



**UNIVERSIDAD CARLOS III DE MADRID
ESCUELA POLITÉCNICA SUPERIOR**

INGENIERÍA INFORMÁTICA

PROYECTO FIN DE CARRERA

Análisis de la eAdministración e identificación de criterios
auditables para la evaluación del grado de implantación.

Autores: **Antonio Sánchez Rosales**
Tutor: **Miguel Ángel Ramos González**

Mayo, 2012

**Análisis de la eAdministración e identificación de criterios auditables para la
evaluación del grado de implantación**

Para Blanca.
Por Sofía.

Gracias a mi mujer, a mi hija y a mi familia por ser como son y saber apoyarme cuando me hace falta.

Gracias a Sergio y a otros compañeros por estos años irrepetibles.



Título: Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación.

Autor: Antonio Sánchez Rosales

Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 25 de Mayo de 2012 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO

PRESIDENTE

ÍNDICE

1	INTRODUCCIÓN Y OBJETIVOS.....	9
1.1	Motivación del proyecto.....	9
1.2	Objetivo del proyecto.....	9
1.3	Estructura del documento.....	10
2	ESTADO DEL ARTE.....	12
2.1	Nuevas tecnologías de información en la Administración Pública.....	16
2.1.1	Administración electrónica.....	17
2.1.2	Modernización de la Administración Pública.....	19
2.1.3	Conceptualización de la gestión.....	20
2.2	La calidad como factor competitivo.....	22
2.2.1	Entorno competitivo de la Administración Pública.....	23
2.2.2	ISO 27002.....	24
2.2.3	Accesibilidad Web.....	25
3	MARCO LEGAL EN ESPAÑA.....	33
3.1	Evolución de los Ayuntamientos en España.....	33
3.2	Previsiones comunitarias sobre la sociedad de la información.....	35
3.3	La Ley 11/2007.....	40
3.3.1	Antecedentes a la Ley 11/2007.....	40
3.3.2	Desarrollo reglamentario de la Ley 11/2007.....	42
3.4	Real Decreto 1671/2009 de 6 de noviembre.....	42
3.5	Real Decreto 3/2010 de 8 de enero.....	45
3.6	Real Decreto 4/2010 de 8 de enero.....	46
3.7	LAECSP.....	50
3.8	Adaptación de procedimientos a la LAECSP.....	55
3.8.1	Requerimientos de adaptación a la LAECSP.....	55
3.9	Ley 59/2003.....	56
3.10	Derechos y obligaciones.....	58
3.10.1	Derechos de los ciudadanos.....	58
3.10.2	Obligaciones de los Ayuntamientos.....	62
3.10.3	LOPD.....	78
3.11	Conexión entre LAECSP y LOPD.....	79
3.12	Reglamento de desarrollo de la Ley Orgánica 15/1999.....	82
3.13	Ley 56/2007.....	83
3.14	Escenarios para el cumplimiento de la Ley.....	84
3.15	Ordenanza reguladora de la eAdministración.....	85
3.16	Ley 17/2009, 23 de noviembre.....	88
3.17	Ley 25/2009, de 22 de diciembre.....	89
3.18	Plan Avanza.....	90
3.18.1	Origen y primeros años.....	90
3.18.2	Ejes de actuación y objetivos de Avanza y Avanza 2.....	91
3.18.3	Estrategia 2011-2015 del Plan Avanza 2.....	93
4	TIPOS DE RELACIONES CON LA EADMINISTRACIÓN... 	95
4.1	Los usuarios de los nuevos servicios administrativos.....	96
4.2	Características de los nuevos servicios administrativos.....	97
4.3	Información a la carta.....	98
4.3.1	Sede electrónica.....	98
4.3.2	Registro telemático.....	101
4.3.3	Notificaciones.....	104



4.3.4	Tablón de anuncios	106
4.3.5	Firma del personal al servicio de las AAPP	107
4.3.6	Habilitación de funcionarios.....	108
4.3.7	Habilitación de terceros	109
4.3.8	Gestión documental	110
4.4	Servicios Centrados en el Ciudadano	122
4.4.1	La Ventanilla Única	122
4.4.2	Las plataformas de llamada	123
4.4.3	Los puntos automáticos de consulta y gestión	124
4.4.4	Las cartas de servicios.....	124
4.4.5	Encuestas de satisfacción	125
4.4.6	Sistema de sugerencias y reclamaciones	126
4.4.7	Carta de derechos del ciudadano.....	126
4.4.8	El defensor del ciudadano	126
5	IDENTIFICACIÓN ELECTRÓNICA.....	127
5.1	La firma electrónica	127
5.1.1	El certificado digital	129
5.1.2	Gestión de certificados. consulta, emisión y revocación.	130
5.1.3	Tipos de certificados	131
5.1.4	Tipos de ficheros de certificados más importantes.....	132
5.2	DNI Electrónico	133
5.2.1	Características	133
5.2.2	DNI Electrónico en España.....	137
5.2.3	Cómo Obtener El DNI Electrónico.....	139
5.2.4	Requisitos para utilizar el DNI electrónico	139
5.2.5	Servicios disponibles con el DNI-e	140
5.2.6	Marco legal.....	143
5.2.7	Autoridades de validación	144
5.2.8	La autoridad de certificación e infraestructuras PKI	145
5.2.9	Infraestructuras de clave pública (PKI).....	146
5.2.10	Usos de la tecnología PKI	147
5.2.11	Seguridad	148
5.3	Comunicación con la Administración.....	152
5.3.1	Uso de los certificados	153
5.3.2	Problemas típicos.....	185
6	PROYECTOS DESTACADOS EN ESPAÑA	193
6.1	Administración Electrónica Estatal y Organismos Oficiales.....	194
6.1.1	Oficina Virtual de La Agencia Tributaria	194
6.1.2	La experiencia de la FNMT-RCM	200
6.1.3	La experiencia del INE	210
6.1.4	Portal 060	220
6.1.5	La Red SARA.....	223
6.1.6	@Firma	236
6.1.7	CITA	240
6.1.8	Portal CIRCE.....	242
6.1.9	El Consejo Superior de Administración Electrónica	244
6.2	eAdministración en Comunidades Autónomas y Diputaciones	244
6.2.1	Diputación de Almería	244
6.2.2	Generalitat Valenciana	249
6.3	eAdministración en las Entidades Locales	254

6.3.1	Ayuntamiento De Madrid	254
6.3.2	Ayuntamiento de Leganés.....	260
7	EADMINISTRACIÓN SIN USAR FIRMA ELECTRÓNICA...	266
7.1	Introducción.....	266
7.2	Concepto de Web 2.0.....	267
7.3	Administración 2.0.....	268
7.4	Blogs	269
7.4.1	Blogs y política	270
7.5	Wikis.....	270
7.5.1	Las Wikis en las Organizaciones.....	271
7.5.2	La Wikis en la Administración Pública.....	272
7.6	Redes sociales.....	272
7.6.1	Redes sociales en la Administración Pública	273
7.6.2	Redes sociales en la política.....	273
7.7	Marketing viral.....	275
7.7.1	Aplicaciones y ventajas en las Administraciones Públicas....	276
8	IDENTIFICACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL GRADO DE IMPLANTACIÓN.....	279
8.1	Análisis de la Ley 11/2007.....	279
8.1.1	Análisis por artículos	280
8.1.2	Análisis en función de ámbitos.....	282
8.2	Implementación de servicios on-line desde la Administración.....	295
9	CONCLUSIONES	303
9.1	Introducción.....	303
9.2	Las TIC.....	304
9.3	Europa.....	306
9.4	España	306
9.5	Administración Electrónica	307
9.6	Tendencias.....	308
9.7	Aportación	310
9.8	Líneas futuras.....	311
10	PRESUPESTO.....	312
10.1	Introducción.....	312
11	GLOSARIO	315
12	Bibliografía.....	319
12.1	Libros.....	319
12.2	Revistas.....	320
12.3	Informes corporativos y congresos.....	320
12.4	Normativa.....	320
12.5	Páginas o documentos electrónicos en la red	321
13	ANEXO	324
13.1	Estadísticas Presentadas por Internet en la AEAT.....	324
14	REFERENCIAS.....	326



GALERÍA DE IMÁGENES

Imagen 2-1 Tabla evolución del uso de Internet.....	13
Imagen 2-2 Gráfica tiempos de conexión a Internet.....	14
Imagen 2-3 Consultas en Internet.....	15
Imagen 2-4 Gráfica de consultas por Internet.....	16
Imagen 3-1 Estados para cumplir con LAECSP.....	84
Imagen 3-2 Artífices de la elaboración del Plan Avanza.....	91
Imagen 3-3 Ejes de actuación del primer Plan Avanza.....	92
Imagen 3-4 ejes de actuación y objetivos del Plan Avanza 2.....	93
Imagen 5-1 Generación y validación.....	129
Imagen 5-2 DNle.....	136
Imagen 5-3 Almacén de certificados.....	147
Imagen 5-4 Certificado digital.....	154
Imagen 5-5 Evolución de los certificados digitales en Cataluña.....	157
Imagen 5-6 Almacén de entidades emisoras.....	160
Imagen 5-7 Opciones de protección de acceso a la clave privada.....	161
Imagen 5-8 BOE firmado electrónicamente.....	164
Imagen 5-9 Servicio de validación y firma electrónica online VALIDE.....	168
Imagen 5-10 Verificación del certificado digital a través de la FNMT.....	169
Imagen 5-11 Servicio de verificación online del código seguro de verificación de la AEAT....	170
Imagen 5-12 Ventana emergente al firmar un documento, solicitando la clave privada.....	171
Imagen 5-13 Formato PDF preparado para firmar.....	172
Imagen 5-14 PDF firmado.....	173
Imagen 5-15 Cuadro de diálogo que muestra Word 2003 para insertar una firma digital.....	174
Imagen 5-16 Documento firmado en Word.....	174
Imagen 5-17 Contrato de entidad certificadora.....	176
Imagen 5-18 Configuración firma digital en Outlook 2003.....	177
Imagen 5-19 Botones para enviar emails certificados en Outlook 2003.....	178
Imagen 5-20 Ejemplo de trámite on-line.....	180
Imagen 5-21 Cifrado de un fichero con <i>AxCrypt</i>	183
Imagen 5-22 Configuración en Outlook 2003 para enviar correo cifrado.....	185
Imagen 5-23 Mensaje para la instalación de una firma digital en el navegador.....	186
Imagen 5-24 Certificado digital caducado.....	188
Imagen 5-25 Ejemplo de acceso no reconocido por el navegador Mozilla Firefox.....	189
Imagen 5-26 Intento de acceso a una Web que solicita certificado.....	190
Imagen 5-27 Análisis de uso de navegadores Web agosto 2011.....	191
Imagen 5-28 Análisis, con versiones, de navegadores Web, agosto 2011.....	192
Imagen 6-1 Servicios para ciudadanos que ofrece la Agencia Tributaria.....	195
Imagen 6-2 Arquitectura de los servicios a través de Internet de la AEAT.....	197
Imagen 6-3 <i>Registro electrónico en el Portal de la AEAT</i>	198
Imagen 6-4 Esquema fechado temporal antes.....	203
Imagen 6-5 Esquema fechado temporal después.....	203
Imagen 6-6 Ejemplo de Notificación.....	209
Imagen 6-7 Evolución de recibidos ARCE sobre total recibidos por mes de referencia.....	214
Imagen 6-8 Intercambio de Ficheros IDA_Padrón.....	218
Imagen 6-9 Intercambio de Registros IDA_Padrón.....	218
Imagen 6-10 .Esquema Funciona.....	219
Imagen 6-11 Accesos registrados del SVDR y del SCDP-CGPJ.....	220
Imagen 6-12 Portal de la red 060.....	221
Imagen 6-13 Estructura de la red SARA.....	224
Imagen 6-14 Formulario para conexión Site to Site.....	232
Imagen 6-15 Esquema conexión Red SARA.....	234
Imagen 6-16 Estructura de la Plataforma @Firma.....	236
Imagen 6-17 Solicitud para integrarse con @Firma.....	239
Imagen 6-18 Ilustración 6-9 Esquema Plataforma Avanza Local.....	241
Imagen 6-19 Esquema de CITA.....	241
Imagen 6-20 Esquema del SIGTE de la Generalitat Valenciana.....	251
Imagen 7-1 Twitter de A. Rubalcaba.....	274

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Imagen 7-2 Perfil de Facebook de Mariano Rajoy.....	275
Imagen 9-1 Implantación eGovernment.....	309
Imagen 13-1 Estadísticas Presentadas por Internet en la AEAT.....	324

TABLAS

Tabla 1 – Uso de firma electrónica por Internet.....	152
Tabla 2 - Descripción de los Derechos y Exigencias por artículos de la Ley 11/2007	282
Tabla 3 – Tabla ejemplo resumen Ley 11/2007.....	283
Tabla 4 – Valores eEurope.....	295
Tabla 5 – Valores de criterios pasados a letras.....	301
Tabla 6 – Tabla de valores por CCAA	302
Tabla 7 – Tabla de valores por servicio	304
Tabla 8 – Tabla nivel adaptación Europea.....	308



1 INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación del proyecto

El proyecto que esta leyendo es fruto de la idea de ayudar a compañeros de profesión a adaptarse lo más rápidamente a las necesidades profesionales que puede suponer un nuevo proyecto con la Administración Pública.

Debido a la experiencia y contada por compañeros de profesión, en el mercado laboral abundan empresas que subcontratan servicios y que en función del proyecto firmado con la empresa, uno puede acabar desarrollando software para distintos ámbitos.

Como profesionales de la informática, no tenemos ninguna limitación para cualquier proyecto software que debamos abordar. Pero, con respecto al conocimiento extra-profesional que se nos exige, no hay otro recurso que poner de nuestra parte tiempo y esfuerzo en asimilar lo más rápidamente el contexto informativo que conlleva el desarrollo de dicho proyecto. Nadie sabe de todo.

A raíz de este objetivo, surgieron otros, como por ejemplo: identificar criterios que fueran medibles o evaluables para todas la Comunidades Autónomas, poder evaluar para un Organismo Público su estado de adaptación a la Administración electrónica y proponer medidas de adaptación a la eAdministración en función del grado de adaptación en el que se encuentre el organismo evaluado.

1.2 Objetivo del proyecto

Este proyecto está enmarcado en un estudio, análisis, medición y recomendaciones para que un organismo público sea capaz de medir su grado de adaptación a la Administración electrónica, del cual se generan dos proyectos.

- Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación.
- Propuesta de herramienta para la evaluación del grado de implantación de la eAdministración en CCAA.

La lectura de cada proyecto por separado dejaría incompleta cualquier parte de ellas. La lectura lógica en primer lugar es la del *Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación*, para continuar con el proyecto *Propuesta de herramienta para la evaluación del grado de implantación de la eAdministración en CCAA*.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

A partir de ahora, el contenido de este proyecto únicamente se centrará en el *Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación*.

Con este proyecto se pretende realizar un análisis que sea referencia en cuanto a la eAdministración en las Administraciones Públicas (AAPP). El objetivo es realizar un análisis de la evolución en la implantación de la eAdministración desde sus orígenes al momento actual, persiguiendo dos fines:

- que cualquier persona necesitada de información sobre la eAdministración, pueda leer este trabajo y conseguir el conocimiento que busca y utilizarlo como un manual de referencia.
- Identificar, mediante el análisis realizado, una serie de criterios que permitan evaluar el grado de implantación de la eAdministración en las AAPP.

El presente documento ofrece una información muy completa del marco legal entorno a la eAdministración, así como las relaciones más representativas de los procedimientos telemáticos actuales, aclara dudas sobre la Firma Electrónica y da a conocer algunos de los proyectos de Organismos Públicos (OOPP) que ya están implantados y en funcionamiento, cómo se ha llegado a ellos y hacia dónde irán evolucionando en el futuro.

Además se ha elaborado un análisis concreto de la principal ley en la eAdministración, la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, esquematizada por principales artículos y por áreas. Se incluye la escala europea para medir la integración de la Administración Electrónica en los OOPP, y el resultado obtenido durante los últimos años a nivel nacional, obteniendo una serie de criterios que en futuros proyectos podrán servir para crear una aplicación que audite el estado de la eAdministración.

1.3 Estructura del documento

El primer gran bloque que el lector de este proyecto se va a encontrar es un estudio del marco legal en España sobre las leyes y Reales Decretos por los cuales se regirán las AAPP a la hora de evolucionar a la eAdministración. Podrá leer cómo a raíz de la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP), se han desarrollado nuevas reglamentaciones necesarias para dar sentido a dicha ley, creando derechos y deberes de las Administraciones Públicas con ellas mismas y con los ciudadanos.

Una vez situado en un contexto legal se analizan las Administraciones Públicas y su relación con los ciudadanos, así como los servicios que las Administraciones Públicas ofertan actualmente al ciudadano mediante comunicación electrónica. Para poder realizar tal comunicación, primero es



necesaria una identificación electrónica, mediante los certificados digitales y el DNI electrónico (DNle), la cual también se analiza en este trabajo.

Identificados los servicios prestados vía electrónica se presentan las herramientas de comunicación disponibles para que el ciudadano pueda acceder a dichos servicios.

Definidos los servicios electrónicos ofertados por las administraciones y las herramientas que permiten acceder a ellos, se realiza un análisis de éstos para determinar las necesidades de seguridad y calidad necesarias para establecer una relación electrónica satisfactoria, eficaz y eficiente entre el ciudadano y las Administraciones Públicas.

Ya situados en el marco legal, y en conocimiento del estado real de la eAdministración y de cómo los ciudadanos pueden interactuar con su Administración, se presentan diferentes ejemplos reales de casos de eAdministración. Este análisis de la realidad abarca desde Organismos Estatales hasta Administraciones Locales.

A continuación se estudian y analizan alternativas para las gestiones que no requieran una identificación digital por parte del ciudadano.

Una vez estudiado el contexto de la eAdministración y habiendo presentado desde todos los puntos de vista posibles, se recopila dicha información y se sintetiza en una serie de tablas y valores que hará medible la adaptación a la eAdministración, sirviendo estos datos como base para crear un sistema de gestión del conocimiento que permita evaluar el nivel de implantación de la Administración electrónica en los Organismo Públicos.

Para concluir el proyecto, se completa el estudio con una serie de conclusiones y una propuesta de posibles vías futuras sobre el ámbito que se trata en el documento.

2 ESTADO DEL ARTE

El continuo cambio en las tecnologías de la información y el rápido crecimiento y expansión que éstas han tenido en los últimos años han cambiado totalmente nuestra forma de vida. La rápida evolución que se ha producido en este sector ha modificado radicalmente nuestra manera de trabajar y nuestra forma de relacionarnos.

En el ámbito empresarial el cambio ha sido enorme. Nadie imagina a día de hoy un puesto de trabajo consistente en una mesa y una máquina de escribir. La introducción dentro de las empresas de ordenadores personales, servidores de datos, conexión de equipos en red, acceso a Internet, han mejorado la forma de trabajar y la eficacia de las empresas, ofreciendo mejores servicios a sus clientes y permitiendo relaciones más fluidas entre sus filiales y con el exterior, así como la mejora del nivel de vida de sus empleados.

Con el nacimiento de Internet se marca un antes y un después. La red de redes nos ofrece millones de páginas con información, con acceso a servicios que antes no teníamos o que teníamos que realizar de una manera que implicaba traslados, colas, tiempos de espera. Cientos de trámites están al alcance de un solo click de ratón. Así mismo, el correo electrónico nos está permitiendo enviar información y contactar con personas y empresas en cuestión de segundos que están al otro lado del planeta, produciendo una mejoría de las comunicaciones y una forma más profesional, flexible y dinámica de trabajar.

Todo esto es lo que ha dado lugar a la denominada Sociedad de la Información, que no es ni más ni menos que recursos técnicos y humanos que ponen a nuestro alcance la posibilidad de distribución y manipulación de la información.

Para reflejar de forma cualitativa el incremento del uso de Internet en la población española, se muestra a continuación una serie de datos obtenidos de la Asociación para la Investigación de Medios de Comunicación (AIMC).

El primer gráfico muestra el Audiencia de Internet en el EGM durante Febrero 2012¹. Este documento contiene información general sobre la evolución de la audiencia de Internet en el Estudio General de Medios (EGM).

Los porcentajes que muestran en las partes más altas de las barras son el porcentaje con respecto a la población de muestra.

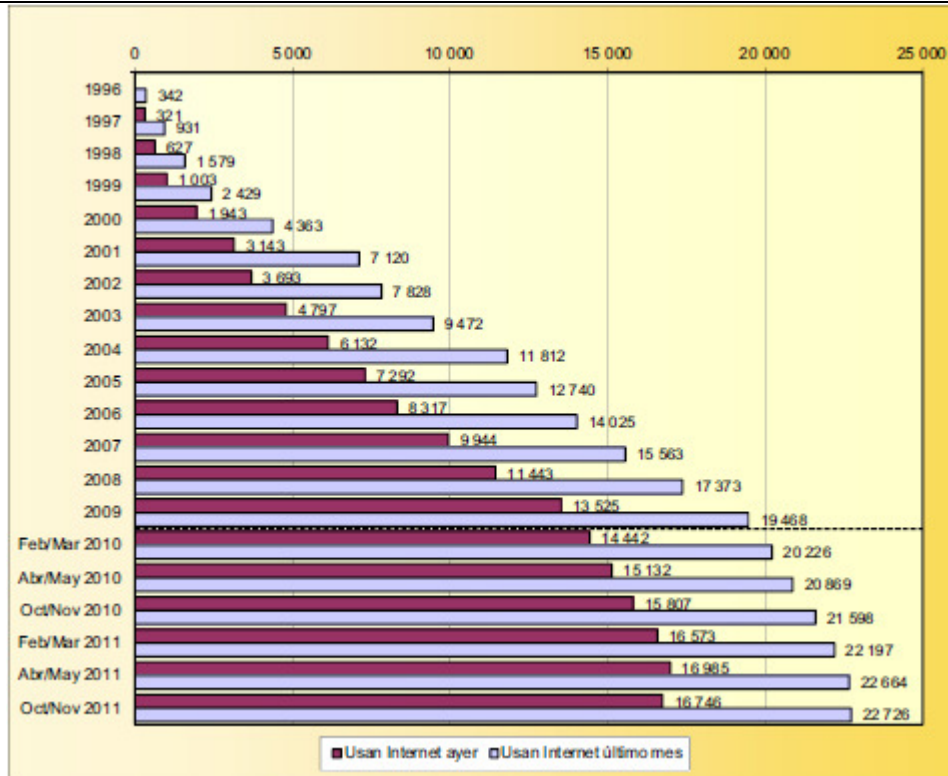


Imagen 2-1 Tabla evolución del uso de Internet

Respecto a la tabla anterior, las en azul más claro, representan los nuevos usuarios que han tenido acceso a Internet.

En la siguiente ilustración se muestra la frecuencia de acceso a Internet catalogado desde los diferentes lugares de acceso. Se constata que desde el hogar y desde la oficina, son los lugares preferidos para conectarse a Internet, además de significativo el número tan alto de veces que lo hacen.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

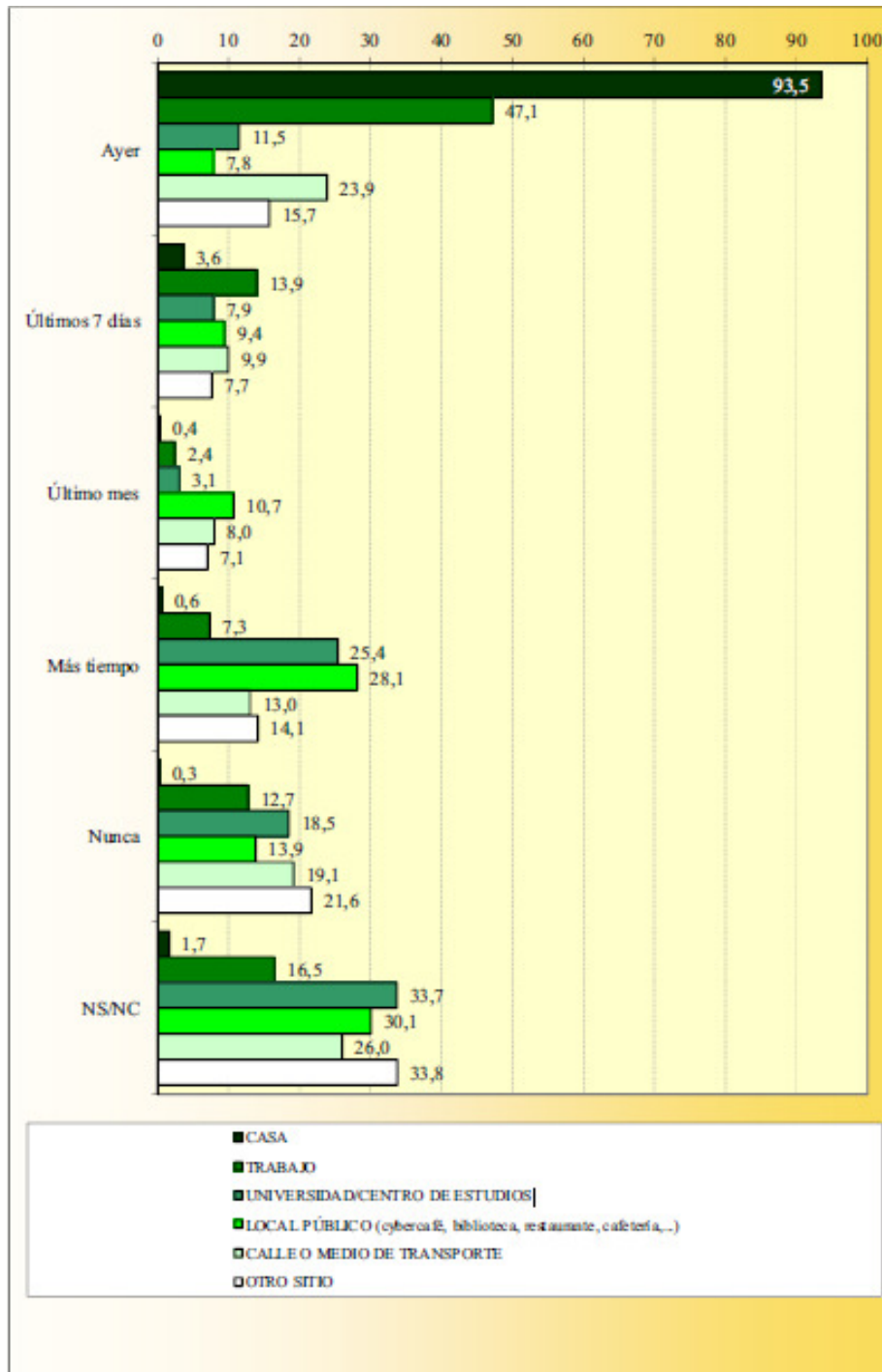


Imagen 2-2 Gráfica tiempos de conexión a Internet

La siguiente tabla muestra las actividades realizadas por Internet de una forma cualitativa. Nótese que la suma de porcentajes es superior al 100% ya que gran parte de informantes declara dos o más respuestas.

Dentro de las 14 primeras actividades que se realizan por Internet figuran las gestiones con las Administraciones Públicas. Eso demuestra el cambio necesario que ya se está produciendo, por parte de las AAPP para poder ser más accesibles a los ciudadanos.

<i>P. Durante los últimos 30 días ¿cuáles de las siguientes actividades ha realizado a través de Internet?</i>		
	Absolutos	%
BASE	34.656	
Lectura de noticias de actualidad	30.781	88,8
Consulta de mapas/callejeros	24.389	70,4
Visualización online vídeos (tipo Youtube)	23.402	67,5
Consulta de previsiones meteorológicas	19.683	56,8
Escuchar música online (sin descargar)	16.755	48,3
Consulta cartelera cine/espectáculos	15.532	44,8
Descarga de software	14.997	43,3
Consulta de información financiera	13.016	37,6
Descarga de películas/series	12.856	37,1
Ver películas/series online (sin descargar)	11.954	34,5
Descarga de música	11.471	33,1
Juegos en Red	10.627	30,7
Ver emisiones de cadenas TV en su web	10.487	30,3
Gestiones con la Administración	10.215	29,5
Búsqueda de cursos, masters, formación	9.869	28,5
Visitas a páginas web para "adultos"	9.313	26,9
Buscar información temas de salud	9.026	26,0
Búsqueda de empleo	8.614	24,9
Videoconferencia/Videollamada	7.818	22,6
Realizar una encuesta	7.108	20,5
Apuestas (deportivas, casinos, loterías...)	6.392	18,4
Trabajar en casa conectado al trabajo	6.233	18,0
Descarga de libros electrónicos	6.026	17,4
Recibir información/noticias con RSS	5.351	15,4
Buscar vivienda (compra, alquiler,...)	5.247	15,1
Adquisición de cupones descuento	5.072	14,6
Descarga programa radio para oír después	4.917	14,2
Consulta de información sobre tráfico	3.295	9,5
Descarga emisiones tv para ver después	3.189	9,2
Búsqueda de pareja	1.591	4,6

Imagen 2-3 Consultas en Internet

Ahora se muestran los mismos datos pero de forma gráfica.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

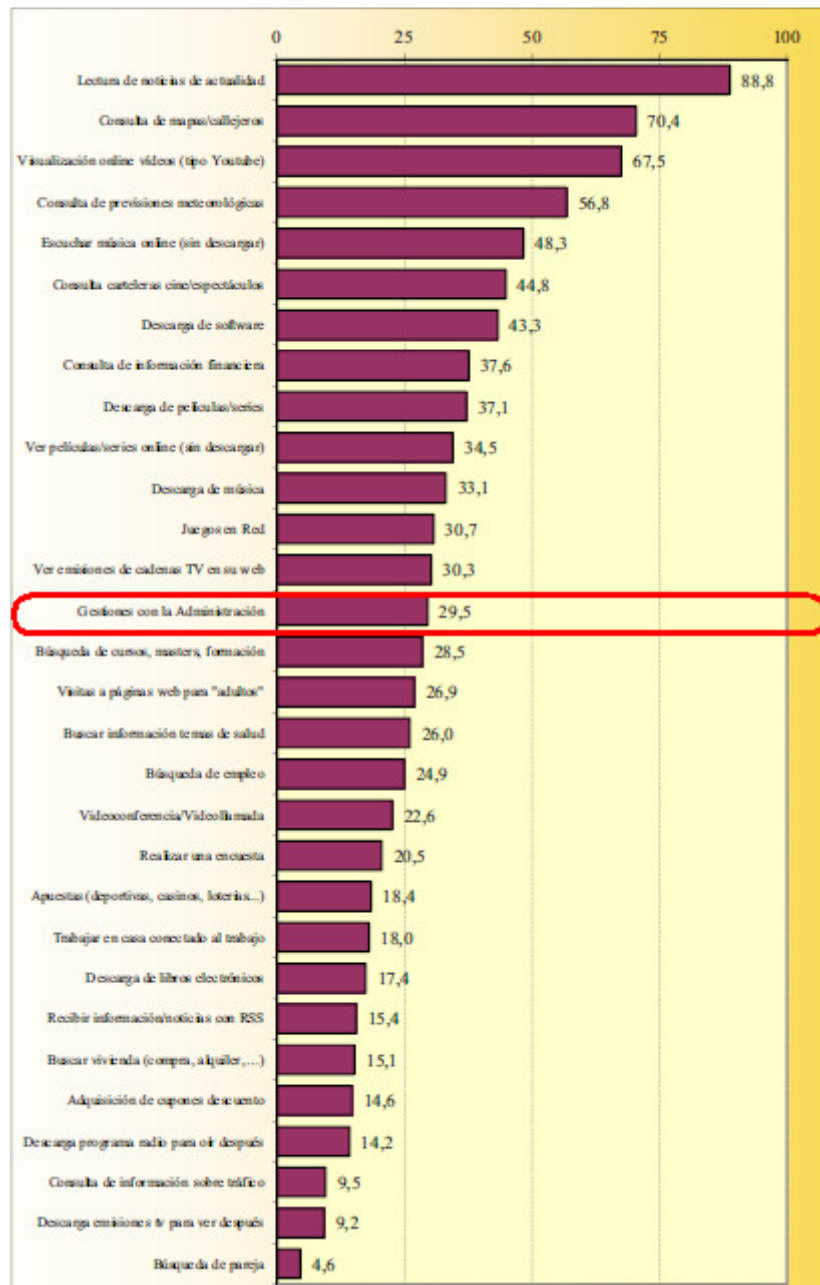


Imagen 2-4 Gráfica de consultas por Internet

2.1 Nuevas tecnologías de información en la Administración Pública

En el siglo XXI, ya se puede decir que ha llegado el momento de modernizar la Administración Pública. Los gobiernos se han puesto manos a la obra para poder adecuarse a las nuevas tecnologías y aceptar el medio que el ciudadano usa, desde hace tiempo, para comunicarse, es decir Internet. Con esta adaptación aparece la Administración Electrónica o eAdministración, debido a la relación electrónica que se establece entre ciudadano y Administración.



Se trata de uno de los cambios más importantes en la historia de las Administraciones Públicas (AAPP), debido a la magnitud del cambio al cual aspira. Tiene influencias en todo el proceso administrativo y hace frente a cuestiones aún hoy sin solucionar, tan relevantes como la brecha digital en los ciudadanos e incluso en las propias AAPP.

2.1.1 Administración electrónica

La Unión Europea ha definido la Administración electrónica como “el uso de las Tecnologías de la Información y las Comunicaciones (TIC) en las Administraciones Públicas, unido a cambios en la organización, con el propósito de mejorar los servicios públicos y los procesos democráticos, y de reforzar el apoyo a las políticas públicas”ⁱⁱ.

La Administración electrónica se refiere a cualquier mecanismo que transforma las oficinas tradicionales, convirtiendo los procesos en papel, en procesos electrónicos, con el fin de crear una oficina virtual, sin papeles. Es decir, es el conjunto de soluciones que las Administraciones Públicas y Organismos dependientes ponen a disposición de los ciudadanos para que puedan acceder a sus servicios públicos a través de medios electrónicos. La administración electrónica alcanza tanto a las comunicaciones internas de una oficina como a las comunicaciones entre oficinas de diferentes organizaciones.

En los últimos años, Internet se ha convertido en una herramienta muy importante e imprescindible para las empresas y ciudadanos por muchas y diferentes razones. Una de las consecuencias más evidentes son las tramitaciones y gestiones de las empresas (y particulares) con la Administración Pública (Seguridad Social, Agencia Tributaria, etc.).

Ya en diciembre del año 2002 el Gobierno aprobó un Real Decreto por el que se podían aumentar las posibilidades de realizar operaciones de carácter tributario a través de Internet para agilizar las relaciones de la Administración con los contribuyentes.

Aunque es en el año 2000 cuando se empieza a extender de forma generalizada el acceso electrónico de los servicios públicos para ciudadanos y empresas, es a partir del año 2004 cuando se produce el mayor impulso para modernizar tecnológicamente las Administraciones Públicas, mejorando servicios ya existentes y creando nuevos como la red 060 que pone al alcance de ciudadanos y empresas la totalidad de servicios electrónicos de todas las Administraciones.

Actualmente existe una Ley que dice que la Administración General del Estado deberá ser totalmente electrónica en el año 2013 y regula el derecho de todos los ciudadanos a relacionarse electrónicamente con las administraciones públicas, así como la obligación de estas a garantizarlo. Por lo tanto, en los últimos años la Administración sigue apostando por el uso de las Nuevas Tecnologías.

La Administración también avanza en torno al imparable fenómeno de Internet. Un claro ejemplo es la Agencia Estatal de Administración Tributaria donde la disponibilidad de los servicios electrónicos es prácticamente total y probablemente sean de los más conocidos por el ciudadano, creciendo de manera importante todos los años los servicios en Internet relacionados con la declaración de impuestos tanto para particulares como para empresas. También la oficina virtual del catastro, puesta en marcha en el año 2003, que dispone de un sistema cartográfico de acceso a la información para evitar que las Administraciones tengan que pedir los datos a los ciudadanos, es otro ejemplo de este progreso.

En definitiva, casi sin darnos cuenta, se ha pasado en unos años de tener que desplazarnos a la administración correspondiente para hacer algún trámite, hacer colas para recoger un formulario, en muchos casos, llevarlo a casa o a la empresa para reunir la información necesaria, cumplimentarlo y volver otro día para entregarlo, a una Administración proactiva donde, gracias al intercambio de información entre las diferentes Administraciones, el ciudadano simplemente tiene que confirmar los datos que la Administración le da o si se ha producido algún cambio.

Para la puesta en marcha de la Administración Electrónica, es necesario cambiar la mentalidad tradicional en la que la organización es el centro de atención, ahora el centro de atención pasa a ser el cliente, éste es el centro de todas las actividades de la organización.

Para lograr estos objetivos es necesario introducir sistemas transparentes de trabajo, eliminando la dependencia específica de personas para realizar las diferentes tareas.

La Administración Electrónica se ha visto impulsada por la aparición de las tecnologías de la información y comunicación (teléfono, Internet, televisión digital terrestre...), facilitando a los clientes la interacción con las organizaciones y a los trabajadores flexibilizando y mejorando las condiciones de trabajo (flexibilidad horaria, teletrabajo, movilidad...).

Las ventajas que ofrece la Administración Electrónica a los clientes de las organizaciones son:

- Disponibilidad

Se puede interactuar con las organizaciones las 24 horas del día (por teléfono con servicios de atención telefónica o por Internet a través de oficinas virtuales). No es necesario ceñirse a un horario de oficinas. Ya no existen los días festivos.

- Facilidad de acceso

Ya no es necesario acudir a la oficina presencial de la organización para realizar las gestiones, se puede hacer desde cualquier parte del mundo a través del teléfono o Internet. Las oficinas están disponibles para los usuarios en cualquier lugar.



- **Ahorro de tiempo**

Para realizar una gestión se puede efectuar desde casa o cualquier lugar que deseemos, sin la necesidad de tener que desplazarse a la oficina presencial, esperar una cola para ser atendido, la atención (explicación de lo que se desea realizar y realización de dicha actividad), y el regreso a casa.

En España la Agencia Tributaria fue pionera en la puesta en marcha de la Administración Electrónica. Actualmente diferentes Administraciones Públicas están desarrollando la eAdministración dentro de programas de mejora y prácticamente todos los organismos disponen de oficinas virtuales en las que ofrecen información y trámites por vía electrónica.

2.1.2 Modernización de la Administración Pública

Todas las organizaciones necesitan estabilidad y continuidad, al tiempo que adaptación e innovación, es decir, necesitan un cambio continuo porque son sistemas abiertos que han de estar en una constante interacción con el medio en que realizan su acción.

Se sabe que los individuos cambian con la educación y la experiencia. No obstante, estos cambios individuales no siempre llevan al cambio de las organizaciones en las que se integran. El cambio organizacional, requiere de otros elementos o factores que pasan por:

- La necesidad de renovación o no de lo que debe permanecer dentro del conjunto de valores de la organización.
- Una adaptabilidad a los fines que, como los de las personas, son cambiantes con el tiempo, así como los medios utilizados para su consecución.
- La necesidad de una estabilidad en todo proceso de cambio, es decir, encontrar un equilibrio entre estabilidad y adaptación, que se presenta como fundamental para la supervivencia y el crecimiento de la organización.

Aparte de la necesidad de cambio que opera en las organizaciones, debido a la continua interacción con el medio que les rodea, existen otros aspectos que mueven a las organizaciones a cambiar:

- El medio en que realizan su gestión, que generalmente es la sociedad, la cual introduce factores y necesidades de forma vertiginosa, que reclaman nuevas actitudes o comportamientos.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Los diferentes objetivos y valores que van a modificarse y consecuentemente, a introducir nuevas metas que, a su vez, requieren una nueva estrategia organizacional para su consecución.
- El elemento técnico, considerado como el conjunto de nuevos métodos o tecnología que incorporados a la misma, ofrezcan unos “productos” más acordes con las exigencias de la sociedad.
- El aspecto humano es el que en definitiva llevará el impulso del cambio a las organizaciones. Por lo tanto, la habilidad de la organización y de sus administradores para dirigir o influir en la conducta de sus recursos humanos será un factor crítico de éxito en el cambio organizacional.

Pero los procesos no siempre ocurren con la aparente facilidad manifestada, sino más bien, al contrario. Existen factores que van a dificultar el proceso de cambio en una organización, factores que se deben determinar y posteriormente, amortiguar con la metodología adecuada. Podríamos establecer, entre otros, como factores que ofrecen resistencia al cambio los siguientes:

- La existencia de actitudes, que basadas en factores como el tiempo, la energía o el dinero que provocará el cambio, rechazan el mismo. Factores que vienen a defender la situación actual vigente. Normalmente estas actitudes están relacionadas con las responsabilidades profesionales dentro de la organización y con la edad de quienes las ejercen.
- La falta de comunicación dentro de la organización constituye otro factor negativo de los procesos de cambio. Si los individuos no perciben claramente el objetivo o las consecuencias del cambio, lo más probable es que se resistan a él. Por el contrario si participan en la aplicación del proceso de cambio es posible que entiendan el por qué se está realizando el mismo y favorezcan su consecución.

En cualquier caso, de lo que se trata es de superar esa resistencia natural a los cambios que pueden producirse en una organización y, para ello, los responsables deben saber que han de anticiparse a las posibles reacciones negativas de los individuos. Unas reacciones que serán diferentes, según sean los cambios previstos o, incluso, según se perciban por los mismos. Para esto, el único camino posible es implicar a todos los individuos de la organización en la consecución de la meta, es decir, en conseguir su compromiso de participación en el cambio a fin de que la resistencia tenga el menor efecto posible, y para ello, solo existe la comunicación amplia con todos los miembros de la organización, una comunicación realista y sincera con las probabilidades de mejoras que el proceso de cambio traerá a toda la organización.

2.1.3 Conceptualización de la gestión

La gestión pública de las administraciones puede ser conceptualizada como la aplicación de aquellos recursos necesarios para alcanzar los objetivos públicos



socialmente deseados y para la consecución de unos fines que la sociedad ha encomendado a dichas administraciones.

El desarrollo y la operatividad de calidad en los servicios públicos se puede abordar en un primer nivel de análisis, en torno a dos variables:

- La naturaleza pública de las organizaciones donde hacer efectiva la calidad.
- El concepto de servicio.

En relación a la variable pública, depende de si nos encontramos ante relaciones en el interior de las organizaciones públicas o relaciones con los ciudadanos, y a la especificidad y diferenciación de servicios que éstas aportan.

En cuanto a la relación con los ciudadanos, la OCDEⁱⁱⁱ, y como consecuencia del campo de paradigma de la nueva gestión pública, incluye entre sus propuestas que la Administración Pública del futuro debe ser una “Administración receptiva”. Una administración receptiva supone fundamentalmente aceptación, dentro de su cultura, de una toma de conciencia por la que se va a tener en cuenta la capacidad de cada persona para hacer frente al proceso administrativo, facilitando su acceso a las prestaciones que tiene derecho a esperar de la Administración.

En el citado informe de la OCDE, hay que entender la receptividad en varias direcciones, el ciudadano tiene derecho a:

- Una Administración comprensible.
- Que sea accesible en el plano espacial, temporal y material.
- Que responda a la que de ella se espera.
- Que permita la participación de los ciudadanos en las decisiones administrativas que les afecten.

La receptividad no es, pues, una acción aislada o individualizada de un funcionario, sino la consecuencia o resultado de un modo con el que la Administración cumple sus funciones.

En el marco de las Administraciones Públicas y respecto al concepto de servicio es necesario y fundamental distinguir entre:

- Calidad de producto

Un producto puede ser analizado en términos de calidad en función de su mayor o menor “conformidad con las especificaciones”, sin embargo, en sus relaciones externas el sector público provee servicios y la medición de calidad plantea importantes problemas. En este sentido, es primordial

considerar que el servicio no es un objeto, sino un *proceso* lo que nos lleva al análisis de otras variables o dimensiones.

- Calidad de servicio

La calidad de los servicios que proveen las administraciones públicas, mediante relación electrónica con el ciudadano.

2.2 La calidad como factor competitivo

Hablar de competitividad en la gestión privada parece algo normal y coherente, así como necesario. Hacerlo en la gestión pública resulta a veces incomprensible por la gigantesca gestión que sobre determinadas parcelas realiza. No obstante, una Administración moderna debe introducir criterios de competitividad entre sus normas de actuación, a pesar de que tenga garantizada la supervivencia en su misión de proveer servicios esenciales a la comunidad. Para ello, debemos partir del hecho de que la administración tiene unos parámetros para medir su actuación, parámetros que le vienen marcados por la Constitución al señalar que su actuación deberá estar marcada por la objetividad y la eficacia.

Evidentemente, existen unos elementos diferenciadores entre gestión pública y gestión privada. Una serie de factores políticos, económicos, sociales e incluso culturales, han venido a mantener y defender esa distinción cuya dinámica persiste en una amplia capa social, y que para avanzar en su eliminación, hay que partir, en primer lugar, de su conocimiento, en el sentido de no estimar que la eficacia y buena gestión es algo excluyente en la gestión pública, sin realizar, la mayoría de las veces, un estudio de las circunstancias en que se produce la misma.

En los últimos años se han producido en España importantes reformas políticas y administrativas, provocadas por la progresiva aplicación de los principios constitucionales y que han afectado muy directamente al modo de gestión de la Administración. Se ha iniciado una tendencia a modificar esos planteamientos clásicos por los que se regía la Administración, a través de la progresiva asunción de la eficacia como norma de actuación, estableciéndose para ello una estrategia, doblemente direccionada:

- Por un lado, deriva su eficacia del fin que persigue, del producto que ofrece, fortaleciendo el compromiso de los funcionarios con los valores públicos que se enmarcan en un Estado Social, Democrático y de Derecho.
- Por otro lado, incorporando principios y técnicas de lo privado dentro del marco de las posibilidades legales de modo que la gestión pública aparezca como el resultado de la Ley, pero a su vez, como consecuencia de alguno de los principios y técnicas de la gestión privada, entre los que hay que destacar los más modernos y expertos sistemas gerenciales.



De este modo, aparecen conceptos y estrategias tales como el control de gastos, presupuestos por programas, técnicas de dirección, funciones de planificación, dirección por objetivos, etc. Estamos, en definitiva, en una nueva forma de concebir la mejora y modernización de la Administración, mediante un proceso abierto de perfeccionamiento en un doble frente. Y todo ello a través de una nueva filosofía que preside hoy en día la actuación de la Administración en sus relaciones con la sociedad.

Pero junto a ello, hay que seguir avanzando y conseguir una Administración competitiva, lo que supone lograr una Administración que introduzca entre sus criterios de actuación de forma permanente y constante, aquellos elementos de la gestión privada que van a posibilitar un mejor análisis y consecución de resultados más acordes con los objetivos o fines que la misma viene dada a conseguir. En definitiva que actúe con eficacia.

De este modo, para unos ciudadanos que piden a la Administración comprensibilidad, la Administración responde con un diseño de receptividad; pero para unos ciudadanos que piden eficacia no es suficiente la comprensibilidad, sino que es necesario avanzar en las ofertas de la Administración hasta conseguir de esta que su actuación venga presidida por criterios de competitividad, que sólo pueden alcanzarse a través de una gestión de calidad.

2.2.1 Entorno competitivo de la Administración Pública

La competitividad en la Administración se determina desde dos aspectos:

- Externa

En todo este proceso de transformación que está experimentando la Administración, hay un punto de partida por parte de los ciudadanos. Para éstos, el único factor valorable de la Administración es el servicio público que presta y que ellos reciben. Su valoración desde los parámetros de la comprensibilidad o comodidad e incluso desde los de la misma titularidad (pública y privada del servicio público), están evolucionando hacia los de eficacia, comodidad, economicidad y para ellos es así, porque pagan los servicios, porque a la hora de su valoración tienen como punto de referencia otros servicios, que por otras organizaciones privadas se les prestan y cuyas premisas de accesibilidad, coste, atención, etc. son similares a los de la Administración. Este análisis comparativo, quizás involuntario, está demandando a la Administración una actitud competitiva desde el momento en que cada mañana abre las oficinas a sus clientes.

Estamos ante unos ciudadanos que demandan de la Administración unos servicios públicos eficaces y bien gestionados y que para su valoración, independientemente de la titularidad pública de los mismos, siempre tienen como referencia los servicios que se les prestan por la gestión privada.

- Interna

Dentro de los aspectos internos, son varios los elementos que podemos encontrar que vienen a defender una actitud competitiva por la Administración. En primer lugar, la existencia de una Administración encaminada en el marco de una Organización Supranacional, la Comunidad Europea, que establece unos principios de movilidad que van a provocar la exigencia de una homogeneización entre sus Administraciones por parte de los ciudadanos en cuanto a los servicios públicos que actualmente vienen recibiendo por las Administraciones de sus respectivos Estados. Así pues, va dirigida a una Administración que entra en relación con otras organizaciones de similares objetivos para homogeneizar su gestión en un ámbito diferente en virtud de la normativa comunitaria.

Pero, por otro lado, dentro del Plan de Modernización, el modelo funcional que se propone, aboga por un sistema integrado de gestión por objetivos, mediante estrategias, programas, seguimientos, etc. Todo ello puede favorecer la defensa de una competitividad administrativa entre las diferentes organizaciones que, de este modo, tienen pautas medibles para reflejar sus avances o retrocesos en los objetivos fijados.

En base a estos planteamientos, podemos afirmar que la competitividad es hoy una exigencia. Que no existe un servicio concebido monolíticamente, sino que el mismo está sometido a una serie de elementos que continuamente valoran y comparan, lo que debe producir en la Administración una actitud competitiva para alcanzar los niveles de satisfacción y opinión que modifiquen los juicios negativos que tradicionalmente los ciudadanos hacen a la Administración.

2.2.2 ISO 27002

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Las normas de seguridad de la información son básicamente dos: ISO 27002 (anteriormente ISO 17799) e ISO 27001^{iv}.

La norma ISO 27002 es una guía de buenas prácticas, recoge los objetivos de control y los controles recomendables y no es certificable. La certificación se realiza con la norma ISO/IEC 27001, que recoge un resumen de estos controles en su Anexo A, como base para desarrollar los Sistemas de Gestión de la Seguridad de la Información (SGSI) de las organizaciones. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios:



- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad de negocio.
- Conformidad.

La ISO 27002 es la única norma que no sólo cubre la problemática de la seguridad en las tecnologías de la información (IT) sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. Este concepto marca la diferencia con el de seguridad informática que, en la práctica, se vino convirtiendo en equivalente de seguridad de sistemas IT, mientras que la norma considera también los riesgos organizacionales, operacionales y físicos de una empresa, con todo lo que esto implica.

Con objeto de mantener las normas relacionadas con la Seguridad de la Información dentro de la serie ISO 2700x, ISO/IEC 27002 sustituye, sólo en la numeración, a ISO/IEC 17799:2005, manteniendo intacto su contenido.

2.2.3 Accesibilidad Web

Iniciativa de Accesibilidad Web

La accesibilidad Web indica la capacidad de acceso a la Web y a sus contenidos por todas las personas, independientemente de las limitaciones propias del individuo (discapacidad) o de las que se deriven del contexto de uso (tecnológico o ambiental). Hablar de Accesibilidad Web es hablar de un acceso universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios.

A pesar de que el surgimiento de la World Wide Web, y su posterior crecimiento exponencial, han supuesto un cambio radical en cuanto a la facilidad de difusión y disponibilidad de la información, las limitaciones y el mal uso por parte de los diseñadores de las tecnologías imperantes de publicación

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Web están dando lugar a situaciones de imposibilidad de acceso a la información por parte de aquellos usuarios con discapacidad.

Con esta idea de accesibilidad nace la Iniciativa de Accesibilidad Web, conocida como *Web Accessibility Initiative (WAI)*. Se trata de una actividad desarrollada por el *World Wide Web Consortium (W3C)*, cuyo objetivo es facilitar el acceso de las personas con discapacidad, desarrollando pautas de accesibilidad, mejorando las herramientas para la evaluación y reparación de accesibilidad Web, llevando a cabo una labor educativa y de concienciación en relación a la importancia del diseño accesible de páginas Web, y abriendo nuevos campos en accesibilidad a través de la investigación en este área.

La idea principal radica en hacer la Web más accesible para todos los usuarios independientemente de las circunstancias y los dispositivos involucrados a la hora de acceder a la información. Partiendo de esta idea, una página Web accesible lo será tanto para una persona con discapacidad, como para cualquier otra persona que se encuentre bajo circunstancias externas que dificulten su acceso a la información (en caso de ruidos externos, en situaciones donde nuestra atención visual y auditiva no estén disponibles, etc.).

Para hacer el contenido Web accesible, se han desarrollado las denominadas Pautas de Accesibilidad al Contenido en la Web (WCAG), cuya función principal es guiar el diseño de páginas Web hacia un diseño accesible, reduciendo de esta forma barreras a la información. WCAG consiste en 14 pautas que proporcionan soluciones de diseño y que utilizan como ejemplo situaciones comunes en las que el diseño de una página puede producir problemas de acceso a la información. Las Pautas contienen además una serie de puntos de verificación que ayudan a detectar posibles errores.

Cada punto de verificación está asignado a uno de los tres niveles de prioridad establecidos por las pautas.

- Prioridad 1: son aquellos puntos que un desarrollador Web tiene que cumplir ya que, de otra manera, ciertos grupos de usuarios no podrían acceder a la información del sitio Web.
- Prioridad 2: son aquellos puntos que un desarrollador Web debería cumplir ya que, si no fuese así, sería muy difícil acceder a la información para ciertos grupos de usuarios.
- Prioridad 3: son aquellos puntos que un desarrollador Web debería cumplir ya que, de otra forma, algunos usuarios experimentarían ciertas dificultades para acceder a la información.

En función a estos puntos de verificación se establecen los niveles de conformidad:

- Nivel de Conformidad "A": todos los puntos de verificación de prioridad 1 se satisfacen.
- Nivel de Conformidad "Doble A": todos los puntos de verificación de prioridad 1 y 2 se satisfacen.

- Nivel de Conformidad "Triple A": todos los puntos de verificación de prioridad 1,2 y 3 se satisfacen.

Las pautas describen cómo hacer páginas Web accesibles sin sacrificar el diseño, ofreciendo esa flexibilidad que es necesaria para que la información sea accesible bajo diferentes situaciones y proporcionando métodos que permiten su transformación en páginas útiles e inteligibles.

Igualmente, se han desarrollado Pautas de Accesibilidad para Herramientas de Autor, cuyo objetivo es ayudar a los desarrolladores de software a la hora de crear herramientas de autor para producir contenido Web accesible. También se han desarrollado Pautas de Accesibilidad para XML, donde se explica cómo asegurar la accesibilidad de aplicaciones basadas en XML. Y por último, Pautas de Accesibilidad para Agentes de Usuario 1.0, donde se explica cómo hacer accesible los navegadores, reproductores multimedia y otras tecnologías asistidas.

Por otro lado, se han desarrollado otro tipo de documentos como las Técnicas para Pautas de Accesibilidad al Contenido en la Web, que ofrecen una serie de ejemplos de etiquetado y explicaciones muy detalladas de cómo implementar las Pautas de Accesibilidad al contenido en la Web.

Un ejemplo de prioridad 1 sería la identificación clara de cualquier cambio de idioma que se pueda producir en el texto de un documento. Es decir, si se utilizan diferentes idiomas es necesario que cualquier cambio esté claramente señalado con el atributo *lang*:

Un ejemplo de código correcto sería el siguiente:

```
<p>  
<q>Buenos días Philip</q>  
<q lang="en">Good morning</q>. Respondió Philip en inglés.  
<q>¿Qué tal estás?</q>  
<q lang="fr">Très bien.</q>  
Volvió a responder, pero esta vez en francés.  
</p>
```

Otro ejemplo de prioridad 1 sería la utilización de la etiqueta *alt* para incorporar texto equivalente al contenido de una imagen cuando se quieren utilizar gráficos, esto permitiría que dispositivos o personas que no pueden visualizar los gráficos, obtengan una representación alternativa textual. El código correspondiente sería:

```

```

Legislación española sobre la Accesibilidad Web en AAPP

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

En cuanto a legislación específica sobre accesibilidad en España, contamos con:

- Instrumento de Ratificación de la Convención de Derechos de las Personas con Discapacidad, dado el 21 de abril de 2008.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información
- Ley 49/2007, de 26 de diciembre, por la que se establece el régimen de infracciones y sanciones
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social. Real Decreto 1494/2007, de 12 de noviembre.
- Ley 30/2007, de 30 de octubre, de Contratos del Sector Público (BOE n. 261 de 31/10/2007)
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 366/2007, de 16 de marzo, por el que se establecen las condiciones de accesibilidad y no discriminación de las personas con discapacidad en sus relaciones con la Administración General del Estado (BOE n. 72 de 24/3/2007).
- Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE).
- Proposición No de Ley "para facilitar el acceso de las personas mayores y con discapacidad en el portal de Internet de la Administración General del Estado".
- Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. Conocida como LIONDAU, esta ley viene a llenar el vacío existente en España de un marco legal amplio y general, similar al que proporcionan en otros países leyes similares y pone de relieve los conceptos de no discriminación, acción positiva y accesibilidad universal.

La ley prevé, además, la regulación de los efectos de la lengua de signos, el reforzamiento del diálogo social con las asociaciones representativas de las personas con discapacidad mediante su inclusión en el Real Patronato y la creación del Consejo Nacional de la Discapacidad, y el establecimiento de un calendario de accesibilidad por



ley para todos los entornos, productos y servicios nuevos o ya existentes.

Uno de los cambios más relevantes respecto a la legislación anterior, recogido en el artículo 20 de la ley, es la inversión de la carga de la prueba, por la que será el demandado, y no el demandante, quien deberá probar su inocencia ante un posible caso de discriminación por razón de discapacidad.

La Ley establece, la obligación gradual y progresiva de que todos los entornos, productos y servicios deben ser abiertos, accesibles y practicables para todas las personas y dispone plazos y calendarios para realización de las adaptaciones necesarias.

Actualmente, el incumplimiento de la Ley 51/2003 más conocida como LIONDAU (Ley de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad), puede suponer multas entre los 301 euros y el millón de euros. No excediendo de 30.000 euros para las leves y 90.000 para las graves. Las muy graves podrán ir acompañadas de la supresión de ayudas y subvenciones.

Ley 34/2002 sobre accesibilidad en AAPP

La Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información y Comercio Electrónico, en su Disposición adicional quinta, obliga a las Administraciones Públicas a adoptar las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a las personas con discapacidad y mayores:

- Imágenes y animaciones: Use el atributo *alt* para describir la función de cada elemento visual.
- Mapas de imagen: Use el elemento *map* y texto para las zonas activas.
- Multimedia: Proporcione subtítulos y transcripción del sonido, y descripción del vídeo.
- Enlaces de hipertexto: Use texto que tenga sentido leído fuera de contexto. Por ejemplo, evite "pincha aquí".
- Organización de las páginas: Use encabezados, listas y estructura consistente. Use CSS para la maquetación donde sea posible.
- Figuras y diagramas: Descríbalos brevemente en la página o use el atributo *longdesc*.
- *Scripts, applets y plug-ins*: Ofrezca contenido alternativo si las funciones nuevas no son accesibles.
- Marcos: Use el elemento *noframes* y títulos con sentido.
- Tablas: Facilite la lectura línea a línea. Resuma.
- Revise su trabajo: Verifique. Use las herramientas, puntos de comprobación y pautas de <http://www.w3.org/TR/WCAG>.

Beneficios de la accesibilidad Web

Entre las ventajas que cuentan las páginas Web que cumplen estándares de accesibilidad se encuentran los siguientes:

- Posicionamiento en Buscadores:

Proporciona un patrón de búsqueda más rápido en los buscadores, por lo que su posicionamiento en estos será mejor. Esto es debido al uso de un esquema de contenidos en la página Web claro y conciso, facilitando una mayor comprensión y claridad. Actualmente en los buscadores se buscan los contenidos de las Páginas Web para así hacer un diagnóstico y generar una lista con los elementos encontrados, si se posee un esquema sencillo y bien estructurado, el patrón de búsqueda será más eficiente con una Página Web accesible.



- Responsabilidad Social Corporativa:

Una página que posea el acceso a sus contenidos enfocado a la posibilidad de acceso de un grupo minoritario demuestra su preocupación social y su compromiso hacia ese colectivo de personas. Esto puede incluir la igualdad de acceso a la información electrónica y a los servicios de la misma forma que el acceso físico a las instalaciones.

- Navegación por dispositivos móviles:

Al incorporar cánones en materia de accesibilidad en un página Web, los contenidos podrán ser visualizados a través de dispositivos móviles como pueden ser teléfonos móviles, PDAs con acceso a Internet. Por lo tanto, un mayor número de visitas y de público objetivo dispondrán de la información y contenidos incluidos en las páginas Web accesibles.

- Reduce el ancho de banda:

Al tener la Página Web accesible se encontrará organizada y estructurada de tal forma que los contenidos y el diseño estén separados y tengan menos peso, minimizando el tiempo de carga de contenidos y de imágenes y videos.

- Mayor Público Objetivo:

A corto plazo, un colectivo de personas con discapacidades sensoriales como la ceguera y la falta de audición suponen un incremento del alcance de las páginas Webs accesibles al estar preparadas para ellos. A medio plazo, el número de público objetivo aumentará debido al uso de los dispositivos móviles y el acceso de los mismos a Internet.

- Mayor usabilidad, mayor claridad y mayor eficiencia:

Al hacer la página Web más accesible los contenidos serán más concisos y claros, repercutiendo directamente en el tiempo de navegación del usuario y en la facilidad de encontrar aquello que estaba buscando, por lo que la eficiencia aumenta.

- Menor tiempo y mayor facilidad de mantenimiento y gestión de Contenidos:

Se crean Páginas Web estructuradas de tal forma que se minimizan los costes en el envío de información innecesaria al usuario. Cualquier cambio en los contenidos o en el diseño de la página Web se hará con más rapidez y eficiencia, siendo su precio más competitivo en el mercado.

- Innovación:

Una página accesible sigue los cánones de la W3C, programada bajo los últimos adelantos en lenguaje de programación. Una ventaja competitiva respecto a Empresas o Administraciones reflejada en el uso de las últimas técnicas de programación Web.

Herramientas de accesibilidad Web

A continuación se indican algunas herramientas que permiten comprobar de manera automática la accesibilidad de una Web:

- TAW (Test de Accesibilidad Web) es una herramienta, desarrollada por la Fundación CTIC, que permite comprobar de forma automática ciertos aspectos de la accesibilidad Web. Sus destinatarios son los profesionales del diseño y desarrollo Web. dependiendo de los puntos de verificación que cumpla un sitio Web tendrá un nivel de accesibilidad, A, AA o AAA.

El TAW funciona introduciendo una URL del sitio Web que se pretende analizar, generando finalmente un informe HTML con información sobre el resultado del análisis.

- HERA es una utilidad para revisar la accesibilidad de las páginas Web de acuerdo con las recomendaciones de las Directrices de Accesibilidad para el Contenido Web 1.0 (WCAG 1.0). HERA realiza un análisis automático previo de la página e informa si se encuentran errores (detectables en forma automática) y qué puntos de verificación de las pautas deben ser revisados manualmente.

La revisión manual es imprescindible para comprobar realmente si la página es accesible. Para poder llevar a cabo esta verificación manual es necesario conocer las directrices de accesibilidad, saber cómo utilizan los usuarios las ayudas técnicas y tener alguna experiencia en diseño y desarrollo de páginas Web.

HERA facilita la revisión manual proporcionando información acerca de los elementos a verificar, instrucciones sobre cómo realizar ese control y dos vistas modificadas de la página (una en modo gráfico, otra del código HTML) con los elementos más importantes destacados con iconos y colores distintivos.

Un formulario permite modificar los resultados automáticos, agregar comentarios a cada punto de verificación e indicar el nombre del revisor. También es posible generar un informe final sobre la revisión, para imprimir o descargar, en diversos formatos (XHTML, RDF y PDF).



3 MARCO LEGAL EN ESPAÑA

La Constitución Española de 1978^v, señala como criterio de actuación para la Administración Pública el de OBJETIVIDAD y EFICACIA, a fin de posibilitar una administración proveedora de servicios esenciales para la Comunidad, a través de dichos criterios y con pleno sometimiento a la Ley y al Derecho.

La Administración Electrónica está teniendo su mayor impulso en los últimos años, motivado en parte por un marco legal que ha permitido llevar las garantías jurídicas que existen en el mundo real al mundo virtual y en otra parte por la evolución de las tecnologías relacionadas y el desarrollo de proyectos como el DNI electrónico. Se pueden destacar especialmente en este sentido la *Ley 59/2003, de 19 de diciembre, de firma electrónica* que establece, entre muchas otras cosas, el concepto de firma electrónica reconocida y la equipara jurídicamente a la firma en papel, dotándola así de plena validez legal para las transacciones electrónicas públicas y privadas.

Por otra parte con la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* y su reglamento de desarrollo se establecen las garantías de confidencialidad de los datos proporcionados por las personas físicas (es decir, los ciudadanos) en estas transacciones.

Hay que mencionar, y en un lugar muy destacado, la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* (LAECSP) a la que en muchas ocasiones se refiere como "Ley de Administración Electrónica" que consagra el concepto de Administración Electrónica en el marco jurídico español y la eleva a la categoría de derecho de los ciudadanos. Es decir, los ciudadanos tienen el derecho de acceder electrónicamente a los servicios de la Administración Pública, y éstos ya no son facultativos para ésta, sino que la capacidad de proporcionarlos se convierte en una obligación para ellas.

3.1 Evolución de los Ayuntamientos en España

Como introducción a la contextualización del marco legal en España, se esbozan los antecedentes dando una visión cronológica de la evolución de la situación en el caso de los ayuntamientos.

A finales de los años 70, los ayuntamientos comenzaron a plantearse la informatización de sus datos más importantes y de las operaciones críticas para su funcionamiento.

El tratamiento manual de datos y operaciones requería cada vez más personal y la obtención de información agregada para apoyar la toma de decisiones era especialmente costosa.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

En una primera fase de informatización, que llegaría hasta finales de los 80, se automatizaron los datos y operaciones directamente relacionados con la obtención de ingresos o con el control de los gastos.

En este período, las aplicaciones estrella fueron las destinadas a gestionar el padrón municipal, la recaudación, la contabilidad y las nóminas. También aparecieron las primeras aplicaciones de registro general de entrada y salida.

En el mercado no existían proveedores especializados en el sector de la administración local, y los ayuntamientos optaron en un primer momento por el desarrollo propio en entornos centralizados.

Al final de esta primera fase, y a pesar del control que cada una de las aplicaciones daba sobre sus datos, y a los importantes ahorros obtenidos respecto a su tratamiento manual, la informatización afectaba únicamente algunas áreas y dentro de estas a unos pocos puestos de trabajo, y la mayor parte del trabajo administrativo seguía realizándose manualmente.

Los departamentos de informática que habían optado por el desarrollo propio, o crecían desmesuradamente o se paralizaban debido al “efecto estela” provocado por el mantenimiento de las aplicaciones desarrolladas. Al mismo tiempo, aparecían en el mercado proveedores y aplicaciones especializadas.

Estudios realizados en aquel momento, estimaban que la informatización realizada afectaba aproximadamente a un 15% del trabajo administrativo de los ayuntamientos, mientras que el restante 85% correspondía principalmente al trámite de expedientes administrativos, que se seguía realizando de forma manual.

Como consecuencia, a finales de los 80, se empezaron a manejar conceptos de *ofimática* o *burótica*, buscando la informatización de los montones de papel sobre el que no se tenían ni datos ni control.

Igualmente, y de forma independiente, se comenzaron a desarrollar aplicaciones para gestionar los fondos documentales de los archivos municipales.

Los intentos de implantación de soluciones ofimáticas con las aplicaciones desarrolladas hasta entonces, presentaban dos dificultades principales:

- Los tratamientos de textos que ofrecían los sistemas sobre los que se habían implementado las primeras aplicaciones, eran complejos de utilizar y poco funcionales.
- Las aplicaciones habían nacido de forma desagregada, sobre bases de datos no relacionales, y pertenecían a proveedores distintos o corrían bajo diferentes sistemas.

Pero el marco legal completo de la Administración electrónica va mucho allá, hay muchas cuestiones concretas como la protección de los datos personales o



la legislación en torno al uso de firmas electrónicas que es imprescindible conocer bien si se quieren concebir nuevos servicios electrónicos.

3.2 Previsiones comunitarias sobre la sociedad de la información

Debe recordarse que el impulso de una Administración electrónica supone también dar respuesta a los compromisos comunitarios y a las iniciativas de eEuropa que desde el 8 de diciembre de 1994 se han puesto en marcha, primero con ocasión de la comunicación de la Comisión con motivo del Consejo Europeo de Helsinki^{vi}.

Después con la comunicación de la Comisión con motivo del Consejo Europeo de Lisboa y Santa María da Feira que dan lugar a que en éste último se ponga en marcha de modo concreto tal iniciativa.

Otras actuaciones significativas han sido:

- El Comunicado de la Comisión Europea eEuropa 2002: Accesibilidad para los Sitios Web Públicos y su Contenido.
- El Plan de Acción eEuropa del Consejo Europeo de Sevilla.
- La comunicación de la Comisión i2010: Una Sociedad de la Información Europea para el crecimiento y el empleo.

El impulso comunitario a la iniciativa eEuropa, que a partir de 2002 en el Consejo de Sevilla y Barcelona pasan a dar la máxima importancia en el Plan de acción al desarrollo de la Administración electrónica, busca aprovechar todas las posibilidades de las nuevas tecnologías, no sólo por sí mismas, sino como un factor determinante del futuro económico de Europa como una de las Economías más avanzadas. Tras los momentos de recesión económica que se viven en Europa, resulta que se va a confiar en las Administraciones Públicas como uno de los motores principales del lanzamiento de las tecnologías de la información, pues son las Administraciones las que, al poder llenar de contenidos la red, estimulan su uso, rompiendo así el círculo vicioso de que si hay pocos contenidos, pocas ventajas para el gran público, no se utiliza la red, y si no se utiliza mucho la red por el gran público son pocos los que se deciden a colocar en ella sus contenidos.

En estos años de vigencia de la iniciativa eEuropa el ámbito de actuación de la Administración electrónica ha crecido considerablemente en sucesivas revisiones. En el año 2003 la Comisión publicó una comunicación sobre el papel de la Administración electrónica en el futuro de Europa en la que señala un conjunto de actuaciones tendentes a mejorar la situación existente y a promover la modernización de las administraciones como medio para lograr los objetivos de Lisboa.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

En noviembre de 2005, tras la publicación de la comunicación relativa a i2010, se aprobó, en la Cumbre de Manchester, una resolución ministerial, con objetivos concretos para el desarrollo de la Administración electrónica en la Unión. Esta resolución dio lugar al desarrollo de una Comunicación que recoge el Plan de Acción sobre administración electrónica i2010, en la que se señala que los éxitos de la Administración Electrónica son ya claramente visibles en varios países de la UE, estimando en 50.000 millones de euros el ahorro anual en toda la Unión que una implantación generalizada de ella podría generar.

Los grandes pilares de esta Comunicación son los siguientes:

- La inclusión social (“ningún ciudadano debe quedarse atrás”).
- La eficacia y la eficiencia contribuyendo de forma significativa a la transparencia, la satisfacción de usuarios, la rendición de cuentas y el aligeramiento de la carga administrativa.
- La medición del impacto y los beneficios de la administración electrónica y la comunicación para compartir experiencias.
- La implantación de servicios electrónicos de gran impacto para ciudadanos y empresas especialmente el de la contratación administrativa.
- El establecimiento de herramientas claves que permitan a los ciudadanos un acceso autenticado, cómodo, seguro e interoperable de los servicios públicos en toda Europa.
- El fortalecimiento de la participación y la adopción de decisiones democráticas (debate y participación efectiva del público en la adopción de decisiones democráticas).

Paralelamente en febrero del 2010, la Comisión hizo pública una comunicación sobre interoperabilidad para los servicios de Administración electrónica europeos, donde se resalta de nuevo la necesidad de modernizar el sector público europeo y de mejorar la interacción entre los organismos involucrados para mejorar las economías de sus países. En efecto, se señala que el mercado único precisa de administraciones públicas modernas y eficaces que faciliten la movilidad y la interacción sin fallo de los ciudadanos y empresas. “Una administración pública moderna, señala la Comunicación, debe apoyarse en una infraestructura TIC (Tecnologías de la Información y las Comunicaciones) compleja y sobre procedimientos racionales de administración en línea, condición sine qua non, para suministrar servicios poco costosos, transparentes y apropiados necesarios para captar las potencialidades ofrecidas por la Sociedad de la Información”.

En la reunión del Consejo de Ministros europeos de Transporte, Telecomunicaciones y Energía, de 8 y 9 de junio de 2006, debatieron sobre ambas comunicaciones, e hizo públicas una serie de conclusiones que refrendaban ambas comunicaciones (*eGovernment for all europeans*), que recoge en gran medida las aportaciones de la declaración Ministerial de Manchester en Noviembre de 2005 e invita, entre otras cuestiones, a los estados miembros a promover, entre otras cosas:



- Asegurar un entorno legal y organizacional adecuado que estimule la creación de servicios electrónicos accesibles, inclusivos, centrados en el usuario.
- Poner en marcha medios seguros de identificación electrónica, teniendo en cuenta el principio de reconocimiento mutuo dentro de la U.E.
- Promoción de la interoperabilidad y el uso de estándares abiertos.

En el contexto internacional, también otros organismos se han interesado en la Administración electrónica como forma de activar la economía y mejorar el gobierno de los países.

La OCDE publicó en 2004 un estudio con un título casi autodescriptivo: “La Administración electrónica: Un imperativo”^{vii}, donde resalta los ahorros que la Administración electrónica puede generar al permitirles aumentar su eficacia. En dicho estudio, la OCDE establece un decálogo para conseguir una Administración electrónica eficaz:

- Liderazgo y compromiso tanto político como administrativo.
- Integración dentro de una política más amplia y en objetivos de prestación de servicios. La administración electrónica como medio, no como fin.
- Colaboración entre organismos, desarrollando infraestructuras compartidas y creando marcos de interoperabilidad.
- Financiación, considerando el gasto TIC como una inversión. Aconseja un marco de financiación central.
- Acceso para todos. Inclusión.
- Elección por parte del usuario de la forma de relacionarse con la Administración
- Implicación ciudadana con procesos de calidad e involucración de los ciudadanos en el proceso político.
- Privacidad. Protección de la misma.
- Responsabilidad, estableciendo quienes son los responsables de los proyectos e iniciativas compartidas.
- Control y evaluación de la demanda, de los costes y de los beneficios esperados y obtenidos.

El Consejo de Europa, desde una perspectiva más social, también está analizando la Administración electrónica como un motor de desarrollo. En diciembre de 2004 el Comité de Ministros adoptó una recomendación donde se señala que la Administración electrónica no son asuntos meramente técnicos, sino de gobernanza democrática.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

En el plano nacional y, sobre todo, internacional, existe coincidencia en señalar la utilización de estas tecnologías como un reto importante, al confiar que las posibilidades que ofrecen permiten afrontar una gran parte de los retos que tiene planteados la Administración Pública en este siglo, la atención a la globalización y a las necesidades especiales de unas sociedades cada vez más complejas, las demandas de mayor eficacia y eficiencia, con los mismos e incluso con menos recursos, la implantación de la cultura de la calidad, etc.

En este contexto una ley de la Administración electrónica se justifica en la creación de un marco jurídico que facilite la extensión y utilización de estas tecnologías. Y el principal reto que la implantación de las TIC en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. Dichos riesgos nacen de, por una parte, la impresión de la mayor fragilidad de la información en soporte electrónico al acceso, manipulación o destrucción, por otra, el miedo a la pérdida de privacidad derivada de la eficiencia con la que las TIC manejan la información, y finalmente de la escasa transparencia de estas tecnologías consecuencia de su fundamento científico, tecnológico que requieren unos conocimientos básicos cuya ausencia determina nuevas formas de coordinación.

Para ello, la legislación debe proclamar y erigirse sobre un principio fundamental como es el de conservación de las garantías constitucionales y legales a los derechos de los ciudadanos y en general de las personas que se relacionan con la Administración pública, cuya exigencia se deriva del artículo 18.4 CE, al encomendar a la Ley la limitación del uso de la informática para preservar el ejercicio de los derechos constitucionales. Esta conservación exige, afirmar la vigencia de los derechos fundamentales no sólo como frente a la Administración telemática que recogen un grupo heterogéneo de las posiciones del ciudadano en sus relaciones con las Administraciones públicas, así como las garantías específicas para su efectividad. La formulación de dicho estatuto debe realizarse con prudencia de forma que:

- La tipificación de estas posiciones no se traduzcan en un efectivo recorte, por omisión, del estatuto actual del ciudadano respecto de la Administración.
- No suponga la generación de fuentes de discriminación respecto de las personas que por razones físicas, intelectuales o económicas no puedan hacer uso de estas tecnologías.

La implantación creciente de las Tecnologías de la Información y la Comunicación en la Administración Pública española está potenciando una serie de servicios de información dirigidos al ciudadano que se caracterizan primordialmente por la incorporación de una filosofía de atención al cliente, procedente en la mayoría de los casos de proyectos de calidad que afectan en general a la gestión total de las actividades de un sector de la Administración, experiencias que se están llevando a cabo formando parte de las políticas de modernización emprendidas por la Administración Pública española desde hace unos años.



Para la nueva cultura administrativa resulta prioritaria la conformación de un nuevo concepto de las relaciones entre las Administraciones Públicas y los ciudadanos, centrada en dos ejes principales:

- Una nueva atención al ciudadano.
- Un nuevo concepto de información al público,

Dos elementos esenciales que no dejan de evolucionar al ritmo de los avances de las tecnologías de la información y la comunicación.

Atender las necesidades informativas de los ciudadanos, adaptarse a sus exigencias y a sus nuevos hábitos de información, ofrecer una información personalizada adaptada a las particularidades de los usuarios, de cara a proporcionar en cada instante una información a la carta son las particularidades de los nuevos servicios de información administrativa que están conformando una nueva forma de comunicación de la Administración con los ciudadanos: más dinámica, más participativa y más cercana.

Claro está que no hay que perder de vista en ningún momento diferentes aspectos que enmarcan en cierto sentido el contexto de las nuevas formas de prestar servicios de información por parte de la Administración:

- El nivel competencial administrativo que presta los servicios, integrado por el ámbito estatal de la Administración General del Estado, la administración autonómica y la administración local.
- El derecho a la información, derecho reconocido por la Constitución española se convierte en política de Estado y en objetivo de las prioridades estratégicas de la Administración en relación con los ciudadanos. Según estos principios, los ciudadanos tienen derecho a solicitar y obtener información sobre los servicios y actividades de las Administraciones Públicas, y salvo en lo que afecte a la seguridad y defensa del Estado y la intimidad de las personas, tienen también derecho a acceder a los archivos y registros administrativos. Ello implica una serie de transformaciones organizativas e iniciativas legislativas encaminadas a crear los mecanismos e instrumentos de difusión y transmisión de su información para facilitar la comunicación de los asuntos públicos.
- La distinta tipología de los usuarios a los que se dirigen los servicios de información administrativa, ya sean los propios ciudadanos, las empresas o la sociedad en su conjunto.
- Una última variable la conformarían las tecnologías de la información y la comunicación, cada vez más integradas en la gestión de las actividades de las Administraciones Públicas, y que constituyen un

elemento imprescindible para configurar las nuevas formas de comunicación entre la Administración y los ciudadanos.

A continuación se pretende realizar un mapa básico de las normas legales más importantes que sirva como punto de orientación a partir del cual hacerse una idea global del marco legal de la Administración electrónica.

3.3 La Ley 11/2007

Su nombre completo Ley 11/2007^{viii}, de acceso electrónico de los ciudadanos a los servicios públicos. Donde a partir de ahora también la veremos escrita con su acrónimo LAECSP.

En este punto desgranaremos los aspectos más relevantes de dicha ley tales como los antecedentes, descripción de la propia ley o la descripción del Reglamento.

3.3.1 Antecedentes a la Ley 11/2007

El 23 de Junio del año 2007 se publicó en el Boletín Oficial del Estado y un día después entró en vigor la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, cuya finalidad es promover el uso de las Tecnologías de la Información y las Comunicaciones en las relaciones entre la Administración Pública y los ciudadanos y entre las diferentes Administraciones Públicas. En virtud de esta Ley, los ciudadanos podrán realizar todas sus gestiones administrativas por medios electrónicos. De esta forma, las Administraciones Públicas quedan obligadas a ofrecer sus servicios por Internet, dispositivos móviles, TDT o cualquier medio electrónico futuro.

Anteriormente a la LAECSP, la Ley 30/1992, de 26 de Noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC) ya recogía en algunos de sus artículos el impulso por parte de la Administración al empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos al objeto de desarrollar su actividad y el ejercicio de sus competencias así como posibilitaba que los ciudadanos pudieran relacionarse con las Administraciones Públicas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos cuando esto fuera compatible con los medios técnicos de que dispusieran éstas. Las avanzadas, para el momento, pero por otra parte prudentes, previsiones legales, muy válidas en 1992, habían quedado desfasadas, ante una realidad en la que el grado de penetración de ordenadores y el número de personas y entidades con acceso en banda ancha a Internet, con las posibilidades abiertas a otras tecnologías y plataformas, no se correspondía ya con los servicios meramente facultativos que la citada Ley permitía y estimulaba a establecer a las distintas Administraciones.



Este desarrollo de la Administración electrónica era todavía insuficiente, en buena medida debido a que las previsiones indicadas en la ley eran facultativas. Es decir, dejaban en manos de las propias Administraciones determinar si los ciudadanos iban a poder de modo efectivo, o no, relacionarse con ellas por medios electrónicos, según que éstas quisieran poner en pie los instrumentos necesarios para esa comunicación. Por esta razón la ley 11/2007 pretendió dar el paso del “podrán” al “deberán” es decir, lo que en la ley 30/1992 se planteaba como algo opcional y recomendable en la ley 11/2007 pasa a ser una obligación.

En resumen, la Ley 30/1992 se limitó a abrir la posibilidad de establecer relaciones telemáticas con la Administración, pero era necesaria otra regulación que garantizara, de modo efectivo, el derecho a establecer relaciones electrónicas con todas las Administraciones Públicas. Las nuevas realidades, exigencias y experiencias que se han ido poniendo de manifiesto, el propio desarrollo de la sociedad de la información, la importancia de una regulación clara, precisa y común de los derechos de los ciudadanos y el cambio de circunstancias tecnológicas y sociales exige actualizar el contenido, muy diferente al de 1992, de la regulación básica que esté hoy a la altura de las nuevas exigencias. Esta regulación común exige, reconocer el derecho de los ciudadanos, y no sólo la posibilidad, de acceder mediante comunicaciones electrónicas a la Administración.

Con la intención de facilitar en el ámbito de la Administración Local la aplicación de estas normativas y teniendo en cuenta el horizonte temporal, el 1 de Enero de 2010 se elaboró desde la Comisión de Modernización y Calidad de la FEMP la *Guía práctica de aplicación de la Ley 11/2007 en la Administración Local*^x. Dicho documento tenía por objeto presentar una guía de introducción y adaptación a la LAECSP para Administraciones Locales, realizando una descripción de los contenidos de la misma, con el objetivo de facilitar su mejor comprensión e interpretación, así como subrayar los aspectos de especial relevancia, para que cualquier Ayuntamiento o Diputación utilizando esta guía pueda, según sus características, orientar su adaptación a la Ley 11/2007 o realizar una planificación acorde a la misma.

