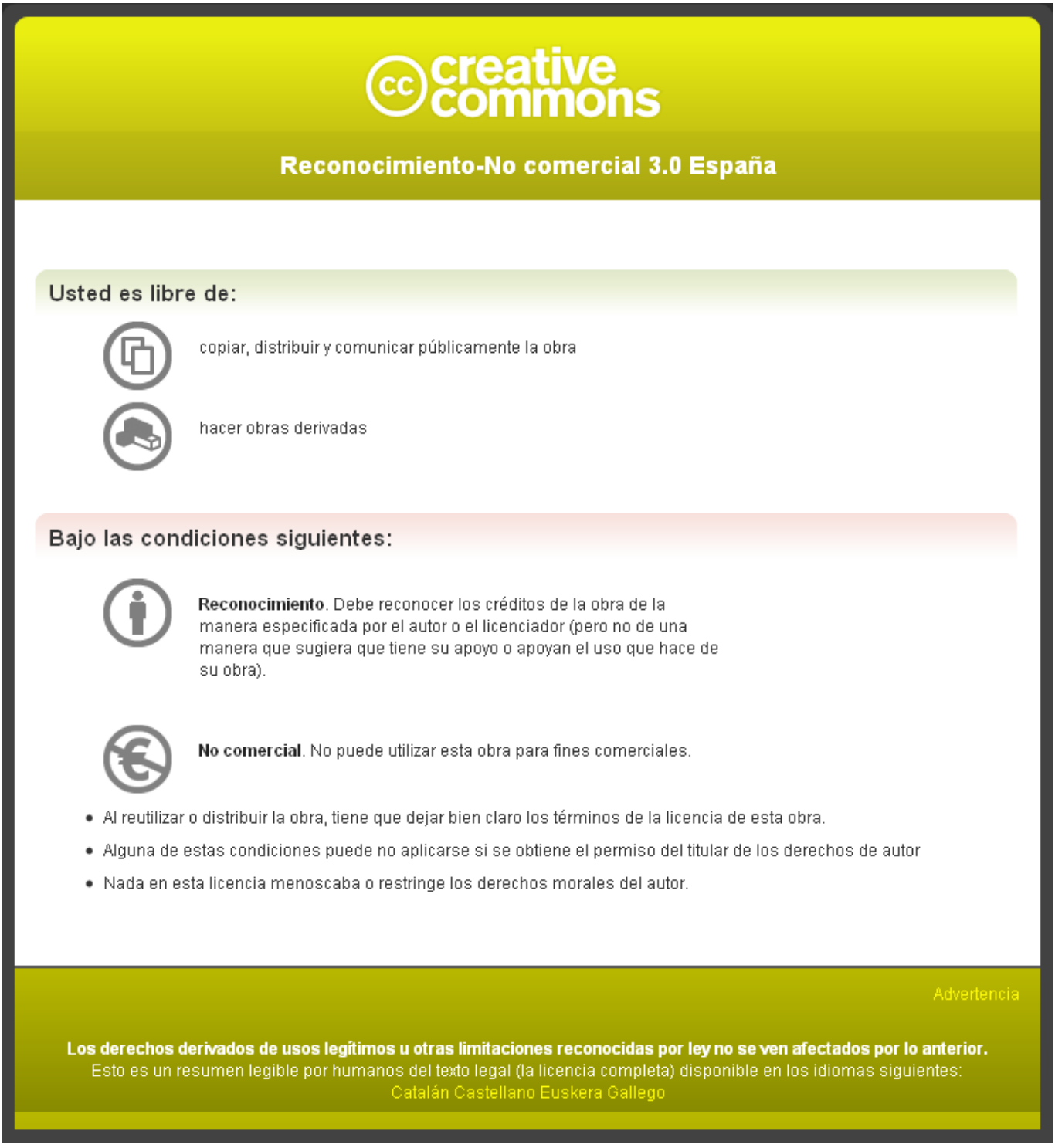
Manual Práctico de Supervivencia en la Administración Electrónic@



Índice

PRIMERA PARTE: MANUAL PRÁCTICO

1. INTRODUCCIÓN A LA ADMINISTRACIÓN ELECTRÓNICA

1.1 Público y Objetivos del Manual

La **Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos** supone un reto como pocos tanto a la Administración y su personal como a los ciudadanos, ya que como dice en su exposición de motivos, supone el paso del *"podrán"* al *"deberán"* en materia de Administración Electrónica convirtiendo la relación con la Administración vía medios electrónicos en un derecho para los ciudadanos y obligación para la Administración.

La ley se muestra particularmente exigente con la Administración General del Estado ya que establece el 31 de diciembre del 2009 como fecha límite para la disponibilidad de estos servicios, cuando en cambio reconoce a CCAA y EELL la condición de disponer de la suficiente financiación para la implantación de estos servicios.

Esto no supone solamente la necesidad de desarrollar las aplicaciones que soporten los servicios electrónicos correspondientes, sino además que el personal administrativo esté preparado para las consecuencias que esto implica, tanto **jurídicas**, **organizativas** como **técnicas**.

Las consecuencias son importantes, los usuarios, tanto ciudadanos como funcionarios van a tener que dominar más que nunca tecnologías de cierta complejidad como **certificados electrónicos** y la **firma electrónica**, lo cual es imposible sin asentar una serie de fundamentos.

El público objetivo de este manual abarca tres perfiles: **empleados públicos**, **ciudadanos y responsables de proyectos de Administración Electrónica**. Para conciliar los intereses de estos diferentes perfiles el manual mantiene una línea orientada principalmente a los empleados públicos y ciudadanos, y añade recuadros específicos que abordan los detalles técnicos que son principalmente de interés para los responsables de proyectos, de modo que el lector no interesado en este nivel de detalle se los pueda saltar fácilmente.

El manual pretende por otra parte cumplir con una doble finalidad: servir como base para una formación completa en Administración Electrónica a la vez que, una vez hayan sido asentados los conocimientos, como manual de consulta que acompañe al usuario en su día a día con la Administración Electrónica.

Por otra parte el conocimiento que abarca este manual es útil mucho más allá de la Administración electrónica. Cuestiones como la firma electrónica o certificados electrónicos no son en absoluto exclusivas a la Administración electrónica, aunque es dónde actualmente más se usan con diferencia. Es de preveer que en un futuro no muy lejano será cada vez más normal su uso en el ámbito privado de servicios y comercio electrónico.

En cuanto a los requisitos para el lector, aunque se abordan puntualmente temas de cierta complejidad técnica, no son necesarios conocimientos más allá de los normales de un usuario medio de informática.

1.2 ¿Qué es la Administración Electrónica?

Definiciones:

- **Comisión Europea de la UE**: *"La Administración electrónica es el uso de las TIC en las AAPP, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas"*
- **Domingo Laborda**[1]: *"Es el uso de las tecnologías de la información y las comunicaciones en la Administración para que, combinadas con ciertos cambios organizativos y nuevas capacidades de los empleados públicos, mejoren la eficacia, la productividad, la agilidad y la comodidad en la prestación de servicios a los ciudadanos."*

La idea clave sobre la Administración Electrónica es que no se trata simplemente de llevar las TIC a la actividad administrativa, sino que constituye un elemento fundamental en los procesos de **modernización administrativa** dentro de los cuales se enmarca que debe llevar a la **mejora y simplificación** de los servicios.

Dicho de otra manera: se quiere menos burocracia, muchísimo menos, no una burocracia por Internet.

Esta idea constituye por tanto uno de los grandes ejes de la **Ley 11/2007**.

1.2.1 Características de la Administración Electrónica

Ventajas:

- Rapidez y comodidad para los usuarios (a cualquier hora):
  - ⇨ Evitar colas, desplazamientos y horarios.
  - ⇨ Acceso a la información más cómodo, fácil y rápido.
  - ⇨ Acceso universal. La ubicación geográfica y proximidad de oficinas administrativas deja de ser un problema, algo especialmente importante en un país como España.
- Fomento de la participación de los ciudadanos (buzones, cuestionarios, etc.), fomentar una relación interactiva y más positiva.
- Impulso de la sociedad de la información: estimula la participación y aprendizaje del ciudadano (idea de estímulos adicionales mediante bonificaciones económicas (plazos para el pago) en Chile al hacer la declaración del IRPF por vía electrónica y el éxito obtenido)
- Simplificación de los procedimientos e integración transparente de diferentes administraciones (soluciones de **ventanilla única**).
- Para la Administración:
  - ⇨ Reducción de costes, tiempos de tramitación, menos errores -> mejor eficiencia y productividad. Mayor satisfacción para funcionarios, contenidos más estimulantes: el peso burocrático del trabajo se puede derivar hacia actividades de asesoramiento y soporte a los ciudadanos y las empresas. Menos uso de papel.
  - ⇨ Mejora de relaciones e imagen, transparencia: con el ciudadano (según la **UE**, un **62%** de los ciudadanos europeos perciben los servicios electrónicos como beneficiosos), entre departamentos y administraciones.
- Impacto en la economía:
  - ⇨ Según estudios del **World Economic Forum** *"los países que más destacan en cuanto a apertura y eficiencia del sector público y en preparación para la administración electrónica son también los primeros en cuanto a rendimiento económico y competitividad."*

[1] Antiguo Director General de Modernización Administrativa del MAP desde 2004 a 2006, y en la actualidad, Director del Observatorio de las Telecomunicaciones y de la Sociedad de la Información.

- ⇨ **Efecto locomotora**: gasto directo en TIC considerable[2], proyectos con función de **piloto** para las empresas privadas, creación de plataformas y servicios eDNI, aumento de la **confianza** para inversores privados, **aprendizaje**, **inclusión** de ciudadanos y empresas.
- ⇨ Mayor abanico de posibilidades de impulso económico en **regiones geográficamente desfavorecidas**.
- ⇨ Menos **carga** para las empresas les reduce costes y aumenta su productividad: contratación electrónica, factura electrónica, modelos de cotización electrónicos en la seguridad social, etc.

Barreras:

- Insuficiente penetración de las TIC en la población española.
- Usabilidad, accesibilidad y falta de experiencia en el uso de las TIC.
- Desconfianza en los medios electrónicos de intercambio de información.
- Desconocimiento de la existencia de la Administración online.
- Recelo de la administración con la seguridad electrónica.
- Falta de integración entre las diferentes administraciones.

1.2.2 Identificación, Autenticación, Integridad, Confidencialidad, Disponibilidad y Conservación

Si se compara la Administración Electrónica con la problemática general de las TIC en el sector privado, la diferencia más característica es la necesidad de mantener en todo momento las mismas garantías de **seguridad jurídica** de las actuaciones administrativas en papel en el plano de la tecnología.

Por tanto no es extraño que el marco legal de la Administración Electrónica concentre su mayor peso en las problemáticas en torno a la seguridad jurídica.

Los conceptos principales en torno a los cuales gira esta problemática son los siguientes:

- **Identificación**: la correcta identificación de remitente y destinatario. Se refiere principalmente a que los datos de identidad estén completos de modo que no pueda haber ambigüedad a la hora de establecer la identidad de una persona física o jurídica.
- **Autenticación**: la garantía de conocer fehacientemente la identidad de una persona física o jurídica. Este concepto guarda una estrecha relación con el **no repudio** (imposibilidad de rechazar la autoría de una determinada acción o documento). La principal herramienta para la autenticación son sistemas de usuario/clave y la firma electrónica. Ambos mecanismos permite asimismo el no repudio.
- **Integridad de la información**: se refiere a que se puede confiar en que una determinada información, por ejemplo, de un documento electrónico no fue manipulada y corresponde a su estado original.
- **Confidencialidad de la información**: guardar el secreto frente a terceros sobre una determinada información, ya sea un documento, comunicación, etc. La herramienta principal para lograr este objetivo es la criptografía.
- **Disponibilidad de la información y los servicios**: se refiere a que la información y/o servicios estén disponibles en todo momento. Esto implica normalmente servicios de alta disponibilidad 24x7, servidores redundados, centros de respaldo, etc.
- **Conservación de la información**: la correcta conservación y archivo de la información de modo que se encuentre disponible e integra aún después de que hayan pasado largos periodos de tiempo.

