizarse en los documentos electrónicos para cumplir con el ENI, se detallan en el documento *Esquema de Metadatos para la gestión del documento electrónico (e-EMGDE)*. El esquema de metadatos es el instrumento que define la incorporación y gestión de los metadatos de los documentos electrónicos a lo largo de su ciclo de vida. Este documento ha sido revisado recientemente y en su versión 2 describe un esquema de metadatos que consta de 30 elementos, divididos en:

- 16 elementos obligatorios
- 7 elementos condicionales (su uso depende del tipo de entidad que se esté describiendo y el contexto en que ésta funciona)
- 7 elementos opcionales (pueden utilizarse bajo circunstancias en que se requiera una descripción más detallada)

3.4 EL EXPEDIENTE ELECTRÓNICO

En cuanto al expediente administrativo electrónico, el art. 70 de la LPAC define el expediente administrativo como el *"conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla"*. Además, *"los expedientes tendrán formato electrónico"*. Por su parte, la NTI del expediente electrónico, derivada del ENI, establece que la estructura de los expedientes electrónicos incluirá los documentos electrónicos, el índice

electrónico firmado por la Administración para asegurar la integridad del expediente y garantizar su recuperabilidad siempre que sea preciso y los metadatos, obligatorios y opcionales que correspondan.

Técnicamente, la asociación de metadatos a los documentos y expedientes se realiza a través de herramientas denominadas *gestores documentales*. Estos programas se utilizan para almacenar y modificar documentos y expedientes electrónicos, así como los correspondientes metadatos obligatorios asociados. Si el gestor documental elegido cumple con el estándar *CMIS*, un estándar abierto que permite a diferentes sistemas de gestión de contenidos interoperar a través de internet, será capaz de interoperar con *Inside*, la solución proporcionada por la AGE para para la gestión de documentos y expedientes electrónicos de acuerdo a las especificaciones del ENI.

3.5 EL PORTAL DE ADMINISTRACIÓN ELECTRÓNICA (PAE)

El Portal de la Administración electrónica (PAe), es el portal de referencia en materia de administración electrónica sobre situación, desarrollo, análisis, novedades e iniciativas en torno a la ella. Integra contenidos y servicios de fuentes muy diversas para presentar la oferta completa de soluciones proporcionadas por diferentes organismos en esta materia.

El Punto de Acceso a sus servicios se presta a través de <https://administracionelectronica.gob.es> y en él se pueden encontrar noticias y eventos, informes, estudios y boletines, normativa, etc. También incluye el directorio de soluciones disponibles para su reutilización, servicios comunes ofrecidos, modelos de datos comunes, especificaciones técnicas, metodologías y guías, etc. Su espacio permite colaborar entre y desde todos los entes que intervienen en la administración electrónica, fomentando la retroalimentación y la reutilización de conocimientos y servicios.

El PAe también incluye el *Centro de Transferencia de Tecnología* (CTT), un directorio general de aplicaciones y soluciones cuyo objetivo es favorecer la reutilización de recursos por todas las AAPP, para poder dar cumplimiento a lo

dispuesto en los arts. 157 y 158 de la LRJAP.

Entre otros recursos, se puede encontrar el catálogo de servicios de Administración Digital de la Dirección de Tecnologías de la Información y de Comunicaciones (DTIC), también se puede encontrar la guía Digitaliza-T!, dirigida a facilitar el cumplimiento de las leyes por parte de las Entidades Locales, mediante las herramientas tecnológicas que la Secretaría General de Administración Digital pone a disposición de todas las AAPP

Este catálogo de servicios prestados por la AGE trata de cubrir las obligaciones que deben ser asumidas por las EE.LL. en materia de administración electrónica, e incluye los siguientes recursos:

- [Punto de Acceso General](#) (PAG): es un portal web y una sede electrónica que integrará gran parte de los servicios electrónicos disponibles para ciudadanos y empresas. Es la evolución del antiguo portal 060. Se regula en el art. 13.a de la LPAC. La DF séptima añade una demora de 2 años tras la entrada en vigor de la Ley, para el efecto de lo dispuesto respecto al PAG.
- [Carpeta Ciudadana](#): forma parte del PAG y permite conocer los expedientes que se tienen abiertos en los distintos organismos, asientos registrales entre Administraciones, los datos en poder de la Administración o las notificaciones electrónicas recibidas.
- [Cl@ve](#): es el sistema de identificación electrónica que se analizará en el apartado 5 de este trabajo.
- [Apoder@](#): registro electrónico de representación y apoderamientos, creado y regulado en el RD 1671/2009 (art. 15), para hacer constar y gestionar las representaciones que los interesados otorguen a terceros. Prorrogado por la DF séptima.
- [Habilit@](#): registro de funcionarios habilitados, creado por el art. 16 del RD 1671/2009 que incluye a los funcionarios que se habiliten por parte de la Administración para actuar en nombre de los ciudadanos que no dispongan de firma electrónica en procedimientos electrónicos. Prorrogado por la DF séptima.