En noviembre de 2009 apareció el Real Decreto 1671/2009 de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios públicos. Este Real Decreto pretende ser un complemento necesario en la Administración General del Estado para facilitar la efectiva realización de los derechos reconocidos en la ley.

Ya iniciado el año 2010 se han publicado dos nuevos Reales Decretos que definen los tan esperados Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

3.3.2 Desarrollo reglamentario de la Ley 11/2007

Para dar forma a la Ley 11/2007 se aprueban una serie de Reales Decretos los cuales se mencionan a continuación por orden cronológico. Estos Reales Decretos al tener un valor informativo muy importante para la eAdministración, y se explicarán con mayor detalle a continuación de este punto.

- **Real Decreto 1671/2009 de 6 de Noviembre**

El Real Decreto desarrolla los derechos reconocidos en la Ley 11/2007, de 22 de junio en el ámbito de la Administración General del Estado.

- **Real Decreto 3/2010 de 8 de Enero. Esquema Nacional de Seguridad**

El Esquema Nacional de Seguridad se compone de los principios esenciales y mínimos para proteger la información.

- **Real Decreto 4/2010 de 8 de Enero. Esquema Nacional de Interoperabilidad**

El Esquema Nacional de Interoperabilidad aglutina una serie de criterios para que las Administraciones públicas puedan interactuar.

3.4 Real Decreto 1671/2009 de 6 de noviembre

El Real Decreto 1671/2009, por el que se desarrolla parcialmente la Ley 11/2007 pretende ser el complemento necesario en la Administración General del Estado para facilitar la efectiva realización de los derechos reconocidos en la Ley 11/2007.

En este sentido es de esperar que las diversas Administraciones desarrollen sus correspondientes textos legales y que en gran medida se basen en este Real Decreto en su elaboración. Este texto se ha construido sobre la base de los siguientes principios estratégicos:

- Procurar la más plena realización de los derechos reconocidos en la Ley 11/2007, de 22 de junio, facilitándolos en la medida que lo permite el estado de la técnica, y la garantía de que no resultan afectados otros bienes constitucionalmente protegidos, como pueden ser la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros.
- Establecer un marco lo más flexible posible en la implantación de los medios de comunicación, cuidando los niveles de seguridad y protección de derechos e intereses previstos tanto en la propia Ley 11/2007, de 22 de junio, como en la legislación administrativa en general. Con ello se persigue un triple objetivo:



- Evitar que la nueva regulación imponga una renovación tal en las soluciones de comunicación con los ciudadanos que impida la pervivencia de técnicas existentes y de gran arraigo.
- Facilitar la actividad de implantación y adaptación a las distintas organizaciones, funciones y procedimientos a los que es de aplicación el real decreto.
- Impedir que la opción rígida por determinadas soluciones dificulte para el futuro la incorporación de nuevas soluciones y servicios.

El real decreto empieza por concretar la manera de realizar el derecho de no aportación de datos y documentos que ya obren en poder de la Administración y especifica las pautas de actuación concretas necesarias para su realización en la práctica administrativa.

A continuación se abordan en profundidad el concepto de sede electrónica, detalles relativos a la creación y operativa de las mismas, y el punto de acceso general de la Administración General del Estado que actualmente se encarna en la Red 060. Se abordan igualmente detalles sobre los certificados electrónicos a usar por las sedes electrónicas y la identificación de las mismas tales como la obligación, en un plazo de 4 meses a partir de la entrada en vigor del Real Decreto, de utilizar nombres de dominio del tipo *gob.es* en todas las sedes electrónicas de la Administración General del Estado.

Se regulan detalles acerca de los sellos electrónicos emitidos por la AGE y sus organismos, los códigos seguros de verificación (necesidad de una Orden Ministerial o resolución de titular de organismo público para su aplicación, procedimiento directo y gratuito para los interesados, posibilidad de utilizar el código seguro de verificación también como modalidad de firma del personal de la AGE), y los demás medios de autenticación y firma del personal. Se prohíbe expresamente la aplicación de los certificados electrónicos para la firma electrónica de documentos y trámites.

Se crea también el concepto de certificado electrónico de empleado público, un certificado electrónico vinculado a un puesto de trabajo que identifica a su titular y se especifican los contenidos mínimos con los que ha de contar.

Por otra parte, se establece el régimen de habilitaciones generales y específicas de personas físicas o jurídicas autorizadas para la presentación electrónica de documentos en representación de los interesados, se detallan algunos aspectos de la identificación y autenticación de ciudadanos por funcionario público y se crea el registro electrónico de apoderamientos de la Administración General del Estado.

En cuanto a los servicios relacionados con el uso de certificados electrónicos se aborda el sistema nacional de verificación y la integración de otras plataformas de verificación como lo pueden ser plataformas de validación de las Comunidades Autónomas.

Una de las cuestiones más importantes es todo lo relativo a los registros electrónicos, a los cuales se les dedica un título entero: el Título IV. Ahí se abordan detalles sobre la creación y operativa de los mismos y se crea el concepto de Registro Electrónico Común al cual se pueden presentar todas aquellas solicitudes, escritos y comunicaciones dirigidos a la AGE o sus Organismos los cuales no estén contemplados en un registro electrónico específico.

En cuanto a las comunicaciones electrónicas, se regula la posibilidad de establecer la obligatoriedad de comunicarse por medios electrónicos con determinados órganos de la AGE en los supuestos del artículo 27.6 de la Ley 11/2007 y mediante Orden Ministerial.

A continuación se tratan las notificaciones electrónicas, se abordan las formas de notificación, especialmente la posibilidad de usar correo electrónico con acuse de recibo “siempre que se genere automáticamente y con independencia de la voluntad del destinatario un acuse de recibo que deje constancia de su recepción y que se origine en el momento del acceso al contenido de la notificación”.

Por otra parte se define el concepto de notificación por comparecencia electrónica y sus características operativas que consiste en un acceso especial a un apartado específico de la sede electrónica con el cual se entiende practicada la notificación.

También ocupan un lugar destacado, el documento electrónico y sus copias. Aquí se tratan detalles sobre las características de los documentos electrónicos y sus metadatos como el disponer de información identificativa suficiente para permitir su individualización, detalles sobre las copias electrónicas como que incluyan su carácter de copia entre sus metadatos, detalles sobre la destrucción de documentos en papel como la necesidad de una resolución del órgano responsable del procedimiento y la prohibición de la destrucción de documentos con valor histórico, artístico u otro carácter relevante.

Se detalla además cómo se han de entender los conceptos de marca de tiempo y sello de tiempo en los documentos administrativos electrónicos siendo la diferencia básicamente que el primero consiste en una simple referencia temporal electrónica en el documento y el segundo en una marca similar, pero con intervención de un tercero de confianza que es el prestador de servicios de sellado de tiempo.

El expediente electrónico, archivo electrónico y conservación de los documentos electrónicos se tratan en los últimos capítulos de este título. Se tratan cuestiones como, por ejemplo, las reglas para determinar los plazos mínimos de conservación de los documentos electrónicos.

Se hace explícita la idea de compulsas electrónicas en el artículo 50 (la Ley 11/2007 no llega a utilizar el término de compulsas como tal aunque su contenido ya establece implícitamente esta posibilidad), que consiste en la



obtención de copias electrónicas a efectos de compulsión, además se detallan cuestiones como que los periodos mínimos de conservación de los documentos electrónicos de un procedimiento se determinan por cada órgano responsable y que los documentos electrónicos incorporados al expediente electrónico han de disponer de formatos de larga duración.

El Reglamento termina con una larga serie de disposiciones en las cuales, entre otras cosas se establecen los plazos de 6 meses para la creación del directorio de sedes electrónicas, 4 meses para la adaptación de las sedes electrónicas y 6 meses para adaptación de los registros electrónicos y se deroga Real Decreto 263/1996, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

3.5 Real Decreto 3/2010 de 8 de enero.

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicio.

Este decreto es de aplicación a todas las administraciones incluidas en el ámbito de aplicación de la Ley 11/2007.

Siguiendo las previsiones del artículo 42 de la Ley 11/2007, en Enero del 2010 han sido publicados el Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad (ENI).

El 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, tiene como objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Tal como se comenta en la exposición de motivos de esta norma, cuenta con una serie de precedentes que han inspirado su contenido, documentos de la Administración en materia de seguridad electrónica, tales como los Criterios SNC, las Guías CCN-STIC del Centro Criptológico Nacional, la Metodología de análisis y gestión de riesgos MAGERIT o el Esquema Nacional de Interoperabilidad.

Tiene en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes y la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

El ENS empieza por definir sus principios básicos que son la seguridad integral, la gestión de riesgos, la prevención, reacción y recuperación, las líneas de defensa, la reevaluación periódica, y la función diferenciada por la cual se entiende que en los sistemas de información se diferenciará:

- El responsable de la información
- El responsable del servicio
- El responsable de la seguridad.

Cabe destacar aquí además que el ENS incluye en las dimensiones de seguridad a tener en cuenta la trazabilidad de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias, un aspecto de seguridad al que la Ley 11/2007 no aludía de una manera explícita.

Se establece que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, la cual debe incluir un número importante de requisitos mínimos. Dada la importancia de este punto se enumera a continuación la lista completa de los mismos, del artículo 11, junto con algunos de los detalles que se especifican en los artículos siguientes:

- Organización e implantación del proceso de seguridad, que deberá comprometer a todos los miembros de la organización.
- Análisis y gestión de los riesgos.
- Gestión de personal, donde destaca el hecho de que todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos en la que se valorarán positivamente los productos certificados.
- Seguridad por defecto, es decir, los sistemas deben diseñarse y configurarse de forma que garanticen, al menos, unos mínimos de seguridad por defecto.

3.6 Real Decreto 4/2010 de 8 de enero.

El Esquema Nacional de Interoperabilidad comprende los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deben ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de



interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica.

Este decreto también es de aplicación a todas las administraciones incluidas en el ámbito de aplicación de la Ley 11/2007.

Las principales obligaciones que se derivan de este real decreto, son:

- Las Administraciones públicas establecerán y publicarán las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que pongan a disposición del resto de Administraciones especificando las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los mecanismos necesarios de gobierno de los sistemas interoperables, así como las condiciones de seguridad aplicables.
- Las Administraciones públicas mantendrán actualizado un Inventario de Información Administrativa, que incluirá los procedimientos administrativos y servicios que prestan de forma clasificada y estructurados en familias, con indicación del nivel de informatización de los mismos. Asimismo mantendrán una relación actualizada de sus órganos administrativos y oficinas de registro y atención al ciudadano, y sus relaciones entre ellos. Dichos órganos y oficinas se codificarán de forma unívoca y esta codificación se difundirá entre las Administraciones públicas.
- Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica, persigue 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, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunde en beneficio de la eficacia y la eficiencia.

Al igual que ocurre en el ENS, se han tenido en cuenta antecedentes como los Criterios SNC y las recomendaciones de la Unión Europea como lo es el Marco Europeo de Interoperabilidad, así como a otros instrumentos y actuaciones elaborados por este programa y que inciden en alguno de los múltiples aspectos de la interoperabilidad, tales como el Centro Europeo de Interoperabilidad Semántica, el Observatorio y Repositorio de Software de Fuentes Abiertas y la Licencia Pública de la Unión Europea. También se atiende a la Decisión 922/2009 del Parlamento Europeo y del Consejo, de 16

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas.

Después de definir el objeto y ámbito de aplicación de la norma (que incluye a todas las administraciones), el ENI comienza enumerando sus principios básicos, que son:

- La interoperabilidad como cualidad integral.
- El carácter multidimensional de la interoperabilidad (es decir, interoperabilidad técnica, semántica y organizativa).
- El enfoque de soluciones multilaterales.

A continuación se abordan con mayor detalle las dimensiones técnicas, semánticas y organizativas de la interoperabilidad. En la parte técnica se desarrolla el principio de neutralidad tecnológica de la Ley 11/2007 en aspectos concretos como los documentos electrónicos emitidos por las Administraciones Públicas y se reitera su importancia haciendo hincapié en el uso de estándares abiertos a todos los niveles considerando su aplicación particularmente inexcusable en la relación con los ciudadanos. Se introduce además el criterio de coste que no suponga una dificultad de acceso para la selección de estos estándares y se provee una definición de uso generalizado por los ciudadanos.

En cuanto a la interoperabilidad semántica ésta se centra fundamentalmente en la creación y publicación, en su momento, a través del Centro de Interoperabilidad Semántica de la Administración de unos modelos de datos de intercambio que serán de preferente aplicación para el intercambio de información entre las Administraciones públicas.

La parte organizativa se centra, por una parte, en la obligación de las administraciones de la especificación y publicación de los requisitos técnicos de los servicios, datos y documentos electrónicos puestos a disposición de otras administraciones y, por otra parte, prevé la creación de inventarios de información administrativa a través de los cuales las administraciones han de publicar sus procedimientos administrativos y servicios.

Merece mención la reutilización y transferencia de tecnología que promueve la libre disposición de las aplicaciones desarrolladas por una Administración a las demás y las condiciones necesarias para ello en el modelo de licencia del software libre. Por otra parte, se establece el compromiso de la Administración General del Estado de mantener a través del CTT un directorio de aplicaciones libremente reutilizables y se describen mecanismos de integración con directorios europeos similares que deben seguir los directorios propios de cada Administración.

La interoperabilidad de la firma electrónica se articula en torno a la política de firma electrónica y de certificados que se desarrollará como parte del futuro desarrollo del propio previsto en la disposición adicional primera y que las



aplicaciones de las Administraciones Públicas deberán respetar. Esta política tratará, entre otras cuestiones, las relacionadas con la interoperabilidad:

- Formatos de firma.
- Los algoritmos a utilizar y longitudes mínimas de las claves.
- Las reglas de creación y validación de la firma electrónica.
- La gestión de las políticas de firma, el uso de las referencias temporales y de sellos de tiempo.
- La normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre Administraciones Públicas.

Por otra parte se tratan los aspectos de interoperabilidad relativos a los prestadores de servicios de certificación en su vertiente organizativa, semántica y técnica. Se abordan cuestiones como la obligación de publicar en su Declaración de Prácticas de Certificación cuestiones como los usos de sus certificados y sus posibles límites, los niveles de acuerdo de servicio, la indicación expresa de aquellos campos de los certificados que por su unicidad puedan ser usados para la identificación o la obligatoriedad de la incorporación, dentro de los certificados, de información relativa a las direcciones de Internet donde se ofrecen servicios de validación por parte de los prestadores de servicios de certificación.

Por último se tratan las obligaciones de las plataformas de validación de certificados electrónicos y de firma electrónica como lo es, por ejemplo, la incorporación de listas de confianza de los certificados interoperables entre las distintas Administraciones Públicas nacionales y europeas.

Otro tema clave es la recuperación y conservación del documento electrónico:

- Se establecen las condiciones para la recuperación y conservación del documento electrónico que prevén, entre otras, cosas como la definición de una política de gestión de documentos por parte de las Administraciones Públicas, la identificación única e inequívoca de cada documento o la clasificación de acuerdo con un plan de clasificación.
- Se establecen medidas de seguridad para asegurar la conservación de los documentos electrónicos, se reitera la obligación de la adecuada protección de los datos personales y se prevé el uso de formatos de firma longeva y otros mecanismos como metadatos de gestión de documentos que permitan la conservación a largo plazo de los documentos electrónicos.
- Se aborda la cuestión del formato de los documentos electrónicos. Se prevén cosas como el uso preferentemente de formatos basados en estándares abiertos y la elección de formatos de documento electrónico normalizados y perdurables que aseguren la independencia de los datos

de sus soportes. Incluso se prevé la posibilidad de copiado auténtico de los documentos ante un posible riesgo de obsolescencia del formato.

- Por último se trata la digitalización de documentos en soporte papel indicando que ésta se deberá ajustar a la norma técnica de interoperabilidad correspondiente a los aspectos del formato estándar utilizado, el nivel de resolución, la garantía de imagen fiel e íntegra y los metadatos asociados al proceso de digitalización.

El Capítulo XI, establece básicamente la obligación de la conformidad de las sedes electrónicas y el ciclo de vida de los sistemas y servicios con el ENI, junto con la obligación para los órganos y entidades de derecho público de establecer los oportunos mecanismos de control y publicar su declaración de conformidad con el ENI. El último capítulo del ENI se compone únicamente de un único artículo que establece la obligación de mantener el ENI actualizado de manera permanente.

El ENI concluye con una serie de disposiciones y un anexo con un glosario de términos muy útil y completo. Entre las disposiciones se puede destacar especialmente la disposición adicional primera que se refiere al desarrollo del Esquema Nacional de Interoperabilidad. Este desarrollo se concretará en una serie de normas técnicas de interoperabilidad e instrumentos de interoperabilidad.

Las normas técnicas se referirán a cuestiones como un catálogo de estándares que satisfagan las previsiones del ENI, metadatos relativos al documento electrónico, estructura y formato del expediente electrónico, la antes mencionada política de firma electrónica y de certificados de la Administración, relación de modelos de datos comunes en la Administración o una política de gestión de documentos electrónicos.

En cuanto a los instrumentos de interoperabilidad estos se compondrán de un inventario de procedimientos administrativos y servicios prestados, el centro de interoperabilidad semántica de la Administración y el directorio de aplicaciones para su libre reutilización.

3.7 LAECSP

La Ley 11/2007 es la primera norma legal con rango de ley que se centra enteramente en la problemática propia de la Administración Electrónica, es por tanto la norma legal de referencia en esta materia.

Su principal objetivo es reconocer y garantizar el derecho del ciudadano a relacionarse por medios electrónicos con las Administraciones Públicas. Por otra parte se pretende impulsar el uso de los servicios electrónicos en la Administración creando las condiciones necesarias, y de manera indirecta ejercer con ello un efecto arrastre sobre la sociedad de la información en general.



Las Administraciones Públicas tienen la obligación de posibilitar el acceso a todos sus servicios electrónicos, incluyendo registros, pago, notificaciones y la consulta del estado de tramitación de sus procedimientos desde el 31 de diciembre del 2009.

La ley se estructura en 5 títulos que se resumen brevemente a continuación:

Título Preliminar. Ámbito de Aplicación y los Principios Generales

Este título aborda los objetivos ya mencionados y expone los fines de la ley tales como el facilitar el ejercicio de derechos y cumplimiento de deberes por medios electrónicos, el acceso a información y a los procedimientos, y la creación de las condiciones de confianza necesaria para que se usen. Esto debe contribuir a una mayor proximidad con el ciudadano y la transparencia administrativa.

Por otra parte debe mejorarse el funcionamiento interno incrementando la eficiencia y eficacia con el uso de las tecnologías de la información, a la vez que simplificar los procedimientos, y promover una mayor participación y transparencia de los mismos para los ciudadanos.

También se declaran una larga serie de principios como el principio de igualdad (entendido como no discriminación de aquellas personas que no disponen de un acceso fácil a medios electrónicos), el respeto a la Ley Orgánica 15/1999, de Protección de Datos personales, la accesibilidad y un especial cuidado en los aspectos de seguridad tanto a nivel jurídico como de la tecnología.

Se pueden destacar también el principio de neutralidad tecnológica y uso de estándares abiertos en el uso de las tecnologías de la información.

Título I. Derecho de los Ciudadanos a relacionarse con las Administraciones Públicas por Medios Electrónicos

Incluye por una parte a nivel general el ejercicio por medios electrónicos de los derechos previstos ¿en? el artículo 35 de la Ley 30/1992 y por otra parte una serie de derechos nuevos como el pago electrónico, la notificación electrónica, las copias electrónicas de documentos, elección del canal a utilizar (al menos sede electrónica, teléfono, presencial), la obtención de los medios de identificación electrónica necesarios, el derecho a utilizar el DNle en cualquier trámite electrónico, la calidad de los servicios electrónicos prestados o el derecho a elegir las aplicaciones o sistemas para relacionarse con las AAPP siempre y cuando estén basadas en estándares abiertos. La especial importancia de la protección de los derechos de los ciudadanos se refleja también en la introducción de la nueva figura del Defensor del usuario de la Administración electrónica.

Título II. Régimen Jurídico de la Administración Electrónica

En este capítulo se abordan cuatro grandes cuestiones:

- El nuevo concepto de sede electrónica,
- Las garantías en torno a la identificación y la autenticación,
- Los registros, comunicaciones y notificaciones electrónicas,
- Los documentos y archivos electrónicos.

La sede electrónica es, como dice el artículo 10, *aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.*

Hasta aquí sería aparentemente la Web institucional de toda la vida, de no ser porque al concepto de sede la ley asocia expresamente ciertas características. Fundamentalmente la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios, el hecho de que la publicación de diarios o boletines oficiales reviste los mismos efectos que la publicación impresa y que puede actuar como sustituta o complemento al tablón de anuncios o edictos. Además, han de tenerse en cuenta las condiciones que han de cumplir las sedes electrónicas de la Administración General del Estado en el marco del Real Decreto 1671/2009.

En cuanto a la identificación y autenticación cabe destacar por una parte que el DNIe se establece como medio universal que debe ser aceptado universalmente por las administraciones para la identificación, autenticación y firma electrónica de los ciudadanos. Se admite el uso de la firma electrónica avanzada como medio seguro de firma de documentos y se regula la admisión de otras alternativas como lo pueden ser combinaciones usuario/clave, con la única limitación de que la Administración en cuestión puede decidir la relación concreta de los correspondientes tipos de certificados admitidos.

Referente a la Administración se detalla el concepto de *sello electrónico* (firma electrónica de la Administración, órgano, etc. que corresponda) diferenciando así este tipo de firma de la firma personal de los empleados públicos. Por otra parte es muy importante la regulación del código seguro de verificación, ya que dará lugar ciertas posibilidades como disponer de un sello automatizado válido y verificable en una copia impresa del documento. Este código se podrá consultar en el órgano administrativo correspondiente para comprobar la veracidad del documento emitido por una Administración conservando así plenas garantías jurídicas también desde una copia impresa de un documento electrónico, lo cual a su vez permite facilitar en gran medida la necesaria convivencia entre mundo electrónico y papel hasta que algún día el papel realmente deje de ser necesario.

Se crean nuevas complejidades con la interoperabilidad y la necesidad del mutuo reconocimiento de la identificación, autenticación y firma basada en



certificados electrónicos. En esa línea se establece la obligación para la Administración General del Estado de disponer de una plataforma de verificación del estado de revocación de certificados electrónicos que actualmente se encuentra implementada con el servicio horizontal @Firma de la Red SARA.

Hay que mencionar especialmente la identificación y autenticación de los ciudadanos por funcionario público. Esta es también una cuestión que anteriormente no se encontraba prevista y que añade una importante mejora de flexibilidad al marco legal que había hasta la fecha en materia de Administración electrónica, ya que permite evitar en gran medida el uso de la vía del papel para aquellas personas que no dispongan de medios o conocimientos para realizar un trámite por la vía electrónica, siempre que lo consienten, aunque el hecho de disponer de la ayuda de un funcionario debería ser en muchos casos un buen motivo para ello.

Se abordan además los registros, las comunicaciones y las notificaciones electrónicas. Se hace referencia a cuestiones como los tipos de documentos admitidos, admitiéndose prácticamente cualquiera, tanto estructurados (formularios Web de la página del trámite) o bien libres (un simple documento Word, por ejemplo), requisitos para los acuses de recibo devueltos al ciudadano, la disponibilidad 24x7 de los registros, requisitos de seguridad en las comunicaciones electrónicas con las Administraciones Públicas, necesidad del consentimiento del ciudadano para las comunicaciones electrónicas, posibilidad de reglamentar el uso obligatorio de la vía electrónica para personas jurídicas o colectivos de personas físicas, práctica de la notificación por medios electrónicos, requisitos y efectos de ello, plazos, etc.

Se define el concepto de documento electrónico administrativo junto con la copia electrónica de documentos, incluyendo documentos digitalizados que originalmente se encontraban en papel, algo que facilitará en gran medida el periodo de transición entre la Administración basada en el papel y la electrónica.

El concepto de expediente administrativo se lleva al mundo de la Administración electrónica con el expediente electrónico, al cual se trasladan en aras de las garantías de integridad del mismo incluso conceptos que se asocian propiamente al mundo del papel como lo es el foliado del expediente.

Título III. De la Gestión electrónica de los Procedimientos

Este título se centra en los aspectos a tener en cuenta en la gestión de los procedimientos administrativos cuando se utilizan medios electrónicos para ello. Se trata de asegurar que el uso de los medios electrónicos no socave las garantías jurídicas propias de los procedimientos, y aprovechar las oportunidades de mejora y simplificación que ofrece para la gestión de los mismos.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

En este sentido se recalcan aspectos como que la gestión electrónica debe respetar la titularidad y el ejercicio de la competencia por la Administración, órgano o entidad que la tenga atribuida o la necesidad de la formación adecuada del personal que utilice los medios electrónicos. Por otra parte el artículo 34 dispone el precepto general de que la aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios irá siempre precedida de la realización de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio.

En lo que resta del título se abordan diversos detalles sobre las fases de iniciación, instrucción y terminación del procedimiento, detalles como la posibilidad de poder aportar copias digitalizadas de documentos al expediente o la posibilidad de poder consultar por vía electrónica el estado de tramitación del expediente.

Título IV. Cooperación entre Administraciones para el Impulso de la Administración Electrónica

En este título se trata la problemática inherente a nuestro modelo de Estado descentralizado en la medida que afecta a las cuestiones propias de la administración electrónica, y la trata a tres niveles:

- En primer lugar se trata desde la perspectiva organizativa e institucional con la creación del Comité Sectorial de Administración Electrónica dependiente de la Conferencia Sectorial de Administración Electrónica que se establece como el órgano técnico de cooperación entre las tres Administraciones en esta materia. Sus principales responsabilidades son velar por la compatibilidad e interoperabilidad de las aplicaciones y sistemas, y la coordinación de programas conjuntos de actuación.
- La interoperabilidad en sí misma. Las TIC se deben utilizar en las relaciones entre las propias administraciones y con los ciudadanos, aplicando medidas informáticas, tecnológicas, organizativas, y de seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica.

Para conseguir este objetivo se definen varias medidas: la creación del Esquema Nacional de Interoperabilidad y del Esquema Nacional de Seguridad (ENS), la Red SARA (Red de comunicaciones de las Administraciones Públicas españolas) y la Red 060 (Red integrada de atención al Ciudadano).

- La cooperación que se aborda es la cooperación mediante el intercambio y reutilización de los sistemas y aplicaciones desarrolladas, y la transferencia de tecnología y de conocimiento entre Administraciones. Aquí se consagra también la idea de un directorio general de aplicaciones para su reutilización que en la realidad ha tomado forma como el Centro de Transferencia de Tecnologías (CTT).

3.8 Adaptación de procedimientos a la LAECSP

El desarrollo del Plan de Actuación tiene como uno de sus focos esenciales la necesidad de adaptar la totalidad de los procedimientos a la LAECSP. La adopción de medidas y la articulación del calendario de adaptación requieren de una previa consideración de la situación de partida, descrita mediante la definición de los requerimientos de adaptación a la Ley, el análisis global de la situación de los procedimientos y un análisis departamental. Instrumentos que fundamentan la estrategia a adoptar por la Administración General del Estado

3.8.1 Requerimientos de adaptación a la LAECSP

Considerando los objetivos fijados por la propia LAECSP, resulta necesaria una definición previa de lo que la Ley requiere para considerar a un procedimiento o actuación administrativa como adaptados a sus requerimientos.

A tal fin, y sin reproducir extensamente los derechos y regulaciones contenidos en la LAECSP, a continuación se incluye una relación de requerimientos que se estiman apropiados para evaluar el grado de adaptación a la LAECSP. Tales requerimientos se han clasificado en una doble categoría:

- Básicos, que constituyen características mínimas que el procedimiento debe cumplir y que no dependen de terceros agentes.
- Adicionales, requerimientos que dependen de agentes externos al procedimiento (por ejemplo, el acceso a datos para no requerirlos) y de factores tecnológicos de interoperabilidad.

Requerimientos Básicos

- Información electrónica. Disponibilidad de información sobre las características y requisitos del procedimiento.
- Iniciación electrónica. Contar con un formulario electrónico conectado a un registro electrónico, que posibilite la presentación por medios electrónicos de las solicitudes, comunicaciones y documentos del procedimiento.
- Pago electrónico. Posibilidad de efectuar pagos a las Administraciones Públicas a través de medios electrónicos.
- Notificaciones y comunicaciones electrónicas. Sistema de notificaciones electrónicas y las comunicaciones con el ciudadano para actuaciones

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

como la presentación de alegaciones, la obtención de información y la realización de consultas.

- Consulta del estado de tramitación. Habilitar sistemas de consulta del estado del expediente; es decir, posibilitar al ciudadano a acceder al estado de tramitación de los procedimientos en los que sean interesados.

Análisis general de los procedimientos.

La relación actual de procedimientos de la Administración General del Estado contenida en el Sistema de Información Administrativa (SIA), cuenta con 2.641 procedimientos administrativos, la mayor parte de los cuales están orientados a servicios a ciudadanos y empresas, salvo un grupo de carácter interno formado por 228 procedimientos, quedando por tanto un total de 2.413 procedimientos administrativos a tener en cuenta para la elaboración del calendario de adaptación.

Aunque con ello no se agotan todos los requerimientos establecidos por la Ley 11/2007, con la finalidad de medir el grado de adaptación de los procedimientos se ha adoptado una clasificación en niveles semejante a la establecida por la Unión Europea:

- Inadaptación total (nivel 0): procedimientos que carecen de información publicada por medios electrónicos.
- Muy baja adaptación (nivel 1): procedimientos de los que sólo se ha publicado información por medios electrónicos.
- Baja adaptación (nivel 2): Procedimientos con información y disponibilidad de formulario de iniciación descargable.
- Adaptación parcial (nivel 3): Procedimientos que permiten su iniciación por medios electrónicos.
- Adaptación total (nivel 4): Procedimientos adaptados a los requisitos fijados por la LAECSP.

A los niveles anteriores se ha añadido un quinto nivel de mayor desarrollo, que se ha denominado proactividad, y que no es exigido por la Ley, pero que ya cumplen algunos procedimientos existentes:

- Proactividad (nivel 5): Procedimientos que interactúan con el ciudadano mediante alertas personalizadas, precumplimentación de datos, etc.

3.9 Ley 59/2003

La Ley 59/2003 de Firma Electrónica incorpora al derecho español la normativa legal europea en materia de firma electrónica, concretamente la Directiva



1999/93/CE por la que se establece un marco comunitario para la firma electrónica. La ley regula fundamentalmente las siguientes cuestiones:

- El concepto de firma electrónica.
- Los certificados electrónicos.
- Los prestadores de servicios de certificación (es decir, que actúan como autoridades de certificación, autoridades de registro, etc.).
- Los dispositivos de creación de firma y de verificación de firma.
- El régimen de supervisión y control.
- El régimen de infracciones y sanciones.

La Ley empieza por el régimen de la prestación de los servicios de certificación estableciendo que no está sujeta a autorización previa y se realizará en régimen de libre competencia. Por otra parte define los tres tipos de firma electrónica:

- Firma electrónica.
- Firma electrónica avanzada.
- Firma electrónica reconocida.

Se matizan aspectos importantes del uso de la firma electrónica en el ámbito de las Administraciones Públicas. Destacar también especialmente los artículos 3.5 y 3.8, introducidos como modificaciones a través de la Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información donde se aclara el concepto de documento electrónico y aspectos relevantes respecto de la admisión de datos firmados electrónicamente como prueba documental en caso de juicio.

Se detallan, también, de manera especialmente intensiva los certificados electrónicos y quienes los expiden, es decir, los prestadores de servicios de certificación. En esta parte tienen especial importancia el concepto de certificado reconocido (el que va asociado a la firma electrónica reconocida) y los requisitos para que un certificado electrónico se pueda considerar como tal, donde destaca la obligación para los prestadores que los expiden de contratar un seguro de responsabilidad civil de, al menos, 3.000.000€. Por otra parte se establece la validez universal del DNI electrónico como medio universal de identificación y firma que cualquier persona física o jurídica ha de reconocer.

El siguiente título se centra en los dispositivos de firma electrónica y los sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica, cabe destacar el hecho de que la certificación de los prestadores se regula sobre una base voluntaria, la definición del concepto de dispositivo seguro de creación de firma, la certificación de este tipo

de dispositivos y la referencia a las condiciones para el reconocimiento de conformidad con la Ley de los productos de firma electrónica.

La Ley termina finalmente con los títulos habituales relativos a la supervisión y control en la materia, y el régimen de infracciones y sanciones.

3.10 Derechos y obligaciones

España es uno de los pocos países de nuestro entorno que ha reconocido por ley el derecho de los ciudadanos a poder relacionarse electrónicamente con las Administraciones Públicas. La ley 11/2007 está articulada en torno a este derecho, declarado en el primer artículo de la Ley.

Artículo 1. Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

Los 8 restantes artículos del Título I de la Ley, de Derechos de los Ciudadanos, desarrollan más en detalle este primer artículo, que supone un cambio sustancial en la forma de entender la relación entre las Administraciones y los ciudadanos, porque pone en manos de éstos la posibilidad de exigir a las Administraciones Públicas como debe suministrarle los servicios.

Este reconocimiento explícito de nuevos derechos ciudadanos, se transforma, del lado de los Ayuntamientos y Administraciones Públicas, en una declaración de deberes: éstas tienen la obligación de hacer efectivo este derecho.

Las Administraciones Públicas son, a su vez, también sujetos de derechos. Están obligadas a cooperar entre sí, y tienen derecho a que las otras administraciones cooperen. En este sentido destaca el derecho de los ciudadanos a *no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información (...)*. Este artículo garantiza el derecho de las administraciones a exigir entre sí el suministro electrónico de dicha información. La obligación de cooperar de todas las administraciones públicas es uno de los grandes impulsores para el desarrollo de la Administración electrónica en nuestro país: sin esta cooperación sería muy difícil lograr la plena aplicación de la ley y permitir que los ciudadanos pudieran relacionarse electrónicamente con las administraciones en igualdad de condiciones de acceso.

3.10.1 Derechos de los ciudadanos



En la *Exposición de motivos VI* de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos se presentan brevemente los derechos que reconoce la ley a los ciudadanos:

“En el Título Primero de la LAECSP están recogidos los derechos de los ciudadanos en sus relaciones con las Administraciones Públicas a través de medios electrónicos. Para garantizar el pleno ejercicio de estos derechos, se establece la obligación de las Administraciones de habilitar diferentes canales o medios para la prestación de los servicios electrónicos. Asimismo, se establece la obligación de cada Administración de facilitar a las otras Administraciones los datos de los interesados que se le requieran y obren en su poder, en la tramitación de un procedimiento, siempre que el interesado preste su consentimiento expreso, el cual podrá emitirse y recabarse por medios electrónicos, al objeto de que los ciudadanos no deban aportar datos y documentos que están en poder de las Administraciones Públicas.”

De este título primero, Derechos fundamentales de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, el artículo en el que se reconocen los derechos de los ciudadanos es el *artículo 6*. En el apartado 1º de este artículo de la LAECSP se hace referencia al *artículo 35* de la Ley 30/1992 por lo que a continuación detallamos su contenido para que en este punto queden recogidos todos los derechos que la Ley 11/2007 reconoce a los ciudadanos, vengán incluidos en esta misma ley o en otras, como es el caso de los derechos enumerados en el *artículo 6.1* al cual hacemos aquí mención.

Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Artículo 35. Derechos de los ciudadanos.

Los ciudadanos, en sus relaciones con las Administraciones Públicas, tienen los siguientes derechos:

- A conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados, y obtener copias de documentos contenidos en ellos.
- A identificar a las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos.
- A obtener copia sellada de los documentos que presenten, aportándola junto con los originales, así como a la devolución de éstos, salvo cuando los originales deban obrar en el procedimiento.
- A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del Ordenamiento Jurídico.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- A formular alegaciones y a aportar documentos en cualquier fase del procedimiento anterior al trámite de audiencia, que deberán ser tenidos en cuenta por el órgano competente al redactar la propuesta de resolución.
- A no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate, o que ya se encuentren en poder de la Administración actuante.
- A obtener información y orientación acerca de los requisitos jurídicos o técnicos que las disposiciones vigentes impongan a los proyectos, actuaciones o solicitudes que se propongan realizar.
- Al acceso a los registros y archivos de las Administraciones Públicas en los términos previstos en la Constitución y en ésta u otras Leyes.
- A ser tratados con respeto y deferencia por las autoridades y funcionarios, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.
- A exigir las responsabilidades de las Administraciones Públicas y del personal a su servicio cuando así corresponda legalmente.
- Cualesquiera otros que les reconozcan la Constitución y las Leyes.

A continuación, presentamos el *artículo 6* de la LAECSP:

Artículo 6. Derechos de los ciudadanos

1. Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el *artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.
2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos:
 - A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas.
 - A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el



consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.

- A la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas.
 - A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos.
 - A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.
 - A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.
 - A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.
 - A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.
 - A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
 - A la calidad de los servicios públicos prestados por medios electrónicos.
 - A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.
3. En particular, en los procedimientos relativos al establecimiento de actividades de servicios, los ciudadanos tienen derecho a obtener la siguiente información a través de medios electrónicos:

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio. Los datos de las autoridades competentes en las materias relacionadas con las actividades de servicios, así como de las asociaciones y organizaciones profesionales relacionadas con las mismas.
- Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios y las vías de recurso en caso de litigio entre cualesquiera autoridades competentes, prestadores y destinatarios.

En resumen, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos por la Ley, un conjunto de derechos complementarios tales como:

- Acceso electrónico a las Administraciones Públicas.
- Elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas.
- No aportar documentación que obre en poder de las Administraciones Públicas.
- La igualdad en el acceso electrónico a los servicios de las Administraciones Públicas.
- Acceder por medios electrónicos a la información de los expedientes.
- Obtener copias electrónicas.
- La conservación en formato electrónico, por parte de las Administraciones Públicas, de los documentos electrónicos que formen parte de un expediente.
- Usar la firma electrónica como medio de identificación y presentación de documentación.
- La garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
- Calidad de los servicios públicos prestados por medios electrónicos.
- Utilizar estándares abiertos para comunicarse con las Administraciones Públicas.

3.10.2 Obligaciones de los Ayuntamientos

Atendiendo a los derechos indicados que la Ley reconoce a los ciudadanos y resto de los articulados en la LAECSP, se pueden inferir una serie de requisitos mínimos y otros opcionales que los Ayuntamientos deben cumplir para su



adecuación a la Ley. Este documento pretende desmenuzar la LAECSP en requisitos concretos que todos los Ayuntamientos deben cumplir para adaptarse a la Ley y categorizarlos de una forma sistemática en áreas de actuación.

Es importante volver a indicar en este punto que en la actualidad, los ayuntamientos que no dispongan de recursos económicos suficientes no estarán obligados a ofrecer los servicios a los que hace mención la Ley 11/2007 puesto que según el *apartado 4* de la *Disposición final tercera, adaptación de las Administraciones Públicas para el ejercicio de derechos*, en relación a la Administración Local, los ciudadanos podrán ejercer los derechos que se les reconoce en el *artículo 6* de la LAECSP a partir del 31 de diciembre de 2009 siempre que lo permitan sus disponibilidades presupuestarias.

Del título primero, Derechos fundamentales de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, los artículos de la LAECSP en los que se indican algunas de las obligaciones que las Administraciones Públicas deberán cumplir son:

Artículo 8. Garantía de prestación de servicios y disposición de medios e instrumentos electrónicos.

1. Las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.
2. La Administración General del Estado garantizará el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de varios canales que cuente, al menos, con los siguientes medios:
 - Las oficinas de atención presencial que se determinen, las cuales pondrán a disposición de los ciudadanos de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 6 de esta Ley, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.
 - Puntos de acceso electrónico, consistentes en sedes electrónicas creadas y gestionadas por los departamentos y organismos públicos y disponibles para los ciudadanos a través de redes de comunicación. En particular se creará un Punto de acceso general a través del cual los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles. Este Punto de acceso general contendrá la

relación de servicios a disposición de los ciudadanos y el acceso a los mismos, debiendo mantenerse coordinado, al menos, con los restantes puntos de acceso electrónico de la Administración General del Estado y sus Organismos Públicos.

- Servicios de atención telefónica que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a los ciudadanos el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores.

Artículo 9. Transmisiones de datos entre Administraciones Públicas

1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.
2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley.

Del título segundo, Régimen jurídico de la Administración electrónica, los artículos en los que se indican algunas de las obligaciones que las Administraciones Públicas deberán cumplir son:

Artículo 10. La sede electrónica

1. La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.
2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.



3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

Artículo 12. Publicación electrónica del tablón de anuncios o edictos.

La publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente.

Artículo 13. Formas de identificación y autenticación.

- Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.
- Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:
 - En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.
 - Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.
 - Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

Artículo 22. Identificación y autenticación de los ciudadanos por funcionario público.

- En los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos en el artículo 13 de los que aquel no disponga, tal identificación o autenticación podrá ser

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

válidamente realizada por funcionarios públicos mediante el uso del sistema de firma electrónica del que estén dotados.

- Para la eficacia de lo dispuesto en el apartado anterior, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.
- Cada Administración Pública mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación regulada en este artículo.

Artículo 24. Registros electrónicos.

- Las Administraciones Públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.
- Los registros electrónicos podrán admitir:
 - Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.
 - Cualquier solicitud, escrito o comunicación distinta de los mencionados en el apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.
- En cada Administración Pública existirá, al menos, un sistema de registros electrónicos suficiente para recibir todo tipo de solicitudes, escritos y comunicaciones dirigidos a dicha Administración Pública. Las Administraciones Públicas podrán, mediante convenios de colaboración, habilitar a sus respectivos registros para la recepción de las solicitudes, escritos y comunicaciones de la competencia de otra Administración que se determinen en el correspondiente convenio.

Artículo 31. Archivo electrónico de documentos.

- Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.
- Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.



- Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Del título tercero, de la gestión electrónica de los procedimientos, los artículos en los que se indican algunas de las obligaciones que las Administraciones Públicas deberán cumplir son:

Artículo 33. Utilización de medios electrónicos.

- La gestión electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa.

Artículo 37. Acceso de los interesados a la información sobre el estado de tramitación.

- En los procedimientos administrativos gestionados en su totalidad electrónicamente, el órgano que tramita el procedimiento pondrá a disposición del interesado un servicio electrónico de acceso restringido donde éste pueda consultar, previa identificación, al menos la información sobre el estado de tramitación del procedimiento, salvo que la normativa aplicable establezca restricciones a dicha información. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados.
- En el resto de los procedimientos se habilitarán igualmente servicios electrónicos de información del estado de la tramitación que comprendan, al menos, la fase en la que se encuentra el procedimiento y el órgano o unidad responsable.

De las disposiciones finales, la disposición en la que se indican algunas obligaciones que las Administraciones Públicas deberán cumplir son:

Disposición final tercera. Adaptación de las Administraciones Públicas para el ejercicio de derechos.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

1. *“...cada Administración Pública hará pública y mantendrá actualizada la relación de dichos procedimientos y actuaciones”.*

En resumen, las Administraciones Públicas tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos por la Ley, las siguientes obligaciones:

- Fomentar múltiples canales de acceso a la información.
- Asegurar la interoperabilidad organizativa, semántica y técnica.
- Validez documental y de gestión de la copia electrónica.
- Herramientas de consulta del expediente electrónico.
- Admitir el DNI-e y demás sistemas de firma electrónica.
- Estrategia documental y repositorio unificado de documentos.
- Cumplimiento de la LOPD.
- Medir la calidad de los servicios prestados.
- Disponibilidad 24x7.
- Calidad de los servicios públicos prestados por medios electrónicos.
- Compatibilidad con los diferentes navegadores y formatos.

La LAECSP cambia radicalmente el panorama de la Administración electrónica, ya que pasa de ser una iniciativa a instancias de la Administración Pública, que definían, implantaban, gestionaban y ponían a disposición del ciudadano los servicios en función de criterios propios, a constituirse como un derecho del ciudadano a comunicarse con las Administraciones por medios electrónicos y por tanto como una obligación para éstas. Esta nueva concepción obliga a definir unas áreas de actuación sobre las que la LAECSP actúa directamente y sobre las que se defina un plan de actuación al que debe dar respuesta cada Ayuntamiento, al igual que el resto de Administraciones Públicas.

Para el cumplimiento de la LAECSP, a nivel de Ayuntamiento, se han definido diferentes áreas de actuación sobre las que se deben poner en marcha las medidas para adaptarse a la Ley:

- Fomentar múltiples canales de acceso a la información.
- Adaptación de los Canales de comunicación: habilitando los medios necesarios para la prestación de Servicios Públicos digitales a los ciudadanos (Art. 8.1).
- Adaptación de procedimientos administrativos a la tramitación electrónica: adaptación de los trámites de los procedimientos administrativos que se inician a instancia de parte, y que deben ser transformados en Servicios Públicos Electrónicos y facilitarse por medios telemáticos a los ciudadanos (Art 9, 10 y Disposición Final tercera).



- Adaptación de la Tecnología de Front-Office: entendido como la tecnología específica de soporte a la Administración Electrónica y que deberá permitir la comunicación entre ciudadanos y Administración (Artículo 10).
- Adaptación de la Tecnología de Back-Office o Sistema de Gestión Integral (SGI): adaptando la tecnología de soporte a los procesos internos de la Administración y su integración con el Front-Office.
- Adaptación organizativa: en este punto se incluirán aquellas medidas reflejadas en la Ley que afectan a la estructura organizativa de las Entidades Locales, las cuales necesitan ser adaptadas a la hora de prestar servicios de Administración Electrónica a la ciudadanía (Art. 22.3).
- Adaptación normativa: las Entidades Locales deberán instrumentar actuaciones de carácter reglamentario, normando las condiciones, las garantías y los efectos jurídicos de los Servicios Públicos Electrónicos en las relaciones con los ciudadanos, dando de esta manera plena seguridad jurídica a estos Servicios (Art. 10.3)

A continuación, se detallan cada uno de los apartados indicados:

Adaptación De Los Canales De Comunicación

La LAECSP en su *Artículo 8.1* establece que “*las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos,...*”, por lo tanto, se puede inferir que será obligatorio que cada Entidad establezca más de un canal de relación con los ciudadanos para la prestación de servicios electrónicos, dejando libertad al Ayuntamiento para decidir cuáles deben ser dichos canales adicionales además del canal de Internet, puesto que el canal telemático, establecido como Sede Electrónica, está definido en el *Artículo 10* de la Ley como canal obligatorio.

Adaptación De Procedimientos Administrativos

Con la Administración electrónica, las Entidades Locales podrán ofrecer servicios administrativos a los ciudadanos por medios electrónicos. Estos servicios se traducen en procedimientos administrativos que normalmente no están adaptados a la Administración Electrónica. Para la correcta gestión electrónica de los mismos es necesaria una herramienta de gestión de expedientes que los automatice y permita a los ciudadanos la iniciación, consulta y resolución telemática de los mismos.

Es necesario, por lo tanto, que los Ayuntamientos realicen una simplificación y racionalización de los procedimientos no sólo para su posterior integración en la Administración Electrónica, sino también para una gestión más eficiente de la

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

actuación administrativa y mejora de la calidad de los Servicios Públicos ofrecidos a los ciudadanos (Artículo 33.1).

Igualmente, para que el ciudadano pueda conocer y acceder a los servicios administrativos que la Entidad Local está ofreciendo a través de Internet, es necesario que exista un inventario actualizado de estos procedimientos públicos, y que el ciudadano pueda consultar para conocer toda la información relativa al procedimiento de su interés así como su fórmula telemática de tramitación (Disposición Final Tercera).

Otro de los derechos del ciudadano reconocido en la LAECSP, es el de no aportar datos que ya obren en poder de las Administraciones. Esto implica que cada Administración Pública deberá poner a disposición del resto de Administraciones los datos en formato electrónico que disponga de los ciudadanos. Para que el resto de Administraciones conozcan los datos y documentos que dispone esa Administración, ésta debería contar con un inventario de estos datos, junto con su forma de acceso a los mismos desde otras Administraciones.

Adaptación de la tecnología del front-office

Para ofrecer los servicios electrónicos a los ciudadanos a los que obliga la LAECSP, es necesaria una actualización de la Tecnología de Front-Office de las Entidades Locales. Por Tecnología de Front-Office se entiende aquellos sistemas informáticos que dan soporte a servicios electrónicos de cara al ciudadano (sistemas informáticos para el soporte de páginas Web, registro telemático, consulta de expedientes, pago telemático, etc.).

Las medidas obligatorias que un Ayuntamiento debe realizar para cumplir la LAECSP en relación con este apartado son las siguientes: portal Web, poner a disposición de los ciudadanos formularios electrónicos de solicitud, identificación digital del ciudadano, identificación digital de la Sede Electrónica, registro electrónico, pago electrónico, comunicaciones electrónicas, notificaciones electrónicas y un sistema electrónico de consulta de estado de la tramitación de un procedimiento. La publicación electrónica del tablón de anuncios y edictos es una medida opcional.

El portal Web de una Entidad Local es el soporte tecnológico para los servicios de la Sede Electrónica y la información administrativa de la Entidad. A través del portal Web se accederá a la oficina virtual de la Entidad Pública, su Sede Electrónica, definida en el Artículo 10 de la LAECSP como "*una dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.*"



El *Capítulo II* del *Título II*, de la identificación y autenticación, está dedicado a describir los sistemas de firma electrónica, que sean conformes a lo establecido en la Ley 59/2003 de Firma Electrónica, que las Administraciones Públicas deben admitir en sus relaciones por medios electrónicos, tanto con ciudadanos como con otras Administraciones Públicas, para garantizar la identificación de los participantes en las comunicaciones, y, en su caso, la autenticidad e integridad de los documentos electrónicos intercambiados.

Los ciudadanos para su identificación y la autenticación de sus actuaciones podrán utilizar en las comunicaciones con las Administraciones Públicas, según la LAECSP artículos 13.2, 14, 15 y 16 y lo que determine cada Administración, los siguientes sistemas de firma electrónica:

- Los incorporados al Documento Nacional de Identidad Electrónico. En todo caso, y con carácter universal las personas físicas podrán utilizar este sistema de firma electrónica en su relación por medios electrónicos con cualquier Administración Pública. Es decir, el empleo del DNI electrónico se regula como un derecho de uso del ciudadano, *artículo 6.2.g*), y por lo tanto como una obligación de los Ayuntamientos, y del resto de Administraciones, de admitirlo (*artículo 13.2.a*) y *art. 14*).
- Sistemas de firma electrónica avanzada. Los ciudadanos podrán utilizar este tipo de sistemas de firma electrónica para identificarse y autenticar sus documentos y actuaciones, siempre que haya sido admitido previamente por la Administración correspondiente (*Artículo 13.2.b*) y *art. 15*). Debido a esto, la ley en su *artículo 15.2*, obliga a las Administraciones a hacer pública, por medios electrónicos, la relación de sistemas de firma electrónica avanzada admitidos. Dicha relación deberá incluir, al menos, información sobre los elementos de identificación utilizados, las características de los certificados electrónicos admitidos, los prestadores que los expiden y las especificaciones de la firma electrónica que puede realizarse con dichos certificados.
- Otros sistemas de firma electrónica: utilización de claves concertadas en un registro previo como usuario, aportación de información conocida por ambas partes u otros sistemas no criptográficos.
- Identificación y autenticación de los ciudadanos por funcionario público: En los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante alguno de los medios descritos anteriormente y que éste no disponga de ellos, tal identificación o autenticación podrá ser realizada por funcionarios públicos mediante el sistema de firma electrónica del que estén dotados. Por este motivo, el Ayuntamiento deberá constituir y tener actualizado un registro de los funcionarios habilitados para dicha actuación (*Artículo 22*).
- Representación de los ciudadanos: Las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para actuar como representantes de los interesados en determinadas relaciones electrónicas (*Artículo 23*).

Por otro lado, las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan en el ejercicio de su competencia según sus distintas áreas de actuación (*artículo 13.3*):

- Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras (*artículo 17*).
- Sistemas de firma electrónica para la actuación administrativa automatizada (*artículo 18*).
- Firma electrónica del personal al servicio de las Administraciones Públicas (*artículo 19*), para poder realizar la identificación y autenticación de los ciudadanos a la cual se hizo mención anteriormente.
- Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes (*artículo 20*).

El registro electrónico

El Registro Electrónico es el elemento esencial para interactuar electrónicamente con la Administración Pública, de forma que se puedan iniciar trámites administrativos, permitiendo la entrada de solicitudes, escritos y comunicaciones, con las mismas implicaciones que el Registro convencional. Se trata, por tanto, de un servicio ubicado en el Front-Office de la Sede Electrónica de la Entidad Local, que hace las funciones de registro de entrada y salida de documentos, incluyendo la emisión de certificaciones, copias auténticas, etc.

La creación de un Registro Electrónico es considerada como una actuación obligatoria, puesto que además de que el Artículo 6 de la Ley establece, como uno de los derechos, la posibilidad de relacionarse con las Administraciones por medios electrónicos, el Artículo 24 establece la creación de registros electrónicos, obligando a que cada Administración Pública disponga de, al menos, un Sistema de Registro Electrónico.

El pago electrónico

El Pago Electrónico no se encuentra explícitamente regulado en ningún artículo de la Ley, aunque sí lo reconoce en el Artículo 6.1 como un derecho del ciudadano en su relación con las Administraciones Públicas, y, por lo tanto, se considera que es una actuación de carácter obligatorio para las Entidades Locales. En las Administraciones Públicas existen numerosos procedimientos administrativos que requieren, tanto para su inicio como para su tramitación, el pago de impuestos, tributos y tasas. La utilización de un Sistema de Pago Telemático permitirá que los contribuyentes no tengan que desplazarse para



realizar el pago de tributos, precios públicos y otros ingresos de derecho público, pudiendo realizar estos pagos fuera del horario normal de atención al público.

Para la publicación electrónica del tablón de anuncios o edictos la Ley en su artículo 12 permite su sustitución o complementariedad en la sede electrónica del organismo correspondiente. El objetivo de la publicación electrónica es facilitar el acceso y mejorar la consulta de información a los ciudadanos y empresas.

Según el artículo 35 de la LAECSP se deberán incluir en las sedes electrónicas de los Ayuntamientos modelos o sistemas electrónicos de solicitud para posibilitar a los ciudadanos la iniciación de un procedimiento administrativo por medios electrónicos. Los interesados podrán aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada (*artículo 35.2*). Las Administraciones Públicas para facilitar y promover el uso de los sistemas o modelos electrónicos de solicitud de iniciación de un procedimiento podrán incluir comprobaciones automáticas de la información aportada respecto a los datos que ya tengan almacenados dicha Administración o cualquier otra, e incluso, ofrecer el formulario cumplimentado con los datos que se posean, a fin, de que el ciudadano tan solo tenga que verificar los datos que se le aporten y, en su caso, completar aquellos datos que faltaran y modificar aquellos que no fueran correctos (*artículo 35.3*).

En cuanto a la consulta de expedientes, la LAECSP en el *artículo 37* reconoce el derecho de acceso a los interesados a la información sobre el estado de tramitación del procedimiento mediante un servicio electrónico. En los procedimientos gestionados en su totalidad electrónicamente, en el *apartado 1º* del *artículo 37* se establece la obligación para los ayuntamientos de poner a disposición de los ciudadanos un servicio electrónico de acceso restringido donde estos puedan consultar, previa identificación, al menos el estado de tramitación del procedimiento. En este caso, la información sobre el estado de tramitación debe comprender la relación de los actos de trámite realizados, indicando su contenido y la fecha en la que fueron dictados. En los procedimientos no gestionados electrónicamente, según el *apartado 2º* del *artículo 37*, se deberá habilitar un servicio electrónico de información del estado de tramitación que indique, al menos, la fase en la que se encuentra el procedimiento y el órgano o unidad responsable.

Las *notificaciones* son un tipo de comunicaciones cuyo emisor (Administración Pública) pretenda dar a conocer una decisión administrativa al receptor (ciudadano). Las *notificaciones electrónicas* deberán estar soportadas por un sistema de notificación que permita acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de la notificación, así como la de acceso a su contenido. La LAECSP en su *artículo 28* regula las notificaciones por medios electrónicos y establece:

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- La libertad de elección del mecanismo de notificación por parte del ciudadano, así como la posibilidad de optar por uno diferente en cualquier momento (*apartados 1º y 2º del artículo 28*).
- La necesidad de que los ciudadanos manifiesten su preferencia o consientan el empleo de medios electrónicos para la recepción de sus notificaciones que les tengan que realizar. (*Artículo 28.2*).
- Las condiciones de validez de las notificaciones electrónicas, que en el *artículo 28.5* las equipara a las notificaciones por comparecencia al acceso electrónico al contenido de las actuaciones administrativas por parte de los interesados.
- Mecanismos de control de la fecha y hora en la que se produzcan la puesta a disposición y el acceso al contenido de las notificaciones por parte de los interesados. (*artículo 28, apartado 2*).

En la actualidad, y como respuesta a la necesidad generada a las Administraciones Públicas por la ley 11/2007, en relación a las notificaciones electrónicas, existen algunas entidades que ofrecen servicios de notificaciones electrónicas fehacientes. Este es el caso de la Plataforma de Notificaciones Electrónicas de la Secretaría de Estado para la Función Pública en colaboración con Correos, SNTS (Sistema de Notificaciones Telemáticas Seguras).

Entre los organismos públicos que han habilitado procedimientos para el envío de notificaciones administrativas por vía telemática con la plataforma SNTS, se encuentran: AEAT, AEPD, Ministerios como el de Justicia, Dirección General de Tráfico, la Seguridad social, muchos ayuntamientos, etc.

Las comunicaciones electrónicas vienen reguladas en el artículo 27 de la LAECSP. Estas comunicaciones serán válidas cuando cumplan las siguientes condiciones:

- Existencia de constancia de la transmisión y recepción de la comunicación electrónica, de las fechas en las que se realizaron, así como del contenido íntegro de las mismas (*Artículo 27.3*).
- Identificación fidedigna del remitente y destinatario de la comunicación (*Artículo 27.3*).
- Los requisitos de seguridad e integridad de las comunicaciones se deberán establecer en cada caso atendiendo al carácter de los datos objeto de aquellas, de acuerdo a criterios de proporcionalidad y conforme a lo establecido en la legislación vigente en materia de protección de datos de carácter personal (*Artículo 27.5*).

Se distinguen los siguientes tipos de comunicaciones:



- Comunicaciones entre Administraciones Públicas: Cuando en una comunicación participen únicamente Administraciones Públicas, se utilizarán preferentemente medios electrónicos, es decir, la ley no impone obligación de que este tipo de comunicación se realice electrónicamente de manera exclusiva. En cuanto a las condiciones que regirán, éstas se determinarán entre las Administraciones Públicas participantes (*Artículo 27.7*).
- Comunicaciones de las Administraciones Públicas hacia los ciudadanos: Las Administraciones Públicas están obligadas a utilizar medios electrónicos en sus comunicaciones con los ciudadanos, siempre que éstos lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán emitirse y recabarse por medios electrónicos (*Artículo 27.2*).
- Comunicaciones de los ciudadanos hacia las Administraciones Públicas: Los ciudadanos podrán elegir en todo momento la manera de comunicarse con las distintas Administraciones, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de Ley se establezca o infiera la utilización de un medio no electrónico. Los ciudadanos podrán, en cualquier momento, optar por un medio distinto al inicialmente elegido (*Artículo 27.1*). Las Administraciones Públicas podrán establecer reglamentariamente la obligatoriedad de que ciertos colectivos, en concreto las 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 medios tecnológicos precisos, se comuniquen con estas Administraciones empleando únicamente medios electrónicos (*Artículo 27.6*). Aquellos medios electrónicos que los ciudadanos puedan utilizar en cada supuesto para comunicarse con las Administraciones Públicas, se deberán publicar en el correspondiente Diario Oficial y en la propia sede electrónica (*Artículo 27.4*)

Adaptación de la tecnología del back-office

En este apartado se procede a valorar aquellos aspectos de la Ley 11/2007 que hacen referencia a la Tecnología Back-Office. Por Back-Office se entienden todos aquellos sistemas internos que permitan la gestión informatizada de la actuación administrativa (sistemas de gestión de expedientes, contabilidad, bases de datos de padrón, etc.).

Según el artículo 9 de la LAECSP, transmisiones de datos entre Administraciones Públicas, cada Administración deberá facilitar los datos del ciudadano disponibles en soporte electrónico al resto de Administraciones. En el apartado 1º de este artículo se indica que para un eficaz ejercicio del derecho de los ciudadanos a no aportar los datos y documentos que obren en poder de las Administraciones Públicas, artículo 6.2.b), cada Administración está obligada a facilitar el acceso al resto de Administraciones a los datos

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

relativos a los interesados que obren en su poder y se encuentren en soporte electrónico. Según se recoge en este apartado del artículo 9, se tienen que especificar las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos, proporcionando las máximas garantías de seguridad, integridad y disponibilidad de los mismos, de conformidad con la Ley Orgánica de Protección de Datos de Carácter personal y su normativa de desarrollo.

En el artículo 31.1 de la Ley 11/2007, archivo electrónico de documentos, se dice que se podrán almacenar por medios electrónicos todos los documentos utilizados en las actuaciones administrativas. En este sentido, la utilización de un archivo electrónico es opcional para los Ayuntamientos, aunque hay que tener también en cuenta que uno de los derechos que la LAECSP reconoce a los ciudadanos, en el artículo 6.2.f), es el de la conservación en formato electrónico por parte de las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente, por lo que, en cierta medida, se puede interpretar que es obligatorio que los ayuntamientos posean un archivo electrónico. Se debe asegurar la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones (apartado 2º, artículo 31). Por último, en el apartado 3º de este artículo 31, se enumeran las medidas de seguridad y de conservación con las que deberán contar los medios o soportes en los que se almacenarán los documentos electrónicos, para garantizar la integridad, autenticidad, confidencialidad, calidad y protección de los mismos. Se deberá asegurar, en particular, la identificación de los usuarios, el control de accesos, y el cumplimiento de las garantías previstas en la legislación de protección de datos.

El *sistema de gestión de expedientes* permitirá dar a conocer a los ciudadanos que lo demanden, el camino administrativo que ha seguido su procedimiento y la situación en la que se encuentra en un momento determinado. En el *artículo 32* de la presente Ley se define el expediente electrónico como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

Adaptación organizativa.

Como es obvio, la implantación de la Administración Electrónica supone un importante cambio organizativo y cultural dentro de las Administraciones Públicas, y de los Ayuntamientos en particular. La LAECSP marca algunas obligaciones que deben asumir las Administraciones para afrontar este cambio organizativo, aunque esta adaptación es inherente al nuevo modelo de gestión y al paradigma de calidad del servicio.

En primer lugar es conveniente realizar una nueva definición de la organización. El objetivo es estructurar la Administración Pública de forma que se garanticen a todos los ciudadanos todos los derechos que la ley 11/2007 les otorga y que estos derechos se presten mediante servicios electrónicos de calidad. Además, en relación con lo dicho, en el *apartado 5 del artículo 3* de la



LAECSP se recoge, como una de las finalidades que persigue esta ley, la contribución a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando así la eficacia y eficiencia de las mismas.

Entre las medidas obligatorias que debe realizar para cumplir la LAECSP en esta área de actuación se encuentra la institución de un Registro de Funcionarios públicos habilitados para que, dichos funcionarios puedan realizar válidamente mediante el uso del sistema de firma electrónica del que hayan sido dotados la identificación y autenticación de los ciudadanos que no dispongan de alguno de los instrumentos previstos en el *artículo 13* de esta ley, para la realización de cualquier operación por medios electrónicos. Para que dicha actuación pueda llevarse a cabo por parte de un funcionario público, el ciudadano deberá identificarse y prestar su consentimiento expreso, del que deberá quedar constancia para los casos de discrepancia o litigio. (*Artículo 22*, Identificación y autenticación de los ciudadanos por funcionario público).

Adaptación normativa.

A continuación se exponen aquellos aspectos de la LAECSP que hacen referencia a la normativa, y que, por su carácter regulador, son el fundamento de todas las actuaciones y desarrollos de la misma, encaminados a establecer las pautas en la relación electrónica de las Entidades Locales y el ciudadano.

El proceso de desarrollo de la Administración Electrónica supone la implantación de diferentes sistemas tecnológicos (Registro electrónico, trámites online, página Web, etc.), que deben estar normados jurídicamente para asegurar las mismas garantías legales que la tramitación tradicional.

Según la LAECSP es necesario que se reglamenten diferentes aspectos específicos incorporados en la misma, unos vinculados al régimen jurídico asociado a la tramitación electrónica y otros asociados a la estructuración de las competencias y los procedimientos relativos a los nuevos servicios puestos a disposición de los usuarios.

3.10.3 LOPD

La Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD) tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente el derecho de las personas a su honor, intimidad y privacidad personal y familiar, que es uno de los derechos fundamentales que recoge la Constitución española.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

Los conjuntos de datos protegidos abarcan cualquier tipo de fichero (informático o en papel), solamente con unas pocas excepciones como el caso de ficheros creados por personas físicas para su uso estrictamente personal o ficheros para la investigación del terrorismo y de formas graves de delincuencia organizada. Además se tipifican algunos casos con un régimen jurídico propio como lo es el caso de ficheros regulados por la legislación del régimen electoral o los propios del Registro Civil.

La ley regula derechos como el derecho de información en la recogida de los datos, la necesidad de consentimiento para su tratamiento o el derecho a su acceso, rectificación y cancelación en cualquier momento. Se define la categoría de datos especialmente protegidos (datos sobre ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual) que gozan de un nivel de protección especialmente reforzado.

Por otra parte se regula cesión de los datos a terceros, tanto a nivel nacional como internacional, donde la regla general es que la cesión tiene que ser consentida por el sujeto del tratamiento de datos, y que la cesión internacional a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley queda prohibida. Sobre esta base se definen excepciones concretas como que la cesión en cuestión esté regulada por una ley, o en el ámbito internacional que el país en cuestión pertenezca a la UE o haya un tratado específico con él a ese respecto.

El Título IV se dedica enteramente a disposiciones sectoriales para el sector público y privado. Se tratan cuestiones como que la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario oficial correspondiente.

En los dos últimos títulos se trata por una parte la Agencia Española de Protección de Datos y por otra parte las infracciones y sanciones, pudiendo llegar estas últimas hasta 600.000€ en el caso de incumplimientos graves.



La Agencia se establece como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se definen sus funciones entre las cuales se pueden desatacar la de Registro de General de Protección de Datos en el cual ha de inscribirse todo fichero que cae dentro del ámbito de esta ley, su función consultora, y su potestad de inspección y potestad sancionadora.

3.11 Conexión entre LAECSP y LOPD

Llegados a este punto se plantea la pregunta sobre cómo se podría hacer compatible el acceso electrónico de los ciudadanos a los servicios públicos, con el respeto y defensa del derecho fundamental a la protección de datos.

La protección de datos es un derecho fundamental y constituye uno de los pilares más importantes para la defensa de los derechos fundamentales de los ciudadanos en la sociedad de la información.

La Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios Públicos, se plantea como el reto más complejo y fascinante para las administraciones en los próximos años.

Garantizar el acceso y la tramitación electrónica de los procedimientos, certificar la Sede Electrónica e identificar y notificar a los administrados que accedan a ella, obtener remotamente cualquier documento, son acciones directamente relacionadas con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD).

Por otro lado, garantizar la seguridad, facilitar la consulta y el derecho de acceso, asegurar la adecuación y veracidad de los registros electrónicos o comunicar datos sólo en los casos previstos por la ley o con el consentimiento del titular son objetivos de la protección de datos absolutamente necesarios para dar cauce a lo dispuesto en la Ley 11/2007.

Existen en general distintos ámbitos jurídicos tratados en el RDLOPD, los cuales conviene tener en cuenta a la hora de poner en marcha los requisitos de la Ley 11/2007:

- La carga de la prueba de haber informado debidamente con todos los requisitos y haber obtenido el debido consentimiento de un usuario para tratar sus datos, recae en el responsable del fichero.
- Se incorporan nuevos requerimientos para llevar a cabo el deber de información correctamente, especificaciones para la obtención del consentimiento, cómo obtener de forma válida un consentimiento tácito.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Se establece la obligación de ofrecer a un cliente en un proceso de contratación la posibilidad de negarse a que se utilicen sus datos para finalidades que no sean estrictamente el cumplimiento del objeto contractual.
- Se determinan las obligaciones del encargado del tratamiento para poder subcontratar todo o parte de sus servicios con las debidas garantías para el responsable del fichero, obligaciones de conservación de datos, contenido de su documento de seguridad, remisión de las peticiones de acceso, rectificación, cancelación y oposición al responsable del fichero, etc.
- Se exponen diversas formas de atender los derechos de acceso, rectificación y cancelación, delimitación de plazos legales para contestar, necesidades de concienciación y difusión del procedimiento en la compañía, la regulación del contenido del derecho de oposición, etc.

En general, el ámbito y contenido del RDLOPD es muy amplio y obliga a todas las entidades públicas y privadas, a revisar sus procedimientos, políticas, cláusulas, documentos de seguridad y medidas de seguridad para lograr la adaptación a la norma.

Entre los aspectos fundamentales recogidos en el articulado de la Ley 11/2007 en relación con la protección de datos y su tratamiento están:

- La garantía de que los datos obtenidos por medio de las comunicaciones electrónicas sean utilizados para el fin preciso para el que fueron solicitados y/o remitidos.
- La obligación de cada Administración de proporcionar, a otras, aquellos datos sobre el ciudadano que obren en su poder, siempre que el interesado haya dado su aprobación previa.

Para la puesta en práctica de estos y otros contenidos de la Ley 11/2007, habrá que tener en cuenta las especificaciones recogidas en el RDLOPD. Pero un aspecto que resulta de vital importancia es que, en el diseño de los procesos administrativos que se definan para cumplir lo establecido en la Ley 11/2007, habrá que tener en cuenta aquellos requisitos exigidos con carácter general en el RDLOPD, alguno de los cuales hemos mencionado.

Existen distintos documentos de referencia, útiles para el conjunto de Gobiernos Locales, que se mencionan a continuación.

Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios Web institucionales y en otros medios electrónicos y telemáticos.

Se trata de un documento cuyo objetivo es regular la publicación de datos de carácter personal que se realice en esos medios, por parte de las



Administraciones Públicas y los órganos administrativos, para adecuarla al derecho fundamental a la protección de datos de carácter personal.

La recomendación pretende descender al detalle de los problemas reales derivados, en cada caso, de la utilización de medios de publicidad electrónica por parte de los agentes administrativos a los que la misma se dirige.

Se abordan, entre otros, temas como la publicación de datos relativos a procedimientos de concurrencia competitiva: procesos selectivos de acceso a la función pública, datos sobre la provisión de puestos de trabajo, publicación de subvenciones, datos sobre obtención de plazas en colegios, etc.

También se contemplan procedimientos de concurrencia no competitiva, como la publicación de resultados de procesos de evaluación de la actividad docente, publicación de ayudas a empleados públicos, etc.

Otras materias tratadas son los listados de colegiados, la publicación de directorios y de censos electorales.

Se ofrece respuesta a otros supuestos de publicidad de la actividad administrativa, tales como los derivados de la publicación de sesiones y acuerdos del Pleno de las Corporaciones Locales y de otros organismos de la Administración Local, la publicación de retribuciones de los empleados públicos, publicación de ponencias y presentaciones, la publicidad del Registro de Intereses de las Corporaciones Locales, y de la publicación de notificaciones y resoluciones administrativas.

En cuanto a la publicación de actas y acuerdos del resto de órganos de la Administración Local en sitios Web institucionales, la recomendación es no publicar datos personales de los ciudadanos que afecten a su derecho al honor, a la intimidad personal o familiar y a la propia imagen.

Recomendación 3/2008, de 30 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre tratamiento de datos de carácter personal en servicios de administración electrónica.

Son recomendaciones que con carácter general intentan hacer compatible el acceso de los ciudadanos a los servicios públicos con el respeto y defensa del derecho fundamental a la protección de datos.

Se intentan regular cuestiones tales como el concepto de encargado del tratamiento de los datos y responsable de fichero, el derecho de información en la recogida de los datos, el consentimiento del interesado, las medidas de seguridad a implantar, el ejercicio de los derechos de rectificación y cancelación, y demás cuestiones establecidas en el RDLOPD.

Contempla además los llamados CAPI (Centros de Acceso Público a Internet) al amparo de lo dispuesto en la Ley 11/2007, que reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios

electrónicos, previendo unos puntos de acceso público, cubriendo así este derecho para el conjunto de la población, eliminando las barreras que limitan el acceso.

Se observan también otras cuestiones ligadas a la Ley 11/2007, como la suscripción a servicios de noticias y servicios de alerta SMS, a las bolsas de empleo, los *chats* institucionales, y los foros de opinión.

3.12 Reglamento de desarrollo de la Ley Orgánica 15/1999

El Real Decreto 1720/2007, que sucede al Real Decreto 994/1999, de medidas de seguridad de los ficheros automatizados que contengan datos personales, supone una revisión enorme que refleja el peso que esta materia ha ido adquiriendo con el tiempo. Si el anterior reglamento constaba de 29 artículos, el actual consta de 158. Por otra parte, hay que destacar también el importante hecho de que a diferencia del anterior, regula también medidas aplicables a los ficheros en papel.

La parte del actual reglamento más destacable es la dedicada a las medidas de seguridad aplicables a ficheros y tratamientos de ficheros automatizados. Se estructura en medidas de seguridad de nivel básico, medio y alto. Esta parte abarca desde el artículo 80 al artículo 104.

En primer lugar el responsable del fichero o tratamiento debe elaborar el documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

Las medidas concretas que el reglamento obliga a cumplir dependen fundamentalmente de la naturaleza de los datos. En ese sentido, las medidas se estructuran a grandes rasgos de la siguiente forma:

- Medidas de *nivel básico*: se aplican a cualquier fichero o tratamiento de datos de carácter personal.
- Medidas de *nivel medio*: estas medidas se aplican cuando los datos personales abarcan información sobre infracciones administrativas o penales, servicios de información sobre solvencia patrimonial y crédito, datos de gestión tributaria, servicios financieros, de la Seguridad Social y mutuas, y datos que permiten la elaboración de un perfil de la personalidad del sujeto.
- Medidas de *nivel alto*: se aplican fundamentalmente a los datos especialmente protegidos (ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual), a los datos con fines policiales recogidos sin consentimiento de las personas afectadas y los datos sobre violencia de género.



Según el nivel de seguridad aplicable a los datos, el reglamento define medidas de seguridad concretas que van desde cosas básicas como un registro de incidencias y asegurar la correcta identificación y autenticación de los usuarios que accedan a los datos personales, medidas de nivel medio como auditorías y control de acceso físico hasta medidas de nivel alto como el cifrado de las comunicaciones o un registro de acceso detallado que guarda cómo mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si fue autorizado o denegado.

3.13 Ley 56/2007

La Ley 56/2007, de 28 de Diciembre, de Medidas de Impulso de la Sociedad de la Información, se enmarca en el conjunto de medidas que constituyen el Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas, Plan Avanza, aprobado por el Gobierno en noviembre de 2005.

Los contenidos se centran principalmente en innovaciones normativas en materia de facturación electrónica y de refuerzo de los derechos de los usuarios y, por otra parte, las modificaciones necesarias en el ordenamiento jurídico para promover el impulso de la sociedad de la información.

En este sentido, se introducen una serie de modificaciones tanto de la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico, como de la Ley 59/2003, de firma electrónica, que constituyen dos piezas angulares del marco jurídico en el que se desenvuelve el desarrollo de la sociedad de la información.

En cuanto a la facturación electrónica se prevén diferentes medidas para su impulso como un plan para la generalización del uso de la factura electrónica y la elaboración de un formato de factura electrónica, que se ha traducido en el formato español Facturae, y la creación de una Web propia sobre la factura electrónica.

En cuanto a las medidas de refuerzo de derechos de usuarios y el impulso de la sociedad de la información se establecen medidas como la obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica (telecomunicaciones, banca, seguros, suministro eléctrico, gas, etc.), medidas para la extensión de servicios de banda ancha, un plan de mejora de los niveles de seguridad y confianza en Internet, mejoras en la planificación de infraestructuras para las canalizaciones de redes de comunicaciones electrónicas, difusión de aplicaciones de fuentes abiertas a través del CENATIC a la sociedad y muchas otras medidas concretas.

Esta revisión del ordenamiento jurídico se completa con otras modificaciones menores de la Ley 32/2003, General de Telecomunicaciones, de la Ley

11/1998, General de Telecomunicaciones y de la Ley 7/1996, de ordenación del comercio minorista.

3.14 Escenarios para el cumplimiento de la Ley.

En este apartado vamos a abordar los posibles estados en los que se pueden encontrar los Ayuntamientos en relación al objetivo del cumplimiento de la ley. Para poder explicarlo se ha sesgado el aspecto de posibles Administraciones Públicas.

Hay que tener en cuenta, por un lado, si un Ayuntamiento posee o no un Sistema de Gestión Integral (SGI) o Back-Office para su tramitación administrativa, y por otro lado, la adaptación de la tecnología de Front-Office y Back-Office o SGI, respectivamente, los ayuntamientos podrán clasificarse según el estadio en el que se encuentren de entre los siguientes:

- Ayuntamientos que no tienen desarrollados ninguno de los tres aspectos mencionados.
- Ayuntamientos que únicamente poseen un Sistema de Gestión Integral o Back-Office.
- Ayuntamientos que tienen un SGI
- Front-Office. Ayuntamientos que poseen un SGI, además de haber realizado la adaptación de las tecnologías
- de Front-Office y Back-Office o SGI para poder realizar la tramitación electrónica de cualquier expediente administrativo.

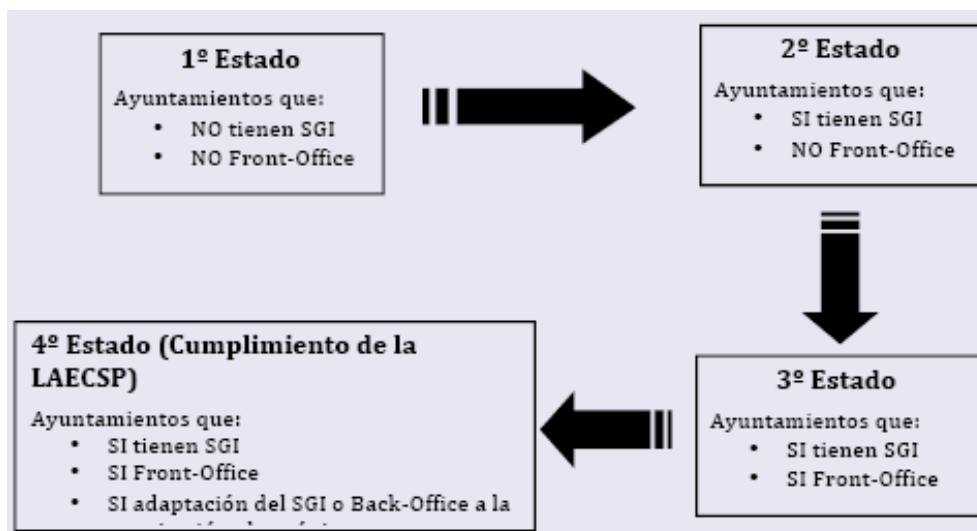


Imagen 3-1 Estados para cumplir con LAECSP

El objetivo final de todo ayuntamiento para adecuarse a la Ley 11/2007 será el conseguir llegar al 4º estado indicado en la clasificación anterior, lo que no significa que los ayuntamientos en 2º o 3º estado puedan establecer



mecanismos intermedios telemáticos de comunicación e interacción con sus ciudadanos que les permitan un cumplimiento parcial de la ley. Eso sí, esto tiene que significar un momento previo hasta llegar al 4º estado y debe quedar referido así en su planificación estratégica y sus presupuestos.

En cualquiera de los casos es necesario el establecimiento de una Sede Electrónica a través de la cual, los ciudadanos puedan acceder a toda la información y a los servicios disponibles. Contendrá la relación de los servicios a disposición de los ciudadanos y el acceso a los mismos, respetando los principios de accesibilidad y usabilidad y basándose en sistemas que permitan las comunicaciones seguras.

3.15 Ordenanza reguladora de la eAdministración

La incorporación a la administración electrónica requiere que cada Administración determine las condiciones e instrumentos de creación de las sedes electrónicas. También es necesario regular los distintos elementos que intervienen en el acceso electrónico de los ciudadanos y en las comunicaciones electrónicas dirigidas a estos: registros, notificaciones y tablones de anuncios electrónicos, habilitación de funcionarios, representación de los interesados, etc.

El marco más adecuado es la aprobación de un instrumento normativo u Ordenanza que además de dar cabida a las necesidades manifestadas, sirva para divulgar entre los ciudadanos los derechos y obligaciones que les otorga la Ley 11/2007 y promueva la utilización de los medios electrónicos puestos a su disposición.

En este capítulo se propone una estructura estándar de ordenanza con el fin de facilitar su elaboración.

Esta estructura estándar se ha dividido en capítulos y los aspectos cuyo tratamiento se propone son los mínimos que deben tenerse en cuenta para asegurar la regulación de los aspectos básicos de la Ley 11/2007.

Estructura tipo:

Descripción y redacción de motivos

CAPÍTULO PRIMERO.

Disposiciones generales.

Artículo 1. Objeto.

Artículo 2. Definiciones.

Artículo 3. Ámbito de aplicación.

CAPÍTULO SEGUNDO.

Principios generales.

Artículo 4. Principios organizativos de la administración electrónica.

Artículo 5. Difusión de la información.

Artículo 6. Procedimiento administrativo electrónico.

Artículo 7. Principios de cooperación con otras Administraciones Públicas.

CAPÍTULO TERCERO.

Derechos y deberes de los ciudadanos en la relación con la administración electrónica.

Artículo 8. Derechos de la Ciudadanía.

Artículo 9. Deberes de la Ciudadanía.

Artículo 10. Cumplimiento de derechos y deberes.

CAPÍTULO CUARTO.

La Sede Electrónica.

Artículo 11. Características de la Sede Electrónica.

Artículo 12. Identificación de interesados y autenticación de su actuación.

Artículo 13. Identificación y autenticación de los Órganos administrativos.

Artículo 14. Identificación y autenticación de las sedes.

CAPÍTULO QUINTO.

La difusión de la información administrativa por medios electrónicos.

Artículo 15. Acceso a la información.

Artículo 16. Información sobre la organización y servicios de interés general.

Artículo 17. Información administrativa

Artículo 18. Tablón de Edictos Electrónico.

Artículo 19. Publicación oficial.

CAPÍTULO SEXTO.

Oficina Virtual, Registro, comunicaciones y notificaciones electrónicas.

Artículo 20. Oficina Virtual.

Artículo 21. Registro Electrónico de entrada y salida de documentos.

Artículo 22. Escritos y documentos susceptibles de registro de entrada.

Artículo 23. Cómputo de plazos en Registro Electrónico.

Artículo 24. Régimen de funcionamiento del Registro Electrónico.



Artículo 25. Autenticidad, integridad, confiabilidad, disponibilidad y conservación del contenido de los asientos electrónicos.

Artículo 26. Las comunicaciones electrónicas.

Artículo 27. Las notificaciones electrónicas.

CAPÍTULO SÉPTIMO.

Los documentos y archivos electrónicos.

Artículo 28. Documento Administrativo electrónico.