[2] Según el informe REINA 2007 el gasto de la Administración del Estado durante 2006 en Tecnologías de la Información y las Comunicaciones se situó en 1.545 millones de euros, en la Administración Local fueron unos 768 millones. El PIB en 2006 fue de 980.954 millones de euros.

1.3 Ejemplos de Servicios destacados de Administración electrónica

1.3.1 Oficina Virtual de la Agencia Tributaria

Cuando se habla de Administración Electrónica en España, se suele citar la Agencia Tributaria como el buque de insignia de la Administración Pública en España.

Durante el conjunto de la Campaña de Renta 2007 se han presentado **18,1 millones** de declaraciones de IRPF, un 6,6% más que el año anterior. De las cuales, **5,6 millones** se presentaron por Internet, un 25% más que el año anterior.

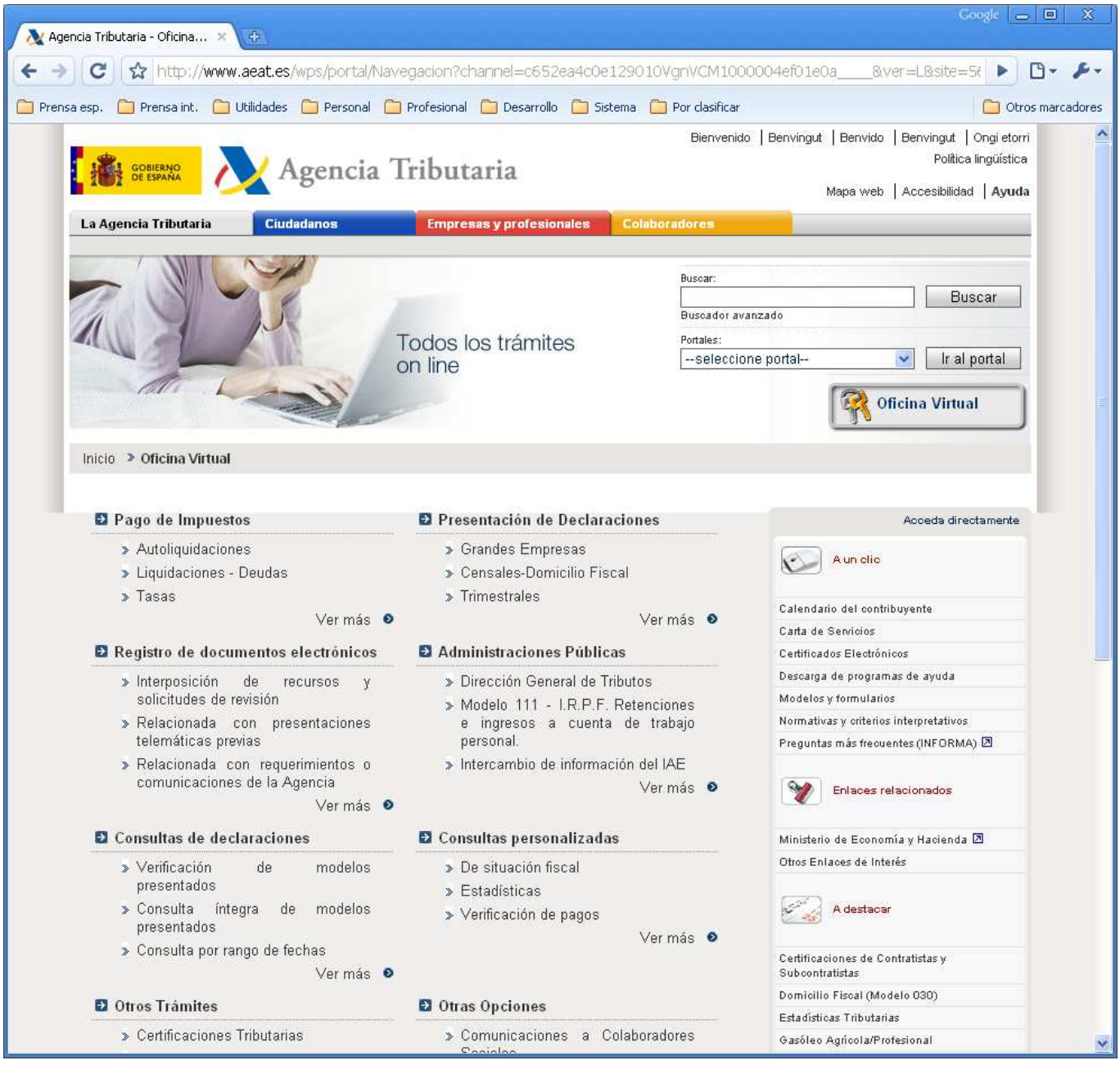


Ilustración 1 – Servicios para ciudadanos que ofrece la Agencia Tributaria.

1.3.2 Portal 060

Es el portal de referencia en el ámbito público y concentrador de las relaciones, interacciones y transacciones entre ciudadanos y Administraciones Públicas.

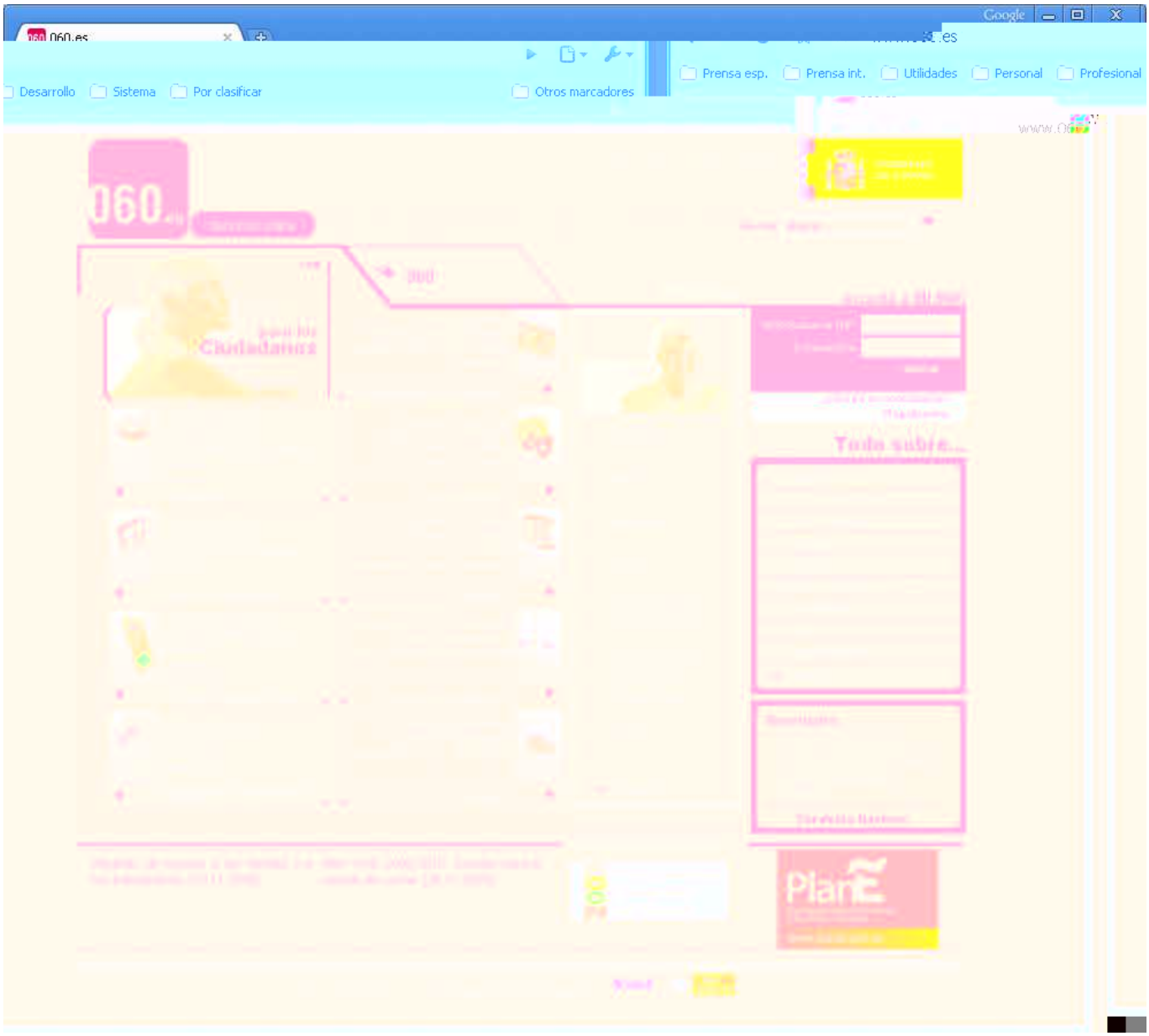


Ilustración 2 – Portal de la red 060.

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.

Hasta la fecha uno de los grandes problemas de la Administración española era que el ciudadano tenía que saber a cual 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 que no tener que saber qué Administración es la competente en su problema, la Red 060 lo determinará para 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).

1.3.3 Portal CIRCE

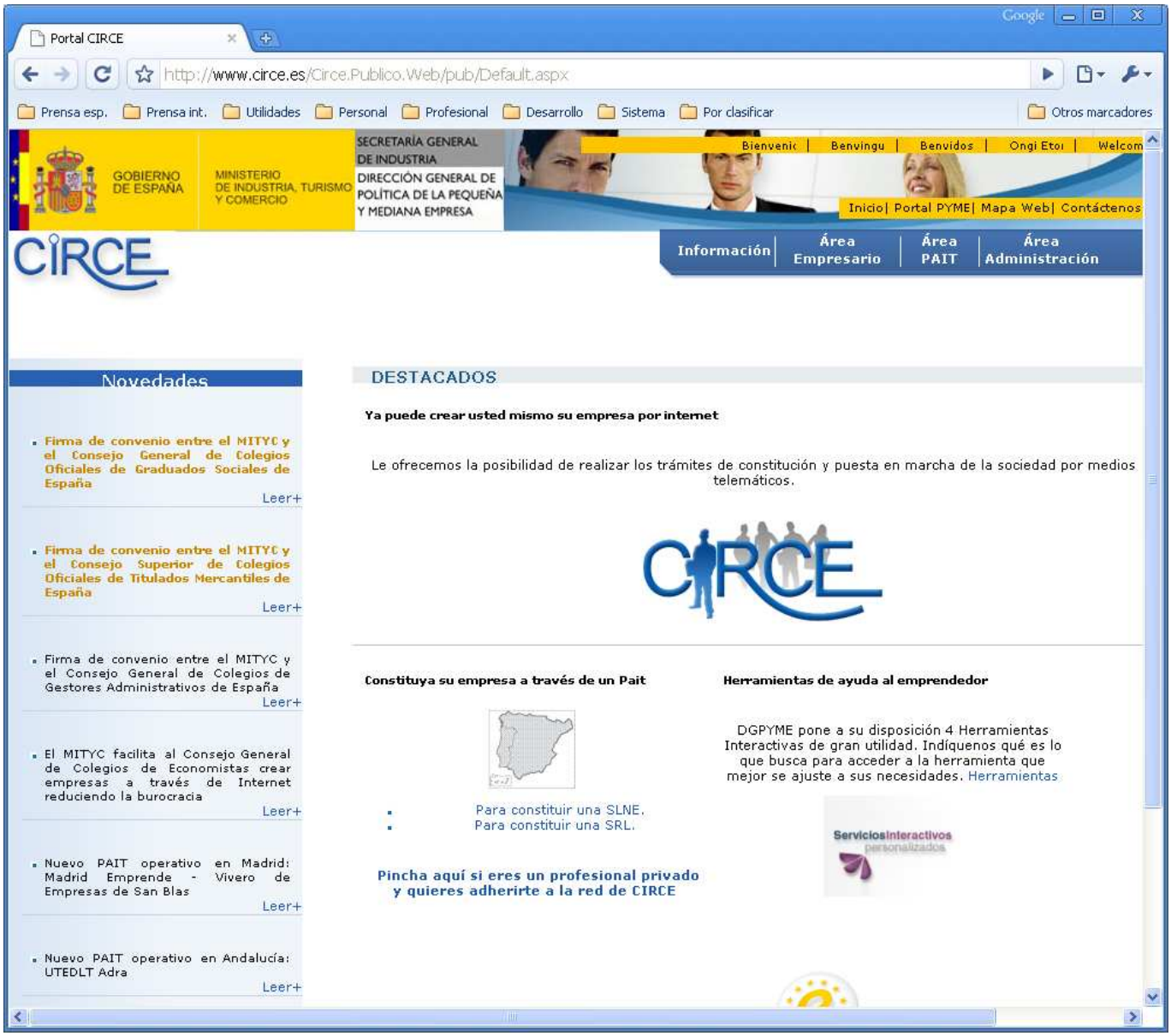


Ilustración 3 – Web del Centro de Información y Red de Creación de Empresas (CIRCE).