- *GEISER / ORVE / SIR*: se trata de una solución integral de registro prestada en modo nube y que proporciona los servicios de registro electrónico, registro presencial, intercambio de registros internos y externos (a través de la plataforma del *Sistema de Interconexión de Registros*, SIR). También afectado por la DF séptima.
- *Inside y Archive*: InSide es un sistema para la gestión de documentos y expedientes electrónicos que cumple los requisitos para que puedan almacenarse y/o obtenerse según el ENI, mientras que Archive es una aplicación web de archivo definitivo de expedientes y documentos electrónicos.
- *Plataforma de Intermediación de Datos (PID)*: está diseñada para el intercambio de datos y acceso a documentos que ya obren en poder de otras AAPP
- *Notific@*: permite la concentración de las notificaciones electrónicas e integra otras plataformas, como la Carpeta Ciudadana del PAG y la Dirección Electrónica Habilitada (DEH) de la FNMT.
- *SIA*: Sistema de información administrativa que incluye la relación de procedimientos y servicios de la AGE y de todas las administraciones participantes (CCAA y EELL), de acuerdo al artículo 9 del ENI.
- *CTT*, anteriormente comentado en este mismo apartado.

Este exhaustivo listado de recursos que la AGE pone a disposición de las administraciones autonómicas y locales cubre gran parte de las necesidades más inmediatas para poder cumplir con los requerimientos necesarios para prestar los servicios ad extra, los relacionados con ciudadanos, empresas y otras

administraciones. Aunque se trata de un buen punto de partida, no debe pasarse por alto la ausencia de la que debería ser la pieza central de una administración electrónica integral: el programa de tramitación electrónica de

“Aunque el interfaz externo de los servicios públicos ha sido digitalizado en su mayor parte, la tramitación interna por parte de la Administración no ha evolucionado de la misma manera”.

— Plan de transformación digital de la AGE y sus OOPP

expedientes. Recientemente, el Minhap ha anunciado la disponibilidad de la plataforma Acced@, que integra una sede electrónica y un completo gestor para la tramitación electrónica de los expedientes que se inician en la sede. Esta plataforma se encuentra funcionando actualmente en diversos organismos tales como el Ministerio de la Presidencia, el Ministerio de Asuntos Exteriores, la UNED o el Ministerio de Defensa y se espera que próximamente pueda ser puesta a disposición de otras Administraciones.

También queremos destacar que algunas de estas herramientas están, a fecha de elaboración de este trabajo, y tras dos meses en vigor de la LPAC y LRJAP, en un estado muy incipiente de desarrollo, como la PID, que proporciona muy escasos contenidos todavía como para que pueda resultar relevante, o Apoder@ y Habilit@, poco desarrolladas y con su entrada en vigor pospuesta. En otros casos, a pesar de que nominalmente las herramientas están en un estado mucho más maduro, el problema es que no se encuentran disponibles todavía para las EE.LL. a pesar de afirmarse lo contrario en la guía mencionada y en el propio portal del PAe. La experiencia profesional del autor, técnico de desarrollo informático en el ámbito de la administración electrónica, tras solicitar la incorporación de una Diputación Provincial a GEISER, es que la herramienta está disponible por el momento tan solo para la AGE.

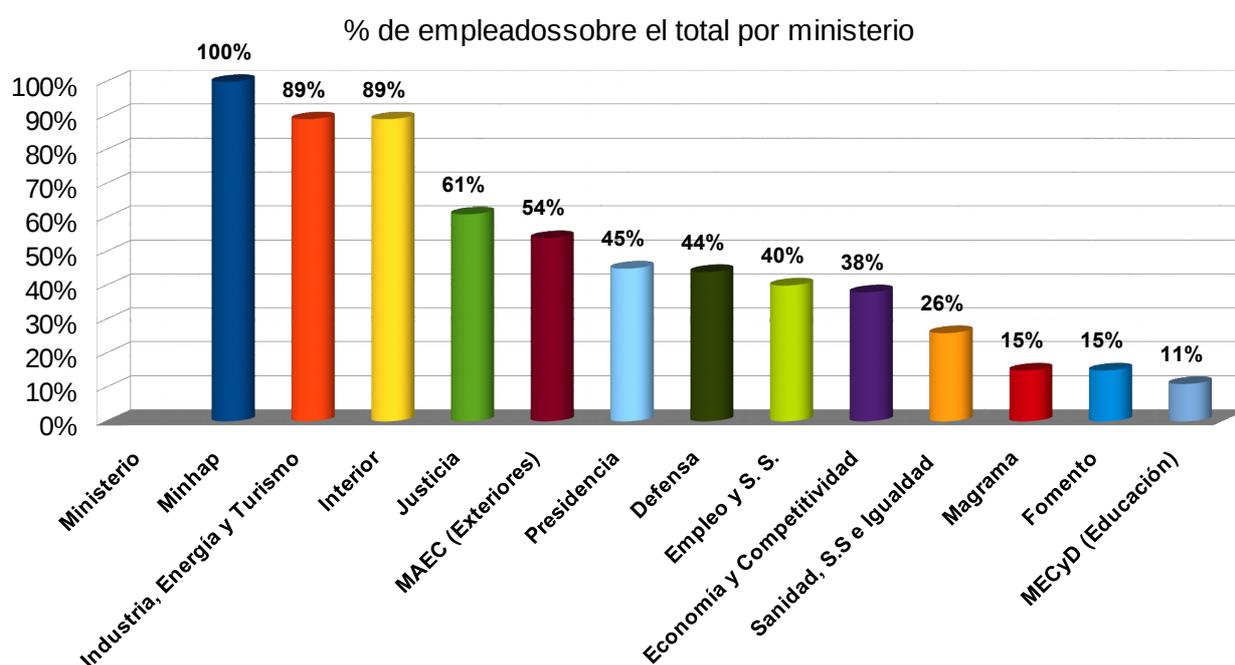
En cualquier caso, la iniciativa de la AGE tratando de liderar la implantación de la e-administración en otros niveles administrativos y poniendo a su disposición las herramientas mencionadas, resulta muy loable y ofrece gran seguridad a pequeñas entidades locales, que afrontan así con algo más de sosiego un proceso que se vislumbra realmente difícil.