Artículo 29. Copias Electrónicas

Artículo 30. Compulsa electrónica de documentos en soporte papel.

Artículo 31. Archivo Electrónico.

Artículo 32. Expediente electrónico.

CAPÍTULO OCTAVO.

Gestión electrónica de los procedimientos. Disposiciones comunes.

Artículo 33. Trámites y procedimientos a los que es aplicable la tramitación electrónica.

Artículo 34. Mecanismo de incorporación de trámites y procedimientos a la tramitación por vía electrónica.

CAPÍTULO NOVENO.

Utilización de medios electrónicos en la tramitación del procedimiento.

Artículo 35. Iniciación del procedimiento administrativo.

Artículo 36. Representación.

Artículo 37. Tramitación del procedimiento administrativo.

Artículo 38. Continuación del procedimiento administrativo electrónico por medios tradicionales.

Artículo 39. Acceso de los interesados a la información sobre el estado de La Tramitación del procedimiento.

Artículo 40. Terminación de los procedimientos por medios electrónicos.

Artículo 41. Actuación administrativa automatizada.

CAPÍTULO DÉCIMO.

Servicio Telemático de Pago.

Artículo 42. Servicio Telemático de Pagos.

DISPOSICIONES TRANSITORIAS.

DISPOSICIONES FINALES.

ANEXO I. Trámites y gestiones municipales disponibles en la sede electrónica

Opcional, ya que quedará contemplado en la definición oficial de la Sede Electrónica de cada Ayuntamiento.

En resumen:

- En el Capítulo Primero, se presentan el objetivo y el ámbito de aplicación
- En el Capítulo Segundo, los principios generales electrónicos definidores de este nuevo concepto de Atención a la Ciudadanía
- En el Capítulo Tercero, se establecen los derechos y deberes de los ciudadanos
- En el Capítulo Cuarto, las características de la Sede Electrónica
- En el Capítulo Quinto, la difusión de la información por medios electrónicos
- En el Capítulo Sexto, la oficina virtual, los registros y notificaciones electrónica
- En el Capítulo Séptimo, los documentos y archivos electrónicos
- En el Capítulo Octavo, la gestión electrónica de los procedimientos
- En el Capítulo Noveno, la utilización de medios electrónicos y la tramitación electrónica del procedimiento
- Y finalmente en el Capítulo Décimo, el servicio telemático de pago

3.16 Ley 17/2009, 23 de noviembre

Para dar cumplimiento a la directiva europea de servicios, se tramitaron dos proyectos de Ley conocidos popularmente como Ley paraguas (Ley 17/2009 de 23 de noviembre) y Ley ómnibus (Ley 25/2009, de 22 de diciembre). Estos proyectos inciden en la administración electrónica en cuanto dictan las normas de funcionamiento de la llamada Ventanilla única.

Se conoce como ley paraguas la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio. Esta diseñada a efectos de acreditar el cumplimiento de los requisitos exigidos para el acceso y ejercicio de una actividad de servicios, las Administraciones Públicas aceptarán los documentos procedentes de otro Estado miembro de los que se desprenda que se cumplen tales requisitos. En el caso de documentos emitidos por una autoridad competente, no se exigirá la presentación de documentos originales o copias compulsadas ni traducciones juradas, salvo en los casos previstos por la normativa comunitaria, o justificados por motivos de orden público y de seguridad pública.



Todos los procedimientos y trámites que supeditan el acceso y ejercicio a una actividad de servicios se podrán realizar electrónicamente y a distancia salvo que se trate de la inspección del lugar o del equipo que se utiliza en la prestación del servicio.

Los prestadores de servicios podrán acceder, electrónicamente y a distancia a través de una ventanilla única, tanto a la información sobre los procedimientos necesarios para el acceso y ejercicio de una actividad de servicios, como a la realización de los trámites preceptivos para ello, incluyendo las declaraciones, notificaciones o solicitudes necesarias para obtener una autorización, así como las solicitudes de inscripción en registros, listas oficiales, asociaciones y colegios profesionales.

Las Administraciones Públicas promoverán que los prestadores de servicios puedan a través de la ventanilla única:

- Obtener toda la información y formularios necesarios para el acceso y ejercicio de su actividad.
- Presentar toda la documentación y solicitudes necesarias.
- Conocer el estado de tramitación de los procedimientos en que tenga la condición de interesado, y recibir la correspondiente notificación de los actos de trámite preceptivos y la resolución de los mismos por el órgano administrativo competente.

3.17 Ley 25/2009, de 22 de diciembre

La Ley 25/2009, de 22 de diciembre o como se conoce popularmente la Ley ómnibus, es la otra ley que fue tramitada, junto a la Ley paraguas para cumplir con las normas de funcionamiento de la Ventanilla única.

Cuando se trate de procedimientos y trámites relativos a una actividad de servicios y a su ejercicio incluida en el ámbito de aplicación de la ley sobre el libre acceso a las actividades de servicios y su ejercicio, los prestadores podrán realizarlos, por medio de una ventanilla única, por vía electrónica y a distancia, salvo que se trate de la inspección del lugar o del equipo que se utiliza en la prestación del servicio.

Asimismo, las Entidades locales promoverán que los prestadores de servicios puedan a través de la ventanilla única obtener toda la información y formularios necesarios para el acceso a una actividad y su ejercicio, y conocer las resoluciones y resto de comunicaciones de las autoridades competentes en relación con sus solicitudes.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Las Administraciones Públicas tendrán permanentemente publicados y actualizados modelos de declaración responsable y de comunicación previa que en todo caso se podrán presentar por vía electrónica.

En particular, en los procedimientos relativos al acceso a una actividad de servicios y su ejercicio, los ciudadanos tienen derecho a la realización de la tramitación a través de una ventanilla única, por vía electrónica y a distancia, y a la obtención de la siguiente información a través de medios electrónicos:

- Los requisitos aplicables a los prestadores establecidos en territorio español, en especial los relativos a los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio.
- Los datos de las autoridades competentes en las materias relacionadas con las actividades de servicios, así como de las asociaciones sectoriales de prestadores de servicios y las organizaciones de consumidores que presten asistencia a los prestadores y destinatarios de los servicios.
- Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios.
- Las vías de reclamación y recurso en caso de litigio entre las autoridades competentes y el prestador o el destinatario, o entre un prestador y un destinatario, o entre prestadores.

3.18 Plan Avanza

3.18.1 Origen y primeros años.

El Plan Avanza constituye una de las cuatro líneas estratégicas del Programa INGENIO 2010^x, iniciativa que fue presentada en junio de 2005 por el Gobierno de España en respuesta a la relanzada Estrategia de Lisboa que aprobó el Consejo Europeo de Primavera en 2005. Ingenio 2010 establecía como objetivo estratégico la convergencia con la Unión Europea en 2010, tanto en renta per cápita como en empleo y en sociedad del conocimiento.

La aprobación del Plan Avanza llegó por acuerdo del Consejo de Ministros el 4 de noviembre de 2005. Con el fin de converger con Europa en materia de Sociedad de la Información, el Plan Avanza agrupa las políticas de I+D+i en este ámbito, procurando la convergencia de comunidades y ciudades autónomas.

El Ministerio de Industria, Turismo y Comercio lideró la redacción del Plan Avanza, que fue elaborado con el acuerdo de los distintos Ministerios de la Administración General del Estado (AGE), otras Administraciones (autonómicas y locales) y agentes involucrados. De este modo, se creó una ponencia sobre

el Plan de Convergencia para que elaborara el informe con las aportaciones de los diferentes actores representados en el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información (CATSI).

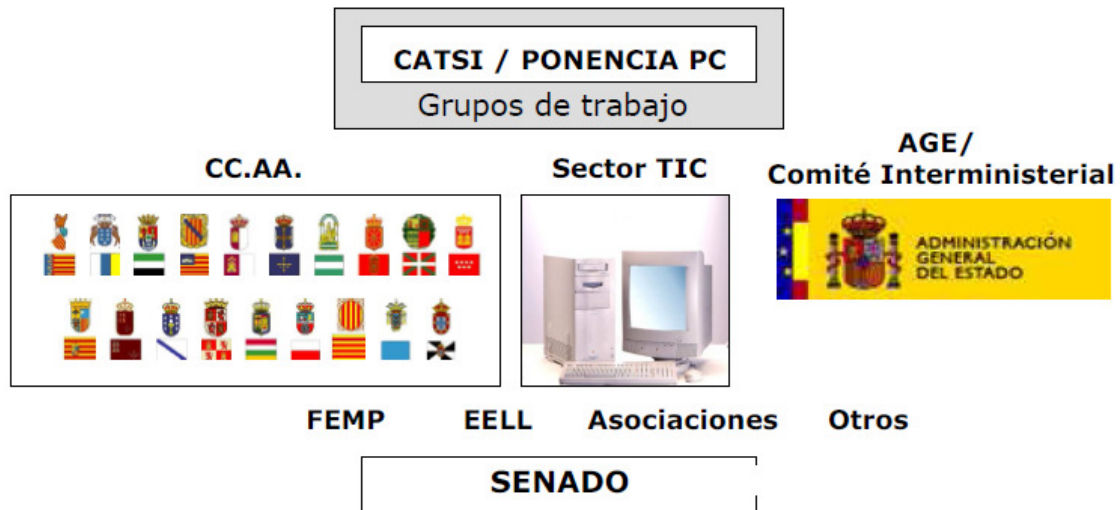


Imagen 3-2 Artífices de la elaboración del Plan Avanza

Posteriormente, el Plan Avanza ve su continuidad con el Plan Avanza 2 aglutinando esfuerzos por construir la Sociedad de la Información en España. Avanza 2 se presentó al Consejo de Ministros el 30 de enero de 2009, con el fin de afianzar los hitos alcanzados en el primer plan Avanza y reforzar o definir nuevas actuaciones a partir de las prioridades identificadas.

Entre los principales objetivos del Plan Avanza 2 se encuentra promover el uso intensivo, productivo y generalizado de las TIC, orientado a la recuperación económica del país.

3.18.2 Ejes de actuación y objetivos de Avanza y Avanza 2

Ciudadanía Digital, Economía Digital, Servicios Públicos Digitales y Contexto Digital fueron los cuatro grandes ejes de actuación en los que se articulaba el Plan Avanza en su concepción original, en sus primeros años, entre 2005 y 2008. Los objetivos y principales iniciativas se sintetizan en el cuadro que se presenta a continuación.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación



Imagen 3-3 Ejes de actuación del primer Plan Avanza

Más adelante, tras la evaluación de los resultados alcanzados y para reforzar determinadas líneas estratégicas se definió el Plan Avanza 2. Las iniciativas del renovado plan se agrupan en cinco ejes de actuación:

1. “Desarrollo del sector TIC”, con el objetivo de apoyar a empresas que desarrollen nuevos productos, procesos, aplicaciones, contenidos y servicios TIC, promoviendo, como prioridades temáticas básicas, la participación industrial española en la construcción de la Internet del Futuro y el desarrollo de contenidos digitales.
2. “Capacitación TIC”, que persigue incorporar masivamente a la Sociedad en Red tanto a ciudadanos como a empresas, con una prioridad reforzada en las pymes y sus trabajadores.
3. “Servicios Públicos Digitales”, mediante la cual se mejorará la calidad de los servicios prestados por las Administraciones Públicas en Red, con énfasis especial en el apoyo a las Entidades Locales y el desarrollo de las funcionalidades del DNI electrónico, de cuyo desarrollo España es pionera a escala internacional.
4. “Infraestructura”, para reforzar el impulso al desarrollo y la implantación de la SI en entornos locales, mejorando la prestación de los servicios públicos electrónicos al ciudadano y las empresas mediante el uso de las TIC.

5. “Confianza, Seguridad y Accesibilidad”, con el doble objetivo de reforzar la confianza en las TIC entre ciudadanos y empresas, mediante políticas públicas de seguridad de la información, y de fomentar la accesibilidad de los servicios TIC.



Imagen 3-4 ejes de actuación y objetivos del Plan Avanza 2

3.18.3 Estrategia 2011-2015 del Plan Avanza 2.

La Comisión Europea presentó el 19 de mayo de 2010 la Comunicación sobre la “Agenda Digital para Europa”^{xi}, cuyo objetivo es promover el desarrollo de la Sociedad de la Información y las TIC para la reactivación económica y la creación de empleo en la UE con el horizonte temporal del año 2020, tomando así el relevo del Programa i2010.

El 16 de julio de 2010 el Consejo de Ministros aprobó la estrategia 2011-2015 del Plan Avanza 2 que se enmarca dentro de las iniciativas que se elaboran en el ámbito europeo.

Tomando como punto de partida el Plan Avanza aprobado en 2005, así como el marco europeo en el que se encuadran este tipo de iniciativas, se han identificado treinta y cuatro retos concretos que debe abordar España en el ámbito de las TIC. En este contexto, la Estrategia 2011-2015 del Plan Avanza 2

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

va a centrar sus esfuerzos en la consecución de los siguientes diez objetivos que facilitarán la superación de los retos definidos:

1. Promover procesos innovadores TIC en las Administraciones Públicas.
2. Extender las TIC en la sanidad y el bienestar social.
3. Potenciar la aplicación de las TIC al sistema educativo y formativo.
4. Mejorar la capacidad y la extensión de las redes de telecomunicaciones.
5. Extender la cultura de la seguridad de la información entre la ciudadanía y las empresas.
6. Incrementar el uso avanzado de servicios digitales por la ciudadanía.
7. Extender el uso de soluciones TIC de negocio en la empresa.
8. Desarrollar las capacidades tecnológicas del sector TIC.
9. Fortalecer el sector de contenidos digitales.
10. Desarrollar las TIC verdes.

Para la consecución de los diez objetivos definidos, se han identificado más de cien medidas concretas que se deben articular, así como los indicadores de seguimiento que medirán su grado de consecución.

Adicionalmente, se ha identificado un conjunto de reformas normativas, necesarias tanto para eliminar barreras existentes a la expansión y uso de las TIC, como para garantizar los derechos de los ciudadanos en la Sociedad de la Información.

El Plan Avanza toma las medidas necesarias para impulsar y alinear a nuestro país en el contexto digital europeo, en línea con los objetivos de la Agenda.



4 TIPOS DE RELACIONES CON LA EADMINISTRACIÓN

La Ley consagra, por consiguiente, la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones. El reconocimiento de tal derecho y su correspondiente obligación se erigen así en el eje central del proyecto de Ley. Pero en torno a dicho eje es preciso abordar muchas otras cuestiones que contribuyen a definir y concretar el alcance de ese derecho. Así por ejemplo tal derecho se hace efectivo de modo real mediante la imposición a todas las Administraciones públicas, en los términos de la ley, de la obligación de que cada una de ellas ponga a disposición de los ciudadanos al menos un punto de acceso único a través del cual los usuarios puedan, de forma sencilla y accesible para todos:

- Acceder a la información y servicios de su competencia
- Presentar solicitudes y recursos
- Presentar ofertas en los procedimientos de contratación pública
- Realizar el trámite de audiencia cuando proceda
- Efectuar pagos
- Acceder a las notificaciones y comunicaciones que les remita la Administración Pública.

En esos puntos de acceso único de cada Administración el ciudadano tiene que poder encontrar con facilidad los medios para dirigirse a las demás Administraciones. Éstas colaboran entre sí y sobre todo con los ciudadanos no sólo facilitándoles el acceso a los servicios de cada una, sino el acceso a las demás, por remisión a las direcciones de las mismas, de forma que para el ciudadano cada Administración sea un punto de referencia de servicios totales multiadministración. No se prescinde del punto de vista de cada Administración con sus competencias y las garantías de su ejercicio, sino que se adopta el punto de vista del ciudadano y de su interés en que se le facilite lo que tiene que hacer con independencia de quién sea competente. También debe encontrar información en dicho punto de acceso único sobre los servicios electrónicos multicanal o que le sean ofrecidos por más de un medio, tecnología o plataforma.

Finalmente ese derecho a relacionarse con las Administraciones Públicas por medios electrónicos tiene también un contenido concreto, que no es sino una manifestación del derecho a relacionarse con la Administración por medios electrónicos, el derecho a conocer por dichos medios cuál es el estado del expediente en cada momento.

La Ley regula el contenido de la información a que los ciudadanos pueden acceder cuando electrónicamente desean saber el estado de los expedientes en que tengan la condición de interesados. Esto exige algún esfuerzo de la Administración, pero sobre todo exige ir adaptando los modos de trabajo hacia una Administración electrónica en plenitud. Si ésta no puede todavía implantarse de una sola vez de modo pleno (al tener que mantener los modos tradicionales en soporte papel puesto que no todos los interesados en un expediente estarán en condiciones ni desearán siempre que el mismo se tramite electrónicamente en su totalidad), al menos los hábitos de trabajo deben irse construyendo con la idea puesta en que la Administración electrónica es una Administración transparente para los interesados, sin perjuicio de garantizar su privacidad, nada ayuda más a ello que tomar conciencia de que cada trámite que haya que realizar todavía en soportes convencionales, debe quedar recogido en un índice electrónico donde se pueda conocer en tiempo real por los ciudadanos el estado y trámite en que se encuentra el expediente.

4.1 Los usuarios de los nuevos servicios administrativos

La Administración, con sus planes de modernización de la gestión y los servicios, pretende responder a los nuevos tiempos y adecuarse a las nuevas exigencias de los ciudadanos, más dinámicos, más formados, más conscientes de sus derechos. Los usuarios han modificado su comportamiento, quieren participar en el desarrollo de procesos y servicios que les afectan, saben priorizar sus necesidades y exigir productos no sólo conformes a pautas y normas, sino también servicios de calidad, personalizados. Desean obtener tanta información como sea posible con el menor esfuerzo, de una forma ágil y rápida, que les permita ganar tiempo para dedicarlo a otras actividades.

Por lo tanto, la Administración Pública se ve obligada a prestar sus servicios, y más concretamente, sus servicios de información, traduciendo las necesidades de los ciudadanos en atributos y características de estos servicios, de manera que exista la mayor equiparación posible entre lo que el usuario espera y aquello que se ofrece. Por ello, se hace imprescindible conocer las necesidades específicas de los diferentes usuarios para adecuar los nuevos servicios ofrecidos por las Administraciones Públicas a las necesidades de información de cada uno de estos grupos. El Subdirector General de Coordinación de Recursos Tecnológicos de la AGE establece una clasificación de usuarios o actores de la Administración electrónica. Estos colectivos serían:

- Los *ciudadanos*, que necesitan información sobre los diferentes servicios de la Administración, y sobre cómo realizar trámites. Buscan facilidad y comodidad en sus relaciones con la administración, que la vía electrónica puede proporcionar, puesto que realizar estos trámites y consultas de forma virtual les evita desplazamientos y les ahorra tiempo. Estos servicios quedan englobados bajo el concepto G2C (*Government to Citizen* o Administración hacia ciudadano).



- Las *empresas*, que en sus relaciones con la Administración pretenden reducir sus costes de transacción y buscan en la administración virtual una forma rápida y económica de hacer negocios y obtener la información pública que necesitan para ello. Estos servicios se conocen bajo la denominación G2B (*Government to Business* o Administración hacia empresas).
- Los *empleados públicos* de la propia Administración, para los que el paradigma virtual va a suponer nuevas formas de trabajo y nuevas formas de relación entre ellos mismos, puesto que se va a crear un espacio virtual común, en el que la cooperación, la compartición de conocimientos y experiencias y la formación continua van a constituir elementos fundamentales. Es lo que se conoce bajo el nombre G2E (*Government to Employee* o Administración hacia empleado).
- *Otras administraciones*, ordenando y buscando sinergias en las relaciones que se establecen entre las distintas administraciones. Se trata del modelo G2G (*Government to Government* o Administración hacia Administración).

4.2 Características de los nuevos servicios administrativos

La utilización de las tecnologías de la información y la comunicación en los entornos administrativo-documentales está desplazando el centro de atención desde los aspectos productivos a la forma en que se suministra información al usuario, a la prestación de servicios de información, que tienden a acomodarse a las necesidades y exigencias de los usuarios, hasta personalizarse y adaptarse a una audiencia individual.

Las prestaciones informativas de la informática mediante los dispositivos de telecomunicación también han contribuido a suprimir limitaciones y restricciones, tanto para los usuarios como para la Administración. Los conceptos tradicionales de espacio y tiempo se ven ampliados, pues el ciudadano, gracias a los nuevos servicios de información, no tendrá que desplazarse para realizar cualquier trámite, ni ajustarse a horarios fijos. El acceso a la información se hace más cómodo, fácil y rápido, ya que con un solo clic del ratón, el usuario podrá obtener toda la información que necesite, y no sólo a través del ordenador, sino mediante cualquier dispositivo, como por ejemplo el móvil.

Los nuevos servicios de información administrativa están abriendo nuevas vías de participación y comunicación de los ciudadanos con la Administración a través de buzones electrónicos de quejas o sugerencias, listas de correo o foros donde expresar opiniones, boletines de noticias para estar continuamente informados de manera actualizada de los asuntos que conciernen a los ciudadanos, o incluso de participación política incidiendo en la labor de sus representantes o mediante el voto electrónico. La vía telemática se convierte, pues, en una auténtica vía de participación ciudadana, produciendo una consolidación de los principios en los que se asientan las democracias.

Por otra parte, además de optimizar el servicio al ciudadano, la Administración electrónica presenta la ventaja de aumentar la eficacia en sus actividades informativo-documentales, ya que la necesaria sistematización de los procesos y la simplificación de los procedimientos en la gestión electrónica, se traduce en una reducción de los tiempos de tramitación y en un ahorro de tipo económico. Pero este ahorro no sólo es económico, sino que hace disponer de más tiempo al gestor administrativo para realizar tareas de valor añadido. Igualmente representa la oportunidad de facilitar la información sobre la gestión, haciendo posible una verdadera transparencia informativa, como requiere todo estado de derecho.

En definitiva, la incorporación de las TIC no sólo permite mejorar la gestión interna de las administraciones, racionalizar sus actividades e incrementar su productividad, sino que además todo ello repercute de forma positiva en la calidad y difusión de los servicios prestados y en la mejora de la atención a los ciudadanos. Gracias a las tecnologías de la información, y especialmente, Internet, las vías para acceder a la información administrativa y para comunicarse con la Administración se han visto ampliadas.

4.3 Información a la carta

Personalizar los servicios de información y documentación administrativa se convierte en uno de los objetivos prioritarios de la Administración Pública española. Con este fin, en algunos sectores de la Administración se están desarrollando una serie de proyectos que persiguen facilitar el acceso de información personalizada a los ciudadanos. Es el caso de la Ventanilla Única, las Plataformas de Llamadas, las Cartas de Servicio, los Puntos Automáticos de Consulta y Gestión, instrumentos inmejorables de información y comunicación.

A continuación se muestra un planteamiento temático de la incidencia que los tres reales decretos han tenido en el desarrollo de la Ley, haciendo un resumen de esta y resaltando las principales aportaciones de los reales decretos en cada uno de los puntos tratados. En el texto se han eliminado las referencias que podrían hacer que pareciera que su aplicación se limita a la Administración General del Estado, dado el carácter supletorio del Real Decreto 1671/2009. Aunque se ha respetado en lo posible la literalidad de las normas, se han eliminado las referencias a otras normas anteriores y al propio articulado, dado el carácter divulgativo del texto, con el fin de hacer más sencilla su comprensión.

4.3.1 Sede electrónica

Ley 11/2007

La Sede Electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad,



gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

El establecimiento de una Sede Electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras.

La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y usabilidad, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

En la sede electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones que pueden presentarse en el mismo.

Real Decreto 1671/2009

Contenido y servicios de las sedes electrónicas

Toda sede electrónica dispondrá del siguiente contenido mínimo:

- Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión y de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.
- Información necesaria para la correcta utilización de la sede incluyendo el mapa de la sede electrónica, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relacionada con propiedad intelectual.
- Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.
- Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Relación de sistemas de firma electrónica que sean admitidos o utilizados en la sede.
- Normas de creación del registro o registros electrónicos accesibles desde la sede.
- Información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la Agencia Española de Protección de Datos.

Las sedes electrónicas dispondrán de los siguientes servicios a disposición de los ciudadanos:

- Relación de los servicios disponibles en la sede electrónica.
- Carta de servicios y carta de servicios electrónicos.
- Relación de los medios electrónicos de acceso.
- Enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.
- Acceso al estado de tramitación del expediente.
- Publicación de los diarios o boletines.
- Publicación electrónica de actos y comunicaciones que deban publicarse en tablón de anuncios o edictos, indicando el carácter sustitutivo o complementario de la publicación electrónica.
- Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.
- Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.
- Indicación de la fecha y hora oficial.

Los órganos titulares responsables de la sede podrán además incluir en la misma otros servicios o contenidos.

No será necesario recoger en las subsedes la información y los servicios indicados cuando ya figuren en la sede de la que aquéllas derivan.

Las sedes electrónicas cuyo titular tenga competencia sobre territorios con régimen de cooficialidad lingüística posibilitarán el acceso a sus contenidos y servicios en las lenguas correspondientes.

Reglas especiales de responsabilidad



El establecimiento de una sede electrónica conllevará la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma. El titular de la sede electrónica que contenga un enlace o vínculo a otra cuya responsabilidad corresponda a distinto órgano o Administración Pública no será responsable de la integridad, veracidad ni actualización de esta última.

La sede establecerá los medios necesarios para que el ciudadano conozca si la información o servicio al que accede corresponde a la propia sede o a un punto de acceso que no tiene el carácter de sede o a un tercero.

4.3.2 Registro telemático

Ley 11/2007

La Ley regula la creación de registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

Estos registros pueden admitir tanto documentos electrónicos normalizados, cumplimentados de acuerdo con formatos preestablecidos, como cualquier solicitud, escrito o comunicación dirigidos a cualquier órgano o entidad del ámbito de la administración titular del registro, pudiendo aportarse asimismo otros documentos, siempre que estos cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad.

La ley contempla la obligación de emitir automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación, incluyendo la fecha y hora de presentación y el número de entrada de registro. Los registros electrónicos también deben generar recibos acreditativos de la entrega de los documentos aportados, de forma que se garantice la integridad y el no repudio de los mismos.

En la sede electrónica de acceso al registro debe figurar la relación actualizada de las solicitudes, escritos y comunicaciones normalizadas que pueden presentarse así como, en su caso, la posibilidad de presentación de cualquier otra solicitud, escrito o comunicación.

También se especifica en la ley que las Administraciones Públicas podrían, mediante convenios de colaboración, acordar con otras administraciones la recepción de las solicitudes, escritos y comunicaciones.

Real Decreto 1671/2009

Creación de los registros

El real decreto establece los contenidos mínimos de las disposiciones de creación de los registros electrónicos:

- Órgano o unidad responsable de la gestión.
- Fecha y hora oficial y referencia al calendario de días inhábiles que sea aplicable
- Identificación del órgano u órganos competentes para la aprobación y modificación de la relación de documentos electrónicos normalizados, que sean del ámbito de competencia del registro, e identificación de los trámites y procedimientos a que se refieren.
- Medios de presentación de documentación complementaria a una comunicación, escrito o solicitud previamente presentada en el registro electrónico.

Medios de presentación no contemplados

Para evitar posibles vías alternativas no controladas de presentación, el real decreto determina que no tienen la condición de registro electrónico los buzones de correo electrónico corporativo asignado a los empleados públicos o a las distintas unidades y órganos, ni los dispositivos de recepción de fax, salvo aquellos supuestos expresamente previstos en el ordenamiento jurídico.

Rechazo de solicitudes

También hace una relación de las Solicitudes, escritos y comunicaciones que pueden ser rechazados en los registros electrónicos:

- Que se trate de documentos dirigidos a órganos u organismos fuera del ámbito de la Administración General del Estado.
- Que contengan código malicioso o dispositivo susceptible de afectar a la integridad o seguridad del sistema.
- En el caso de utilización de documentos normalizados, cuando no se cumplieren los campos requeridos como obligatorios, o cuando contenga incongruencias u omisiones que impidan su tratamiento.
- Que se trate de documentos que deban presentarse en registros electrónicos específicos.

En estos casos, establece la obligación de informar al remitente del documento, con indicación de los motivos del rechazo así como, cuando ello fuera posible, de los medios de subsanación de tales deficiencias y dirección en la que pueda presentarse. Cuando el interesado lo solicite se



remitirá justificación del intento de presentación, que incluirá las circunstancias de su rechazo.

Si el rechazo no se ha producido automáticamente, a pesar de concurrir alguna de las circunstancias descritas, el órgano administrativo competente requerirá la correspondiente subsanación, advirtiendo que, de no ser atendido el requerimiento, la presentación carecerá de validez o eficacia.

Interrupción del servicio

El real decreto detalla las circunstancias de interrupción del servicio por el tiempo imprescindible sólo cuando concurren razones justificadas de mantenimiento técnico u operativo. La interrupción deberá anunciarse a los potenciales usuarios del registro electrónico con la antelación que resulte posible.

En supuestos de interrupción no planificada en el funcionamiento del registro electrónico, y siempre que sea posible, se dispondrán las medidas para que el usuario resulte informado de esta circunstancia así como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. Alternativamente, podrá establecerse un redireccionamiento que permita utilizar un registro electrónico en sustitución de aquél en el que se haya producido la interrupción.

Emisión de justificantes

Se desarrolla en el Real Decreto la emisión de justificantes que contemplaba la Ley.

El registro electrónico emitirá automáticamente por el mismo medio un recibo firmado electrónicamente, con el siguiente contenido:

- Copia del escrito, comunicación o solicitud presentada, siendo admisible a estos efectos la reproducción literal de los datos introducidos en el formulario de presentación.
- Fecha y hora de presentación y número de entrada de registro.
- En su caso, enumeración y denominación de los documentos adjuntos al formulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos.
- Información del plazo máximo establecido normativamente para la resolución y notificación del procedimiento, así como de los efectos que pueda producir el silencio administrativo, cuando sea automáticamente determinable.

Observaciones

Aunque la ley daba la posibilidad de acordar convenios con otras administraciones para la recepción de las solicitudes, escritos y comunicaciones, el Real Decreto limita la recepción por la Administración del Estado a los escritos dirigidos a la propia Administración del Estado. No tiene sentido en el entorno telemático la recepción de solicitudes, escritos y comunicaciones dirigidos a una administración distinta a la receptora.

4.3.3 Notificaciones

Ley 11/2007

La Ley dice que para que la notificación se practique utilizando algún medio electrónico se requerirá que el interesado haya señalado dicho medio como preferente o haya consentido su utilización. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento podrán emitirse y recabarse por medios electrónicos.

El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales.

Cuando, existiendo constancia de la puesta a disposición transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.

Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en la Ley 30/1992.

Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dicho acceso.

Real Decreto 1671/2009

Práctica de la notificación

Cuando, como consecuencia de la utilización de distintos medios, electrónicos o no electrónicos, se practiquen varias notificaciones de un mismo acto administrativo, se entenderán producidos todos los efectos jurídicos derivados de la notificación, incluido el inicio del plazo para la interposición de los recursos que procedan, a partir de la primera de las notificaciones correctamente practicada. Las Administraciones públicas podrán advertirlo de este modo en el contenido de la propia notificación.



Se entenderá consentida la práctica de la notificación por medios electrónicos respecto de una determinada actuación administrativa cuando, tras haber sido realizada por una de las formas válidamente reconocidas para ello, el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación. La notificación surtirá efecto a partir de la fecha en que el interesado realice dichas actuaciones. El resto de las resoluciones o actos del procedimiento deberán notificarse por el medio y en la forma que proceda conforme a lo dispuesto en la Ley y el Real Decreto.

En la solicitud de modificación del medio de notificación preferente deberá indicarse el medio y lugar para la práctica de las notificaciones posteriores. El cambio de medio a efectos de las notificaciones se hará efectivo para aquellas notificaciones que se emitan desde el día siguiente a la recepción de la solicitud de modificación en el registro del órgano u organismo público actuante.

Formas de notificación

La práctica de notificaciones por medios electrónicos podrá efectuarse, de alguna de las formas siguientes:

- Mediante la dirección electrónica habilitada para la notificación
 - Serán válidos los sistemas de notificación que cumplan, al menos, los siguientes requisitos:
 - Acreditar la fecha y hora en que se produce la puesta a disposición del interesado del acto objeto de notificación.
 - Posibilitar el acceso permanente de los interesados a la dirección electrónica correspondiente, a través de una sede electrónica o de cualquier otro modo.
 - Acreditar la fecha y hora de acceso a su contenido.
 - Poseer mecanismos de autenticación para garantizar la exclusividad de su uso y la identidad del usuario.

Los ciudadanos podrán solicitar la apertura de esta dirección electrónica, que tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará esta dirección electrónica, comunicándose así al interesado.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, la dirección electrónica habilitada será asignada de oficio y podrá tener vigencia indefinida.

- Mediante sistemas de correo electrónico con acuse de recibo

Se podrá acordar la práctica de notificaciones en las direcciones de correo electrónico que los ciudadanos elijan siempre que se genere automáticamente y con independencia de la voluntad del destinatario un acuse de recibo que deje constancia de su recepción y que se origine en el momento del acceso al contenido de la notificación.

- Mediante comparecencia electrónica en la sede

La notificación por comparecencia electrónica consiste en el acceso por el interesado, debidamente identificado, al contenido de la actuación administrativa correspondiente a través de la sede electrónica del órgano u organismo público actuante.

Para que la comparecencia electrónica produzca los efectos de notificación, se requerirá que reúna las siguientes condiciones:

Con carácter previo al acceso a su contenido, el interesado deberá visualizar un aviso del carácter de notificación de la actuación administrativa que tendrá dicho acceso.

El sistema de información correspondiente dejará constancia de dicho acceso con indicación de fecha y hora.

- Otros medios de notificación electrónica que puedan establecerse, siempre que quede constancia de la recepción por el interesado en el plazo y en las condiciones que se establezcan en su regulación específica.

4.3.4 Tablón de anuncios

Ley 11/2007

La ley dice que la publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente. Permite de hecho, la eliminación del tablón de anuncios en soporte papel.



Real Decreto 1671/2009

El Real Decreto establece que las notificaciones y publicaciones electrónicas cumplan las siguientes exigencias técnicas:

- Aseguren la autenticidad del organismo que lo publique.
- Aseguren la integridad de la información publicada.
- Dejen constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.
- Aseguren la autenticidad del destinatario de la publicación o notificación.

4.3.5 Firma del personal al servicio de las AAPP

Ley 11/2007

La identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio.

Cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

Podrá utilizarse la firma electrónica basada en el Documento Nacional de Identidad.

Real Decreto 1671/2009

Tipos de firma electrónica mediante medios de autenticación personal

- Firma basada en el Documento Nacional de Identidad electrónico.
- Firma basada en certificado de empleado público al servicio de la Administración.
- Sistemas de código seguro de verificación.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Los sistemas de firma electrónica basados en certificados facilitados específicamente a sus empleados por la Administración sólo podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con otras Administraciones públicas cuando éstas lo admitan.

La firma electrónica deberá cumplir con las garantías que se establezcan en las políticas de firma que sean aplicables.

Los certificados emitidos para la firma, se denominarán *certificado electrónico de empleado público* y tendrán, al menos, el siguiente contenido:

- Descripción del tipo de certificado en el que deberá incluirse la denominación *certificado electrónico de empleado público*.
- Nombre y apellidos del titular del certificado.
- Número del documento nacional de identidad o número de identificación de extranjero del titular del certificado.
- Órgano u organismo público en el que presta servicios el titular del certificado.
- Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.

4.3.6 Habilitación de funcionarios

Ley 11/2007

Identificación y autenticación de los ciudadanos por funcionario público

La Ley dice que en los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos, de los que aquel no disponga, tal identificación o autenticación podrá ser válidamente realizada por funcionarios públicos mediante el uso del sistema de firma electrónica del que estén dotados.

Para la eficacia de lo dispuesto, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

Cada Administración Pública mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación prevista.



Real Decreto 1671/2009

Identificación y autenticación de los ciudadanos por funcionario público

Para llevar a cabo la identificación y autenticación de los ciudadanos por funcionario público en los servicios y procedimientos para los que así se establezca, y en los que resulte necesaria la utilización de sistemas de firma electrónica de los que aquéllos carezcan, se requerirá que el funcionario público habilitado esté dotado de un sistema de firma electrónica admitido por el órgano u organismo público destinatario de la actuación para la que se ha de realizar la identificación o autenticación. El ciudadano, por su parte, habrá de identificarse ante el funcionario y prestar consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

Se mantendrá actualizado un registro de los funcionarios habilitados en la entidad para la identificación y autenticación regulada en este artículo. Mediante el correspondiente Convenio de colaboración podrá extender sus efectos a las relaciones con otras Administraciones públicas.

4.3.7 Habilitación de terceros

Ley 11/2007

La Ley contempla la posibilidad de habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados. Dicha habilitación deberá especificar las condiciones y obligaciones a las que se comprometen los que así adquieran la condición de representantes, y determinará la presunción de validez de la representación salvo que la normativa de aplicación prevea otra cosa. Las Administraciones Públicas podrán requerir, en cualquier momento, la acreditación de dicha representación.

Real Decreto 1671/2009

El real decreto regula la habilitación contemplada en la Ley, y distingue entre representación habilitada y apoderamiento.

Representación habilitada

La habilitación requiere la firma previa de un convenio entre el Ministerio u organismo público competente y la corporación, asociación o institución interesada (colegios profesionales, asociaciones profesionales...).

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Los Convenios de habilitación surten efectos tanto en relación con la corporación, asociación o institución firmante como con las personas, físicas o jurídicas, que tengan la condición de colegiados, asociados o miembros de aquéllas. Para hacer efectiva la habilitación, estas últimas deben suscribir un documento individualizado de adhesión que recoja expresamente la aceptación de su contenido íntegro.

Las personas o entidades habilitadas para la presentación electrónica de documentos en representación de terceros deben ostentar la representación necesaria para cada actuación. La Administración podrá requerir en cualquier momento a las personas habilitadas la acreditación de la representación que ostenten, siendo válida la otorgada a través de los documentos normalizados que apruebe la Administración para cada procedimiento.

La habilitación sólo confiere a la persona autorizada la condición de representante para intervenir en los actos expresamente autorizados. No autoriza a recibir ninguna comunicación de la Administración en nombre del interesado, aun cuando ésta fuera consecuencia del documento presentado.

La representación habilitada sólo permite la presentación de solicitudes, escritos o comunicaciones en los registros electrónicos correspondientes al ámbito de la habilitación.

Apoderamiento

Se crea el registro electrónico de apoderamientos en el ámbito de la Administración del Estado. En él, se podrán hacer constar las representaciones que los interesados otorguen a terceros para actuar en su nombre de forma electrónica ante la Administración General del Estado y/o sus organismos públicos vinculados o dependientes.

Cada Departamento Ministerial y organismo público determinará los trámites y actuaciones de su competencia para los que sea válida la representación incorporada al registro de apoderamientos. Además, caso de entender que hay falta o insuficiencia de la representación formalmente incorporada al registro de apoderamientos podrán requerir al interesado la correspondiente subsanación.

4.3.8 Gestión documental

La gestión documental es el elemento clave de la Administración electrónica en general y de la tramitación electrónica y la interoperabilidad en particular. Es el ámbito que la normativa desarrolla con más profundidad dedicándole una parte importante de los contenidos del Real Decreto 1671/2009 y la mayor parte del Esquema Nacional de Interoperabilidad.



Ley 11/2007

El documento electrónico

Las Administraciones Públicas pueden emitir válidamente los documentos administrativos por medios electrónicos siempre que incorporen una o varias firmas electrónicas.

Los documentos administrativos deben incluir una referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.

Copias electrónicas

Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las Administraciones Públicas en soporte papel tendrán la consideración de copias auténticas.

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

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

Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

El archivo electrónico de documentos

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

Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes electrónicos, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Expediente electrónico

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

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

La remisión de expedientes podrá ser sustituida a todos los efectos legales por la puesta a disposición del expediente electrónico, teniendo el interesado derecho a obtener copia del mismo.

Real Decreto 1671/2009

El documento electrónico

Los documentos electrónicos deberán cumplir los siguientes requisitos para su validez:

- Contener información de cualquier naturaleza.
- Estar archivada la información en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.



- Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

Los documentos administrativos electrónicos deberán, además de cumplir las anteriores condiciones, haber sido expedidos y firmados electrónicamente, y ajustarse a los requisitos de validez previstos en la Ley 30/1992.

Se asociará a los documentos electrónicos la información relativa a la firma del documento así como la referencia temporal de los mismos.

Los metadatos

El decreto introduce en la normativa el concepto de metadato, concepto básico para la implantación de la Administración electrónica.

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, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento.

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.

Una vez asociados los metadatos a un documento electrónico, no podrán ser modificados en ninguna fase posterior del procedimiento administrativo, con las siguientes excepciones:

- Cuando se observe la existencia de errores u omisiones en los metadatos inicialmente asignados.
- Cuando se trate de metadatos que requieran actualización, si así lo dispone el Esquema Nacional de Interoperabilidad.

Independientemente de los metadatos mínimos obligatorios, los distintos órganos u organismos podrán asociar a los documentos electrónicos metadatos de carácter complementario, para las necesidades de catalogación específicas de su respectivo ámbito de gestión, realizando su inserción de acuerdo con las especificaciones que establezca al respecto el Esquema Nacional de Interoperabilidad. Los metadatos complementarios no estarán sujetos a la prohibición de modificación.

Copias electrónicas de los documentos electrónicos

Las copias electrónicas generadas que, por ser idénticas al documento electrónico original no comportan cambio de formato ni de contenido, tendrán la eficacia jurídica de documento electrónico original.

En caso de cambio del formato original, para que una copia electrónica de un documento electrónico tenga la condición de copia auténtica, deberán cumplirse los siguientes requisitos:

- Que el documento electrónico original, que debe conservarse en todo caso, se encuentre en poder de la Administración.
- Que la copia sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.
- Que incluya su carácter de copia entre los metadatos asociados.
- Que sea autorizada mediante firma electrónica.

Se podrán generar copias electrónicas auténticas a partir de otras copias electrónicas auténticas siempre que se observen estos requisitos.

Los órganos emisores de los documentos administrativos electrónicos o receptores de los documentos privados electrónicos, o los archivos que reciban los mismos, están obligados a la conservación de los documentos originales, aunque se hubiere procedido a su copiado conforme a lo establecido.

El documento electrónico, autenticado con la firma electrónica del órgano u organismo destinatario, resultado de integrar el contenido variable firmado y remitido por el ciudadano en el formulario correspondiente empleado en la presentación, será considerado también copia electrónica auténtica de documentos electrónicos presentados conforme a sistemas normalizados o formularios.

Copias electrónicas de documentos en soporte no electrónico

Se define como *imagen electrónica* el resultado de aplicar un proceso de digitalización a un documento en soporte papel o en otro soporte que permita la obtención fiel de dicha imagen.

Se entiende por *digitalización* el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra, del documento.



Cuando sean realizadas por la Administración, las imágenes electrónicas tendrán la naturaleza de copias electrónicas auténticas, siempre que se cumplan los siguientes requisitos:

- Que el documento copiado sea un original o una copia auténtica.
- Que la copia electrónica sea autorizada mediante firma electrónica.
- Que las imágenes electrónicas estén codificadas conforme a alguno de los formatos y con los niveles de calidad y condiciones técnicas especificados en el Esquema Nacional de Interoperabilidad.
- Que la copia electrónica incluya su carácter de copia entre los metadatos asociados.
- Que la copia sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.

No será necesaria la intervención del órgano administrativo depositario del documento administrativo original para la obtención de copias electrónicas auténticas, cuando las imágenes electrónicas sean obtenidas a partir de copias auténticas en papel.

Copias en papel de los documentos públicos administrativos electrónicos realizadas por la propia Administración

Para que las copias emitidas en papel de los documentos públicos administrativos electrónicos tengan la consideración de copias auténticas deberán cumplirse los siguientes requisitos:

- Que el documento electrónico copiado sea un documento original o una copia electrónica auténtica del documento electrónico o en soporte papel original, emitidos conforme a lo previsto en el presente real decreto.
- La impresión en el mismo documento de un código generado electrónicamente u otro sistema de verificación, con indicación de que el mismo permite contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u organismo público emisor.
- Que la copia sea obtenida conforme a las normas de competencia y procedimiento, que en cada caso se aprueben, incluidas las de obtención automatizada.

Destrucción de documentos en soporte no electrónico

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Los documentos originales y las copias auténticas en papel o cualquier otro soporte no electrónico admitido por la ley como prueba, de los que se hayan generado copias electrónicas auténticas, podrán destruirse si se cumplen los siguientes requisitos:

- La destrucción requerirá una resolución adoptada por el órgano responsable del procedimiento o, en su caso, por el órgano responsable de la custodia de los documentos, previo el oportuno expediente de eliminación, en el que se determinen la naturaleza específica de los documentos susceptibles de destrucción, los procedimientos administrativos afectados, las condiciones y garantías del proceso de destrucción, y la especificación de las personas u órganos responsables del proceso.
- Que no se trate de documentos con valor histórico, artístico o de otro carácter relevante que aconseje su conservación y protección, o en el que figuren firmas u otras expresiones manuscritas o mecánicas que confieran al documento un valor especial.

Se deberá incorporar al expediente de eliminación un análisis de los riesgos relativos al supuesto de destrucción de que se trate, con mención explícita de las garantías de conservación de las copias electrónicas y del cumplimiento de las condiciones de seguridad que, en relación con la conservación y archivo de los documentos electrónicos, establezca el Esquema Nacional de Seguridad.

Referencia temporal de los documentos administrativos electrónicos

Se asociarán a los documentos administrativos electrónicos una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:

- *Marca de tiempo*, entendiéndose por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.
- *Sello de tiempo*, entendiéndose por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

La información relativa a las marcas y sellos de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad.



Imágenes electrónicas aportadas por los ciudadanos

Los interesados podrán aportar al expediente, en cualquier fase del procedimiento, copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada. La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos. Las mencionadas imágenes electrónicas carecerán del carácter de copia auténtica.

Las imágenes electrónicas presentadas por los ciudadanos deberán ajustarse a los formatos y estándares aprobados para tales procesos en el Esquema Nacional de Interoperabilidad. En caso de incumplimiento de este requisito, se requerirá al interesado para la subsanación del defecto advertido.

La presentación documental que realicen los interesados en cualquiera de los lugares de presentación establecidos, podrá acompañarse de soportes conteniendo documentos electrónicos.

Obtención de copias electrónicas de documentos electrónicos

Los ciudadanos podrán ejercer el derecho a obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan condición de interesados.

La obtención de la copia podrá realizarse mediante extractos de los documentos o se podrá utilizar otros métodos electrónicos que permitan mantener la confidencialidad de aquellos datos que no afecten al interesado.

Obtención de copias electrónicas a efectos de compulsas

Cuando los interesados deseen aportar copias compulsadas al procedimiento, y siempre que los originales no deban obrar en el procedimiento, la oficina receptora, si cuenta con los medios necesarios, deberá proceder a la obtención de copia electrónica de los documentos presentados.

Estas copias digitalizadas serán firmadas electrónicamente y tendrán el carácter de copia compulsada o cotejada, sin que en ningún caso se acredite la autenticidad del documento original.

Archivo electrónico de documentos

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Se deberán conservar en soporte electrónico todos los documentos electrónicos que formen parte de un expediente administrativo, así como aquellos otros que, tengan valor probatorio de las relaciones entre los ciudadanos y la Administración.

La conservación de los documentos electrónicos podrá realizarse bien de forma unitaria, o mediante la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos así como para la comprobación de la firma electrónica de dichos datos.

Conservación de documentos electrónicos

Para preservar la conservación, el acceso y la legibilidad de los documentos electrónicos archivados, podrán realizarse operaciones de conversión, de acuerdo con las normas sobre copiado de documentos electrónicos.

Los responsables de los archivos electrónicos promoverán el copiado auténtico con cambio de formato de los documentos y expedientes del archivo tan pronto como el formato de los mismos deje de figurar entre los admitidos en la gestión pública por el Esquema Nacional de Interoperabilidad.

Formación del expediente electrónico

Los expedientes electrónicos dispondrán de un código que permita su identificación unívoca por cualquier órgano de la Administración en un entorno de intercambio interadministrativo.

El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado electrónicamente.

Los expedientes electrónicos estarán integrados por documentos electrónicos, que podrán formar parte de distintos expedientes, pudiendo incluir asimismo otros expedientes electrónicos si así lo requiere el procedimiento. Excepcionalmente, cuando la naturaleza o la extensión de determinados documentos a incorporar al expediente no permitan o dificulten notablemente su inclusión en el mismo conforme a los estándares y procedimientos establecidos, deberán incorporarse al índice del expediente sin perjuicio de su aportación separada.

Los documentos que se integran en el expediente electrónico se ajustarán al formato o formatos de larga duración, accesibles en los términos que determine el Esquema Nacional de Interoperabilidad

Real Decreto 4/2010 de 8 de enero. Esquema Nacional de Interoperabilidad

Recuperación y conservación del documento electrónico

Las Administraciones Públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

- La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.
- La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.
- La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.
- La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.
- La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones Públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas.
- El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.
- El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.
- La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor

probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

- La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.
- Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.
- Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.
- La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, como de su tratamiento y conservación en archivos o repositorios electrónicos.
- La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos electrónicos.

Repositorios electrónicos

Las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

Seguridad

Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimiento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.



Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo. La firma longeva incluye información acerca del momento en que se produjo la firma, todos los certificados que conforman la cadena de confianza y la información fiable del estado de los certificados en dicho instante, es decir, incluye todo el material que puede demostrar la autenticidad, la validez y el no repudio de la existencia de un documento en un determinado instante, más allá del periodo de validez del material de confianza que se utilizó en su momento.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Formatos de los documentos

Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

Digitalización de documentos en soporte papel

La digitalización de documentos en soporte papel por parte de las Administraciones Públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:

- Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada.
- Nivel de resolución.
- Garantía de imagen fiel e íntegra.
- Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

4.4 Servicios Centrados en el Ciudadano

La Ley de Acceso Electrónico de los ciudadanos a los Servicios Públicos *“consagra la relación con las Administraciones Públicas como un derecho de los ciudadanos y como una obligación correlativa para las Administraciones”*. La Ley cambia el modelo de *“las Administraciones podrán ofrecer acceso electrónico”* por *“las Administraciones deberán ofrecer acceso electrónico”*.

El objetivo de las medidas contempladas en esta línea estratégica es mejorar el acceso de los ciudadanos a los servicios públicos adaptándolos más a las necesidades de la ciudadanía, garantizar la inclusión para que todos se beneficien de servicios más fáciles de usar, más seguros y más innovadores, favorecer la participación ciudadana en el diseño de los servicios y darlos a conocer para fomentar su utilización.

Para ello se profundizará en el establecimiento de un sistema de atención integral al ciudadano al que se acceda por todos los canales posibles y desde cualquier lugar, que suministre servicios interactivos y transaccionales, en su más alto grado, y que sea el punto de entrada a toda la Administración del Estado. No discriminar a los usuarios para que todos hagan uso de los servicios en línea disponibles y hacer que la comunicación sea bidireccional, es decir que el ciudadano participe activamente en las actuaciones administrativas, es otro objetivo de estas actuaciones.

El desarrollo de esta línea estratégica se estructura en los siguientes puntos:

4.4.1 La Ventanilla Única

La ventanilla única es el resultado del proyecto PISTA, iniciado tras un Acuerdo de Consejos de Ministros el 4 de abril de 1997. En este proyecto participan desde febrero de 1996 los tres niveles de la Administración Pública: Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades Locales, que mediante convenios han implantado progresivamente un sistema global e intercomunicado de registros, que posibilita la transmisión telemática de asientos registrales y de todo tipo de solicitudes, escritos, comunicaciones y documentos dirigidos por los



ciudadanos a la AGE y presentados en cualquiera de los registros de los órganos que subscriben el convenio. Con ello se pretende que los ciudadanos puedan comunicarse con las grandes Administraciones territoriales a través de sus propios municipios evitándole desplazamientos e inconvenientes.

Además, la Ventanilla Única como servicio de información administrativa ofrece al ciudadano información general y específica sobre la tramitación de procedimientos y proporciona los impresos normalizados necesarios para iniciarlos, de manera que agiliza notablemente la gestión de los procedimientos y mejora la información a los administrados. Actualmente ya hay algunas Comunidades Autónomas y municipios que tienen convenios establecidos con el MAP y que ofrecen este servicio de ventanilla única a sus ciudadanos, incluso a través de Internet. Las perspectivas son que este sistema de información y gestión de los procedimientos se extienda a todas los sectores de la administración.

Garantías de información a través de la ventanilla única

Los prestadores y los destinatarios podrán obtener, a través de la ventanilla única y por medios electrónicos, la siguiente información, que deberá ser clara e inequívoca:

- Los requisitos aplicables a los prestadores establecidos en territorio español, en especial los relativos a los trámites necesarios para acceder a las actividades de servicios y su ejercicio, así como los datos de las autoridades competentes que permitan ponerse en contacto directamente con ellas.
- Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a los prestadores y a los servicios.
- Las vías de reclamación y los recursos que podrán interponerse en caso de litigio entre las autoridades competentes y el prestador o el destinatario, o entre un prestador y un destinatario, o entre prestadores.
- Los datos de las asociaciones sectoriales de prestadores de servicios y las organizaciones de consumidores que presten asistencia a los prestadores y destinatarios de los servicios.

Las Administraciones Públicas adoptarán medidas para fomentar que en la ventanilla única pueda accederse a la información contemplada en el presente artículo en otras lenguas comunitarias.

4.4.2 Las plataformas de llamada

Es un servicio de información y atención al ciudadano que está siendo progresivamente utilizado en numerosas administraciones a través del teléfono o fax (implantación de servicios 112, 010, 012, 061...). Mediante una llamada

telefónica o el envío de un fax, el ciudadano puede realizar consultas o incluso iniciar gestiones administrativas, y de esta manera, puede comunicarse con la Administración sin desplazarse físicamente. Por otra parte, la tecnología permite añadir valor a este servicio al poder garantizar un servicio 24x7 todos los días del año, rápido y personalizado.

4.4.3 Los puntos automáticos de consulta y gestión

Pretenden convertirse en una nueva forma de comunicación entre la Administración y los ciudadanos, más accesibles y cercanos al público. Estos Puntos Automáticos de Consulta y Gestión, distribuidos por la ciudad, llevarán la información administrativa a la calle para facilitar el acceso de la misma al ciudadano. Éste, además de recibir la información necesaria sobre todos los servicios públicos, puede también a través de estos puntos, dar inicio a la tramitación de algún asunto, o presentar sugerencias y reclamaciones ante las posibles deficiencias de los servicios de la Administración, a través de su cuenta de correo electrónico, puesto que proporcionan servicio gratuito de acceso a Internet. Las expectativas de difusión que pueden alcanzar estos Puntos de Información son muy amplias, pues se pretende que actúen como puntos automáticos de consulta y gestión, al igual que los cajeros automáticos de las entidades financieras, incluso podrían compartir la red de cajeros bancarios mediante convenios.

4.4.4 Las cartas de servicios

Las Cartas de Servicios son documentos que informan a los ciudadanos sobre las condiciones en que se prestan los servicios por parte de los organismos públicos, los niveles de calidad con los que se ofrecerán dichos servicios y los derechos de los usuarios en relación con éstos. Se trata de un instrumento de comunicación administrativa, puesto que facilita información útil al ciudadano sobre las unidades administrativas y a la vez fomenta la participación de éste al proporcionarle las vías para conocer sus necesidades, sugerencias y expectativas. Pero además, constituye una herramienta idónea para la mejora continua de los servicios públicos, puesto que contiene compromisos explícitos y mensurables a través de indicadores cuantificables que sirven para evaluar continuamente estos servicios.

Los objetivos de las Cartas de Servicio son:

- Facilitar el ejercicio de los derechos a los ciudadanos.
- Impulsar iniciativas de mejora dentro de la Administración.
- Controlar el grado de cumplimiento por parte de la Administración de los compromisos contraídos con los ciudadanos.
- Incrementar el grado de satisfacción de los ciudadanos respecto a los servicios prestados en la Administración.



- Informar a los ciudadanos sobre los niveles de calidad en los servicios prestados.
- Informar sobre el sistema de sugerencias y reclamaciones.

El contenido mínimo de las Cartas de Servicios se recoge en folletos divulgativos que se encuentran a disposición del ciudadano en las unidades prestadoras de servicios como en las oficinas de atención al ciudadano, e igualmente a través de Internet, en las páginas Web de estas unidades administrativas. Son muchas las entidades públicas que han implantado este sistema de comunicación con los ciudadanos: Correos y Telégrafos, el Museo del Prado, la Oficina Española de Patentes y Marcas, el Centro de Información Administrativa, la Mutualidad General de Funcionarios Civiles del Estado (MUFACE), la Comunidad de Madrid, etc.

4.4.5 Encuestas de satisfacción

Las encuestas de satisfacción son el instrumento para medir el grado de satisfacción de los ciudadanos y los usuarios directos de los servicios, y poder dar así una respuesta adecuada a las necesidades de los ciudadanos. Pueden ser de dos tipos:

- Encuestas de opinión: orientadas fundamentalmente a conocer las prioridades de los ciudadanos en general, es decir, qué quieren. Se realizan a efectos de asignar eficazmente los recursos de que dispone la Administración.
- Encuestas de satisfacción: miden la diferencia entre lo que los ciudadanos obtienen y lo que desearían obtener, es decir, entre percepción y expectativa. Se realizan sobre los usuarios de un servicio en concreto, preguntándoles, fundamentalmente, sobre las condiciones en que desean que se les preste ese servicio.

Aspectos:

- La percepción que el cliente tiene del servicio en cuestión, es decir, cómo valora el servicio recibido (servicio real).
- La expectativa del servicio antes de recibirlo, es decir, la valoración del servicio que le gustaría recibir (servicio ideal).
- Los aspectos o atributos del servicio que considera más importantes (horario, condiciones ambientales, lenguaje claro, amabilidad, rapidez en la respuesta, facilidad en la navegación, en el caso de un servicio de información electrónico...).
- Además aporta un aspecto de compenetración entre ciudadano y administración, al hacerles partícipes de sus opiniones, ya sean buenas o malas, sin tener que recurrir a presentar una queja.

4.4.6 Sistema de sugerencias y reclamaciones

La implantación de un Sistema de Sugerencias y Reclamaciones consiste en un medio de participación del ciudadano, mediante el cual éste puede hacer llegar su queja o reclamación a la Administración, en el caso de que haya sufrido alguna desatención, tardanza o cualquier anomalía en su relación con el ciudadano o haya observado algún mal funcionamiento de los servicios pueda hacer llegar su queja o reclamación a la Administración.

Por otro lado, se trata de una fuente de información muy valiosa, puesto que permite obtener datos tanto de los puntos fuertes como de las deficiencias de la organización, por lo cual se trata de una fuente indirecta de conocimiento de la calidad de los servicios prestados. De esta forma, se consideran las sugerencias y reclamaciones como oportunidades de mejora para la Administración, a la vez que los propios ciudadanos colaboran y participan, a través de este cauce, en el diseño de unos servicios públicos de mayor calidad.

4.4.7 Carta de derechos del ciudadano

La Carta de Derechos del Ciudadano es un documento que contiene de forma clara y exhaustiva el listado de los derechos que los ciudadanos pueden exigir en sus relaciones con la Administración. Se trata de una iniciativa más de aquellas administraciones que han implantado un sistema de calidad para la prestación de sus servicios al ciudadano, y que han generado instrumentos sencillos que hacen más fácil el ejercicio de los derechos ciudadanos, como es el caso de la Comunidad de Madrid.

Consiste, de nuevo, en una especie de compromiso adoptado por la Administración, que se responsabiliza ante los ciudadanos de forma expresa del cumplimiento efectivo de sus derechos, y a la vez, éstos pueden contar con un documento único, que les facilita el conocimiento de la ley. De estos documentos se hace una amplia difusión, utilizando todas las vías posibles con el fin de que los ciudadanos conozcan su existencia.

4.4.8 El defensor del ciudadano

La creación de las figuras de los Defensores del Ciudadano (Defensor del Contribuyente, del Paciente, del Viajero, etc.) es otra forma para mejorar la calidad de los servicios prestados por la Administración y de establecer una vía de comunicación entre la Administración y los ciudadanos. Consiste en unas instancias independientes y especializadas en sectores concretos, a las cuales los ciudadanos puedan recurrir con sus quejas y reclamaciones con los servicios públicos, sin necesidad de tener que indagar acerca de quién es el órgano responsable para resolver su problema. Asimismo, el análisis de las cuestiones planteadas por los ciudadanos es una forma de conocer la calidad de los servicios prestados por una unidad administrativa concreta.

5 IDENTIFICACIÓN ELECTRÓNICA

5.1 La firma electrónica

En la nueva Administración Pública electrónica, la firma electrónica hace posibles las relaciones electrónicas entre la Administración y el ciudadano.

La firma electrónica es el equivalente electrónico de nuestra firma manuscrita. Para resumirlo de forma sencilla, es un conjunto de datos que nos permiten acreditarnos y cerrar acuerdos por medios electrónicos, principalmente por Internet. En España, desde el año 2003, la firma electrónica tiene el mismo valor a efectos legales que la firma manuscrita^{xii}.

Las funciones principales que ofrece la firma electrónica son:

- Identificación del firmante: la firma identifica al firmante de forma única igual que su firma manuscrita.
- Integridad del contenido firmado: es posible verificar que los documentos firmados no hayan sido alterados por terceras partes.
- No repudio del firmante: un documento firmado electrónicamente no puede repudiarse por parte de su firmante.

Con el uso de certificados electrónicos el ciudadano puede probar su identidad, autenticarse, ante un tercero. En muchos servicios públicos, como lo es, por ejemplo, la consulta del saldo de puntos de la DGT, con esto será suficiente para poder acceder a los servicios electrónicos ofrecidos.

Sin embargo, en los trámites de cualquier procedimiento administrativo necesitará además firmar mediante firma electrónica de un modo similar a como lo haría por la vía tradicional del papel.

En este apartado se responde a qué es la firma electrónica, la respuesta no es del todo trivial, tiene sus matices y puntos de vista. Conviene ver la definición del artículo 3 de la Ley 59/2003, de Firma Electrónica:

Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

- La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

- Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
- 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.

Esta definición corresponde también a la que da la Directiva 1999/93/CE por la que se crea el marco común de firma electrónica para la Unión Europea, de hecho la Ley 59/2003 es su transposición española.

Por otra parte es necesario distinguir entre firma electrónica y firma digital. Los términos de firma digital y firma electrónica se utilizan con frecuencia como sinónimos, pero este uso en realidad es incorrecto.

Mientras que firma digital hace referencia a una serie de métodos criptográficos, la firma electrónica es un término de naturaleza fundamentalmente jurídica y más amplio desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

Un ejemplo claro de la importancia de esta distinción es el uso por la Comisión Europea. En el desarrollo de la Directiva 1999/93/CE que establece un marco europeo común para la firma electrónica empezó utilizando el término de firma digital en el primer borrador, pero finalmente acabó utilizando el término de firma electrónica para desacoplar la regulación legal de este tipo de firma de la tecnología utilizada en su implementación.

Aclarados los matices anteriores, se puede concluir que cuando se habla de firma electrónica tanto en el ámbito privado como el público, en la mayoría de los casos la solución subyacente será una firma digital basada en un esquema de clave pública/privada basado en un algoritmo de cifrado RSA y que utiliza certificados X.509 para la acreditación de la identidad del firmante. Por otra parte cuando en los párrafos antes citados se habla de medios que el firmante debe mantener “bajo su exclusivo control” se refiere básicamente a la clave privada utilizada para la creación de la firma digital.

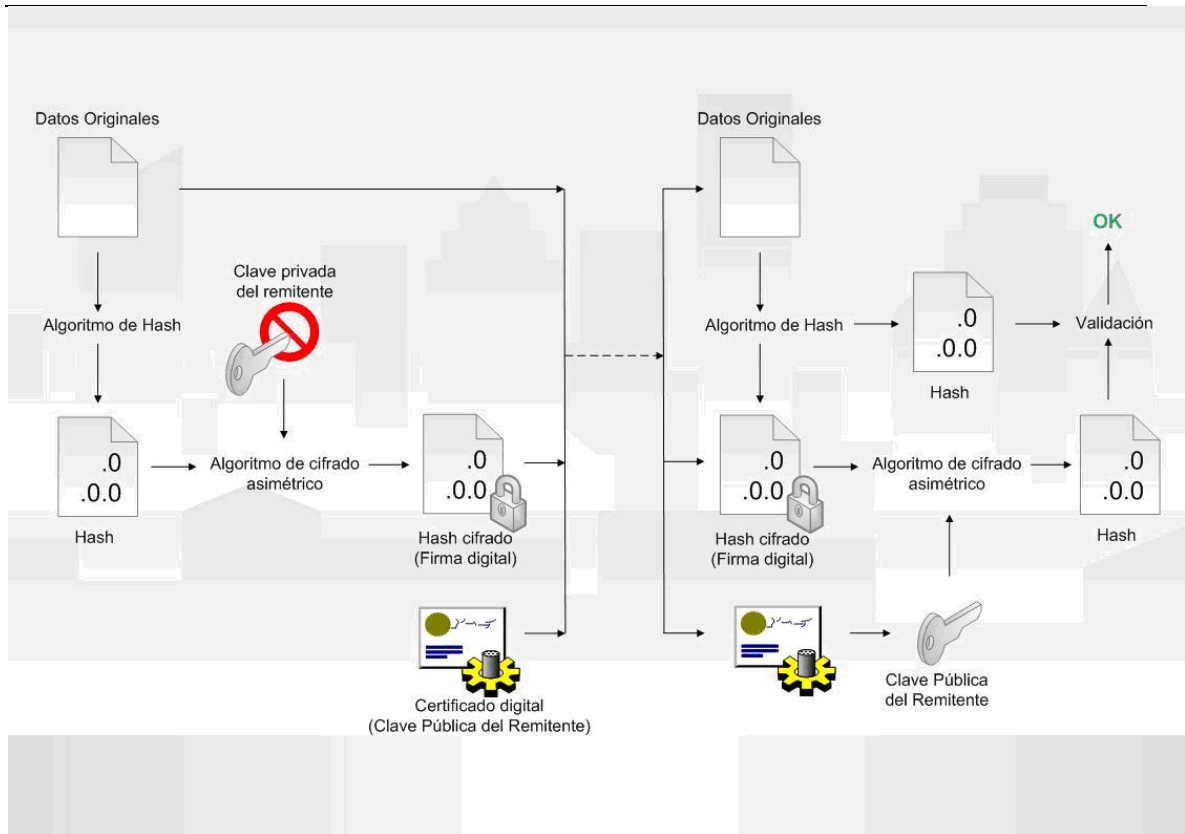


Imagen 5-1 Generación y validación

5.1.1 El certificado digital

Para poder firmar digitalmente documentos es necesario disponer de un certificado digital. Un certificado es un documento electrónico que es expedido por una Autoridad de Certificación y que identifica a una persona (física o jurídica) con un par de claves. La misión del certificado es validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta.

Contiene la información necesaria para firmar digitalmente e identificar a su propietario. Entre otros datos que se incluyen en el certificado de usuario están:

- nombre,
- NIF,
- algoritmo y claves de firma,
- fecha de expiración y
- organismo que lo expide.

La misión de la Autoridad de Certificación es dar fe de que la firma electrónica se corresponde con un usuario concreto. Con el fin de cumplir esto las Autoridades de Certificación deben mantener y proteger todos los datos de los certificados que expiden.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

El funcionamiento del proceso de firma electrónica de un documento consiste en que:

- El emisor obtiene un resumen del documento a través de una función de Hash, estas funciones son unidireccionales, aplicables a bloques de cualquier tamaño y que siempre originan un resultado fijo y muy pequeño. La propiedad más importante de ese resumen o Hash es que dos documentos diferentes siempre producen resúmenes diferentes, es imposible encontrar un documento alternativo que genere el mismo Hash. El resumen obtenido se cifra con la clave privada del firmante y se obtiene la firma electrónica del documento.
- El receptor del mensaje firmado utiliza la clave pública del emisor para descifrar la firma, obtiene el resumen del documento recibido y comprueba que es igual que el resumen que le ha llegado cifrado en la firma electrónica. De esta forma se garantiza que el contenido del mensaje no ha sido manipulado.

La firma electrónica, por sí misma, no aporta confidencialidad al mensaje pero es habitual que los mensajes firmados electrónicamente se suelen enviar cifrados con la misma clave privada utilizada para mayor seguridad.

Algunos ejemplos de operaciones que se pueden realizar actualmente haciendo uso de la firma digital son:

- Realización de la Declaración de la Renta a través de Internet.
- Recepción y envío de documentos con las Administraciones Central, Autonómica y Local.
- Firma de correos electrónicos.
- Firma de facturas electrónicas.

5.1.2 Gestión de certificados. consulta, emisión y revocación.

Una vez emitidos los certificados, no pueden usarse sin más si se quieren tener plenas garantías de seguridad, sino que es necesario cerciorarse de la validez del certificado, principalmente de su autenticidad y vigencia.

En cuanto a la autenticidad es suficiente contar con la instalación del certificado raíz de la autoridad de certificación (CA) en el equipo informático que se está usando.

Para comprobar la vigencia del certificado es necesario consultar el propio certificado, ver si aún no ha expirado (similar a cómo se haría con un DNI o una tarjeta de crédito). Pero además hay que consultar a la entidad emisora del certificado, la autoridad de certificación, para comprobar si el certificado en cuestión no fue revocado y aún sigue en vigor (aquí es válido también el símil



de una tarjeta de crédito revocada antes de su fecha de caducidad por robo, etc.).

En cuanto a esta tarea de ofrecer información de validación se habla también específicamente de autoridades de validación, que pueden ser entidades especializadas en esta tarea o bien puede asumir ese papel la propia CA. De manera similar existe el papel de autoridades de registro (de la identidad del sujeto del certificado) que igualmente puede ser ejecutado por la misma CA o bien puede ser ejecutado por otra entidad en colaboración con la CA.

La consulta sobre la validez del certificado la realizan normalmente los servidores de la entidad que presta el servicio en cuestión contra los servidores de la CA correspondiente. Por ejemplo: si un ciudadano realiza su declaración del IRPF por Internet, cuando firme electrónicamente uno de los servidores de la AEAT consultará a la FNMT si el certificado que está usando el ciudadano se encuentra vigente, la FNMT comprobará en su base de datos de certificados si es así y le responderá a la AEAT, y ésta finalmente aceptará o denegará el envío de la declaración del ciudadano.

5.1.3 Tipos de certificados

Existen diferentes tipos de certificados digitales, en función de la información que contiene cada uno y a nombre de quién se emite el certificado:

- Certificado personal, que acredita la identidad del titular.
- Certificado de pertenencia a empresa, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- Certificado de representante, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- Certificado de persona jurídica, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- Certificado de atributo, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal (por ejemplo: Médico, Director, Casado, Apoderado de..., etc.).
- Además, existen otros tipos de certificado digital utilizados en entornos más técnicos:
 - Certificado de servidor seguro, utilizado en los servidores Web que quieren proteger ante terceros el intercambio de información con los usuarios.

- Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

5.1.4 Tipos de ficheros de certificados más importantes

Cuando se solicita un certificado a un proveedor el certificado emitido por éste será entregado generalmente como un fichero que el usuario importará en su ordenador. Es conveniente hacer una copia de seguridad del certificado, junto con la clave privada y que esta información esté protegida frente a terceros que de obtenerla podrían firmar en nombre del usuario original. Un poco más adelante se verá cómo hacerlo.

Por otra parte el usuario necesitará distribuir en diferentes ocasiones su clave pública, por ejemplo, cuando envía un correo electrónico o documento firmado. En esta ocasión, sólo debe usarse el certificado, no debe distribuirse la clave privada.

En definitiva, existen diferentes escenarios de uso de certificados y claves, y ello ha dado lugar a una serie de formatos estándar con diferentes propósitos que se listan a continuación.

Extensiones y descripciones:

- **p12:** Corresponde al estándar PKCS#12 que define un formato de fichero habitual para almacenar claves privadas juntas con su correspondiente certificado, protegido por un PIN similar al usado para proteger el acceso a un teléfono móvil.
- **px:** Formato de fichero equivalente, predecesor de PCKS#12.
- **crt:** Formato para almacenar certificados X.509v3.
- **pem:** Privacy Enhanced Mail security certificate. Formato que se desarrolló específicamente en su momento para el uso de certificados con correo electrónico. Actualmente también se usa para distribución de claves privadas.
- **cer:** Formato muy frecuente para la distribución de certificados X.509. Es típico que una autoridad de certificación distribuya su certificado raíz con este formato.
- **p7b:** Formato de estructura de firma electrónica PKCS#7, pero que no embebe el documento electrónico firmado, solamente el certificado y/o lista de certificados revocados.
- **key:** Formato para la distribución de claves privadas.



5.2 DNI Electrónico

El documento nacional de identidad electrónico hace posible la identidad digital individual de cada ciudadano.

El DNI electrónico (DNLe) inició su expansión en España en el mes de Marzo de 2006. Su implantación ha supuesto un paso fundamental en el desarrollo de la sociedad de la información.

A continuación se analiza el impacto del DNI electrónico en la Sociedad de la Información desde las dos perspectivas que nos ocupan:

- El ciudadano y
- La Administración.

Los cambios tecnológicos desde la aparición de Internet han supuesto un vuelvo ¿vuelco? del patrón tradicional de prácticas de consumo, contratación, acceso a la información, comunicaciones y relación con las Administraciones Públicas. Estos cambios han abierto un abanico de opciones para el desarrollo de nuevos servicios y procesos, tanto para el sector público como privado.

Igualmente, y de forma paralela a la ampliación de la oferta de procesos y servicios, se han desarrollado nuevas formas de realizar transacciones fraudulentas como suplantación o captura de información de transacciones por un tercero. Una de las principales causas de estas prácticas fraudulentas es no poder identificar con certeza quienes son los participantes en esa transacción virtual.

Para asegurar la identidad del agente, persona, participante en la transacción y permitir firmar documentos electrónicos (jurídicos, de la Administración...) se está implantando (en España se inició la implantación en el año 2006) el documento nacional de identidad electrónico. El DNLe (Documento Nacional de Identidad Electrónico) comenzó a sustituir al DNI tradicional en el año 2006.

El DNI electrónico representa, además de un avance en materia de seguridad, un catalizador para el desarrollo de servicios online de la Administración Pública y el sector privado, permitirá agilizar los trámites administrativos, mayor seguridad en la Red y como consecuencia un aumento considerable del comercio electrónico.

5.2.1 Características

El DNI electrónico provee un sistema de seguridad que permite identificar a una persona dentro de una transacción electrónica. En el año 2006 se inició su emisión en España, emitiéndose en menos de un año más de 120.000 documentos.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Es una nueva versión del DNI tradicional, cuya principal diferencia son los nuevos elementos de seguridad. En el marco de la directiva Europea sobre firma electrónica, en la que se establece que los países miembros adoptarán PKI (*Public Key Infrastructure*) certificados, el DNle contiene un chip electrónico que almacena información del ciudadano e incorpora los certificados digitales que permitirán la identificación, autenticación y firma electrónica en transacciones electrónicas.

En el chip criptográfico se recogen los siguientes datos sobre el titular en formato digital:

- Datos de filiación del titular.
- Imagen digitalizada de la fotografía.
- Imagen digitalizada de la firma manuscrita.
- Plantilla de la impresión dactilar.
- Certificado reconocido de autenticación y de firma.
- Certificado electrónico de la autoridad emisora.
- Par de claves de cada certificado electrónico.

Físicamente, se parece mucho al anterior DNI, ya que ambos tienen las mismas medidas (85,60 mm X 53,98 mm), tamaño que comparten las tarjetas de débito y crédito habituales. Está fabricado con un material semejante: policarbonato de última generación que lo hace más duradero que el DNI tradicional (10 años aproximadamente).

En el anverso del documento, se detallan los datos:

- apellidos y nombre del titular,
- fecha de nacimiento,
- sexo,
- nacionalidad,
- fotografía en blanco y negro y
- número de documento.

Además, hay varios elementos de seguridad que impiden la falsificación del mismo:

- kinegrama de difracción microscópica,
- holograma tridimensional sobre la fotografía del titular,
- tintas visibles con luz ultravioleta,



- imagen cambiante en la parte izquierda y
- un chip criptográfico (explicado anteriormente).

En el reverso, se detallan la fecha y el lugar de nacimiento, nombre de los progenitores, domicilio, provincia y nación de residencia. Del mismo modo, aparecen el equipo de expedición del documento y los caracteres OCR-B de lectura automática, similares al DNI actual (alfanumérico: letras, números y símbolos).

Algunas de las características físicas principales que lo diferencian del DNI tradicional:

- Material más resistente, policarbonato (duración más de 10 años, soporta temperaturas de más de 200 grados centígrados).
- Chip que permite suscribir la firma electrónica.
- Fabricación por la Fábrica Nacional de Moneda y Timbre (FNMT).
- Datos grabados mediante láser y luz ultravioleta, difíciles de falsificar.
- Tiempo de tramitación: unos 10 minutos, la digitalización de los datos y la grabación en el chip son automáticas.

Son componentes altamente privados y por la seguridad del ciudadano, el chip está cifrado y protegido por unas claves de acceso (PIN) elegidas por el titular. Se pretende que el DNLe sea infalsificable e intransferible.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

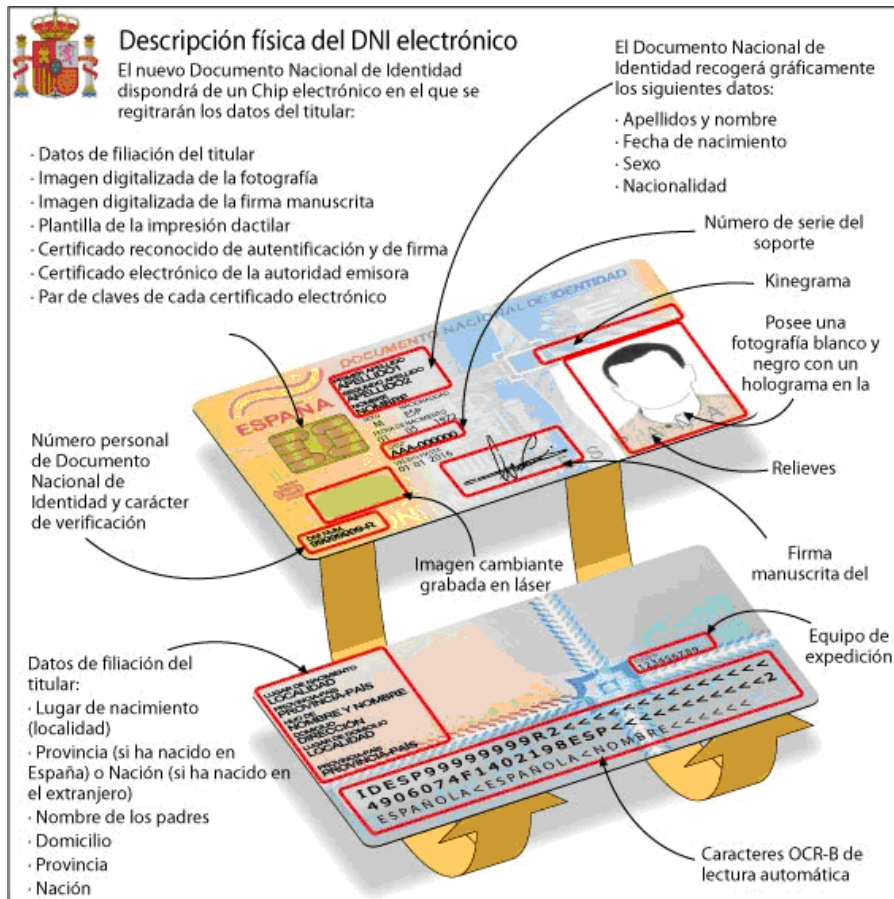


Imagen 5-2 DNle

Ahora bien, la principal diferencia con el DNI tradicional es su funcionalidad. Cabe considerar la enorme diferencia que hay entre el DNI electrónico y el DNI tradicional:

- Un DNI tradicional sirve para acreditar nuestra identidad ante terceros, pero no es capaz de firmar por nosotros.
- Por su parte el DNI electrónico, sin embargo, además de acreditarnos electrónicamente, es capaz de señalar nuestra presencia remotamente y puede firmar en nuestro nombre, si se introduce la clave adecuada.

Este hecho tan trascendental se debe reflejar en toda la legislación asociada a su utilización y aunque parezca algo imposible o improbable, el usuario debe estar protegido ante los posibles malos usos de la tecnología, tanto por parte de los delincuentes como de la Administración, quedando bien claro lo que se puede y lo que no se puede hacer con el DNI digital.

Por lo tanto, mientras que la pérdida o sustracción del DNI tradicional no supone un riesgo grave para el usuario ya que normalmente requiere la presencia del usuario para su utilización, que es autenticado *biométricamente* por el interlocutor, mediante su firma y su fotografía, no es así con un DNI electrónico. En este caso, si se ve comprometida su seguridad, este



instrumento, herramienta, electrónico puede obrar en nuestro nombre con total independencia y sin nuestro consentimiento, o conocimiento, con el riesgo que ello supone para nosotros y nuestros bienes. Además, debemos tener en cuenta que el DNI electrónico, por su naturaleza intrínseca, tendrá muchos más usos y funciones que las que tiene un DNI tradicional. Aumentarán considerablemente los ámbitos de aplicación, el interés por el producto y sus funcionalidades y con ello, las áreas de riesgo potencial para los usuarios.

Por ello, consideramos que la tecnología seleccionada debe ser segura y flexible para que dicha seguridad pueda tener perpetuación en el tiempo.

Por otra parte, el hecho de incorporar un chip, no debe eliminar la posibilidad de su uso como DNI tradicional, por lo que deberá disponer de los sistemas de seguridad y de la información necesaria, que permita su uso como tal. Además, siempre que se establezca un sistema de gestión basado en el DNI electrónico, debe haber un procedimiento alternativo tradicional, que permita usar el DNI electrónico como si fuera un DNI tradicional.

5.2.2 DNI Electrónico en España

A pesar del desconocimiento general, el funcionamiento del nuevo DNI es muy sencillo. El ciudadano puede estar seguro del funcionamiento del DNle, ya que es más fiable que su antecesor.

Los españoles podrán utilizarlo en multitud de trámites administrativos, comerciales, personales o profesionales. Su uso extendido supondrá la eliminación casi total del papel, ya que permite realizar cualquier trámite desde casa, con el ordenador personal y a cualquier hora del día. No será necesario desplazarse personalmente al edificio público o sede de la Administración que corresponda para solucionar gestiones habituales con Hacienda, la Seguridad Social o el INEM (empadronamiento, pago de multas, renovación del carné de conducir, declaración de la Renta, etc.) Todo podrá resolverse, tramitarse, desde casa, ya que el DNle verifica la personalidad del individuo y otorga validez jurídica a su firma en cualquier trámite.

La Administración está dedicando un esfuerzo importante por desarrollarlo y darlo a conocer. Sin embargo, la gran mayoría de los españoles aún no sabe qué es el DNle.

Un estudio realizado en el año 2009 por la Dirección General del Estado, sobre los hábitos de Internet en el que se entrevistó a 2.075 españoles, revela que el uso y el conocimiento del DNle por parte de los usuarios, aún no se encuentra tan extendido como en otros países europeos.