Desde el año **2003** la normativa que regula las sociedades limitadas ofrece 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 en general.

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**), llevará a cabo el intercambio de la documentación necesaria para la creación de empresas.

1.3.4 Sociedad Pública de Alquiler

Ilustración 4 – Web de la Sociedad Pública de Alquiler (SPA).

La Sociedad Pública de Alquiler nace con el fin de favorecer la creación de un mercado de alquileres más sólido y dinámico. Su función principal es la intermediación entre inquilino y arrendador no sólo para la realización de transacciones de alquiler, sino también para ofrecer una serie de servicios que proporcionen mayor seguridad jurídica a ambas partes, lo cual ha sido identificado como una de las principales causas del mal funcionamiento del mercado de alquiler español.

1.3.5 Servicios del Ayuntamiento de Madrid

El ayuntamiento de Madrid es un ejemplo de una entidad local con un amplio elenco de servicios electrónicos.

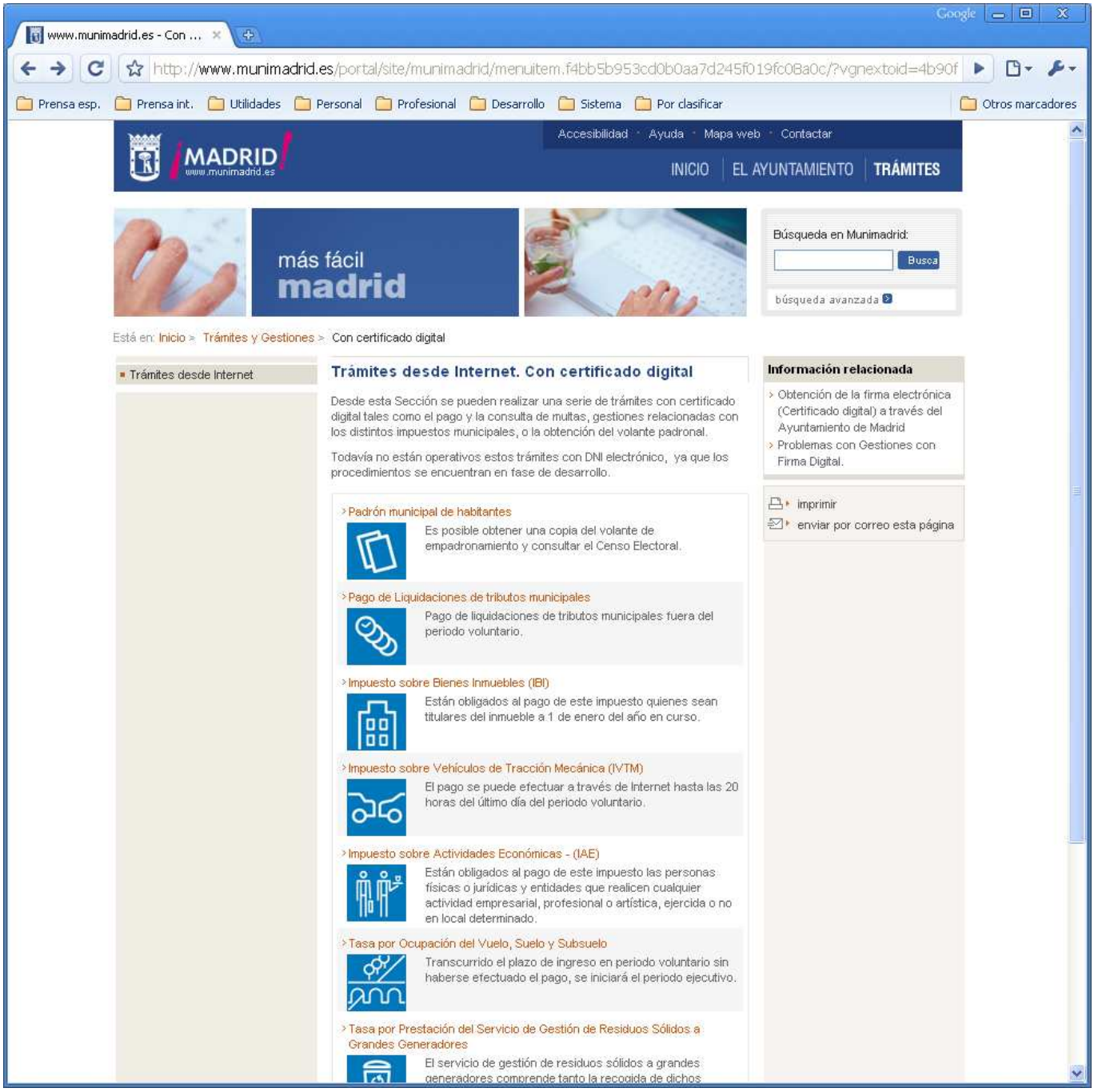


Ilustración 5 – Servicios de Administración Electrónica del Ayuntamiento de Madrid.

Práctica: acceso mediante certificado a un servicio electrónico

Acceder al servicio de consulta de saldo de puntos de la Dirección General de Tráfico:

http://www.dgt.es/portal/es/oficina_virtual/permiso_por_puntos/

Este portal dispone de dos métodos de acceso, con y sin certificado. Comparar las diferencias.

1.4 Administración Electrónica no es sólo usar la Firma Electrónica

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, poco a poco, 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 **Gobernanza** o la **Administración 2.0**

Profundizaremos sobre estas cuestiones en el apartado **Internet e Innovación en la** Administración Pública.

2. La Tecnología de la Administración Electrónica

Tal como lo indica su propio nombre la Administración Electrónica es un concepto impregnado de tecnología. Aunque lo deseable es que sus usuarios necesiten la menor cantidad de conocimientos técnicos posibles es imprescindible que conozcan y domine unos conceptos técnicos, no asumir este hecho sería como pretender ser un usuario de informática sin aprender a utilizar un ratón.

Es por tanto importante asentar estos fundamentos técnicos propios de la Administración Electrónica, ya que sólo así los usuarios, tanto ciudadanos como funcionarios, podrán entender lo que está ocurriendo realmente cuando realizan sus operaciones, resolver los problemas que les surjan y obtener un nivel de confianza adecuado en lo que están haciendo, máxime cuando se trata de de actuaciones sensibles por sus repercusiones jurídicas como lo son las actuación de la Administración Pública.

2.1 Conceptos Fundamentales

Si hubiera que destacar algún aspecto técnico de la Administración Electrónica sobre los demás, éste sería sin duda la seguridad, ya que el problema clave del empleo de las TIC y de la automatización de las actividades administrativas mediante las TIC es que la Administración tiene que llevar al terreno de las TIC las garantías jurídicas a las que tiene derecho el ciudadano y las empresas.

Esto ha hecho que la **firma electrónica** y el uso de **certificados electrónicos** sean las tecnologías clave en la aplicación de las TIC a las actividades propias de la Administración. Es por tanto esencial comprender estos conceptos y los principios y técnicas subyacentes sobre las que se asientan y que se presentan a continuación.

Como se verá a continuación estas tecnologías se asientan fundamentalmente sobre métodos de **criptografía** que se verán a continuación.

2.1.1 Criptografía Simétrica

La **criptografía simétrica** es el método criptográfico que usa una **misma clave** para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número n de personas que necesitan comunicarse entre sí, el número de claves necesarias para la comunicación privada entre 2 personas se dispararía. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Existen muchos métodos de criptografía simétrica, posiblemente el más importante sea actualmente **AES** (**Advanced Encryption Standard**), también conocido como **Rijndael**.

Estos algoritmos se usan en aplicaciones concretas donde el intercambio de claves no resulta problemático. Por ejemplo para la confidencialidad de documentos personales.

Una aplicación ejemplo es la utilidad open source (código abierto)[3] **TrueCrypt** (ver **Anexo I**) que permite crear **unidades de disco virtuales encriptadas**. Estas unidades de disco son virtuales porque en realidad no existen físicamente como discos, sino que las crea la utilidad a partir de un fichero encriptado con una clave elegida por el usuario. Sin embargo la utilidad lo presenta al usuario como si fuera una unidad de disco más del sistema.

El usuario simplemente arranca esta utilidad como cualquier programa e introduce la clave para lograr la mayor comodidad y naturalidad posible en su uso. Así el usuario lee y graba datos como el cualquier otra unidad física, pero los datos se almacenarán cifrados y serán inaccesibles para quien no tenga las claves.

Resulta muy útil para guardar la información sensible que se quiera proteger frente a terceros, especialmente de cara a guardar copias de seguridad de la misma. Es interesante, por ejemplo, para información como claves personales de acceso a otros sistemas (cuentas de bancos, documentos con información sensible, cuentas de sitios de Internet, etc.)

2.1.2 Criptografía Asimétrica

La **criptografía asimétrica** es el método criptográfico que usa un **par de claves** para el envío de mensajes. Las dos claves pertenecen a la misma persona. Una clave es **pública** y se puede entregar a cualquier persona o publicarla en algún sitio fácilmente accesible, la otra clave es **privada** y el propietario debe guardarla de modo que nadie tenga acceso a ella.

Además, los métodos criptográficos garantizan[4] que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Idea clave

Lo que se cifra con una clave, se puede descifrar con la otra, pero nunca con la misma. La diferencia en elegir una opción u otra es las aplicaciones que permite.

Es decir, si se cifra un mensaje o documento con la clave privada, se podrá descifrar con la clave pública, sin embargo no se puede descifrar utilizando de nuevo la clave privada. Igualmente, si se cifra con la clave pública, se podrá descifrar con la clave privada.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.

Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

[3] Término con el que se conoce al software distribuido y desarrollado libremente, con pleno acceso al código fuente. Generalmente, aunque no siempre, es además gratuito.

[4] En términos rigurosos no se trata de una garantía absoluta, sino de una probabilidad tan ínfima de que se puede considerar despreciable.

Idea clave

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la **confidencialidad** del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la **identificación** y **autenticación** del remitente, ya que se sabe que sólo pudo haber sido él quien utilizó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la **firma electrónica** a veces llamada **firma digital**.

La criptografía asimétrica tiene pocas desventajas. Entre los pocos que tiene, la más importante, si cabe, es el esfuerzo de cálculos matemáticos que implica, lo que la hace considerablemente más lento que la criptografía simétrica. Sin embargo, en las aplicaciones prácticas hay múltiples opciones para solucionar este problema.