4 OBSTÁCULOS ACTUALES PARA LA IMPLANTACIÓN DE LA ADMINISTRACIÓN ELECTRÓNICA

Una vez analizadas las bases que establecen la firma electrónica de documentos como la herramienta básica para el desarrollo de la administración electrónica, cabría esperar que su utilización en las administraciones públicas fuese masiva y generalizada: más de 44 millones de DNle emitidos, numerosas disposiciones normativas que avalan su uso o que incluso obligan a ello... Pero nada más lejos de la realidad.

La implantación y uso en la AGE, Ministerios, Organismos y Agencias es bastante irregular, encontrándose casos de utilización generalizada en algún Ministerio, hasta otros en estado incipiente de implantación.

Implantación de la firma electrónica en la AGE



Fuente: [REINA 2016 Las TIC en la Administración del Estado](#)

En lo que respecta a ciudadanos y empresas, solo un pequeño porcentaje de gente ha hecho uso de su DNI electrónico o certificado de persona jurídica hasta la fecha. Y el motivo es que si los certificados de otras agencias certificadoras son difíciles de usar, el DNI lo complica todo mucho más: la

estricta política de certificación establecida por la Dirección General de la Policía obliga a introducir el PIN hasta la saciedad, en ocasiones incluso sin tener intención de hacer uso de los certificados, el software asociado es muy pesado, no existe un teléfono de atención que funcione bien y ni aun siendo un experto, resulta fácil de usar sin problemas. A esto hay que añadir los problemas propios de los certificados en soporte tarjeta, puesto que el lector es un elemento hardware relativamente poco evolucionado y de escasa implantación (Gallego, 2015).

Tampoco entre los ciudadanos y empresas, grandes beneficiarios de las facilidades prometidas por la administración electrónica, se detecta un uso habitual de estos servicios. Ni siquiera existe una gran demanda o exigencia para la puesta en marcha de los servicios electrónicos a los que las administraciones ya vienen obligadas. En la actualidad existe la percepción generalizada de que estos servicios no funcionan bien o no son seguros. A ello hay que añadir el desconocimiento de su uso tanto a nivel técnico como de usuario, la dificultad operativa de los mismos y la falta de unificación de la identificación, autenticación y acceso. (Carpio, 2015).

Entre las numerosas dificultades técnicas que el usuario de la administración electrónica, sea este funcionario o ciudadano puede encontrar, se cuentan aspectos de difícil comprensión para la persona no experta en nuevas tecnologías, como podrían ser la incorrecta instalación del certificado, contar con una versión incompatible del navegador, carecer del certificado raíz para la validación de los certificados utilizados en la firma, ausencia de controladores (*drivers*) del lector de tarjetas o de la tarjeta criptográfica utilizada, incompatibilidades entre los diversos elementos software que intervienen en el proceso (sistemas operativos, navegadores, applets, plugins, visores...) y otras muchas.

Así pues, podemos entender la aportación de la firma electrónica a la administración electrónica desde dos enfoques diferentes:

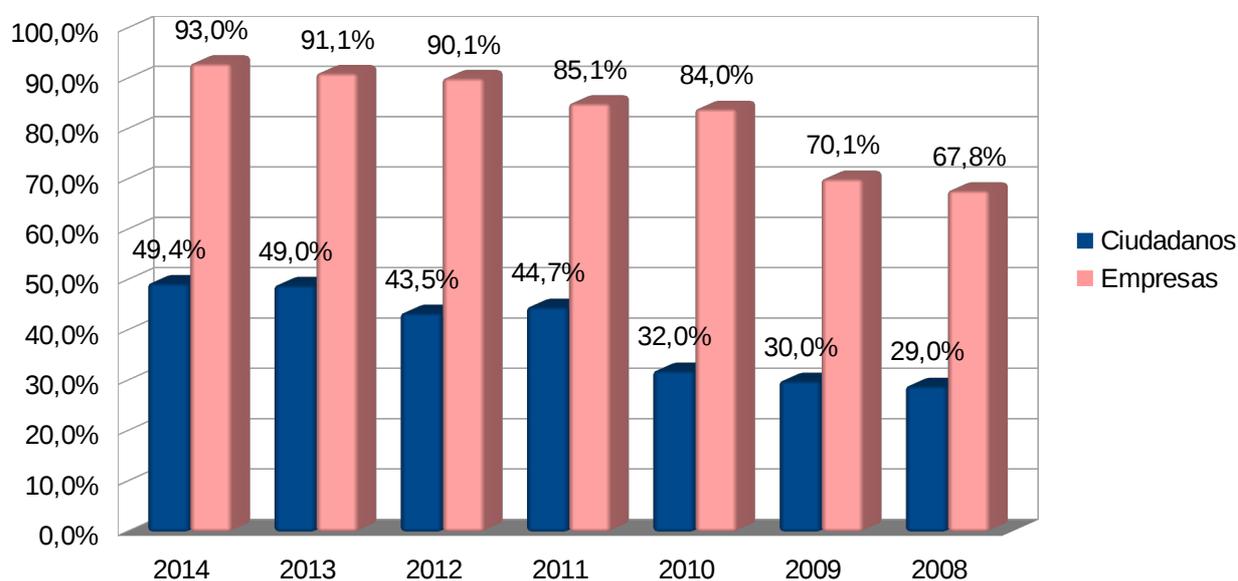
1. Como la herramienta que proporciona las garantías jurídicas de identificación y autenticación requeridas en los procedimientos

electrónicos

2. O como la herramienta que dificulta el uso de los procedimientos electrónicos introduciendo numeros elementos de carácter técnico que hacen de un sencillo trámite una misión solo apta para expertos.

Podría decirse que la firma electrónica constituye la mayor aportación al desarrollo de la administración electrónica, al tiempo que se erige también como el mayor obstáculo para su implantación y uso masivo.

Uso directo de los servicios electrónicos



Fuente: [Boletín de indicadores del Observatorio de Administración Electrónica, septiembre 2016](#)

5 FACILITANDO LA FIRMA: LA LEY 39/2015 Y CL@VE

Esta situación ha llevado a un estancamiento en el desarrollo de los servicios de administración electrónica en nuestro país, donde, a pesar de disposiciones como la LAECSP o la implantación del DNI-e, tan solo la Agencia Tributaria ha conseguido avanzar de forma constante en la implantación de trámites electrónicos y en número de usuarios de estos servicios.

El motivo es que, de alguna manera, este organismo ha esquivado las obligaciones legislativas y de seguridad que imponía la LAECSP y ha ido dictando sus propias normas, demostrando que son fiables y funcionan. O incluso ha venido imponiendo a los empresarios la obligación del empleo de medios electrónicos (Menéndez, 2016). Como consecuencia de esto, las Administraciones públicas en general y la producción legislativa posteriormente, van siguiendo la pista del caso de éxito de la AEAT y los nuevos servicios que se están implantando, como el sistema de claves concertadas ([Cl@ve](#)), no son sino una copia de lo que esta agencia ha venido haciendo hasta ahora (Gallego, 2015).

Cl@ve se regula en la Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

Se trata de un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Incluye y complementa los actuales sistemas de acceso y firma basados en certificados electrónicos, como el DNle y ofrece además la posibilidad de realizar firma en la nube, mediante certificados electrónicos centralizados, es decir certificados electrónicos almacenados y custodiados por la Administración Pública. Estos certificados centralizados, o *certificados en la nube* permiten al ciudadano firmar documentos electrónicos desde cualquier dispositivo con conexión a Internet sin necesidad de ningún equipamiento adicional y liberándolo de gran parte de

los requisitos software asociados.

De esta manera, la gran mayoría de los problemas tecnológicos que se han enumerado anteriormente quedarían resueltos para el usuario final, al no requerir del uso de tarjetas criptográficas y sus correspondientes lectores, ni utilizar certificados electrónicos almacenados en el navegador, ni máquinas virtuales de java para el acceso a la clave privada del certificado para realizar la firma. Mediante este sistema de almacenamiento en la nube, el certificado correspondiente al usuario firmante, sea persona física, jurídica o funcionario de la Administración pública española, obra ya en poder de la propia administración y tan solo se requiere la autorización del titular para poder realizar una firma electrónica. Esta autorización se podrá conceder accediendo a la plataforma Cl@ve mediante un sistema ligero de claves concertadas basado en usuario y contraseña y confirmando su uso a través de un sistema de validación complementario, como la recepción de un código temporal a través de un mensaje de teléfono móvil, de forma similar a como operan la mayoría de los sistemas de banca electrónica.

Este nuevo enfoque de la firma electrónica basada en servicios en la nube, descarga al usuario de la responsabilidad de custodia de los certificados expresada en los documentos de políticas de firma de los prestadores de servicios de certificación e imposibilita el uso de dispositivos seguros de creación de firma expresados en el artículo 3.3 de la LFE. Al ser estos dos de los aspectos básicos del sistema de firma electrónica reconocida existente hasta ahora, que era la que tenía la misma validez que la manuscrita, ha sido necesario su reconocimiento entre los sistemas de firma válidos mediante la pertinente modificación ordenada por la LPAC en la Disposición final segunda que dispone incluir un nuevo apartado 11 en el artículo 3 de la LFE con la siguiente redacción: *“11. Todos los sistemas de identificación y firma electrónica previstos en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley de Régimen Jurídico del Sector Público tendrán plenos efectos jurídicos”*.