Curiosamente, la población mayor de edad es la que tiene más constancia de las utilidades del documento electrónico, siendo el sector de 31 a 40 años los *más informados* (ocho de cada diez encuestados).

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Por el contrario, los menores de 16 años apenas reconocen el uso del DNI electrónico (un 35 por ciento), y entre la población de 16 a 20 años, este porcentaje asciende hasta la mitad.

Por otro lado, la encuesta señala que el 85 por ciento de los españoles nunca ha utilizado el DNI electrónico.

Consideran que esta falta de información es responsabilidad del Gobierno (62%), los propios ciudadanos (31%) y los medios de comunicación (7%). Sólo un 8% de la muestra confiesa haber buscado información por su cuenta. Esta minoría argumenta que se ha hecho poca publicidad del DNle, aunque sí existe información que el ciudadano puede buscar como la Web oficial *www.dnielectronico.es*.

Por otra parte, las empresas empiezan a interesarse. La gran mayoría no dispone de lectores de DNle, pero sabe que serán imprescindibles a muy corto plazo. Para poder utilizar el DNle, son necesarios elementos hardware (ordenador personal, desde Pentium III, y lector de tarjetas con estándar ISO 7816) y software (sistema operativo Microsoft, Linux, Unix o Mac, cualquier navegador de Internet y módulos criptográficos). Se estima que el desembolso económico no será muy elevado y que el Gobierno prestará ayudas y subvenciones para la adaptación del mercado al nuevo documento identificativo.

Para conseguir una utilización masiva, deberá transmitir seguridad, claridad y facilidad en su uso.

De acuerdo con la Ley de Firma Electrónica, el DNle permite acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados como dispositivos de firma electrónica.

La Dirección General de la Policía (Ministerio de Interior) actúa como Autoridad de Certificación (AC), mientras que la Autoridad de Registro está constituida por todas las oficinas de expedición del DNle.

El DNle español cuenta con dos certificados, cuyo uso conjunto proporciona las garantías de autenticidad de origen y no repudio de origen:

- Certificado de Autenticación: Garantiza electrónicamente la identidad del ciudadano al realizar una transacción.
- Certificado de Firma: Permite al ciudadano no firmar trámites o documentos al sustituir la firma manuscrita por la electrónica en las relaciones con terceros.

Los certificados emitidos tienen una duración de 30 meses, para cuya renovación el ciudadano debe desplazarse nuevamente a la entidad emisora.

En Bélgica, por ejemplo, el ciudadano decide si se incluye o no el certificado de firma electrónica en el DNle.



Otro distintivo del DNle español con respecto a otros países es que en la tarjeta de identidad se incorpora la dirección del ciudadano, además de en el chip, en el caso español, la dirección viene en la tarjeta lo que implica que cambios domiciliarios hagan necesario un nuevo proceso de expedición y no únicamente de información.

El DNle en España se encuentra realizando programas de información y capacitación a los ciudadanos, informando sobre las ventajas, seguridad y característica de la información contenida en el nuevo documento nacional de identidad.

5.2.3 Cómo Obtener El DNI Electrónico

El ciudadano que solicite por primera vez su DNI electrónico y, por tanto, los certificados electrónicos asociados, deberá acudir a una Oficina de Expedición del DNI electrónico:

- Para solicitar la expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los documentos necesarios.
- La entrega del Documento Nacional de Identidad y de los certificados asociados se realizará personalmente a su titular en la misma jornada en que solicite su expedición.
- Finalizada la fase de gestión documental y la personalización física de la tarjeta, comienza la fase de personalización lógica con la carga de datos en el chip de la tarjeta soporte. La generación de claves se realizará, en la tarjeta y en presencia del titular, tras la habilitación de un PIN aleatorio que se entrega en un sobre ciego.

5.2.4 Requisitos para utilizar el DNI electrónico

Para la utilización del DNI electrónico es necesario contar con un equipamiento mínimo de elementos informáticos: equipo informático con conexión a Internet y un lector compatible, que permiten el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

El software específico para utilizar el DNI electrónico puede obtenerse gratuitamente en el área de descargas de la Web del DNI electrónico, <http://www.dnielectronico.es>.

Igualmente para solicitar su expedición puede solicitarse cita a través de Internet en <https://www.citapreviadnie.es>.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Aun así las previsiones de la Policía y la Guardia Civil sobre la vigencia del antiguo DNI apuntan a que este documento estará vigente hasta el año 2017, a pesar del empuje del DNI electrónico.

5.2.5 Servicios disponibles con el DNI-e

Ofrecer servicios a los ciudadanos y a las empresas por medios telemáticos es un objetivo prioritario tanto para la Administración General del Estado, como para las Administraciones de las Comunidades Autónomas

- Servicios DNI-e de la Administración General del Estado
 - Agencia Española de Protección de Datos
 - Gerencia de Informática de la Seguridad Social
 - INEM - Servicio Público de Empleo Estatal
 - Ministerio de Administraciones Públicas
 - Ministerio de Administraciones Públicas - MUFACE
 - Ministerio de Administraciones Públicas - INAP
 - Ministerio de Cultura
 - Ministerio de Economía y Hacienda - Dirección General del Catastro
 - Ministerio de Economía y Hacienda - Dirección General de Costes de Personal y Pensiones Públicas
 - Ministerio de Economía y Hacienda - Dirección General de Defensa de la Competencia
 - Ministerio de Economía y Hacienda - Dirección General de Seguros y Fondos de Pensiones
 - Ministerio de Economía y Hacienda - Dirección General del Tesoro y Política Financiera
 - Ministerio de Economía y Hacienda - Instituto de Contabilidad y Auditoría de Cuentas
 - Ministerio de Economía y Hacienda - Junta de Contratación
 - Ministerio de Economía y Hacienda- Inspección General
 - Ministerio de Economía y Hacienda- Dirección General de Patrimonio
 - Ministerio del Interior
 - Ministerio de Industria, Turismo y Comercio -Red.es
 - Ministerio de Fomento
 - Ministerio de Industria, Turismo y Comercio



- Instituto Nacional de Estadística
- Ministerio de Medio Ambiente y Medio Rural y Marino
- Ministerio de Medio Ambiente y Medio Rural y Marino - FEGA
- Ministerio de Sanidad y Consumo- Instituto de Salud Carlos III
- Ministerio de Trabajo e Inmigración
- Ministerio de Trabajo e Inmigración - FOGASA
- Ministerio de Ciencia e Innovación
- Comisión del Mercado de las Telecomunicaciones
- Ministerio de Justicia
- Comisión Nacional de la Competencia

- Servicios DNI-e de las Comunidades Autónomas
 - Cantabria
 - Comunidad Foral de Navarra
 - Junta de Andalucía
 - Junta de Castilla y León
 - Principado de Asturias
 - Xunta de Galicia
 - La Rioja
 - Junta de Extremadura
 - Oficina Virtual de la CCAA de Madrid
 - Gobierno Vasco
 - Junta de Comunidades de Castilla - La Mancha
 - Comunidad Autónoma de la Región de Murcia

- Servicios DNI-e de la Administración Local
 - Diputación de Albacete
 - Oficina Virtual de la Diputación de Huelva
 - Oficina Virtual del Ayuntamiento de Gijón
 - Oficina Virtual del Ayuntamiento de Cartagena
 - Organismo de Gestión Tributaria-Diputación de Barcelona
 - Ayuntamiento de Alicante
 - Ayuntamiento de San Sebastián
 - Concello de Santiago de Compostela

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Organismo Autónomo de Recaudación y Gestión Tributaria de la Diputación de Badajoz
- Ayuntamiento de Vigo
- Agencia Provincial de Administración Tributaria – Diputación de Granada
- Ayuntamiento de Pontevedra
- Ayuntamiento de Irún
- Ayuntamiento de Écija
- Ayuntamiento de Portugalete
- Ayuntamiento de Getxo
- Ayuntamiento de Ermua
- Ayuntamiento de Basauri
- Ayuntamiento de Vitoria-Gasteiz
- Ayuntamientos Guipuzcoanos
- Diputación Foral de Bizkaia
- Diputación Foral de Alava
- Diputación Foral de Gipuzkoa
- Diputación de Badajoz
- Oficina Virtual de Atención al Ciudadano del Ayuntamiento de Granollers
- Diputación Provincial de Ciudad Real
- Ayuntamiento de Barcelona
- Ayuntamiento de Sant Feliu de Llobregat
- Ayuntamiento de Jaén
- Ayuntamiento de Chiva
- Ayuntamiento de Ontinyent
- Ayuntamiento de Mislata

- Otros Organismos Públicos
 - Servicios telemáticos del Banco de España
 - Notificaciones Telemáticas Seguras
 - Instituto Español de Comercio Exterior
 - Instituto Gallego de Promoción Económica
 - Agencia Estatal de Administración Tributaria
 - Correos
 - Registradores de la Propiedad



- Sector Privado
 - Ibercaja
 - Caja Canarias
 - Banco Sabadell
 - Caixa Laietana
 - Caixa Sabadell
 - Caja Duero
 - Bilbao Bizkaia Kutxa-BBK
 - Caixa Manresa
 - Cajamar
 - Caja Rioja
 - Barclays
 - MAPFRE
 - Inversis Banco
 - Caja España de Inversiones, Caja de ahorros y Monte de Piedad
 - Caixa Penedès
 - Caixa Terrassa
 - R. Cable y Telecomunicaciones de Galicia, SA
 - Caja Rural
 - Caja de Ávila

Algunos de sus organismos, como la Agencia Estatal de Administración Tributaria, han sido pioneros en la puesta en marcha de servicios de una enorme comodidad (muchos ciudadanos ya presentan su declaración del IRPF de esta forma) basados en la firma electrónica, por lo que los primeros esfuerzos, lógicamente, se han focalizado en garantizar la compatibilidad de los servicios ya existentes con el DNI electrónico.

5.2.6 Marco legal

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 1586/2009, de 16 de octubre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

5.2.7 Autoridades de validación

La Autoridad de Validación es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.

La información sobre los certificados electrónicos revocados (no vigentes) se almacena en las denominadas listas de revocación de certificados (CRL).

En la Infraestructura de Clave Pública adoptada para el DNI electrónico, se ha optado por asignar las funciones de Autoridad de Validación a entidades diferentes de la Autoridad de Certificación, a fin de aislar la comprobación de la vigencia de un certificado electrónico de los datos de identidad de su titular.

Así, la Autoridad de Certificación (Ministerio del Interior, Dirección General de la Policía) no tiene en modo alguno acceso a los datos de las transacciones que se realicen con los certificados que ella emite y las Autoridades de Validación no tienen acceso a la identidad de los titulares de los certificados electrónicos que maneja, reforzando, aún más si cabe, la transparencia del sistema.

Para la validación del DNI electrónico se dispone de dos prestadores de Servicios de Validación:

- Fábrica Nacional de Moneda y Timbre (Real Casa de la Moneda), que prestará sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.
- Ministerio de Administraciones Públicas, que prestará los servicios de validación al conjunto de las Administraciones Públicas.

La prestación de estos servicios de validación se realiza en base a *Online Certificate Status Protocol* (OCSP), lo que, en esencia, supone que un cliente OCSP envía una petición sobre el estado del certificado a la Autoridad de Validación, la cual, tras consultar su base de datos, ofrece, vía HTTP, una respuesta sobre el estado del certificado. El servicio de validación está disponible de forma ininterrumpida todos los días del año.



5.2.8 La autoridad de certificación e infraestructuras PKI

Como se ha podido ver anteriormente, una autoridad de certificación (la abreviación CA proviene de su nombre en inglés: *Certification Authority*) avala la entidad de los sujetos/objetos a los que expide los certificados, es decir, actúa de manera muy parecida a un notario que da fe de un acto jurídico. Para ello firma sus certificados emitidos, avalando así la identidad del dueño del certificado emitido. A su vez pone a disposición su propio certificado con su clave pública, lo que permitirá la comprobación de sus firmas electrónicas. Por otra parte, ofrece servicios para la verificación de la validez del certificado, ya que los certificados a pesar de indicar su plazo de expiración pueden ser revocados antes en cualquier momento, de modo que una correcta verificación de la validez de un certificado debería consultar si éste aún no fue revocado.

Aunque generalmente se emiten certificados a los sujetos finales, también es posible emitir certificados para autoridades de certificación de un rango menor, lo cual puede ser conveniente por motivos operativos para delegar y distribuir la expedición de los certificados.

Un ejemplo muy cercano es el DNI electrónico dónde la Dirección General de la Policía actúa como Autoridad de Certificación raíz y a la vez dispone de Autoridades de Certificación intermedias o subordinadas. La CA raíz emite sólo certificados para sí misma y sus Autoridades de Certificación intermedias, y serán éstas las que emitan certificados para titulares del DNI.

En general este mecanismo responde a la idea de jerarquías de certificación, es decir, puede haber una cadena en la que las sucesivas CA de la cadena jerárquica avalan la identidad de las CA del nivel jerárquico inferior. Se comprende por tanto que al validar un certificado se recorre la cadena de confianza jerarquía hacia arriba hasta la autoridad de certificación raíz del árbol.

Pueden surgir preguntas sobre las CA como ¿y quién avala al certificado de esta última CA? ¿Cómo sé que el certificado de la CA es auténtico y no alguno que alguien haya falsificado de algún modo?

La respuesta es que la cadena de confianza empieza con el certificado de esta última CA. El almacén de certificados, que como su nombre indica es el lugar donde se guardan los certificados en el ordenador en cuestión, contiene un apartado especial para los certificados raíz. Si una determinada CA se encuentra en este apartado quiere decir que se confía en ella. Las CAs más importantes como la Fábrica Nacional de Moneda y Timbre (FNMT) ya vienen preinstaladas, es decir, asumimos que nos podemos fiar del criterio del fabricante que al incluirlas las ha considerado de confianza.

Si una determinada CA no se encuentra en el almacén ésta no se reconocerá como CA de confianza y por tanto no se confiará en los certificados emitidos por ella. En este caso hay que instalar su certificado raíz en el almacén de certificados. De nuevo será esencial en qué basamos nuestra confianza.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Generalmente esta instalación pasará por descargar el certificado raíz de la CA desde su Web, lo que implica que confiamos en la seguridad de su sitio Web.

Existen muchas Autoridades de Certificación y por tanto todas las entidades importantes ya suelen venir preinstaladas. Aunque hay excepciones, como la versión actual del navegador Web Firefox que usa su propio almacén de certificados, por ejemplo, aún no incorpora por defecto a la FNMT y hay que instalar por tanto su certificado raíz manualmente.

También puede ocurrir, como en el caso reciente de la FNMT, que una CA renueve sus certificados raíz de modo que estos no se incorporen o se incorporen tarde a las preinstalaciones de los almacenes de certificados.

5.2.9 Infraestructuras de clave pública (PKI)

Cuando se habla de Autoridad de Certificación hay que hablar también de infraestructuras de clave pública.

En criptografía, una infraestructura de clave pública (o, en inglés, PKI, *Public Key Infrastructure*) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

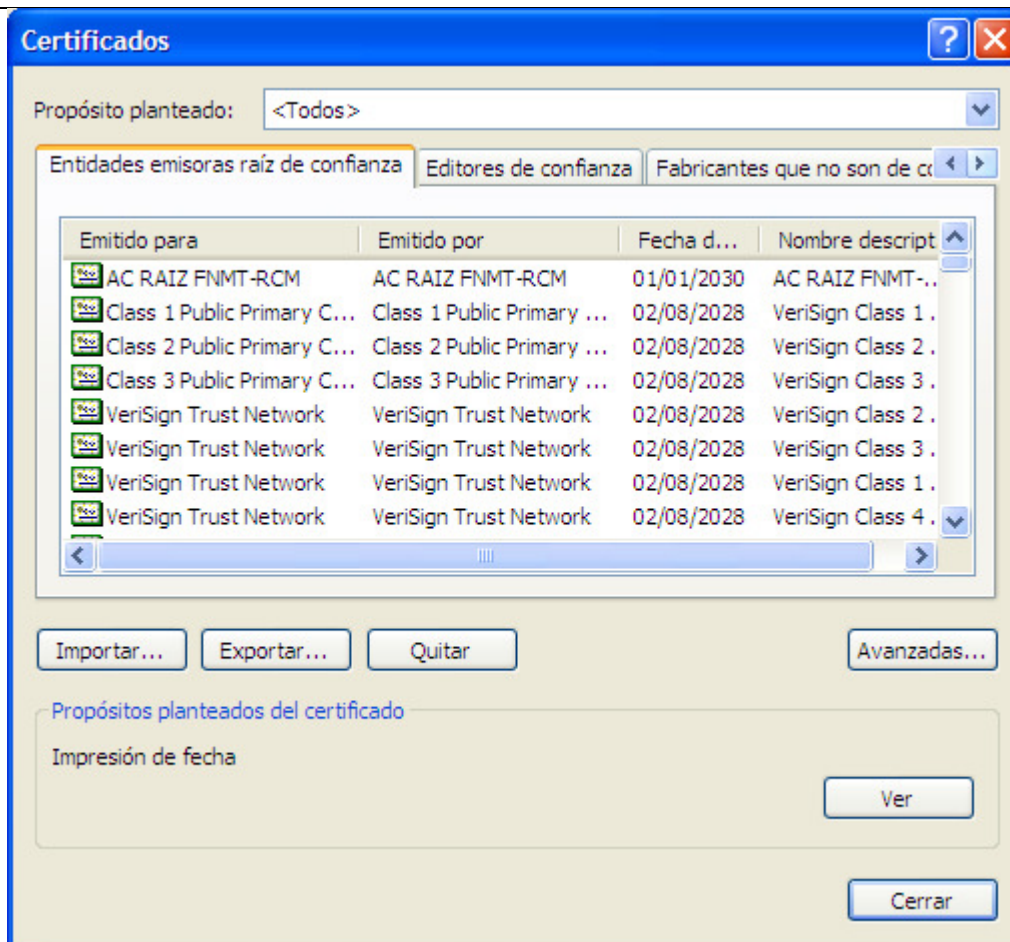


Imagen 5-3 Almacén de certificados

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

Una PKI parte de una autoridad de certificación raíz y es característico el uso de un certificado de esta autoridad autofirmado por ella. Una organización puede crear su propia PKI (lo que puede ser sumamente conveniente) y gestionar dentro de ella sus propios certificados. El problema será que para que su certificado raíz sea reconocido por los navegadores los usuarios tendrían que importarlo expresamente al no pertenecer al conjunto que el fabricante suministra por defecto con el navegador.

5.2.10 Usos de la tecnología PKI

Los principales aplicaciones del uso de certificados e infraestructuras PKI son las siguientes:

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Autenticación de usuarios y sistemas (login), identificación del interlocutor.
- Cifrado de datos digitales.
- Firmado digital de datos (documentos, software, etc.) y sellado de tiempo.
- Confidencialidad en las comunicaciones mediante técnicas de cifrado.
- Garantía de no repudio (por ejemplo: negar que cierta transacción tuvo lugar o que cierta persona es el autor de una firma electrónica).

5.2.11 Seguridad

Para hacer uso del DNI electrónico en los términos expuestos anteriormente, éste provee las siguientes funciones de seguridad:

Autenticación

La tarjeta DNle dispone de distintos métodos de autenticación, mediante los que una entidad externa demuestra su identidad o el conocimiento de algún dato secreto almacenado en la tarjeta. La correcta realización de cada uno de estos métodos permite obtener unas condiciones de seguridad que podrán ser requeridas para el acceso a los distintos recursos de la tarjeta.

- **Autenticación de usuario (PIN)**

La tarjeta DNle soporta verificación de usuario (CHV, *Card Holder Verification*). Esta operación es realizada comprobando el código facilitado por la entidad externa a través del correspondiente comando.

Cada código CHV tiene su propio contador de intentos. Tras una presentación válida de PIN, el contador de reintentos correspondiente es automáticamente puesto a su valor inicial (típicamente = 3). El contador de intentos es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. Es posible desbloquear un código tras una correcta presentación de la huella dactilar del usuario, que en este caso actúa de código de desbloqueo. A su vez estas presentaciones de huellas tienen su propio contador de intentos. Si el número de intentos de presentación de huella dactilar se agota, no será posible realizar la operación de desbloqueo. Es posible cambiar el código de CHV a un nuevo valor presentando el valor actual o presentando la huella dactilar.

El código PIN es personal e intransferible, por tanto, únicamente debe ser conocido por el titular de la tarjeta en cuestión.

- **Autenticación de usuarios mediante datos biométricos**

La tarjeta DNle permite realizar una identificación biométrica del titular de ésta, si bien esta función sólo estará disponible en puntos de acceso controlados.

La aplicación que accede al DNle, una vez conocida la información sobre las huellas contenidas en la tarjeta, decide sobre qué huella va a proceder a verificar, solicitando al portador que coloque el dedo adecuado. Tras obtener los datos biométricos desde el dispositivo lector de huellas, presenta la información biométrica a la tarjeta a través del correspondiente comando. Tras las comprobaciones iniciales de condiciones de uso y seguridad, la tarjeta procede, mediante su algoritmo *Match on Card*, a evaluar la correspondencia entre la huella presentada y la referencia.

Si la evaluación supera el umbral, la verificación es correcta. En caso contrario, la tarjeta anota una presentación errónea sobre esa huella devolviendo el número de intentos restantes.

▪ **Autenticación de aplicación**

El propósito de este método de autenticación es que la entidad externa demuestre tener conocimiento del nombre y valor de un código secreto. Para realizar esta autenticación de aplicación, se utiliza un protocolo de desafío respuesta, con los siguientes pasos:

- La aplicación pide un desafío a la tarjeta.
- La aplicación debe aplicar un algoritmo a este desafío junto con el correspondiente código secreto y nombre de la clave.
- La tarjeta realiza la misma operación y compara el resultado con los datos transmitidos por la aplicación. En caso de coincidir, considera correcta la presentación para posteriores operaciones.
- Autenticación mutua.

Este procedimiento permite que cada una de las partes (tarjeta y aplicación externa) confíe en la otra, mediante la presentación mutua de certificados, y su verificación.

En el proceso, también se incluye el intercambio seguro de unas claves de sesión, que deberán ser utilizadas para cifrar todos los mensajes intercambiados posteriormente. Este servicio permite el uso de diferentes alternativas, que podrán seleccionarse implícitamente en función de la secuencia de comandos, o explícitamente, indicando su identificador de algoritmo en un comando de gestión de entorno de seguridad anterior (MSE).

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Las dos opciones disponibles están basadas en la especificación '*CWA 14890-1 Application Interface for smart cards used as Secured Signature Creation Devices – Part 1*', y son las siguientes:

- Autenticación con intercambio de claves (*descrita en el capítulo 8.4 de CWA 14890-1*).
- Autenticación de dispositivos con protección de la privacidad, (*descrita en el capítulo 8.5 de CWA 14890-1*).

Securización de mensajes

La tarjeta DNle permite la posibilidad de establecer un canal seguro entre el terminal y la tarjeta que cifre los mensajes transmitidos. Para el establecimiento es necesaria la autenticación previa del terminal y la tarjeta, mediante el uso de certificados. Durante la presencia del canal seguro los mensajes se cifran y autentican, de tal forma que se asegura una comunicación *uno a uno* entre los dos puntos originarios del canal.

El canal seguro puede ser requerido por la aplicación o puede ser una restricción de acceso impuesta a algún recurso de la tarjeta. Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas de la tarjeta y el terminal mediante certificados que serán verificados por ambas partes. A continuación se realiza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticado.

Una vez concluido el protocolo para el establecimiento de la semilla común todos los mensajes deben transmitirse cifrados.



Desbloqueo y cambio de PIN

Se permite el cambio de PIN, mediante la presentación del valor antiguo. Es posible también el cambio de PIN bajo determinadas condiciones tras la realización de una verificación biométrica.

Debido a la criticidad de esta operación, el cambio de PIN se ha de realizar siempre en condiciones de máxima confidencialidad y en terminales específicamente habilitados a tal efecto o con las debidas condiciones de seguridad, exigiéndose por tanto, el establecimiento de un canal seguro.

El cambio de PIN, haciendo uso de la huella dactilar (desbloqueo), únicamente está permitido en dispositivos autorizados por la Dirección General de la Policía (DGP) y no se puede realizar, bajo ningún concepto, en otros terminales.

Funcionalidad criptográfica

- Claves RSA
La tarjeta DNle es capaz de generar y gestionar claves RSA. La generación de la pareja de claves RSA sigue el estándar PKCS#1 v1.5. Se usa el algoritmo Miller-Rabin como test de primalidad.
- Hash
La tarjeta DNle es capaz de realizar Hash de datos con el algoritmo SHA1. Es posible realizar todo el proceso en la tarjeta o finalizar un Hash calculado externamente. Después de finalizar cualquier operación de Hash, el código resultante es almacenado en la memoria de la tarjeta para ser usado posteriormente por un comando. El Hash sólo permanece en memoria hasta la siguiente operación.
- Firmas electrónicas
La tarjeta DNle tiene capacidad para la realización de firmas electrónicas de dos modos diferentes:
 - Modo raw
 - Modo relleno PKCS#1

Intercambio de claves

La operación de intercambio de claves es usada para compartir claves simétricas o de sesión entre dos entidades. Es posible cifrar una clave (Ks) con la clave pública de un destinatario, la cual puede ser cargada en la memoria de la tarjeta protegida mediante una clave RSA. El destinatario puede descifrar la clave (Ks) usando la clave privada RSA correspondiente.

Cifrado

La tarjeta puede realizar operaciones 3DES-CBC (triple cifrado, descifrado utilizando DES) con claves de 16 bytes (k1, k2, k1). Para realizar operaciones 3DES en la tarjeta, la clave de 16 bytes de longitud debe ser cargada en memoria. El proceso de carga está protegido por algoritmo RSA. La clave permanece en memoria hasta que se finaliza la sesión con la tarjeta o se carga una nueva.

Aplicaciones de firma

Uno de los principales usos del DNI electrónico es la realización de firma electrónica. Para utilizar esta funcionalidad de firma, numerosas aplicaciones pueden ser empleadas, ya que éstas acceden a las capas o módulos intermedios de CSP y PKCS, que proporcionan un interfaz estándar de acceso a la tarjeta.

Requisitos de seguridad del entorno

Para el correcto y seguro funcionamiento de la tarjeta DNle se han de utilizar los módulos criptográficos CSP y PKCS, que se encuentran en la dirección www.dnielectronico.es/descargas/.

Estos módulos contienen lo necesario para establecer un entorno seguro en la operación con el DNI electrónico y satisfacer los requisitos de seguridad aplicables al entorno de las tecnologías de la información descritos en el perfil de protección CWA 14169.

5.3 Comunicación con la Administración

La relación con la Administración Pública telemática es un hecho. En España, más de un 40% de ciudadanos se han puesto en contacto mediante certificados digitales de firma electrónica según el estudio de AIMC de febrero 2010^{xiii}.

Uso del certificado digital de firma electrónica a través de Internet		
	Absolutos	%
BASE	36.000	100,0
Sí, en la última semana	4.655	12,9
Sí, en el último mes	3.804	10,6
Sí, en el último año	4.884	13,6
Sí, hace más de un año	1.863	5,2
No, nunca	20.529	57,0
NS/NC	265	0,7

Tabla 1 – Uso de firma electrónica por Internet



Una vez vistos algunos ejemplos concretos de Administración electrónica y algunos de sus conceptos técnicos fundamentales, llega el momento de tocar la práctica del uso de estos servicios.

5.3.1 Uso de los certificados

Todo usuario de los servicios de Administración electrónica se enfrenta a una serie de tareas que ha de realizar para poder utilizar sus servicios con éxito. A continuación se desglosan estas tareas.

Obtener certificados electrónicos

El primer paso para poder trabajar con los servicios de Administración electrónica es la obtención de un certificado electrónico personal. No todos los servicios electrónicos requieren el uso de certificados electrónicos, de hecho, las oficinas virtuales de las diferentes Administraciones suelen ofrecer la opción de usuario y contraseña. No obstante, en este caso también es habitual que no se ofrezcan todos los servicios electrónicos por esta vía, las restricciones afectarán normalmente a los más sensibles.

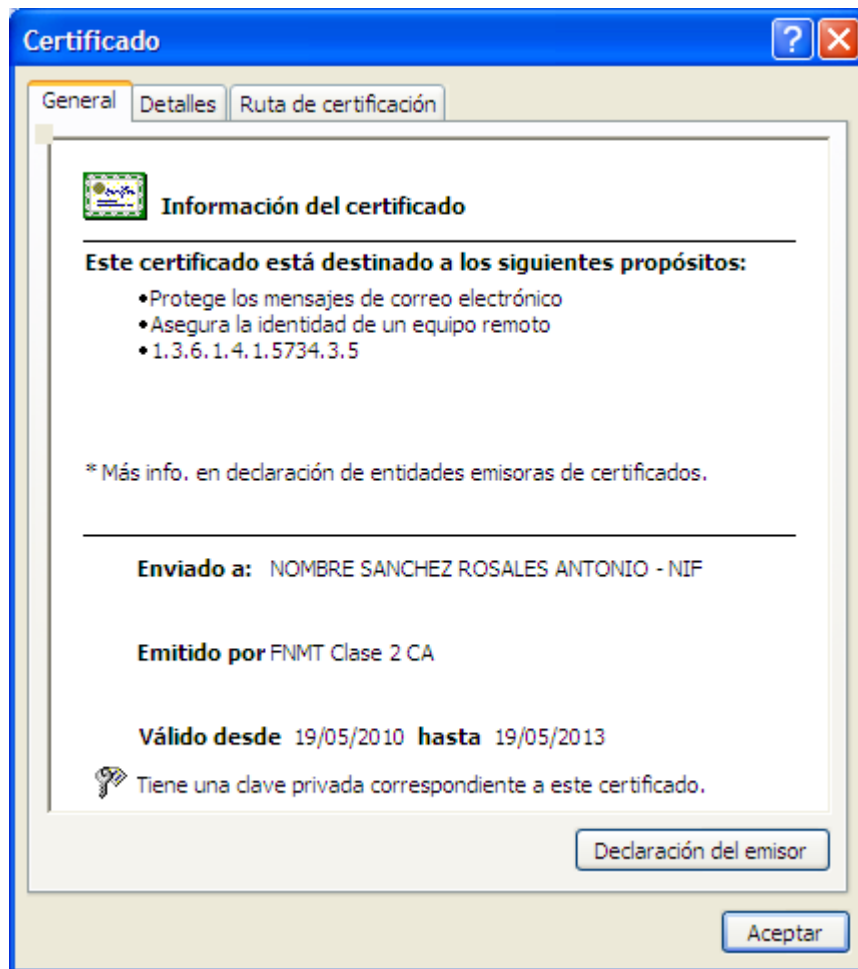


Imagen 5-4 Certificado digital

Por otra parte, según el caso, cuando se usa alguna forma de identificación alternativa a un certificado electrónico personal también será necesario un alta del usuario que requiere normalmente como mínimo rellenar un formulario con preguntas sobre determinados datos personales, o bien una llamada telefónica en la cual a través de unas preguntas específicas se comprueba la identidad del ciudadano para proporcionarle un usuario y contraseña. En algunos casos incluso se pide un acto presencial.

De cualquier modo, esta vía va a limitar al usuario al organismo en cuestión. Es decir, incluso dentro de la misma Administración Pública el usuario y contraseña obtenidos en un sitio normalmente no servirán para utilizarlos en otro servicio de esa misma Administración y lógicamente mucho menos para utilizarlo con otra distinta.

Teniendo en cuenta estas limitaciones y que con un poquito más de esfuerzo se puede obtener gratuitamente un certificado personal válido en cualquier sitio y que en el caso del DNle ya viene incluido *de serie* no parece razonable utilizar otros medios que no sean certificados electrónicos para relacionarse con la Administración.



Obtener un certificado personal

La acreditación de la identidad del interesado o interesados, es decir, la identificación y autenticación, mediante firma manuscrita, de los mismos son un requisito estándar para interactuar con la Administración Pública que viene ya formulado en la Ley 30/1992.

Como se ha podido ver anteriormente, en el mundo electrónico la identificación y autenticación se realiza mediante certificados electrónicos acreditando así la identidad de la persona física o jurídica a la que pertenece y que ha sido expedido por una entidad confiable a esos efectos (la autoridad de certificación) como, por ejemplo, la Fábrica Nacional de Moneda o Timbre (FNMT) o una comisaría (DNI electrónico).

En el caso de las personas físicas un certificado electrónico viene a sustituir por tanto la acreditación tradicional vía DNI, independientemente de que sea el certificado electrónico propio del DNLe o cualquier otro certificado electrónico admitido por la Administración, como lo pueden ser los certificados emitidos por la FNMT.

En este sentido no importa si se utilizan los certificados del DNLe u otro certificado electrónico, siempre que sean emitidos por una de las autoridades de certificación reconocidas por la Administración en cuestión. Incluso se pueden utilizar a la vez, el DNLe en unos trámites y otros certificados en otros distintos, no importa.

Por tanto, ante las diferentes opciones de certificados electrónicos disponibles, en primer lugar hay que plantearse qué tipo de certificado se quiere usar, hay básicamente tres grandes opciones con diferentes pros y contras en cada caso:

- **DNI electrónico (DNLe):** este es, hoy por hoy, la solución *natural* para el ciudadano. Al ser el DNI un documento obligatorio es una vía muy eficaz y cómoda de proveer a toda la población de certificados electrónicos. Legalmente tiene la peculiaridad que en el artículo 14 de la Ley 11/2007 se establece la obligación para todas las Administraciones de admitirlo como medio de identificación, autenticación y firma electrónica. De hecho, ésta es la estrategia mediante la cual la Administración pretende lograr un impulso masivo del uso de firma electrónica en particular y de los servicios de administración electrónica en general. Tiene además dos grandes ventajas en cuanto a su seguridad:
 - Las claves se generan en la propia tarjeta criptográfica y nadie podrá copiarlas ya que nunca salen de la tarjeta. Por tanto es absolutamente necesario hacerse con la tarjeta para suplantar la identidad del firmante, de modo que éste se dará cuenta enseguida de ello si ocurre.
 - Por otra parte las tarjetas tienen asociado su propio PIN para el cual hay que hacer las mismas advertencias en cuanto a su

custodia como en el caso de los ficheros con claves privadas, de modo que aunque se sustraiga una tarjeta el suplantador tendría que conocer además el PIN para utilizarla.

- **Certificado en tarjeta criptográfica (tarjeta inteligente):** técnicamente es similar al DNle, de hecho el DNle es una tarjeta inteligente. Pero estas tarjetas se orientan típicamente en primer término a puestos de trabajo o el ejercicio de competencias. En la Administración Pública, por ejemplo, este tipo de certificados se está usando cada vez más dentro para sus empleados públicos y son proporcionados por el propio organismo a su plantilla. Cabe pensar que serán la opción por excelencia para implantación del nuevo concepto de certificado electrónico de empleado público del Real Decreto 1671/2009.
- **Certificado en un fichero, instalable en cualquier equipo:** es la opción más simple, pero también la más expuesta a riesgos, ya que el certificado y la clave privada se guardarán en general en un fichero del tipo .p12 (es decir, ficheros que almacenan la clave privada junto con el certificado). El ejemplo clásico de este tipo de certificados son los expedidos *toda la vida* por la FNMT. Si el usuario lo custodia adecuadamente no hay de qué preocuparse, además este formato contempla un PIN de protección para impedir su uso en caso de sustracción. Pero la falta de disciplina en la custodia de este PIN, que se manifiesta en cosas como la frecuente costumbre de apuntar las claves en algún papel o dejar el fichero en algún dispositivo inadecuado (por ejemplo una llave USB que pasa a otras personas), ponen en peligro la clave privada y pueden ser una vía para que un tercero suplante fácilmente la identidad del titular del certificado sin que éste lo sepa.

Una vez elegida la opción más adecuada se debe solicitar el certificado a la autoridad de certificación en cuestión. Generalmente se siguen los siguientes pasos (pueden variar ligeramente según la CA concreta):

- Generación de un par de claves en la máquina local, en el caso de un certificado en fichero, o en la tarjeta criptográfica, una clave es privada o secreta (sólo debe disponer de ella el propio interesado) y otra es pública (la puede conocer cualquiera).
- Envío de la clave pública a la autoridad de certificación para que ésta cree el certificado, la clave privada ni siquiera se facilita a la CA, es totalmente personal, no debe salir jamás de las manos de su titular.
- Personarse en la autoridad de registro (normalmente una oficina auxiliar de la CA) correspondiente para acreditar la identidad (esto se hace normalmente presentando el DNI). En caso de personas jurídicas se exigirá la correspondiente documentación (escrituras, poderes de quien solicita el certificado, etc.).

- Si se ha solicitado una tarjeta, instalación del correspondiente software en el equipo donde se vaya a usar y adquisición de un lector de tarjeta inteligente adecuado.
- Si se ha solicitado un certificado en fichero, obtener el certificado vía descarga del mismo en Internet, envío por correo electrónico, etc. En el caso de la FNMT, por ejemplo, se descarga e instala automáticamente en el navegador desde el cual se solicitó. A partir de ahí se puede exportar del almacén de certificados y almacenar la copia en algún lugar seguro. Ésta se realizará generalmente en un fichero .p12 que incluye certificado y clave privada.

Como ejemplo de la evolución de emisión de certificados electrónicos en los últimos años, a continuación se muestra un gráfico en el que se puede apreciar la evolución de emisión de certificados digitales en Cataluña desde 2003 hasta 2009. A modo de pequeño análisis, se observa como en el año 2007 se produce un salto cuantitativo en cuanto al número de certificados, llegando a realizar más del 200% de certificados estimados por parte de la Agencia Catalana de Certificación (CATCert). No es coincidencia que ese mismo año fuese cuando se aprobó la LAESCP y que todo el personal administrativo correspondiente de las Administraciones Públicas tuviera que hacerse un certificado digital. Para terminar con la ilustración, se observa como en el año 2007 la evolución real supera con creces a los objetivos del CATCert.

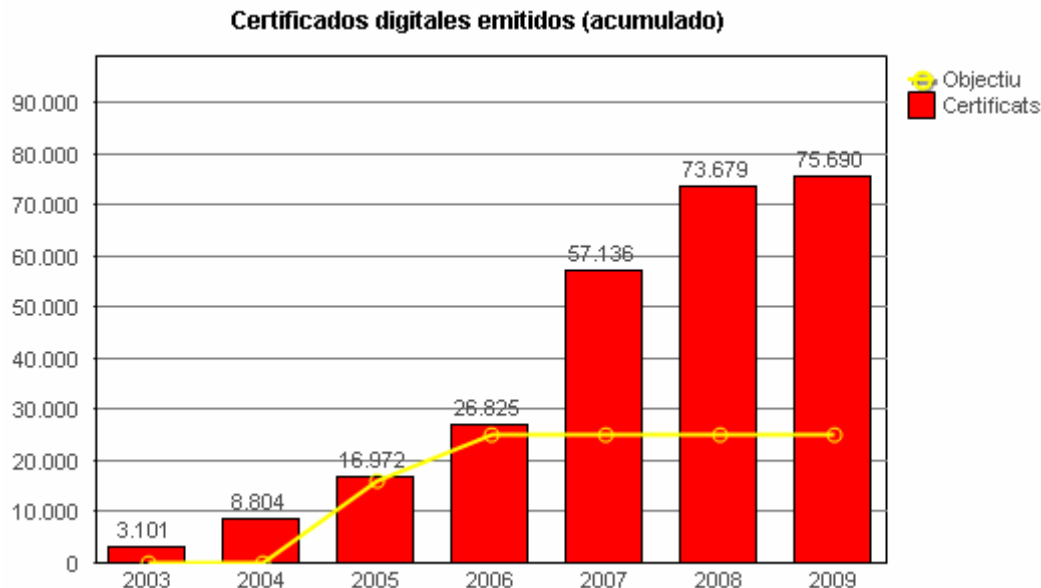


Imagen 5-5 Evolución de los certificados digitales en Cataluña.

Por último, es importante reseñar que una persona no tiene porqué limitarse a un solo certificado para todo. Es muy común, por ejemplo, la expedición de certificados o tarjetas para puestos de trabajo, aunque el usuario ya tenga el DNI electrónico u otro certificado personal.

Obtener el DNle

El Ministerio del Interior ha habilitado un extenso portal con mucha información interesante, aplicaciones y manuales en torno al DNI electrónico o DNle.

A continuación se reproduce la guía básica para la obtención del DNle publicada en este portal:

- El ciudadano que solicite por primera vez su DNI electrónico y, por tanto, los certificados electrónicos asociados, deberá acudir a una Oficina de Expedición del DNI electrónico. Estas oficinas de expedición son normalmente comisarías.
- Para solicitar la expedición del DNle será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los documentos necesarios.
- La entrega del DNI y de los certificados asociados se realizará personalmente a su titular en la misma jornada en que solicite su expedición.
- Finalizada la fase de gestión documental y la personalización física de la tarjeta, comienza la fase de personalización lógica con la carga de datos en el chip de la tarjeta soporte. La generación de claves se realizará, en la tarjeta y en presencia del titular, tras la habilitación de un PIN aleatorio que se entrega en un sobre ciego.

Existe una Web de ayuda, www.usatudni.es/dnie, puesta en marcha dentro del marco de actuación del Plan Avanza 2 y consiste en un punto de formación y ayuda sobre el DNle.

Gestionar certificados electrónicos y medios de firma electrónica

Tanto en las relaciones con los servicios de Administración Electrónica como en el trabajo con firma electrónica y certificados electrónicos en general será necesario realizar algunas tareas preparatorias y de gestión, especialmente como particular, es decir, como un usuario de informática que no cuenta con el apoyo de un departamento de informática.

Alta de certificados en el almacén de certificados

Una de las primeras tareas con las que probablemente se tendrá que enfrentar el usuario es el alta de certificados. Por una parte si ha solicitado un certificado personal en fichero, y lo quiere utilizar en un equipo diferente al que usó para



solicitarlo deberá importar su copia del certificado y clave privada contenida en un fichero con extensión .p12 (o .pfx). Por otra parte, en alguna ocasión puede ser necesario importar certificados raíz de determinadas autoridades de certificación para poder reconocer sus certificados.

El lugar para dar de alta claves privadas y certificados es el almacén de certificados del equipo, y puede ser el propio del navegador u otras aplicaciones que usen certificados, o del sistema operativo.

Navegadores como Internet Explorer o Google Chrome usan el almacén de certificados del sistema operativo, mientras que, por ejemplo, Firefox mantiene su propio almacén. En otros casos, como las aplicaciones para trabajar con documentos PDF, Adobe Reader o Adobe Acrobat, se ofrece la posibilidad de o bien mantener un almacén propio de certificados, o bien utilizar el almacén del sistema operativo.

Los casos de aplicaciones, como Firefox, que no se integran con el almacén del sistema operativo son bastante incómodos porque será necesario importar los certificados y claves privadas expresamente en el almacén de la aplicación, aunque ya se encuentren en el almacén del sistema operativo. Es de suponer que esto mejore en el futuro y que termine centralizado en algún directorio.

Tal como se puede apreciar en la imagen siguiente, los almacenes suelen diferenciar diferentes apartados dentro del almacén, según tipo de certificado en cuestión. Así un certificado raíz de una autoridad de certificación normalmente se almacenará en un apartado diferente al de los certificados personales.

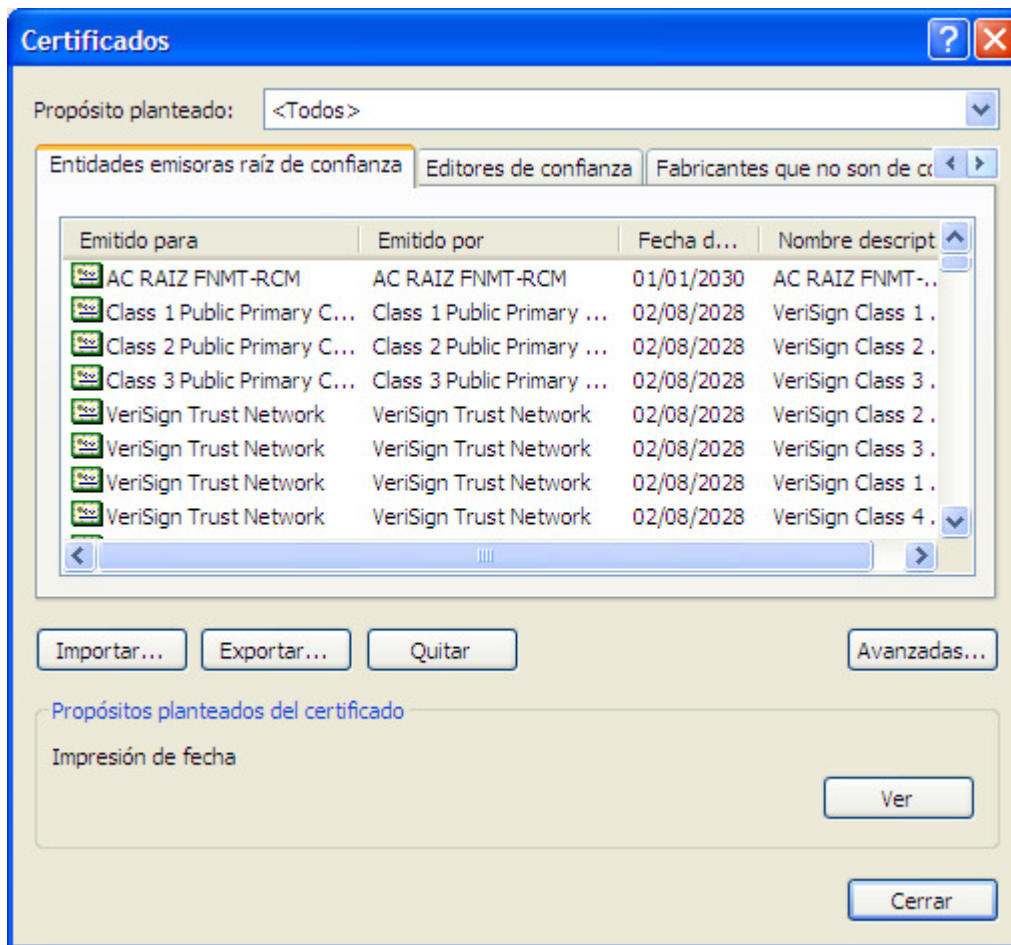


Imagen 5-6 Almacén de entidades emisoras

En el caso de tener que importar un certificado raíz de una autoridad de certificación o certificados de autoridades de certificación intermedias éstos se encontrarán disponibles en sus sedes electrónicas. En el caso, por ejemplo, del BOE éste ofrece los enlaces de descarga para los certificados raíz e intermedio de la FNMT que usa en la firma de sus boletines.

Estos certificados se podrán instalar directamente en el almacén de certificados al hacer clic sobre su enlace, según el navegador en cuestión se instalarán en el correspondiente almacén.

El otro caso básico, ya mencionado anteriormente, es la importación de un certificado personal y clave privada contenidos en un fichero .p12 o .pfx en un equipo que no disponga de él. Supongamos por ejemplo, que se solicita el certificado electrónico de la FNMT desde el navegador Web del ordenador de casa y se quiere utilizar para un determinado propósito en el ordenador del trabajo.

En este caso, después de completar el proceso de solicitud del certificado, éste se habrá quedado, junto con la clave privada en el almacén de certificados correspondiente al navegador utilizado. En el caso de usar Windows se habría quedado en su almacén.

Por tanto, si ahora se quiere utilizar este certificado y la clave privada para autenticarse y realizar firmas electrónicas desde otros equipos lo primero que hay que hacer es exportar ambos desde el almacén en cuestión, lo que dará como resultado el mencionado fichero .p12 o .pfx.

A continuación habrá que llevarse este fichero de copia al ordenador en cuestión e importarlo, al ser un formato estándar se puede intercambiar incluso entre distintos tipos de ordenadores.

En el ordenador en el cual se quiera importar el certificado personal junto con la clave privada se deberá ir al almacén de certificados en cuestión, el cual ofrecerá una manera de importar el fichero .p12 o .pfx.

5.3.1.1 Validación de certificados y firmas electrónicas

Como se ha podido ver, los certificados electrónicos proporcionan las garantías de la autenticidad de la identidad del firmante y la integridad de un documento electrónico y de cualquier otro tipo de fichero electrónico como lo podría ser, por ejemplo, un fichero de música o video.

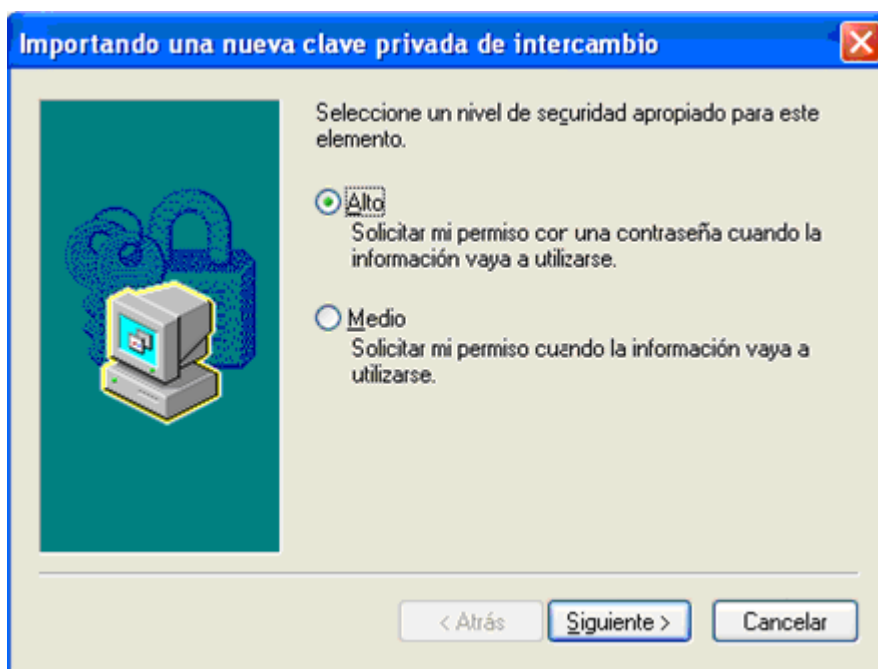


Imagen 5-7 Opciones de protección de acceso a la clave privada

Para poder confiar plenamente en un certificado electrónico usado en una firma electrónica ha de comprobarse principalmente que éste cumpla una serie de condiciones:

- Haya sido emitido por una autoridad de certificación en la que confiamos.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Se encuentre entre las entidades raíz y/o intermedias del almacén de certificados.
- El certificado no haya expirado, ni haya sido revocado.

Esta validación de la firma electrónica y el certificado en el que está basada lo hará una herramienta concreta, dependiente del formato utilizado en la firma electrónica. En las actividades profesionales, por ejemplo de un funcionario, estas tareas se realizarán en la medida de lo posible automáticamente por las aplicaciones que el profesional utiliza en su trabajo. En una aplicación de gestión de un procedimiento, será la propia aplicación de gestión del procedimiento la que validará de manera transparente para el funcionario si las firmas electrónicas son válidas. El sistema, incluso, ni aceptará documentos firmados electrónicamente. Un registro electrónico, por ejemplo, valida en el acto la firma electrónica del ciudadano, y si no es válida, ni procede a dar entrada al documento en cuestión.

No obstante, no siempre el trabajo con documentos con firma electrónica se realiza dentro de una aplicación de gestión especializada, esto podría ser el caso, por ejemplo, de dos organismos que se intercambian por correo electrónico una serie de documentos firmados electrónicamente para un propósito determinado o una empresa que envía una factura firmada electrónicamente a otra empresa o una Administración que no dispone de una recepción automatizada de facturas electrónicas.

En estos casos será necesario validar las firmas electrónicas de manera “manual”, es decir, los usuarios que trabajan con estos documentos tendrán que utilizar herramientas para la validación de las firmas electrónicas, cuya elección dependerá de los formatos concretos de firma digital utilizada.

Formatos de firma digital

Los formatos de firma electrónica más habituales con los que se encontrará el usuario son los siguientes:

- Documentos PDF con firma electrónica incorporada en el propio fichero .pdf y que recientemente se han constituido como el estándar ISO 32000-113 junto con el estándar PAdES14 (ETSI (TS) 102 778) que introduce características para el cumplimiento con la Directiva 1999/93/CE.
- Firmas electrónicas con formato *XML Signature (XML-DSig)/XAdES* que es un formato muy adecuado para el intercambio de información con firma electrónica entre máquinas. Se usa, por ejemplo, en el formato de factura electrónica *Facturae*. Puede contener al documento firmado (modos *enveloped* y *enveloping*) o referenciarlo mediante una URI (modo *detached*).
- Firmas electrónicas con formato PCKS#7/CMS/CAAdES que se adjuntan como fichero con una extensión .p7b, .p7c, .p7m o .p7s al documento



firmado. De modo similar a lo anterior, el documento firmado puede estar contenido o ser referenciado en el fichero de firma generado.

En la práctica esta complejidad de formatos de firma electrónica generalmente el usuario de administración electrónica no la ve directamente, serán las aplicaciones a través de las cuales se relacione con la Administración Pública las que se encarguen de ello. Recordemos el ejemplo anterior del registro electrónico que comprueba las firmas electrónicas efectuadas en la entrada al registro y las rechaza en caso de una validación fallida.

En el marco de las actividades en la administración electrónica, la necesidad de validar firmas electrónicas se da principalmente en los siguientes casos: en los documentos que el ciudadano aporte a la Administración, los documentos electrónicos emitidos por la Administración, y en los acuses de recibo emitidos por un registro electrónico.

Casi siempre estos documentos serán documentos PDF, aunque desafortunadamente aún se puede observar en algunas ocasiones la mala práctica de devolver al ciudadano directamente un acuse de recibo con firma en un formato diferente, por ejemplo, XML, difícil de usar para un usuario medio en informática, en vez de un documento PDF. No obstante, estos casos serán cada vez más residuales y los acuses de recibo que verá el ciudadano se emitirán prácticamente en su totalidad como documentos PDF, fáciles de manejar para cualquier usuario.

Para ver un ejemplo de un documento PDF emitido por una Administración Pública basta con descargarse de la Web del Boletín Oficial del Estado cualquier documento emitido a partir del año 2009, que es la fecha a partir de la cual ha empezado a funcionar el BOE electrónico que emite documentos PDF con una firma electrónica de este organismo. A continuación se puede ver como un documento del BOE, con el software Adobe Reader, está firmado electrónicamente (debe ser a partir de la versión 9).

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

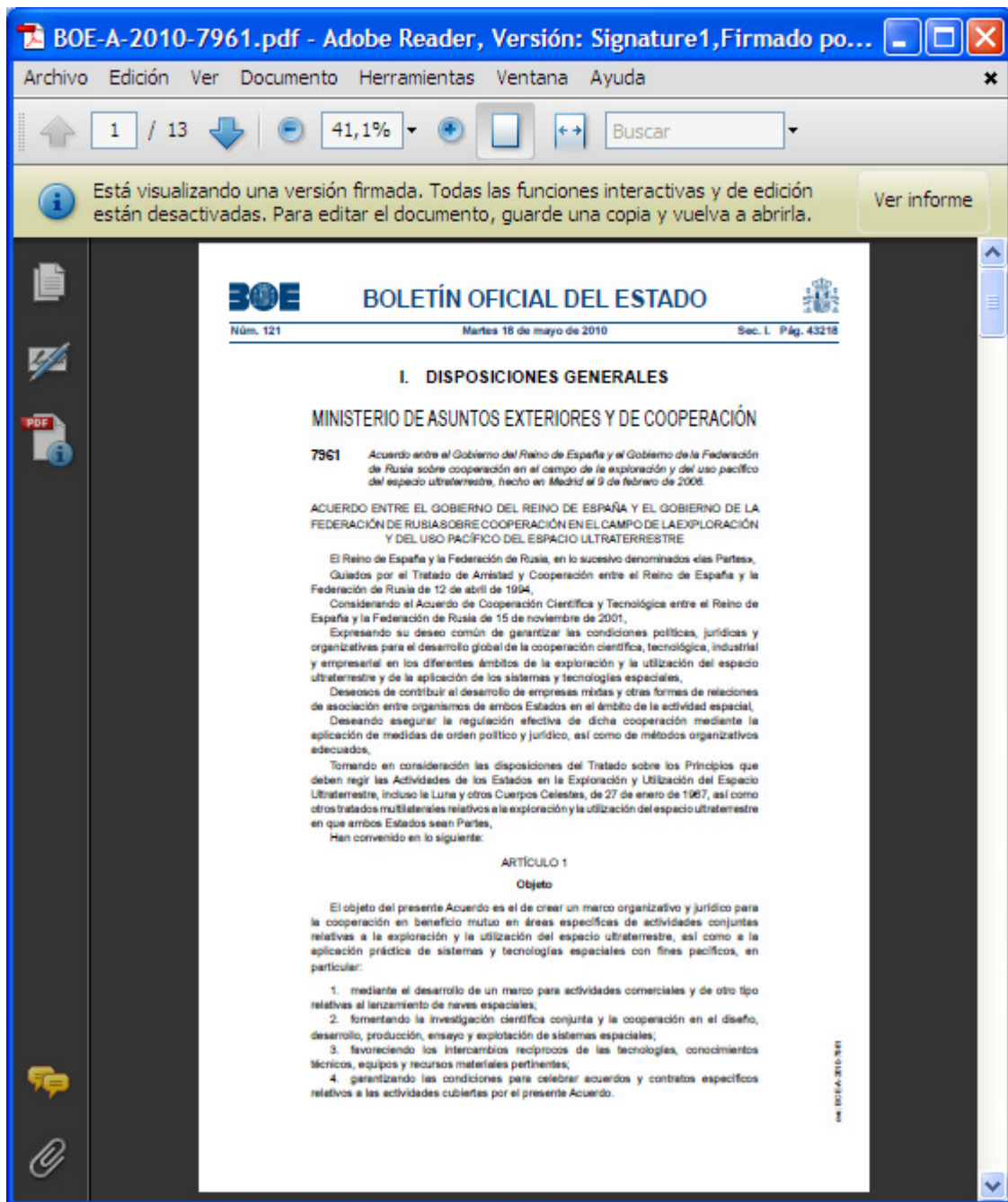


Imagen 5-8 BOE firmado electrónicamente

Validar documentos PDF firmados electrónicamente

El formato PDF se está posicionando como el estándar de facto en la Administración Pública. Cuenta con cuatro grandes ventajas:

- En primer lugar es un formato universal, con un gran soporte tanto de herramientas gratuitas como los editores *OpenOffice*, *KOffice* o el lector *Adobe Reader* como de herramientas comerciales como *Adobe Acrobat* o *Microsoft Office* que dispone de complementos que permiten guardar los documentos en formato PDF. Por otra parte es el estándar de facto en la Web para la publicación de documentos electrónicos.



- En segundo lugar se puede crear a partir de prácticamente cualquier formato: un documento Word, una hoja *Excel*, una presentación *PowerPoint*, documentos similares generados con *OpenOffice* o *KOffice*, etc.
- La tercera gran ventaja es su carácter multiplataforma, es decir, se puede usar por usuarios del sistema operativo Windows, las diferentes variantes de Linux y Unix, y por los usuarios de Mac OS.
- Finalmente cuenta con un excelente soporte integrado a la firma electrónica. A esto hay que añadir la disponibilidad de una herramienta gratuita como lo es *Adobe Reader*. Ambas cosas simplifican al usuario considerablemente el uso de documentos con firma electrónica.

Documentos PDF con sello de tiempo

Con el tiempo los ciudadanos se encontrarán en cada vez más ocasiones con documentos PDF emitidos por una Administración Pública que, además de la firma electrónica, contendrán un sello de tiempo emitido por una tercera parte de confianza, una autoridad de sellado de tiempo (*TSA – Timestamping Authority*).

El sello de tiempo, como indica su nombre, se usa en esta ocasión como evidencia electrónica que certifica y garantiza que la firma electrónica fue realizada en el momento que certifica el sello. El sello de tiempo puede actuar como evidencia electrónica para muchos propósitos diferentes, un ejemplo puede ser el uso de un sello electrónico para acreditar la fecha y hora exacta en un asiento de un registro electrónico.

Es importante resaltar aquí la distinción que hace el Real Decreto 1671/2009 de Desarrollo de la Ley 11/2007 entre el concepto de *sello de tiempo* que sería *la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento*, tal como se ha explicado arriba frente al concepto de *marca de tiempo* que sería *la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo*, es decir, la simple inclusión de la información de una fecha y hora en el documento electrónico, sin la acreditación de la misma por parte de una TSA.

Validar firmas electrónicas con formato XML Signature/Xades

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

El formato *XML Signature/XAdES* está basado en XML y no es por tanto un formato muy apto para ser manipulado directamente por usuarios finales. Como ya se ha podido ver antes, está más orientado al intercambio, procesado automático y almacenamiento a largo plazo de documentos firmados electrónicamente por las aplicaciones informáticas.

XAdES son las siglas en inglés de *XML Advanced Electronic Signatures* (firma electrónica avanzada XML) que es el estándar general utilizado en la Administración Pública española y europea, de hecho la especificación de XAdES hace referencia a que este estándar se ha diseñado teniendo en cuenta específicamente los requisitos de firma longeva y aquellos formulados en la Directiva 1999/93/CE por la que se establece un marco común para la firma electrónica en la Unión Europea. Se ha implementado como un conjunto de extensiones a las recomendaciones XML-DSig haciéndolas adecuadas para la firma electrónica avanzada

Un ejemplo de su aplicación en la Administración es el formato estándar de factura electrónica *Facturae*, el cual prevé XAdES como formato de firma.

Este estándar fue desarrollado por el W3C (*World Wide Web Consortium*), un consorcio internacional que produce estándares para la World Wide Web, dirigido por Tim Berners-Lee, el inventor de la Web.

Por sus características se está utilizando principalmente para el manejo de firma electrónica en el Back-Office de las aplicaciones de la Administración. De cara al ciudadano, se siguen utilizando en gran medida documentos PDF firmados, fundamentalmente por comodidad para éste, aunque a veces se observa la práctica de devolverle o permitirle descargar documentos con este formato. Por ejemplo, como acuse de recibo que complementa a la pantalla de la entrada de un asiento en un registro electrónico en la que se comunica al usuario que el asiento fue realizado con éxito.

No obstante, es posible que un usuario, ya sea ciudadano o funcionario, se encuentre con la necesidad de tener que validar en un momento determinado un documento con una firma electrónica en formato XML-DSig/XAdES. Entre las diferentes herramientas que se pueden utilizar en este caso cabe destacar, entre otras cosas, por su carácter gratuito la utilidad INTECOfirma que ha desarrollado el Instituto Nacional de las Tecnologías de la Comunicación (INTECO), que utiliza el estándar de firma electrónica XAdES en su versión 1.3.2.

Aparte de esto la herramienta permite validar también certificados, el usuario interesado puede comprobar, por ejemplo, la validez de los certificados de su DNle con el servicio de validación de certificados electrónicos del Ministerio del Interior que viene configurado por defecto para ello. También permite firmar documentos con el formato XAdES, esto se verá más adelante un poco más en detalle.



Validar firmas electrónicas con formato Pkcs#7/Cms/Cades

El formato de firma PKCS#7 es un formato *clásico* en la firma electrónica. CMS (siglas en inglés de *Cryptographic Message Syntax*) es el estándar IETF (Internet *Engineering Task Force*) que se basa en la sintaxis de PKCS#7, se puede utilizar para firmar digitalmente, crear códigos resumen, autenticarse o cifrar cualquier tipo de información digital.

De una manera análoga a lo que ocurre en XAdES, CAdES define un conjunto de extensiones a CMS que adaptan este estándar para que cumpla con las previsiones de la Directiva 1999/93/CE. Existen diversas herramientas para la validación de firmas de este tipo.

Validar firmas electrónicas mediante servicios online en la Web

Poco a poco empiezan a estar también disponibles servicios de validación en los sitios Web de las diferentes Administraciones Públicas. Es de esperar que conforme se vayan implantando más sedes electrónicas habrá más servicios de este tipo disponibles para ciudadanos y funcionarios.

Por otra parte, hace relativamente poco se ha puesto en marcha el servicio de validación y firma electrónica *VALIDe*. En este sitio el Ministerio de la Presidencia pone a disposición de ciudadanos y funcionarios un conjunto de utilidades avanzadas que simplifica el uso de la firma electrónica para los trámites por medios electrónicos con ciudadanos, Administración o empresas.

En este sitio se podrán realizar tareas como consultar la validez de un documento firmado electrónicamente, realizar una firma electrónica, comprobar la validez de un certificado digital emitido por cualquier entidad de servicio de certificación reconocida, etc.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación



Imagen 5-9 Servicio de validación y firma electrónica online VALIDe.

Otro ejemplo de un servicio de verificación de firma electrónica de la FNMT. El resultado de validar un certificado digital válido se muestra en la siguiente Ilustración 5-10:

CERES > Ciudadanos > Verificar estado > COMPROBAR ESTADO CERTIFICADO - Windows Internet Explorer

https://www.cert.fnmt.es/index.php?cha=cit&sec=8&fpage=1&lang=e

CERES > Ciudadanos > Verificar estado > COMPROB...

Bienvenido | Benvingut | Benvido | Ongi etorri | Welcome

Mapa | Contacto | Enlaces | Legislación | Noticias

CERES


Obtenga el **CERTIFICADO DE USUARIO CON SU DNIE**

Obtenga el **CERTIFICADO DE USUARIO**

Qué es CERES
 Ciudadanos
 Empresas
 Adm. Pública

Certificado de usuario Obtener el certificado Renovación de certificado Anulación de certificado
 Modificar datos **Verificar estado** Soporte Técnico Otros servicios
 Firma Electrónica Móvil Contacto Preguntas Frecuentes

COMPRUEBE SU PETICIÓN DE USUARIO
 COMPROBAR ESTADO CERTIFICADO


Real Casa de la Moneda
 Fábrica Nacional de Moneda y Timbre

CIUDADANOS

VERIFICAR ESTADO

COMPROBAR ESTADO CERTIFICADO

COMPROBACION DE SU CERTIFICADO

Estimado Sr/Sra. SANCHEZ.


Su certificado acaba de ser verificado. Esta usted en disposición de un Certificado Digital Valido y no Revocado.

Con este Certificado usted deberá de poder acreditarse correctamente ante los Servicios ofrecidos por entidades relacionadas con la Fabrica Nacional de Moneda y Timbre.

1.- Verifique no obstante que el NIF, Nombre y Apellidos están correctamente escritos en esta pantalla, y coinciden exactamente con su D.N.I. En caso de ser correctos y tener alguna dificultad al acceder a los Servicios ofrecidos por otras Entidades, serán ellas directamente las que podrán aconsejarle en la resolución de dichas dificultades, ya que su certificado está funcionando correctamente, según acaba de comprobar.

Identificador	Valor
INFORMACIÓN SOBRE LA IDENTIDAD (Valores Personales)	
Nombre	ANTONIO
Primer Apellido	SANCHEZ
Segundo Apellido	ROSALES
NIF	53416689V
Dirección de Correo Electrónico	
INFORMACIÓN SOBRE LAS CLAVES (Valores Técnicos)	
Numero de Serie del Certificado	
Autoridad Emisora	OU=FNMT CLASE 2 CA, O=FNMT, C=ES
Propietario	CN=NOMBRE SANCHEZ ROSALES ANTONIO - NIF 53416689V, OU=, OU=FNMT CLASE 2 CA, O=FNMT, C=ES
Comienzo de la Validez del Certificado	19 de mayo de 2010
Fin de Validez del Certificado	19 de mayo de 2013

2365225
Certificados activos a fecha: 19/05/2010
Unión Europea


MINISTERIO DE ECONOMÍA Y HACIENDA

Copyright © 2005. Reservados todos los derechos | Aviso Legal | Declaración de prácticas de certificación
ceres@fnmt.es

Internet 100%

Imagen 5-10 Verificación del certificado digital a través de la FNMT

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Validar códigos seguros de verificación que actúan como sello electrónico

En las sedes electrónicas se completará la verificación de los certificados electrónicos y firma electrónica basada en certificado con los servicios de validación de los códigos seguros de verificación. Con este tipo de servicios se puede acceder al documento original del cual se tiene una copia electrónica o en papel, tecleando el código seguro de verificación (CSV) se podrá descargar el original y cotejarlo con el propio.

Uno de los primeros organismos que ha puesto en marcha un servicio de este tipo es la Agencia Tributaria, en la siguiente ilustración se puede apreciar la pantalla que aparece al usuario cuando accede a este servicio.

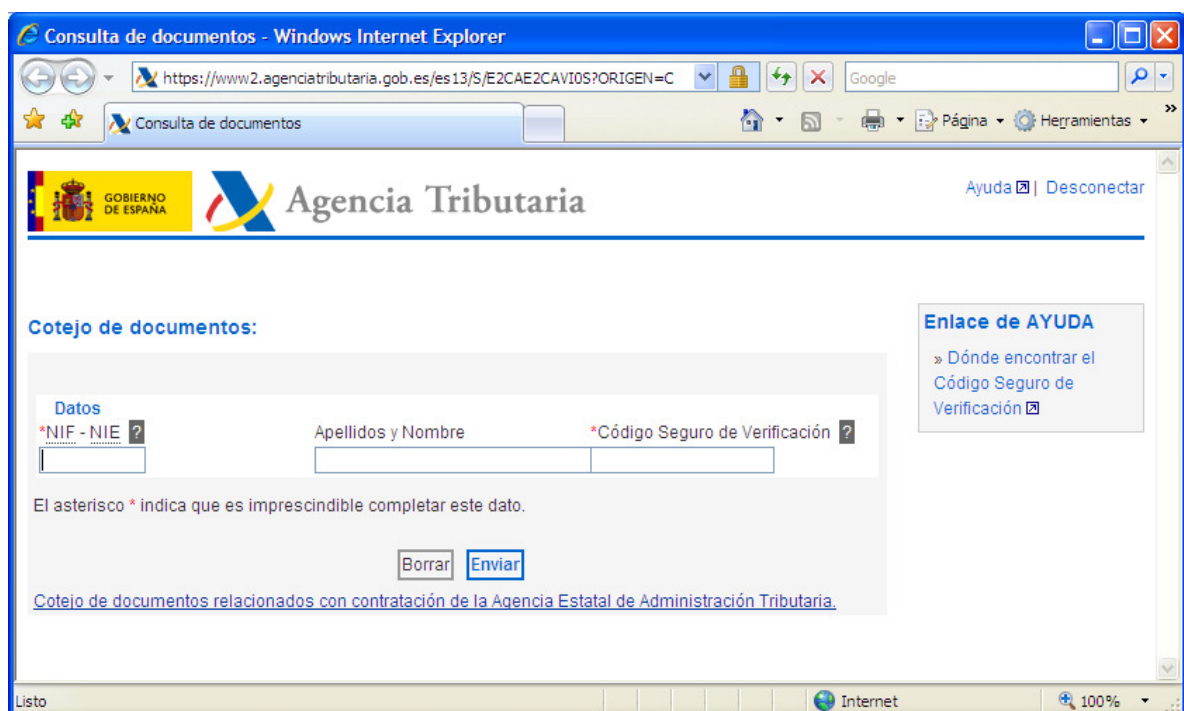


Imagen 5-11 Servicio de verificación online del código seguro de verificación de la AEAT

Firmar documentos electrónicamente

Visto el abanico de diferentes opciones de validación de documentos firmados electrónicamente y de certificados electrónicos se examinarán de un modo similar a continuación las opciones más importantes de realizar firmas electrónicas.

Al igual que la validación, la firma electrónica se debería realizar en la mayoría de los casos mediante una aplicación de gestión especializada que ya incorpora las funcionalidades necesarias para firmar y/o generar documentos con firma electrónica. El caso típico de una aplicación de este tipo sería una aplicación Web de un registro electrónico ante el cual presentar un documento

para un determinado procedimiento administrativo, por ejemplo, la declaración de la renta. Por otra parte los profesionales, los funcionarios, utilizarán a su vez aplicaciones internas en las que se harán cosas como, por ejemplo, la emisión de una resolución.

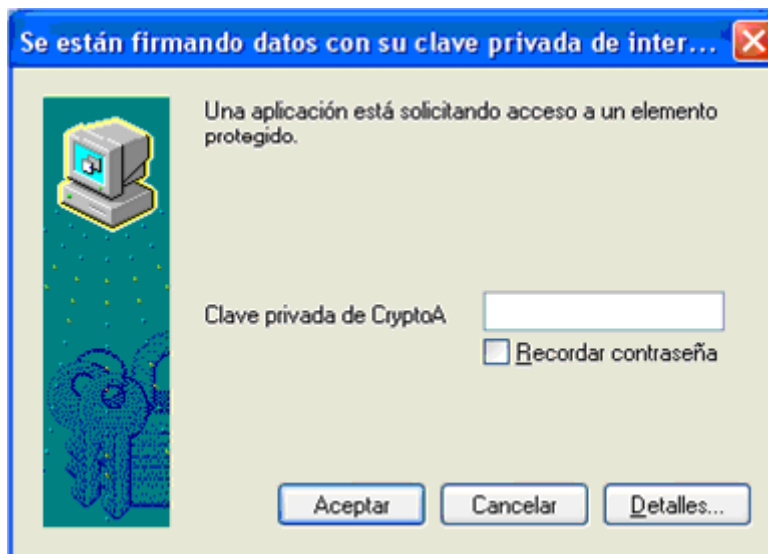


Imagen 5-12 Ventana emergente al firmar un documento, solicitando la clave privada.

No obstante, también aquí a veces habrá casos en los que será necesario crear una firma electrónica en un documento de una manera *manual*, es decir, no usando una aplicación de gestión especializada. Se proponen, por tanto, a continuación una serie de herramientas que pueden ser las adecuadas para esta situación.

Firmar documentos PDF

Por las razones ya anteriormente comentadas, el formato PDF es un formato sumamente adecuado para intercambiar documentos electrónicos entre usuarios. En el caso de la firma electrónica destacada además la posibilidad de crear un documento PDF a partir de prácticamente cualquier tipo/formato de documento, lo que permite, por ejemplo, convertir una presentación PowerPoint en un documento PDF y firmarlo electrónicamente.

Para poder crear y firmar electrónicamente documentos PDF a partir de cualquier tipo de documento en general será por tanto necesario o bien adquirir la versión profesional (*Adobe Acrobat*) que no es gratuita, o bien utilizar alguna herramienta alternativa a la de Adobe que puede ser también comercial o gratuita como lo es el caso, por ejemplo, de *PDFCreator* que ya soporta firma electrónica, cifrado y generación de documentos PDF en formato PDF/A para el archivo a largo plazo de los mismos.

La firma electrónica con este tipo de herramientas es muy sencilla. Además según el producto en cuestión pueden ofrecer opciones adicionales. Adobe

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Acrobat, por ejemplo, ofrece la posibilidad de generar un gráfico configurable, similar a la rúbrica de una firma manuscrita, que permite insertar en el lugar del documento que el usuario quiera.

Ejemplo PDF firmable.pdf - Adobe Reader

Archivo Edición Ver Documento Herramientas Ventana Ayuda

1 / 2 68,1% Firmar Buscar

Por favor, rellene el siguiente formulario. Puede guardar los datos escritos en este formulario. Resaltar campos

Datos Generales

D./Dña. con D.N.I. n.º en concepto de Solicitante

comparece en representación de con N.I.F. n.º

y con domicilio social en Localidad

Provincia **Ávila** domiciliada a efectos de notificación en:

Localidad Provincia **Ávila** Código Postal Teléfono

Fax Correo electrónico

Datos Bancarios

Titular Banco o Caja

Agencia Domicilio

Localidad Número de Cuenta

EXPONE:

Que desea solicitar la subvención convocada por la CONSEJERÍA DE ECONOMÍA Y EMPLEO:

(1)	Programa	Cuantía solicitada
	II	Revitalización comercial

(1) Indicar el número de proyectos para los que se solicita ayuda

DOCUMENTACIÓN QUE SE APORTA:

Cuando no sean Entidades Locales	En su caso, expediente en el que se encuentra
CIF de la entidad	
DNI del representante	
Acreditación de la representación	
Escritura o Acta, y Estatutos	
Certificado de la entidad financiera	
Memoria individualizada de cada feria o certamen solicitado	
Otros	

Para Entidades Locales

DNI del representante

Imagen 5-13 Formato PDF preparado para firmar

Firmar formularios PDF

Una alternativa a los formularios Web para generar documentos estructurados son los formularios PDF. En ese sentido los ciudadanos se encontrarán en más de una ocasión Administraciones Públicas que en vez de utilizar formularios Web en sus trámites utilicen este tipo de formularios.

A diferencia de los documentos PDF convencionales que no sean formularios este tipo de formularios pueden ser firmados con la herramienta gratuita *Adobe Reader* si han sido convenientemente preparados para ello. Naturalmente también es posible utilizar otros lectores de documentos PDF alternativos que soporten el uso de formularios y firma electrónica.

En la Ilustración 5-13 y la Ilustración 5-14 se puede apreciar el proceso de cumplimentación del formulario y su firma con el lector *Adobe Reader* y su resultado del proceso. Obsérvese que también en este ejemplo se ha utilizado un gráfico de rúbrica de firma.

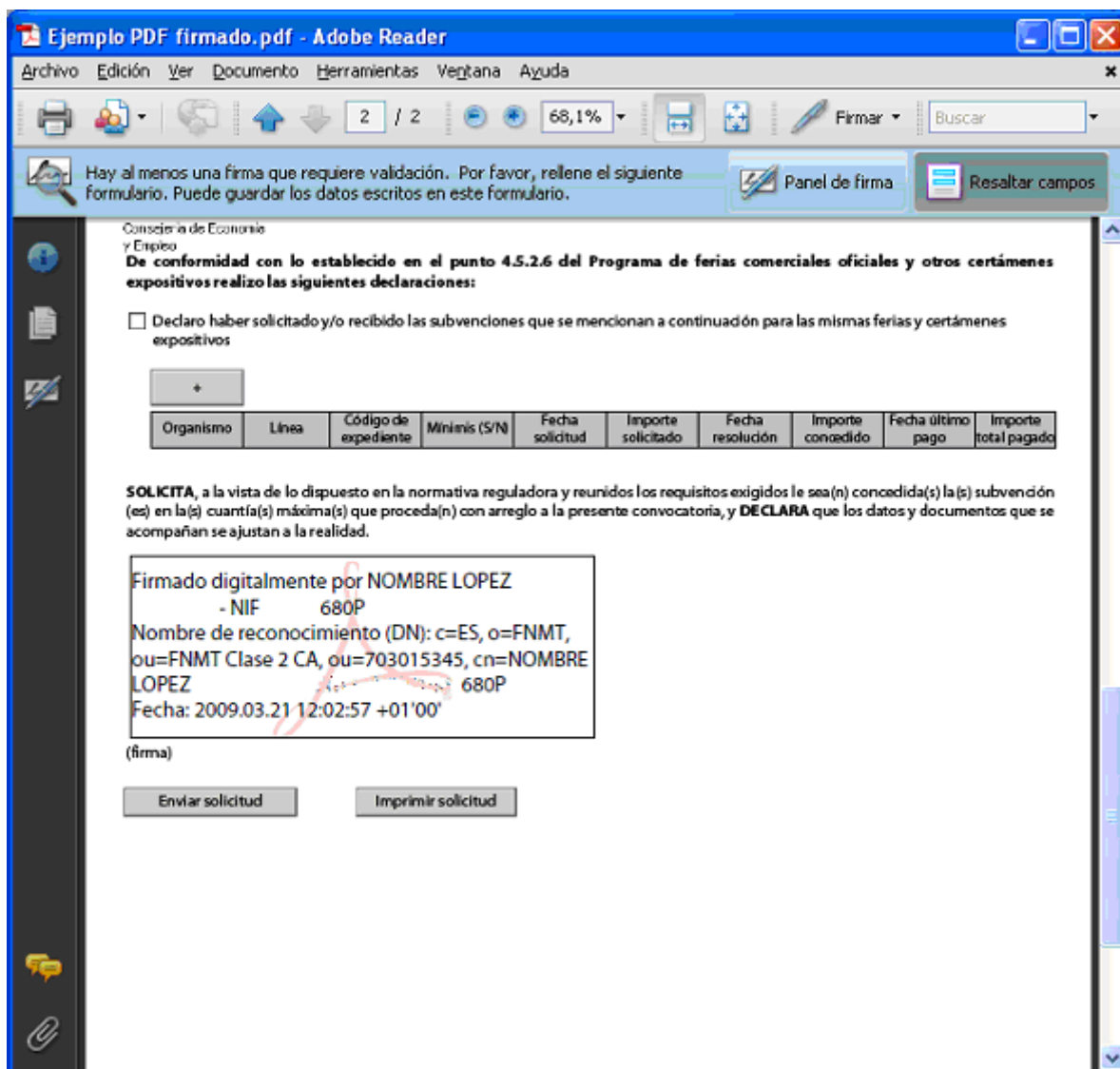


Imagen 5-14 PDF firmado

Firmar de documentos Microsoft Word

Anteriormente se ha explicado cómo cuando se inicia algún trámite por la vía electrónica, se completa un formulario y finalmente se firma y envía. En otras ocasiones será necesario firmar documentos directamente en el equipo del usuario. En este caso hay diferentes opciones que se detallan a continuación.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

El mismo editor del documento incorpora el soporte necesario para firmar un documento, en este caso se puede añadir una firma digital a través del Menú Herramientas/Opciones/Pestaña Seguridad (versión Word 2003). Una vez ahí pulsando el botón de “Firmas digitales...” aparece el cuadro de diálogo que se muestra debajo de estas líneas.

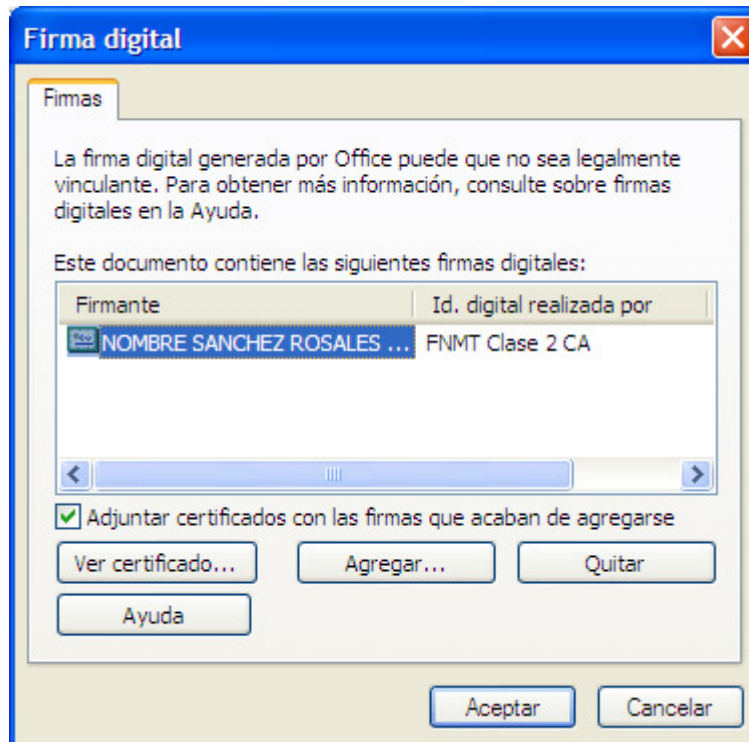


Imagen 5-15 Cuadro de diálogo que muestra Word 2003 para insertar una firma digital

Una vez firmado el documento se podrá reconocer por el icono rojo con forma de sello que aparece en la barra de estado en la parte inferior de la ventana de Word.