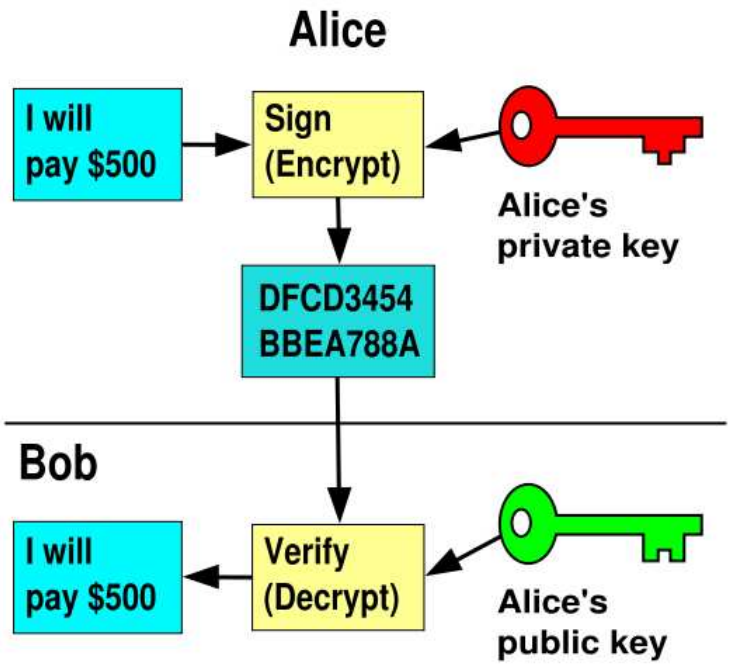


Ilustración 6 – Ejemplo de cifrado asimétrico: Alice cifra un mensaje con su clave privada ("I will pay $500") y lo envía a Bob. Bob puede descifrarlo, ya que tiene la clave pública de Alice. Bob sabe además así con certeza que fue Alice quien envío este mensaje. Si Bob quisiera enviar un mensaje secreto a Alice que sólo ella pueda leer podía usar su clave pública para cifrarlo y Alice su clave privada para descifrarlo.

En la comunicación de mensajes muy largos como puede ser, por ejemplo, la comunicación segura con un sitio Web como un banco se suele emplear en combinación con la **criptografía simétrica** (más rápido). Se usa primero un algoritmo asimétrico en una serie de mensajes cortos para establecer un **canal seguro** intercambiar sobre ese canal una clave simétrica acordada entre el navegador del usuario y el servidor del banco, y a continuación se cifran el resto de la comunicación esa clave simétrica.

Práctica: ejemplo de uso de claves simétricas

Instalación de los programas open source **TrueCrypt**, **AxCrypt** y **KeePass**. Practicar el uso de los programas.

Detalles técnicos sobre Criptografía Asimétrica

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un solo sentido que aprovechan propiedades particulares, por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil. Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso. Por ejemplo, si tenemos un número compuesto por dos factores primos y conocemos uno de los factores, es fácil calcular el segundo.

Dado un cifrado de clave pública basado en factorización de números primos, la clave pública contiene un número compuesto de dos factores primos grandes, y el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. El algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos, para que el descifrado sea fácil si poseemos la clave privada que contiene uno de los factores, pero extremadamente difícil en caso contrario.

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe probar hasta 2^{80}-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con un clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

2.1.3 Funciones y Códigos Hash (funciones resumen)

En informática, **Hash** se refiere a una función o método para generar claves o llaves que representen de manera unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una **función hash** o **algoritmo hash**, también se utiliza el término **función resumen** o **huella digital**.

En definitiva se trata de resumir una ristra de bytes de cualquier longitud en un código **hash** o **digest** es el resultado de dicha función o algoritmo y que tiene la gran ventaja de ser prácticamente **único** para una combinación de bytes y de **longitud fija**.

Según el algoritmo utilizado la probabilidad de **colisión** de códigos hash (que para diferentes entradas se genere el mismo código hash) es prácticamente despreciable.

Existen diferentes algoritmos, uno de los más populares son **SHA** (**Secure Hash Algorithm**) con una longitud clásica de 160 bits (SHA-1) o **MD5** (**Message-Digest Algorithm 5**) con una longitud de 128 bits.

Idea clave

La longitud de los códigos hash es fija, no depende de la longitud de los documentos originales por muy grandes que estos sean, sirve para identificarlos unívocamente y no permite deducir el documento original a partir del cual se han generado.

Estas propiedades serán esenciales en el uso de estos códigos en la **firma electrónica**.

Así el resultado de aplicar un algoritmo MD5 al texto *"Esto sí es una prueba de MD5"* sería e99008846853ff3b725c27315e469fbc (representación hexadecimal[5]). Un simple cambio en el mensaje nos da un cambio total en la codificación hash, en este caso cambiamos dos letras, el «sí» por un «no»: *"Esto no es una prueba de MD5"* = dd21d99a468f3bb52a136ef5beef5034

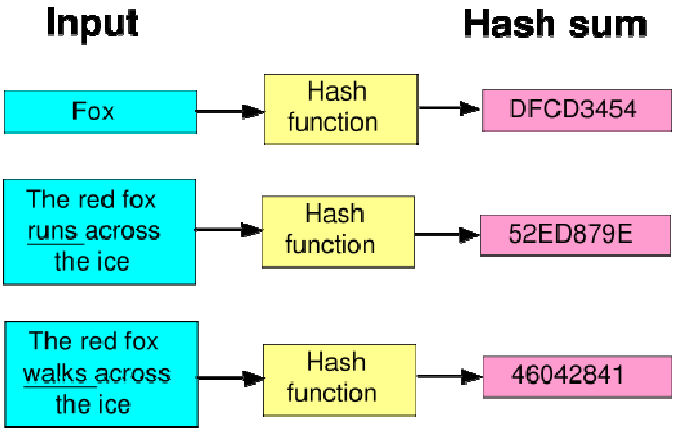


Ilustración 7 – Creación de códigos hash o digest.

El abanico de aplicaciones para este tipo de funciones es enorme. Unos pocos ejemplos son los siguientes:

- **Comprobación de integridad de ficheros**: se usa mucho en la descarga de ficheros grandes (por ejemplo: videos) desde Internet para comprobar que el archivo no esté corrupto (que ninguno de sus bytes esté cambiado). Se adjunta un código MD5 con el fichero y con una herramienta que analiza el fichero se comprueba el código MD5 que produce ese fichero, si son iguales es que hay la total certeza de que el fichero descargado es idéntico al original.
- **Identificación de ficheros independientemente de su nombre**: esta funcionalidad se usa mucho en redes P2P, ya que entre otras cosas permite detectar qué ficheros de los usuarios son en realidad los mismos (aunque tengan diferentes nombres) y distribuir así la descarga de los mismos.
- **Autenticación de usuarios**: cuando un usuario se da de alta en cualquier servicio surge un problema muy importante; la confidencialidad de su clave de usuario. Sólo la debería conocer él, ¿pero cómo evitar que la conozca el personal administrador de las máquinas que tiene acceso a todas las bases de datos, de usuarios, etc.? La solución son de nuevo los códigos hash: cuando un usuario se da de alta, no se da alta su clave, sino un código hash de la misma. Así es imposible saber cuál fue la clave elegida por el usuario, se mantiene su secreto. Sin embargo, al entrar en el sistema y teclear la clave original, el sistema puede comprobar fácilmente si es correcto aplicando de nuevo la misma función hash y comparando el resultado con el hash almacenado. Si coincide es que la clave introducida es correcta.
- **Firma electrónica**: supone una solución muy eficiente al problema de la lentitud cifrado de documentos grandes con claves asimétricas. Se verá en detalle más adelante.

Práctica: comprobar códigos MD5

Bajar cualquier fichero de Internet para el cual se haya adjuntado un código de comprobación MD5.

Por ejemplo: http://tomcat.apache.org/download-60.cgi

Utilizar una herramienta (por ejemplo: MD5 Checker) para realizar la comprobación.

[5] Una representación de números muy utilizada en informática, ya que se adapta mejor a la naturaleza física de los circuitos de los ordenadores que la representación decimal convencional.

2.2 Certificados digitales (Certificados electrónicos)

Un **certificado digital** es un documento digital mediante el cual un **tercero de confianza** (una **autoridad de certificación**) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Para ello este tercero de confianza exige los requisitos para identificar con garantías absolutas al sujeto del certificado. Si es una persona particular, por ejemplo, le exigirá que se persone con su DNI.

Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar **UIT-T X.509**. El certificado contiene usualmente el **nombre de la entidad certificada**, **número de serie**, **fecha de expiración**, una copia de la **clave pública del titular** del certificado (utilizada para la verificación de su firma digital) y la **firma digital de la autoridad emisora del certificado** de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

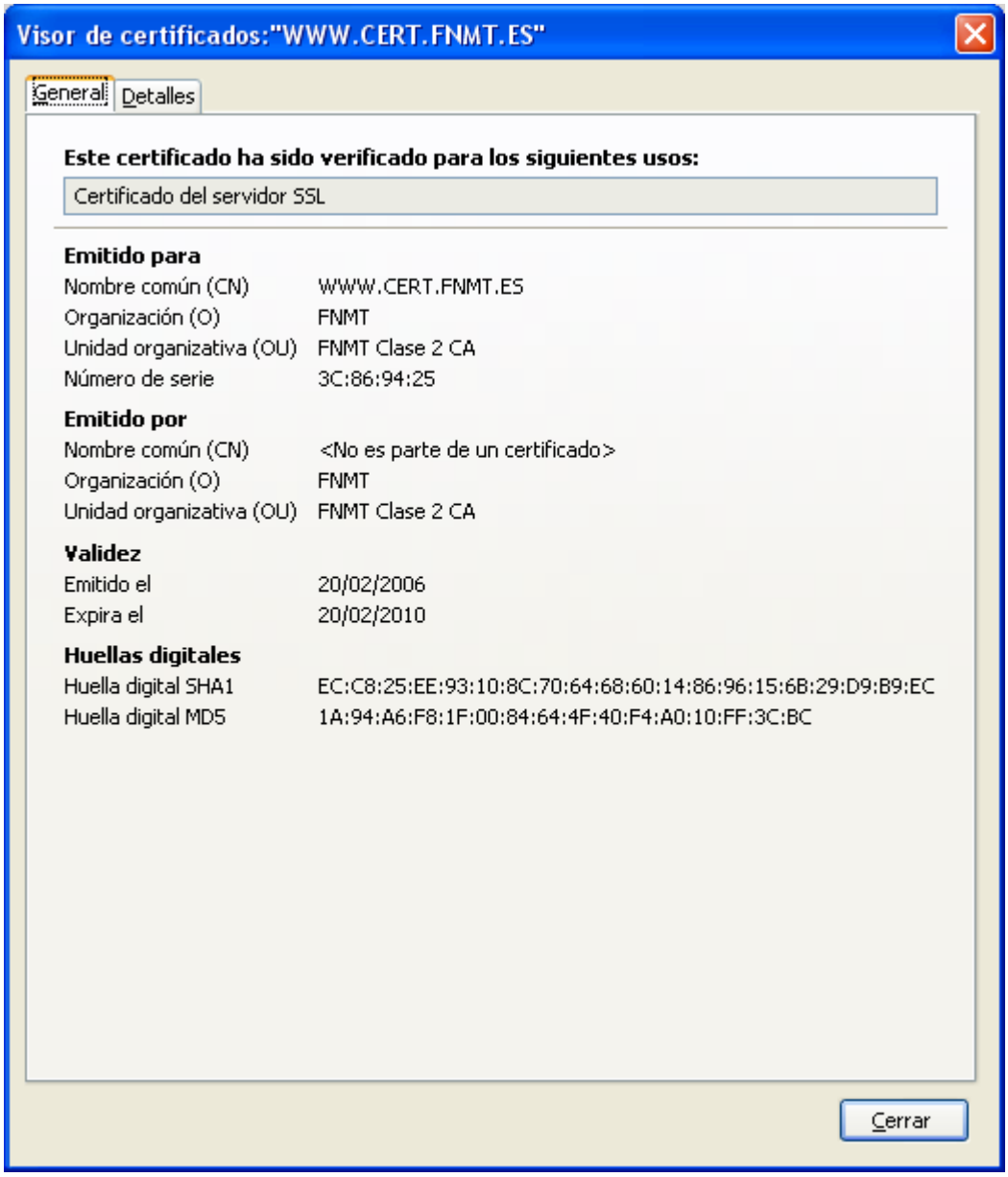


Ilustración 8 – Certificado que usa la FNMT para identificar su servidor del sitio Web. Como se puede apreciar, la entidad certificada corresponde al nombre de dominio de Internet ***www.cert.fnmt.es***, la sede electrónica se encuentra en **http://www.cert.fnmt.es/**

Práctica: inspeccionar los certificados que se encuentran en la máquina del usuario

Se propone hacer con, al menos, dos navegadores diferentes, por ejemplo Internet Explorer y Firefox para observar las diferentes filosofías de almacenamiento de los certificados (en este caso se el Explorar usa el almacén de Windows, mientras que Firefox usa un almacén propio independiente).