Cl@ve dispone de dos sistemas de claves concertadas:

- *Cl@ve PIN*: sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios. Es el sistema PIN24H de la AEAT.
- *Cl@ve permanente*: sistema de contraseña de mayor validez temporal destinado a usuarios habituales. Es un sistema de acceso mediante usuario y contraseña, reforzado con claves de un solo uso por SMS, a los servicios de Seguridad Social. Este sistema será además el que permitirá el acceso al ciudadano a la firma en la nube .

El alta en estos sistemas de claves concertadas y los servicios de firma en la nube requieren que el ciudadano se registre previamente en el sistema, aportando los datos de carácter personal necesarios.

6 CONCLUSIONES

La implantación de la administración electrónica persigue la simplificación de la vida de los usuarios, así como también de la propias administraciones, quienes se ven obligadas a proporcionar sus servicios por vía electrónica y a impulsar su uso entre la población.

Se ha realizado un gran esfuerzo, tanto tecnológico como normativo para salvar los obstáculos que actualmente lastran el desarrollo de la administración electrónica. El paso legislativo dado en esta ocasión, a través de las Leyes 39 y 40 parece dirigirse en la buena dirección, ya que, más allá del reconocimiento del derecho de los ciudadanos a relacionarse electrónicamente con las administraciones, establece ésta como la única vía de relación para los obligados electrónicos, al tiempo que impone la adopción del procedimiento electrónico como el procedimiento habitual y la gestión documental electrónica en el seno de todas las administraciones.

A este respecto, estimamos que uno de los puntos que deberían revisarse del articulado actual de la LPAC, es la exclusión de los obligados electrónicos de entre los beneficiarios de la asistencia técnica que las AAPP deben prestar en las oficinas de asistencia en materia de registros. No es coherente que quienes resultan obligados a la relación electrónica, carezcan del soporte técnico necesario para poder cumplir con esa obligación.

Del mismo modo, la exclusión de la necesidad de la firma electrónica para dar por practicada una notificación, bastando con el simple acceso a su contenido mediante comparecencia en la sede electrónica o a través de la plataforma Notific@ en la Carpeta Ciudadana o la Dirección Electrónica Habilitada, se antoja una amenaza para el destinatario, a quien sin duda se le facilita la recepción de la notificación, pero a costa de ver mermadas sus garantías. Aún cuando la Administración remita un aviso al dispositivo electrónico y/o a la dirección de correo electrónico del interesado que éste haya comunicado, informándole de la puesta a disposición de una notificación, tal como establece la LPAC, ese envío no garantiza su recepción y su

conocimiento efectivo por parte del destinatario, quien podría no recibir tal aviso y desconocer la existencia de la notificación, o aún conociéndola, no conseguir completar el acceso a la notificación por dificultades técnicas de la plataforma Notifica@, incidencia que se viene dando con cierta frecuencia, al menos en este periodo inicial de implantación y de extensión masiva de su uso. Situaciones todas ellas en las que la notificación se entendería rechazada en el plazo de diez días y desplegaría efectos sin llegar a ser conocida por el interesado.

En cuanto a la novedad técnica que supone [Cl@ve](#), su objetivo es tratar de atajar el punto débil de los servicios de identificación y firma electrónica que conforman la base de la administración electrónica: su usabilidad. El uso de sistemas de claves concertadas y de firma en la nube debe descargar a los usuarios de la complejidad técnica asociada a los certificados electrónicos y facilitar e incentivar el uso de las soluciones de administración electrónica.

Sin embargo, el que debería suponer el mayor avance en el desarrollo de la administración electrónica y que ya la LAECSP establecía como uno de sus objetivos, la *simplificación de los procedimientos administrativos*, no parece que sea afrontado de forma decisiva en ninguna de las disposiciones que se han ido adoptando. Sí que se reconoce como uno de los principios que deberán inspirar el proceso de transición electrónica, pero no se manifiesta en modo alguno en el articulado de la normativa. De hecho, los procesos diseñados en la mayor parte de las administraciones, se limitan a tratar de reproducir el procedimiento existente en papel en un entorno electrónico.

Cuando se plantea la transición a la electrónica en una entidad, se manifiesta inmediatamente la necesidad de diseñar un modelo de descripción de procedimientos adaptado a las particularidades del ámbito electrónico, antes que implementar el uso de metadatos (García González, 2015). La aplicación de las nuevas tecnologías al procedimiento debe suponer una revisión y reformulación del mismo, proceso que se ha llevado a cabo de forma diferente en cada administración (Sánchez, 2015).