Lo que es muy importante a tener en cuenta es que Word, con cualquier edición del documento volverá a eliminar la firma digital (previa advertencia al usuario), ya que al modificar el documento la firma digital deja de ser válida (se ha violado la integridad del documento firmado).

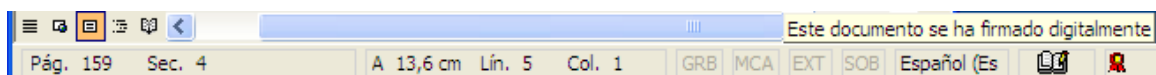


Imagen 5-16 Documento firmado en Word

Firmar con formato XML Signature/Xades



Por las razones ya comentadas sobre validación de firma electrónica y certificados hoy por hoy sería extremadamente raro que un usuario final se vea ante la necesidad de realizar una firma en formato XML-DSig y/o XAdES. Sin embargo, la herramienta INTECOFirma, no solamente permite validar documentos con este formato de firma, sino realizar firmas electrónicas con este formato.

Esta opción es menos cómoda que la gestión de la firma desde el propio editor del documento, pero tiene la ventaja de ser totalmente independiente de un producto concreto como Microsoft Word o Acrobat y utilizar estándares de firma digital de modo que los ficheros de firma creados serán intercambiables entre diferentes aplicaciones.

Por otra parte, sin embargo, cabe esperar que el uso de XAdES se extienda más hacia los usuarios finales a medida de que los editores y lectores de documentos electrónicos soporten este estándar. En el caso del Office 2010, por ejemplo, ya se ha anunciado la integración de XAdES para firma electrónica²². De modo que a medio plazo quizás adquiera un nivel de uso similar o incluso superior a los documentos PDF con firma electrónica en los usuarios finales.

Firmar con formato PKCS#7/CMS/CADES

El caso de tener que firmar un documento electrónico con un formato de firma PKCS#7, CMS o CADES en la práctica será también una auténtica rareza y a diferencia de lo que ocurre con XAdES no cabe pensar que esta situación cambie a medio plazo. En este caso existen algunas herramientas que permiten realizar una firma con este tipo de formato.

Un ejemplo de una herramienta instalable en el ordenador es Dfirma Desktop de CamerFirma. También existen herramientas online como lo es, por ejemplo, la herramienta Web de Xólido.

A continuación se muestra un ejemplo del contrato de una entidad certificadora como Camerfirma, concretamente como entidad certificadora de las Cámaras de Comercio, por su ámbito internacional cumple con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación



Imagen 5-17 Contrato de entidad certificadora

Enviar un correo electrónico con firma

Igual que ocurre para otros usos de la firma y el cifrado no hay una manera única de enviar un mensaje de correo firmado electrónicamente, sin embargo, los fundamentos técnicos que se han ido repasando en este manual son los mismos.

Por tanto, una vez bien asentados y con un poco de práctica, debería ser razonablemente fácil hacerse con el manejo de cualquier programa de correo electrónico que permita el uso de firmas digitales. Por su gran extensión, se repasará un ejemplo concreto del uso de la firma electrónica en Outlook 2003.

En primer lugar hay que asignar el certificado a su cuenta de E-mail:

1. Con Microsoft Outlook abierto se escoge del menú Herramientas, Opciones. Saldrá el cuadro de diálogo “Opciones”.
2. En la ventana de Opciones que se abre a continuación, se selecciona la pestaña Seguridad.
3. Presionar el botón de “Configuración...”. Aparece el cuadro de diálogo hijo del anterior recuadro “Cambiar la configuración de seguridad” que se aprecia en la ilustración. Presionar primero sobre el botón “Elegir...” que está al lado del campo “Certificado de firma”, y en la ventana que se abre escoger el certificado personal que se desee utilizar de la lista que se despliega. Luego realizar lo mismo con el campo “Preferencias de cifrado”.
4. Presione sobre el botón de Aceptar. En el cuadro de diálogo “Opciones”, coloque una marca sobre “Agregar firma digital a los mensajes salientes” y pulse el botón de Aceptar.

Si se ha marcado la opción de firma comentada, el botón de la izquierda se encontrará pulsado por defecto, si para un mensaje concreto no quiere firma basta con pulsarlo para deshabilitar esta opción.

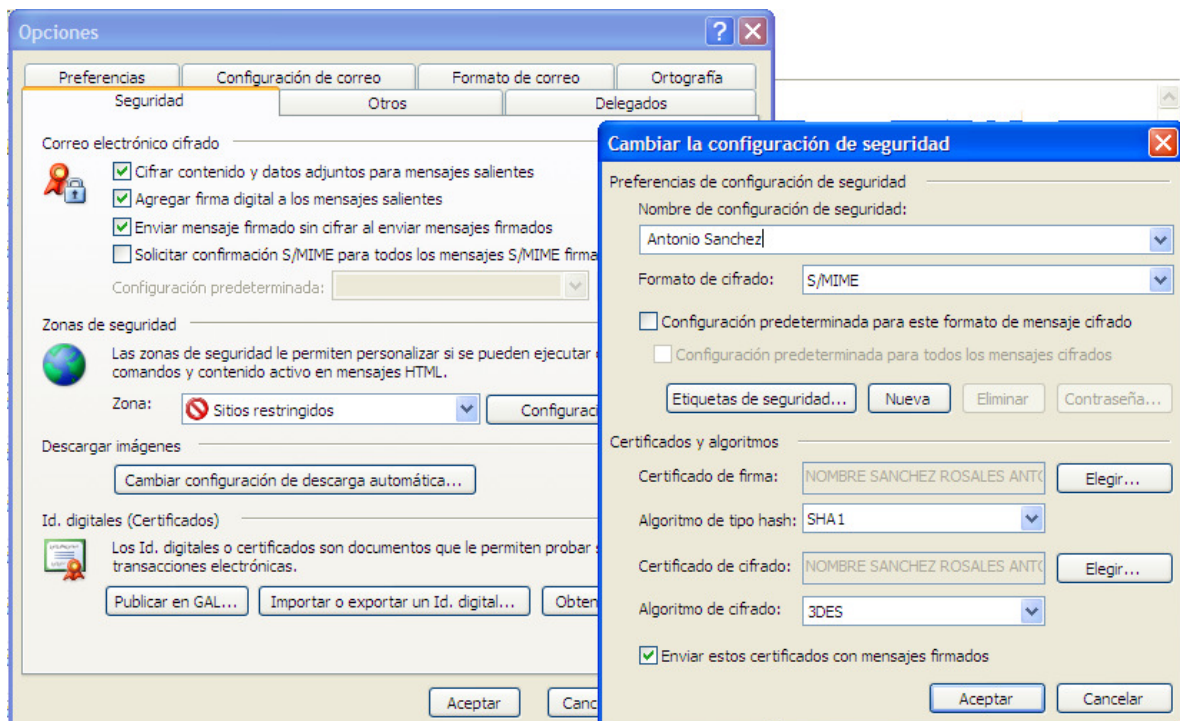


Imagen 5-18 Configuración firma digital en Outlook 2003

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Para firmar un mensaje de correo electrónico y permitir que su identidad sea verificable, solo tiene que enviarlo de la manera habitual, Microsoft Outlook firmará sus mensajes automáticamente. De todos modos en la barra de herramientas de la ventana de edición del mensaje encontrará los botones siguientes:



Imagen 5-19 Botones para enviar emails certificados en Outlook 2003

Para ello es necesario rellenar un formulario inicial con los datos del usuario en cuestión, algunas veces incluso pide adjuntar información, y una vez completado todo se firma y se envía.

Firma electrónica en formularios Web

Sin duda, una de los aspectos más útiles y productivos de la Administración electrónica para el ciudadano es la posibilidad de poder iniciar y completar trámites completamente online ahorrando así desplazamientos engorrosos, paciencia y ausencias en el trabajo.

Adjuntar ficheros

Los ficheros se adjuntan como en cualquier otra aplicación, pero tienen su problemática peculiar desde un punto de vista legal, ya que en algunos casos se pueden requerir documentos adjuntos (certificados, etc.) que deban estar firmados.

Para poder usarse estos documentos deberán ser emitidos por tanto de manera electrónica y constar de una firma electrónica válida según las condiciones que se especifiquen en la sede del órgano al que el ciudadano se está dirigiendo, es decir, normalmente una firma avanzada basada en un certificado X.509.

Otra vía puede ser el concepto de copia electrónica que introduce la Ley 11/2007 y que permite también efectuar compulsas electrónicas. Pero en este caso ya se rompe la comodidad de cadena electrónica completa y sería necesario un desplazamiento a una oficina física para realizar la copia en cuyo caso ya se pierde en gran medida el beneficio de la vía telemática.

En cualquier caso, en la mayoría de los casos no se producirá esta situación y aquellos en los que se produce irán disminuyendo en el tiempo conforme se avanza en la implantación de la Administración Electrónica.



En la ilustración siguiente se puede apreciar como un usuario ficticio ha rellenado algunos de los campos obligatorios, otros aún quedan por rellenar. Generalmente los formularios marcan de manera gráfica los campos obligatorios (en este caso están marcados con un asterisco) y comprueban antes del envío que el usuario los ha rellenado correctamente.

Se puede apreciar además que el usuario ha adjuntado un fichero como documento anexo, en este caso el trámite en cuestión no requiere expresamente documentos adjuntos con firmado, sino que simplemente se ofrece de una manera abierta que el usuario adjunte documentación que crea relevante para el recurso, algunos de estos documentos pueden estar firmados.

Por ejemplo: si se está recurriendo una denegación de una solicitud fuera de plazo se podría adjuntar el acuse de recibo electrónico emitido originalmente por el registro en el caso de haber cursado la solicitud por la vía telemática.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Ministerio de Sanidad y Consumo. Instituto de salud Carlos III - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

MINISTERIO DE SANIDAD Y CONSUMO

Instituto de Salud Carlos III

Reclamaciones previas a la vía judicial laboral

(*) Campos de cumplimentación obligatoria

1.- DATOS DEL INTERESADO

Nombre: PEPITO (*)

Primer Apellido: LOPEZ (*)

Segundo Apellido: LOPEZ

DNI/NIF/Pasaporte: 11111111P (*)

2.- DATOS DEL REPRESENTANTE

A rellenar en caso de representación del interesado. Adjuntar poder electrónico de representación como fichero anexo.

Nombre Representante:

DNI/NIF/Pasaporte:

3.- LUGAR O MEDIO A EFECTOS DE NOTIFICACIÓN

Indicar su preferencia a efectos de notificación:

Preferencia de notificación: Dirección Postal Correo Electrónico Fax

País: España (*)

Provincia: - selecciona - (*)

Municipio: (*)

Calle: (*)

Código Postal: (*)

Teléfono: (*)

Correo Electrónico: (*)

Fax: (*)

4.- ACTO OBJETO DE REVISIÓN

Acto a Revisar: Resolución XXX (*)

Expone: Mi exposición... (*)

Solicita: Mi solicitud. . (*)

Órgano al que se dirige:

5.- FICHEROS ANEXOS

Plan Curso eAdmin.odt

Añadir Eliminar

Examinar...

Firmar y enviar

Terminado registroelectronico.isciii.es [ningún diccionario activo]

Imagen 5-20 Ejemplo de trámite on-line

Firmar un formulario

Una vez completados los datos del formulario el usuario ha de firmarlo y enviarlo. En este momento el navegador presentará la lista de certificados de



los que dispone el usuario (si tiene más de uno instalado) y preguntará por el PIN28 asociado a la clave privada para firmar.

Un caso algo peculiar que actualmente se presenta hoy por hoy muy pocas veces, pero que en el futuro conforme más empresas y todo tipo de organizaciones se adhieran a la Administración Electrónica será más frecuente, es el uso de múltiples firmas. Puede ser el caso, por ejemplo, en solicitudes de ayudas para proyectos de I+D donde ha de firmar todo el equipo científico del proyecto.

En este caso no basta con simples formularios, sino que las aplicaciones han de prever mecanismos más sofisticados como, por ejemplo, una carpeta o presolicitud para los solicitantes donde cada uno de ellos pueda realizar su firma en diferentes momentos antes del envío definitivo, ya que si se trata de muchas personas en la práctica será inviable reunirlos todos para firmar en el mismo momento, aparte de ser impracticable hacerlo sobre el mismo formulario (todos tendrían que tener instalado su certificado en la máquina en cuestión).

También es peculiar la problemática para los responsables tanto públicos como del sector privado. Estas personas tienen muy poco tiempo disponible y han de firmar a veces decenas de documentos que otra persona les ha preparado previamente en un portafirmas.

En este sentido actualmente ya se están usando portafirmas electrónicos para la gestión de expedientes electrónicos. Así, este tipo de personas no tienen que entrar en cada uno de los expedientes y/o aplicaciones de gestión correspondientes, sino que disponen de una aplicación Web aparte que actúa como un portafirmas convencional, es decir, presenta una lista con todos los documentos a firmar, que posiblemente otra persona haya preparado previamente. De este modo se traslada la comodidad y efectividad del portafirmas tradicional también al mundo de la Administración Electrónica.

Acuse de recibo

Siempre que se envía un formulario, al igual que en un trámite en papel, entrará en un registro electrónico y éste ha de expedir un acuse de recibo. Según el artículo 25 de la Ley 11/2007 este acuse de recibo debe consistir en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

Trabajar con documentos confidenciales

Cifrar Documentos

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

A veces es necesario mantener la confidencialidad de un documento o fichero por contener información sensible, independientemente de que este fichero se encuentre o no firmado electrónicamente.

Un ejemplo muy común puede ser un fichero con diferentes claves de acceso personales, para acceder a determinados sitios Web, aplicaciones en la oficina del trabajo, etc.

Obviamente esto es una muy mala práctica, especialmente cuando hay alternativas muy buenas para manejar este tipo de información, y hacerlo además muy cómodamente.

El estándar de criptografía más importante en este sentido es AES (*Advanced Encryption Standard*) basado en el algoritmo de cifrado Rijndael, y es el sucesor al mítico DES (*Data Encryption Standard*), ambos fueron adoptados como estándares federales por el Gobierno de EEUU y se convirtieron a partir de ahí en los estándares de referencia en todo el mundo.

Afortunadamente existen muchas herramientas de buena calidad, libres y open source para el cifrado con AES, muy útiles para cualquier usuario, profesional o doméstico. Una de ellas, con un enfoque general es *AxCrypt*, tiene como ventaja particular que al integrarse con el explorador de Windows resulta especialmente cómoda y rápida de usar. Así con hacer un click de ratón se tiene cifrado el fichero con los datos. A partir de aquí la herramienta pedirá una clave para el cifrado que usará para aplicar el algoritmo de cifrado AES al fichero. Una vez cifrado se podrá descifrar de manera similar con un click del botón derecho del ratón, y ya podemos tener perfectamente protegida la información sensible.

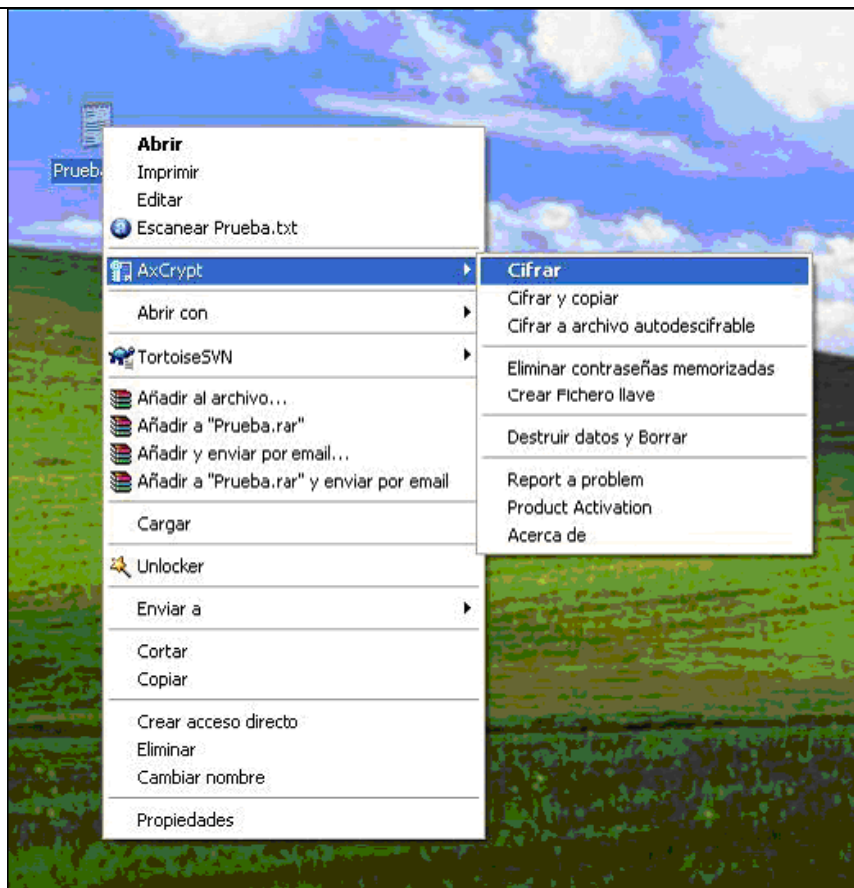


Imagen 5-21 Cifrado de un fichero con AxCrypt

Por otra parte existen aplicaciones más especializadas que implementan un almacén de llaves para mantener todo tipo de claves de acceso e información en un único sitio y bien protegida con una clave maestra para acceder a este almacén.

El uso de este tipo de herramientas no es solamente algo muy conveniente, sino que en muchos casos será una cuestión sensible, incluso muy sensible desde un punto de vista jurídico.

Un ejemplo muy claro es la problemática en torno a los datos personales, regulada fundamentalmente en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007 que la desarrolla y establece medidas muy concretas para los ficheros informáticos.

Así, por ejemplo, el Real Decreto establece una serie de medidas de seguridad en las cuales indican que para los datos personales altamente sensibles tales como datos de salud, afiliación sindical, religión, creencias, etc., entre las cuales se recomienda almacenarlos cifrados si los datos están almacenados en disco, dentro de las instalaciones. Si se almacenasen en dispositivos de salida o portátiles estarían obligados a almacenar los datos cifrados y la LOPD prevé sanciones en caso de incumplimiento.

Enviar un correo electrónico cifrado

Al cifrar un mensaje de correo electrónico el remitente se asegura de que sólo el destinatario del mismo pueda ver y leer su contenido, incluyendo el de los archivos adjuntos. Para cifrar un mensaje de correo electrónico se debe disponer de la clave pública del destinatario del mensaje.

Para ello hay diferentes posibilidades, una es recibir la clave pública (se repite en cierto modo) llave pública de un emisor en particular cuando éste le envía un mensaje de correo electrónico digitalmente. Otra es dar de alta el fichero del certificado en los contactos de Outlook si se dispone de él.

En general si se quiere cifrar por defecto se puede proceder a marcar la opción de cifrar el contenido en las opciones generales, vista en el apartado de firma de un mensaje. No obstante, si bien esta opción puede ser conveniente para la firma electrónica será raro que la mayoría de los mensajes se envíen cifrados, por tanto, en este caso conviene por lo general dejar esta opción deshabilitada y habilitar la opción de cifrado de manera individual por cada mensaje.

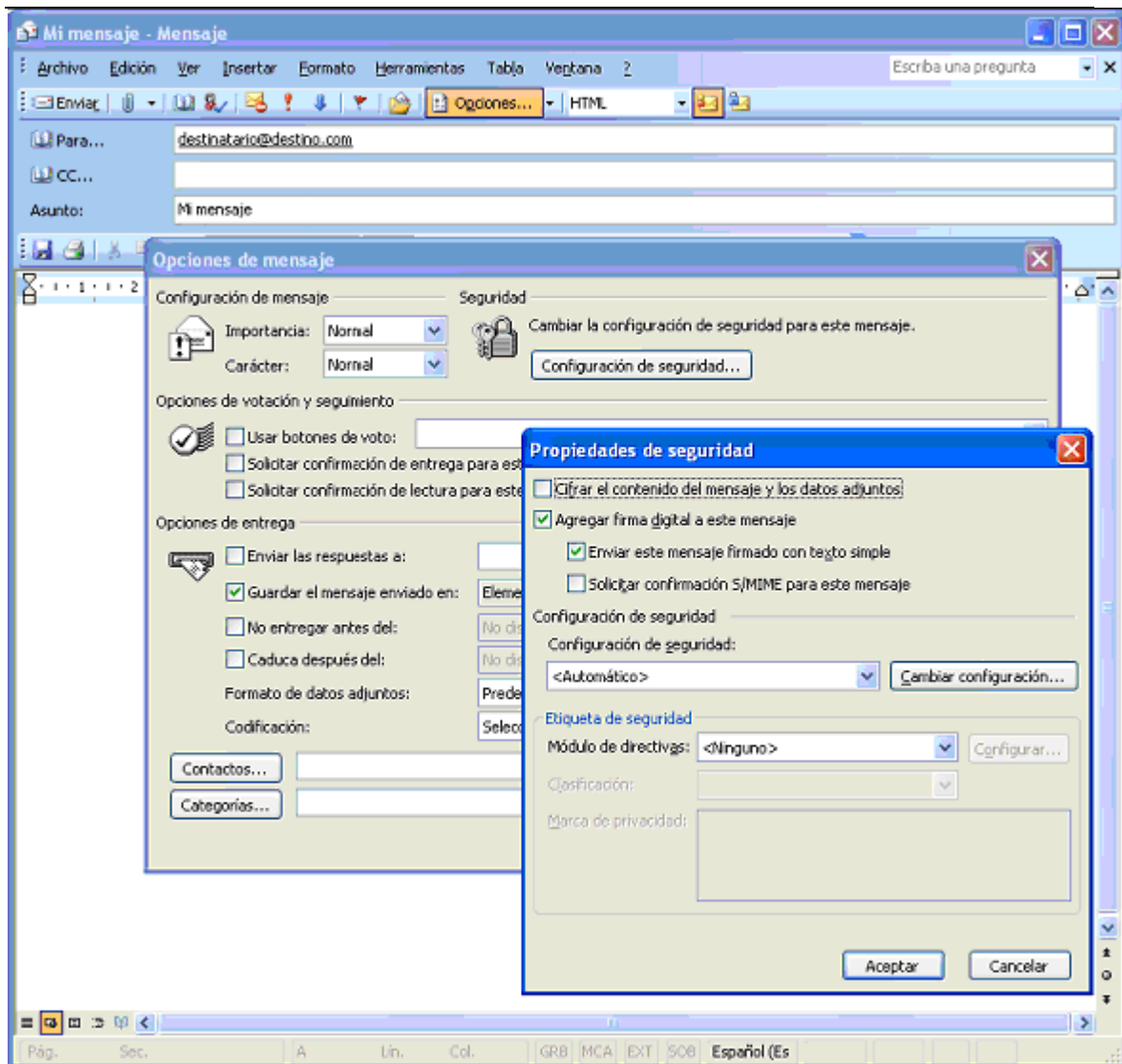


Imagen 5-22 Configuración en Outlook 2003 para enviar correo cifrado

5.3.2 Problemas típicos

En el acceso a los servicios de Administración electrónica y a sitios que usen certificados en general se pueden presentar diversos problemas, algunos se pueden confundir además entre sí. Desgranaremos aquí algunos de los patrones de problema más importantes.

Mensajes desconcertantes

Uno de los grandes problemas que aún persisten actualmente en la administración electrónica y en el uso de la firma digital desde un navegador Web es que no existe una funcionalidad estandarizada entre navegadores para poder realizar las firmas.

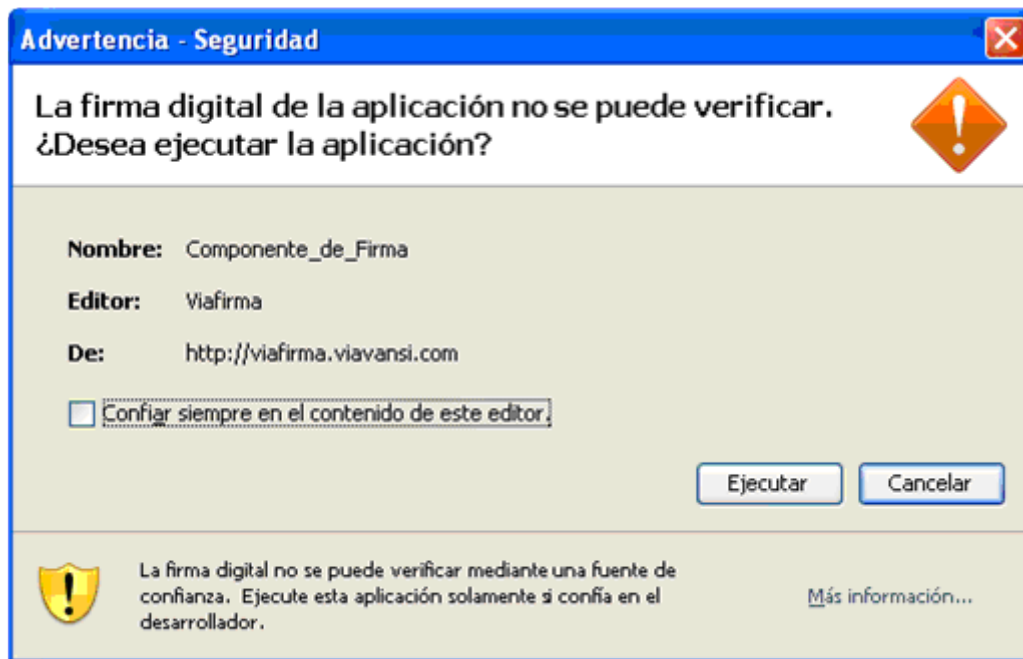


Imagen 5-23 Mensaje para la instalación de una firma digital en el navegador.

Como esta funcionalidad no existe por defecto en el navegador ha de ser implementada por el sitio Web. La manera habitual de hacerlo es mediante un componente de firma digital que el navegador descarga del sitio y esto resulta ser bastantes veces una fuente de problemas y desconcierto para los usuarios ya que, por motivos relacionados con la seguridad del usuario, los navegadores, según estén configurados, suelen poner sus pegas a este proceso de descarga e instalación del componente de firma.

Por si fuera poco existen además dos tecnologías diferentes para la implementación de estos componentes, cada una con sus requisitos específicos:

- Los *Applets* implementados en el lenguaje de programación Java, un estándar abierto.
- Los componentes *ActiveX*, una tecnología propietaria de Microsoft.

Estos componentes son en definitiva pequeños programas que se instalan en el navegador y pueden realizar todo tipo de funciones que complementan la funcionalidad de las páginas Web, como lo es precisamente firmar electrónicamente documentos.

En el caso de los *Applets* el requisito fundamental es disponer una máquina virtual Java instalada. Según el caso, en algunas ocasiones el sitio Web detecta que el usuario no dispone de ella y permite su instalación sobre la marcha y en otros se remite al usuario a su descarga e instalación manual. La gran ventaja de Java es que se trata de una tecnología multiplataforma que funciona con prácticamente todos los navegadores y todos los sistemas operativos.



Superado este escollo de los requisitos para poder ejecutar este tipo de componentes según el sistema concreto del usuario y su configuración particular su navegador pondrá más o menos pegas a la instalación de los componentes de firma.

Uso de un certificado que ha caducado

Este es un problema que se puede dar muy fácilmente, ya que la Ley 59/2003 de firma electrónica limita la vigencia de un certificado electrónico a un máximo de 4 años, de modo que después de este periodo el usuario ha de renovar el certificado para poder continuar usándolo tanto para los servicios de Administración Electrónica como para servicios en el sector privado.

Por tanto no es extraño que a un usuario se le pase la renovación aunque el proveedor de servicios suele avisar a los usuarios por correo electrónico u otros medios con bastante antelación.

En este caso generalmente el sitio Web al que estamos accediendo deberá estar preparado para diagnosticar este problema y reportarlo correctamente al usuario. El mensaje concreto y comportamiento depende del sitio Web concreto, por tanto debería avisar al usuario con un mensaje que especifique claramente que éste ha intentado acceder con un certificado caducado. Pero si la Web accedida no se ha implementado con cuidado puede mostrar mensajes de errores genéricos con el certificado confundiendo con ello al usuario, diciendo, por ejemplo, que el usuario no posee un certificado válido o que no se reconoce su certificado cuando en realidad el problema es que está, a pesar de ser perfectamente válido, caducado. Por otra parte, por si esto fuera poco, el comportamiento concreto depende también del almacén de certificados.

Ante cualquier anomalía, con respecto al certificado de usuario, que ocurra al intentar acceder a una Web que lo requiera es recomendable comprobar que éste se encuentra en el almacén que corresponde y que sigue estando en fecha.

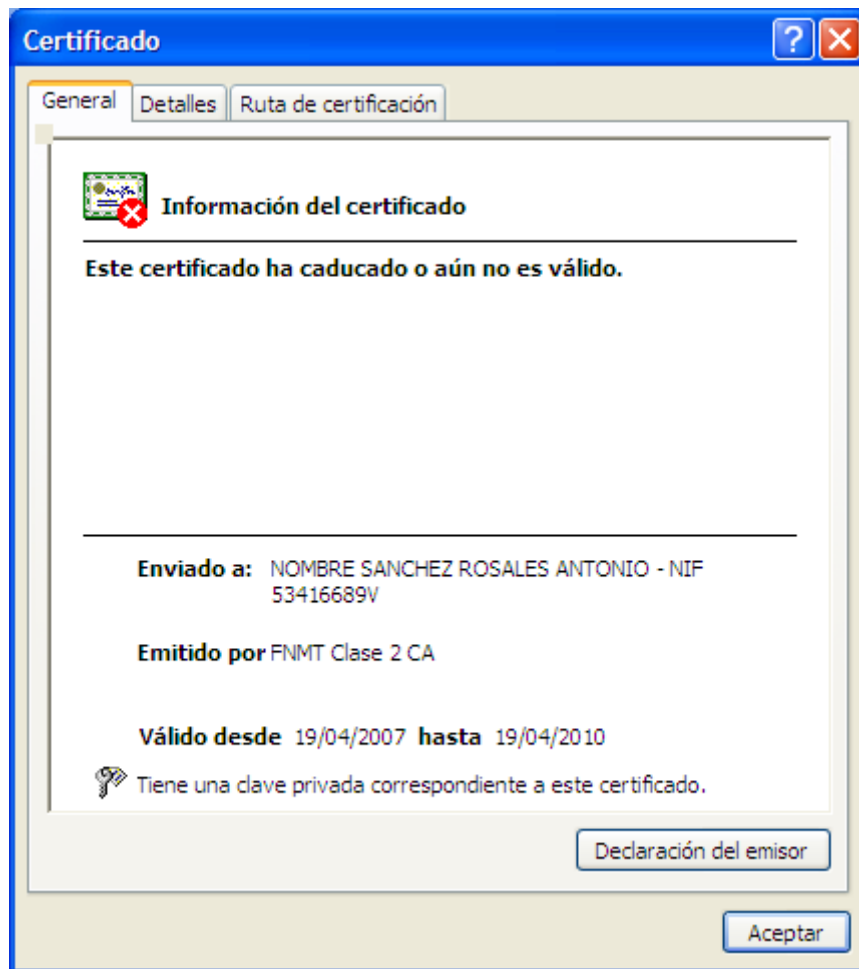


Imagen 5-24 Certificado digital caducado

El Navegador no reconoce el certificado

Algunas veces puede suceder que al acceder a algún sitio Web este sitio utilice un certificado que el navegador no reconoce. Que ocurra esto depende fundamentalmente de dos factores:

- Los certificados que el navegador tenga instalados por defecto.
- Lo conocido y relevante que sea el sitio al que se está accediendo.

Los sitios que usan este tipo de certificados lo hacen fundamentalmente con el propósito de que el usuario pueda confiar en su identidad. Así en el caso de la banca, venta por Internet o la Administración, por ejemplo, el usuario puede estar tranquilo de poder intercambiar de manera segura información sensible o realizar transacciones económicas.

Por otra parte si el sitio utiliza además una conexión cifrada HTTPS sabrá que la información intercambiada, incluso en el caso que un tercero la interceptase, está completamente protegida, ya que al estar convenientemente cifrada al tercero en cuestión le resultaría completamente inservible.

Cuando se produce por alguno de estos motivos un error de reconocimiento del certificado de la Web en cuestión el navegador avisará de ello y algunas veces incluso aconsejará no entrar en el sitio. Según el fabricante, los navegadores pueden ofrecer también mecanismos específicos de tratar el problema de los sitios cuyo certificado no se reconoce.

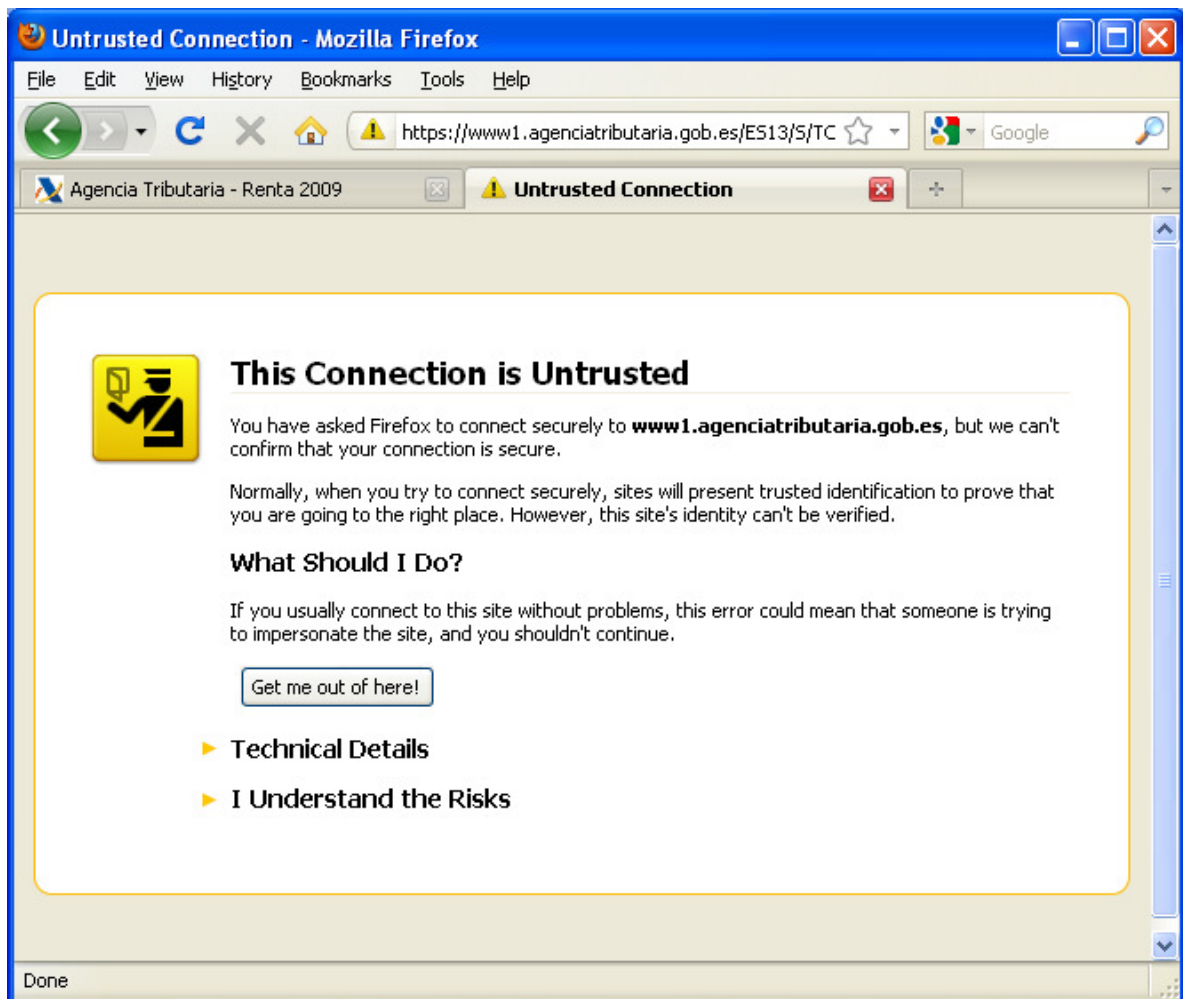


Imagen 5-25 Ejemplo de acceso no reconocido por el navegador Mozilla Firefox

La creciente concienciación sobre la importancia de la seguridad en Internet ha hecho que los fabricantes hayan hecho las versiones recientes de sus navegadores muy sensibles a estos casos. Así las últimas versiones suelen dar mensajes con un aspecto bastante alarmante, como en la vista de la imagen anterior donde antes ni siquiera avisaban asustando incluso en bastantes ocasiones al usuario cuando en realidad el problema detectado no es en realidad tan crítico. En estos casos, simplemente conviene detenerse y leer con tranquilidad las diferentes opciones que el navegador ofrece para escoger la adecuada en ese momento.

Se puede concluir para estos casos que si se da la situación y se trata de un sitio al que se prevé acceder con cierta frecuencia merece la pena descargarse

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

su certificado e instalarlo. En general estos sitios ofrecerán sus certificados para su descarga en su Web. En cualquier caso hay que asegurarse de tener la absoluta certeza de que se está accediendo al sitio deseado (que su URL, la dirección que aparece en el navegador) es la correcta.

De lo contrario hay que actuar teniendo en cuenta que se trata de un sitio cuya identidad se desconoce, es decir, no se puede confiar en él y por tanto no se debe intercambiar información sensible con él.

El usuario no dispone de un certificado digital

Este caso es relativamente fácil de identificar, ya que al usuario se le mostrará el aviso pertinente. No obstante, como se ha mencionado anteriormente, puede ser que en realidad el usuario sí disponga del certificado pero este haya caducado.

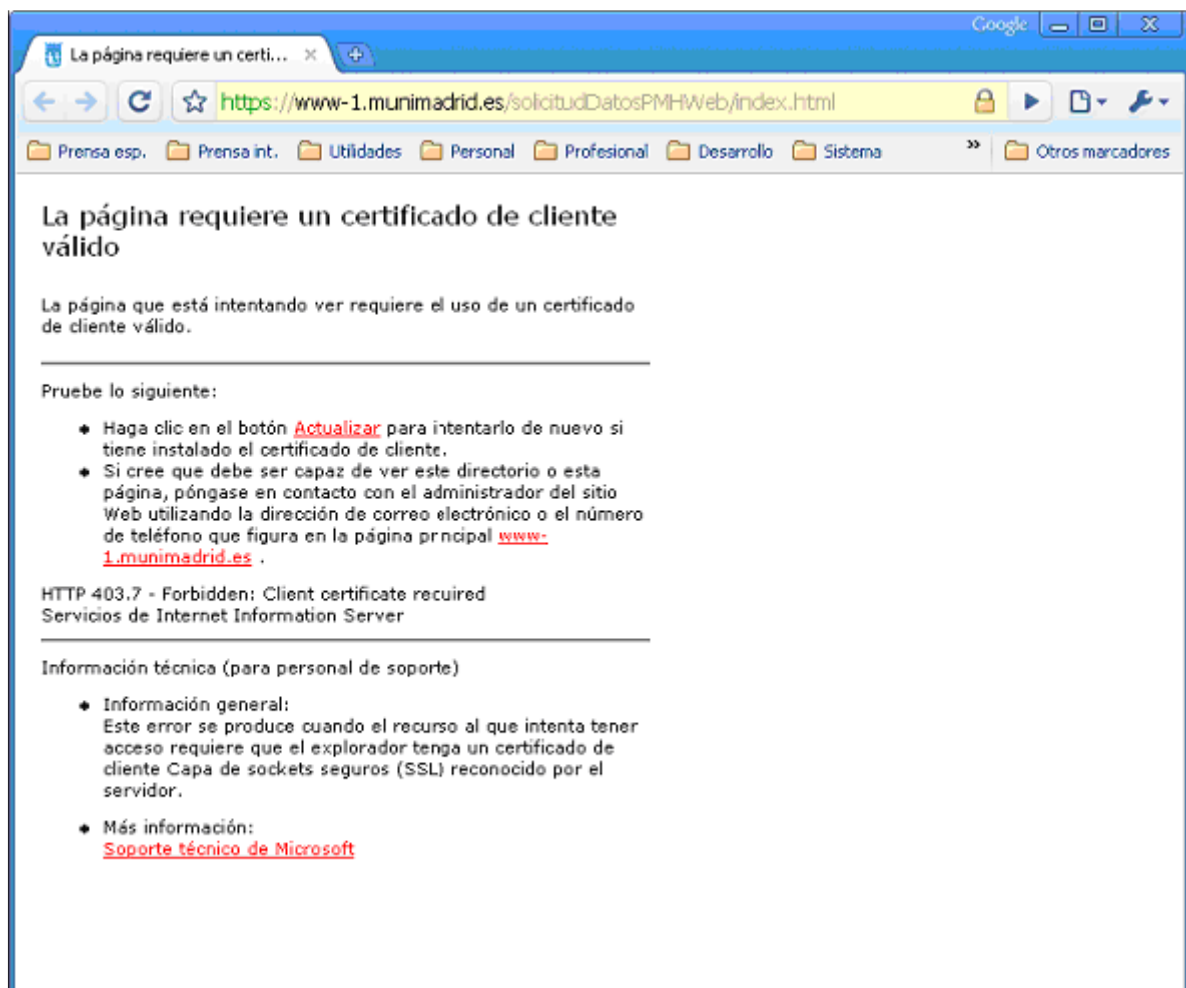


Imagen 5-26 Intento de acceso a una Web que solicita certificado.

Problemas de compatibilidad tecnológica. Las limitaciones del principio de neutralidad tecnológica

A pesar de que el principio de neutralidad tecnológica se ha convertido con el artículo 4.i de la Ley 11/2007 en un precepto legal *garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos*, en la práctica este principio no llega tan lejos como sería deseable.

Sus límites se manifiestan en la práctica principalmente con aquellos usuarios que utilizan los navegadores Web y sistemas operativos más *exóticos* o menos comunes. Es decir, usuarios que usen navegadores como Google Chrome, Opera, Safari de Apple, o Konqueror o Epiphany en Linux. El uso de estos navegadores está creciendo considerablemente teniendo cada vez más adeptos.

En el mes de agosto de 2011, *Global Web Stats*^{xiv}, publicó, como resultado de un estudio realizado, que el navegador más utilizado era *Internet Explorer* con un porcentaje del 35,4%, mientras que su más directo rival era, con un 26,7%, *Firefox*.

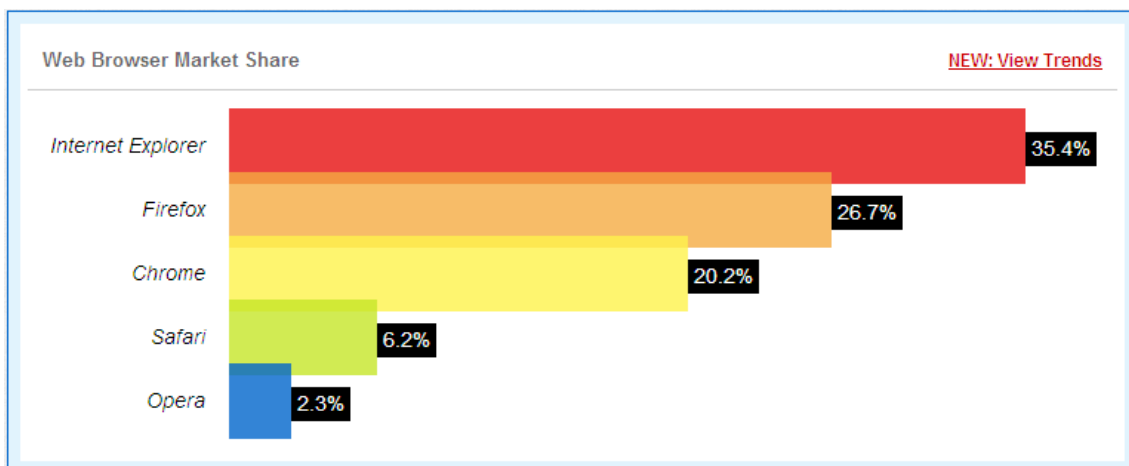


Imagen 5-27 Análisis de uso de navegadores Web agosto 2011

Entrando más en detalle en este análisis, conviene apreciar que existen diferentes versiones de cada navegador. Los datos resultantes en base a este *handicap* fueron:

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Web Browsers		
1	Internet Explorer 8	18.72%
2	Chrome 13	16.03%
3	Firefox 5	8.42%
4	Firefox 6	7.74%
5	Internet Explorer 7	7.50%
6	Firefox 3.6	7.40%
7	Internet Explorer 9	6.53%
8	Safari 5	5.33%
9	Internet Explorer 6	2.64%
10	Chrome 12	2.49%

Imagen 5-28 Análisis, con versiones, de navegadores Web, agosto 2011

Aunque en los datos se observan en los porcentajes reflejados en algunos casos décimas, estas suponen un gran número de usuarios.

Cabe destacar sobre este estudio el aumento del uso del modo de compatibilidad de Internet Explorer 8 (IE8), que permite visualizar correctamente WebSites que no cumplen los estándares Web, así como el hecho de que Internet Explorer 6 (IE6) siga utilizándose, teniendo en cuenta que fue lanzado en 2001.

6 PROYECTOS DESTACADOS EN ESPAÑA

Uno de los fundamentos para el desarrollo de la Administración Electrónica ha sido la creación de proyectos/servicios de carácter horizontal que las Administraciones y Organismos puedan utilizar para desarrollar sus servicios electrónicos.

Se pueden destacar algunos de ellos:

- **Plataforma SARA:** La Infraestructura Común de Comunicaciones (Red SARA) es una Red privada de comunicaciones que permite transferencias seguras entre todas las Administraciones Públicas, evitando la necesidad de tener que tender redes específicas para cada tarea administrativa. La Red interconecta todos los Departamentos ministeriales y todas las Comunidades Autónomas, actualmente está en fase de extensión a las Entidades Locales. Está integrada en la red europea de Administración Electrónica TESTA, que sirve la conexión a los recursos de todos los Estados miembros de la Unión Europea.
- **@Firma:** Es la plataforma de validación de certificados electrónicos que al ser *multi-PKI* permite validar la autenticación mediante certificado electrónico y la firma mediante certificado para los certificados de múltiples autoridades de certificación. Esto es vital, ya que existen en la actualidad decenas de prestadores de servicios de certificación diferentes, y sin una plataforma de este tipo cada organismo tendría que soportarlos todos o a gran parte y esto entrañaría una complejidad técnica y de gestión considerable. Con @Firma un único punto de acceso, ubicado en la red SARA, permite prácticamente el soporte de todos de un plumazo.
- **DNI electrónico:** El DNI electrónico supone un hito en la Administración Electrónica, ya que implica romper una de las mayores barreras de acceso a los servicios avanzados de ésta, disponer de un certificado electrónico personal. Con el nuevo documento se convierte el documento convencional en tarjeta inteligente, con dos certificados electrónicos:
 - uno para autenticación y
 - otro para firma electrónica.
- **Red 060:** La Red 060 es un portal que crea un único punto de acceso para los ciudadanos desde el cual pueden acceder a los servicios de la tres Administraciones (Estado, Autonómica y Local) sin la necesidad de conocer a qué Administración concreta corresponde un servicio o trámite concreto.
- **Notificaciones Telemáticas Seguras:** Este Servicio permite al ciudadano o a la empresa recibir todas las notificaciones procedentes

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

de las Administraciones Públicas en un buzón asociado a su *Dirección electrónica Única* (DEU). La recepción de las notificaciones es confidencial y segura, proporcionando al ciudadano, en su correo electrónico habitual, un aviso de recepción de notificación y un medio para elegir, para cada procedimiento, si desea ser notificado de forma electrónica.

A continuación se detallan los ejemplos que se han citado sobre estas líneas y se añaden otros más.

6.1 Administración Electrónica Estatal y Organismos Oficiales.

6.1.1 Oficina Virtual de La Agencia Tributaria

Cuando se habla de Administración electrónica en España, se suele citar la Agencia Tributaria como el buque insignia de la Administración Pública en España en este campo^{xv}.

Durante el año 2009 se realizaron por Internet un total de 51.472.066 declaraciones. Siendo las declaraciones de "*autoliquidación impuesto valor añadido*" las que más movimientos registraron con un total de 11.612.486.

En el anexo del documento, se puede ver toda la tabla desglosada por tipos de movimientos y por año, desde el 2005 hasta el 31 de enero de 2010.

The screenshot shows the website of the Agencia Tributaria (Tax Agency) in a web browser. The browser address bar shows the URL: <http://www.aeat.es/wps/portal/Navegador?channel=c552ea4c0e129010VgrWCM1000004ef01e0a...&ver=L&site=5X>. The website header includes the logo of the Government of Spain and the text "Agencia Tributaria". There are navigation tabs for "La Agencia Tributaria", "Ciudadanos", "Empresas y profesionales", and "Colaboradores". The "Ciudadanos" tab is selected. Below the header, there is a search bar with a "Buscar" button and a "Portal" dropdown menu. A large banner image shows a person working on a laptop with the text "Todos los trámites on line". Below the banner, there is a "Oficina Virtual" button. The main content area is divided into several sections:

- Pago de Impuestos:** Autoliquidaciones, Liquidaciones - Deudas, Tasas. [Ver más](#)
- Registro de documentos electrónicos:** Interposición de recursos y solicitudes de revisión, Relacionada con presentaciones telemáticas previas, Relacionada con requerimientos o comunicaciones de la Agencia. [Ver más](#)
- Consultas de declaraciones:** Verificación de modelos presentados, Consulta íntegra de modelos presentados, Consulta por rango de fechas. [Ver más](#)
- Otros Trámites:** Certificaciones Tributarias.
- Presentación de Declaraciones:** Grandes Empresas, Censales-Domicilio Fiscal, Trimestrales. [Ver más](#)
- Administraciones Públicas:** Dirección General de Tributos, Modelo 111 - I.R.P.F. Retenciones e ingresos a cuenta de trabajo personal, Intercambio de información del IAE. [Ver más](#)
- Consultas personalizadas:** De situación fiscal, Estadísticas, Verificación de pagos. [Ver más](#)
- Otras Opciones:** Comunicaciones a Colaboradores.

On the right side, there is a "Acceda directamente" section with links to "A un clic" (Calendario del contribuyente, Carta de Servicios, Certificados Electrónicos, Descarga de programas de ayuda, Modelos y formularios, Normativas y criterios interpretativos, Preguntar más de cuentas (INFORMA)), "Enlaces relacionados" (Ministerio de Economía y Hacienda, Otros Enlaces de Interés), and "A destacar" (Certificaciones de Contabilistas y Subcontratistas, Domicilio Fiscal (Modelo 030), Establecimientos Tributarios, Casilla Agrícola/Profesional).

Imagen 6-1 Servicios para ciudadanos que ofrece la Agencia Tributaria

La experiencia de la AEAT

Muchos de los trabajos realizados por la AEAT durante los últimos cinco años han generado resultados que confluyen con el mandato de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) y lo ya realizado facilitará su cumplimiento. Se categorizan las tareas más importantes a realizar en cinco grupos y describiremos en qué medida los objetivos han sido ya alcanzados y en cual deben ser implementados todavía.

A todas ellas deben sumarse la tareas necesarias para cumplir el mandato del art. 6.2.b de la LAECSP, que establece que no se podrán pedir datos de los que ya dispone la Administración lo que, más allá de la aplicación de reglas de interoperabilidad exigirá el desarrollo de numerosos servicios Web en coordinación con otros órganos de la Administración que han sido identificados y clasificados en 28 categorías.

a) Desarrollo de la sede

En la actualidad la AEAT dispone de un portal www.aeat.es que contiene más de 40.000 páginas en el que se incluye su Oficina Virtual, que responde al art. 10 de la LAECSP, que define el concepto de sede concebida como una dirección electrónica única con determinados requisitos.

Su adaptación ha llegado a alcanzar los grados de accesibilidad y usabilidad deseables y proporcionar un servicio seguro y robusto. Una parte importante es la oferta normalizada, precisa y oportuna de información sobre los más de 250 procedimientos de la AEAT.

Su mantenimiento se realiza hoy de forma colaborativa por distintos Departamentos de la AEAT. Con carácter horizontal el Gabinete coordina la publicación de notas de prensa y el Departamento de Planificación y Relaciones Institucionales (DOPRI) atiende los aspectos lingüísticos, aprueba el libro de estilo y preside el Comité de Comunicación. El Departamento de RR.HH. aporta los contenidos en materia de recursos humanos y los referentes a concursos y subastas. Los Departamentos Verticales (Gestión, Inspección, Aduanas) coordinan los materiales que son incorporados mediante un Gestor de Contenidos.

La AEAT ha impulsado acciones en dos bloques para garantizar la calidad del servicio prestado. Robustecer la plataforma y mejorar la calidad y accesibilidad de los contenidos.

En la actualidad se utiliza un sistema esquematizado (véase la siguiente figura). Los servicios de Oficina Virtual en los que se debe autenticar al

contribuyente se prestan en el host de la AEAT. Existen otros servidores externalizados desde los que se sirve la información estática (40.000 páginas de información institucional y legislación) difundándose luego estos contenidos a través de AKAMAI.

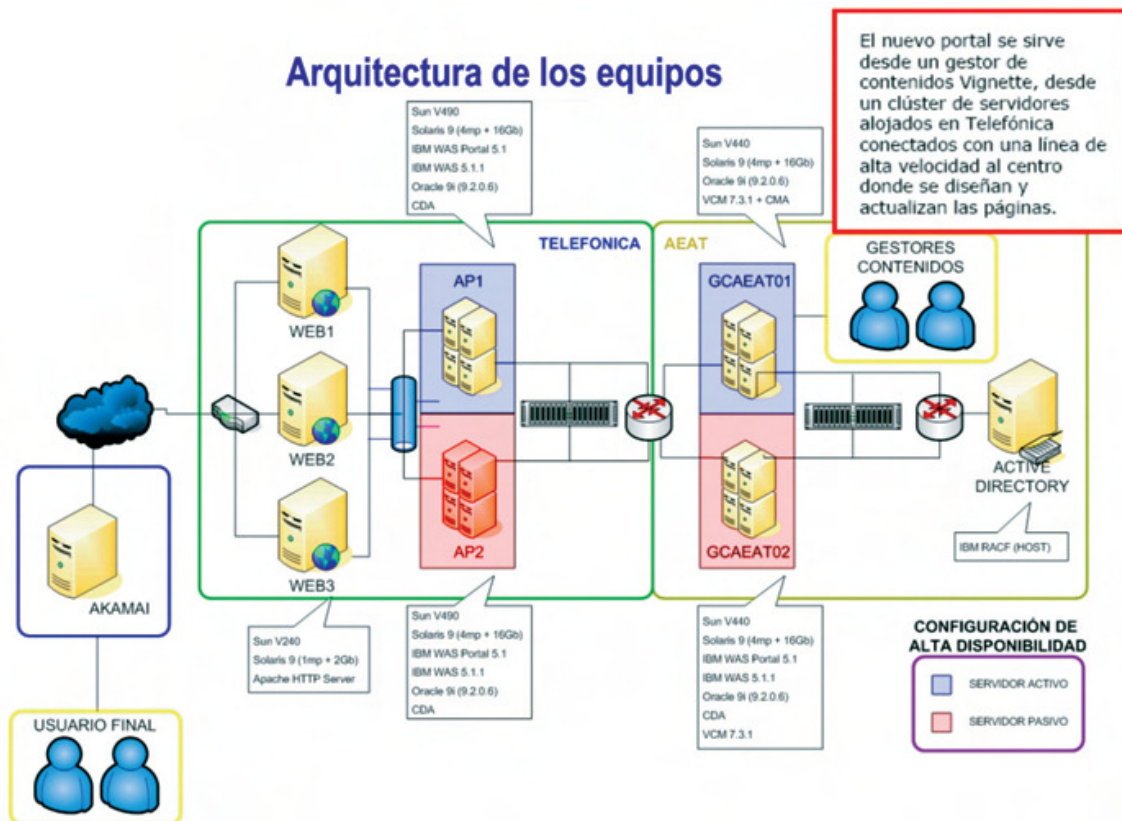


Imagen 6-2 Arquitectura de los servicios a través de Internet de la AEAT.

Con objeto de mejorar la calidad de los contenidos, en enero de 2008 fueron evaluados, por un tercero, distintos parámetros de la calidad de la relación entre la AEAT y un contribuyente a través de la Oficina Virtual. Entre los conceptos analizados estaban: grado de cumplimiento de los objetivos del usuario que accede, tiempo empleado, número de reintentos, facilidad de interpretación de la interfaz, problemas de interacción, problemas de estética y problemas de comportamiento del sistema.

Para ello un colectivo formado por estudiantes, empresarios y profesionales de distintas especialidades y comerciales, entre otros, analizó distintos servicios (obtención de certificados, presentación de declaraciones, cambios de domicilio...) identificando áreas de mejora (calidad del buscador, texto de los botones, ayudas, etc.) y realizando una auditoría de usabilidad que ha

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

conducido, tras centenares de horas de trabajo, a la modificación del Portal, que fue sometido a un nuevo test en junio de 2008 con funciones relacionadas con el borrador y la solicitud de cita previa. Como consecuencia se ha modificado el libro de estilo y en la actualidad dos equipos de desarrollo están reconfigurando los contenidos mediante la aplicación de un nuevo gestor de contenidos. Con ello se espera que la sede de la AEAT alcance los mejores niveles de accesibilidad y usabilidad posibles.

La información sobre los más de 250 procedimientos identificados será mantenida por los distintos Departamentos utilizando la tecnología implantada, que se apoya en un gestor de contenidos y en el empleo de 51 plantillas en las que se insertan 72 tipos de componentes.

b) Iniciación de los trámites telemáticos

Pueden diferenciarse dos tipos de procedimientos. Aquellos que se inician mediante el envío por el contribuyente de información estructurada y aquellos en los que la iniciación se produce utilizando el servicio de Registro. Hoy muchos de los procedimientos disponen de iniciación electrónica desde la propia aplicación gestora, siendo ejemplo aquellos por los que se solicita y acepta un borrador del Impuesto sobre la Renta o la presentación de una declaración sumaria o de importación. Otros procedimientos disponen de medios específicos para ser iniciados desde el Registro del Portal.

The image shows a screenshot of the AEAT (Agencia Tributaria) website. At the top, there is a navigation bar with the logo and name 'Agencia Tributaria' on the left, and links for 'Política lingüística', 'Ayuda | Mapa web | Accesibilidad' on the right. Below this is a secondary navigation bar with tabs for 'La Agencia Tributaria', 'Ciudadanos', 'Empresas y profesionales', 'Colaboradores', and 'Directorio A-Z'. The main content area has a breadcrumb trail: 'Inicio > Oficina Virtual > Registro de documentos electrónicos'. A large banner image shows a woman using a laptop with the text 'Todos los trámites on line'. To the right of the banner is a search box labeled 'Buscar:' and a dropdown menu labeled 'Ir al portal de:' with the option '--seleccione portal--'. Below the banner is a section titled 'Registro de documentos electrónicos' with a list of services: 'Interposición de recursos y solicitudes de revisión', 'Relacionada con presentaciones telemáticas previas', 'Relacionada con requerimientos o comunicaciones de la Agencia', 'Corrección de Declaraciones Informativas', 'Presentación de documentos Otros Organismos', 'Relacionado con el tipo impositivo reducido de IVA', 'Procedimiento para bonificaciones de la Seguridad Social', and 'Procedimiento solicitud de NIF para un menor por una entidad de crédito'. To the right of this list is a section titled 'Acceda directamente' with a list of links: 'A un clic', 'Calendario del contribuyente', 'Carta de Servicios', 'Certificados de usuario', 'Descarga de programas de ayuda', 'Modelos y formularios', 'Normativas y criterios interpretativos', and 'Preguntas más frecuentes (INFORMA)'. At the bottom right of this section is a link for 'Enlaces relacionados'.

Imagen 6-3 Registro electrónico en el Portal de la AEAT.

c) Pago



En la actualidad y como ha sido descrito pagos electrónicos pueden realizarse bien a través de la pasarela de pago bien ingresando y luego remitiendo el Número de Referencia Completo (NRC)^{xvi}. Han sido identificados, en la revisión realizada, algunos procedimientos cuyo número en términos absolutos es reducido.

d) Notificaciones

Desde junio del año 1993 han sido realizadas 12.023.251 notificaciones electrónicas y desde junio de 2006 más de seis millones de comunicaciones siendo el propósito de la AEAT impulsar activamente en el futuro tanto el uso del DEU como la notificación por comparecencia.

e) Control de la tramitación

En la actualidad existe la posibilidad de conocer a través de Internet algunos estados de tramitación en algunos procedimientos. Facilitar el acceso con carácter general y de una forma simple obliga en primer lugar a determinar cuáles son esos estados y el formato y contenido de la información. A ello se une la dificultad de gestionar su ciclo de vida (a partir de cuándo y durante cuánto tiempo), el acceso por asesores autorizados y apoderados y las formas de auditoría.

La identificación y cambio de todos los módulos que es necesario modificar para informar con precisión, oportunidad y seguridad de los estados de tramitación de los cerca de 250 procedimientos de forma normalizada incorporando las adecuadas garantías de privacidad y auditabilidad supone un trabajo complejo que se desarrollará progresivamente comenzando con los procesos en los que el número de usuarios interesados es mayor.

f) Copia electrónica

Al DIT llega información en muy diversos formatos: algunos estructurados como EDI o XML, otros simples empleados en confirmaciones, ficheros con declaraciones información en registros planos, otros que son el resultado de escanear algo e introducirlo por registro y ficheros MP3 (conversaciones del CAT) entre otros.

La LAECSP define en su Artículo 25 las normas de funcionamiento de los registros electrónicos señalando que «...Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.»). y también que «...Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.»

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Surge la obligación de generar una copia auténtica de todo lo presentado por el contribuyente. La aplicación de Registro soluciona esta cuestión para los documentos, que hace referencia el Artículo 25 de la LAECSP, donde menciona las normas de funcionamiento de los registros electrónicos señalando que «...Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.»). y también que «...Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.»

Sin embargo para el caso de presentación de formularios normalizados es preciso algo más pues el recibo al que hace referencia el artículo 25 debe incluir información adicional a la propia declaración (fecha, hora, número registro,...) por tanto se requiere crear nuevos documentos electrónicos “recibos acreditativos de entrega” para cada presentación/declaración recibida incluidos los centenares de millones de declaraciones telemáticas que figuran en las bases de datos de la AEAT.

Tendríamos para cada declaración normalizada dos documentos electrónicos, el enviado por el contribuyente con su firma electrónica y el recibo acreditativo de entrega que lo referencia. Dicho recibo acreditativo será un documento electrónico asociado a la declaración indicando la clave del documento admitido, fecha-hora y garantizando la integridad del mismo al incluir una huella del mismo y finalmente la validez del recibo se garantizará con un código seguro de verificación, en adelante CSV aplicando el artículo 30, apartado 5).

Hoy en día existe la posibilidad en la opción Cotejo de documentos mediante Código Seguro de Verificación de la Oficina Virtual.

g) Conclusión

Durante el ejercicio del 2009 han sido presentadas por Internet 46.904.455 declaraciones. Durante el año en curso del 2010 la AEAT ha atendido más de 326.000 llamadas de los contribuyentes, enviado 241.891 mensajes a móviles, registrado más de 245.000 documentos en su registro electrónico^{xvii}. Las auditorías y las encuestas muestran el reconocimiento del ciudadano a la magnitud del trabajo realizado y el volumen de los servicios prestados. El trabajo realizado ha sido y es necesario para consolidar la confianza del ciudadano, mostrar la seguridad y eliminar las barreras del espacio y el tiempo.

La AEAT busca hoy la prestación continua de servicios de creciente calidad y complejidad mediante el uso de tecnologías que permitan la prestación de servicios de forma transparente a ciudadanos siempre conectados.

6.1.2 La experiencia de la FNMT-RCM



Introducción

Desde el momento en el que se creó como institución la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM), el objetivo fundamental de esta ha sido el desarrollo, fabricación y distribución de productos diversos, garantizando la total seguridad y autenticidad de los mismos^{xviii}.

Con la evolución de la actual Sociedad de la Información y de las Comunicaciones, la FNMT-RCM inició en 1996 un nuevo reto mediante su proyecto CERES. CERES, acrónimo de Certificación Española, nació con la intención de realizar tareas de I+D sobre un área de negocio que por aquel entonces no dejaba de ser más que un mundo por descubrir y en la que la FNMT-RCM fue pionera: La seguridad en las transacciones realizadas mediante medios telemáticos.

La FNMT-RCM fue designada por el artículo 81 de la Ley 66/1997, de 30 de diciembre, desarrollada por el Real Decreto 1290/1999, de 23 de julio, para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de las comunicaciones de la Administración General del Estado y sus organismos públicos, a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT).

Tras la labor de I+D, la FNMT-RCM comenzó a prestar servicios como Autoridad de Certificación en el año 1998. El año siguiente, en 1999, la Agencia Estatal de Administración Tributaria (AEAT) apostó por la FNMT-RCM como Autoridad de Certificación de confianza para la emisión de certificados válidos para la relación telemática con los ciudadanos.

El inicio en la prestación de los servicios de certificación sirvió a la vez de base para el estudio de los servicios de valor añadido que posteriormente pasarían a ser ofrecidos. Estos servicios fueron, por un lado el fechado digital de documentos electrónicos y la validación de certificados digitales, y por otro lado, los certificados de atributos, íntimamente ligados a los certificados digitales emitidos por la Autoridad de Certificación.

Tras esto se desarrollaron plataformas para la prestación de servicios, en las que CERES actuaba como tercero de confianza, permitiendo realizar por ejemplo notificaciones telemáticas, custodias electrónicas o incluso proyectos piloto de votaciones haciendo uso de la Red.

Simultáneamente, y debido a la necesidad del almacenamiento en un soporte físico seguro de las claves privadas asociadas a un certificado, el departamento de tarjetas de la FNMT implementó tanto física como lógicamente una tarjeta criptográfica que cumpliera con esas características. Sería la denominada tarjeta Ceres.

Esta experiencia, junto al interés mostrado por la Dirección General de la Policía por desarrollar un Documento Nacional de Identidad electrónico (DNIE)

que permitiese a los ciudadanos realizar trámites administrativos a través de Internet, con garantías tanto de autenticidad como de no repudio, permitieron iniciar un proyecto, en el que la FNMT-RCM asesoró técnicamente en muchos campos y en los que se constituyó como Autoridad de Validación y proveedor del soporte físico para el DNle.

Fechado Digital

Antecedentes

La Unión Europea a través de su programa ETS (*European Trusted Services*)^{xix} subvencionó en 1998 varios proyectos relacionados con las infraestructuras de clave pública y terceras partes de confianza. La FNMT-RCM, participó en uno de estos proyectos, junto al entonces Organismo Autónomo de Correos y Telégrafos, la Universidad Politécnica de Cataluña y el Ministerio de Administraciones Públicas (MAP). El objetivo de este proyecto fue la evaluación de los aspectos funcionales y no funcionales del servicio, los requisitos de calidad, el análisis de riesgos y posibles ataques y la presentación de posibles escenarios de uso. Por otro lado, dentro de la fase de desarrollo piloto, se implementó un servicio de fechado digital sobre documentos multimedia, con el fin de demostrar la funcionalidad y utilidad del servicio.

Tras el éxito de este proyecto, la FNMT-RCM abrió varias líneas de avance sobre el servicio de fechado digital. Por un lado, se involucró, dentro del grupo de trabajo PKIX (*Public Key Infrastructure using X.509*) de IETF (*Internet Engineering Task Force*)^{xx}, en la elaboración de la RFC (*Request For Comments*) correspondiente al servicio. Por otro lado, se establecieron contactos con ISO para participar como editores en la redacción de la norma de fechado digital. Finalmente, y con el objetivo de ser pioneros en la prestación de este servicio, la FNMT-RCM comenzó el desarrollo de su propio servicio de fechado digital, inicialmente basándose en los borradores de PKIX-IETF y posteriormente en la RFC.

El servicio

El fechado digital de documentos electrónicos puede definirse como la génesis de evidencias que demuestran la existencia de un documento en un instante preciso en el tiempo. Esta prueba de existencia o certificado temporal puede, a su vez, ser aplicada como base para probar circunstancias más elaboradas, fundamentalmente en escenarios de no repudio.

Formalmente se puede demostrar mediante técnicas de fechado la existencia de un documento 'antes' y 'después' de un instante en el tiempo:

'ANTES': Fechado de un documento D en el momento t0

t0: F(D,t0)

Se demuestra la existencia del documento D en el instante t_0 . D existía antes de t_0 porque de otra forma no se pudo fechar. O de otro modo; D no se creó después de t_0 .

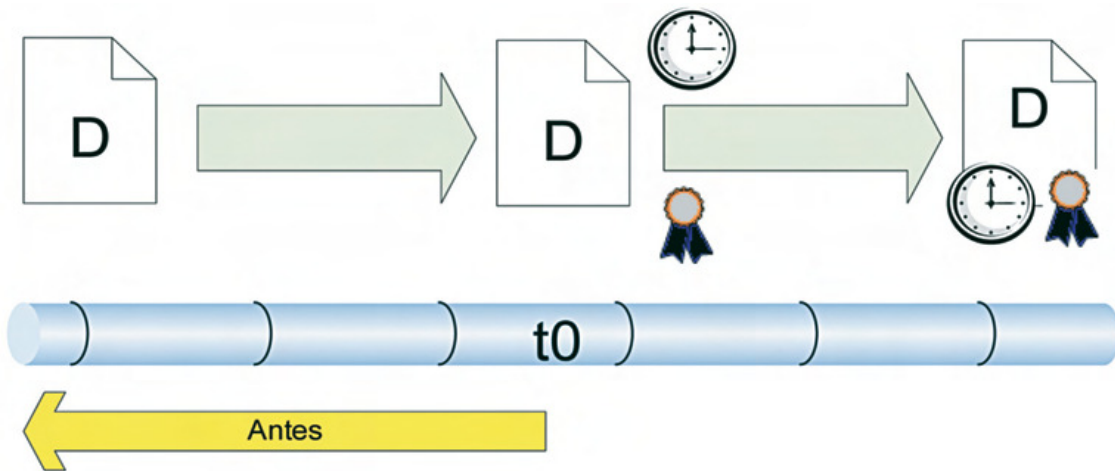


Imagen 6-4 Esquema fechado temporal antes

‘DESPUES’: Inclusión de información no predecible en el pasado

t_0 : $TT := F(X, t_0)$;

t_1 : $D++TT$ (Documento concatenado con la información no predecible).

Se demuestra que el documento ($D++TT$) no pudo crearse antes de la emisión de la información TT , es decir se creó después de t_0 .

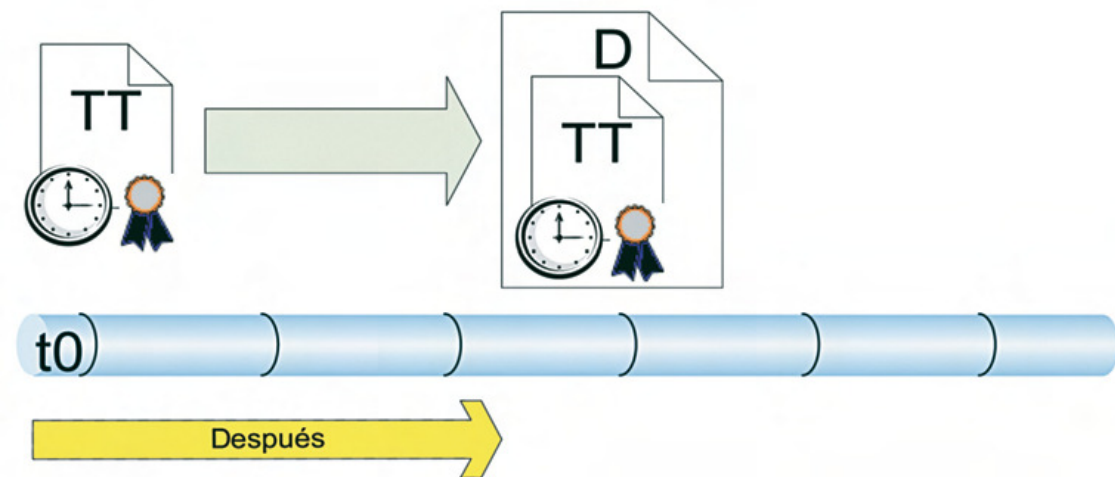


Imagen 6-5 Esquema fechado temporal después

La combinación de ambos conceptos permite desarrollar técnicas útiles para asociar la existencia de un documento con un intervalo de tiempo.

INTERVALO:

t_0 : $TT := F(X, t_0)$;

t_1 : $H(D, TT)$;

t_2 : $F(H(D, TT), TT, t_2)$

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Se demuestra que D existe después de t_0 (no puede haber sido destruido antes) y anteriormente a t_2 . El intervalo (t_0, t_2) delimita un periodo de existencia de D.

En general, se hace necesaria una entidad que certifique el tiempo al que se asocia un documento para dar consistencia legal a las evidencias. Esta entidad es la que se denomina TSA o autoridad de fechado digital. La TSA es una tercera parte de confianza (TTP) que asocia un tiempo “certificado” a los documentos, siendo su firma sobre el certificado temporal suficiente para dotar validez al mismo.

La TSA centraliza la emisión de certificados temporales. El papel que jugará esta entidad será producir, almacenar, verificar y en su caso renovar certificados temporales.

El protocolo más extendido para este servicio es el denominado protocolo simple. Este protocolo es sencillo en su implementación, rápido, con bajos requisitos de almacenamiento en la Autoridad, permite el sellado de tiempo de cualquier tipo de información digital, y protege la confidencialidad de los datos fechados. Este es el usado por la FNMT-RCM.

El protocolo simple constituye una opción idónea en escenarios de baja complejidad donde el grado de confianza en la TSA es muy alto, tal y como sucede con la TSA de la FNMT-RCM.

Existen otros protocolos, que aunque no aportan menor seguridad al proceso, sí tienen otros inconvenientes que hacen que su utilidad quede prácticamente restringida a entornos académicos.

Terminamos chocando con una reflexión fundamental frente a frente con el fechado digital; una tecnología incipiente, en desarrollo, con nuevas técnicas que se adaptan a las complejas situaciones que se presentan en el entorno PKI: La ventana abierta por el fechado digital presenta un amplio espectro de aplicaciones posibles que contribuyen a crear un nuevo concepto de servicio público a través de redes abiertas. El fechado digital no complementa como se ha creído “tradicionalmente” sino que se erige en pilar central de la ventanilla única soportada por estructuras de clave pública.

Autoridad de validación

Antecedentes

La base fundamental de cualquier PKI son los certificados. Aunque estos certificados pueden tener diferentes usos, el más común de ellos es la firma digital. En los procesos en los que intervienen operaciones de firma digital, las aplicaciones destinadas a este efecto se dedican exclusivamente a tareas criptográficas, dejando de lado la verificación del certificado usado para ello. Esto es debido a que la tarea tanto de verificación formal como de la validez del



propio certificado utilizado para la firma debe ser llevada a cabo por el destinatario del mensaje.

La mayor parte de las autoridades de certificación suelen poseer un directorio genérico, con acceso LDAP o X.500, en donde son publicados tanto los certificados, como el estado de los mismos, estos últimos almacenados en CRLs (Listas de Revocación de Certificados). Para comprobar el estado de revocación se podrían consultar estas listas, o bien utilizar otros mecanismos de validación que utilizan protocolos estándar, como puede ser el OCSP (*On line Certificate Status Protocol*), el SCVP (*Simple Certificate Validation Protocol*), el XKMS (*XML Key Management Specification*), u otros.

La FNMT-RCM, simultáneamente con el desarrollo del servicio de fechado digital, inició un proyecto para la implementación de su propia Autoridad de validación, basándose en la recomendación existente para el protocolo OCSP. El objetivo establecido en primera estancia fue la validación de los certificados utilizados por clientes que hacían peticiones de fechado digital. Sin embargo, este objetivo fue ampliado poco tiempo después y el servicio se comenzó a prestar de manera global. Actualmente la FNMT-RCM está constituida como Autoridad de validación para los certificados de varias PKIs, entre las que cabe destacar la de la propia FNMT-RCM o la del DNle.

El servicio

El protocolo OCSP está especificado por el grupo de trabajo PKIX de IETF en la RFC 2560, publicada en junio de 1999. El objetivo de este protocolo es la consulta del estado de uno o más certificados de clave pública X.509, evitando al usuario final la complicada consulta y tratamiento de las CRLs emitidas por la autoridad de certificación. El cliente emite una petición OCSP y deja en suspenso la aceptación de las operaciones llevadas a cabo con el certificado en cuestión hasta que el servidor le devuelve una respuesta.

En este protocolo se especifican los datos que deben ser intercambiados entre una aplicación que desea conocer el estado de un certificado y el servidor que proporciona este estado. Básicamente es necesario que la aplicación cliente proporcione una lista de uno o más registros, en la que se incluyan los números de serie de los certificados a validar y el identificador del emisor de los mismos. Estos datos podrían, opcionalmente, ir firmados. Una vez recibida la petición, el servidor responde con una lista acorde a los datos solicitados y en la que se incluye el estado de los certificados solicitados así como el intervalo de validez durante el cual esos datos son válidos. La respuesta del servidor debe de ir obligatoriamente firmada por la Autoridad de validación.

La trivialidad de este servicio no permite dejar de lado, ni abstraerse de la potencia y los beneficios que es capaz de proporcionar. Según la propia especificación, una de las características que posee es la capacidad para responder a peticiones, de manera veraz, sobre el estado de certificados pertenecientes a diferentes autoridades de certificación, siempre y cuando se

disponga de la información asociada a los mismos, ya sea o bien mediante accesos a fuentes de datos o bien mediante el acceso a otros servicios de validación. Esto es lo que se denomina validación de certificados multiCA.

Certificación de atributos

Antecedentes

La certificación de atributos es la asignatura pendiente del mundo de las PKIs. Aunque su necesidad es más que clara, la mayor parte de las entidades usuarias han desistido de utilizarla. La escasez de información, de proveedores que suministren el servicio y por otro lado la inexistencia de aplicaciones que hagan uso del mismo, suponen el mayor "handicap" para un servicio de gran utilidad.

La FNMT-RCM inició en 2000 su propio proyecto para el desarrollo de una autoridad de certificación de atributos y actualmente entra dentro de su catálogo de servicios ofrecidos.

El servicio

La recomendación X.509 v3 de ITU-T, aparte de sentar las bases para los certificados de clave pública, introdujo el concepto de certificado de atributos. Posteriormente, la revisión 4 de esa misma recomendación sirvió para profundizar en el campo de la certificación de atributos.

Una definición muy genérica de certificado de atributos podría ser: "Un certificado de atributos es un documento electrónico, firmado electrónicamente por una autoridad de certificación de atributos, cuyo contenido liga un determinado atributo a una identidad (certificado de clave pública)". Sin embargo, esta definición da cabida a que cualquier tipo de documento electrónico firmado electrónicamente que certifique una determinada característica (por ejemplo, un correo electrónico), sea automáticamente ascendido a la categoría de certificado de atributos (lo cual podría ser una infraestructura de certificados de atributos perfectamente válida, siempre y cuando las entidades que fuesen a verificar la validez de los atributos sean humanos y acuerden como se van a procesar esos atributos). Como de lo que se trata es de tratamientos automatizados de datos, es necesario definir determinados formatos para facilitar esta tarea, y aquí es donde interviene la anteriormente citada recomendación X.509.

El certificado de atributos es una estructura representada en ASN.1 y cuyo contenido básico es el poseedor del atributo o atributos, el emisor del mismo, un número de serie, el periodo de validez y finalmente una secuencia de uno o más atributos. Toda esta información deberá ir necesariamente firmada por la autoridad de certificación de atributos.

El tratar de implementar una infraestructura de certificación de atributos propia puede llegar a ser una tarea formidablemente pesada, ya sea por tener que



tratar con sus estructuras de datos (el ASN.1 tiene sus rarezas, y los compiladores que facilitan su manejo no son herramientas ni comunes ni asequibles), ya sea por los recursos de los que sería necesario disponer para el desarrollo de los elementos de la infraestructura. Afortunadamente, hace tiempo que se cuenta con infraestructuras de clave pública consolidadas, muchas de las cuales son capaces de emitir certificados de atributos, como es el caso de la FNMT-RCM, y se cuenta con librerías capaces de entender y utilizar los mismos en diversidad de plataformas. Por otra parte, una estructura mínima de certificación de atributos cuenta con los siguientes participantes:

PKI, es la infraestructura de clave pública encargada de proporcionar el soporte apropiado para que pueda existir una infraestructura de certificación de atributos. Sus funciones serán las características de una PKI (gestión de certificados de clave pública, registro de usuarios, etc.).

Autoridad de Registro de Atributos (ARA). Recibe solicitudes de certificados de atributos por parte de los usuarios de la infraestructura, verifica (ya sea mediante una consulta telemática a un repositorio o mediante procedimientos tradicionales) si el usuario puede tener ese certificado de atributos, y solicita el certificado de atributos a la Autoridad de Certificación de Atributos (ACA). Asimismo, recibe peticiones de revocación de atributos y solicita las mismas a la ACA.

ACA, recibe solicitudes de emisión y revocación de certificados de atributos, emite y revoca certificados de atributos, publica lo anterior en un repositorio y lo pone a disposición de los usuarios.

Usuario, pudiendo ser poseedor o no de un certificado de atributos. Si lo posee podrá hacer uso de él en aquellos ámbitos que así lo necesiten. Si no lo posee, lo que podrá hacer es verificar los certificados de atributos de otros usuarios.

Sobre el papel, los certificados de atributos resuelven de una manera muy elegante determinadas deficiencias que presentan las infraestructuras de clave pública tal como están desplegadas hoy en día. Lamentablemente, no están lo suficientemente extendidos, probablemente debido a varios factores:

- Así como existen muchas aplicaciones que utilizan actualmente certificados de clave pública (navegadores, programas de correo electrónico, etc.), no hay aplicaciones equivalentes que utilicen certificados de atributos.
- Problemas de estandarización, el formato del certificado de atributos y las listas de certificados de atributos está formalizado, pero no ocurre lo mismo con los atributos en sí. Es necesario un esfuerzo de normalización (o una amplia base de usuarios que comience a utilizar unos determinados atributos de una determinada manera), para que distintas aplicaciones sean capaces de procesar distintos atributos.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

En relación al tema anterior, no existe un repositorio global donde se pudiese consultar qué atributos están definidos, cuál es su formato, cuál es su utilización y donde se puedan insertar atributos nuevos. Crear uno sería una buena idea.

Falta de información, probablemente debido a su escasa utilización, estos certificados son poco conocidos, lo cual crea un círculo vicioso.

Notificación telemática

Antecedentes

Los servicios que se han comentado en anteriores apartados son la base de cualquier PKI. Tomando como base estos servicios, se pueden llevar a cabo implementaciones de aplicaciones o nuevos servicios, que haciendo uso de la firma electrónica constituyan una evolución tecnológica y un gran avance en actividades cotidianas de personas y empresas. Entre estos servicios se encuentra la notificación telemática.

La notificación telemática tiene su base en el correo postal certificado y su objetivo fundamental es garantizar el no repudio de comunicaciones efectuadas entre dos partes.

El servicio

El correo postal certificado es solicitado por una entidad u organismo notificador con la intención de informar a uno o varios ciudadanos o empresas. La entrega del mensaje se suele realizar, por vía postal y se garantiza gracias a la firma de un certificado que queda custodiado por la entidad postal, y pudiendo ser devuelto un acuse de recibo al origen, en caso de que esto sea requerido.