2.3 Autoridades de Certificación e Infraestructuras de Clave Pública (PKI)

Como se ha podido ver anteriormente, una autoridad de certificación (en adelante **CA**, de su nombre en ingles: Certification Authority) avala la entidad de los sujetos a los que expide los certificados, es decir, actúa de manera muy parecida a un notario que da fe de un hecho jurídico.

Para ello firma con su clave privada los 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 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 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 sujetos, 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 que y a la vez dispone de Autoridades de Certificación subordinadas. La CA raíz emite sólo certificados para si misma y sus CAs subordinadas, y serán éstas las que emiten 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.

La pregunta que surge ahora es: ¿y quien avala al certificado de esta última CA? ¿Cómo sé que el certificado de la CA es auténtico y no es alguno que alguien haya falsificado de algún modo?

La respuesta es que el certificado de esta última CA hay que instalarlo en el almacén de certificados del propio ordenador (y que luego usarán los navegadores). La idea gira de nuevo en torno a la confianza. 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, un ejemplo de un sitio de este tipo se puede apreciar en la **Ilustración 9**.

Existen muchas autoridades de certificación y por tanto soportarlas todas instalando sus certificados raíz en el ordenador personal sería una tarea muy molesta para los usuarios finales, por ese motivo todas las entidades importantes ya suelen venir preinstaladas en los navegadores. Aunque hay excepciones, la versión actual de Firefox[6], por ejemplo, aún no incorpora por defecto a la FNMT y hay que instalar por tanto su certificado manualmente.

2.3.1 Infraestructuras de Clave Pública (PKI)

Cuando se habla de autoridad de certificación hay que hablar también de **infraestructuras de clave pública**.

[6] En el momento de la redacción de este documento la versión 3.0.6

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.

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.

Ilustración 9 – Página de FNMT/CERES para la descarga de su certificado raíz. Obsérvese que la FNMT también usa autoridades de certificación subordinadas o intermedias.

Una PKI parte una **autoridad de certificación raíz** y es característico el uso de un certificado de esta autoridad auto-firmado por ella.

Siguiendo en la línea del ejemplo anterior sobre el Instituto de Salud Carlos III, éste podría 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 usuario tendrían que importarlo expresamente al no pertenecer al conjunto que el fabricante suministra por defecto con el navegador.

2.3.2 Usos de la Tecnología PKI

Los principales aplicación del uso de certificados e infraestructuras PKI son las siguientes:

- Autenticación de usuarios y sistemas (login).
- Identificación del interlocutor.
- Cifrado de datos digitales.
- Firmado digital de datos (documentos, software, etc.).
- Confidencialidad en las comunicaciones mediante técnicas de cifrado.
- Garantía de no repudio (negar que cierta transacción tuvo lugar).
- Sellado de tiempo.

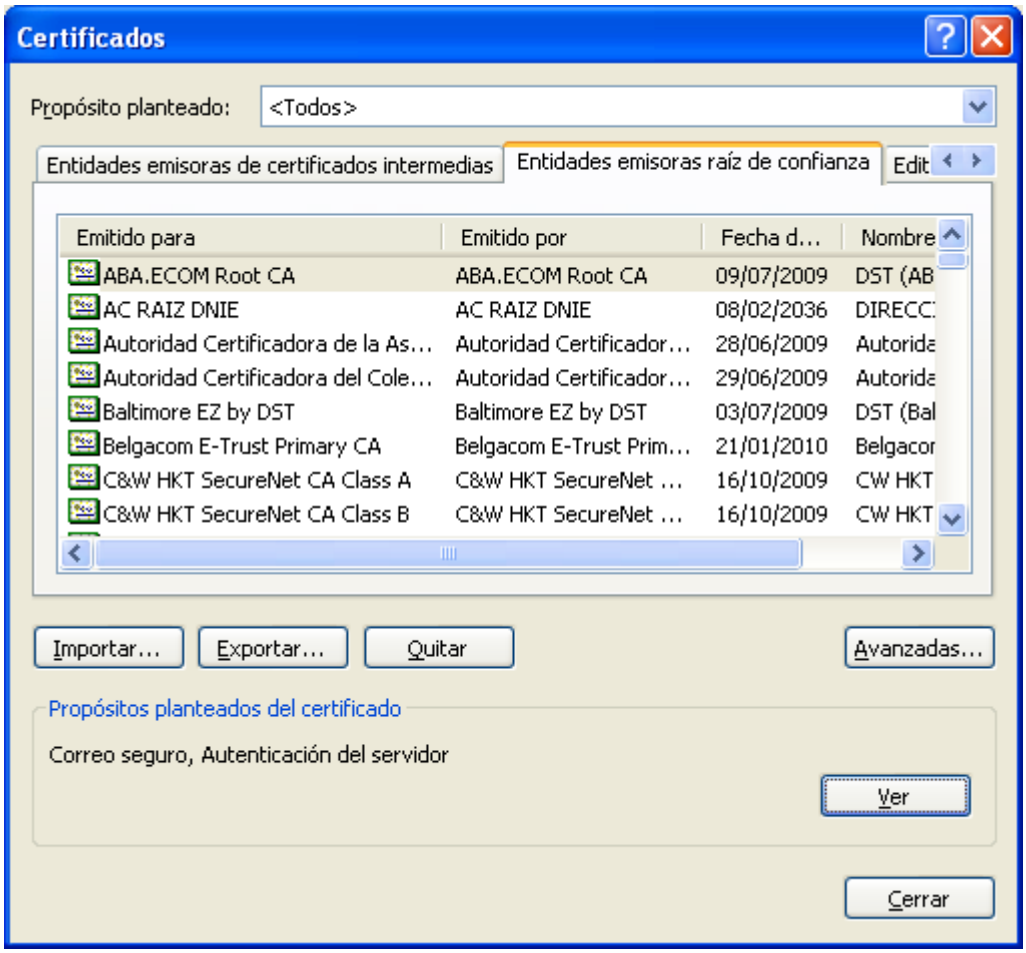


Ilustración 10 – Almacén de certificados de Windows. Está disponible para cualquier aplicación (navegadores, email, firma y verificación de documentos electrónicos, etc.), no obstante existen aplicaciones como el navegador Web Firefox que gestionan su propio almacén. Obsérvese como la CA raíz de la Dirección General del la Policía se encuentra entre ellas.

2.3.3 Gestión de Certificados. Consulta, Emisión y Revocación.

Tal como ya comentamos anteriormente, 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 en el equipo informático que se está usando como ya fue comentado anteriormente.

Para la vigencia es necesario consultar el propio certificado, ver si aún no ha expirado (similar a cómo se haría con 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[7].

2.3.4 Tipos de Certificados

Existen diferentes tipos de certificado digital, 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. (p.ej. 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.

[7] **Nota técnica**: en aras de una mayor sencillez del ejemplo se ha simplificado algo la problemática. Actualmente en la Administración la norma general es validar contra la plataforma Multi-CA del MAP, @Firma. La gran ventaja que ofrece es que en un único punto de acceso permite validar contra un largo número de CAs, un problema muy importante para la Administración, ya que debe admitir un elevado número de CAs en las relaciones con los ciudadanos y empresas.

De no existir @Firma sería necesario para cada unidad administrativa que preste servicios electrónicos que requieran el uso de certificados configurar y mantener enlaces con todas las CAs que haya que soportar. Con @Firma esta complejidad recae sobre el MAP y las unidades administrativas sólo se tienen que preocupar de su conexión con @Firma.

@Firma es accesible para todas las Administraciones a través de la Red SARA.

Práctica: descargar un certificado raíz de una autoridad de certificación
Descargar el certificado de la FNMT, y descargar el certificado del ISCIII desde la oficina virtual. Instalar ambos en Firefox. Comprobar que en el almacén de certificados de Windows ya existe el certificado de la FNMT, pero que no existe el certificado del ISCIII, importarlo. Crear con Openssl/XCA una PKI propia y emitir certificados personales que luego más adelante se usarán en otras prácticas.

2.3.5 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 y que corresponde a la pareja de clave privada/pública que el usuario ha tenido que generar previamente.

Es conveniente hacer una copia de seguridad del certificado, junto con la clave privada y que ésta información esté protegida frente a terceros que de obtenerla podrían firmar en nombre del usuario original.

Por otra parte el usuario querrá 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. Conviene tener muy claro qué elementos incluye cada formato, por razones obvias especialmente cuando incluye la clave privada.

Extensión	Descripción
*.p12	Corresponde al estándar PKCS[8]#12 que define un formato de fichero habitual para almacenar claves privadas juntas con su correspondiente certificado, protegido por una clave secreta.
*.pfx	Formato de fichero equivalente, predecesor de PCKS#12.
*.crt	Formato para almacenar certificados X.509v3.
*.pem	Privacy Enhanced Mail security certificate. Formato que desarrollo 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	Similar a *.cer, pero con un formato diferente.
*.key	Formato para la distribución de claves privadas.

Práctica: importar un certificado y hacer una copia de seguridad en un formato que incluya la clave privada
Importar el certificado personal en el repositorio del sistema operativo o el navegador. Una vez importado, exportarlo de manera que contenga la clave privada y protegerlo contra uso por terceros.

[8] En criptografía PKCS (Public Key Certificate Standards) se refiere al grupo de estándares elaborados por la empresa RSA Security que son los estándares de facto en las PKIs actuales.

2.4 Firma Electrónica

Desafortunadamente la Administración Pública todavía cuenta con un amplio abanico de tópicos ampliamente conocidos, eso hace que si se la habla de innovación en la Administración Pública quizás sea vea a más de una persona poniendo caras raras. Pero aunque parezca increíble en algunos campos efectivamente es innovadora, uno de ellos son las TIC y algo tan importante como el uso de la firma electrónica.

La idea del comercio electrónico en Internet ha calado ya desde hace tiempo, pero, ¿cuantos proveedores de servicios electrónicos ha visto que permitan el uso de certificados electrónicos en sus transacciones? ¿Cuántos bancos…?

Caja Madrid, una de las entidades más avanzadas en este aspecto, por ejemplo, sí ofrece esta posibilidad[9], 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. Es decir, se sigue usando en el fondo un sistema de usuario/clave.

Sin embargo a día de hoy el uso de certificados electrónicos es ya algo completamente habitual en los servicios que la Administración Pública y será el futuro en el sector privado también conforme se implante más y más el uso de certificados electrónicos y en particular del DNI electrónico para lo cual la Administración electrónica está actuando como líder que genera un efecto arrastre sobre el sector privado.

Ilustración 11 – ¿Esto es una firma electrónica?

La pregunta evidente que toca responder ahora es: ¿qué es la firma electrónica? La respuesta tiene sus matices y puntos de vista, veamos por tanto algunas definiciones de diferentes fuentes:

En primer la definición del **artículo 3** de la **Ley 59/2003, de Firma Electrónica**:

> ***Artículo 3. Firma electrónica, y documentos firmados electrónicamente.***
>
> 1. *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.*
> 2. *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 que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.*

[9] Esto es cierto a fecha de 26/02/2009. Es posible que en un futuro cambie su política de autenticación eliminando la necesidad de claves de usuario.