En general, las instituciones enfocan la transición a la administración

electrónica con una visión limitada de la simplificación administrativa, seguramente constreñidas por el hábito del trabajo excesivamente centrado en el procedimiento y con un enfoque excesivamente burocrático. El propósito de simplificar se centra en reducir las trabas burocráticas detectadas en la lógica propia del procedimiento y las estructuras administrativas clásicas (cargas administrativas), que no tienen en cuenta las posibilidades ofrecidas por las nuevas tecnologías, ni realizar un rediseño integral de las estructuras y los procesos que permitiría aplicar el doble nivel de optimización, tanto procedimental como tecnológico.

Pero, a nuestro entender, el punto donde debería trasladarse el debate, va mucho más allá que a la imprescindible simplificación y el rediseño y normalización de los procedimientos: se trata de las exigencias de seguridad que se le imponen a los actos administrativos al ser trasladados al ámbito electrónico.

Como ejemplo vivido en la experiencia personal del autor en su trabajo como técnico en nuevas tecnologías en una administración local, podríamos contar situaciones de incongruencia en los documentos electrónicos, derivadas de la abundante información y garantías que se le exigen a una firma electrónica frente a la firma manuscrita. En la tramitación en papel, una resolución administrativa podía redactarse con un pie de firma en el que constase la fecha de adopción de la resolución y sin embargo, ser firmada días después por cuestiones de disponibilidad de los firmantes, sin que el documento final mostrara en modo alguno esa discrepancia. Los efectos administrativos tenían lugar desde el momento de adopción de la resolución. Actualmente y debido a que cada una de las dos firmas obrantes en un decreto (por ejemplo) contienen la fecha y la hora de la firma, podría darse el caso de que en los metadatos de creación del documento constara una fecha (la de redacción), en el pie de firma otra (la de adopción del acuerdo que es a partir de cuando debería tener efecto), una tercera fecha en la firma electrónica del alcalde o presidente y una cuarta fecha en la firma correspondiente al secretario de la corporación. En la versión electrónica del documento, incluso se pondría de manifiesto la posible

mala praxis de haber firmado el secretario con anterioridad a haberse producido la firma del presidente, cuestión que quedaba absolutamente indistinguible en el documento en papel. Surgen así cuestiones jurídicas nuevas derivadas de esta sobreinformación aportada por la firma electrónica, como cual es la fecha de efecto de la resolución del ejemplo ¿la de su adopción? ¿la de la firma del presidente? ¿la de la firma del secretario, que debería ser la última y dejaría así completo el documento?

La misma situación puede producirse en la elaboración de un certificado de un acuerdo adoptado por un órgano colegiado (Comisiones, Pleno,...) Si existen dos, tres o incluso cuatro fechas diferentes, ¿cuál es la fecha de efectos?

Pareciera que en el caso de un decreto debería ser el momento en el que el alcalde o presidente plasme su firma electrónica, dado que es quien ostenta la potestad resolutoria en ese documento. Lo contrario sucede con una resolución emanada de un órgano colegiado: en este caso, es la firma del secretario, quien certifica con su capacidad de fe pública que tal acuerdo existió.

En cualquier caso, y como queda apuntado, la nueva información que en aras de la seguridad jurídica aporta la firma electrónica, supone también un aumento de la complejidad del procedimiento, no solo técnico por la realización de dichas firmas, sino incluso jurídico por las posibles discrepancias.

Como propuesta en aras de la simplificación de los procedimientos y tratando de sacar provecho de las nuevas garantías que ofrecen los certificados electrónicos, en nuestra opinión, debería cuestionarse la necesidad de esa doble firma en documentos como los comentados. El art. 205 del *Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales (ROF)*, dispone que el Alcalde firmará en las certificaciones para significar que el Secretario o funcionario que las expide y autoriza está en ejercicio del cargo y que su firma es auténtica. Como contrapartida, la firma del secretario en un decreto sirve para constatar que la firma que hay al lado de la suya corresponde al Alcalde o Presidente y que éste se encuentra en ejercicio de su

cargo. Pues bien, si como hemos visto en este trabajo, los prestadores de servicios de certificación emiten certificados electrónicos de personal adscrito a la administración, en los que consta la relación existente entre su titular y una entidad pública, con expresión del cargo que ocupa, debería ser suficiente con esta garantía como prueba de que el alcalde o el secretario son los firmantes del documento que a cada cual le compete, sin necesidad de la segunda firma para corroborar un dato que ya vienen garantizado en el propio certificado.

En general, podemos decir que el uso de la administración electrónica resulta excesivamente complejo tanto en su funcionamiento técnico como procedimental. Cabría preguntarse porqué una persona puede hacer uso de servicios como la banca electrónica, mediante la cual puede realizar transferencias entre cuentas bancarias o invertir en productos financieros complejos, con un sistema simple de identificación basado en usuario y contraseña (hoy en día reforzado por procesos de verificación adicionales como el envío de claves a través de sms) y sin embargo, debe hacer uso de un sistema tan garantista como la firma electrónica para la simple solicitud de un certificado de empadronamiento.

¿Cual es el motivo trascendental por el que la presentación de una instancia o una queja en su Ayuntamiento requiere de su identificación y autenticación electrónica fehaciente, mientras que puede contratar los servicios de telecomunicaciones de su hogar o el seguro de un vehículo mediante una simple llamada telefónica?