Si este escenario es trasladado al entorno de las transacciones electrónicas vuelven a surgir tres actores. Por un lado, la entidad u organismo emisor de la notificación; en el extremo opuesto el ciudadano o empresa receptora y entre ambos un tercero de confianza que preste el servicio de notificaciones electrónicas. Todo esto englobado en un marco que proporciona la máxima seguridad.

Pero, ¿qué ventajas proporciona el uso del sistema de notificaciones electrónicas? Básicamente, el sistema garantiza la seguridad de las transacciones y la rapidez en la tramitación, a la vez que se produce un ahorro más que considerable en los costes a los que las entidades notificadoras deben hacer frente.

La inexistencia de recomendaciones o normativa aplicable a este tipo de aplicaciones, obliga a que los implementadores desarrollen sus propios mecanismos de acceso e interfaces, basándose únicamente en los requisitos definidos para el sistema.

Centrándonos en el servicio ofrecido por la FNMT-RCM, el notificador hará uso de unas librerías, proporcionadas por la FNMT-RCM, para integrar su aplicación con el envío de notificaciones. Estas librerías permiten el envío de notificaciones, así como la comprobación del estado de una determinada notificación. Una vez realizada esta integración, el notificador deberá registrarse en el servicio para poder proceder a los envíos, además de estar en posesión de un certificado digital X.509 emitido por la FNMT-RCM, válido y no revocado, así como de su correspondiente clave privada de manera que se permita la autenticación de forma segura del mismo.

Un paquete de notificación se compone básicamente de un título, un cuerpo de mensaje, un fichero (opcional) y una lista de destinatarios.

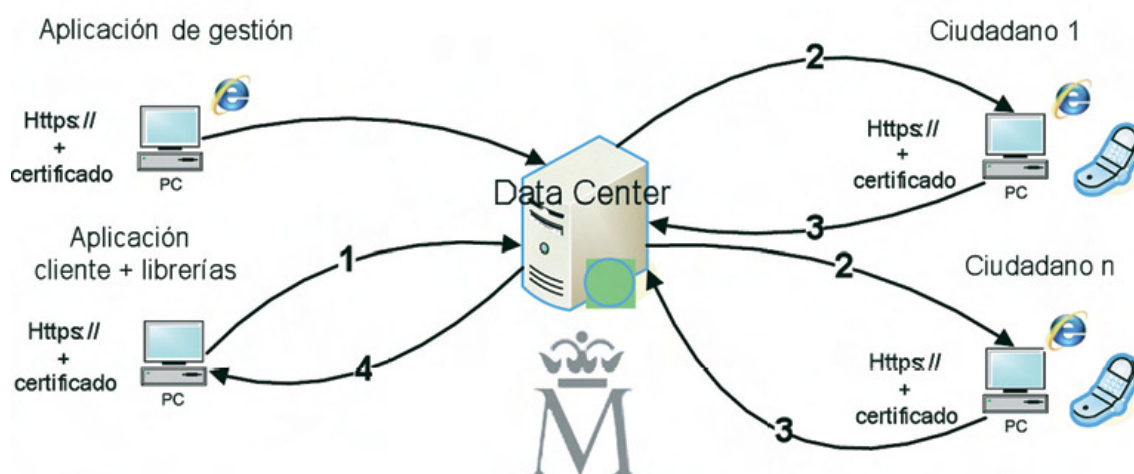


Imagen 6-6 Ejemplo de Notificación

Una vez que el notificador ha compuesto el paquete con la notificación y se lo ha enviado a la FNMT-RCM cifrado y firmado (1), esta procede a la comprobación de la entidad del solicitante y de los permisos que tiene atribuidos. Si los datos son correctos se realiza la custodia de la notificación, se pone a disposición del destinatario/s (2) y se devuelve un recibo fechado y firmado al notificador indicando que la notificación ha sido recibida (3-4).

La FNMT-RCM, como prestador del servicio y al único efecto de dar fe de lo acontecido, tiene un acceso limitado a las notificaciones practicadas. Dicho acceso limitado no permite en ningún caso, a ningún empleado o colaborador externo de la FNMT-RCM, el acceso a las notificaciones. El procedimiento de acceso se regula en los procedimientos de seguridad internos y está basado en un sistema de concurrencia de al menos 4 personas, con carácter ejecutivo dentro de la FNMT-RCM. Todo acceso es anotado en un libro de control de accesos donde se hace constar al menos, la fecha, la hora, el motivo justificado del acceso así como los intervinientes y su cualificación.

El tiempo de custodia inicial de las notificaciones telemáticas será de 5 años, prorrogables.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

La FNMT-RCM como prestador de servicios de Dirección Electrónica Única (DEU) proporciona a todos los usuarios que lo soliciten una dirección en Internet que le permite recibir las notificaciones de todos los notificadores que hayan suscrito un acuerdo con el prestador de servicios de notificación. Esta dirección única es una URL y el acceso a la misma se realiza mediante el protocolo *https* con autenticación de cliente.

Cuando la notificación se recibe en la FNMT-RCM, esta envía un correo electrónico a los destinatarios avisándoles de la existencia de una notificación disponible depositada en sus DEUs e incluyendo un link que permita a cada usuario ir a su DEU con mayor facilidad y rapidez. De manera opcional, y siempre y cuando el notificador así lo haya solicitado, este aviso podrá ser enviado también al teléfono móvil del destinatario/s por medio de un mensaje corto SMS.

El ciudadano que se conecta con su DEU debe estar en posesión de un certificado digital emitido por la FNMT-RCM, así como de su clave privada, de manera que se pueda proceder a su autenticación y a la comprobación de la validez de su certificado.

Una vez que el ciudadano se ha autenticado se le muestra la pantalla de acceso a su DEU, invitándole a firmar un comprobante de acceso para poder visualizar sus notificaciones. Una vez que esta acción se ha producido se guarda esta firma y se le muestra un Webmail con acceso a sus notificaciones.

Si el notificador solicitó acuse de recibo, el notificado estará obligado a firmar un nuevo comprobante de acceso a esa notificación y esa prueba será enviada al notificador y quedará custodiada en la FNMT-RCM.

El sistema permite que, una vez leída una notificación, esta pueda ser respondida por el notificado, de manera que el notificador pueda recibir dicha respuesta.

Cuando una notificación es enviada se selecciona un periodo de validez de la misma, de manera que si transcurrido ese periodo no se ha recibido confirmación de acceso, se podrá establecer un método alternativo de envío de notificación. Es en este momento cuando entraría en juego el concepto de correo mixto.

6.1.3 La experiencia del INE

Introducción

El Instituto Nacional de Estadística (INE) se configura como un órgano administrativo autónomo y adscrito al Ministerio de Economía y Hacienda a través de la Secretaría de Estado de Economía.



Su actividad está fundamentalmente regulada por la Ley 12/1989 de la Función Estadística Pública (LFEP) además de los Reglamentos europeos que se promueven en el área estadística^{xxi}. La producción estadística del INE queda explicitada en las operaciones que le son atribuidas en el Plan Estadístico Nacional, de vigencia cuatrienal, y los distintos programas anuales. Estos programas anuales pueden incorporar operaciones que, por razón de urgencia o exigencia europea, deban realizarse sin que hayan sido previamente contempladas en el Plan Estadístico Nacional^{xxii}.

El propósito del INE es conseguir que los ciudadanos, las empresas, los investigadores, las organizaciones públicas y privadas y las Administraciones Públicas conozcan y utilicen adecuadamente la información producida por el Sistema Estadístico Nacional en la toma de sus decisiones. Ello conlleva producir estadísticas adecuadas, fiables y consistentes, en plazos oportunos, de acuerdo con las necesidades de los usuarios, con lo establecido en el Plan Estadístico Nacional y con lo acordado con los organismos internacionales.

Entre las funciones del INE, además de la citada producción de estadísticas, también se encuentra, atribuida por la Ley 7/1985 Reguladora de las Bases del Régimen Local, la coordinación de los Padrones municipales de todos los ayuntamientos y de éstos con el Padrón de españoles residentes en el extranjero para subsanar posibles errores y evitar duplicidades entre los mismos. Asimismo el INE, a través de la Oficina del Censo Electoral, está encargado de la formación y mantenimiento del Censo Electoral (Ley Orgánica 5/1985 del Régimen Electoral General).

Existe pues una doble vertiente en el trabajo del INE: de una parte la producción estadística de censos y encuestas y de otra la tarea de coordinación y mantenimiento de registros administrativos que le son encomendados. En ambas tareas, el impulso de las nuevas tecnologías de comunicación se revela muy importante para la mejora de la calidad estadística y de la eficacia administrativa. Y en ambas, tiene especial importancia la relación que se establece entre un órgano de la Administración y los ciudadanos entendidos en sentido amplio (personas físicas, personas jurídicas y entes sin personalidad) tal como hace la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP).

Reducción de carga a las empresas.

En la realización de operaciones estadísticas, el INE, según lo establecido en la LFEP, puede solicitar datos de todas las personas físicas y jurídicas, nacionales y extranjeras, residentes en España. Las estadísticas para cuya elaboración se exigen datos con carácter obligatorio se establecen por ley. Pero más allá de la obligatoriedad, la base de la relación con los informantes de las operaciones es, fundamentalmente, la confianza que éstos depositan en los órganos estadísticos. Esta confianza es, a su vez reforzada por los principios recogidos en la LFEP y en el Código de Buenas Prácticas de las Estadísticas Europeas: garantía de secreto estadístico sobre las informaciones

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

individuales, proporcionalidad en las demandas de información de acuerdo a los fines de cada operación, etc.

En los últimos ocho años, se ha duplicado tanto el número de operaciones como el de cuestionarios recogidos en encuestas por muestreo. Esto se debe, en buena parte, a exigencias de la Unión Europea que confluyen, en el caso español, con las necesidades de las administraciones autonómicas que, dada su capacidad competencial, requieren datos para formular sus propias políticas locales.

Las oficinas de estadística deben responder a este fenómeno al tiempo que, necesariamente, han de tener en consideración la carga que supone para los informantes la respuesta a un número cada vez mayor de encuestas.

En este contexto, el INE consideró prioritario diseñar una estrategia a corto, medio y largo plazo que aligerase la carga administrativa que soportan las empresas como consecuencia de los requerimientos estadísticos. En el año 2003 se estableció un grupo de trabajo con este objetivo y se diseñaron un conjunto de proyectos destinados a mitigar esta carga desde dos puntos de vista:

- La reducción de la carga objetiva, integrada esencialmente por el coste y el tiempo que necesitan los informantes para cumplimentar las obligaciones estadísticas. La coordinación y cooperación entre administraciones así como el uso racional de fuentes administrativas serán los más importantes puntos de apoyo en este aspecto.
- La reducción de la carga subjetiva, basada en la percepción del informante. Aunque la carga percibida es función de la carga real, hay ciertas características que hacen que merezca la pena considerarla separadamente: el tamaño de la empresa informante, el periodo en que se realiza la recogida, los incentivos que puedan recibir los informantes por la colaboración son factores que influyen en esta percepción. Además, la tecnología puede jugar un importante papel al facilitar la extracción y transmisión de la información que es requerida a las empresas.

Aprovechando las oportunidades que las tecnologías brindan para mejorar la relación con los informantes se dispone, desde 2005, de la posibilidad de que las empresas puedan cumplimentar sus cuestionarios por Internet, un canal añadido a los ya tradicionales de envío por correo postal, fax o teléfono, que pretende incidir en la reducción de carga que soportan permitiendo, en algunas operaciones, el envío de ficheros XML con información que puede generarse directamente de los sistemas de información de las empresas.

El sistema ARCE



El sistema ARCE (Almacenamiento y Recogida de Cuestionarios Económicos)^{xxiii} permite a las empresas la cumplimentación de los cuestionarios de las encuestas económicas del INE a través de Internet.

Características generales del sistema

ARCE es un sistema que se encuentra completamente integrado en el procedimiento de recogida habitual de las encuestas económicas, lo que permite a cada empresa decidir el modo de remisión de la información entre una variedad de canales que incluyen el correo postal, el fax o el teléfono además de la cumplimentación electrónica. En los procesos de tratamiento de la información se asegura la integración de los canales y el conocimiento inmediato del registro de cualquier cuestionario de forma que se eviten duplicidades, reclamaciones de envío, etc.

Inicialmente, las empresas reciben del INE un cuestionario en papel junto con las claves que permiten el acceso al sistema ARCE donde pueden cumplimentar la información del cuestionario en forma electrónica.

El sistema permite el registro de los usuarios lo que facilita en lo sucesivo la cumplimentación de cualquier cuestionario para ese usuario, recibiendo comunicaciones a través del correo de esperar el envío postal.

Además el sistema presenta las siguientes ventajas para los informantes:

- Permite realizar pruebas de cumplimentación de cuestionarios.
- Permite elegir la lengua de cumplimentación de los cuestionarios.
- El cuestionario generado electrónicamente tiene la misma apariencia que el cuestionario en papel para facilitar la búsqueda de informaciones a los usuarios ya familiarizados con los cuestionarios en papel.
- Avisos personalizados de cumplimentación de información.
- Entrega de un certificado de la cumplimentación y posibilidad de obtener copia de la misma.
- Puede conocerse el histórico de colaboraciones y los últimos cuestionarios cumplimentados.
- Posibilidad de obtener directamente los últimos datos publicados de la encuesta que está cumplimentando así como información metodológica de interés: objetivos de la encuesta, principales características de la operación, etc.
- En algunas operaciones puede obtenerse información estadística a medida respecto al sector de actividad al que pertenece la empresa.
- Ayudas en línea para la cumplimentación.
- Cargas de ficheros XML generados directamente por los sistemas de información de las empresas y que pueden dar respuesta directa a los cuestionarios.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Se observa una mayor calidad en la recogida de información por este sistema lo que repercute en un menor tiempo de depuración de los datos tanto para el INE como para los informantes que, a menudo, deben aclarar la causa de las inconsistencias detectadas. De esta forma, el número de contactos que recibe el informante es menor, como también es menor el tiempo empleado en estas aclaraciones.

Implantación del sistema y evolución del grado de utilización

El sistema ARCE entró en funcionamiento el 1 de diciembre de 2005 con las encuestas de Índice de Comercio al por Menor y la Estadística de Transporte de Viajeros. Actualmente integra todas las encuestas económicas tanto coyunturales como estructurales salvo las encuestas medioambientales.

El siguiente gráfico recoge la evolución mensual del porcentaje de cuestionarios recibidos a través de ARCE respecto al total de cuestionarios recibidos desde enero de 2006 a diciembre de 2007 (del 10,17 al 20%).

Se observa una evolución positiva en la utilización de ARCE y parece que aún no se ha alcanzado un punto de estabilización.

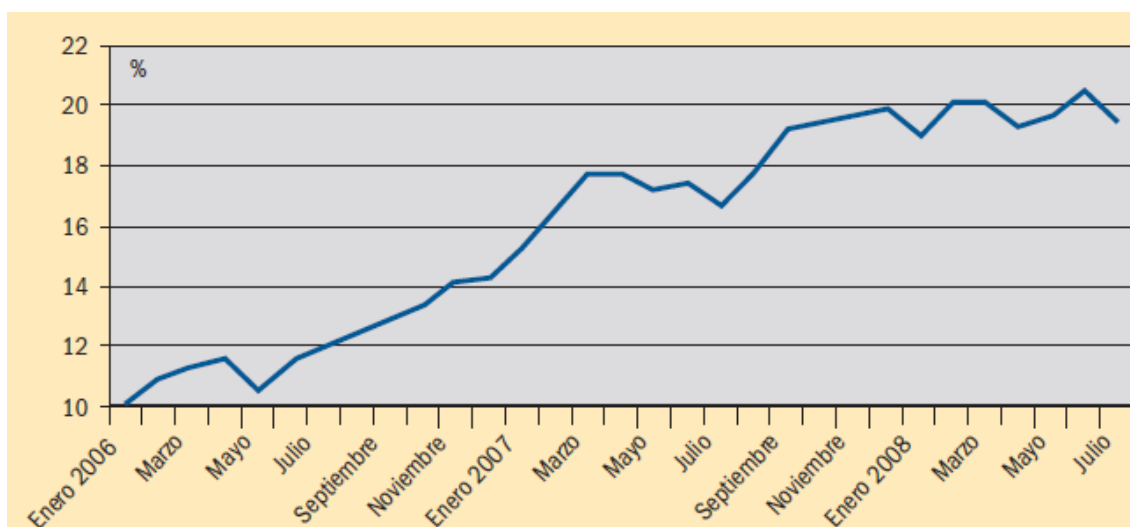


Imagen 6-7 Evolución de recibidos ARCE sobre total recibidos por mes de referencia

Medidas para promover la utilización de ARCE

Frecuentemente, los canales alternativos en la recogida de información tienen un periodo de asimilación por los usuarios en el que conviene desarrollar acciones de promoción. En particular, desde 2006 se han venido realizando las siguientes acciones:

- En primavera de 2006 se editó un tríptico y un señalador de página sobre ARCE para su distribución entre los informantes.
- En octubre de 2006 se realizó el envío de correos electrónicos a las unidades informantes de encuestas coyunturales industriales y del Índice



de Comercio al por Menor y de Transporte de Viajeros, dando a conocer el sistema y las ventajas de cumplimentar la información a través de ARCE.

- En diferentes ocasiones se ha realizado el envío de comunicaciones a los Delegados Provinciales del INE comunicando los avances tecnológicos que se incluían en el sistema, las tasas de respuesta conseguidas e instando a que todo el personal de recogida realizase promoción de ARCE entre los informantes con los que contactarían.
- A finales de 2007 se realizó una encuesta entre informantes para conocer las causas por las que no usaban el sistema:
 - El 50% de los informantes decía preferir otros medios.
 - El 25% no conocía la existencia de este servicio.
 - El 11% indicaba tener problemas técnicos.
 - El 7% no disponía de acceso a Internet.
 - El 3% no lo creía seguro.

Desarrollos previstos

- Actualmente se trabaja para conseguir un nivel de accesibilidad de la aplicación que responda a las actuales exigencias normativas en esta materia.
- Se pretende ampliar la posibilidad de remitir cuestionarios en formato XML en otras operaciones estadísticas añadidas a las actualmente existentes.
- Está previsto incluir una página personalizada dedicada a la unidad informante.
- Se estudia también la posibilidad de incluir la totalidad de los controles de validación en los cuestionarios electrónicos. Esto incrementará la calidad de las informaciones recibidas aunque puede tener algún efecto pernicioso sobre las tasas de respuesta obtenidas por esta vía.
- Se está diseñando la integración de las plataformas que componen el sistema de recogida de datos de encuestas económicas en una sola aplicación que permita el acceso tanto de los informantes como de los responsables de la recogida en el INE para obtener información puntual del estado de recogida de cualquier operación estadística y de la colaboración de cualquier unidad informante.

Intercambio de información entre Administraciones y la reducción de carga administrativa a los ciudadanos

Ya se ha señalado que un adecuado intercambio de información entre Administraciones Públicas de la información contenida en los registros administrativos, puede servir a efectos estadísticos para la reducción de carga que soportan ciudadanos y empresas. El INE ya trabaja en estos intercambios con otros organismos de la Administración General.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Los siguientes proyectos, relacionados con la coordinación del Padrón Municipal de Habitantes y comunicación de datos padronales, inciden también en la reducción de carga administrativa para los ciudadanos, que en este caso no viene derivada de la actividad estadística. Entre sus objetivos está dar respuesta a la demanda de supresión del certificado de empadronamiento establecida en el Real Decreto 523/2006 y encajan, estos proyectos, en las siguientes disposiciones de la LAECSP:

- Art 3.5 y 3.7 que establecen entre los fines de esta ley los de intentar contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y eficiencia de las mismas así como al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas.
- Art. 6.2 que establece el derecho de los ciudadanos a no aportar datos y documentos que obren en poder de otra Administración Pública.
- Art. 9 que establece que cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y que sean necesarios para la tramitación o resolución de los procedimientos de su competencia.
- Art. 27.6 que insta a las Administraciones Públicas a utilizar preferentemente medios electrónicos en las comunicaciones entre ellas.

Sistema IDA_Padrón

Este sistema establece un servicio seguro de intercambio de datos padronales entre las Corporaciones Locales (CL) y el INE, cuya finalidad es permitir las tareas de coordinación que el INE tiene encomendadas que cumple con los siguientes objetivos:

- Facilitar el intercambio de información entre las CL y el INE.
- Comunicaciones seguras de bajo coste, utilizando protocolos HTTPS de Internet y en su caso utilizando certificados digitales para el cifrado/firmado de la información cuando el protocolo de intercambio es SMTP/POP3 .
- Multicanalidad y operaciones en modo desatendido. Para no discriminar por razones técnicas a las CL, el intercambio de información puede realizarse por medios manuales en soporte magnético o por medios telemáticos de forma atendida (subsistema IDA_Web) o de forma desatendida (subsistema J_INE).
- Consultas de estados de tramitación. Todos los intercambios de ficheros, se registran en el LOG de actividad, que está disponible por medio de IDA_Web, para que en todo momento, la CL conozca en qué situación se encuentra el fichero intercambiado.
- Independencia entre datos y aplicaciones. El sistema se basa en el intercambio de ficheros estandarizados que son el resultado final de las diferentes aplicaciones de gestión por ello, el sistema de intercambio de datos es independiente de la aplicación que los genera.



- Reducción del tráfico de información. Con una validación de los datos a intercambiar en origen (subsistema J-IdaVal), se consigue que la CL pueda conocer y tratar errores comunes, antes de intercambiar el fichero al INE y con ello reducir el tráfico de información

De forma resumida, se plantea el esquema funcional del sistema:

Cuando la CL debe enviar al INE los datos de variaciones padronales, podrá elegir cualquiera de las tres vías permitidas.

- Envío en soporte físico a la Delegación Provincial del INE que validará el fichero y lo cargará en las bases de datos centrales a través de la Intranet del INE.
- En modo atendido. Por medio de J_IdaVal, tratará el fichero (valida y comprime) y en su caso lo cifrará y firmará (optativo) y lo enviará manualmente al INE por medio de IDA_Web.
- En modo desatendido. Por medio de J_INE, a través de J_IdaVal, realizará los procedimientos de validación, compresión, cifrado/firmado (requerido) y se enviará automáticamente al INE por medio de protocolo SMTP/POP3.

Cualquier intercambio de información se registra en el LOG de actividad (disponible a través de IDA_Web). Cuando el envío es por medios telemáticos, se trata por medio de J_Telco para: comprobar la firma del fichero accediendo a @Firma, descomprimir/descifrar el fichero, realizar el apunte en el Registro Telemático del INE y devolviendo el acuse de recibo.

Tras ser procesados los ficheros recibidos en el INE, se pueden detectar incidencias o errores que son comunicados a la CL por la misma vía y con las mismas características con que fueron recibidos en el INE.

Finalmente, el resultado final de este procedimiento de validación y carga de ficheros de variaciones es la actualización y consolidación de los correspondientes padrones municipales y de otras informaciones referentes a errores/incidencias y de tratamientos manuales. Toda esta información, se pone a disposición de las CL a través de protocolos HTTPS (IDA_Cónsul).

Asimismo, una de las fases más importantes en la coordinación padronal del INE, es el procedimiento de obtención de las cifras oficiales de población resultantes de la revisión anual del Padrón municipal que requiere el tratamiento y contraste simultáneo y en pocos días de diferentes ficheros (fichero de cifras del ayuntamiento, fichero de reparos, fichero de alegaciones, etc...). Todos estos ficheros pueden ser descargados o enviados mediante IDA-Padrón.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

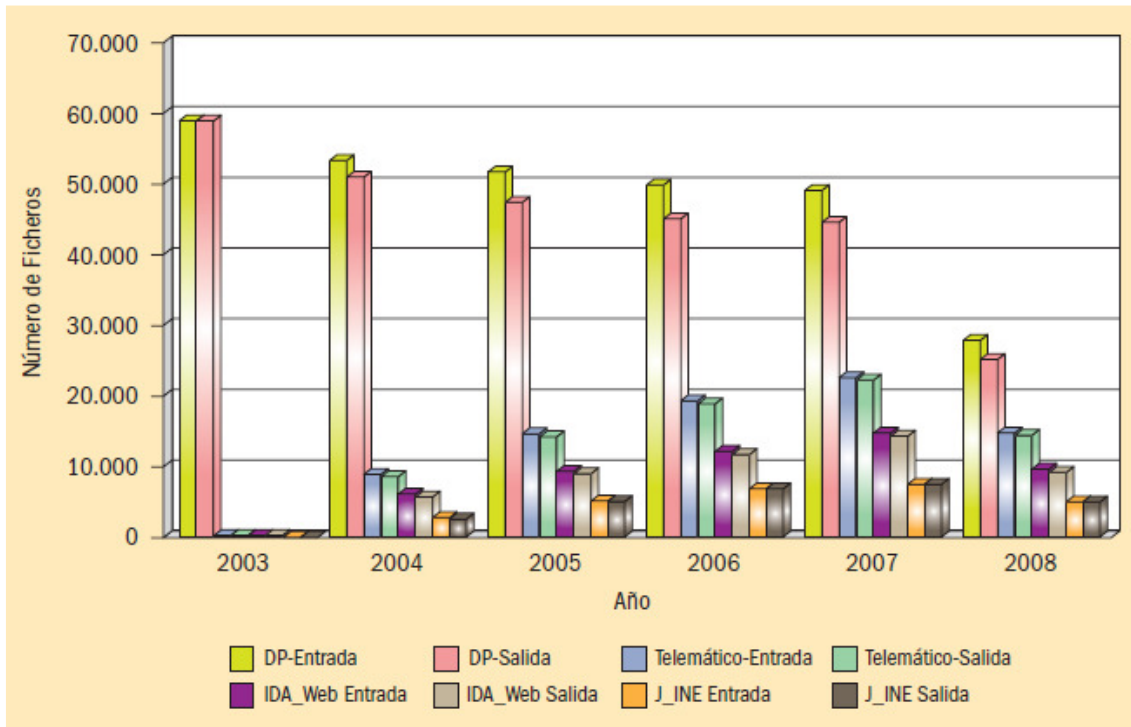


Imagen 6-8 Intercambio de Ficheros IDA_Padrón

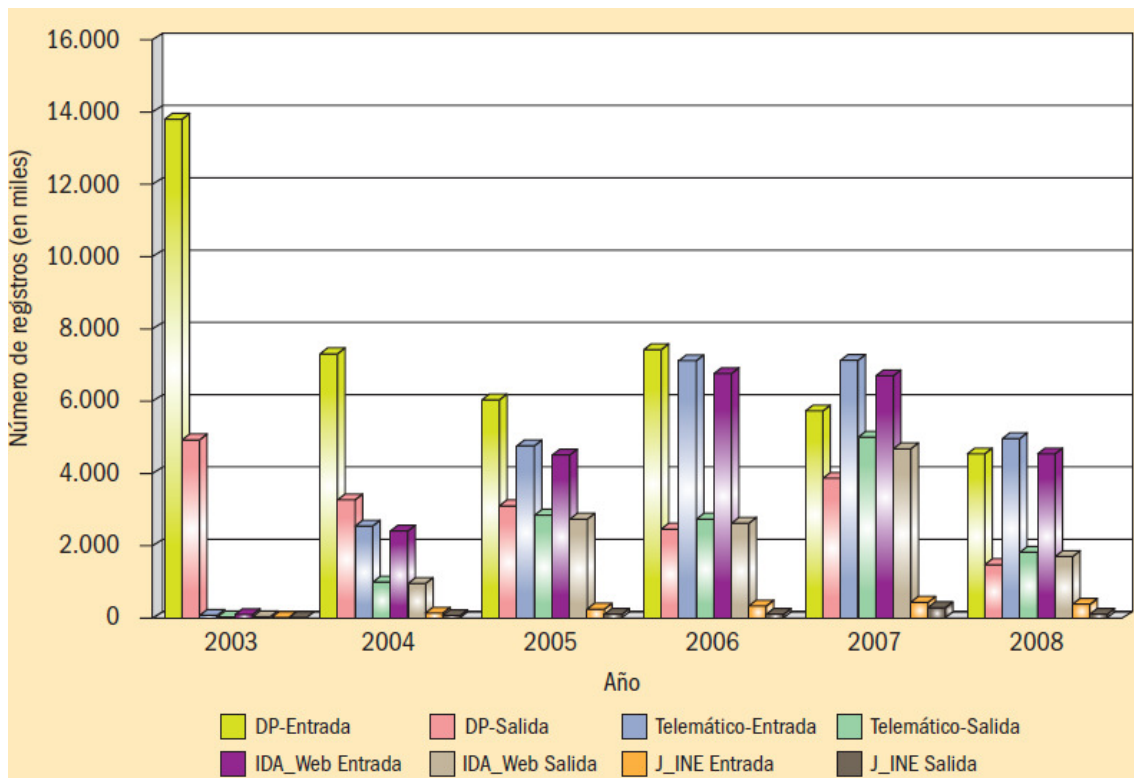


Imagen 6-9 Intercambio de Registros IDA_Padrón

Servicio de Verificación de Datos de Residencia (SVDR) y Servicio de Consulta de Datos Padronales del Consejo General del Poder Judicial (SCDP-CGPJ)

Estos dos sistemas, diferentes en su concepción, en la práctica son similares pues ambos acceden a la base del INE. En el SVDR, los organismos adheridos utilizan el MAP como pasarela de interconexión con el INE a través de la Intranet Administrativa, mientras que el SCDP-CGPJ realiza una conexión directa al INE a través del Punto Neutro Judicial.

En SVDR se consigue dar respuesta al artículo 6 de la LAECSP en cuanto a la eliminación de la necesidad de que el ciudadano para determinados procedimientos administrativos presente el correspondiente certificado de empadronamiento.

Por el contrario, el SCDP-CGPJ lo que pretende es dar un servicio a la Administración de Justicia que precisa obtener el dato de domicilio de las personas incurso en procedimientos judiciales y de esta forma lograr una eficaz tutela de los derechos de los ciudadanos y una agilización de los procesos.

Las solicitudes de uno y otro sistema, se realizan mediante Servicios Web basados en protocolos estándar (SOAP sobre HTTPS) y con un formato de intercambio estándar (XML) y para garantizar el contenido e integridad de los mensajes, la identidad de los remitentes y el no repudio, se utiliza la recomendación de W3C XMLDSIG.

En las siguientes figuras puede verse el esquema funcional de ambos sistemas así como el número de documentos que han sido obtenidos por los usuarios.

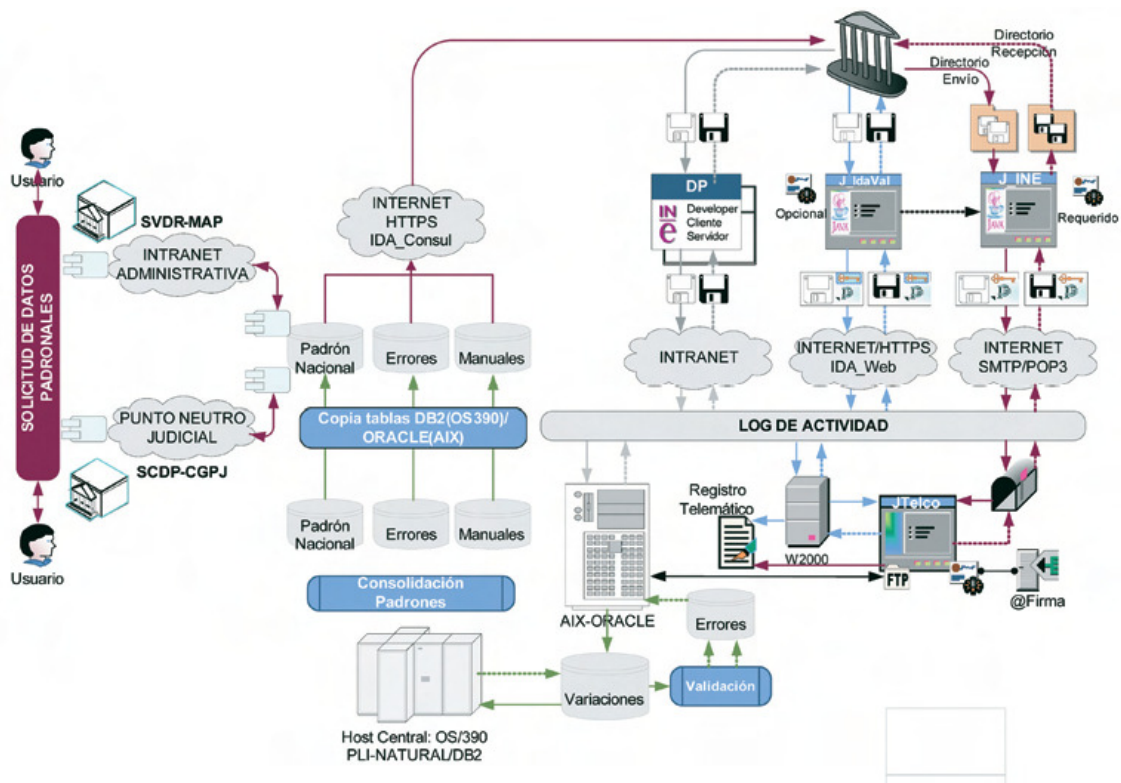


Imagen 6-10 .Esquema Funciona

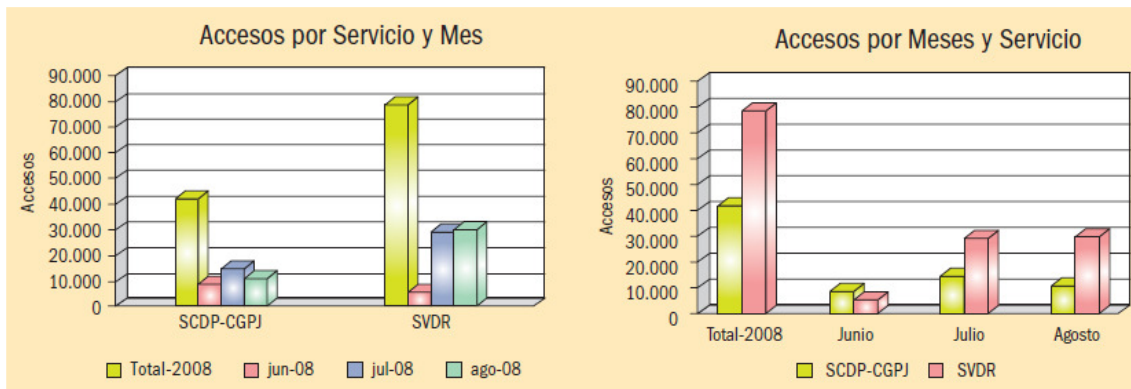


Imagen 6-11 Accesos registrados del SVDR y del SCDP-CGPJ

6.1.4 Portal 060

Es el portal de referencia en el ámbito público y concentrador de las relaciones, interacciones y transacciones entre ciudadanos y Administraciones Públicas.

La Red 060 es una iniciativa del Ministerio de la Presidencia, que permite a los ciudadanos y a las empresas acceder a los servicios públicos de cualquiera de las tres administraciones con las que tienen que relacionarse (Administración General del Estado, autonómica y local).

Pretende facilitar la vida a ciudadanos y empresas, de manera que puedan acceder a los servicios sin necesidad de conocer la estructura interna de todas las administraciones o lugares físicos o virtuales donde se ubican.

En este sentido el portal de la Red 060 actúa como la referencia en el ámbito público para la atención al ciudadano y concentrador de las relaciones, interacciones y transacciones entre ciudadanos y Administraciones Públicas.



Imagen 6-12 Portal de la red 060

El gran objetivo de la Red 060 es integrar servicios de todas las Administraciones en un punto único para mejorar la atención ciudadana:

- Mediante la construcción de un sistema integral de atención al ciudadano, de forma coordinada entre las tres administraciones.
- Que ofrezca múltiples canales y servicios avanzados e interactivos basados en la integración de los procesos administrativos de información y gestión.
- Que fomente la participación del ciudadano, la transparencia y accesibilidad de la actividad pública.

Servicios de la Red 060

El gran objetivo de la Red 060 es integrar servicios de todas las Administraciones (estatal, regional y local) para mejorar la atención ciudadana:

- Mediante la construcción de un sistema integral de atención al ciudadano, de forma coordinada entre las tres administraciones.
- Que ofrezca múltiples canales y servicios avanzados e interactivos basados en la integración de los procesos administrativos de información y gestión.
- Que fomente la participación del ciudadano mediante herramientas como foros en Internet y la transparencia y accesibilidad de la actividad pública.

Canales disponibles

- Oficinas locales de atención presencial. De esta red de oficinas ya forman parte más de 1300 ayuntamientos y 13 comunidades autónomas. Se permite realizar desde ellas los trámites.
- El teléfono 060 donde se facilita información sobre los servicios ofrecidos por todas las administraciones.
- Portal de Internet www.060.es donde se recopilan todos los servicios electrónicos ofrecidos por todas las administraciones.

Servicios de la Red 060

Los ciudadanos pueden obtener información sobre trámites y servicios o realizar determinadas gestiones. Ejemplos de estos servicios son:

- Pedir cita médica.
- Hacer la declaración de la renta.
- Alquilar una vivienda.
- Pedir cita para renovar el DNI.
- Etc.

Hasta la fecha uno de los grandes problemas de la Administración española era que el ciudadano tenía que saber a cuál de las tres Administraciones dirigirse para la prestación de un determinado servicio o la consulta de información. La Red 060 se convierte por tanto en un punto único de acceso que simplifica la relación del ciudadano con la Administración al no tener que



saber qué Administración es la competente en su problema, la Red 060 lo determinará por él.

Se pretende en este sentido la creación de un espacio virtual aglutinador y clasificador de servicios interactivos, personalizados y de valor añadido en las vertientes de información y transacción. El portal 060 será el instrumento del canal Internet del repositorio de datos y servicios 060 (que dará servicio a otros canales como el teléfono, los SMS, oficinas presenciales y TDT).

Es por tanto el sitio de referencia para que un ciudadano resuelva cualquier asunto. Desde la tramitación de un permiso de obra, el pago de una multa o la búsqueda de información de las becas a las que puede acceder para los estudios de sus hijos. El portal le llevará directamente al servicio y Administración concreta en cuestión.

6.1.5 La Red SARA

El artículo 43 de la Ley 11/2007 establece la obligación de crear una red de comunicaciones que interconecte las Administraciones Públicas españolas entre sí, con otras redes de las Instituciones Europeas y de otros Estados miembros, para el intercambio de información y servicios entre ellas.

La Red SARA permite la interconexión de las administraciones públicas, facilitando el intercambio de información y servicios entre ellas. A través de la Red SARA los Ministerios, las Comunidades Autónomas, los Entes Locales y otros organismos públicos pueden interconectar sus redes de una manera fiable, segura, capaz y flexible.

Con esta interconexión se pretende por una parte la prestación de servicios horizontales para todas las administraciones tales como, por ejemplo, los servicios de validación de firma electrónica que ofrece *@Firma* o servicios como el registro electrónico común, de modo que los diversos organismos de las tres administraciones ya no se tienen que preocupar de implementarlos por su cuenta, sino que pueden apoyarse en los servicios que se ofrecen desde esta red.

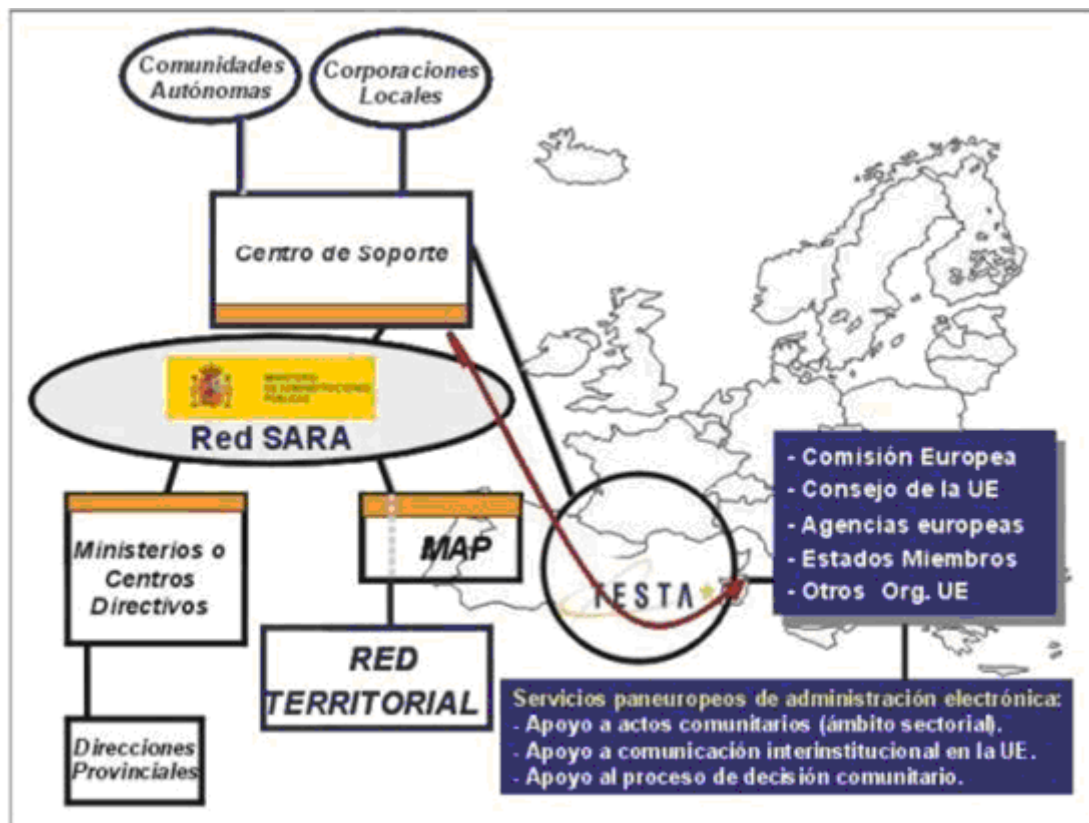


Imagen 6-13 Estructura de la red SARA

Por otra parte se pretende facilitar con esta interconexión la implementación de servicios interadministrativos, es decir, que requieren interacción entre administraciones o diferentes órganos de una misma Administración, de modo que se puedan ofrecer servicios electrónicos sencillos al ciudadano, aunque en su implementación requieran una interacción compleja entre diferentes instituciones. El ejemplo por excelencia de un servicio de este tipo sería el cambio de domicilio, ya que implica trámites en las tres administraciones estatal, autonómica y local, y sin embargo por la vía electrónica se convierte de cara al ciudadano en un solo acto.

Además, a través del enlace de la Red SARA con la red transeuropea TESTA las Administraciones Públicas españolas se pueden interconectar con redes de instituciones europeas y de administraciones de otros Estados miembros de la UE, para el despliegue y acceso a los servicios paneuropeos de administración electrónica.

Características de la red SARA:

- **Fiabilidad:** La red SARA está diseñada con tecnología de última generación VPLS (*Virtual Private LAN Services*) que la dota de gran capacidad de transmisión de datos. Además, su diseño y tecnología le permiten ofrecer una muy alta disponibilidad para garantizar en todo momento la continuidad del servicio, lo cual se complementa con la existencia de un Centro de Soporte 24 x 7 con unos exigentes acuerdos de nivel de servicio (SLA's).



- Seguridad: SARA implementa medidas de seguridad entre las que destaca el establecimiento de VPNs. Es una red extremadamente segura en la que todo el tráfico circula cifrado por la Troncal. De esta manera queda asegurada la confidencialidad de la información que viaja a través de la red SARA.
- Capacidad: Esta red cuenta con un ancho de banda de 1 Gbps en Ministerios y CPD's (10 veces más que su predecesora), y 100 Mbps en cada Comunidad Autónoma (50 veces más caudal) lo que permite asegurar la capacidad para absorber las exigentes demandas tanto de las aplicaciones existentes como de los nuevos servicios de administración electrónica.
- Calidad de Servicio (QoS): La tecnología VPLS utilizada en el diseño de la red SARA permite dotarla de mecanismos de calidad de servicio para tratar cada dato transmitido de acuerdo a su naturaleza (voz, video, datos), lo cual establece un nuevo abanico de servicios multimedia a incorporar.
- Punto-multipunto: La red SARA está diseñada con un modelo de conexión punto-multipunto (*todos con todos*) mediante el cual no existe un nodo central en el que convergen todas las conexiones y por tanto se eliminan posibles puntos únicos de fallo. Esta topología se complementa perfectamente con la arquitectura de seguridad existente, en la cual los mecanismos de seguridad están distribuidos en cada nodo, si bien la política es homogénea y con gestión centralizada.
- Flexibilidad: En el diseño de la red SARA se ha tenido en cuenta la posibilidad de que esta red pueda evolucionar y crecer a medida que lo hagan las necesidades de la Administración.

Organismo

Ministerio de Presidencia. Dirección General para el Impulso de la Administración Electrónica.

Servicios vía SARA

En ese sentido el Ministerio de la Presidencia ofrece a través de la Red SARA un conjunto de servicios horizontales, utilizables por cualquier Administración, que ayudan a acelerar el proceso de implantación de la Administración electrónica.

Plataforma De Firma Electrónica @Firma

Con la Plataforma de servicios de validación y firma electrónica *multi-PKI @Firma*, las Administraciones Públicas disponen de los instrumentos necesarios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva.

Con esta plataforma se resuelve el problema de tener que conectar con diferentes autoridades de certificación para la validación de los certificados emitidos cada uno de ellas. *@Firma* hace de puente con todas ellas ofreciendo un único punto de acceso para las administraciones sin tener que preocuparse de la Autoridad de Certificación (CA) a la que pertenece un certificado concreto a validar. Por otra parte el mantenimiento para los organismos es prácticamente nulo ya que la incorporación de nuevas CAs se convierte en transparente para ellos.

La importancia de *@Firma* la avalan sus cifras, según los últimos datos del CTT la autoridad de sellado de tiempo de *@Firma, TS@*, ha experimentado una rápida evolución en el número de sellados de tiempo mensuales. Durante el mes de Abril se registraron dos millones de sellados de tiempo mensuales, así como más de un millón de validaciones de firmas y certificados.

Este servicio está teniendo también un papel destacado dentro de las iniciativas de *eGovernment* de la Unión Europea dentro del marco del programa IDABC (*Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*) llevando a cabo diversos estudios sobre la creación de servicios federados de validación de certificados y firmas electrónicas.

VALIDe

Las Administraciones Públicas ofrecen a los ciudadanos servicios públicos electrónicos en los que se necesita firma electrónica y métodos avanzados de identificación o autenticación basados en certificados digitales. Debido a los múltiples certificados que pueden utilizarse para la identificación y la firma, implantar sistemas que soporten todas las funcionalidades y relaciones con las CAs puede resultar complejo y costoso.

VALIDe es un sistema que determina la validez y vigencia de los certificados digitales que se indiquen, a través del servicio ofrecido por la plataforma de firma electrónica *@Firma*. Esto permite validar los certificados de múltiples infraestructuras de clave pública (PKI), entre ellas la del DNI electrónico.

Además, dispone de múltiples utilidades de valor añadido, entre las que se encuentran la generación y validación de firmas electrónicas en múltiples formatos.

Este servicio funciona como un servicio no intrusivo o cerrado, que puede ser utilizado por todos los interesados de las distintas Administraciones Públicas, tanto estatal, como autonómica o local.



Los servicios ofrecidos a los organismos se pueden catalogar en cuatro bloques:

- Validar Certificado: permite validar el estado de un certificado digital emitido por cualquier entidad de servicio de certificación reconocida, tanto en autenticidad, vigencia y estado de no revocación.
- Validar Firma: permite consultar la validez de un documento firmado electrónicamente con múltiples formatos y tipos de certificados, como facturas electrónicas, contratos, etc.
- Realizar Firma: permite firmar electrónicamente un documento con cualquier certificado reconocido con las máximas garantías de integridad y autenticidad.
- Demostrador de servicios de @Firma: proporciona un demostrador del funcionamiento de los servicios Web para las Administraciones que deseen integrar los servicios de validación y firma de la plataforma @Firma en sus servicios electrónicos, para evaluar todos los servicios y realizar las pruebas funcionales necesarias.

Verificación de Datos de Identidad (SVDI) y Datos de Residencia (SVDR)

En la Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos, LAECSP, se reconoce el derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados.

Sin embargo, en los procedimientos administrativos, ha sido habitual la petición de documentos acreditativos de identidad y del lugar de residencia a efectos de verificar estos datos personales. Con el Real Decreto 522/2006, y Real Decreto 523/2006, de 28 de abril, se suprime la necesidad de aportar estos documentos en todos los procedimientos de la AGE y de sus organismos públicos vinculados o dependientes. No obstante, la verificación de estos datos, sigue siendo esencial para la tramitación de los procedimientos.

El Servicio de Verificación de Datos de Identidad (SVDI) y de Datos de Residencia (SVDR), permite que cualquier organismo de la Administración, pueda verificar dichos datos, sin necesidad de solicitar la aportación de los correspondientes documentos acreditativos, permitiendo así hacer efectiva esta supresión.

Las consultas a los servicios de verificación de datos, se pueden realizar de dos maneras:

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- De forma automatizada, desde una aplicación de gestión de un trámite, adaptadas para invocar los servicios Web proporcionados a través de la Red SARA.
- O bien por un empleado público autorizado mediante un cliente Web.

Supresión de Certificados en Soporte Papel (SCSP)

El derecho del ciudadano a “*no presentar documentos [...], que ya se encuentren en poder de la Administración actuante*”, está reconocido en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los servicios públicos.

Para facilitar ejercer este derecho, se ha definido un sistema de intercambio de datos entre administraciones, basado en el *artículo 15* del Real Decreto 263/1996, modificado por Real Decreto 209/2003, que permite la sustitución de los certificados administrativos en soporte papel por el envío, a través de medios telemáticos y con los requisitos de seguridad previstos, de aquellos datos que sean necesarios para el ejercicio, por un organismo, de sus competencias en el marco de un procedimiento administrativo.

La finalidad del servicio es evitar que el ciudadano tenga que aportar, en sus trámites, certificados o documentos acreditando información que tenga la Administración actuante. Algunos organismos ofrecen en formato digital la información contenida en los certificados en papel, diferenciándose dos casos:

- Los llamados comúnmente "certificados", que deben cumplir las condiciones de certificado telemático (ahora certificado electrónico) descritas en el artículo 14 del Real Decreto 263/1996 modificado por Real Decreto 209/2003, esto es, estar firmado digitalmente por la autoridad competente para expedirlos, y llevar código de verificación para poder comprobar su veracidad en caso de ser impreso.
- La información intercambiada entre organismos de la AGE u otras administraciones, que debe reunir las condiciones del *artículo 15*. Los organismos que más utilizan esta vía son la AEAT y la Tesorería General de la Seguridad Social, utilizando formatos diferentes de intercambio.

Notificaciones Telemáticas Seguras (SNTS)

Tal y como se recoge en la Ley 30/1992, de procedimiento administrativo y en Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos, los ciudadanos tienen el derecho a elegir el lugar de notificación, por tanto podrán decidir que se le notifique en su *Dirección Electrónica Única* (DEU). Por tanto, los Departamentos y organismos de la Administración están obligados a facilitar este derecho.



El objetivo del servicio es facilitar las relaciones entre el ciudadano y la Administración, facilitando un buzón seguro y confidencial en el que pueda recibir todas las notificaciones de la AGE y en particular:

- Agilizar la recepción de las notificaciones que la Administración practica a los ciudadanos y empresas, mediante un sistema de notificación a través de medios telemáticos y con las mismas garantías que aquellas recibidas por vía postal.
- Reducir la burocracia y reducir costes a la Administración.
- Ofrecer una dirección electrónica única con carácter gratuito a todos los ciudadanos y empresas que lo soliciten, en la cual recibir notificaciones telemáticas seguras. También, si ha facilitado una dirección de correo electrónica, recibirá en esa dirección un preaviso de notificación.
- Disponer de un sistema, de uso general para cualquier Organismo público, a través del cual notifiquen vía Internet a los ciudadanos de cualquier comunicación asociada a la tramitación de sus expedientes administrativos.
- Mejorar la imagen que tienen de la Administración los ciudadanos.

Sistema de Interconexión de Registros (SIR)

El Sistema de Interconexión de Registros permite la implantación del concepto de ventanilla única telemática. Permite la transmisión de información registral desde un registro a otro, de forma que se pueda tener conocimiento en tiempo real de la información del asiento registral, en el registro destino, aunque la entrada se haya producido en cualquier registro del sistema, obteniendo una imagen del documento presentado.

La obligación de la AGE de interconectar sus oficinas de registro se recoge en el *artículo 24.4* de la ley 11/2007, de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

El proyecto se inicia en enero de 2007 realizándose el primer piloto en Noviembre de 2008. El sistema permite la interconexión de las oficinas de registro para permitir el acceso a los asientos registrales de las comunicaciones a ellas dirigidas a través de cualquier otro punto, así como la consulta de imágenes de los documentos correspondientes. Abarca el ámbito AGE de Comunidades Autónomas y Entidades Locales.

Para ello, con carácter previo, se ha definido el formato de los documentos electrónicos y los servicios electrónicos necesarios para el intercambio de información entre Registros.

El sistema de intercambio de asientos registrales usa como base el sistema de Mensajería Electrónica de Registros ya existente. Adicionalmente se ha

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

implantado un Centro de Control global de todas las transacciones efectuadas, para el control y seguimiento de cualquier transmisión de información efectuada.

Pasarela de Pagos

La pasarela de pagos pretende mejorar la disposición de la Administración del Estado para adoptar el pago telemático en sus trámites.

Permite al organismo dar un servicio de pago telemático de tasas al Ciudadano a través de Internet. Con esto, se facilita al ciudadano la gestión que debe realizar, ya que, unido al trámite electrónico puede realizar el pago correspondiente de manera sencilla y sin tener que desplazarse a la entidad correspondiente.

Como resultado se consigue:

- Evitar desplazamientos del ciudadano para realizar autoliquidaciones de tasas.
- Hacer posible el pago electrónico en los Organismos de la AGE que lo soliciten.
- Un servicio homogéneo de pago electrónico en la Administración.
- Una elevada seguridad en las transacciones económicas, basado en el uso de certificados electrónicos y de firma electrónica.

Como consecuencia de la integración de Pasarela de Pagos en los Organismos, el ciudadano podrá utilizar un entorno de pago integrado con el trámite a realizar, disponible en la Web del propio Organismo o a través de “*Mis pagos*” en la Red 060.

Requisitos de uso

Por el momento, no requiere convenio con el Ministerio de Presidencia, si bien el Ministerio de Presidencia ha firmado convenios con casi todas las Comunidades Autónomas.

Los Ayuntamientos se conectan a través del nodo de su Comunidad Autónoma, aunque para ello se puede firmar un anexo de adhesión al convenio.

Si no se tuviese acceso a esta red, se puede habilitar temporalmente un acceso a reproducción en algunos de los servicios, como es el caso de @Firma (únicamente mientras se gestiona la integración a la red SARA).



El acceso a la red SARA debe realizarse a través de la Comunidad Autónoma, en caso de desconocer a quién dirigirse se solicitaría apoyo al contacto y soporte mencionados.

Cómo se gestiona el acceso a la Red SARA

Nota: se toma como ejemplo el procedimiento establecido en la Comunidad de Madrid.

En el caso de la Comunidad de Madrid el proceso sería el siguiente:

A) Ayuntamientos a la Red SARA SSL VPN

1. Enviar una solicitud de Acceso SARA, designando un Coordinador Técnico del Ayuntamiento, junto con la petición de alta al sistema de dicho coordinador, a:

Dirección General de Calidad de los Servicios y Atención al Ciudadano

C/ Gran Vía, 18 2ª planta, 28013 – Madrid.

El Coordinador Técnico del Ayuntamiento será el interlocutor técnico con ICM (Informática y Comunicaciones de la Comunidad de Madrid) para:

- Autorizaciones de acceso de los usuarios del Ayuntamiento.
- Reporte de incidencias o problemas del Servicio.
- Cumplimentar el Modelo de solicitud: Ficha de solicitud de alta del Coordinador Técnico www.madrid.org/ayuntamientos_ae.

2. Autorización de usuarios de acceso del Ayuntamiento.

El Coordinador Técnico del ayuntamiento, mediante esta ficha, mantendrá actualizada la relación de usuarios del Ayuntamiento que estén capacitados para el acceso a SARA, a través de este Servicio. Ficha de solicitud de alta de empleados del Ayuntamiento www.madrid.org/ayuntamientos_ae.


Una vez cumplimentada la ficha y firmada por el Coordinador Técnico, se deberá escanear el documento (si no se ha utilizado firma electrónica para la firma del mismo) y se enviará por correo electrónico a la dirección ICM_DASC_PRESIDENCIA@madrid.org.

De esta forma se tiene acceso al servicio Ayuntamientos a la Red SARA SSL VPN a través de un *usuario* y un *password*.

B) Conexión Site to Site. Acceso entre sistemas del Ayuntamiento y Comunidad de Madrid

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Las conexiones “*Site to Site*” se establecen técnicamente entre el Coordinador Técnico del Ayuntamiento y el personal Técnico de la Dirección de Comunicaciones de ICM. El establecimiento del contacto inicial se realizará a través de la Dirección General de Calidad de los Servicios y Atención al Ciudadano y para su inicio es requisito el cumplimentar y remitir el siguiente cuestionario:



(Ficha para la creación de la red privada virtual con la CM a través de Internet)

Administración Local			
Ubicación			
Contacto			
e-mail			Teléfono
Subred GTA cliente (cumplimentar por la CM)	Servicios básicos en Red SARA: <input type="checkbox"/> DNS <input type="checkbox"/> Proxy <input type="checkbox"/> MTA <input type="checkbox"/> NTP <input type="checkbox"/> SOCKS (no operativo aún) <input type="checkbox"/> UDDI (no operativo aún)	Servicios no básicos en Red SARA: <input type="checkbox"/> Aplicaciones Cliente/Servidor <input type="checkbox"/> Otras (Especificar requisitos)	

DESCRIPCIÓN GENERAL

En la Red SARA conviven todos aquellos servicios que conforman la Intranet Administrativa. En concreto el MAP delega en cada Comunidad Autónoma unos servicios generales que pueden servir para alcanzar servicios de la Intranet Administrativa de una forma transparente o con menor o ninguna participación de los intermediarios (“Servicios básicos en Red SARA”). Por otro lado, el ofrecimiento de “Servicios no básicos” en Red Sara obliga a los intermediarios a un encaminamiento directo entre cliente y servicio con las consiguientes acciones técnicas. Pero en ambos casos el diálogo en Red SARA se debe realizar usando el direccionamiento ip GTA que el MAP asigna a las administraciones públicas. Es por ello que a la administración local se le asignará un direccionamiento GTA cliente a usar dentro de la red privada virtual establecida con la CM y que el servicio básico de DNS sólo ofrece registros GTA.

La red privada virtual con la CM se establece a través de Internet teniendo como punto de establecimiento el nombre público de Internet:

accesovpn.madrid.org

Imagen 6-14 Formulario para conexión Site to Site

Requisitos de la VPN A TRAVÉS DE INTERNET

El establecimiento de la red privada virtual se basa en *IPSec* cuyos parámetros de configuración en el extremo de CM son:

- Cifrado: 3DES.



- Firma: Hash SHA-1.
- Autenticación: certificados con verificación local (en CM) de CRL.

El procedimiento a seguir en la emisión de certificados será el siguiente:

El Ayuntamiento generará en su equipo, extremo de la red privada virtual, la solicitud de firma de su certificado (CSR).

El Ayuntamiento enviará por correo electrónico a *< cuenta correo a usar >* el CSR generado en el paso anterior con los siguientes parámetros:

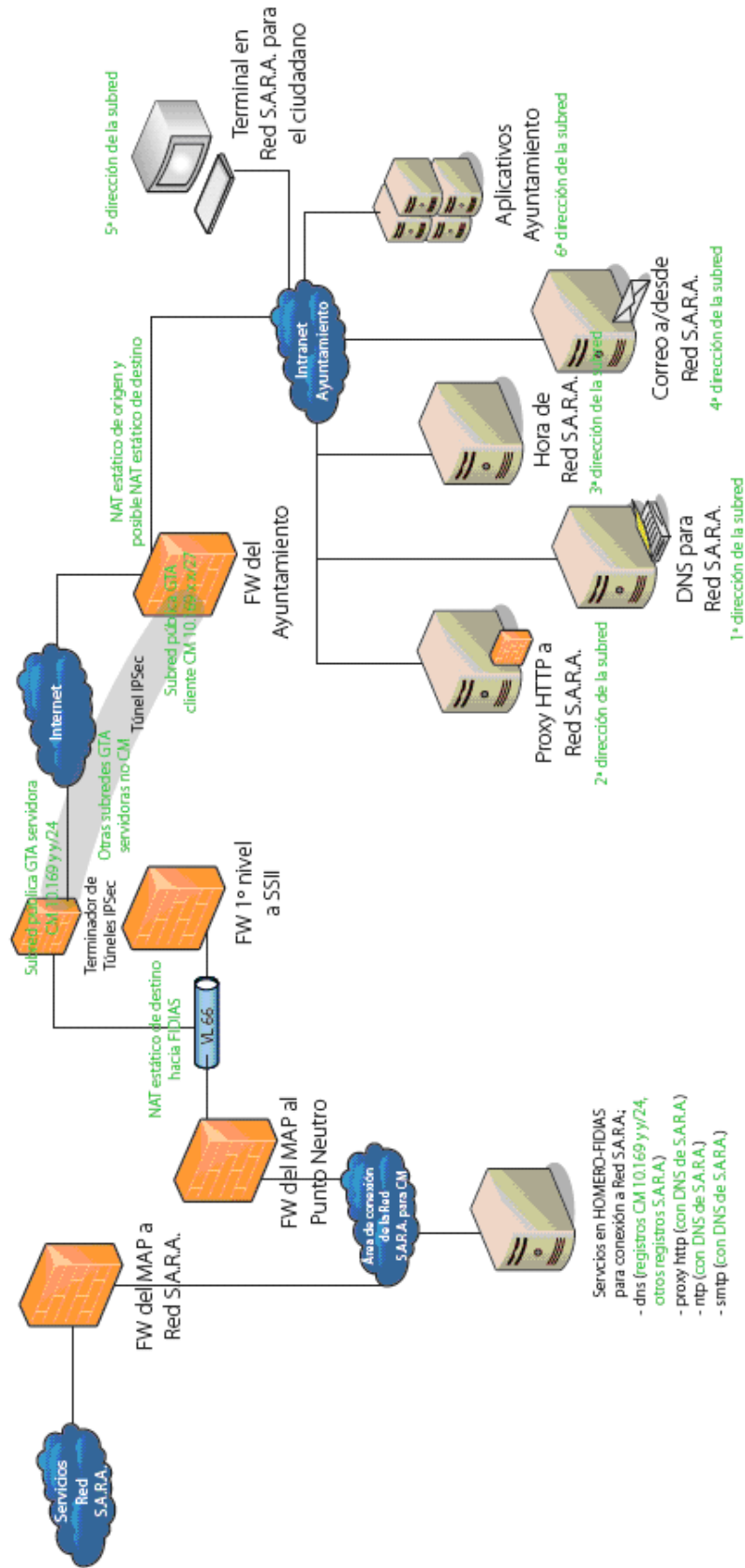
O = "Nombre del Ayuntamiento"

C = es (indica el código del país)

La CM, a la recepción del correo, firmará el CSR y anexará además el certificado raíz de la autoridad de certificación para su instalación en el equipo del Ayuntamiento.

A continuación se muestra una imagen con la interestructura de conexión para la red VPN.

Análisis de la eAdministración e identificación de criterios auditable para la evaluación del grado de implantación



Arquitectura Sistema S.A.R.A.
AyuntamientosSicelSicite

Imagen 6-15 Esquema conexión Red SARA



Posteriormente, es necesario remitir a la Comunidad Autónoma (en este caso, ICM) los siguientes datos:

- CSR con la solicitud del certificado en formato PKCS10 con los siguientes parámetros:
 - CN=Ayuntamiento de XXXXXXXXXX, OU=Comunidad Autónoma , C=ES
 - La IP pública del equipo desde el que se establece la conexión al servidor de túneles.

Y por parte del departamento de mantenimiento y seguridad de la Comunidad (ICM):

- El direccionamiento asignado con el que la entidad debe presentarse 10.xxx.xx.x/xx, así como los parámetros de configuración para la VPN:
 - Fase 1: Cifrado 3DES, Hash MD5. Autenticación con certificado, sin verificación CRL. Grupo DH 2.
 - Fase 2: Cifrado 3DES, Hash MD5., indicando la IP pública del firewall con la que la entidad debe terminar xxx.xx.xxx.xxx, así como los rangos de la red SARA a los que tendrá acceso dicha entidad y que en el caso de querer acceso a servicios tales como @firma, deberá notificar a soporte técnico de dicha herramienta de validación y firma electrónica.

Dificultades más comunes

En el caso de la configuración *Site to Site* a través de la red SARA, y en concreto en el caso de la Comunidad de Madrid, la dificultad estriba en la interlocución y acceso a los responsables de ICM. No se dispone de teléfono de soporte ni correo genérico de acceso público.

Otro de los motivos que dificulta el acceso a la red SARA es la necesidad de cumplimiento de todos los protocolos de actuación en los que implica el contacto con el nivel de soporte inicial que es el propio Ministerio de Presidencia, para después acceder al interlocutor correspondiente de cada comunidad autónoma y por último en este caso, contactar con el organismo encargado de la gestión del Servicio.

En el caso de las administraciones locales, la dificultad de acceso estriba en la necesidad de disponer de *routers* de acceso con la tecnología y sistemas operativos que soporte los protocolos de cifrado y seguridad exigidos para la interconexión a la red SARA.

Como solución se propone que en la ficha explicativa de los servicios y requisitos de acceso a la red SARA se publiquen las tablas de contactos y accesos de cada comunidad autónoma, disponiendo de una dirección de correo y teléfono de soporte.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Para terminar diremos que la red SARA es un instrumento fundamental para seguir avanzando en el desarrollo de la administración electrónica, lo que en definitiva supone mejorar el servicio prestado a los ciudadanos.

6.1.6 @Firma

Es la solución tecnológica en la que se basa la implementación de la Plataforma de validación y firma electrónica del Ministerio de Presidencia. La versión actual de @Firma es la 5.0 y constituye una evolución de la versión 4.0 a partir de la aportación de múltiples Organismos Públicos cooperantes.

Es un producto robusto e integral, desarrollado inicialmente por la Junta de Andalucía, cedido al resto de las Administraciones Públicas con el objeto de fomentar y extender el desarrollo de la Administración Electrónica y la Sociedad de la Información.

Es una solución basada en software libre, estándares abiertos y en java: servidores Web Apache, JBOSS, Sistema Operativo Solaris/Linux, AXIS, etc. Y se puede acceder sin coste alguno ni compromiso con diferentes CAs, a unos 60 certificados de 12 entidades diferentes, entre los que está el DNle.

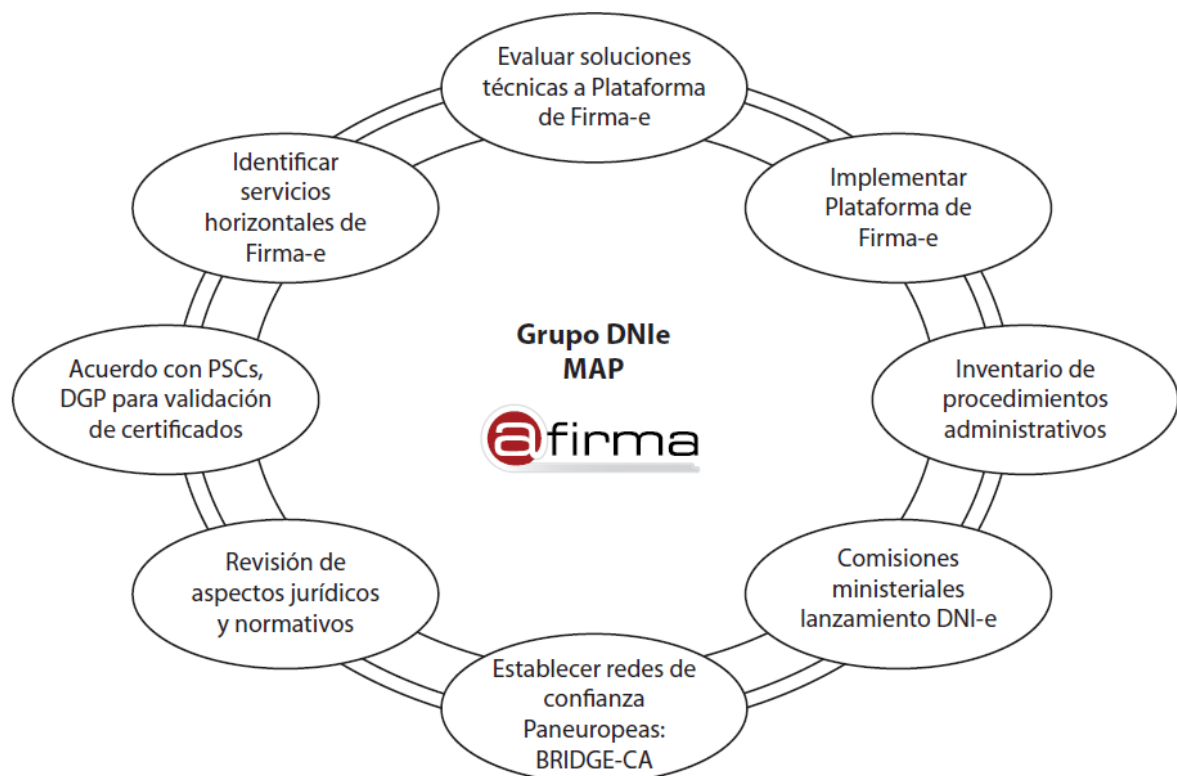


Imagen 6-16 Estructura de la Plataforma @Firma

Servicios:



- Validación de certificados X.509 según la RFC 3280, de las Autoridades de Certificación incluidas en la plataforma.
- Funcionalidades de firma: La plataforma permite varias modalidades de firma.
- Validación de la firma de un elemento firmado.
- Proporciona un cliente de firma que permite a los ciudadanos que accedan a los servicios de Administración Electrónica, firmar electrónicamente los documentos.
- Sellado de Tiempo (TSA) según el estándar RFC 3161 para certificar temporalmente todas las operaciones de validación y firma que se realizan a través de la plataforma.
- Gestión y administración de los Prestadores de Servicios de Certificación adheridos. Todas las operaciones realizadas en la plataforma son registradas para la auditoría y trazabilidad del sistema.

La plataforma @firma es una solución de referencia para cumplir con las medidas de identificación y autenticación descritas en el Capítulo II de la Ley 11/2007. Para acceder a los servicios indicados es necesario disponer de accesibilidad a la Plataforma @firma desde los sistemas de información del Organismo en cuestión a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que ofrece servicios de intranet entre las Administraciones Públicas.

Requisitos de uso

Para acceder a los servicios es necesario disponer de accesibilidad a la Plataforma desde los sistemas de información del Organismo en cuestión, a través de la red SARA (explicada anteriormente), que ofrece servicios de intranet entre las Administraciones Públicas. Estos sistemas que soportan los servicios de administración electrónica disponibles para los ciudadanos y empresas, accederán a la Plataforma a través de servicios Web implementados en tecnología Microsoft o Java.

Si no se posee un convenio o acuerdo con el Ministerio de Presidencia o con la Comunidad Autónoma de acceso e integración a la Red Sara, es necesario remitir una carta de solicitud de acceso al Director General para el Impulso a la Administración Electrónica para regularizar este aspecto, y asumir que se permite el acceso al entorno de producción de @Firma.

Es necesario comprometerse a informar de los servicios que se tuvieran preparados para admitir el DNle, al MPA ¿MAP? y se publicaría en la Web del DNI electrónico.

Pasos a seguir

1. El Organismo debe ponerse en contacto con el servicio de soporte (CAU) de @firma, indicando el Organismo (Ministerio, Comunidad Autónoma o Entidad

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Local) que desea integrarse en el servicio, así como los datos de contacto del mismo:

eMail:soporte.afirma5@map.es

teléfono: 902 93 44 05

2. El servicio de Soporte (CAU) se pondrá en contacto con dicho Organismo para informar de los prerequisites que son necesarios para iniciar la integración.

Para ello es necesario:

- Conocer si el Organismo tiene convenio con la FNMT (para poder validar sus certificados).
- Trasladar al Organismo el compromiso de informar al Ministerio de Presidencia de los servicios que utilicen la plataforma para admitir el DNle, para publicarlo en la Web del DNI electrónico.
- Informar al Organismo que los servicios se ofrecen a través de la red SARA, y que durante las pruebas se pueden hacer pruebas controladas en un entorno de preproducción habilitado al efecto desde Internet.

3. Una vez informados los prerequisites, habiendo respondido el Organismo, el servicio de Soporte (CAU) le proporciona al mismo la documentación de bienvenida, que se compone de:

- ACL (formulario para el control de acceso).
- Documentación
- Pasos iniciales para la integración con @firma.
- Servicios de @firma.
- Manual del Integrador del Cliente de Firma @firma.
- Manual de Programación de *Web Service* de @firma.

4. El Organismo debe devolver el ACL debidamente cumplimentado al servicio de Soporte (CAU) para finalizar el proceso de integración.

Ejemplo de ACL: Elegir en primera instancia si la conexión es a través de OCSPResponder (*Online Certificate Status Protocol* (OCSP)) es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados) o *Web Services*.

DATOS A RELLENAR POR SISTEMAS	
IP ORIGEN (si es un rango, indicar la máscara)	IP ACTUAL
RESPONSABLES DE SISTEMAS	
Nombre y Apellidos	
Teléfono	
Email	
DATOS A RELLENAR POR EL ORGANISMO	
ENTORNO (Marcar con una X)	
REPRODUCCIÓN	
PRODUCCIÓN	
CERTIFICADOS ADMITIDOS	
Tipos de certificados que se van a utilizar (por Autoridad de Certificación y tipo de persona física, persona jurídica, componente, ...)	
¿Disponen de convenio en vigor con la FNMT-RCM para la prestación de servicios de certificación?	
Indique fecha de caducidad del convenio:	
APLICACIÓN 1 (que va a usar el servicio)	
Nombre de la aplicación	
Descripción de la aplicación	
Unidad Organizativa	
<u>Responsable</u>	
Nombre y Apellidos	
Teléfono	
Email	
Lista de los servicios telemáticos que se soportarán con la aplicación URL donde se ubican los servicios telemáticos	
...	
APLICACIÓN N (que va a usar el servicio)	
Nombre de la aplicación	
Descripción de la aplicación	
Unidad Organizativa	
<u>Responsable</u>	
Nombre y Apellidos	
Teléfono	
Email	
Lista de los servicios telemáticos que se soportarán con la aplicación URL donde se ubican los servicios telemáticos	
Formato de la Firma de Respuesta	
Método de Autorización	

XAdEST (Firma XML avanzada con sellado temporal)	▼
XMLDSignature (Firma XML Básica)	
XAdESBES (Firma XML Avanzada)	
XAdEST (Firma XML avanzada con sellado temporal)	
Sin método de autorización	▼
Sin método de autorización	
Usuario y Password	
Certificado	

Imagen 6-17 Solicitud para integrarse con @Firma

5. En el caso de una conexión haciendo uso del certificado de componente, es necesario remitir al servicio de @Firma el certificado con la clave pública que se va a utilizar en las conexiones con @Firma, así como el formato de exportación del certificado.

6. Para el acceso a pre-producción es necesario indicar la IP de salida del organismo que desea conectarse a este entorno.

7. El servicio de Soporte (CAU) informará debidamente de los parámetros de conexión con los servicios: URL, identificador de aplicaciones,...

Las URL de los servicios son las siguientes:

- Desarrollo (SARA):

<http://des-afirma.redinteradministrativa.es/afirmaws/services/>

- Producción (SARA):

<http://afirma.redinteradministrativa.es/afirmaws/services/>

- Pre-producción Desarrollo (Internet):

<http://217.15.39.2/afirmaws/services/>

En este último caso, siempre con el permiso de la Coordinación del proyecto del MPR.

Dificultades más comunes

La necesidad de integrarse en la red Sara para hacer uso del servicio en entorno de desarrollo o explotación.

En el caso de que el acceso al entorno de desarrollo no requiriera el cumplimiento de todas las especificaciones técnicas, podrían realizarse pruebas en un entorno similar al de producción, con el consiguiente ahorro de tiempo que conlleva la tramitación administrativa de solicitud y acceso a la red Sara.

6.1.7 CITA

Los Servicios públicos son las prestaciones que las Administraciones Públicas ponen a disposición de los ciudadanos, sin discriminación alguna, y cuya utilización les aporta ventajas o beneficios. Es característica intrínseca el no buscar el fin de lucro en la actividad que se desarrolla, sino la satisfacción y el bienestar de los ciudadanos, ya que el Servicio Público se considera como el Servicio técnico prestado al público de una manera regular y constante mediante una organización de medios personales y materiales cuya titularidad pertenece a una Administración Pública y bajo un régimen jurídico especial.

Las prestaciones que utilizan las TIC, como soporte para su funcionamiento, y para su implementación y desarrollo, son llamados Servicios Públicos Digitales.

Con la aprobación de la ley 11/2007, de 22 de junio, de Acceso electrónico de los ciudadanos a los Servicios Públicos, se obliga a las administraciones públicas a tomar las medidas necesarias para garantizar este nuevo derecho a los ciudadanos. La Dirección General para el Desarrollo de la Sociedad de la Información, a través de sus instrumentos de actuación, contribuye a hacer

efectivo el cumplimiento de esta ley, fundamentalmente en el ámbito de las entidades locales.

En esta ilustración se pueden ver los instrumentos de los que se compone la Plataforma Avanza Local.



Imagen 6-18 Ilustración 6-9 Esquema Plataforma Avanza Local

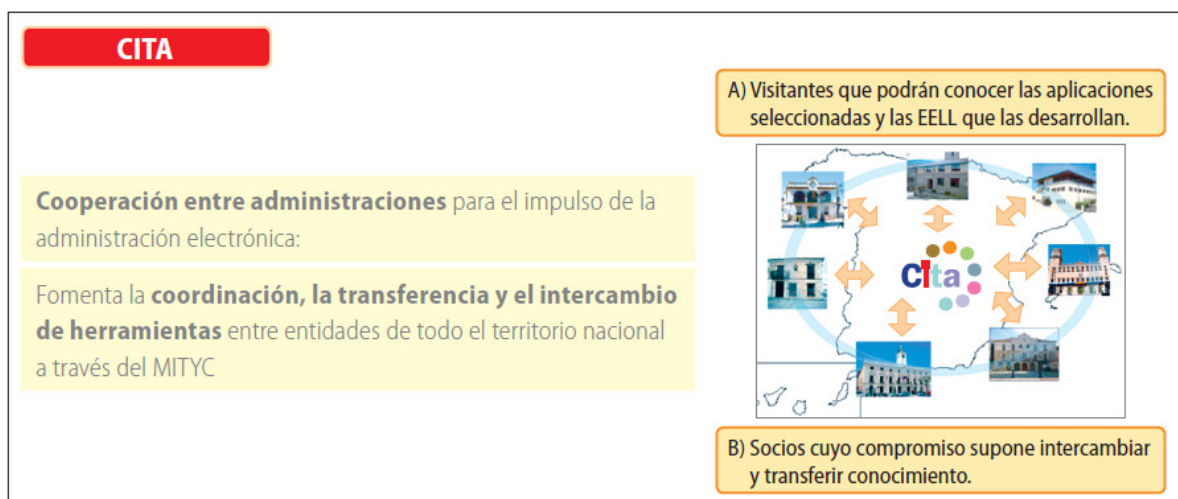


Imagen 6-19 Esquema de CITA

6.1.8 Portal CIRCE

La normativa que regula las sociedades limitadas ofrece, desde el año 2003, la posibilidad de realizar los trámites de constitución y puesta en marcha de la Sociedad Limitada de Nueva Empresa (SLNE) por medios telemáticos. Esta posibilidad se extiende en el año 2006 a las Sociedades de Responsabilidad Limitada. Actualmente se están tramitando ¿no estará ya publicado? las modificaciones legislativas necesarias para que también puedan realizarse los trámites para constituirse como Empresario Individual (Autónomo).

El Sistema de Tramitación Telemática (STT) del Centro de Información y Red de Creación de Empresas (CIRCE) es un sistema informático de tramitación de expedientes electrónicos que, a través del Documento Único Electrónico (DUE), lleva a cabo el intercambio de la documentación necesaria para la creación de empresas.

La tramitación telemática consiste en la realización de los trámites de constitución y puesta en marcha de una sociedad por medios telemáticos, evitando desplazamientos y reduciendo tiempos y costes en el proceso de creación de una empresa. Se evita, por ejemplo, el tener que volver a rellenar datos de la empresa en cada una de las administraciones con las que hay que realizar trámites, ya que el sistema se encargará de enviar a cada agente aquellos datos que necesite.

El Sistema de Tramitación Telemática de la red de Puntos de Asesoramiento e Inicio de Tramitación (PAIT) permite que cualquier persona pueda constituir una empresa por Internet, rellenando el DUE, que sustituye a diversos formularios de la Seguridad Social, Agencia Tributaria, etc. La tramitación del DUE es gratuita.

Para crear una empresa de este modo, el emprendedor dispone de dos posibilidades:

- Contactar con el PAIT más cercano, donde encontrará información y asesoramiento para poner en marcha su proyecto empresarial y podrá realizar la tramitación administrativa de constitución de su empresa por medios telemáticos.
- Cumplimentar el DUE a través de Internet, en cuyo caso un PAIT Virtual le prestará asesoramiento durante el proceso. Si se opta por esta modalidad, se necesitará disponer de un certificado de firma electrónica.

Los trámites que se realizarán de forma telemática son los siguientes:

- Reserva de la Denominación Social (sólo para SLNE).
- Otorgamiento de la Escritura de Constitución (el emprendedor deberá de acudir al notario para su firma).

- Solicitud del CIF provisional.
- Liquidación del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos.
- Documentados
- Inscripción en el Registro Mercantil Provincial.
- Trámites en la Seguridad Social / Instituto Social de la Marina.
- Solicitud del CIF definitivo.



Imagen 6-11 Web del Centro de Información y Red de Creación de Empresas (CIRCE)

Además, el emprendedor también dispone de la posibilidad de dar de alta los ficheros de datos personales que vaya a utilizar en la Agencia de Protección de Datos y contratar un pack de presencia en Internet. Próximamente se incluirá la posibilidad de realizar trámites con la Oficina Española de Patentes y Marcas, lo que permitirá la reserva de una marca y/o una denominación social.

El mayor problema que existe actualmente para la ampliación a nuevos trámites o nuevas administraciones es la necesidad de cambios legislativos, de

modo que el DUE pueda sustituir a los formularios que se estén utilizando en la actualidad y la tramitación que se realice tenga completa validez legal.

6.1.9 El Consejo Superior de Administración Electrónica

El Consejo Superior de Administración Electrónica es el órgano colegiado adscrito al Ministerio de la Presidencia, encargado de la preparación, la elaboración, el desarrollo y la aplicación de la política y estrategia del Gobierno en materia de tecnologías de la información, así como del impulso e implantación de la administración electrónica en la Administración General del Estado. Actuará en pleno y en comisión permanente y dependen funcionalmente de él las Comisiones Ministeriales de Administración Electrónica, los Comités Técnicos y grupos de trabajo o ponencias especiales creadas para desarrollar sus funciones.