3. *Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un **certificado reconocido** y generada mediante un **dispositivo seguro de creación de firma**.*
4. *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.*
5. *[…]*

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.

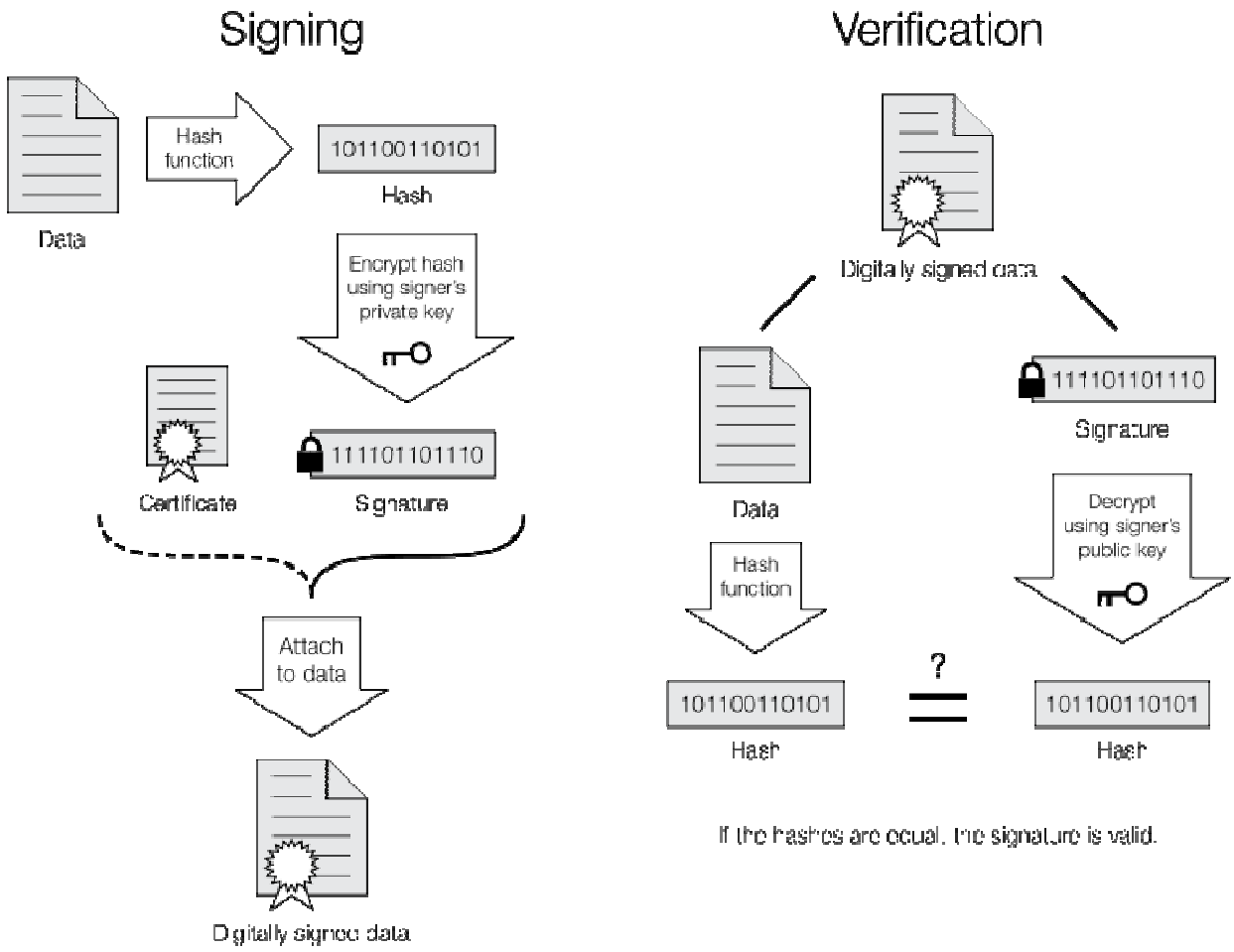


Ilustración 12 – Generación y validación de una firma electrónica.

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, firma electrónica es un término de naturaleza fundamentalmente **legal** y más amplia 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 europea 1999/93/CE** que estable 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 basado en un algoritmo de cifrado **RSA** y que utiliza certificados **X.509** para la acreditación de la identidad del firmante.

Técnicamente ocurre lo que se muestra la **Ilustración 12**, al firmar se genera primero un código hash o diggest a partir del documento/fichero firmado que se cifra. Éste código cifrado se adjunta al documento, junto con el certificado del firmante.

Para comprobar la firma el documento se generará de nuevo este mido código hash. Por otra parte se usa la clave pública para descifrar el código hash que generó el firmante y se comprueba si coinciden ambos. Si es así, no hay duda de que ha sido el firmante quien ha firmado el documento.

Idea clave

Se dice con frecuencia que tal usuario "firma con su certificado electrónico" un documento electrónico.

Aunque esta expresión es uso común y perfectamente aceptable en el día a día hay que recordar que técnicamente en realidad es totalmente incorrecta: los certificados no se usan para firma nada, sino que sirven para comprobar la identidad del firmante.

Lo que ocurre exactamente es lo siguiente: El usuario firma con su clave privada, el certificado electrónico avala su identidad con respecto a la correspondiente clave pública, de modo que al verificar la firma (el descifrado con la clave pública) si ésta se realiza con éxito, el certificado sirve para saber que la clave privada usada en la firma efectivamente es la pareja de la clave pública del certificado y que por tanto el propietario de esa clave privada es el que indica el certificado y que nadie salvo él pudo firmar.

2.5 El DNI electrónico

En España se expide desde marzo del año 2006 un tipo especial de documento de identidad denominado DNI electrónico.

El nacimiento del Documento Nacional de Identidad electrónico (DNIe) responde a la necesidad de otorgar identidad personal a los ciudadanos para su uso en la nueva Sociedad de la Información, además de servir de impulsor de la misma. Así, el DNIe es la adaptación del tradicional documento de identidad a la nueva realidad de una sociedad interconectada por redes de comunicaciones.

Por otra parte, desde un punto de vista legal, responde al marco de las directivas de la Unión Europea, dentro del cual el Estado español ha aprobado un conjunto de medidas legislativas, como la **Ley 59/2003 de Firma Electrónica** y el **Real Decreto 1553/ 2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica**, para la creación de instrumentos capaces de acreditar la identidad de los intervinientes en las comunicaciones electrónicas y asegurar la procedencia y la integridad de los mensajes intercambiados.

2.5.1 Información incluida

El DNI electrónico contiene dos certificados X509v3 de ciudadano (uno de autenticación y otro de firma) y claves privadas asociadas, que se generarán e insertarán durante el proceso de expedición del DNI electrónico.

- **Certificado de autenticación**: El Ciudadano podrá, a través de su Certificado de Autenticación, certificar su identidad frente a terceros, demostrando la posesión y el acceso a la clave privada asociada a dicho certificado y que acredita su identidad.
- **Certificado de firma electrónica reconocida o cualificada**: Permitirá realizar y firmar acciones y asumir compromisos de forma electrónica, pudiéndose comprobar la integridad de los documentos firmados por el ciudadano haciendo uso de los instrumentos de firma incluidos en él. Lógicamente, mediante la firma, también se consigue la no repudiación por parte del ciudadano de esos documentos.

El DNI electrónico no contiene ninguna otra información relativa a datos personales ni de cualquier otro tipo (sanitarios, fiscales, tráfico, etc.).

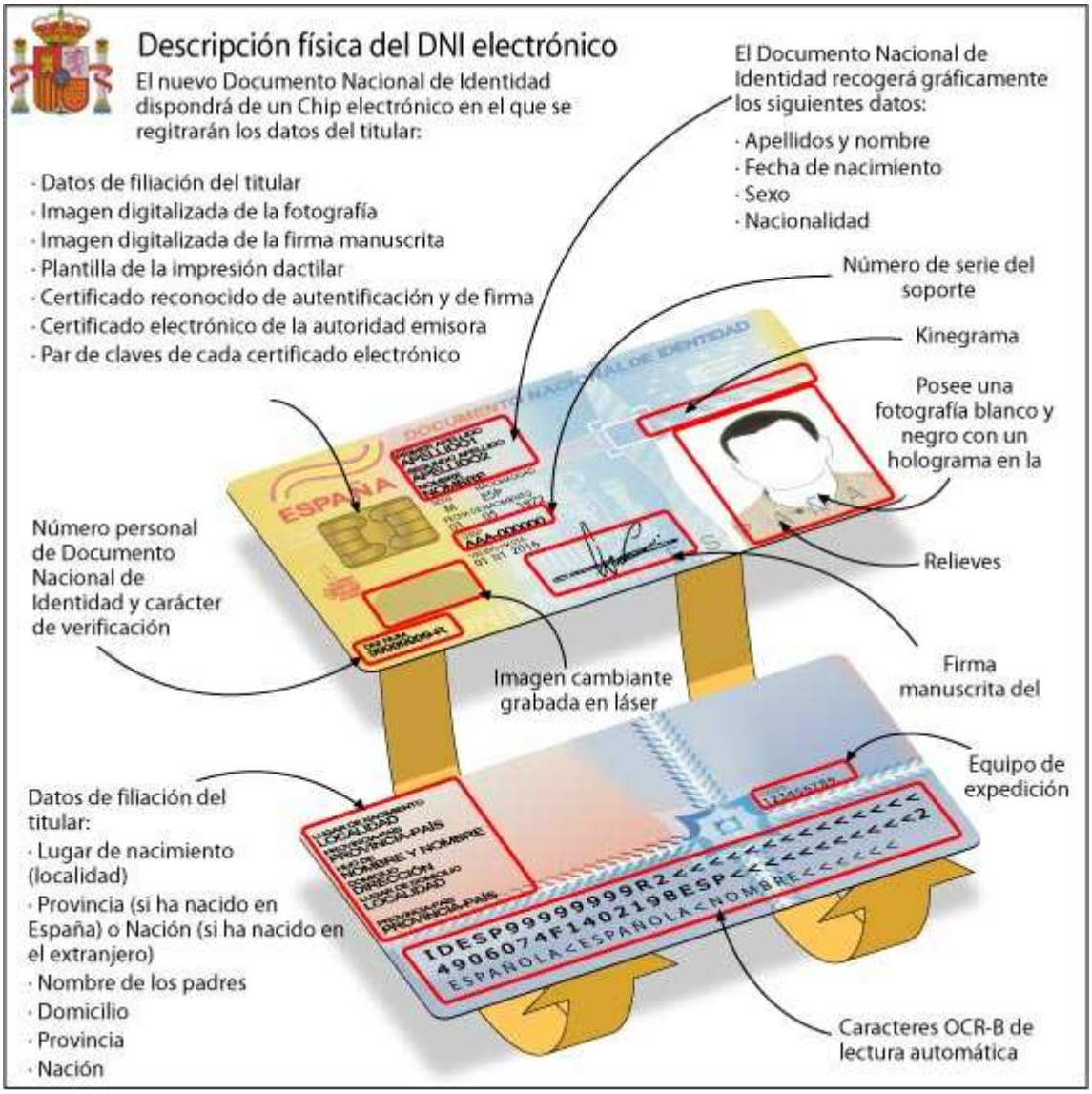


Ilustración 13 – Componentes del DNI electrónico.

2.5.2 Utilización

El uso del nuevo DNI electrónico requiere que el usuario recuerde la clave que se le asignó cuando lo obtuvo y que puede cambiar en sistemas automatizados instalados en las dependencias policiales en las que se expide el DNI. Para ello solo es necesario identificarse con la huella dactilar.

Los elementos necesarios para poder usar el DNI electrónico son los siguientes:

- **DNI electrónico**: Obviamente se debe sustituir el DNI tradicional por el electrónico en una comisaría. Se debe recordar la clave personal que además de ser alfanumérica acepta símbolos y diferencia las mayúsculas de las minúsculas.