¿Qué hace que un trámite administrativo en apariencia sencillo, como una solicitud de licencia menor de obras, sea de imposible tramitación electrónica para muchas personas que, sin embargo, contratan con normalidad sus viajes de vacaciones, vuelos, estancias en hoteles o realizan sus compras por internet?

El amplio desarrollo normativo de nuestro marco jurídico, unido al excesivo formalismo y complejidad procedimental de la tramitación administrativa, suponen los siguientes escollos a vencer en este tortuoso camino de las Administraciones Públicas hacia los mundos virtuales en el siglo XXI.

BIBLIOGRAFÍA

Carpio Carro, M. (2015). La firma electrónica. *El Consultor De Los Ayuntamientos y De Los Juzgados Municipales*, 7(155), 495.

Delgado Gómez, A. (2011). Normativa de referencia. en Coordinadora de asociaciones de archivos (Ed.), *Administración de documentos y archivos textos fundamentales* (pp. 39). Madrid: Ministerio de cultura.

Dirección General para el impulso de la Administración Electrónica. (2011). *Guía de aplicación de la norma técnica de interoperabilidad de documento electrónico* (1a edición electrónica ed.). Madrid:

FEMP. (2011). *Experiencias de éxito en e-administración de las entidades locales* (2011th ed.). Madrid: Federación Española de Municipios y Provincias.

Fernández Scagliusi, María de los Ángeles. (2016). La reforma del procedimiento administrativo: La nueva ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas. *Estudios De Deusto: Revista De La Universidad De Deusto*, 63(2), 127.

Gallego García, F. (2015). La firma electrónica: Aspectos tecnológicos. *El Consultor De Los Ayuntamientos y De Los Juzgados Municipales*, 7(155), 548.

Gamero Casado, E. (2016). Panorámica de la administración electrónica en la nueva legislación administrativa básica. *Revista Española De Derecho Administrativo*, (175), 15-27.

García González, M. (2016). Administración electrónica: Por qué implantar una política de gestión de procesos institucionales en las administraciones públicas. *El Profesional De La Información*, Vol. 25 (Número 3. Dedicado a: Metamedios y audiencias), 473-484.

Martín Rebollo, L. (1992). La administración en la constitución. *Congreso "La Reforma De La Constitución" : La Rioja, Abril De 1992*, Logroño. , Vol. 5.

Melón Muñoz, A., & Linares Gil, M. I. (2010). *Administración electrónica*. Madrid: Francis y Taylor.

Menéndez Sebastián, E. M. (2016). La implementación de la administración electrónica en las nuevas leyes (ejemplar dedicado a: Las nuevas leyes de procedimiento administrativo común y régimen jurídico del sector público). *El Cronista Del Estado Social y Democrático De Derecho*, (63, Octubre 2016), Iustel, págs. 28-37.

Ministerio de Hacienda y Administraciones Públicas. (2013). Minhap (Ed.), *Informe de la comisión para la reforma de las administraciones pública* (2013th ed.). Madrid: Gobierno de España.

Moreno Bonilla, V., & Pérez Almarza, V. (2009). en Comisión de Modernización y Calidad de la FEMP (Ed.), *Guía práctica de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos : LAECSP (2009)* (2009th ed.). Madrid: Federación Española de Municipios y Provincias.

Moreno Bonilla, V., & Pérez Almarza, V. (2010). *Incidencia del desarrollo reglamentario en la adaptación de las administraciones locales a la ley 11/2007: Anexo a la guía práctica de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos (2010)* (2010th ed.). Madrid: Federación Española de Municipios y Provincias.

Oficina de Seguimiento de la Red de Municipios Digitales de Castilla y León. (2008). In Oficina de Seguimiento de la Red de Municipios Digitales de la Junta de Castilla y León (Ed.), *Guía de adaptación de las EELL a la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos* (2008th ed.) Junta de Castilla y León.

Sánchez Sánchez, Z. (2016). Las nuevas leyes de régimen jurídico y procedimiento administrativo: Afianzamiento de la administración electrónica en las relaciones internas de la administración y con los ciudadanos. In R. (.). Rivero Ortega, M. D. (.). Calvo Sánchez & M. M. (.). Fernando Pablo (Eds.), *Instituciones de procedimiento administrativo común: Novedades de la ley 39/2015 del procedimiento administrativo común de las administraciones públicas* (1st ed., pp. 43-66) Juruá.