Está regulado por el Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la administración electrónica. Según el *artículo 3.1*, desde la entrada en vigor de dicho Real Decreto, el Consejo Superior de Informática y para el Impulso de la Administración Electrónica pasará a denominarse Consejo Superior de Administración Electrónica.

6.2 eAdministración en Comunidades Autónomas y Diputaciones

Hasta ahora todos los ejemplos mostrados han sido servicios de la Administración General del Estado. Pero la Administración electrónica se encuentra igualmente fuertemente implantada en las Comunidades Autónomas, aunque naturalmente con un enfoque más orientado a la naturaleza de estas entidades y sus competencias específicas.

6.2.1 Diputación de Almería

Las actuaciones que la Diputación de Almería viene desarrollando para el cumplimiento de la Ley 11/2007, siguen las directrices que al respecto les marca la Asamblea General y la Comisión Permanente del Convenio Marco para la Implantación y Mantenimiento de la Red Provincial de Comunicaciones y Servicios de Teleadministración que en esta provincia agrupa a diversos entes locales para la búsqueda conjunta de soluciones eficientes en la aplicación de las tecnologías de la Información y las Comunicaciones^{xxiv}.

ACTUACIONES

Adaptación de Procedimientos Administrativos



Se ha aprobado un sistema basado en la transparencia de actuaciones y el compartir entre todos los entes adheridos al convenio marco, y otros de otras provincias que así lo han solicitado, la información referente a Inventario y Clasificación de Procedimientos e Inventario de Documentos y Datos, en un proceso de revisión continua^{xxv}.

Y de conformidad con lo previsto en el *artículo 34* de la Ley, en lo que respecta a Diputación, se ha creado una Comisión que lidere el Proceso de Racionalización de Procedimientos, como paso previo a su implantación en el tramitador electrónico.

Adaptación Normativa

Con objeto de regular todos los aspectos que afectan a la Administración Electrónica, de forma coordinada entre todos los Entes Locales que comparten soluciones y sistemas en la Red Provincial, se ha elaborado, siguiendo un proceso participado con información electrónica de los sucesivos borradores, un Reglamento Regulator de la Administración Electrónica, aprobado inicialmente por el Pleno de Diputación el 28 de enero y aprobado y publicado el 6 de Abril de 2009. Reglamento que si bien sólo es de aplicación directa a la Diputación, está redactado pensando en su aplicación a todos los Entes Locales adheridos al Convenio Marco que expresamente aprueben hacerlo propio y publiquen el anexo en el mismo previsto con las particularidades que libremente acuerden.

Adaptación Organizativa

La necesidad que la Ley plantea de redefinir la organización e instituir un registro de funcionarios habilitados para representar a los ciudadanos en actuaciones concretas, así como la posibilidad de establecer un sistema de adopción de Acuerdos de Órganos Colegiados por medios electrónicos, pasa por la definición de un Plan de Modernización y Calidad de los Servicios y el establecimiento de Planes de Formación acordes con los instrumentos y objetivos.

Pero en cualquier caso estas actuaciones parten de la premisa de que no se trata de crear una organización paralela para los servicios de administración electrónica, sino de redefinir las funciones y organización actuales partiendo de la nueva realidad de tener que atender al ciudadano, además de por el canal tradicional, por el canal electrónico, pues se constata que las dificultades no son tecnológicas sino el tratar de conseguir:

- El cambio en la forma de trabajar.
- Hacer “una vez” pensando en Multicanal.
- Conseguir el apoyo de TODOS.
- Hacer del cambio la rutina.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Trabajar en Equipo, en Red.
- Poner la Información y el Conocimiento a disposición de la Comunidad.
- Formación y Participación CONTINUAS.

Adaptación de los Canales de Comunicación

La Ley 11/2007 obliga a las Entidades Locales a poner a disposición de los ciudadanos más de un canal de comunicación y que uno sea electrónico. Por ello, se hace necesario habilitar al menos, junto al canal tradicional de atención presencial, el canal telemático. Pero sin perder de vista que se trata de distintos canales para el acceso a la misma información, por lo que se hace imprescindible organizarla atendiendo a los siguientes criterios:

- Toda la información debe estar en Bases de Datos.
- Pero solo una vez, para que esta sea consistente.
- Organizada por Naturaleza, con distintos clasificadores que faciliten su localización.
- Control de cambios que pudieran producirse
- Autores responsables las mismas personas y órganos que la generan actualmente en la Administración. Cambiar el modo de hacer, pensar en multicanal.
- Sistema de Información General basado en la creación de bases de datos multientidad que faciliten el acceso a la información por su naturaleza, con independencia de la Entidad que la ofrece (empleo público, perfil del contratante, etc...).

Y aunque no sean obligatorios inicialmente, la Red Provincial está preparando la incorporación de nuevos canales: Plataforma SMS en pruebas, TDT, etc.

Adaptación de la Tecnología Front-Office

La Red Provincial cuenta con un sistema de publicación de contenidos Web, basado en un gestor de contenidos de las sedes electrónicas, basado en bases de datos de información general multientidad y, en su caso acceso a bases de datos de gestión de la entidad. Accesos que, siempre que sean libres, se realizan mediante un sistema de URL parametrizables. Estilos de páginas, Bases de Datos y URL parametrizables en constante revisión y evolución puesto que lo que se hace para uno sirve para todos.

DNS del tipo topónimo .es para todos los entes locales territoriales, con identidad digital de la sede certificada HTTPS por la FNMT en virtud del Convenio suscrito por la Junta de Andalucía.^{xxvi}



Sistema de acceso ciudadano a la oficina virtual, basado en el Concepto de Carpeta Ciudadana o posibilidad de acceder a los formularios electrónicos de solicitud y a toda la información particular a la que tenga acceso un DNI concreto, bien de forma directa o bien en representación de otro que así previamente lo haya autorizado y conste en el fichero de terceros de la Entidad. Posibilitando que el ciudadano para acceder pueda utilizar cualquier certificado de Identidad Digital reconocido por *@Firma v.5* de la Secretaría de Estado para la Función Pública que se ha instalado en la Red Provincial.

Utilización de la tecnología *TiProceeding* (software libre del repositorio de la Consejería de Innovación de la Junta de Andalucía) como interfaz de relación con el ciudadano, para iniciar procedimientos, consultar los que le afecten, y recibir notificaciones y comunicaciones electrónicas^{xxvii}.

Sistema de Registro Telemático E/S integrado en el Registro General de la Entidad, y posibilidad de entregar cualquier documento utilizando el Formulario de Solicitud General que permite añadir documentos binarios al expuesto y/o solicita de la misma.

Implantación en la Red Provincial de una pasarela de pago telemática, lo que posibilita que los Entes Locales de la provincia, no tengan gastos financieros por operaciones de cobro, tan sólo una demora de unos días en la fecha valor de la operación.

Regulación del Boletín Oficial de la Provincia en Formato Electrónico, así como de los respectivos Tablones de Anuncios.

Adaptación de la Tecnología Back-Office

En el proceso continuo de adaptación de los sistemas de gestión de la Red Provincial, podemos destacar:

Respecto a la necesidad de Facilitar los datos del ciudadano disponibles en soporte electrónico al resto de Administraciones Públicas. La Red Provincial está abierta a la firma de los convenios necesarios y participa activamente en distintos foros de normalización. Pues ello sólo será posible cuando las Administraciones definan el modelo de datos y los *Web Service* necesarios:

- DGT (Conductores, Vehículos, Seguros).
- Secretaría de Estado para la Función Pública (Notificación de Domicilio).
- FEMP.
- Comunidad Autónoma.
- Red Provincial.
- Registro de Contratistas.

- Terceros...

Respecto al establecimiento de Firma Electrónica para el personal al servicio de las Entidades Locales, todo el personal de la misma cuenta con un certificado X.509 de firma electrónica acordado (ID de la Red Provincial basado en un sistema de registro personal) con plena validez jurídica para las relaciones internas, no sólo en la propia entidad, sino con cualquiera de la Red Provincial o dominios declarados de confianza. ID que también se utiliza para controlar el acceso a las aplicaciones basado en claves. Asimismo, todos los sistemas que se están desarrollando en la actualidad posibilitan el uso alternativo de certificados personales reconocidos por @Firma (DNI-e, C2 FNMT, etc.) ya que en el ID de la Red Provincial se incluye el DNI de su titular y por tanto también puede acreditarlo en virtud de que vaya incluido en un certificado reconocido.

Los sistemas de la Red Provincial, también utilizan certificados de dispositivo de la FNMT, como sistema de Firma Electrónica para la actuación administrativa automatizada, agilizando así las respuestas ya que no tienen que pasar por el portafirmas de ninguna persona física.

Garantizar la seguridad en entornos cerrados de comunicación. La Red Provincial, como entorno cerrado de comunicación entre las oficinas de los entes adheridos, está dotada de dispositivos procedimentales, lógicos y físicos de seguridad. Dispositivos que están en permanente revisión para hacer frente a los nuevos problemas que se vayan presentando.

Integración en la Red de Comunicaciones de las Administraciones Públicas. La Red Provincial está interconectada con la Red NEREA^{xxviii} de la Junta de Andalucía y ésta a su vez lo está con la Red SARA de la Administración General del Estado, lo que posibilita las relaciones entre los entes de la Red Provincial y cualquier otro conectado a dichas redes.

Emisión de documentos administrativos en formato electrónico. La plataforma @Firma instalada en la Red Provincial posibilita la utilización del Portafirmas @Firma también instalado para la firma de cualquier fichero binario utilizando certificados reconocidos como el DNle o el C2 de la FNMT no solo para los ciudadanos que quieran presentarlos, sino también para todo el personal de las Administraciones Locales.

Archivo electrónico. El Reglamento de Administración Electrónica, regula el establecimiento de una comisión encargada de establecer las condiciones en que éste deba realizarse, en especial cuando pudiera implicar la destrucción de otros soportes. La Red Provincial cuenta en la actualidad con los sistemas *TiDoc* de la plataforma *TiProceeding*, así como de *Alfresco*.

Implantación de un Sistema de Tramitación de Expedientes electrónico, basado como se ha indicado en *TiProceeding* (con motor de *workflow TiFlows*) que permite usar cualquier proceso definido en el estándar XPD, que puede definirse con cualquier herramienta de definición de modelado y flujos de trabajo que cumpla el estándar XPD, como sería el caso de *Jawe*, sistema



multientidad que puede integrarse mediante *tool* o *WS* con cualquier base de datos de gestión existente o accesible por la Red (no sólo Provincial, sino también de NEREA Y SARA).

Y, finalmente, indicar que, con objeto de poder sacar un mayor rendimiento a todos los flujos que se vayan definiendo, se está revisando el modelo de datos corporativo de la Red Provincial, así como dotando a las aplicaciones de gestión de *Web Services* con objeto de que puedan interconectarse con el tramitador de expedientes o con otras aplicaciones que respondan al modelo SOA. Tales como:

- Tablas Comunes.
- Registro General de Entrada con Oficina Telemática.
- Nueva Hacienda Local y Recaudación.
- Nuevo Padrón de Habitantes (pruebas).
- Nuevo Sistema de Gestión de Policías (proyecto)...

Todo ello en un proceso de revisión continua sin fin que no y que exige empezar cuanto antes a quien aún no lo haya iniciado.

6.2.2 Generalitat Valenciana

Introducción

La Generalitat Valenciana, las Diputaciones de Alicante, Castellón y Valencia, junto con la Federación Valenciana de Municipios y Provincias son conscientes del esfuerzo necesario para que las Entidades Locales de la Comunitat Valenciana alcancen el cumplimiento de la Ley 11/2007, y en este sentido firmaron el 24 de julio de 2008 un convenio marco de colaboración en materia de Administración Electrónica.

El primer resultado de este convenio es el proyecto Plataforma de Administración Electrónica para Entidades Locales, que ofrecerá diferentes soluciones que permitirán a las Entidades Locales cumplir con los nuevos requerimientos legales en cuanto a administración electrónica^{xxix}.

La Plataforma de Tramitación Electrónica se basa en un modelo con cinco directrices:

- Integrador, la plataforma es el resultado de la suma de diferentes componentes que se ponen al servicio de las Entidades Locales de forma integral.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Flexible, permitiendo concebir implantaciones personalizadas en función de la evolución tecnológica y organizativa de cada Entidad Local.
- Reutilizable, los componentes de la plataforma se compartirán entre las Entidades Locales y otras Administraciones Públicas.
- No intrusiva, permite convivir con la arquitectura de componentes preexistentes de las Entidades Locales.
- Sostenible, cualquier evolución de la plataforma estará disponible para todos los adheridos, lo que permite incorporar evoluciones con menor impacto presupuestario.

No se trata de empezar de cero, sino de analizar en qué punto se encuentra cada Entidad Local y complementar los servicios que ya ofrece. En este sentido, la Plataforma de Administración Electrónica se presenta como una solución común y global que mediante la colaboración de las distintas Entidades Locales, permitirá alcanzar el objetivo común en el plazo indicado.

Plataforma de eAdministración

La plataforma de eAdministración proporciona una base tecnológica fiable, moderna y segura, que sirve como base para el desarrollo eficiente de servicios para los ciudadanos:

- Solución integral en el ámbito de la Administración Electrónica, con un enfoque global aunque con componentes unitarios reutilizables e intercambiables.
- Técnicamente innovador, aunque fruto de la experiencia acumulada en múltiples proyectos realizados en el ámbito de la Administración Electrónica.
- Arquitectura tecnológica de última generación.
- Utilización de estándares. Para el desarrollo de la plataforma se han incorporado los más importantes estándares del mercado.
- Arquitectura orientada a servicios.
- Solución no intrusiva gracias a una arquitectura de conectores, que facilitan la integración con sistemas ya implantados en las Entidades Locales (herramientas de back-office como padrón, gestión tributaria, contabilidad, etc.).

El diseño de la plataforma ha buscado en todo momento la integración no disruptiva en los entornos tecnológicos de las Entidades Locales. Entendemos que se han realizado inversiones previas para dotarse de sistemas y servicios electrónicos, que no necesariamente deben amortizarse y sustituirse por los correspondientes de la plataforma. El conveniente análisis de cada organización nos llevará a decidir cuál es la estrategia óptima de incorporación de los componentes de la Plataforma de Administración electrónica.

La plataforma está compuesta por varios componentes principales:

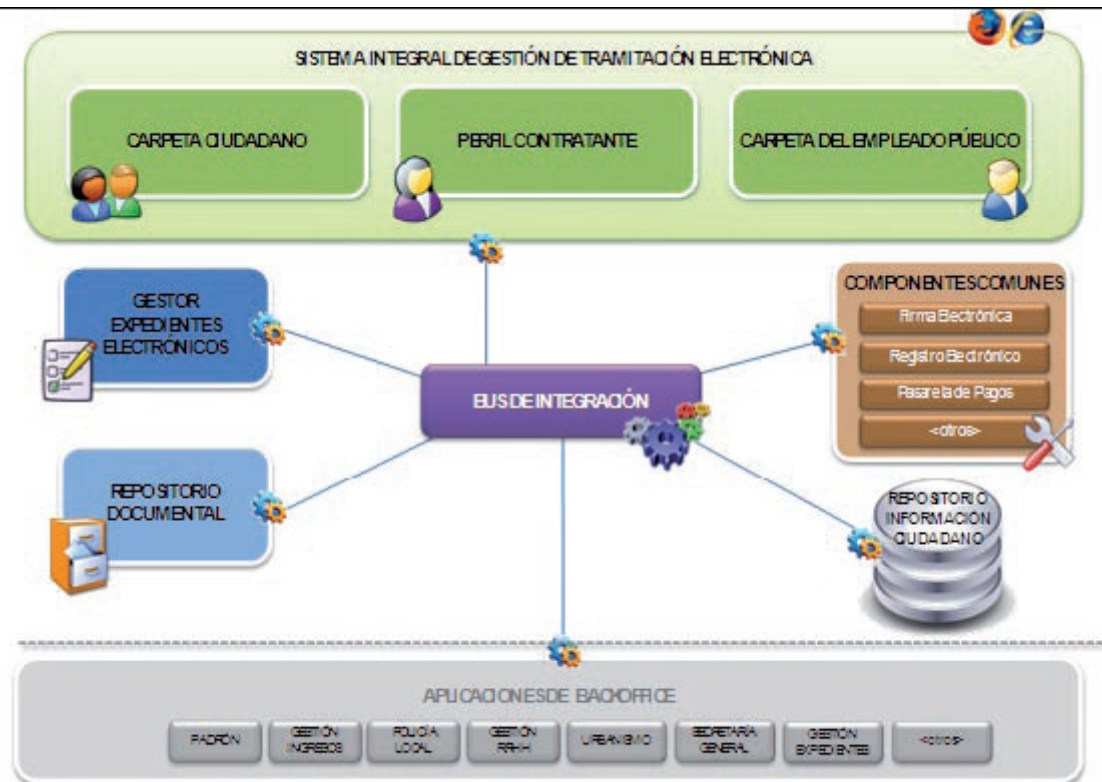


Imagen 6-20 Esquema del SIGTE de la Generalitat Valenciana

Sistema integral de gestión de tramitación electrónica

En la plataforma, los procesos de negocio trascienden las fronteras de la Entidad Local para llegar hasta ciudadanos y empresas. El ciudadano se convierte en un usuario más de la plataforma, constituyendo el origen y el fin de los procedimientos administrativos.

Dentro de las actividades que conforman un trámite administrativo encontramos varias que son desempeñadas por los ciudadanos: registro electrónico, firma electrónica, solicitudes, subsanaciones, etc.

En la plataforma, ciudadanos y empleados públicos trabajan en un mismo entorno, facilitando el acercamiento y la transparencia objeto de la Ley 11/2007.

El objetivo principal de la plataforma es ofrecer telemáticamente a los ciudadanos los mismos servicios que tradicionalmente se prestan de forma presencial, manteniendo las mismas garantías (calidad del servicio, garantía jurídica, etc.) Y es precisamente este componente el que ofrece la Carpeta del Ciudadano, como el espacio privado donde los ciudadanos y empresas podrán interactuar telemáticamente con las Entidades Locales.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Los servicios de las Entidades Locales también son empleados por las empresas y por ello la plataforma incluye un servicio como el Perfil del Contratante que cumple al 100% con lo exigido por la Ley de Contratos del Sector Público permitiendo la publicación electrónica de toda la información contractual (pliegos de condiciones, adjudicaciones, etc.).

Los empleados de las Entidades Locales tendrán a su disposición una Carpeta del Empleado Público donde podrán desempeñar su labor y disponer de una completa trazabilidad del estado de los diferentes trámites a su cargo.

Gestor expedientes electrónicos

La tramitación de los diferentes servicios que ofrecen las Entidades Locales puede ser compleja, en el gestor de expedientes electrónicos se definen los diferentes circuitos de tramitación aplicables a cada servicio con la visibilidad que el ciudadano tendrá de ellos. Los circuitos de tramitación incluyen opciones como: notificaciones, secuencias de aprobación, generación de documentos, firmado digital, etc.

Repositorio documental

La tramitación electrónica continúa teniendo una fuerte dependencia documental, pero en este caso más allá de la frontera del papel y del archivo físico, sustituyéndolos por los documentos electrónicos y el repositorio documental centralizado. Los documentos estarán siempre disponibles desde cualquier ubicación y con las mismas garantías jurídicas y de seguridad.

Repositorio de información del ciudadano (RIC)

Los diferentes servicios electrónicos se sustentan sobre las herramientas de back-office de las Entidades Locales, por lo que para garantizar un servicio con disponibilidad 24 horas al día y 7 días a la semana (24x7) se construye un repositorio con un resumen de la información de interés del ciudadano. Completando esta información, básicamente, la que se muestra en la Carpeta del Ciudadano (datos personales básicos, histórico de trámites, situación de los trámites en curso, etc.). La plataforma asegura una disponibilidad completa de esta información abstrayendo de cara al ciudadano posibles paradas de servicio de las herramientas de back-office de las Entidades Locales por labores de mantenimiento, copias de datos, etc.

Componentes comunes

Los componentes descritos hasta el momento hacen uso de toda una serie de herramientas comunes necesarias para el desempeño de sus funciones. El ejemplo más claro puede ser el de Registro Electrónico de Entrada/Salida o las funcionalidades de Firma Digital y Pasarela de Pagos. Los componentes



nativos de la plataforma emplean estas herramientas, pero la ventaja es que han sido diseñadas para poder emplearse por cualquier sistema de información ya operativo en las Entidades Locales.

- **Autenticación y Firma Electrónica:**
Permiten la identificación del ciudadano de forma electrónica. Dan validez legal a los acuerdos y documentos aportados, mediante el uso de certificados electrónicos acreditados por Entidades Certificadoras.
- **Sistema de Avisos/Notificaciones:**
Se encarga de la gestión de avisos, alertas y notificación de resoluciones. Abarca tanto las notificaciones fehacientes como los avisos no fehacientes. Se identificarán los canales para efectuar las comunicaciones fehacientes y las no fehacientes (SMS, Correo Electrónico).
- **Registro de E/S:**
Realiza el registro de toda la documentación que entra o sale de la Administración, bien sea por métodos electrónicos o mediante métodos presenciales.
- **Directorio de la Organización:**
Permite la autenticación de los empleados públicos en el resto de componentes de la plataforma.
- **Pasarela de Pagos:**
Es el componente encargado de la interacción y el pago de servicios de forma electrónica. Los pagos electrónicos podrán tratarse de forma puntual (licencias de obra), o de forma periódica (recibos del IBI).
- **Sellado de Tiempos:**
Se encarga de certificar la fecha y hora para el registro electrónico, los procesos de firma y el sistema de notificaciones entre otros.
- **Gestión de la Representación de Terceros:**
Se encarga de gestionar las representaciones de unos ciudadanos por otros.

Bus de integración

El Bus de Integración es un componente interno de todo el sistema, que se encarga de coordinar las comunicaciones entre todos los componentes, actuando como garante de la interoperabilidad. Esto posibilita integrar cualquier sistema de información dentro de la plataforma simplemente con conectarlo al bus de integración, como es el caso de las herramientas de back-office en uso actualmente en las Entidades Locales.

6.3 eAdministración en las Entidades Locales

6.3.1 Ayuntamiento De Madrid

Un caso especial lo es la Administración electrónica en el ámbito de las entidades locales. Este caso destaca, entre otras cosas, por su heterogeneidad en cuanto a disponibilidad de recursos. En España hay más de 8.000 municipios y la mayoría son municipios pequeños con recursos escasos a los cuales les resulta difícil poner en marcha servicios de administración electrónica, ya que esa escasez en recursos se traduce en falta de personal y conocimiento en TIC y dificultades para financiar los equipos informáticos necesarios^{xxx}.



Imagen 6-13 Servicios de eAdministración del Ayuntamiento de Madrid.

Ante esta difícil problemática el Ministerio de Administraciones Públicas ha lanzado diferentes iniciativas entre las cuales cabe destacar especialmente las ayudas económicas y subvenciones como la iniciativa *eModel* para proyectos de interés para la modernización local o nivel organizativo y tecnológico, los servicios horizontales a través de la Red SARA y la iniciativa del Centro de Transferencia de Tecnologías (CTT) que pretende impulsar el intercambio y reutilización de conocimiento y de proyectos concretos entre las administraciones.



La filosofía detrás de estas iniciativas consiste en proveer por una parte un abanico de servicios horizontales a todas las administraciones en aras de agilidad, simplicidad y optimización de costes ya que así se consigue que las diferentes administraciones y organismos no los tengan que implementar por su cuenta.

Por otra parte se trata de hacer la Administración electrónica más viable para aquellos organismos que por su naturaleza disponen de más dificultades económicas, técnicas y organizativas para integrarse en los servicios de administración electrónica (pequeños ayuntamientos, organismos de reducido tamaño y presupuesto, etc.).

El Ayuntamiento de Madrid viene desarrollando estrategias de modernización incorporando nuevos servicios y gestiones, y simplificando y normalizando la gestión administrativa como base para la tramitación electrónica, todo ello acompañado de la transformación y modernización de los sistemas de gestión interna.

Medidas Generales de Desarrollo de la eAdministración en el Ayuntamiento de Madrid

Entre las principales actuaciones que se han realizado destacan:

- Creación de la Comisión de Coordinación de las Nuevas Tecnologías de la Información y de las Comunicaciones, para coordinar las actuaciones que en materia de sistemas de información y comunicaciones adopten los órganos que integran la Administración municipal y establecer las directrices e iniciativas en relación con las políticas y estrategias de actuación para la modernización de la Organización en este sentido.
- Definición, desarrollo e implantación de una plataforma de servicios básicos para dar soporte al desarrollo de la tramitación electrónica y otras actuaciones en materia de la Administración electrónica.
- Se han llevado a cabo dos estrategias: la actualización y mejora de aquellos servicios que ya estaban disponibles o en fase de desarrollo e implantación, y la definición, diseño e implantación de aquéllos que todavía no se hubieran abordado, pero que eran significativos para el desarrollo de la administración electrónica.
- Estas actuaciones se han concretado en el diseño de soluciones para los servicios básicos de administración electrónica: Firma digital, diseño y gestión de formularios, registro electrónico, consulta de tramitación, información centralizada al ciudadano, custodia documental, interoperabilidad externa y notificaciones telemáticas.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Implantación de una plataforma corporativa para la gestión de contenidos y portales Internet e Intranet y un modelo de gestión integral de contenidos desconcentrado y coordinado para ambos entornos.
- Puesta en marcha de un nuevo portal Internet (*www.munimadrid.es*) y una nueva Intranet (*Ayre^{xxxí}*) sobre la plataforma corporativa de gestión de contenidos y portales.
- Realización de un estudio de todos los procedimientos tramitados por el Ayuntamiento de Madrid, y agrupación de los mismos en familias definidas en función del contenido y la tramitación de dichos procedimientos. Se trata de sistematizar la identificación y propuesta de medidas de administración electrónica aplicables a todos los procedimientos incluidos en cada familia.

Entre los servicios actualmente disponibles en la Web municipal, accesibles con y sin certificado digital, se encuentran los siguientes:

- Cita previa para la realización de diversas gestiones.
- Padrón: Solicitud de volante, modificación datos, consulta del censo.
- Tributos municipales: Pago, domiciliación bancaria, sistema especial de pago IBI, autoliquidación.
- Autoliquidación, pago, domiciliación de tasas.
- Multas de circulación: pago en periodo voluntario, consulta.
- Servicios Sociales: Programa de ayuda a domicilio para recién nacidos.
- Madrid Salud: Adopción animales domésticos. Solicitud de servicios de la unidad técnica de control de vectores (plagas).
- Dirección General de Deportes: reserva pistas de tenis. Resultados y clasificaciones de competiciones deportivas municipales.
- Bibliotecas Públicas Municipales: renovación de préstamos, solicitud nuevas adquisiciones.
- Incidencias de Medio Ambiente: solicitud cubos, papeleras, contenedores. Retirada muebles y enseres, vehículos abandonados. Limpieza de la vía pública.

Medidas concretas de eAdministración

Información centralizada y multicanal al ciudadano

El objetivo ha sido facilitar al ciudadano información sobre los servicios municipales, incluyendo los formularios normalizados y las fichas informativas de los procedimientos, de manera que se mejoren las vías de información y la



prestación de servicio, así como la agilidad en la tramitación de los procedimientos administrativos.

- Desarrollo de la oficina virtual de consultas, Trámites y gestiones, con y sin certificación electrónica.
- Coordinación de los diferentes medios de atención al ciudadano a través del proyecto Línea Madrid que engloba los tres canales de atención bajo unos mismos criterios de calidad: oficinas de atención presencial, teléfono 010 y Web municipal.
- Elaboración y publicación de un inventario de procedimientos y trámites administrativos y realización de fichas explicativas de descripción de los distintos procedimientos contenidos en el catálogo.
- Impresos y formularios:
 - Normalización y mecanización.
 - Puesta a disposición de los impresos y formularios en la Web y dotación a los mismos de funcionalidades de cumplimentación.
 - Redacción de un *Manual de estilo para la normalización y elaboración de impresos*.
- Establecimiento de convenios de colaboración con otras administraciones o entidades para el intercambio seguro de información.
- Publicación electrónica del Boletín Oficial del Ayuntamiento de Madrid.
- Desarrollo del Tablón de Edictos Electrónico para facilitar la consulta de la información de actos y comunicaciones por ciudadanos y empresas mediante su publicación electrónica en la Web municipal.

Inicio electrónico

Proyectos realizados:

- Sección en *www.munimadrid.es* de trámites y gestiones.
- Revisión de la información, normalización y mecanización de los impresos disponibles para su cumplimentación y descarga en la Web municipal.

Proyectos en marcha:

- Implantación del Registro electrónico.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Estudio de la documentación que está siendo solicitada en los procedimientos administrativos, para determinar si es susceptible de simplificación. Esto facilita la implantación de los procedimientos por medios electrónicos desde el punto de vista del anexo de documentación a la solicitud electrónica, y también es la base para el establecimiento de medidas de interoperabilidad con otras Administraciones.
- Desarrollo de un portal específico de trámites y gestiones.

Medios de pago electrónicos

Pago por Internet. El Ayuntamiento de Madrid tiene habilitados medios de pago por Internet para tributos y multas:

- Mediante tarjeta de crédito o débito de cualquier banco.
- Por Banca Electrónica, si se es cliente de este servicio de alguna de las entidades colaboradoras.
- Con certificado digital de clase 2CA (FNMT), si se dispone de él y además se es cliente de una Entidad colaboradora.

Firma electrónica

- Creación de Oficinas de Acreditación. Se han creado 23 oficinas de acreditación que dan servicio a los ciudadanos así como una oficina central de acreditación interna dependiente de la Subdirección General de Administración Electrónica encargada de planificar la acreditación del personal directivo y de los trabajadores municipales y de coordinar las actuaciones con el resto de las oficinas de acreditación y con la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda. Recientemente se ha creado una red de oficinas de acreditación interna en todas las Áreas de Gobierno y Organismos Autónomos, además de en otras unidades específicas.
- Implantación de Procedimientos Administrativos Municipales. Se han incorporado progresivamente procedimientos administrativos en los que interviene la firma electrónica al servicio de los ciudadanos a través de la Oficina Virtual de la página Web *munimadrid* (padrón, volante y consulta de censo, multas, consulta y pago de tributos), e internos para los funcionarios municipales tales como la incorporación al Proyecto de Remisión Electrónica de Documentos (RED) de la Seguridad Social, Acceso al Registro Sanitario de la Comunidad de Madrid, Tramitación de la Contratación electrónica (PLYCA), Servicio de Asesoramiento Empresarial (PAIT), y Consulta de Datos Catastrales (Punto de Información Catastral).



- Implantación de la Tarjeta Criptográfica que se ha extendido a todo el conjunto de los trabajadores municipales con diversas utilidades y especialmente para la incorporación de la firma electrónica para su uso en los diversos procedimientos.

Plataformas y tramitación de expedientes

- El Ayuntamiento de Madrid cuenta con varias plataformas de tramitación de expedientes para diferentes áreas de actuación: sistemas integrados de gestión económico financiero y de recursos humanos (basado en la herramienta SAP), PLYCA (Programa de Licitación y Contratación Administrativa), Útil (Gestión de ingresos municipales), SIGSA como gestor de procedimientos administrativos.
- Se está desarrollando un nuevo tramitador de expedientes general para procedimientos que no dispongan de los específicos citados anteriormente para que, además de mecanizar y organizar la gestión administrativa, aporte las funcionalidades que se requieren para el cumplimiento de las obligaciones que derivan de la Ley 11/2007, tales como la posibilidad de inicio electrónico de los procedimientos, la aportación de documentación por los mismos medios, la notificación telemática, o la información al interesado del estado de tramitación de los expedientes.
- Por otro lado, también se está desarrollando un módulo específico en SAP para la tramitación de los expedientes de subvenciones.

Gestión de representantes

Se ha desarrollado la aplicación de Gestión de la Representación. Dicho sistema se integra en la plataforma horizontal de servicios básicos del Ayuntamiento de Madrid y permite la gestión de representantes, representados y representaciones y la consulta al sistema desde servicios de usuario final.

Como proyectos piloto se han desarrollado:

- La consulta a través de la Web de los datos relativos a pagos a acreedores del Ayuntamiento de Madrid gestionados por la Tesorería Municipal, que puede hacerse por representantes de los acreedores debidamente autorizados y cuya representación se haya comunicado al Ayuntamiento de Madrid.
- La identificación del conductor responsable de la infracción por Internet, mediante el uso de certificado digital. Se trata de que el titular del vehículo, a quien se dirige en primer lugar la notificación de la infracción, pueda realizar el trámite de identificar al

conductor del vehículo de forma electrónica, al igual que su representante como en el caso de las empresas de alquiler de Vehículos sin conductor.

6.3.2 Ayuntamiento de Leganés

A comienzos del año 2010^{xxxii} el Ayuntamiento de Leganés tiene implementada una herramienta de gestión de expedientes administrativos con la que realiza la tramitación de aproximadamente un 85% de la carga de trabajo administrativo de la institución.

La herramienta almacena datos relacionados con cada expediente, emite documentos cruzando estos datos con plantillas predeterminadas, almacena documentos producidos externamente, genera los correspondientes registros de entrada y salida y los relaciona con el expediente, y puede integrar los procedimientos con la aplicación de recaudación para la emisión y seguimiento de liquidaciones y recibos y con la de contabilidad para permitir la realización de los apuntes contables y el seguimiento y gestión de las facturas.

La tramitación genera información exhaustiva sobre las operaciones realizadas y la documentación tratada, pudiendo consultarse tanto los trámites y documentos de cada expediente como los datos de su tramitación desde cualquier puesto autorizado de la organización. También se obtiene información agregada dirigida a dar soporte a la toma de decisiones o a la emisión de informes o memorias.

La herramienta de gestión de expedientes está en fase de integración con un sistema de gestión documental que preclasifica de forma automática los documentos captados o generados a partir de su registro o de su tratamiento en el correspondiente expediente. Esta aplicación permite la posterior gestión independiente de los documentos sin emplear las aplicaciones que los generan o utilizan y es la base de un repositorio documental único para toda la documentación gestionada en la organización.

El ciudadano tiene acceso, con certificado electrónico, al *Servicio Leganés 24 horas Online*^{xxxiii}, donde puede consultar parte de la información de los expedientes en los que figura como interesado o representante:

- hoja de ruta de trámites administrativos realizados,
- estado del expediente,
- relación de la documentación presentada y registros generados.

Hasta 2009, se accedía al servicio mediante una clave que se obtenía por Internet, en los telecentros municipales o presencialmente, siendo precisa la personación del interesado al menos una vez en las oficinas del Servicio de



Atención del Ciudadano para la comprobación de su identidad y la firma de un contrato de adhesión al servicio

El Servicio Leganés 24 horas Online permite ofrecer algunos otros servicios por Internet:

- Descargarse documentos de padrón (volantes),
- De recaudación (cartas y justificantes de pago),
- Domiciliar recibos y pagar los recibos pendientes.

La aplicación que soporta estos servicios adicionales, en entorno Web, resuelve de forma eficaz la emisión automática de algunos documentos y la tramitación de procedimientos sencillos, pero no es una herramienta adecuada para la realización de trámites más complejos.

El servidor Web está certificado como servidor seguro. La implantación de la herramienta de gestión de expedientes ha supuesto un gran avance en cuanto a la productividad conseguida a la hora de tramitar, al control que permite del seguimiento de los expedientes y a la información que se posee de los mismos.

Limitaciones de las herramientas implantadas

Las principales limitaciones de las aplicaciones actualmente implantadas podrían concretarse en los siguientes puntos:

- Aunque los documentos generados electrónicamente se guardan como un objeto no modificable y los recibidos se escanean y guardan con la misma seguridad, no incorporan las firmas correspondientes y no pueden considerarse un documento *seguro* en sentido estricto. Durante la tramitación de los expedientes es necesario imprimir la documentación en papel y firmarla, siendo el expediente físico el único que tiene valor administrativo.
- La información a la que el ciudadano puede acceder por Internet es parcial. Sólo ve los trámites realizados, no ve los documentos. Esta limitación tendría fácil solución técnica.
- La tramitación electrónica es exclusivamente *interna*, ya que el ciudadano, aunque puede consultar sus expedientes, no puede interactuar con la institución realizando solicitudes, aportando documentos o recibiendo notificaciones o requerimientos.

La superación de estas limitaciones despejaría el camino para el cumplimiento de la LAECSP.

Actuaciones básicas necesarias

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

La solución de estos problemas requiere las siguientes acciones:

- Implantación definitiva de la herramienta de gestión documental que gestione todos los documentos producidos por la gestión de expedientes, los recibidos electrónicamente, los provenientes del escaneado masivo de documentos de entrada en la organización y en general cualquier documento gestionado o producido por las distintas aplicaciones del Ayuntamiento. La clasificación de los documentos deberá automatizarse en lo posible e ir unida a la producción o captación de los mismos en las correspondientes aplicaciones.
- Implantación de una herramienta de firma electrónica y validación de originales electrónicos de terceros integrada con la gestión documental y con las distintas aplicaciones, que permita la firma individual o masiva de la documentación en el momento de su producción o la incorporación de los documentos a un sistema de portafirmas electrónico que incluya los distintos circuitos de firma, en los casos en que el firmante del documento sea distinto del productor o que exista más de un firmante para el documento.
- Implantación de un registro telemático que incluya un sistema de notificación electrónica y que se integre con la aplicación de gestión documental y con las aplicaciones actuales de registro y gestión de expedientes.

Otras actuaciones de cara al cumplimiento de otros requerimientos de la LAECSP, serían:

- Integrar funcionalidades que permitan la interoperabilidad con otras administraciones.
- Diseñar una plataforma multicanal en entorno Web para la gestión de los expedientes administrativos que contemple la comunicación con el ciudadano vía correo electrónico, SMS y MMS y asegure la accesibilidad de los ciudadanos con discapacidad.

Migración a un entorno Web

Actualmente está prevista la migración gradual de todas las aplicaciones del sistema central de gestión municipal, diseñadas en entorno cliente servidor, a aplicaciones en entorno Web.

Sustituir la actual aplicación de gestión de expedientes por una aplicación en entorno Web posibilitará la tramitación vía Web, tanto a tramitadores internos no conectados en red como a los ciudadanos, permitiendo que estos últimos reciban la consideración de un tramitador más del expediente.

Esta migración no resolverá por sí misma los problemas anteriormente expuestos, sino que los trasladará a otro entorno, si no se implantan las acciones a las que se ha hecho referencia anteriormente.



Al haberse afrontado en primer lugar, se dará un desfase entre la disponibilidad de esta herramienta de gestión de expedientes en entorno Web y la disponibilidad de las futuras herramientas Web que en su actual versión cliente-servidor están integradas con la herramienta a la que sustituye, con lo que se perderían parte de las ventajas de la herramienta actual si no se contemplara la integración provisional de la nueva herramienta con las restantes aplicaciones en entorno cliente-servidor del actual sistema central de gestión municipal.

Por otra parte, la migración a la nueva herramienta de gestión de la definición de los procedimientos actualmente implantados no será inmediata, ni mucho menos, y habrá que pensar en una convivencia en el tiempo de la aplicación en ambos entornos.

Habría que actuar con la siguiente secuencia:

1. Implantar de forma inmediata las aplicaciones de gestión documental, firma electrónica y registro telemático, integrándolas con la actual herramienta de gestión de expedientes en entorno cliente servidor, buscando así el cumplimiento de la LAECSP en el plazo más breve de tiempo posible y sin perder las ventajas de la actual integración.
2. Desarrollar la nueva herramienta de gestión de expedientes en entorno Web, asegurando su integración con las restantes aplicaciones del sistema central de gestión municipal, sean estas las actuales (en cliente servidor) o las que las vayan sustituyendo (en entorno Web).

El cambio cultural, formación y comunicación

La tramitación electrónica exige a los tramitadores un cambio radical en su forma de actuar. El problema no es la utilización de los medios electrónicos para producir los documentos. El problema es la desaparición del papel como soporte físico de la firma y los sellos que dan plena validez al documento.

En la actualidad se sigue trabajando para recibir documentos electrónicos en diferentes formatos y de escanear y validar todo documento en papel que se presente por registro. Los documentos en papel serán archivados y tras la operación de registro y sustituidos en el trámite por sus copias electrónicas válidas. La producción de los documentos posteriores y su firma será electrónica, y únicamente si el ciudadano prefiere la notificación en papel volverá a aparecer un documento no electrónico. En todo caso cualquier documento no electrónico tendrá su correspondiente documento electrónico válido en el expediente que será el utilizado para la tramitación.

Mediante la formación a los registradores podemos implicar a los funcionarios en el cambio, siguiendo dos líneas básicas:

- Formación respecto al cumplimiento de la normativa.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Formación que familiarice a los funcionarios con el nuevo entorno y disipe la desconfianza en la consistencia y validez de las nuevas herramientas.

La comunicación interna, sobre todo la que transmita a los empleados municipales la implicación de los puestos directivos con el cambio, puede ser determinante en la formación de la opinión respecto al nuevo entorno y en su aceptación. Un plan de comunicación de la adaptación a la LAECSP facilitaría el proceso.

Necesidad de mantenimiento 24 horas 365 días al año

Es evidente que con la nueva Ley los horarios de los servicios administrativos de los Ayuntamientos pasan a prestarse en un horario de 24 horas todos los días del año. Ya no hay días hábiles o inhábiles a efectos de información y registro.

En el mercado existen servicios que ofrecen la supervisión continua de la Web del Ayuntamiento e incluso son capaces de ofrecer a los usuarios la visualización de las páginas en caso de caída de los sistemas. Pero no pueden emular los sistemas de cobro de tributos, o el de los Registros de Entrada. En los casos en que la interacción con el ciudadano exija el funcionamiento del sistema de gestión, sólo la restauración inmediata de los sistemas y/o del servidor Web puede restablecer el servicio.

Hay acciones de restauración que pueden realizarse online, pero no es posible en todos los casos, dependiendo del origen físico o lógico del problema.

Siempre puede pensarse en una duplicación de al menos una parte de los sistemas con lo que esto supone en el aumento de los costes de mantenimiento y operación.

La posición del Archivo en el nuevo entorno de gestión

Esta nueva situación plantea un nuevo reto, cómo afecta la implantación de una herramienta de gestión documental a los responsables de los archivos municipales.

Las herramientas de gestión documental, al basar la gestión de todos los documentos en la creación de un repositorio único, independientemente del ciclo de vida en que se encuentren los documentos tratados, permiten extender a toda la organización los procedimientos de gestión que hasta ahora estaban limitados a la parte del ciclo de vida correspondiente al archivo definitivo.

Como destinatario final de todos los documentos, el responsable del archivo debe ser un elemento clave en la implantación de este tipo de herramientas. Además, en la mayor parte de los ayuntamientos, sólo los responsables del Archivo poseen los conocimientos técnicos y experiencia profesional suficientes



para implantar, y en su caso administrar, un sistema de gestión documental integrado.

7 EADMINISTRACIÓN SIN USAR FIRMA ELECTRÓNICA

7.1 Introducción

Aunque la Administración electrónica se asocia en primer lugar con la oferta de información y servicios por la vía electrónica, así como con trámites por vía electrónica, el concepto actual de Administración electrónica es considerablemente más amplio.

En este sentido hay que destacar especialmente las herramientas y filosofía que giran en torno a la idea clave de interacción con el internauta que se encuentra detrás del concepto de Web 2.0, una idea que ha calado hondo en el ámbito de la Administración electrónica, ya que presenta muchas oportunidades innovadoras de emplear las tecnologías para mejorar los servicios al ciudadano y conseguir mayores niveles de democracia a través de la participación directa del mismo en la actividad pública.

Así se están introduciendo herramientas como Blogs, Wikis o foros de opinión para participación de los ciudadanos en la actividad pública. Estas herramientas son además idóneas para poder llevar a la práctica las ideas modernas, sobre la relación con el ciudadano que se encuentran detrás de conceptos ampliamente debatidos como la Administración 2.0.

Desafortunadamente la Administración Pública todavía cuenta con un amplio abanico de tópicos ampliamente conocidos, eso hace que si se habla de innovación en el sector público quizás aún se vea a más de una persona poniendo caras raras. Pero efectivamente es innovadora en más de un campo, y mucho. Uno de ellos son las TIC y algo tan importante como el uso de la firma electrónica en sus procedimientos administrativos y servicios públicos.

La idea del comercio electrónico en Internet ha calado ya desde hace tiempo, pero, no muchos proveedores de servicios electrónicos del sector privado han permitido el uso de certificados electrónicos en sus transacciones. Bankia, por ejemplo, ha sido una de las primeras entidades que ofrece esta posibilidad, pero sólo como alternativa a la introducción manual del número de DNI, es decir, aún usando certificado (el DNI electrónico concretamente) es necesario usar una clave de usuario. Por tanto se sigue usando en el fondo un sistema de usuario/clave, de manera redundante con respecto al DNLe. El usuario no percibe ninguna ventaja, sino más bien inconvenientes, más trabajo, ya que ha de introducir primero el PIN del DNI, y luego su código de acceso del banco.

El caso de Bankia no es en absoluto aislado y hay que felicitar particularmente a Bankia por la innovación que supone la introducción del DNLe en los servicios de banca electrónica, pero a la vez es necesario reseñar que ésta manera no es coherente con las posibilidades ni la filosofía del DNLe, el cual puede y debe servir para acabar de una vez por todas con la colección de claves y códigos de acceso a los diferentes servicios disponibles en la red. La gracia del DNLe radica precisamente en esto, en acceder con un solo PIN de manera totalmente



segura a cualquier servicio en la red y olvidarse de nombres de usuario y claves.

Cabe pensar que la situación de Bankia responda a motivos concretos y temporales, ya que el uso del DNle por la banca es un motor poderoso para impulsar su uso por parte de los ciudadanos. De lo contrario, un mal uso, puede contribuir a crear una percepción negativa del mismo en los ciudadanos.

En cualquier caso, el soporte del DNle en el sector privado es poco frecuente. Sin embargo, a día de hoy, el uso de certificados electrónicos es ya algo completamente habitual en los servicios que la Administración Pública ofrece. Lo será también el futuro en el sector privado conforme se implante más y más su uso y en particular el DNI electrónico. Pero en este momento es fundamentalmente la eAdministración quien está actuando como líder que genera un efecto arrastre sobre el sector privado.

Por otra parte, la Administración electrónica, aunque se suele asociar principalmente a la tramitación de procedimientos administrativos, va en realidad mucho más allá de trámites electrónicos, abarca el uso de las TIC dentro de la Administración para innovarla, junto con los cambios organizativos para la mejorar los servicios públicos. Una vertiente especialmente interesante es la aparición del concepto de Web 2.0 y su papel dentro de la Administración electrónica, ya que plantea vías innovadoras de comunicación y difusión masiva, y bien utilizadas muy eficaces.

A continuación se repasan algunos ejemplos de cómo ya se están utilizando estas nuevas herramientas en las organizaciones, en la Administración y en la política.

7.2 Concepto de Web 2.0

El término, Web 2.0 fue acuñado por *Tim O'Reilly* en 2004^{xxxiv} para referirse a una segunda generación en la historia de la Web basada en comunidades de usuarios y una gama especial de servicios, como las redes sociales, los blogs, los wikis, etc, que fomentan la colaboración y el intercambio ágil de información entre los usuarios.

Los promotores de la aproximación a la Web 2.0 creen que el uso de la Web está orientado a la interacción y redes sociales, que pueden servir contenido que explota los efectos de las redes, creando Webs interactivas y visuales. Es decir, los sitios Web 2.0 actúan más como puntos de encuentro, o Webs dependientes de usuarios, que como Webs tradicionales.

Quizás el ejemplo por excelencia de la Web 2.0 sea la Wikipedia, una enciclopedia dónde cualquiera puede participar en los contenidos. Una sofisticada organización avala la calidad de los mismos evitando actos de vandalismo y garantiza que la información sea fiable.

De todas formas, el principio básico es muy simple: una comunidad amplia tiene capacidad suficiente para crear, mantener y evolucionar contenidos de

calidad y la supervisión por la comunidad tiene tal alcance y fuerza que consigue a su vez que actos aislados malintencionados no lleguen a prosperar.

El éxito de este concepto colaborativo ha sido tan rotundo que ya en el año 2005 la revista *Nature* valoró la calidad de la Wikipedia como muy cercana a la Enciclopedia Británica^{xxxv} y actualmente no pocas voces sostienen que ésta incluso ha sido superada por la Wikipedia, aparte de que la supera ampliamente en cantidad y detalle de artículos (En enero del 2010 la Wikipedia en inglés contenía casi 3.200.000 artículos frente a 500.000 en la Enciclopedia Británica).

7.3 Administración 2.0

El concepto de Web 2.0 también ha calado en el ámbito de la Administración Pública, aunque aún ha trascendido demasiado poco a la realidad del día a día y los servicios de la Administración. Sin embargo, es un tema recurrente en las ponencias relacionadas con la Administración Pública y la correspondiente blogosfera.

En este sentido se puede destacar, por ejemplo, que el lema del *Tecnimap 2007* fue “*Administración 2.0: nuevos servicios, nuevos derechos*”. Es un concepto que se ha consolidado en la blogosfera sobre Administración Pública, aunque aún hay discusiones importantes sobre lo que abarca y lo que no el término^{xxxvi}.

Podríamos enumerar los rasgos principales que podrían transformarse de la Administración 1.0:

- De una administración tutelar que decide sobre los servicios que reciben los ciudadanos y no estudia la demanda a receptiva, en la que los ciudadanos pueden opinar sobre los servicios que reciben y cuáles son sus prioridades.
- De conservadora, apegada a la separación de competencias y a los viejos procesos en los que aplica las nuevas tecnologías a innovadora y colaborativa, que identifica las oportunidades de las nuevas tecnologías, las posibilidades de utilizarlas en los procedimientos y la interoperabilidad entre Departamentos y Administraciones.
- De la pasividad de trasladar al ciudadano parte de sus tareas (hacer de mensajeros entre administraciones, estar pendiente de las renovaciones, plazos, etc.) a hacer la declaración, solucionar los asuntos, intermediar, evitar el trámite, ser proactiva.
- De rígida y controladora por encima de la eficacia a adaptar sus estructuras y cultura a los cambios de la sociedad.
- De subvencionar con poco control sobre el retorno de la inversión a incentivar la innovación y el desarrollo y la promoción de las empresas del país fuera de sus fronteras.
- De la consabida burocracia cuyo exagerado cumplimiento de las normas fomentan una resistencia pasiva al cambio, y tendente a la desconfianza



y a la ineficiencia a modernizar la organización, la gestión y el marco normativo para estar acorde con el nuevo contexto.

- De distante para el ciudadano, que es ajeno a sus cambios, a reconocer el derecho a participar en las decisiones e incluso en el diseño de servicios en la Administración. Ser próxima, ser mi administración.
- De compleja en el lenguaje administrativo y laberínticos procedimientos a sencilla y transparente.

7.4 Blogs

Blogosfera es el término bajo el cual se agrupa la totalidad de Weblogs y se deriva de la palabra inglesa *blogosphere*. Debido a que los blogs o las bitácoras están conectadas por medio de enlaces, comentarios, históricos y referencias han creado y definido su propia cultura. Por lo tanto, la blogosfera como palabra y concepto es inherente a los Weblogs.

Podemos considerar blogosfera como un sistema virtual, en el que se establecen comunidades de Weblogs, categorizados temáticamente o por perfiles de interés. Estos conforman, pues, el mensaje y la blogosfera, el lugar para habitar en Internet.

La blogosfera cumple una importante misión en cuanto a la transmisión de información interna que sirve a múltiples propósitos como una simple comunicación de noticias e información actual, el debate sobre problemáticas propias de la Administración, la difusión de proyectos, la formación personal de los empleados públicos y personas que trabajan con la Administración (proveedores, etc.). Incluso ha habido iniciativas como sondeos de opinión sobre propuestas concretas y políticas públicas en las Administraciones Públicas.

En definitiva ofrece una fuente de información importantísima para los empleados públicos y afines que les conecta de una manera mucho más activa con la vida de la Administración, lo cual supone sin duda un enriquecimiento profesional.

Por otra parte, no hay que olvidar que puede ser una vía importante para que la ciudadanía en general conozca mejor los problemas de la Administración, problemas que desgraciadamente se presentan de manera muy simplista y sesgada en los medios tradicionales, y que han contribuido de manera esencial a la mala imagen de la Administración y en particular de los funcionarios ante la opinión pública. Esperando por tanto que a medio plazo se puedan convertir también en una fuente de información valiosa para el público que le aporte un mejor conocimiento y criterio sobre el mundo de la Administración Pública y contribuya así a un debate más cualificado sobre la Administración y la función pública en los medios.

La característica quizás más diferenciadora de estos blogs frente a los medios tradicionales de difusión masiva (incluyendo las Webs convencionales con sus

secciones de notas de prensa, etc.) es su carácter independiente y la interactividad y realimentación que supone la sección de comentarios, la cual permite palpar no solamente la visión del propio autor, sino del público. Supone por tanto un enriquecimiento de perspectiva considerable y una transparencia mucho mayor, ya que el contenido no se construye unilateralmente como en los medios tradicionales.

7.4.1 Blogs y política

Aunque supone desviarse algo del ámbito de este proyecto, hay que hacer una mención al uso de los blogs e Internet en general en el ámbito político.

En los últimos años se ha intensificado el uso de Internet como medio de comunicación para los políticos, son muy conocidos los ejemplos del uso de las nuevas tecnologías en las campañas políticas de Barack Obama o Rosa Díez en el caso de España. En el caso de Obama, aparte de ser un reconocido “fan” de las nuevas tecnologías, ha encontrado en ellas un canal adicional a través del cual reforzar de manera muy eficaz su campaña y hacerla más atractiva para determinados segmentos del público.

En el caso de Rosa Díez quizás haya que destacar más el hecho de que la Web fuera un canal alternativo a las campañas tradicionales que ha permitido a su partido articular y difundir una campaña con una inversión muy reducida que llegó a un número de personas inalcanzable por vía tradicional con las limitaciones económicas propias de un partido joven.

Estos ejemplos muestran que Internet ha llegado a la política para quedarse. Cabe esperar que la política utilizará cada vez más y de forma cada vez más intensa y diversa este medio. Una manifestación de ello son los blogs personales de políticos concretos con los cuales pretenden comunicarse directamente con los ciudadanos y palpar de cerca sus opiniones. A día de hoy parece que medios de comunicación instantánea como Twitter^{xxxvii} está funcionando mejor en la comunicación con el ciudadano, además, permite al ciudadano conocer mejor el pensamiento del político en cuestión sobre temas actuales y decidir con mayor criterio si se sienten identificados con él o no e incluso responderle.

7.5 Wikis

El término “Wiki” procede del Hawaiano y significa *rápido* y eso es exactamente lo que caracteriza a las Wikis, ser un medio rápido, sencillo, pragmático y eficaz para la creación de contenido. Lo que hace tan novedoso y exitoso el concepto es que se trata de sitios Web cuyas páginas pueden ser editadas de manera colaborativa por múltiples voluntarios a través de su navegador. Es decir, no hace falta instalar ningún programa de edición colaborativa, sólo hace falta un navegador, son fáciles y rápidas de utilizar, y por tanto las barreras de entradas para poder participar en un proyecto Wiki son mínimas.



La aplicación de mayor peso y a la que le debe su mayor fama hasta el momento ha sido la creación de enciclopedias colaborativas, género al que pertenece la Wikipedia^{xxxviii}. Existen muchas otras aplicaciones más cercanas a la coordinación de informaciones y acciones, o la puesta en común de conocimientos o textos dentro de grupos.

La mayor parte de los wikis actuales conservan un historial de cambios que permite recuperar fácilmente cualquier estado anterior y ver quién hizo cada cambio, lo cual facilita enormemente el mantenimiento conjunto y el control de usuarios destructivos. Habitualmente, sin necesidad de una revisión previa, se actualiza el contenido que muestra la página wiki editada.

Resulta por otra parte fascinante que algo tan abierto y con un nivel de control aparentemente muy reducido, comparado con la confección tradicional de contenidos, y con jerarquías de mando comparativamente planas y pequeñas como, por ejemplo, la Wikipedia sea capaz de producir contenido tan extenso y de una calidad tan alta que resiste además de una manera notable a ataques de vandalismo.

7.5.1 Las Wikis en las Organizaciones

Todas estas características hacen que las Wikis sean un instrumento cada vez más popular para usarse dentro de las organizaciones, tanto privadas como públicas. Se están convirtiendo así en herramientas de gestión de conocimiento auto-organizadas y muy eficaces ya que no requieren grandes reuniones, planificaciones y coordinaciones, sino que permiten que su contenido se construya poco a poco casi solo.

En el ámbito de la gestión de conocimiento es un hecho bien conocido que las relaciones y las conversaciones entre las personas de la organización son las que verdaderamente crean innovación. El conocimiento, la sinergia, la motivación, la cultura y los valores constituyen una parte fundamental del capital intelectual de la organización.

La tecnología, al contrario de lo que aún se afirma con frecuencia, abre las puertas a la relación y a la conversación de manera total, universal, transparente, en red. La tecnología no excluye la relación humana, muy al contrario la potencia hasta su máxima expresión proveyendo nuevas vías de aprendizaje que contribuyen a realizar el concepto de organización inteligente.

En ese sentido el uso de las Wikis dentro de una organización puede ser un vehículo para llevar a cabo esta interacción productiva de las personas que componen la organización, suponen una vía eficaz y fácil de explicitar todo el conocimiento generado y evitan que se quede inmerso en las cabezas de personas concretas, llevándolo a la organización.

Lo importante en este sentido no es tanto que los gestores planifiquen y coordinen el contenido, sino que impulsen el uso de este medio por sus equipos e intervengan en los conflictos si se producen. Sin el impulso institucional difícilmente prosperará una iniciativa de este tipo, pero una vez

sentadas las bases, y con el impulso adecuado, su desarrollo es extraordinariamente sencillo y ágil.

7.5.2 La Wikis en la Administración Pública

A diferencia de los blogs hoy por hoy y a pesar de sus indudables ventajas aún no hay muchas referencias de Wikis de Administraciones Públicas, pero poco a poco se van desarrollando proyectos como, por ejemplo, el proyecto Wikanda promovido por la Junta de Andalucía^{xxxix}, , una Wiki especializada en todo que gira en torno a esta Comunidad Autónoma o la Madripedia^{xl}, promovida por el Ayuntamiento de Madrid. Otro ejemplo es el portal e-Catalunya^{xli}, una iniciativa de la Generalitat de Cataluña para impulsar la sociedad del conocimiento en esta Comunidad.

De todos modos la referencia en cuanto a Wikis accesibles al público más importante es probablemente la propia Wikipedia ya que contiene numerosos artículos sobre la Administración Pública, Derecho administrativo, Administración electrónica, etc.

Por razones obvias es más difícil evaluar el grado de uso interno de Wikis, pero ya se están utilizando en los diferentes organismos de la Administración Pública española como herramientas de gestión de conocimiento. Un uso muy propicio es la documentación de procedimientos de trabajo o la documentación, manuales, etc. de las aplicaciones corporativas.

7.6 Redes sociales

Las redes sociales en Internet son en este momento probablemente el fenómeno Web 2.0 que con más fuerza se está desarrollando y el más generalista y popular. Una red social es una estructura social en Internet con forma de red donde sus nodos son individuos (a veces denominados actores) y las aristas relaciones entre ellos. Las relaciones pueden ser de distinto tipo, profesionales, ocio, amistad, etc. También es el medio de interacción de distintas personas como por ejemplo juegos en línea, chats, foros, etc.

La explosión de este fenómeno en los últimos años llama enormemente la atención, así por ejemplo, Facebook, la red social que se suele mencionar como ejemplo por excelencia creció desde su apertura al público en el año 2006 hasta más de 600 millones de usuarios en la actualidad (Enero 2011^{xlii}).

Este ejemplo se orienta fundamentalmente al ocio y la creación de círculos de amistades, por su parte están calando también muy hondo las redes profesionales como LinkedIn o Xing, y es previsible que a medio plazo incluso sustituyan al tradicional Curriculum Vitae. El objetivo de este tipo de redes es facilitar las relaciones profesionales e ir creando una malla de contactos. Si alguien tiene 50 contactos, a través de los mismos puede llegar a cientos de ellos que sus conocidos pueden facilitarle.



Por otra parte, estas redes tienen otra enorme utilidad a la hora de recuperar los contactos propios: cuando un usuario rellena su perfil en LinkedIn, por ejemplo, y va indicando las organizaciones por las que ha pasado a lo largo de su trayectoria profesional la herramienta automáticamente presentará las personas que pertenecen a la red LinkedIn de cada una de esas organizaciones. De ese modo no es nada raro recuperar un buen número de contactos que se creían perdidos o que se han descuidado con el tiempo.

Una vez recuperados estos contactos, se dispone de información actualizada sobre ellos y una manera muy fácil para contactarles directamente si se desea. Incluso se pueden utilizar funciones como solicitar recomendaciones de compañeros de trabajo que estos redactarán a través de la herramienta si están de acuerdo, lo cual puede ser útil para la promoción profesional.

Pero la utilidad no se limita solamente a contactar con otros profesionales, sino que permite otras múltiples formas de interacción que pueden ser muy productivas, se pueden formular, por ejemplo, consultas a otros profesionales, difundir presentaciones profesionales, realizar sondeos de opinión, recabar opiniones sobre una empresa, etc. No todos estos servicios se encuentran libres de coste, suele ser gratuita la publicación de un perfil personal y de pago determinados servicios avanzados del estilo de los mencionados.

7.6.1 Redes sociales en la Administración Pública

La utilidad más evidente dentro del sector público es la creación de una red de contactos con otros profesionales del sector público y privado, otros empleados públicos o profesionales afines a través de la cual se puedan localizar contactos interesantes, ya sea para la propia movilidad de los funcionarios dentro de la Administración, la localización de expertos en determinadas materias o la contratación de profesionales y proyectos.

7.6.2 Redes sociales en la política

Seguramente el ejemplo más paradigmático de las redes sociales en política sea la campaña electoral de Barack Obama. El presidente se ganó durante su campaña el apoyo de 3 millones de seguidores en Facebook y otros 121.000 en Twitter, además de los 19 millones de visitas que recibió su canal en YouTube. McCain sólo recabó el respaldo de 600.000 personas en el primer caso, 5.000 en el segundo y 2 millones de vistas en el tercer caso.

En España el uso de redes sociales en política también empieza a prosperar, algunos ejemplos son el caso del candidato al Gobierno de España por el partido socialista, Alfredo Pérez Rubalcaba, el cual hace uso de una cuenta de mensajería Twitter.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación



Imagen 7-1 Twitter de A. Rubalcaba

Por su parte, el candidato del partido Mariano Rajoy, tiene creado un perfil en el portal Facebook.

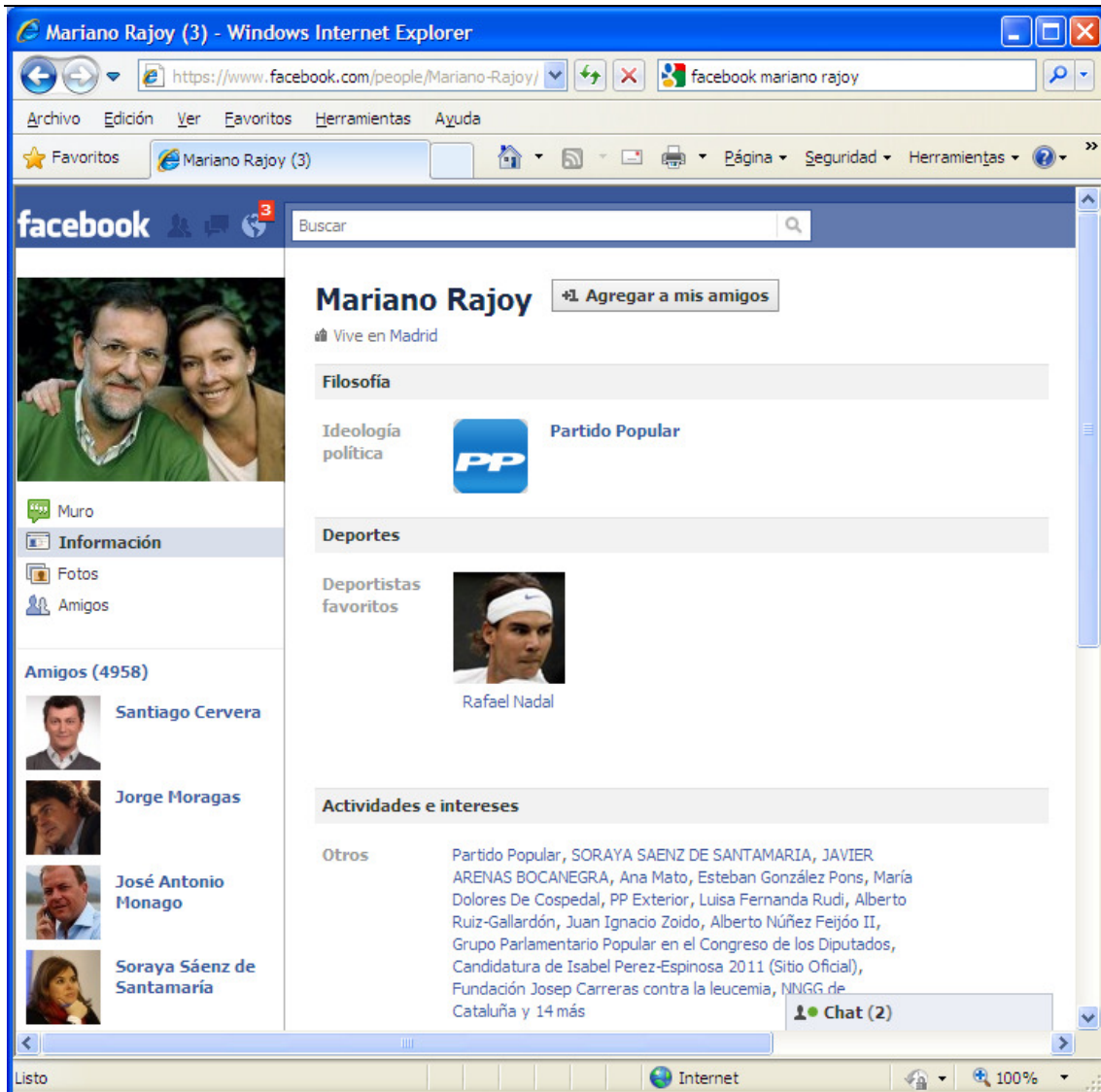


Imagen 7-2 Perfil de Facebook de Mariano Rajoy

Una variante curiosa del uso de las redes sociales es la página en Twitter creada para la comunicación de las actuaciones del Gobierno^{xliii} a los usuarios de esta red. De este modo no es necesario que los usuarios acudan a la Web del Gobierno para mantenerse al día, sino que vía Twitter se pueden suscribir a esta información y automáticamente se les envían las noticias sobre las medidas.

7.7 Marketing viral

El marketing viral o la publicidad viral son términos empleados para referirse a las técnicas de marketing que intentan explotar redes sociales preexistentes para producir incrementos exponenciales en la penetración de una marca o producto (*brand awareness*) mediante procesos de autorreplicación viral análogos a la expansión de un virus informático. Se suele basar en el boca a

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

boca mediante medios electrónicos, usa el efecto de red social creado por Internet y los modernos servicios de telefonía móvil para llegar a una gran cantidad de personas rápidamente.

También se usa el término marketing viral para describir campañas de marketing encubierto basadas en Internet, incluyendo el uso de blogs, de sitios aparentemente *amateurs*, y de otras formas de *astroturfing*, (término utilizado en campañas de relaciones públicas en el ámbito de la propaganda electoral y los anuncios comerciales que pretende dar una impresión de espontaneidad, fruto de un comportamiento con base social), diseñadas para crear el boca a boca para un nuevo producto o servicio.

Frecuentemente, el objetivo de las campañas de marketing viral es generar cobertura mediática mediante historias *inusuales*.

La popularidad creciente del marketing viral se debe a la facilidad de ejecución de la campaña, su coste relativamente bajo, (comparado con campañas de correo directo), buen *targeting*, y una tasa de respuesta alta y elevada. La principal ventaja de esta forma de marketing consiste en su capacidad de conseguir una gran cantidad de posibles clientes interesados, a un bajo costo.

La hipótesis es que si esa publicidad llega a un usuario *sensible* (es decir, interesado en el producto ofrecido), ese usuario *se infectará* y puede entonces seguir infectando a otros usuarios sensibles. Mientras cada usuario infectado envíe en media el correo a más de un usuario sensible (es decir, que la tasa reproductiva básica sea mayor a uno), los resultados estándares en epidemiología implican que el número de usuarios infectados crecerá de manera exponencial.

La tarea más difícil para cualquier compañía consiste en adquirir y retener una gran base de clientes. Mediante el uso de Internet y los efectos de la publicidad por e-mail, los esfuerzos de comunicación negocio-a-cliente (*business-to-consumer* o *B2C*) consiguen mucho mayor impacto que muchas otras herramientas. El marketing viral es una técnica que evita las molestias del spam o las frecuentemente abusivas campañas telefónicas, impulsa a los usuarios de un producto/servicio específico a contárselo a sus amigos. Esa es una recomendación *boca a boca* positiva.

7.7.1 Aplicaciones y ventajas en las Administraciones Públicas

En la Administración Pública es tan importante que los servicios públicos sean de calidad como que el ciudadano los conozca. El éxito de ejemplos como la Red 060, servicios concretos con un gran impacto (en comodidad, etc.) como el cambio de domicilio a través de Internet, o campañas de sensibilización como aquellas desarrolladas por la Dirección General de Tráfico depende en gran medida de su difusión e imagen ante los ciudadanos.

Esto, si cabe, se vuelve aún más importante en relación a la Administración electrónica, ya que a través de los nuevos servicios electrónicos está cambiando radicalmente y para mejorar la relación con los ciudadanos y empresas, además tiene el potencial de ejercer un efecto tractor sobre la



sociedad impulsando su integración en la sociedad de la información, algo esencial en los nuevos modelos económicos donde el uso de las TIC y sus efectivos positivos sobre la productividad de un país se han convertido en un condicionante clave para la prosperidad de cualquier país.

En ese sentido se puede considerar la implantación de la Administración electrónica como política pública no solamente un beneficio en términos de facilidades y comodidad para ciudadanos y empresas, sino un elemento estratégico de las políticas públicas.

Para poder conseguir esto resulta vital atraer a ciudadanos y empresas, es necesario acabar con la imagen tradicional negativa de la Administración a través de unos servicios modernos y atractivos, y para ello a su vez es necesario un *marketing* intenso y adecuado de estos servicios. En este contexto el marketing viral puede ser una nueva herramienta muy valiosa para llegar a los ciudadanos, especialmente en campañas concretas, no solamente por su eficacia como vehículo, sino por la imagen de modernidad y sofisticación asociada al uso de estos medios. Además, su bajo coste puede permitir desarrollar más campañas con el mismo o menor presupuesto, algo que en los tiempos actuales recobra especial importancia.

En España, por el momento, aún no se ha explotado mucho la vía del marketing viral dentro de las Administraciones Públicas, pero existen suficientes ejemplos fuera de España que pueden servir como base de ideas.

Un ejemplo magnífico de marketing viral vuelve a ser de nuevo la campaña electoral de Barack Obama, ya se comentó que el uso de las redes sociales en Internet que es un componente de su estrategia de marketing viral, pero esta estrategia va mucho más allá.

Con la ayuda de su equipo, ha creado una estrategia de comunicación multicanal sin precedentes que ha conseguido que Obama estuviera en todas partes: más de 1600 vídeos publicados en su página de YouTube, su propio Twitter, Facebook, MySpace, etc. Y no podemos dejar de mencionar todo el contenido que los seguidores de Obama han creado extraoficialmente para su candidatura presidencial.

Sus vídeos fueron un gran hito, se puede destacar especialmente el concurso “Obama en 30 segundos” en el cual se anima a los ciudadanos a crear y enviar un vídeo sobre Obama, el premio es que el ganador podrá ver su video en un anuncio por televisión. Esta iniciativa obtuvo como resultado el envío de más de 1.100 videos y se calcula que unos 5 millones de votantes. Es realmente llamativa la semejanza en calidad de los trabajos de particulares con trabajos realizados por profesionales, y la originalidad de alguna de las contribuciones. El vídeo ganador y otros finalistas se pueden ver en el enlace: <http://obamain30seconds.org/>.

Por otra parte el diseño de la Web personal de Obama^{xliv}, es un caso de estudio excelente sobre comunicación política. El sitio dispone de muchos elementos que han generado un efecto de marketing viral, por ejemplo:

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Una descripción detallada del plan de Obama y su postura acerca de los diferentes asuntos políticos.
- Una calculadora para el ahorro de impuestos.
- Una red social.
- Un servicio de donación online: "Donate and get a gift" (dona y obtén un regalo).
- "Goodies" para personalizar el ordenador.
- Tienda online de artículos relacionados con la campaña (chapas, camisetas, etc.)
- Invitaciones a eventos.
- Enlaces a: Facebook, Myspace, Youtube, Flickr, Digg, Twitter, eventful, Linkedin, blackplanet, faithbase, eons, glee, MiGente, MyBatanga, AsianAve, DNC Partybuilder.

8 IDENTIFICACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL GRADO DE IMPLANTACIÓN

Una vez realizado un análisis detallado de los contenidos que pueden influir en el ámbito de la eAdministración a la hora de crear software, queda patente que el temario es muy extenso. Sin un análisis, toda esta información seguiría siendo útil, pero muy difícil de digerir.

Para poder cumplir con uno de los objetivos de este estudio, concretamente el de poder ayudar a profesionales informáticos a tener un conocimiento de base sobre la Administración electrónica, se presentarán en formato de tablas unos análisis detallados de la Ley 11/2007, agrupados mediante diferentes puntos de vista y sin marcar ninguna diferencia entre Organismos Públicos.

Por otro lado la Administración Pública española tiene transferidas muchas de sus competencias a las CCAA. El proceso de descentralización territorial ha sido muy profundo en España, pasando de ser el país más centralista de Europa en 1978 a ser uno de los países más descentralizado del mundo en la actualidad.

De esta manera, las Comunidades Autónomas han pasado a ocupar una posición más visible en el escenario político, dada la capacidad de relación directa con los ciudadanos a través de los servicios que gestionan.

Hasta este momento del estudio no se ha hecho diferencia entre los diferentes Organismos Públicos. Todo lo expuesto hasta ahora, engloba a todas las competencias públicas. Ahora bien, en el momento de evaluarlas no se pueden definir los mismos criterios para todas, ya que sus competencias para con los ciudadanos no son las mismas.

Sabiendo que hay que hacer diferencias en las cuestiones a evaluar en los Organismos Públicos, este proyecto se inclina a determinar el estudio por Comunidades Autónomas a raíz de los datos cuantitativos realizados por una encuesta del Observatorio de Administración Electrónica (OAE). Existen más formas de estudio y evaluación, pero no existen datos cuantitativos de todas las CCAA conjuntas y en un mismo marco temporal que respondan a las mismas cuestiones.

8.1 Análisis de la Ley 11/2007

Una vez expuesto el análisis de la situación actual en relación a la eAdministración a través del presente documento se realizará una disección de la ley 11/2007 con el fin de conseguir obtener unos conceptos claros y entender la relación que existe entre todos los contenidos que en ella aparecen.

Para conseguir tal fin, se realizarán dos tipos de análisis, a saber:

- Análisis por artículos
- Análisis por función de ámbitos

8.1.1 Análisis por artículos

Con este primer análisis, se persigue tener al alcance una descripción de los derechos y exigencias de los artículos relevantes de la ley 11/2007 y así poder servir de referencia y poder realizar consultas de una manera rápida y sintetizada.

Se recuerda que una de las principales novedades que presenta la Ley 11/2007 es la de pasar de la declaración de impulso de los medios electrónicos e informáticos en las Administraciones Públicas, concretado en la práctica en la posibilidad de que éstas o algunos de sus Órganos permitan las comunicaciones por medios electrónicos, a que estén obligadas a hacerlo porque la ley reconoce el derecho de los ciudadanos a comunicarse electrónicamente con ellas.

Esta ley consagra una serie de los derechos para los ciudadanos y, en contraposición, establece exigencias para las Administraciones Públicas a las que hay que dar respuesta.

Art.	<i>Descripción de los Derechos y Exigencias</i>
6.1.	Formular solicitudes por medios electrónicos.
6.1.	Realizar consultas por medios electrónicos de algún trámite concreto.
6.1.	Efectuar pagos, realizar transacciones, por medios electrónicos.
6.1.	Oponerse a las resoluciones y actos administrativos por medios electrónicos.
6.1.	Presentar alegaciones, manifestar consentimiento, entablar pretensiones,...
6.2. a)	Elegir, entre los disponibles, el canal para relacionarse con la Administración.
6.2. b)	A no aportar los datos y documentos que obren en poder de las AAPP...
6.2. d)	A conocer por medios electrónicos el estado de tramitación de sus procedimientos.
6.2. e)	A obtener copias electrónicas de documentos electrónicos de su expediente electrónico.
6.2. g)	A obtener los medios de identificación electrónica, utilizar DNI-e,...
6.2. i)	Garantía de la seguridad y confidencialidad de los datos que custodian.
6.3. a)	Información, por medios electrónicos, de los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio.
6.3. b)	Información, por medios electrónicos, sobre las autoridades competentes en materia de actividades de servicios, así como de las asociaciones y organizaciones profesionales relacionadas con las mismas.



6.3. c)	Información, por medios electrónicos, de los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios y las vías de recurso en caso de litigio entre cualesquiera autoridades competentes, prestadores y destinatarios.
7.1.	Defensor del usuario de la Administración electrónica (Administración General del Estado).
8.1.	Garantía de acceso a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada: Oficinas de atención presencial con disponibilidad de medios, cumplimiento de los niveles de accesibilidad en el canal telemático...
8.2. b)	Sede electrónica.
8.2. c)	Servicios de atención telefónica.
9.1.	Facilitar a otras AAPP el acceso a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico.
10.	Establecimiento de una sede electrónica, que conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y servicios.
11.	Publicación electrónica del Boletín Oficial del Estado.
12.	Publicación electrónica del tablón de anuncios o edictos en la sede electrónica.
13.	Admitir DNI-e, firma electrónica avanzada, u otros (claves concertadas, etc.).
13.3.	Sistemas de firma electrónica para su actuación administrativa.
18.	Sello electrónico del órgano, entidad o código seguro.
19.2.	Firma electrónica del personal (identifica conjuntamente al titular del puesto de trabajo o cargo y al órgano en el que presta sus servicios).
21.	Interoperabilidad de la identificación y autenticación por medio de certificados electrónicos.
22.1.	Identificación y autenticación del ciudadano por funcionario público.
22.3.	Registro de funcionarios habilitados para la identificación o autenticación.
23.	Habilitación de terceros representantes.
24.	Registro electrónico de entrada. Calendario días inhábiles.
24.	Registro electrónico de salida. Calendario.
25.2.	Relación actualizada de procedimientos.
28.	Práctica de la notificación por medios electrónicos.
29.	Documento administrativo electrónico, con firmas electrónicas y referencia temporal.
30.	De papel a electrónico, de electrónico a papel, y de electrónico a electrónico.
31.	Archivo electrónico: medidas de seguridad, autenticidad y confidencialidad, calidad, protección y conservación de los documentos almacenados.
32.	Expediente electrónico. Conjunto de documentos electrónicos, índice electrónico, ...
33.2.	Formación del personal que vaya a utilizar los contenidos electrónicos.
34.	Análisis de rediseño funcional y simplificación de los procedimientos.
37.	Acceso de los interesados a la información... (art. 6.1.).

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

39.	Actuación administrativa automatizada.
40.	Comité Sectorial de Administración electrónica.
41.	Interoperabilidad de los Sistemas de Información (art. 21).
43.	Red de comunicaciones de las Administraciones Públicas españolas.
44.	Red Integrada de Atención al Ciudadano. Ventanillas Únicas (Directiva Servicios).

Tabla 2 - Descripción de los Derechos y Exigencias por artículos de la Ley 11/2007

* En verde las obligatorias a 1-1-2011

8.1.2 Análisis en función de ámbitos

Una vez realizado un resumen por artículos de la Ley 11/2007, se muestra un nuevo análisis en función de los ámbitos definidos para el análisis de la Ley 11/2007.

Se entiende por “ámbito” una agrupación de aspectos que contempla la Ley 11/2007. Todas estas agrupaciones son válidas para cualquier Administración Pública.

Mediante el análisis de los aspectos clave que contempla la Ley, se han determinado 15 ámbitos para la elaboración del estudio sobre el grado de aplicación de la misma.

A continuación se muestran los 15 ámbitos:

- Igualdad y accesibilidad a los servicios y canales de acceso a los servicios
- Expediente electrónico
- Acceso electrónico al estado e información de expedientes
- Interoperabilidad
- Seguridad jurídica
- Ventanilla Única
- Documento administrativo electrónico y copias electrónicas de documentos
- Firma electrónica
- Estándares abiertos
- Sede administrativa electrónica
- Registro electrónico
- Cumplimiento de los plazos de adaptación a la Ley
- Notificaciones electrónicas

Estos ámbitos han sido a su vez analizados y organizados en función de los derechos y obligaciones que establece la Ley: derechos de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas y obligaciones de éstas para hacer efectivo este derecho.

A continuación se muestra a modo explicativo un ejemplo de las tablas que se muestran más adelante, describiendo qué conceptos aparecerán en las casillas correspondientes, pudiendo visualizar la tabla como una matriz que relaciona



los Principios Generales de la Ley 11/2007 comprendidos en el estudio con los derechos y obligaciones reconocidos, detallando los principales artículos que los recogen y los ámbitos determinados para el estudio que engloban a todos ellos.

En este campo aparecerán los Principios Generales existentes en la Ley 11/2007	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	Se describe el derecho que tiene el ciudadano.
Principales Obligaciones de las AAPP	Se describe la obligación de la AAPP.
Art. relativos a los Derechos	Número de artículo en el que aparece.
Art. relativos a los Obligaciones	Número de artículo en el que aparece.
Ámbitos definidos para el análisis de la Ley 11/2007	Aquí se indican de entre los 15 ámbitos obtenidos, cuáles son aplicables.