- **Lector de tarjetas inteligentes**[10]: El lector de tarjetas inteligentes debe ser válido para el uso del DNI electrónico. Para ello debe ser compatible con la norma **ISO 7816** (1, 2 y 3) o tener una velocidad mínima de 9.600 bits por segundo.
- **Programa informático**: Por último el ciudadano deberá descarga el software que proporciona la Dirección General de la Policía en el área de descargas del portal del DNI electrónico.

2.6 Conexiones Seguras HTTPS

Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas **HTTPS**, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

El sistema HTTPS utiliza un cifrado basado en la tecnología **Secure Socket Layer** (**SSL**) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP.

De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no puede ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Los protocolos HTTPS son utilizados por navegadores como: Safari, Internet Explorer, Mozilla Firefox, Opera y Google Chrome, entre otros.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

En la **Ilustración 14** se puede apreciar un ejemplo de una conexión segura, en este caso con la Web de Cajamadrid.

[10] Una tarjeta inteligente (smart card), o tarjeta con circuito integrado (TCI), es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada. Se reconocen fácilmente por los contactos metálicos en su carcasa (en el caso de tarjetas de contacto) que conectan la tarjeta al dispositivo lector. El estándar más importante (en tarjetas de contacto) es ISO/IEC 7816, es por tanto el usado por el DNIe. Existen no obstante otros estándares como Java Card o ISO/IEC 14443 para tarjetas sin contacto.

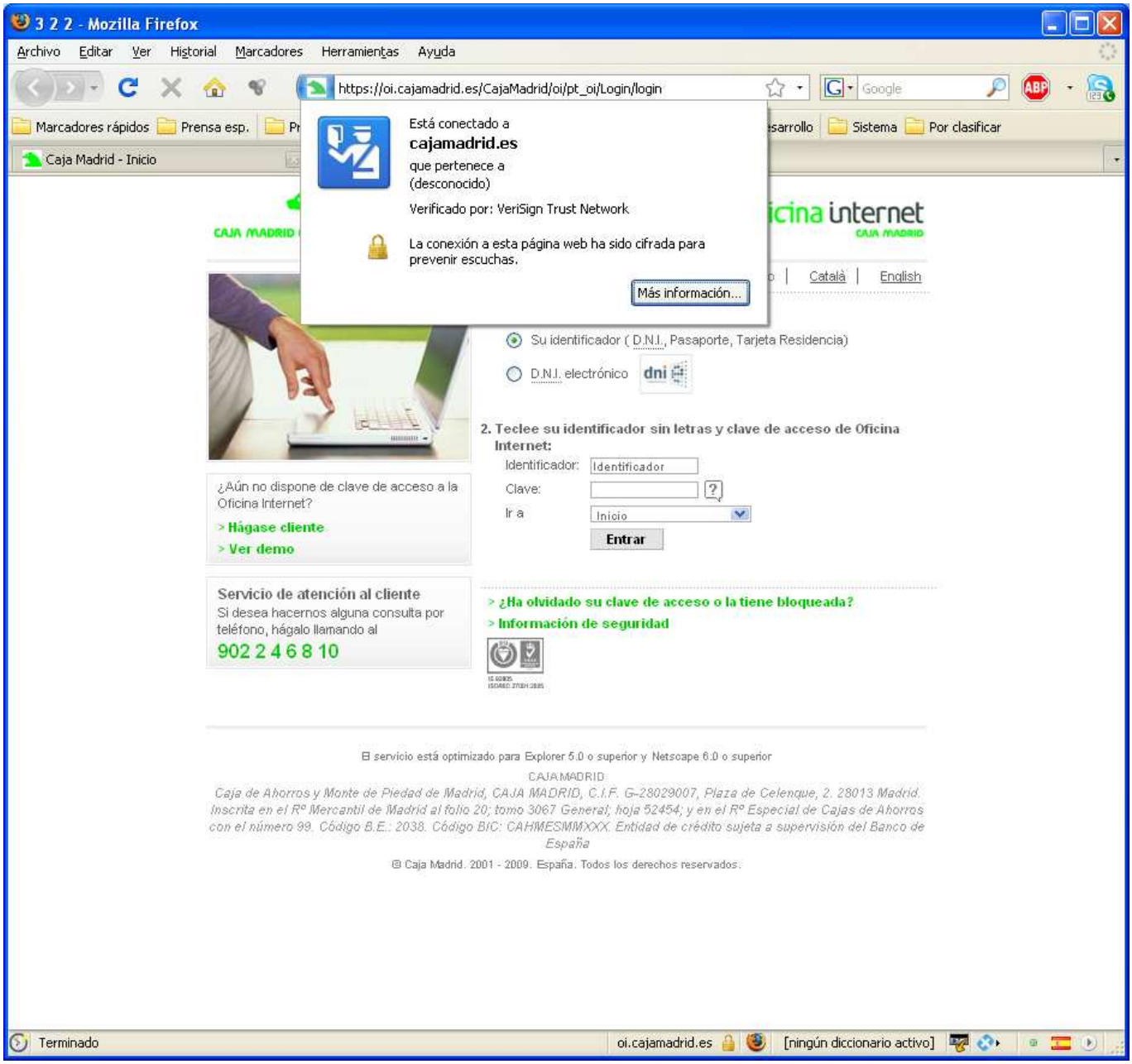


Ilustración 14 – Conexión segura con Cajamadrid con el navegador Firefox.

El navegador (Firefox) usa un recuadro azul que rodea el icono del sitio Web (el oso verde) junta a la barra de la dirección Web para indicar al usuario que el certificado de la conexión segura ha sido reconocido por el navegador (es decir, el certificado raíz que usa Cajamadrid se encuentra en el almacén de certificado que usa el navegador, ese certificado raíz pertenece a la empresa Verisign Trust Network). Además indica con un icono de un candado en el pie de la ventana que se ha establecido una conexión segura y que por tanto el usuario puede confiar en ella.

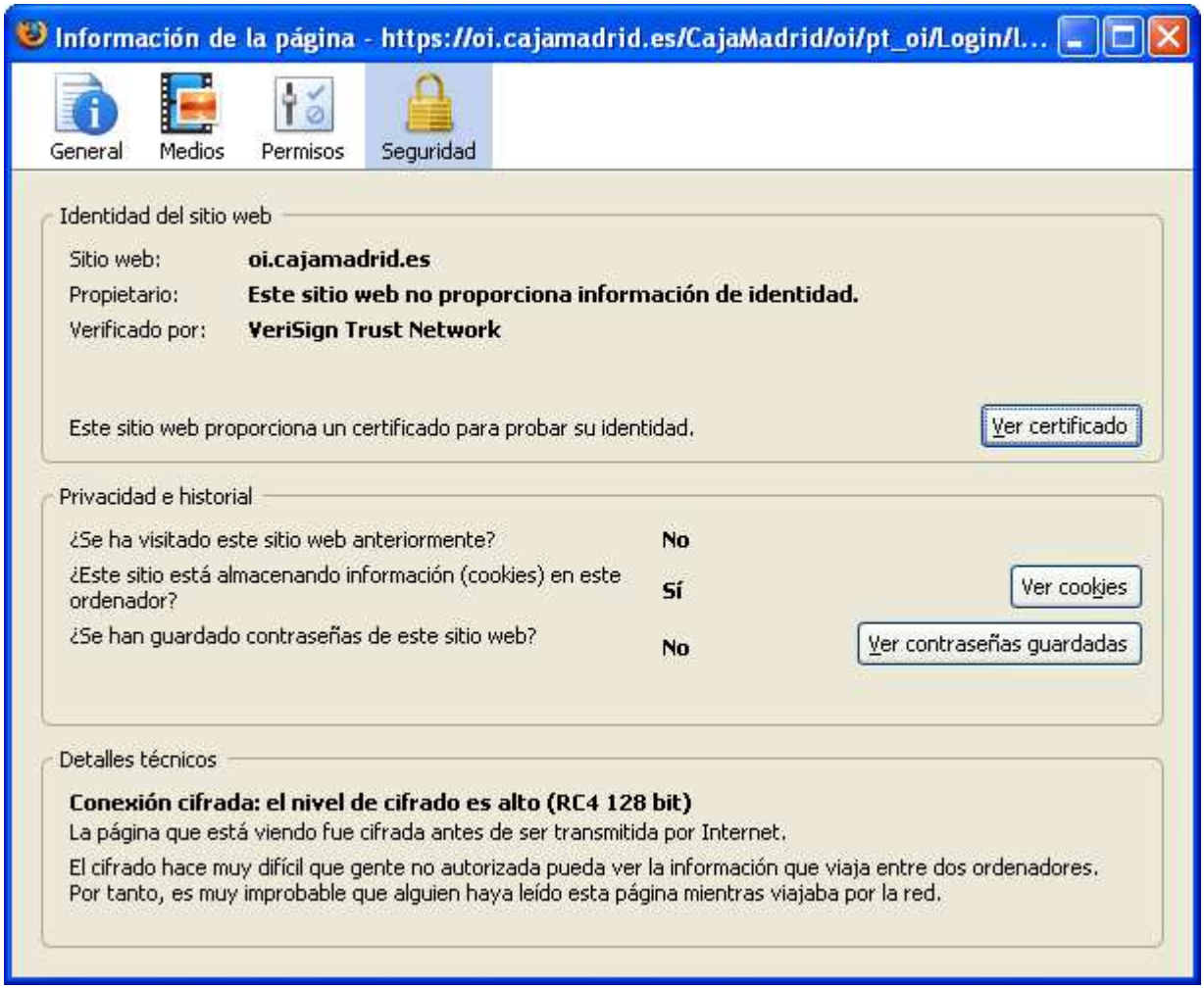


Ilustración 15 – Información del certificado empleado por el sitio Web de Cajamadrid.

Si el usuario hace "click" en el recuadro azul antes mencionado el navegador proporciona la información adicional que se puede apreciar en la **Ilustración 15**.

Cuando un sitio se identifica frente al navegador con su certificado de servidor, el navegador comprueba que efectivamente se trata de un certificado válido. Asume que es así cuando el certificado presentado cuenta con una autoridad de certificación que figura entre las del almacén del navegador. Si no es así asume que se podría tratar de un certificado falso, emitido por alguien que no es quien dice ser, aunque en la práctico esto sería un caso raro, lo normal será que la CA del certificado raíz no esté dada de alta en el almacén que usa el navegador.

En el caso de que no la autoridad de certificación no se encuentre entre las conocidas para el navegador, éste avisará de ello al usuario. Un ejemplo, para el caso de Firefox, se puede apreciar en la **Ilustración 16**.