NORMATIVA

Constitución Española De 1978, BOE n. 311, de 29/12/1978 (1978). Obtenido de <https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>

Ley 30/1992, De 26 De Noviembre, De Régimen Jurídico De Las Administraciones Públicas y Del Procedimiento Administrativo Común (LRJAP), BOE, n. 285, 27 de noviembre, pp. 40300-40319 (1992). Obtenido de <http://www.boe.es/buscar/doc.php?id=BOE-A-1992-26318>

Real Decreto 263/1996, De 16 De Febrero, Por El Que Se Regula La Utilización De Técnicas Electrónicas, Informáticas y Telemáticas Por La Administración General Del Estado, BOE n. 52, de 29 de febrero, pp. 7942-7946 (1996). Obtenido de <https://www.boe.es/buscar/doc.php?id=BOE-A-1996-4594>

Ley 59/2003, De 19 De Diciembre, De Firma Electrónica (LFE), BOE, n. 304, de 20 de diciembre, pp. 45329-45343 (2003). Obtenido de <https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399>

Ley 11/2007, De 22 De Junio, De Acceso Electrónico De Los Ciudadanos a Los Servicios Públicos (LAECSP), BOE, n. 150, 23 de junio, pp. 27150-27166. (2007). Obtenido de http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352

Real Decreto 3/2010, De 8 De Enero, Por El Que Se Regula El Esquema Nacional De Seguridad En El Ámbito De La Administración Electrónica (ENS), BOE, núm. 25, de 29 de enero, pp. 8089-8138 (2010). Obtenido de <http://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330>

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), BOE, n. 25, 29 de enero, pp. 8139-8156 (2010). Obtenido de <http://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331>

Resolución De 28 De Junio De 2012, De La Secretaría De Estado De Administraciones Públicas, Por La Que Se Aprueba La Norma Técnica De Interoperabilidad De Política De Gestión De Documentos Electrónicos, BOE, n. 178, 26 de julio, pp. 53776-53780 (2012). Obtenido de

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2012-10048

Ley 39/2015, De 1 De Octubre, Del Procedimiento Administrativo Común De Las Administraciones Públicas (LPAC), BOE, n. 236, de 2 de octubre, pp. 89343-89410 (2015). Obtenido de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10565

Ley 40/2015, De 1 De Octubre, De Régimen Jurídico Del Sector Público (LRJSP), BOE n. 236, de 2 de octubre, pp. 89411-89530 (2015). Obtenido de http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10566

Real Decreto 951/2015, De 23 De Octubre, De Modificación Del Real Decreto 3/2010, De 8 De Enero, Por El Que Se Regula El Esquema Nacional De Seguridad En El Ámbito De La Administración Electrónica, BOE n. 264, de 4 de noviembre, pp. 104246-104267 (2015). Obtenido de <http://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881>

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 (eIDAS), (2014). Obtenido de <https://www.boe.es/doue/2014/257/L00073-00114.pdf>

RECURSOS WEB

Almonacid Lamelas, V. (2016). Blog de Víctor Almonacid. Consultado el 15/11/2016, en <https://nosoloaytos.wordpress.com/>

Centro Criptológico Nacional. (2016). *800 guías esquema nacional de seguridad*. Consultado el 15/11/2016, en <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html>

Cuerpo Nacional de Policía. (2016). Portal del DNI electrónico. Consultado el 15/11/2016, en <https://www.dnielectronico.es>

Ernst & Young. (2011). *ESQUEMA NACIONAL DE SEGURIDAD: Guía para responsables*. Consultado el 15/11/2016, en https://www.pozuelodealarcon.org/recursos/doc/Vivir_Pozuelo/NNTT/Ponencias_Servicios_Cloud/10967_31103110201112387.pdf

Gamero Casado, E. (2015). La administración electrónica y la nueva ley 39/2015 del procedimiento administrativo común. Consultado el 15/11/2015, en <http://www.uco.es/coseg/documentos/admon-electr-ley-39-2015.pdf>

Gamero Casado, E. (2016). Obligaciones de administración electrónica y transparencia. Consultado el 15/11/2016, en [http://www.dipalme.org/Servicios/Fiestas/Fiestas.nsf/CE9BB965E6EB10AEC1257F53002899FC/\\$file/20160222%20Gamero-Dipalme-%20Obligaciones%20admon%20electronica.pdf](http://www.dipalme.org/Servicios/Fiestas/Fiestas.nsf/CE9BB965E6EB10AEC1257F53002899FC/$file/20160222%20Gamero-Dipalme-%20Obligaciones%20admon%20electronica.pdf)

Gobierno de España. (2016). Cl@ve identidad electrónica para las administraciones. Consultado el 15/11/2016, en http://clave.gob.es/clave_Home/clave.html

Ministerio de Hacienda y Administraciones Públicas. (2016). Portal de administración electrónica. Consultado el 15/11/2016, en <http://administracionelectronica.gob.es/>

Ministerio de industria, energía y turismo. (2016). *Lista de confianza de*

prestadores de servicios de certificación (TsL). Consultado el 15/11/2016, en <https://sede.minetur.gob.es/Prestadores/Paginas/Inicio.aspx>

Real Casa de la Moneda - Fábrica Nacional de Moneda y Timbre. (2016). *Declaraciones, políticas y prácticas de certificación de la fábrica nacional de moneda y timbre - real casa de la moneda*. Consultado el 15/11/2016, en <https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion>

Secretaría de Estado de Administraciones Públicas. (2016). *Normas técnicas de interoperabilidad*. Consultado el 15/11/2016, en https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#.WCrY93XhA_5

Serrano Delgado, F. (2010). *Administración electrónica*. Consultado el 15/11/2016, en <http://es.slideshare.net/fserrano/administracin-electrnica-1-historia-share>;