Tabla 3 – Tabla ejemplo resumen Ley 11/2007

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Principio de Accesibilidad y Principio de Igualdad	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	<ul style="list-style-type: none"> - Derecho a la igualdad en el acceso electrónico a los servicios de las AAPP - Derecho a que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se relacionen con las AAPP por medios no electrónicos. - Derecho a la accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensible, garantizando especialmente la accesibilidad universal y el diseño para todos de los soportes, canales y entornos con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones. - Sin perjuicio de lo dispuesto en el artículo 13.2, las AAPP podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados. - Derecho a elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las AAPP. - Derecho a poder elegir en todo momento la manera de comunicarse con las AAPP, sea o no por medios electrónicos.
Principales Obligaciones de las AAPP	<ul style="list-style-type: none"> - Las AAPP deberán habilitar diferentes canales o medios para prestación de los servicios electrónicos, garantizando el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos. - Incorporar las características necesarias para garantizar la accesibilidad de aquellos colectivos que lo requieran. - Las AAPP deben facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso. - Las AAPP deben garantizar que aquellos ciudadanos que por cualquier motivo (no disponibilidad de acceso a las nuevas tecnologías o falta de formación) no puedan acceder electrónicamente a la Administración Pública, dispongan de los medios adecuados para seguir comunicándose con la Administración con los mismos derechos y garantías. - La AGE garantizará el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de varios canales que cuente, al menos, con los siguientes medios: art. 8.2.a, 8.2.b y 8.2.c (oficinas de atención presencial con asistencia y orientación, puntos de acceso electrónico, servicio de atención telefónica). - Las AAPP utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse y recabarse por medios electrónicos. - Reglamentariamente, las AAPP podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados 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.
Art. relativos a los Derechos	Exposición de Motivos Capítulo I y II, 6.2.a, 27.1, 27.6 6.2.c, 6.2.k
Art. relativos a los Obligaciones	3.2, 8.1 , 23, 3.2, 8.2, 27.2, 27.6
Ámbitos definidos	Igualdad, accesibilidad a los servicios y canales de acceso

LOPD, Principio de Igualdad, Principio de Accesibilidad, Principio de Legalidad, Principio de Cooperación, Principio de Seguridad, Principio de Proporcionalidad, Principio de Responsabilidad y Calidad, Principio de Neutralidad Tecnológica y de adaptabilidad al Progreso, Principio de Simplificación Administrativa, Principio de Transparencia y Publicidad del Procedimiento de Cooperación, Principio de Seguridad, Principio de Proporcionalidad, Principio de Responsabilidad y Calidad

<p>Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos</p>	<ul style="list-style-type: none"> - Derecho a que el uso de medios electrónicos no signifique merma alguna del derecho del interesado en un expediente a acceder al mismo en la forma tradicional. - Derecho a la conservación en formato electrónico por las AAPP de los documentos electrónicos que formen parte de un expediente. - Derecho a emplear los medios de comunicación y notificación previstos en los artículos 27 y 28 de la Ley para ejercer el derecho a presentar alegaciones en las instrucciones de los procedimientos electrónicos. - Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.
<p>Principales Obligaciones de las AAPP</p>	<ul style="list-style-type: none"> - Las AAPP se adaptarán a lo dispuesto en la Ley para el ejercicio de derechos reconocidos en los artículos 6.2.f, 31.2, 32, 35, 36, 38 y 39. - Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. - La iniciación de un procedimiento administrativo a solicitud de interesado por medios electrónicos requerirá la puesta a disposición de los interesados de los correspondientes modelos o sistemas electrónicos de solicitud en la sede electrónica que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares en los términos establecidos en el apartado i) del artículo 4 y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.
<p>Art. relativos a los Derechos</p>	<p>Exposición de Motivos Capítulo II y III, 6.2.f, 27.3, 36.3</p>
<p>Art. relativos a los Obligaciones</p>	<p>Exposición de Motivos Capítulo II y III, 31.2, 32, 35, 36, 38, 39</p>
<p>Ámbitos definidos para el análisis de la Ley 11/2007</p>	<p>Expediente electrónico</p>

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

LOPD, Principio de Accesibilidad, Principio de Cooperación, Principio de Responsabilidad y Calidad, Principio de Transparencia y Publicidad del Procedimiento	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	<ul style="list-style-type: none"> - Derecho a la igualdad en el acceso electrónico a los servicios de las AAPP - Derecho de los interesados a acceder en línea a verificar la situación de sus expedientes electrónicos y conocer por medios electrónicos, sin mengua de todas las garantías de la privacidad, el estado de tramitación de los procedimientos en los que sean interesados. - Derecho a que el uso de medios electrónicos no signifique merma alguna del derecho del interesado en un expediente a acceder al mismo en la forma tradicional.
Principales Obligaciones de las AAPP	<ul style="list-style-type: none"> - Las AAPP deben facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso. - Las AAPP deben garantizar que aquellos ciudadanos que por cualquier motivo (no disponibilidad de acceso a las nuevas tecnologías o falta de formación) no puedan acceder electrónicamente a la Administración Pública, dispongan de los medios adecuados para seguir comunicándose con la Administración con los mismos derechos y garantías. - Las AAPP deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada. - Los medios o soportes en que se almacenen documentos asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos. - En los procedimientos administrativos gestionados en su totalidad electrónicamente el órgano que tramita el procedimiento pondrá a disposición del interesado un servicio electrónico de acceso restringido, donde éste pueda consultar, previa identificación, el estado de su trámite. Para el resto de procedimientos se habilitarán igualmente servicios electrónicos de información del estado de tramitación que comprendan, al menos, la fase en que se encuentra el procedimiento y el órgano o unidad responsable.
Art. relativos a los Derechos	Exposición de Motivos Capítulo I y II, 6.2.c, 6.2.d, 37
Art. relativos a los Obligaciones	2, 3.2, 8.1, 31.3, 37.1, 37.2
Ámbitos definidos para el análisis de la Ley 11/2007	Acceso electrónico al estado e información de expedientes



LOPD, Principio de Cooperación, Principio de Proporcionalidad

Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos

- Derecho a no aportar los datos y documentos que obren en poder de las AAPP, dando el consentimiento para obtención de sus datos de carácter personal.

Principales Obligaciones de las AAPP

- Cada Administración deberá facilitar el acceso de las restantes administraciones públicas a los datos relativos a los interesados, en la tramitación de un procedimiento, que se le requieran, obren en su poder y se encuentren en soporte electrónico siempre que el interesado preste su consentimiento expreso, el cual podrá emitirse y recabarse por medios electrónicos, al objeto de que los ciudadanos no deban aportar datos y documentos que están en poder de las AAPP.

- Con objeto de facilitar y promover su uso, los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso, ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete.

- La Administración General del Estado, las Administraciones Autonómicas y las entidades que integran la Administración Local, así como los consorcios u otras entidades de cooperación constituidos a tales efectos por éstas, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las AAPP españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

Art. relativos a los Derechos

6.2.b

Art. relativos a los Obligaciones

9, 5.3, 41, 42, 43

Ámbitos definidos para el análisis de la Ley 11/2007

Interoperabilidad

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

LOPD, Principio de Legalidad, Principio de Seguridad, Principio de Responsabilidad y Calidad	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	<ul style="list-style-type: none"> - Derecho a relacionarse con las AAPP por medios electrónicos en condiciones de seguridad jurídica. - Derecho a disponer de condiciones de confianza en el uso de los medios electrónicos. - Derecho a la garantía de seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las AAPP. - Derecho a un mismo nivel de garantías y seguridad al existente para la utilización de medios no electrónicos.
Principales Obligaciones de las AAPP	<ul style="list-style-type: none"> - Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal. - En el intercambio electrónico de datos en entornos cerrados de comunicación deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan. - El Esquema Nacional de Seguridad establecerá la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, estando constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. - Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal.
Art. relativos a los Derechos	1.1, 3.3, 6.2.i
Art. relativos a los Obligaciones	3.3, 20.4, 42, 27.5
Ámbitos definidos para el análisis de la Ley 11/2007	Seguridad jurídica



Exposición de Motivos I, Principio de Accesibilidad, Principio de Cooperación, Principio de Transparencia y Publicidad del Procedimiento

Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos

- Derecho en los procedimientos y trámites relativos al acceso y ejercicio con o sin establecimiento de actividades de servicios, a obtener por medios electrónicos los procedimientos y trámites, datos de autoridades, asociaciones y organizaciones, medios y condiciones de acceso a registros y bases de datos públicos, y vías de recurso (Trasposición de los Art. 6,7 y 8 de la Directiva 2006/123/CE, relativa a los servicios en el mercado interior - Directiva de Servicios).

Principales Obligaciones de las AAPP

- Imposición, al menos en el ámbito de la AGE y en los términos de la Ley, de la obligación de poner a disposición de ciudadanos y empresas al menos un punto de acceso general a través del cual los usuarios puedan de forma sencilla, acceder a la información y servicios de su competencia.

- El punto único electrónico deberá mantenerse coordinado, al menos, con los restantes puntos de acceso electrónico de la AGE y sus Organismos Públicos y se implantarán espacios comunes o ventanillas únicas para obtener la información prevista en el artículo 6.3 de esta Ley y para realizar los trámites y procedimientos a los que hace referencia el apartado a) de dicho artículo.

- Las AAPP garantizarán una cooperación en materia de interoperabilidad de sistemas y aplicaciones (Interoperabilidad de los SI; Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad; Red de comunicaciones de las AAPP españolas; Red integrada de atención al ciudadano).

Art. relativos a los Derechos

Exposición de Motivos Capítulo I, 6.3

Art. relativos a los Obligaciones

Exposición de Motivos Capítulo I, 41, 42, 43, 44

Ámbitos definidos para el análisis de la Ley 11/2007

Ventanillas únicas

**Análisis de la eAdministración e identificación de criterios auditables para la
evaluación del grado de implantación**

LOPD, Principio de Simplificación Administrativa, Principio de Cooperación, Principio de Seguridad, Principio de Legalidad	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	<ul style="list-style-type: none"> - Derecho a que, en su caso, los documentos convencionales se transformen en documentos electrónicos y a que un documento electrónico opere con plena validez en modo convencional. - Derecho a la conservación en formato electrónico por las AAPP de los documentos electrónicos que formen parte de un expediente. - Derecho a obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado. - Derecho a iniciar un procedimiento administrativo por medios electrónicos y a aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada.
Principales Obligaciones de las AAPP	<ul style="list-style-type: none"> - Las AAPP deben regular la validez de los documentos y sus copias y la forma de que el documento electrónico opere con plena validez en modo convencional y, en su caso, la forma en que los documentos convencionales se transformen en documentos electrónicos. - Las AAPP deberán considerar los supuestos considerados en el Art. 31 sobre almacenamiento electrónico de documentos administrativos, la conservación de documentos electrónicos que afecten a derechos o intereses de los particulares, las medidas de seguridad de los medios o soportes en que se almacenen documentos y la garantía de su integridad, autenticidad, confidencialidad, calidad, protección y conservación. - La iniciación de un procedimiento administrativo a solicitud de interesado por medios electrónicos requerirá la puesta a disposición de los interesados de los correspondientes modelos o sistemas electrónicos de solicitud en la sede electrónica que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares en los términos establecidos en el apartado l) del artículo 4 y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales. - Las AAPP deberán considerar los supuestos considerados en el Art. 30 sobre la consideración de copias auténticas, copias electrónicas, imágenes electrónicas, sello electrónico, eliminación de originales en soporte papel y códigos electrónicos de autenticación de documentos electrónicos generados a partir de soporte papel.
Art. relativos a los Derechos	Exposición de Motivos Capítulo III,6.2.f, 6.2.e, 35.2
Art. relativos a los Obligaciones	29.2, 31.1, 31.2, 31.3, 35.1, 30.1, 30.2, 30.3, 30.4, 30.5
Ámbitos definidos para el análisis de la Ley 11/2007	Documento administrativo electrónico y copias electrónicas de documentos



Principio de Legalidad, Principio de Seguridad, Principio de Responsabilidad y Calidad	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	<ul style="list-style-type: none">- Derecho a obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.- Derecho a la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las AAPP.- Derecho a la identificación y autenticación de los ciudadanos por funcionario público.- Sin perjuicio de lo dispuesto en el artículo 13.2, las AAPP podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados.
Principales Obligaciones de las AAPP	<ul style="list-style-type: none">- Las AAPP admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, utilizando sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente, sistemas de firma electrónica para la actuación administrativa automatizada, firma electrónica del personal al servicio de las AAPP, e intercambio electrónico de datos en entornos cerrados de comunicación.- Los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las AAPP como válidos para relacionarse con las mismas.- La relación de sistemas de firma electrónica avanzada admitidos, con carácter general, en el ámbito de cada Administración Pública, deberá ser pública y accesible por medios electrónicos.- Las AAPP podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.- Las AAPP mantendrán actualizado un registro de los funcionarios habilitados para la identificación o autenticación regulada en el artículo 22.
Art. relativos a los Derechos	6.2.g, 6.2.h, 13.2, 14, 15.1, 22, 23
Art. relativos a los Obligaciones	13.1, 13.3, 15.2, 15.3, 16, 17, 18, 21, 22, 23
Ámbitos definidos para el análisis de la Ley 11/2007	Firma electrónica

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicos	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	- Derecho a elegir las aplicaciones o sistemas para relacionarse con las AAPP siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.
Principales Obligaciones de las AAPP	- Las AAPP garantizarán la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las AAPP, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las AAPP utilizarán estándares abiertos así como en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos. - La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos. - Las AAPP mantendrán directorios actualizados de aplicaciones para su libre reutilización, especialmente en aquellos campos de especial interés para el desarrollo de la administración electrónica y de conformidad con lo que al respecto se establezca en el Esquema Nacional de Interoperabilidad.
Art. relativos a los Derechos	6.2.k
Art. relativos a los Obligaciones	10.5, 35, 42.4, 46.1
Ámbitos definidos para el análisis de la Ley 11/2007	Estándares abiertos

Principio de Accesibilidad, Principio de Cooperación, Principio de Responsabilidad y Calidad, Principio de Simplificación Administrativa	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	- Derecho de los ciudadanos a comunicarse electrónicamente con la Administración disponiendo de una «sede» administrativa electrónica con la que establecer las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad. - Derecho a disponer de medios para la formulación de sugerencias y quejas que sean identificables. - Derecho a los principios de accesibilidad y usabilidad, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado.
Principales Obligaciones de las AAPP	- Las AAPP crearán direcciones electrónicas disponibles a los ciudadanos llamadas "sedes electrónicas", como lugares de prestación de servicios electrónicos e información con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, usabilidad, neutralidad, estándares abiertos e interoperabilidad.
Art. relativos a los Derechos	Exposición de Motivos Capítulo I, 10
Art. relativos a los Obligaciones	Exposición de Motivos Capítulo III, 10
Ámbitos definidos para el análisis de la Ley 11/2007	Sede administrativa electrónica

Principio de Accesibilidad, Principio de Cooperación, Principio de Simplificación Administrativa	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	- Derecho a disponer de registros electrónicos en las sedes electrónicas que permitan la presentación de solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro horas.
Principales Obligaciones de las AAPP	- Las AAPP crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones del ámbito de la administración titular del registro, pudiendo habilitar sus registros mediante convenios de colaboración para recepcionar aquellas competencias de otra Administración. - Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.
Art. relativos a los Derechos	24, 25, 26
Art. relativos a los Obligaciones	24, 25, 26, 29.2
Ámbitos definidos para el análisis de la Ley 11/2007	Registro electrónico

La Ley consagra la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones. El reconocimiento de tal derecho y su correspondiente obligación se erigen así en el eje central del proyecto de Ley	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	- Derecho a que se cumpla el objeto de la Ley en su ámbito de aplicación. - Derecho a ejercer los derechos reconocidos en el Art. 6 de la Ley.
Principales Obligaciones de las AAPP	- Las AAPP se adaptarán a lo dispuesto en la Ley para el ejercicio de derechos reconocidos en el artículo 6 en relación con la totalidad de los procedimientos y actuaciones de su competencia. En el ámbito de la AGE y organismos públicos vinculados o dependientes a partir del 31 de diciembre de 2009. En el ámbito de las CCAA y Entidades que integran la Administración Local, a partir del 31 de diciembre de 2009, siempre que lo permitan sus disponibilidades presupuestarias.
Art. relativos a los Derechos	Exposición de Motivos Título preliminar. Disposición final tercera
Art. relativos a los Obligaciones	Exposición de Motivos Título preliminar. Disposición final tercera
Ámbitos definidos para el análisis de la Ley 11/2007	Cumplimiento de los plazos de adaptación a la Ley

**Análisis de la eAdministración e identificación de criterios auditables para la
evaluación del grado de implantación**

Exposición de Motivos I, Principio de Igualdad, Principio de Accesibilidad, Principio de Legalidad, Principio de Seguridad, Principio de Simplificación Administrativa, Principio de Transparencia y Publicidad del Procedimiento	
Principales Derechos de los ciudadanos a relacionarse con las AAPP por medios electrónicos	<ul style="list-style-type: none"> - Las AAPP podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados 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. - Derecho a que el interesado señale como preferente o haya consentido la utilización para que la AAPP le practique notificaciones utilizando algún medio electrónico, sin perjuicio de lo dispuesto en el artículo 27.6. - Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la Ley 30/1992, excepto en los casos previstos en el artículo 27.6.
Principales Obligaciones de las AAPP	<ul style="list-style-type: none"> - Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento citados en el Art. 28.1 podrán emitirse y recabarse, en todo caso, por medios electrónicos. - El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido. - Cuando, existiendo constancia de la puesta a disposición transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el artículo 59.4 de la Ley 30/1992, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso. - Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dichos acceso. - Podrán adoptarse y notificarse resoluciones de forma automatizada en aquellos procedimientos en los que así esté previsto.
Art. relativos a los Derechos	27.3, 27.6, 28.1, 28.4
Art. relativos a los Obligaciones	28.1, 28.2, 28.3, 28.5, 36.3, 38.2
Ámbitos definidos para el análisis de la Ley 11/2007	Notificaciones electrónicas

8.2 Implementación de servicios on-line desde la Administración

Una vez diseccionada la Ley 11/2007, se intenta llevar a cabo otro de los objetivos de este proyecto, identificar mediante el análisis realizado una serie de criterios que permitan evaluar el grado de implantación de la eAdministración en las AAPP.

Por un lado esta el cómo valorar el grado de implantación. Para poder medir el nivel de adaptación de los servicios on-line desde las AAPP, se mide mediante la escala eEurope. Para poder marcar un nivel donde no se tenga ninguna actividad realizada, se añade un nivel 0 y así se consigue catalogarlo. La tabla resultante muestra los valores de dichos niveles:

Nivel 0	No existe información
Nivel 1: Información	La información necesaria para comenzar el procedimiento para obtener el servicio público está disponible on-line
Nivel 2: Interacción en un camino	<p>La página Web accesible públicamente ofrece la posibilidad de obtener de un modo no-electrónico (descargando formularios) el formulario en papel para comenzar el procedimiento para obtener el servicio.</p> <p>Un formulario electrónico utilizado para solicitar el formulario no-electrónico se considera también dentro del nivel 2</p>
Nivel 3: Interacción en dos caminos	<p>La página Web accesible públicamente ofrece la posibilidad de realizar un envío electrónico a través de un formulario electrónico oficial, de comenzar el procedimiento para obtener el servicio.</p> <p>Esto implica que debe ser un formulario de autenticación de la persona (física o jurídica) que solicita los servicios para alcanzar el nivel 3.</p>
Nivel 4: Manejo de casos electrónicos completos	<p>La página Web accesible públicamente ofrece la posibilidad de tratar por completo el servicio público por medio de la Web, incluyendo la resolución y la entrega.</p> <p>No es necesario ningún otro procedimiento formal en papel para el solicitante del servicio.</p>
Nivel 5: Personalización	<p>El solicitante recibe el servicio automáticamente, basado en el registro previo de un evento, de forma que éste es personalizado.</p> <p>Este 5º nivel de sofisticación introduce dos conceptos extras:</p> <ul style="list-style-type: none">- La idea de un servicio de entrega pro-activo- La idea de un servicio automático de entrega. <p>No existe la necesidad de que el usuario demande tal servicio.</p>

Tabla 4 – Valores eEurope

Poder realizar un análisis de los Organismos Públicos en cuanto a su adaptación a la eAdministración, ha supuesto un problema que no estaba planteado a priori. Se ha comentado que cada Organismo Público tiene unas competencias diferentes y por lo tanto no pueden ser catalogadas por las mismas características. Por lo tanto, en este proyecto se ha tomado la decisión de centrar el estudio en un único Organismo Público, el referido a las Comunidades Autónomas.

Teniendo determinado el Organismo Público a estudiar, se ha buscado toda la información posible sobre ellos. Gracias a fuentes de información como los repositorios de información Web de las CCAA y a estudios públicos como los realizados por la ONTSI, OEA y otros privados como los llevados a cabo por Telefónica entre otros, se pueden obtener unos datos medibles.

Conociendo los valores estándares de la escala eEurope, se pueden puntuar los criterios que permiten evaluar el nivel de implantación de la eAdministración en la Comunidad Autónoma que se quiera evaluar.

Habiendo analizado los datos de los que se disponen para poder medirlos, los factores que se pueden extrapolar a todas las comunidades para conocer el grado de adaptación de la eAdministración son los siguientes:

1. Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados
2. Cita previa
3. Quejas y sugerencias de los ciudadanos
4. Expedición de licencias de caza y pesca
5. Impuesto de sucesiones
6. Ubicación de servicios
7. Oferta de Empleo Público
8. Certificado de estar al corriente de las obligaciones fiscales
9. Autorización de Instalaciones Eléctricas de Baja Tensión
10. Consulta Bibliotecas Públicas
11. Gestión de residuos medioambientales
12. Cambio de médico
13. Preinscripción en centros de enseñanza
14. Comunicación de accidentes laborales
15. Comunicación de la apertura del centro de trabajo
16. Solicitud de la tarjeta sanitaria
17. Sistema de información geográfica de identificación de parcelas agrícolas (SIGPAC)
18. Cambio de centro sanitario
19. Legislación/normativa autonómica
20. Reserva de plazas en albergues
21. Oferta de empleo privado
22. Expedición de permisos de caza y pesca



La fecha de los datos analizados corresponden a los años 2007, 2008 y 2009. En años posteriores no se han publicado más datos cuantificables a nivel nacional. Se entiende que a raíz de la Ley 11/2007 existirían unas partidas presupuestarias para adaptarse a dicha Ley y de ahí que determinados organismos se interesaran por cuantificar la mayoría de los datos posibles.

Hasta el último año mencionado, 2009, se podían observar similitudes en los procesos a evaluar, pero una vez pasado ese año, cada CCAA hacía valer sus criterios, que eran todos muy diferentes entre ellas, haciendo imposible aunar algún criterio que sirviera para más de dos CCAA.

De todas las Comunidades Autónomas, el análisis realizado refleja los datos de cinco, por ser las más representativas y en cuanto mayor número de datos se han podido obtener. Las seleccionadas son las siguientes:

- Junta de Andalucía.
- Junta de Castilla y León
- Generalitat de Cataluña
- Generalitat Valenciana
- Comunidad de Madrid

Los datos, resumidos en tablas donde se muestran los criterios y los años junto a sus valores, son los siguientes. En algunos años y para algunos factores no existen datos, los cuales han sido etiquetados como N.d. (No disponible).

**Análisis de la eAdministración e identificación de criterios auditables para la
evaluación del grado de implantación**

Junta de Andalucía

Criterios	Andalucía		
	2007	2008	2009
Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados	4	4	4
Cita previa	4	4	4
Quejas y sugerencias de los ciudadanos	4	4	4
Expedición de licencias de caza y pesca	4	4	4
Impuesto de sucesiones	2	N.d.	N.d.
Ubicación de servicios	4	N.d.	N.d.
Oferta de Empleo Público	4	4	4
Certificado de estar al corriente de las obligaciones fiscales	4	4	N.d.
Autorización de Instalaciones Eléctricas de Baja Tensión	4	4	4
Consulta Bibliotecas Públicas	4	4	4
Gestión de residuos medioambientales	4	4	4
Cambio de médico	4	4	N.d.
Preinscripción en centros de enseñanza	4	N.d.	4
Comunicación de accidentes laborales	0	N.d.	N.d.
Comunicación de la apertura del centro de trabajo	2	2	N.d.
Solicitud de la tarjeta sanitaria	2	N.d.	N.d.
Sistema de información geográfica de identificación de parcelas agrícolas (SIGPAC)	4	4	4
Cambio de centro sanitario	4	N.d.	N.d.
Legislación/normativa autonómica	1	1	N.d.
Reserva de plazas en albergues	N.d.	4	4
Oferta de empleo privado	N.d.	4	1
Expedición de permisos de caza y pesca	N.d.	N.d.	4

Junta de Castilla y León

Criterios	Castilla y León		
	2007	2008	2009
Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados	4	4	4
Cita previa	0	0	0
Quejas y sugerencias de los ciudadanos	3	3	3
Expedición de licencias de caza y pesca	3	3	4
Impuesto de sucesiones	4	N.d.	N.d.
Ubicación de servicios	4	N.d.	4
Oferta de Empleo Público	3	4	4
Certificado de estar al corriente de las obligaciones fiscales	1	1	
Autorización de Instalaciones Eléctricas de Baja Tensión	5	5	4
Consulta Bibliotecas Públicas	3	3	4
Gestión de residuos medioambientales	2	3	4
Cambio de médico	0	0	4
Preinscripción en centros de enseñanza	4	N.d.	2
Comunicación de accidentes laborales	1	1	N.d.
Comunicación de la apertura del centro de trabajo	4	4	N.d.
Solicitud de la tarjeta sanitaria	4	N.d.	N.d.
Sistema de información geográfica de identificación de parcelas agrícolas (SIGPAC)	4	4	4
Cambio de centro sanitario	0	N.d.	N.d.
Legislación/normativa autonómica	N.d.	1	N.d.
Reserva de plazas en albergues	N.d.	0	N.d.
Oferta de empleo privado	N.d.	4	3
Expedición de permisos de caza y pesca	3	N.d.	4



Generalitat de Cataluña

Criterios	Cataluña		
	2007	2008	2009
Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados	4	4	4
Cita previa	4	4	4
Quejas y sugerencias de los ciudadanos	3	3	4
Expedición de licencias de caza y pesca	4	4	N.d.
Impuesto de sucesiones	4	N.d.	
Ubicación de servicios	4	N.d.	4
Oferta de Empleo Público	3	3	3
Certificado de estar al corriente de las obligaciones fiscales	0	N.d.	N.d.
Autorización de Instalaciones Eléctricas de Baja Tensión	2	2	2
Consulta Bibliotecas Públicas	3	N.d.	3
Gestión de residuos medioambientales	4	4	4
Cambio de médico	4	N.d.	N.d.
Preinscripción en centros de enseñanza	4	N.d.	4
Comunicación de accidentes laborales	4	4	N.d.
Comunicación de la apertura del centro de trabajo	4	4	N.d.
Solicitud de la tarjeta sanitaria	3	N.d.	N.d.
Sistema de información geográfica de identificación de parcelas agrícolas (SIGPAC)	3	4	N.d.
Cambio de centro sanitario	4	N.d.	N.d.
Legislación/normativa autonómica	4	4	N.d.
Reserva de plazas en albergues	N.d.	4	4
Oferta de empleo privado	N.d.	3	3
Expedición de permisos de caza y pesca	4	N.d.	N.d.

Generalitat Valenciana

Criterios	Valencia		
	2007	2008	2009
Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados	4	4	4
Cita previa	4	4	4
Quejas y sugerencias de los ciudadanos	3	4	4
Expedición de licencias de caza y pesca	2	2	3
Impuesto de sucesiones	2	N.d.	N.d.
Ubicación de servicios	4	N.d.	4
Oferta de Empleo Público	4	2	2
Certificado de estar al corriente de las obligaciones fiscales	2	2	N.d.
Autorización de Instalaciones Eléctricas de Baja Tensión	4	4	4
Consulta Bibliotecas Públicas	2	2	4
Gestión de residuos medioambientales	4	4	4
Cambio de médico	2	2	N.d.
Preinscripción en centros de enseñanza	4	N.d.	4
Comunicación de accidentes laborales	0	2	N.d.
Comunicación de la apertura del centro de trabajo	2	2	N.d.
Solicitud de la tarjeta sanitaria	1	N.d.	N.d.
Sistema de información geográfica de identificación de parcelas agrícolas (SIGPAC)	3	N.d.	4
Cambio de centro sanitario	2	N.d.	N.d.
Legislación/normativa autonómica	4	4	N.d.
Reserva de plazas en albergues	N.d.	4	4
Oferta de empleo privado	N.d.	2	4
Expedición de permisos de caza y pesca	3	N.d.	3

**Análisis de la eAdministración e identificación de criterios auditables para la
evaluación del grado de implantación**

Comunidad de Madrid

Criterios	Madrid		
	2007	2008	2009
Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados	2	2	2
Cita previa	4	4	4
Quejas y sugerencias de los ciudadanos	4	4	4
Expedición de licencias de caza y pesca	4	4	1
Impuesto de sucesiones	2	N.d.	N.d.
Ubicación de servicios	2	N.d.	4
Oferta de Empleo Público	2	2	2
Certificado de estar al corriente de las obligaciones fiscales	4	2	N.d.
Autorización de Instalaciones Eléctricas de Baja Tensión	3	2	2
Consulta Bibliotecas Públicas	1	1	4
Gestión de residuos medioambientales	3	3	4
Cambio de médico	1	1	N.d.
Preinscripción en centros de enseñanza	2	N.d.	2
Comunicación de accidentes laborales	1	1	N.d.
Comunicación de la apertura del centro de trabajo	3	4	N.d.
Solicitud de la tarjeta sanitaria	2	N.d.	N.d.
Sistema de información geográfica de identificación de parcelas agrícolas (SIGPAC)	2	2	4
Cambio de centro sanitario	1	N.d.	N.d.
Legislación/normativa autonómica	1	1	N.d.
Reserva de plazas en albergues	N.d.	3	4
Oferta de empleo privado	N.d.	2	4
Expedición de permisos de caza y pesca	4	N.d.	1

En el análisis para la recopilación de valores, existen casos en los que parece que existe un retroceso en la creación de dichos servicios al ciudadano. Esto es posible a varios factores, siendo el más probable una mala medición de los datos.

Para terminar, se muestran todas las tablas unificadas. Para ello el nombre de los factores se identifican mediante letras, siendo el resultado el siguiente:

Letra	Descripción
A	Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados
B	Cita previa
C	Quejas y sugerencias de los ciudadanos
D	Expedición de licencias de caza y pesca
E	Impuesto de sucesiones
F	Ubicación de servicios
G	Oferta de Empleo Público
H	Certificado de estar al corriente de las obligaciones fiscales
I	Autorización de Instalaciones Eléctricas de Baja Tensión
J	Consulta Bibliotecas Públicas
K	Gestión de residuos medioambientales
L	Cambio de médico
M	Preinscripción en centros de enseñanza
N	Comunicación de accidentes laborales
O	Comunicación de la apertura del centro de trabajo
P	Solicitud de la tarjeta sanitaria
Q	Sistema de información geográfica de identificación de parcelas agrícolas (SIGPAC)
R	Cambio de centro sanitario
S	Legislación/normativa autonómica
T	Reserva de plazas en albergues
U	Oferta de empleo privado
V	Expedición de permisos de caza y pesca

Tabla 5 – Valores de criterios pasados a letras

La tabla completa resultante es la siguiente:

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

CCAA	Andalucía			Castilla y León			Cataluña			Valencia			Madrid		
	2007	2008	2009	2007	2008	2009	2007	2008	2009	2007	2008	2009	2007	2008	2009
A	4	4	4	4	4	4	4	4	4	4	4	4	2	2	2
B	4	4	4	0	0	0	4	4	4	4	4	4	4	4	4
C	4	4	4	3	3	3	3	3	4	3	4	4	4	4	4
D	4	4	4	3	3	4	4	4	N.d	2	2	3	4	4	1
E	2	N.d	N.d	4	N.d		4	N.d	N.d	2	N.d	N.d	2	N.d	N.d
F	4	N.d	N.d	4	N.d	4	4	N.d	4	4	N.d	4	2	N.d	4
G	4	4	4	3	4	4	3	3	3	4	2	2	2	2	2
H	4	4	N.d	1	1	N.d	0	N.d	N.d	2	2	N.d	4	2	N.d
I	4	4	4	5	5	4	2	2	2	4	4	4	3	2	2
J	4	4	4	3	3	4	3	N.d	3	2	2	4	1	1	4
K	4	4	4	2	3	4	4	4	4	4	4	4	3	3	4
L	4	4	N.d	0	0	4	4	N.d	N.d	2	2	N.d	1	1	N.d
M	4	N.d	4	4	N.d	2	4	N.d	4	4	N.d	4	2	N.d	2
N	0	N.d	N.d	1	N.d	N.d	4	4	N.d	0	2	N.d	1	1	N.d
O	2	2	N.d	4	N.d	N.d	4	4	N.d	2	2	N.d	3	4	N.d
P	2	N.d	N.d	4	N.d	N.d	3	N.d	N.d	1	N.d	N.d	2	N.d	N.d
Q	4	4	4	4	N.d	N.d	3	4	N.d	3	N.d	4	2	2	4
R	4	N.d	N.d	0	N.d	N.d	4	N.d	N.d	2	N.d	N.d	1	N.d	N.d
S	1	1	N.d	1	1	N.d	4	4	N.d	4	4	N.d	1	1	N.d
T	N.d	4	4	N.d	0		N.d	4	4	N.d	4	4	N.d	3	4
U	N.d	4	1	N.d	4	3	N.d	3	3	N.d	2	4	N.d	2	4
V	N.d	N.d	4	3	N.d	4	4	N.d	N.d	3	N.d	3	4	N.d	1

Tabla 6 – Tabla de valores por CCAA

9 CONCLUSIONES

Una vez descrito el análisis sobre la eAdministración, se exponen una serie de conclusiones intentando puntualizar todos los puntos de vista de la Administración electrónica, desde Europa hasta las Comunidades Autónomas, comentar las TIC, la propia eAdministración y sus tendencias futuras, terminando en la aportaciones y líneas futuras de este proyecto.

9.1 Introducción

El efecto más directo de la Ley 11/2007 ha sido el importante incremento de los procedimientos de las Administraciones Públicas accesibles mediante Internet. Según la información que proporciona la Dirección General del Estado para el Impulso de la Administración Electrónica del Ministerio de Política Territorial y Administración Pública, a finales del año 2010 en la Administración General del Estado ya eran totalmente accesibles on-line el 99% de sus procedimientos de alto impacto y el 92% de todos sus procedimientos. Dado que los procedimientos más utilizados por los ciudadanos están clasificados como de “alto impacto”, los procedimientos ya adaptados a la Ley, esto es, totalmente accesibles on-line, cubren el 98% de toda la tramitación que los ciudadanos realizan con la Administración General del Estado.

En la Administración General del Estado, la consecución de estos elevados niveles de accesibilidad ha sido posible gracias al importante esfuerzo realizado por todos los departamentos ministeriales y a la creación y utilización de un conjunto de infraestructuras y servicios comunes que han actuado como habilitadores para el despliegue de los servicios electrónicos de cada departamento ministerial. Parte de esta infraestructura común está constituida por la red de comunicaciones SARA, que conecta a todos los ministerios entre sí y a estos con Comunidades Autónomas y Entidades Locales y que a su vez tiene conexión con la red académica y de investigación RedIris, que proporciona acceso a los servicios comunes. Entre estos servicios comunes destacan la infraestructura relacionada con la identificación electrónica (documento nacional de identidad electrónico, con 23 millones de DNle emitidos hasta mayo de 2011, y la plataforma de validación de certificados y firma electrónica @firma, que en los cinco primeros meses del año 2011 ha realizado casi 30 millones de validaciones) y la infraestructura de notificación electrónica (en mayo de 2011 había ya alcanzado la cifra de casi 150.000 direcciones electrónicas y se habían realizado más de 780.000 notificaciones electrónicas en los cinco primeros meses del año), según datos de la Dirección General del Estado.

Esta importante mejora en el nivel de desarrollo de la Administración electrónica en España también ha sido puesta de relieve en los estudios que realizan organismos internacionales, como la Comisión Europea y la Organización de las Naciones Unidas.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Para constatar estos datos se muestran la siguiente tabla, cuyos datos han sido obtenidos mediante ONTSI e INE.

Datos madurez de los servicios				
Objetivos	Ámbito	2010	2009	2008
Ciudadanos	España	97%	85%	77%
Empresas	España	100%	94%	93%
Procedimientos y servicios adaptados Ley 11/2007 en AGE	AGE	92%	83%	19%
Disponibilidad de procedimientos y servicios en CCAA	CCAA	72%	67%	10%

Tabla 7 – Tabla de valores por servicio

9.2 Las TIC

Las TIC han sido y están siendo un factor de cambio relevante para la organización y funcionamiento de las Administraciones Públicas, debido a las posibilidades que incorporan y que hacen posible una gestión mucho más eficiente:

- Agilizando la comunicación e intercambio de datos.
- Desarrollando estructuras horizontales.
- Permitiendo trabajar a distancia y crear espacios virtuales de generación de conocimiento.

Sin embargo, las TIC son únicamente un instrumento para el cambio. La adopción del uso de las TIC en la Administración Pública, como mínimo, implica:

- Dotar de infraestructuras tecnológicas y de acceso a éstas, tanto a la Administración como a la ciudadanía.
- Organizar toda la información disponible, como carta de servicios, actividades, legislación, cartografías, recursos turísticos, planos territoriales, campañas de prevención, ayudas y subvenciones, equipo de gobierno y oposición, concursos, licitaciones, etc. y mantenerla actualizada, de forma que las personas que la necesitan la puedan encontrar, acceder y entenderla.



- Establecer canales de comunicación bidireccional y multidireccional con formas de participación activa entre la administración y la ciudadanía.
- Gestionar la capacidad de escuchar a la ciudadanía, a partir de los mecanismos de participación que se hayan puesto en marcha, y de darle respuestas.
- Disponer que todos los trámites que una persona, empresa u otra institución pública necesita realizar con la Administración, desde pedir hora al médico hasta gestionar una licencia de obras, para poner algunos ejemplos, se puedan tramitar utilizando las tecnologías de la información y las comunicaciones, con herramientas como Internet o el teléfono móvil, que son las que tenemos actualmente, o las que nos pueda proveer el futuro.
- Cooperar con otras administraciones para simplificar de cara a la ciudadanía las gestiones con la Administración. Eso implica apostar por tecnologías que permitan la interoperabilidad de los datos procedentes de diferentes Administraciones, la utilización de estándares tecnológicos que faciliten el intercambio de datos y el acceso desde dispositivos múltiples. Cada institución tiene sus propias competencias y es propietaria y responsable de cierta información, pero la ciudadanía no tiene por qué saber a qué institución o departamento tiene que acudir en cada momento según las necesidades que tenga, ni tener que ir recurriendo instituciones y territorio en busca de documentación indispensable, llevando papeleo arriba y abajo, para acceder a un servicio concreto.
- Asegurar la identificación unívoca del ciudadano o ciudadana que se pone en contacto con la administración de forma digital y la veracidad de los datos que se tramitan dentro de los marcos de confidencialidad y confianza adecuados para cada tipo de interacción, utilizando la firma digital o el DNI electrónico.

Llegar a este estado, donde la Administración Pública y la ciudadanía actuarán de forma natural para ejercer sus derechos y deberes en una sociedad propia de la era de la información, sólo será posible si se establece un proceso de aprendizaje y de adaptación.

Por lo tanto, aunque ya se ha empezado a hacer trabajo para que la Administración Pública haga un uso eficiente de las TIC, las tareas futuras a realizar serían:

- Investigación e innovación, para ir construyendo las aplicaciones que faciliten el acceso, la gestión y la interoperabilidad de la información: Web semántica, sistemas de información geográfica, utilización de estándares, etc.
- Alfabetización digital, para que todas las personas sepan cuáles son los instrumentos, como se utilizan las TICs y qué posibilidades y oportunidades ofrecen.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

- Alfabetización informacional, para que el funcionariado y ciudadanía tengan las competencias mínimas para gestionar la información y comunicarse digitalmente con los otros en función del contexto, el objetivo y el destinatario del mensaje.
- Gestión del conocimiento, para que todo lo que se aprende y se gestiona se comparta y todos los frentes que hay abiertos confluyan en el objetivo común de conducir la Administración Pública a la Sociedad de la Información.
- Gestión del cambio, para poner los fundamentos que aseguren que todos estos cambios se adaptarán correctamente venciendo las resistencias que puedan ir surgiendo.
- Conseguir llegar a la Administración y al Gobierno electrónico, que posibilita el uso de las TIC, será posible si se hace desde la filosofía que nació y se expandió por Internet: desde el trabajo en red, la innovación, la cooperación, la pasión, el respeto y la implicación personal.

9.3 Europa

La Agenda Digital para Europa marca la estrategia de Europa en Sociedad de la Información hasta el año 2020 con objeto de conseguir una economía más productiva y competitiva, con mayores niveles de empleo y cohesión social y con menores niveles de emisión de carbono.

Si nos fijamos en los datos de EuroStat 2011 a nivel empresa de los últimos años, ha aumentado el número de compañías que utilizan Internet para recibir pedidos, comprar o vender, que han enviado o recibido facturas electrónicas y que utilizan firma electrónica con sus clientes y/o proveedores, aspecto en el que España es uno de los países líderes. A pesar de estos datos positivos, el número de empleados que utiliza ordenadores conectados a Internet muestra una cierta estabilidad. Posiblemente, tras incorporar las tecnologías a los procesos productivos, las empresas están ahora poniendo sus esfuerzos en la utilización de tecnologías de la información para relacionarse con otras compañías y sus clientes.

9.4 España

En cuanto a España, la Sociedad de la Información sigue creciendo en hogares y empresas: un 70% de los hogares disponía ya de ordenador y el número de hogares con 3 o 4 servicios (considerando fijo, móvil, Internet y televisión de pago) alcanzaba el 55% en 2011 frente al 52% del año anterior, según el estudio realizado por la función Orange. Si consideramos el número de internautas de 10 o más años que han accedido alguna vez a Internet, se superaban los 27 millones de internautas y aumentan de manera importante los usos en actividades nuevas, como las redes sociales. Es de destacar el denominado apagón analógico del 3 de abril de 2010 y el encendido digital de la televisión digital terrestre (TDT), que permitió a los ciudadanos acceder a una televisión de más canales con mayor calidad.

También se mantiene la actitud positiva hacia las tecnologías con un reconocimiento de los ciudadanos hacia el papel que juegan en la educación y en el mundo laboral. Los ciudadanos verían con buenos ojos que es necesario que las Administraciones Públicas contribuyesen a su conocimiento y difusión.

El comercio electrónico B2C alcanzó en 2010 (datos de la fundación orange) 9.100 millones de euros, lo que supone un incremento del 17,3% respecto a 2009, con 10,9 millones de internautas compradores.

9.5 Administración Electrónica

La Ley 11/2007 reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. El efecto más directo de la Ley ha sido que el 98% de los procedimientos de las Administraciones Públicas a principios de 2011 ya eran totalmente accesibles online. Esto significa que actualmente se cubre de manera online casi al 100% de toda la tramitación que los ciudadanos realizan con la Administración General del Estado.

En cuanto a indicadores, destacan las infraestructuras relacionadas con la identificación electrónica (documento nacional de identidad electrónico, con 23 millones de DNle emitidos hasta mayo de 2011, y la plataforma de validación de certificados y firma electrónica @firma, que en los cinco primeros meses del año 2011 ha realizado casi 30 millones de validaciones, según la Dirección General del Estado).

Según un informe de la Comisión Europea el 95% de una serie de servicios públicos que consideran básicos, (son 20 puntos donde doce se basan en los ciudadanos y ocho en las empresas) se encuentran disponibles a través de Internet en España, superando el 82% de media de UE y con un considerable incremento de 15 situando a España en el octavo lugar en una lista de 32 países en 2009. A continuación se puede ver los datos.

	2003	2004	2006	2007	2009
Austria	68	72	83	100	100
Malta	s.d.	40	75	95	100
Portugal	37	40	60	90	100
Reino Unido	50	59	71	89	100
Eslovenia	s.d.	45	65	90	95
Suecia	67	74	74	75	95
Estonia	s.d.	63	79	70	90
Finlandia	61	67	61	67	89
Dinamarca	72	58	63	63	84
Irlanda	56	50	50	50	83
España	50	55	55	70	80
Francia	45	50	65	70	80
Holanda	26	32	53	63	79
Alemania	40	47	47	75	74

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

UE 27	s.d.	s.d.	s.d.	59	71
Bélgica	35	35	47	60	70
Italia	45	53	58	70	70
Luxemburgo	15	20	25	40	68
Letonia	s.d.	5	10	30	65
Hungría	s.d.	15	50	50	63
Lituania	s.d.	40	40	35	60
Rep.Checa	s.d.	30	30	55	60
Eslovaquia	s.d.	15	20	35	55
Polonia	s.d.	10	20	25	53
Chipre	s.d.	25	35	45	50
Grecia	32	32	30	45	45
Rumania	s.d.	s.d.	s.d.	35	45
Bulgaria	s.d.	s.d.	s.d.	15	40

Tabla 8 – Tabla nivel adaptación Europea

* s.d.: Sin datos

Otro punto interesante es la puesta a disposición pública de datos de las Administraciones para su uso por ciudadanos y empresas, permitiendo nuevos modelos de negocio, lo que se ha dado en llamar el sector *infomediario*. Este concepto se desarrolla en el proyecto *Propuesta de herramienta para la evaluación del grado de implantación de la eAdministración en CCAA* que continua a este estudio.

La Sociedad de la Información sigue avanzando pasos y serán necesarios nuevos métodos de medida, que nos proporcionen información para estudiar un fenómeno que cada día impacta más en nuestras vidas.

9.6 Tendencias

La Banda Ancha ultrarrápida mejora la calidad y velocidad de las comunicaciones y servirá como soporte para el crecimiento de la industria de contenidos digitales. El *cloud computing* (concepto que permite ofrecer servicios electrónicos a través de la red), permitirá nuevas utilidades de geoposicionamiento para los usuarios, posibilitando el crecimiento de los tablets y dispositivos individuales de acceso a la información, tales como dispositivos móviles, smartphones, tablets o PDAs.

España se sitúa entre los 10 mejores países del mundo en implantación del *eGovernment* (eAdministración) subiendo 11 puestos a principios de 2010. Ocupando el noveno puesto pero siendo la mejor subida de posición de entre los 10 primeros puestos.







Country	E-Government 2010	Rank 2010	Rank 2008	Rank Change
 Republic of Korea	0.8785	1	6	+5 ↑
 United States of America	0.8510	2	4	+2 ↑
 Canada	0.8448	3	7	+4 ↑
 United Kingdom of Great Britain and Northern Ireland	0.8147	4	10	+6 ↑
 Netherlands	0.8097	5	5	--
 Norway	0.8020	6	3	-3 ↓
 Denmark	0.7872	7	2	-5 ↓
 Australia	0.7863	8	8	--
 Spain	0.7516	9	20	+11 ↑
 France	0.7510	10	9	-1 ↓

Imagen 9-1 Implantación eGovernment

Las AAPP han trabajado muy bien (y siguen haciéndolo) con la eAdministración, ya que presenta muchas oportunidades innovadoras de emplear las tecnologías para mejorar los servicios al ciudadano y conseguir mayores niveles de democracia a través de la participación directa del mismo en la actividad pública. Sin olvidar la obligatoriedad que de por ley les está siendo impuesta.

Tomando como punto de partida el Plan Avanza aprobado en 2005, así como el marco europeo en el que se encuadran este tipo de iniciativas, se han identificado treinta y cuatro retos concretos que debe abordar España en el ámbito de las TIC. En este contexto, la Estrategia 2011-2015 del Plan Avanza 2 va a centrar sus esfuerzos en la consecución de los siguientes diez objetivos que facilitarán la superación de los retos definidos:

1. Promover procesos innovadores TIC en las Administraciones Públicas.
2. Extender las TIC en la sanidad y el bienestar social.
3. Potenciar la aplicación de las TIC al sistema educativo y formativo.
4. Mejorar la capacidad y la extensión de las redes de telecomunicaciones.

5. Extender la cultura de la seguridad de la información entre la ciudadanía y las empresas.
6. Incrementar el uso avanzado de servicios digitales por la ciudadanía.
7. Extender el uso de soluciones TIC de negocio en la empresa.
8. Desarrollar las capacidades tecnológicas del sector TIC.
9. Fortalecer el sector de contenidos digitales.
10. Desarrollar las TIC verdes.

El Plan Avanza toma las medidas necesarias para impulsar y alinear a nuestro país en el contexto digital europeo, en línea con los objetivos de la Agenda.

9.7 Aportación

Para comentar la aportación de este proyecto, hay que volver a recordar la motivación del mismo. La motivación del proyecto es ayudar a profesionales informáticos a ponerse al día lo más rápidamente, si tuviesen que desarrollar software para las Administraciones Públicas.

Una vez leído este trabajo, queda cubierta la motivación principal del mismo, al quedar descrito el entorno de la eAdministración desde todos los ámbitos, tanto legales como actuaciones a todos los niveles (Europeos, Nacionales, Comunidades Autónomas y Administraciones Locales).

En lo referente a la Administración Pública en España, la Ley 11/2007 es la que marca las directrices a tomar para afrontar el reto de la eAdministración. Para ello se desarrollan ampliamente una serie de conceptos, derechos para los ciudadanos y obligaciones a las Administraciones Públicas.

Como es de esperar, resulta una ley especialmente compleja y amplia. Para ello se consigue sintetizar la ley:

Por Apartados: Consiste en una tabla resumen de todos los artículos relevantes de la ley, acompañados de un resumen. Además se marcan cuales son de obligatoriedad de cumplimiento a partir del año 2010.

Por Ámbitos: Por un lado se consigue catalogar una serie de ámbitos que se tratan en la propia Ley, por otro se resumen todas las obligaciones de las AAPP y los derechos de los ciudadanos y por último todos los principios que se mencionan de forma implícita o explícita en la Ley 11/2007. Se reflejan en unas tablas agrupados por ámbitos y se cruzan todos los valores que se han mencionado anteriormente.

Por otro lado se ha intentado aportar una serie de criterios que pudieran servir para evaluar a una Administración Pública. Esta idea se enfocó a las Comunidades Autónomas.

Se ha sintetizado una serie parámetros para poder evaluar el nivel de implantación de la eAdministración en las CCAA. Además se ha conseguido



obtener una serie de datos por años, pudiendo tener un repositorio de dichos datos durante tres años, lo que están comprendidos entre 2007 y 2009.

9.8 Líneas futuras

Siguiendo el ciclo que se ha empezado con este proyecto, el de análisis y sintetización de una serie de parámetros para poder evaluar el nivel de implantación de la eAdministración en las CCAA, el siguiente paso que se propone sería llevarlo a la práctica mediante una aplicación software.

Otra línea futura plausible sería plantear una serie de medidas de ajuste en función del resultado obtenido en la evaluación de los procesos identificados en este proyecto. Este apartado sería compatible con el anterior mencionado, el de la aplicación software.

Sería deseable una aplicación que permita la explotación de la información obtenida mediante la evaluación de procesos, mediante la creación de informes que permitan realizar comparativas entre Comunidades así como evaluar la evolución a lo largo del tiempo del nivel de implantación de la eAdministración en ellas.

De esta forma se puede proporcionar una clasificación de estos criterios en categorías, que aporte valor añadido a la evaluación del nivel de adaptación de la eAdministración, logrando ponderar según su importancia no sólo los criterios sino también las categorías.

Otro trabajo que se podría realizar a raíz del presente es la realización de una toma de datos más actual una vez que estuviesen disponibles para las CCAA analizadas, y así poder actualizar los datos de las futuras aplicaciones posibles que se han mencionado anteriormente.

Para terminar las conclusiones, decir que el trabajo me ha servido para tener una idea mucho más concreta de la eAdministración, que los procesos de adaptación son complejos debido a la adecuación y automatización de trámites que se realizaban en papel y ahora deben estar automatizados, lo que además implica aplicar seguridad a los sistemas al tratar información sensible y datos de carácter personal, y tener que cumplir unos requisitos marcados por la Ley.

Asegurar además la autenticación de los usuarios, facilitar el acceso electrónico de los ciudadanos, etc. Todo este proceso de transformación o adaptación implica el análisis para convertir todos los trámites administrativos en procesos automatizables y cumplir la ley de Administración electrónica.

10 PRESUPUESTO

10.1 Introducción.

Como recomendación en los proyectos de la Universidad Carlos III, se ha creado un proyecto cuantitativo para poder cuantificar el coste que ha tenido dicho proyecto. Se ha seguido las líneas de actuación recomendadas por la misma Universidad.

El resultado se muestra en la siguiente factura dónde se puede ver los costes imputados para el desarrollo del proyecto.



Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

Autor:

Antonio Sánchez Rosales

Departamento:

Departamento de Informática

Descripción del Proyecto:

- Título	Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación.	
- Duración (meses)	9	
Tasa de costes Indirectos:	0	0%

Presupuesto total del Proyecto (valores en Euros):

Euros 16.362,75 €

Desglose presupuestario (costes directos)

PERSONAL

Nombre y Apellidos	Categ.	Dedicación (hombres mes) a)	Coste hombre mes	Coste (Euro)	Firma de conformidad
Antonio Sánchez Rosales	Ingeniero	1,00	1.800,00	1.800.00 0,00	
Hombres mes		1	Total	1.800.00	

a) 1 Hombre mes = 131,25 horas. Máx anual de dedicación de 12 hombres mes (1575 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable d)
Ordenador Personal	700,00	100	9	60	105,00
Impresora	99,00	100	9	60	14,85
Infraestructura ADSL	50,00	100	9	60	14,85
Papelería	75,00	100	9	60	7,50
Recambio Impresora	125,00	100	9	60	18,75
Compra de libro: Administración electrónica y procedimiento administrativo	12,00	100	9	60	1,80
Total					162,75

d) Fórmula de cálculo de la Amortización:

A = nº de meses desde fecha de facturación en que el equipo es utilizado

B = periodo de depreciación (60 meses)

C = coste del equipo (sin IVA)

D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
Total		0,00

OTROS COSTES DIRECTOS DEL PROYECTO

Descripción	Empresa	Costes imputable
Total		0,00

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Resumen de costes

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	16.200,00 €
Amortización	162,75 €
Subcontratación de tareas	0
Costes de funcionamiento	0
Costes Indirectos	0
Total	16.362,75 €

Por lo tanto, el presupuesto total de este proyecto asciende a un total de **16.362,75** euros.



11 GLOSARIO

(Por orden alfabético)

AAPP: Administraciones Públicas.

ADSL: (Asymmetric Subscriber Line, ADSL). La línea de abonado digital asimétrica, donde se atribuye más anchura de banda a la descarga que a la telecarga, y la línea de abonado digital de alta velocidad (High Rate Digital Subscriber Line, HDSL) se consideran las tecnologías DSL dominantes. Normalmente, cada conexión alcanzará una velocidad de entre 1,544 mbps y 512 Kbps en sentido descendente y alrededor de 128 Kbps en sentido ascendente.

AEAT: Agencia Estatal de la Administración Tributaria.

AGE: Administración General del Estado

AIMC: Asociación para la Investigación de Medios de Comunicación

API: (Application Programming Interface).

ARCE: Almacenamiento y Recogida de Cuestionarios Económicos.

B2B: (Business to Business). Negocio a Negocio. Es la relación comercial establecida, por medio de redes telemáticas entre dos empresas o compañías.

B2C: (Business to Consumer). Negocio a Cliente. Es la relación comercial establecida, por medio de redes telemáticas, entre una empresa y un cliente final.

Banda ancha: Red capaz de alcanzar altas velocidades de transmisión de información (ej. xDSL, Cable, LMDS, etc). También puede entenderse como una característica de ciertos canales de comunicaciones cuyo intervalo de frecuencias de transmisión les permite el transporte simultáneo de una elevada cantidad de información como, por ejemplo, imágenes, sonido, televisión, datos, voz, etc.

Blog: Servicio prestado a través de Internet que cuenta con un elevado grado de actualización y donde suele existir una recopilación cronológica de uno o varios autores. Es frecuente la inclusión de enlaces en las anotaciones y suele estar administrado por el mismo autor/a que lo crea donde plasma aspectos que, a nivel personal, considera relevantes o de interés.

BOMEH: Boletín Oficial del Ministerio de Economía y Hacienda.

CATSI: El Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, presidido por el Ministro de Industria, Turismo y Comercio o por la persona en quien delegue, es un órgano asesor del Gobierno en materia de telecomunicaciones y sociedad de la información.

CCAA: Comunidades Autónomas.

CERES: Certificación Española.

CIS: (Commonwealth of Independent States). Comunidad de Estados Independientes. La Comunidad de Estados Independientes, está compuesta por los siguientes países: Armenia, Azerbaiyán, Bielorrusia, Georgia, Kazajstán, Kirguistán, Moldavia, Rusia, Tayikistán, Turkmenistán, Ucrania y Uzbekistán.

CMT: La Comisión del Mercado de las Telecomunicaciones (CMT) es una entidad de Derecho Público. Es el organismo regulador independiente español para el mercado de las telecomunicaciones y de los servicios audiovisuales. Nace en el año 1996 durante el proceso de liberalización de las telecomunicaciones en España y fue creada en virtud de lo dispuesto en el Real Decreto-Ley 6/1996, de 7 de junio, de Liberalización de las Telecomunicaciones. Está adscrita al Ministerio de Industria, Turismo y Comercio, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

Comercio Electrónico (CE): Transacciones realizadas a través de redes basadas en protocolos de Internet (TCP/IP) o sobre otras redes telemáticas. Los bienes y servicios se contratan a través de estas redes, pero el pago o entrega del producto pueden realizarse off-line, a través de otro cualquier canal.

Correo Electrónico (e-mail): Transmisión electrónica de mensajes (incluyendo texto y archivos adjuntos) desde un ordenador a otro situado dentro o fuera de la organización. Incluye el correo electrónico por Internet u otras redes telemáticas.

CRL: Lista de Renovación de Certificados.

DIRCE: El Directorio Central de Empresas (DIRCE) reúne en un sistema de información único, a todas las empresas españolas y a sus unidades locales ubicadas en el territorio nacional. Su objetivo básico es hacer posible la realización de encuestas económicas por muestreo. Se actualiza una vez al año, generándose un nuevo sistema de información a 1 de enero de cada período.

DNI: Documento Nacional de Identidad.

DNle: Documento Nacional de Identidad electrónico.

Estrategia de Lisboa: También conocida como Agenda de Lisboa o Proceso de Lisboa es un plan de desarrollo de la Unión Europea. Fue aprobado por el Consejo Europeo en Lisboa el 23 y 24 de marzo de 2000.

EuroStat: Statistical Office of the European Communities, oficina europea de estadística



FNMT-RCM: Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda.

GOV: Public Governance and Territorial Development Directorate.

HTTPS: Hypertext Transfer Protocol Secure.

INAP: Instituto Nacional de Administración Pública.

Internet World Stats: Sitio web internacional que ofrece estadísticas de uso mundial de Internet, población y de mercado TIC, por países y regiones del mundo. (<http://www.internetworldstats.com/>)

INE: Instituto Nacional de Estadística.

INFOMEDIARIO: Web que facilita la entrada a agentes o empresas que no estaban posicionadas en el sector de la actividad que realicen.

INTECO: Instituto Nacional de Tecnologías de la Comunicación.

IRIS: Image Recognition Integrated System.

ISO: Organización Internacional de Normalización.

LAECSP: Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

LOPD: Ley Orgánica 15/1999, de Protección de Datos de carácter personal.

LRJAP: Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del procedimiento administrativo común.

NIF: Número de Identificación Fiscal.

OAE: Observatorio de Administración Electrónica.

OCDE: Organización para la Cooperación y el Desarrollo Económico

PDAE: Plan Director de Administración Electrónica.

PKI: Public Key Infrastructure.

PKIX: Public Key Infrastructure using X.590.

PYMES: Pequeña y Mediana Empresa.

SARA: Sistema de Aplicaciones y Redes para la Administración.

SCDP-CGPJ: Servicio de Consulta de Datos Patronales del Consejo General del Poder Judicial.

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

SETSI: Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información

SGER: Sistema Electrónico de Gestión de Expedientes y Registros.

SIA: Servicio de Información Administrativa.

SOROLLA: Sistema Informático de Apoyo a la Gestión Económica de los Centros Gestores Públicos.

TIC: Tecnologías de la Información y las Comunicaciones.

UE: Unión Europea.

URL: Uniform Resource Locator.

W3C XMLDSIG: Modelo de firma digital.



12 BIBLIOGRAFÍA

12.1 Libros

Administración electrónica y procedimiento administrativo, ed. Ministerio de Economía, Secretaría General Técnica (2004). ISBN: 84-9720-054-3

Administraciones Públicas Españolas, autores Crespo González, J. y Pastor Albaladejo, G. ed. McGraw Hill, (2002).

Aplicación de la Ley 11 / 2007 de acceso electrónico de los ciudadanos a los Servicios Públicos online en las CC AA españolas, ed. Fundación Orange (abril 2010)

Estudio comparativo 2008 de los servicios públicos on-line en las Comunidades Autónomas, ed. Cap Gemini y Fundación Orange, (Abril,2008).

Indicadores eEurope 2005, ed. ONTSI (Febrero, 2009).

Guía práctica de la Ley 11/2007, de acceso electrónico a los ciudadanos a los servicios públicos (LAECSP), ed. FEMP, ISBN: 978-84-92494-03-3

La Administración electrónica en España, ed. FUNDACIÓN TELEFÓNICA (2007), ISBN: 978-84-08-07422-9

La administración electrónica y el servicio a los ciudadanos, ed. Ministerio De Economía y Hacienda (2009), ISBN: 9788497201544

La Administración Pública que España necesita, ed. Círculo de Empresarios, (Abril, 2007).

La Sociedad de la Información en España 2008. Diciembre, ed. Fundación Telefónica (2008)

Las TIC en la Administración Local del Futuro, ed. Fundación Telefónica (2008), ISBN: 978-84-08-08124-1

Las TIC en los hogares españoles, 29ª oleada, ed. ONTSI, (2010), ISSN 1989-7766

Libro Blanco para la Reforma del Gobierno Local, ed. Ministerio de Administraciones Públicas (2005).

Plan de acción para la reducción de cargas administrativas, ed. Gobierno de España, (Junio, 2008).

Análisis de la eAdministración e identificación de criterios auditables para la evaluación del grado de implantación

Plan estratégico ley de acceso electrónico de los ciudadanos a los servicios públicos. Ed. Gobierno de España (diciembre, 2007).

UN eGovernment Survey 2008, from e-Government to connected governance, ed. Naciones Unidas, (2008).

12.2 Revistas

España avanza en el uso y convergencia de las TIC. Noviembre, ed. Ceprede, N-Economía, (2008). Artículo

Nota de prensa sobre el Plan de Acción del ministro de Justicia para los próximos tres años, ed. Ministerio de Justicia (marzo, 2009).

Planes de modernización autonómicos y locales. Revista Sociedad de la Información, (noviembre 2007). Artículo

12.3 Informes corporativos y congresos

Encuesta de uso de TIC y comercio electrónico en las empresas 2009-2010. ed. Instituto Nacional de Estadística (INE), (2010)

Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares 2010. ed. Instituto Nacional de Estadística (INE), (2011)

Plan de acción sobre Administración electrónica i2010. ed. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones (2006).

Plan de Gobierno 2007-2010, ed. Generalitat de Cataluña, (2007)

Presentación Plan Avanza 2, ed. Ministerio de Industria, Turismo y Comercio (enero, 2009).

Presupuestos 2009, unos presupuestos para hacer frente a la crisis y proteger a los sectores más vulnerables, ed. Generalitat de Cataluña, (2009)

12.4 Normativa

B.O.C.M.

http://www.madrid.org/cs/Satellite?language=es&pagename=Boletin%2FPage%2FBOCM_home

B.O.E.

<http://www.boe.es>



Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, BOE número 298 de 14/12/1999, páginas 43088 a 43099 (12 págs.), Referencia: BOE-A-1999-23750

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE número 150 de 23/6/2007, Referencia: BOE-A-2007-12352

Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio. BOE-A-2009-18731, Páginas: 99570 a 99593 – 24 págs

Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio, BOE número 308 de 23/12/2009, páginas 108507 a 108578 (72 págs.), Referencia: BOE-A-2009-20725

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, BOE número 312 de 29/12/2007, páginas 53701 a 53719 (19 págs.), Referencia: BOE-A-2007-22440

Ley 59/2003, de 19 de diciembre, de firma electrónica, BOE número 304 de 20/12/2003, páginas 45329 a 45343 (15 págs.), Referencia: BOE-A-2003-23399

Real Decreto 3/2010, de 8 de enero, BOE número 25 de 29/1/2010, páginas 8089 a 8138 (50 págs.), Referencia: BOE-A-2010-1330

Real Decreto 4/2010, de 8 de enero, BOE número 25 de 29/1/2010, páginas 8139 a 8156 (18 págs.), Referencia: BOE-A-2010-1331

Real Decreto 1671/2009, BOE número 278 de 19/10/2009, páginas 97921 a 97948 (28 págs.), Referencia: BOE-A-2009-18358

12.5 Páginas o documentos electrónicos en la red

Administración Electrónica de la C.A.M.
http://www.madrid.org/cs/Satellite?language=es&pagename=AdministracionElectronica%2FPage%2FSAEL_home

Agencia Notarial de Certificación S.L. Unipersonal
<http://www.ancert.com/>

Agencia de Tecnología y Certificación Electrónica de la Generalitat Valenciana
<http://www.accv.es>

ANF - Autoridad de Certificación
<http://www.anf.es/security/cont.html?lang=es>

Asociación para la Investigación de Medios de Comunicación (AIMC)

**Análisis de la eAdministración e identificación de criterios auditables para la
evaluación del grado de implantación**

<http://www.aimc.es>

Autoridad Certificadora de Banesto. Banesto CA.

<http://ca.banesto.es/>

Consejo General de la Abogacía Española

<http://www.acabogacia.org>

Consejo Superior de Cámaras de Comercio, Industria y Navegación

<http://www.camerfirma.com/>

Comisión Europea

http://ec.europa.eu/index_es.htm

Datos estadísticos a nivel europeo

<http://inza.wordpress.com/2010/01/25/espana-en-el-top-ten-de-la-administracion-electronica/>.

Dirección General de la Policía Nacional

<http://www.dnielectronico.es/>

EuroStat

<http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/>

FNMT

<http://www.cert.fnmt.es>

Forja del Centro de Transferencia de Tecnología (Forja-CTT)

<http://forja-ctt.administracionelectronica.gob.es>

Generalitat de Catalunya

<http://www.gencat.cat/>

Generalitat Valenciana

<http://www.gva.es>

INAP – Instituto Nacional de Administraciones Públicas

<http://www.inap.es>

Junta de Andalucía

<http://www.juntadeandalucia.es>

Junta de Castilla y León

<http://www.jcyl.es/>

Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI)

<http://www.ontsi.red.es/index.action>

Observatorio Nacional del Software de Fuentes Abiertas.

<http://www.observatorio.cenatic.es>

PAe - Portal de Administración Electrónica



<http://administracionelectronica.gob.es/>

Portal de Administración General del Estado destinado a la relación del ciudadano con la Administración Pública

<http://www.060.es/>

Proyecto APORTA

<http://www.aporta.es>

Servicio de Certificación del Colegio de Registradores

<http://www.registradores.org/>

UN Public Administration Programme

http://www2.unpan.org/egovkb/global_reports/10report.htm

W3Counter

<http://www.w3counter.com/>

13 ANEXO

13.1 Estadísticas Presentadas por Internet en la AEAT.

Fuente:

<http://www.aeat.es/AEAT/Contenidos Comunes/La Agencia Tributaria/Tramites on Line/Otros Servicios/ESTADISTICAS/Declaraciones presentadas por Internet/estadinet31012010.pdf>

MODELOS	2010(1)	2009(1)	2008	2007	2006	2005
005 EXENCIONES IMPUESTO MATRICULACIÓN	7.666	82.674	172.788	181.888		
006 EXENCIÓN Y N.S. SIN RECONOCIMIENTO PREVI	163					
030 CAMBIO DE DOMICILIO Y OTROS DATOS	3.024	88.802	86.126	76.479	58.300	43.704
036 MODELO CENSAL			13.494	888.497	711.342	520.342
038 OPERACION ENTIDADES INSCRITAS REG. P	40	225	198	187	115	
039 COMUNICACION CENSO GRUPO ENTIDADES I	-	986	9			
100 IMP. SOBRE LA RENTA DE LAS PERSONAS	-	-	6.956.750	5.673.505	4.503.134	3.796.041
104 IRPF. SOLICITUD DE DEVOLUCION	-	-	1.355.909	1.548.658	1.676.777	1.713.870
110 IRPF. RETENCION TRABAJO PERSONAL	-	6.085.742	4.226.774	1.490.395	827.894	651.741
111 RETENC. E INGR. A CTA. GRANDES EMPRES	-	454.921	485.045	460.294	414.182	381.456
115 IRPF-ISS. RET.ARREND.INMUEBLES URBAN	-	2.189.059	1.424.415	403.645	182.905	131.276
117 RETENCIONES E INGRESO A CUENTA	-	1.048	1.990	1.572	1.608	1.487
123 RET. CAP. MOB. (EXCEPTO INT. E IMPLI)	-	224.416	160.412	51.645	30.201	22.921
124 RET. CAP. MOB. REND. IMPLICITOS GRAL	-	945	868	586	489	413
126 RET. E INGR. A CTA. CAP. MOB. INTERE	-	2.652	2.315	1.788	1.419	1.238
128 RET. OPERAC. CAPITALIZ Y CONTRATOS SEG	-	1.498	1.147	786	568	463
130 IRPF. PAGO FRACCIONADO	-	2.184.106	1.805.691	1.174.969	880.624	700.194
131 IRPF. PAGO FRACCIONADO - MODULOS	-	836.410	681.173	294.982	90.129	68.568
140 DEDUCCION POR MATERNIDAD	2.918	38.624	40.601	34.641	29.525	26.123
141 COM. DEL NACIMIENTO O ADOPCIÓN DE HIJOS	1.455	18.732	16.404			
180 RETENCION ARRENDAMIENTO INMUEBLES UR	-	702.735	801.800	781.798	535.808	432.038
181 PRESTAMOS HIPOTECARIOS	-	91				
182 DEC. INFORMATIVAS DE DONACIONES	-	5.360	7.808	6.923	5.104	2.689
184 ENTIDADES EN RÉGIMEN ATRIB. DE RENTA	-	-	206.893	194.741	167.777	145.181
187 TRANSMISION DE PARTICIPACIONES	-	152	236	196		
188 RET. RENTAS OPERACIONES CAPITAL Y SE	-	128	262	245	205	167
189 DECL. INFORMATIVA VALORES SEGUROS RENTAS	-	128	153			
190 RETENCIONES TRABAJO PERSONAL	-	1.892.982	2.150.019	2.123.988	1.653.747	1.392.572
193 RENDIMIENTOS EXPLICITOS CAPITAL MOBI	-	102.877	110.480	109.323	65.311	51.996
198 OPERACIONES INTERVENIDAS POR FEDATAR	-	595	3.572	2.352	2.270	2.151
20P I. SOCIEDADES PERIÓDICA	-	1.651	2.690	2.147	300	
200 IMP. SOBRE SOCIEDADES - DEC. ANUAL	-	-	1.450.538	1.423.810	1.286.917	389.698
202 IMP. SOCIEDADES. PAGO A CUENTA	-	1.218.873	1.049.357	175.323	46.395	31.292
210 IR. NO RESIDENTES SIN ESTABLEC.PERMA	9	818	104.118	6.039	3.945	2.167
211 RET ADQUISICION INMUEBLES NO RESIDEN	1	333	233	254	57	37
212 IRNR N RESID. SIN E.P. TRANS INMUEBL	1	511	394	327	188	155
213 G.E. BIENES INMUEBLES NO RESIDENTES	-	145	118	45	22	3
214 IP/IRNR NO RESIDEN. SIN E.P. SIMPLIF	-	-	13	75.159	60.603	22.927
215 IP/IRNR NO RESIDEN. SIN E.P. COLECTI	-	697	344	123	49	11
216 IR. NO RESIDENTES SIN ESTABLEC.PERMA	-	70.161	57.424	36.093	28.745	20.267
218 I.S./I.R. NO RESID. PAGO FRACCIONADO	-	84.117	94.448	90.535	81.292	74.020
220 IS REGIMEN DE CONSOLIDACION FISCAL	-	-	10	2.272	1.412	
295 PROD. FINANCIEROS. ENTID. EXTRANJERA	-	-	-	-	-	-
298 IMP. RENTAS NO RESIDENTES SIN ESTABLE	-	17.383	24.175	22.369	17.420	12.295
299 DECL. RENTAS PF RESIDENTES EST U.E.	-	-	36	36	36	37
300 IVA. TRIMESTRAL	-	-	5.448.653	3.024.695	2.198.467	1.688.396
303 AUTOLIQUIDACIÓN IMPUESTO VALOR AÑADI	-	11.612.486				
308 I.V.A. REG ESP REC EQUI SUJ PAS OCAS	-	1.689	429	149	33	28
309 I.V.A. DECLAR. LIQUIDA NO PERIODICA	-	3.964	2.452	816	457	194
310 IVA. SIMPLIFICADO	-	385.083	278.529	172.580	97.468	75.546
311 IVA. SIMPLIFICADO - DECL. FINAL	-	143.557	140.369	103.715	61.745	55.121
320 I.V.A. GRANDES EMPRESAS	-	-	343.182	336.204	296.026	267.000
322 IVA GRUPO DE ENTIDADES MODELO INDIVI	-	68.240	51.810			
330 I.V.A. EXPORTADORES	-	-	222.372	222.817	220.676	177.223
340 LIBRO DE IVA	-	217.354				
341 I.V.A. DEVOL REG AGRICOLA GANADERIA	-	333	220	157	110	78
345 PLANES FONDO PENSIONES Y SISTEMAS AL	-	1.606	5.147	5.032	4.145	3.493
347 DECLARACION ANUAL DE OPERACIONES CON	-	-	1.956.920	1.855.369	1.532.288	1.298.179
349 DECLARACION OPERACIONES INTRACOMUNIT	-	486.206	547.277	488.095	398.277	307.451
353 IVA GRUPO ENTIDADES MODELO AGREGADO	-	8.721	6.781			
360 SOL.DEV.IVA EMPR.PROF. ESTABLECIDOS	-	11				
370 I.V.A. DECLARACION TRIMESTRAL ORDINA	-	14.226	7.123	3.960	2.323	1.307
371 I.V.A. DECLARACION TRIMESTRAL FINAL	-	4.490	4.140	2.587	1.508	1.190
380 IVA ASIMILADO A LA IMPORTACIÓN	1.452	11.784	11.335	10.307	7.789	5.422
390 DECLARACION ANUAL DE IVA	-	2.164.386	2.716.938	2.579.556	1.711.568	1.386.061
430 IMPUESTO SOBRE PRIMAS DE SEGUROS	-	4.648	2.962	1.669	975	632
480 IMPUESTO SOBRE LAS PRIMAS DE SEGUROS	-	375	343	180	138	73
500 II.EE. DOCUMENTO ADMINISTRATIVO DE ACOMPAÑAMIENTO	136.325	1.636.273	1.748.720	1.770.955	1.630.976	1.655.485

Imagen 13-1 Estadísticas Presentadas por Internet en la AEAT



MODELOS	2010(1)	2009(1)	2008	2007	2006	2005
503 II.EE. DOC. ADMINISTRATIVO SIMPLIFICADO DE ACOMPAÑAMIENTO	290	4.185	3.659	3.694	2.425	1.246
510 II.EE. Declaración Operaciones Recepción resto U.E.	175	1.916	1.880	1.576	716	510
511 II.EE. NOTAS DE ENTREGA A TIPO REDUCIDO VENTAS EN RUTA	736.624	6.575.523	6.671.643	6.623.986	5.385.745	5.447.594
512 II.EE. RELACIÓN ANUAL DESTINATARIOS PRODUCTOS TARIFA 2ª	9	41	39	39	38	33
520 II.EE. PARTE RESULTADO OPERACIONES DE TRABAJO	176	2.673	2.536	2.414	1.648	2.153
553 II.EE. Resumen Trimestral Movimientos en Fábricas y Depósitos Fiscales de Vino y Bebidas Fermentadas	3.839	18.003	17.822	14.740	7.223	4.886
554 II.EE. Declaración de Operaciones en Fábricas y Depósitos Fiscales de Alcohol	87	988	994	889	573	474
555 II.EE. Impuesto sobre Productos Intermedios. Declaración de operaciones en Fábricas y Depósitos Fiscales	341	3.363	3.382	3.147	2.169	1.888
557 II.EE. Declaración de operaciones en Fábricas y Depósitos Fiscales de Bebidas Derivadas	372	3.950	3.831	3.545	2.218	1.921
558 II.EE. Declaración de Operaciones en Fábricas y Depósitos Fiscales de Cerveza	128	1.559	1.446	1.349	1.179	931
560 II.EE. Sobre la Electricidad	29.253	121.977	45.892	21.811	7.753	5.527
561 II.EE. Sobre la Cerveza	79	1.339	1.273	1.208	745	647
562 II.EE. Sobre productos intermedios	208	3.036	3.083	2.804	1.565	1.451
563 II.EE. Sobre el Alcohol y Bebidas derivadas	286	4.586	4.642	4.057	2.289	2.096
564 II.EE. Sobre Hidrocarburos	216	2.572	2.241	1.796	803	749
566 II.EE. Sobre Labores del Tabaco	44	572	562	562	429	402
569 II.EE. Sobre Ventas Minoristas de determinados Hidrocarburos	5.784	23.037	22.569	18.336	5.209	4.183
570 II.EE. Declaración de Operaciones en Fábricas y Depósitos Fiscales de Hidrocarburos	300	3.454	3.327	2.600	1.105	852
576 I.E. DETERM. MEDIO TRANSPORTE	68.992	961.485	1.199.025	1.611.119	1.646.628	20.885
580 II. EE. Declaración de Operaciones en Fábricas y Depósitos Fiscales de Labores de Tabaco	71	859	963	952	758	760
806 TASAS JURISDICCIONALES	2.770	42.832	31.555	24.180	24.779	17.361
714 IMP. EXTRAORDINARIO SOBRE EL PATRIMO	-	-	-	152.131	113.953	80.580
840 IMP. ACTIVIDADES ECONOMICAS	8.079	44.320	40.172	29.794	23.473	15.783
C36 MODELO CENSAL - NUEVA VERSION	209.728	1.471.847	1.304.555	259.261		
M30 CAMBIO DE DOMICILIO POR EL M.A.P.	619	14.115	13.781	8.274	4.744	175
RIC RESERVA PARA INVERSIONES EN CANARIAS	-	154	5.534	7.076		
VEG VISADO DE ENCOMIENDA DE GESTIÓN	213	38				
V08 IEDMT. MODELO 06. VALIDACION INTERNE	16.167	254.890	403.411	557.333	520.614	
V38 MODELO CENSAL - VALIDACION INTERNET	51.823	177.482	97.373	349.375	476.616	279.537
TOTAL	1.289.727	41.826.426	45.890.175	36.451.343	29.820.200	23.484.910
DECLARACIONES DE ADUANAS COMERCIO EXTERIOR						
DUA DE EXPORTACIÓN	291.918	4.060.793	4.332.661	4.439.629	4.339.759	4.158.813
DUA DE IMPORTACIÓN	265.907	3.550.802	4.147.993	4.183.940	3.841.637	3.664.719
EXPEDICIÓN Y RECEPCIÓN DE TRÁNSITOS	45.797	524.868	544.129	631.668	513.675	491.831
INTRASTAT (comercio intracomunitario)	62.068	741.086	740.042	714.873	700.312	670.451
DOCUMENTOS VINCULACIÓN A DEPÓSITOS	19.102	288.629	250.328	213.406	271.131	280.702
DECLARACIONES SUMARIAS Y MANIFIESTOS CARGA	35.680	479.463	449.732	532.095	510.018	539.984
TOTAL	720.472	9.645.640	10.464.885	10.613.611	10.176.532	9.806.506
TOTAL	2.010.199	51.472.066	56.355.060	47.067.552	39.996.732	33.291.410

(1) Ejercicio Incompleto

(2) Desde 2005 incluye la petición de borrador.

14 REFERENCIAS

- ⁱ <http://www.aimc.es/-Audiencia-de-Internet-en-el-EGM-.html>
- ⁱⁱ http://europa.eu/legislation_summaries/information_society/strategies/l24226b_es.htm
- ⁱⁱⁱ OCDE (1996): La Administración al servicio del público, Ministerio para las Administraciones Públicas, Madrid, 3.^a edición.
- ^{iv} <http://www.iso.org/iso/home.html>
- ^v en su artículo 103
- ^{vi} Decisión nº 3/94 de la Comisión Mixta CEE-AELC «Tránsito Común» de 8 de diciembre de 1994 por la que se modifica el Apéndice II del Convenio, de 20 de mayo de 1987, relativo a un régimen de tránsito común (DO L 371 de 31.12.1994, p. 6/8)
- ^{vii} <http://browse.oecdbookshop.org/oecd/pdfs/free/4203074e5.pdf>
- ^{viii} http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2007-12352
- ^{ix} www.femp.es/files/566-751-archivo/GUIA%20LEY%2011-2007.pdf
- ^x www.ingenio2010.es
- ^{xi} http://europa.eu/legislation_summaries/information_society/strategies/si0016_es.htm
- ^{xii} LEY 59/2003, del 19 de diciembre, de firma electrónica
- ^{xiii} <http://www.aimc.es/-Audiencia-de-Internet-en-el-EGM-.html>
- ^{xiv} <http://www.w3counter.com/globalstats.php>
- ^{xv} *La administración electrónica y el servicio a los ciudadanos*
- ^{xvi} <https://aeat.es/dmgefax.html>
- ^{xvii} www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf
- ^{xviii} *La administración electrónica y el servicio a los ciudadanos*
- ^{xix} <http://cordis.europa.eu/infosec/src/ets.htm>
- ^{xx} <http://www.ietf.org/>
- ^{xxi} *La administración electrónica y el servicio a los ciudadanos*



- xxii <http://www.ine.es/normativa/leyes/plan/legplan.htm>
- xxiii <https://arce.ine.es/ARCE/PreparaPrincipal.do;jsessionid=063787CE49DFC4CF7633EA977CE98358?valorHtml=ayuda>
- xxiv Guía práctica de la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP)
- xxv <http://www.dipalme.org/Servicios/Informacion/Informacion.nsf/referencia/Diputacion+Provincial+de+Almeria+RPC+RPC-IF-EX-001>
- xxvi <http://www.rpc.almeria.es>
- xxvii <http://www.dipalme.org/Servicios/Informacion/Informacion.nsf/referencia/Diputacion+Provincial+de+Almeria+Diputacion+DP-URLS-CC>
- xxviii <http://www.juntadeandalucia.es/rednerea/nerea/index.php>
- xxix Guía práctica de la Ley 11/2007, LAECSP
- xxx Guía práctica de la Ley 11/2007, LAECSP
- xxxi http://www-1.munimadrid.es/SBAE_262_SF_SIGE_Internet/indicador.do?Key=271
- xxxii Guía práctica de la Ley 11/2007, Guía práctica de la Ley 11/2007, LAECSP
- xxxiii <https://www.leganes.org/public/login.aspx?returnurl=e-participa/carpeta/errorbrowse.aspx?AppScope=CIUDADANO>
- xxxiv <http://oreilly.com/web2/archive/what-is-web-20.html>
- xxxv <http://www.nature.com/nature/journal/v438/n7070/full/438890a.html>
- xxxvi <http://vozyvoto.es/2007/12/11/los-rasgos-de-la-administracion-20/>
- xxxvii <http://twitter.com/>
- xxxviii <http://www.wikipedia.com>
- xxxix <http://www.wikanda.es>
- xl <http://www.madripedia.es>
- xli <http://ecatalunya.gencat.net>
- xlii <http://www.facebooknoticias.com/2011/01/09/facebook-empieza-2011-con-600-millones-de-usuarios-registrados/>
- xliii <http://twitter.com/#!/GobiernoEspanol>

^{xliv} *<http://www.barackobama.com>*