Cuando se da esta situación lo más aconsejable es incluir el certificado de la autoridad de certificación que figura en el certificado raíz en el almacén de certificados. Para ello se puede acudir a la correspondiente CA y descargar el certificado en cuestión. En el caso de la FNMT, por ejemplo, se puede descargar en la siguiente dirección Web: http://www.cert.fnmt.es/index.php?cha=adm&sec=1&page=199

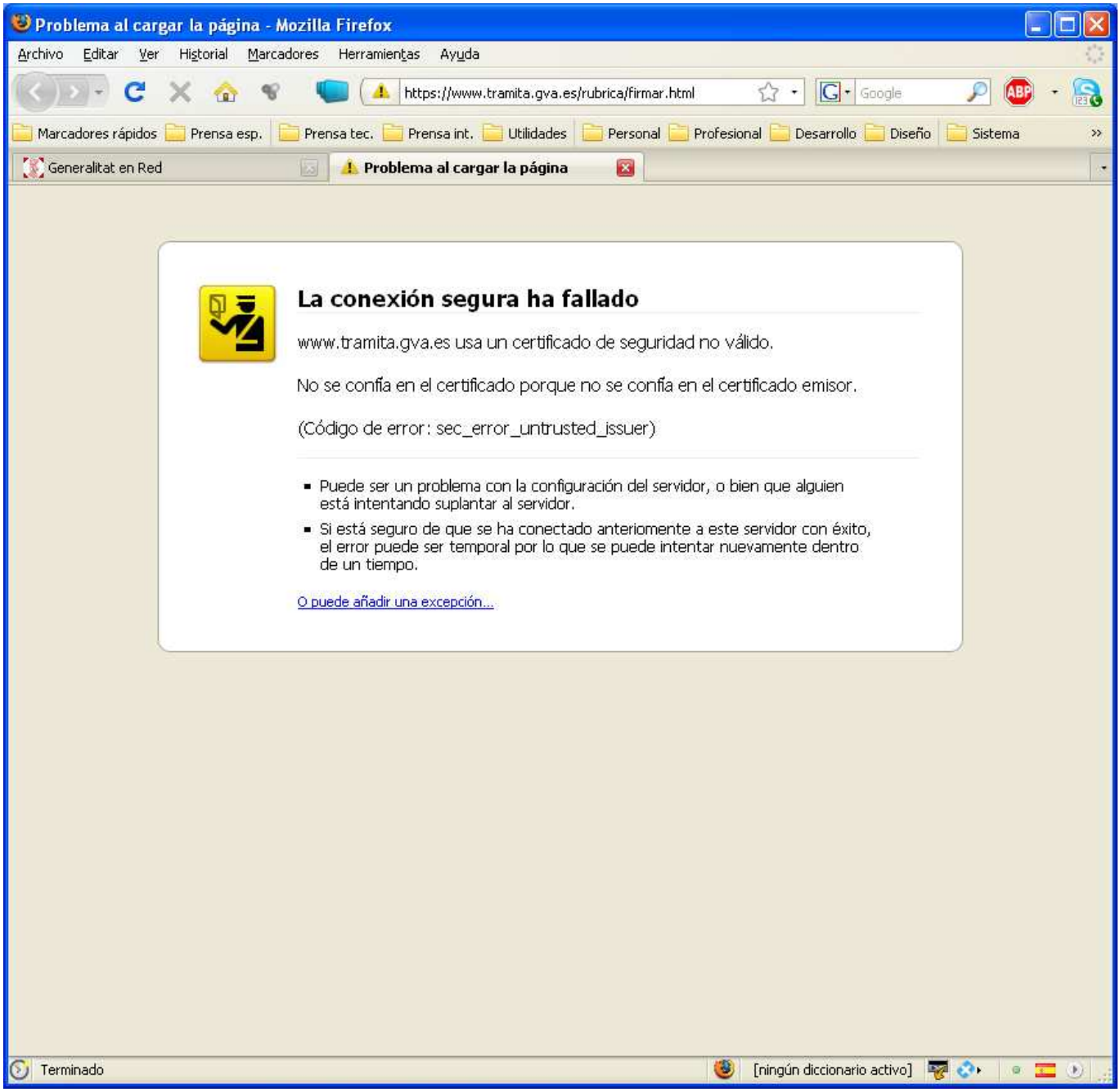


Ilustración 16 – Pantalla que muestra el navegador Firefox al establecer una conexión https con un sitio cuyo certificado no identifica como de confianza por no existir el certificado de la autoridad de certificación raíz correspondiente en el almacén de certificados.

Según el fabricante, los navegadores pueden ofrecer también mecanismos específicos de tratar el problema de los sitios cuyo certificado no se reconoce. Vea el apartado **3.2.2 El sitio Web (sede electrónica) del organismo usa un certificado que nuestro Navegador no reconoce** para más detalles.

Detalles técnicos sobre SSL

Para establecer un canal seguro el cliente y el servidor siguen un protocolo denominado "Handshake" que funciona del siguiente modo:

- El cliente envía un mensaje ClientHello especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados Challenge de Cliente o Reto). Además puede incluir el identificador de la sesión.
- Después, recibe un registro ServerHello, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.
- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.
- El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.
- Cliente y servidor negocian una clave secreta (simétrica) común llamada master secret, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este master secret (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una función pseudoaleatoria cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Esto se especifica en el RFC 2104).
- Protección contra varios ataques conocidos (incluyendo ataques man-in-the-middle), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.
- La función pseudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

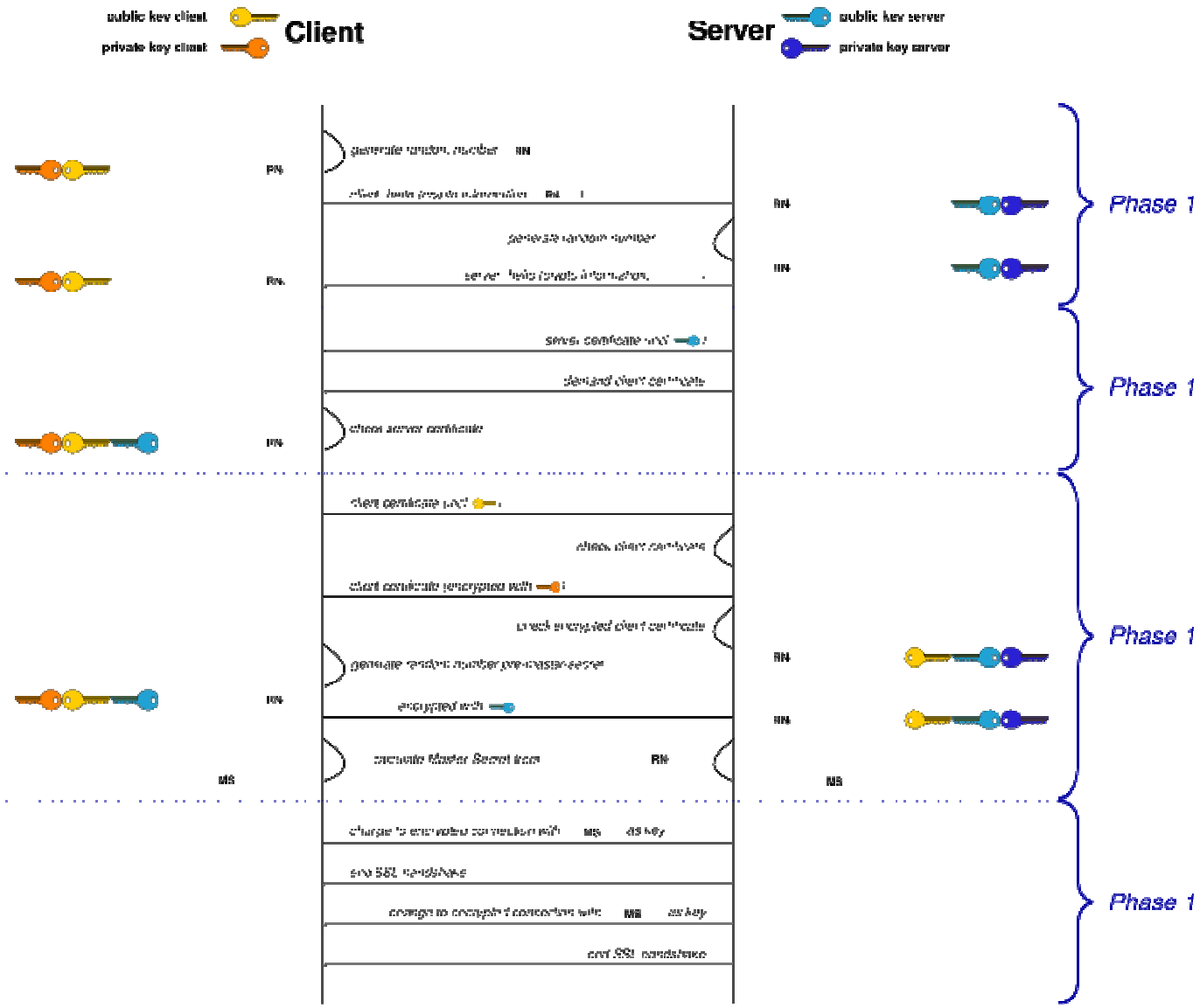


Ilustración 17 – Establecimiento de una conexión SSL. Más información en **http://en.wikipedia.org/wiki/Transport_Layer_Security**

3. LA ADMINISTRACIÓN ELECTRÓNICA EN LA PRÁCTICA

3.1 Tareas típicas

3.1.1 Obtener un certificado personal

En primer lugar hay que plantearse qué tipo de certificado se quiere obtener, hay básicamente 3 grandes opciones con diferentes pros y contras:

- **Certificado en fichero para su instalación en cualquier equipo**: es la opción más sencilla, pero también la más expuesta a riesgos, ya que el certificado y la clave privada se guardarán general en un fichero del tipo .p12 (es decir, ficheros que almacenan la clave privada). Si el usuario lo custodia adecuadamente no hay de qué preocuparse, además este formato contempla una clave de protección. Pero la falta de disciplina, tal 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 se use para otros fines) ponen en peligro la custodia y pueden ser una vía para que un tercero suplante la identidad del dueño del certificado sin que éste lo sepa.
- **Certificado en tarjeta criptográfica (tarjeta inteligente)**: más engorroso al requerir la adquisición de un lector, pero también considerablemente más seguro. Tiene 2 ventajas fundamentalmente que refuerzan su seguridad; las claves se generan en la 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 asociadas un PIN similar al usado en telefonía móvil para el cual hay que hacer las mismas advertencias en cuanto a su custodia como en el caso de los ficheros con claves privadas.
- **DNI electrónico**: técnicamente este caso es idéntico al anterior. Simplemente tiene la gran ventaja de usar este documento obligatorio para más funciones de las tradicionales, de hecho esta es la estrategia mediante la cual la Administración pretende lograr un impulso masivo del uso de firma electrónica en general y de la Administración Electrónica en particular.

Una vez elegida la correspondiente opción toca solicitar el certificado a la autoridad de certificación en cuestión. Generalmente se siguen los siguientes pasos (pueden variar ligeramente según la CA concreta):

1. Generación del par de claves en la máquina local (en el caso de un certificado en fichero) o en la tarjeta criptográfica y envío de la pública a la autoridad de certificación para que ésta cree el certificado.
2. Personarse en la autoridad de registro correspondiente para acreditar la identidad (esto se hace normalmente presentando el DNI convencional). En caso de personas jurídicas se exigirá la correspondiente documentación (escrituras, poderes de quien solicita, etc.).
3. Si se ha solicitado una tarjeta, instalación del correspondiente software en el equipo dónde se vaya a usar y adquisición de un lector de tarjeta inteligente adecuado.
4. 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 equipo desde el cual se solicitó.
5. Con el certificado instalado en el navegador o en su caso en otras aplicaciones, hacer una copia de seguridad. Ésta se realizará generalmente en un fichero .p12 que incluye certificado y clave privada.
6. ¡Disfrutar de los servicios electrónicos con certificado disponibles!

En cualquier caso hay que tener en cuenta 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.

3.1.2 Obtener el DNIe

El Ministerio del Interior ha habilitado un portal muy extenso con mucha información interesante, aplicaciones y manuales en torno al DNI electrónico o DNIe. El portal se encuentra en la siguiente dirección: http://www.dnielectronico.es/

A continuación se reproduce la guía básica para la obtención del DNIe publicada en este portal:

1. 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 comisarias, un lista completa se encuentra aquí: http://www.policia.es/cged/dni/mapa_oficinas.htm
2. Para solicitar la expedición del DNIe 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.
3. La entrega del DNI y de los certificados asociados se realizará personalmente a su titular en la misma jornada en que solicite su expedición.
4. 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.

3.1.3 Trabajar con formularios

Sin duda, una de los aspectos más útiles y productivos de la Administración Electrónico para el ciudadano es la posibilidad de poder iniciar y completar trámites completamente online ahorrando así desplazamientos engorrosos, paciencia y ausencias en el trabajo.

Para ello es necesario rellenar un formulario inicial como el de la **Ilustración 18** con los datos del usuario en cuestión, algunas veces incluso pide adjuntar información, y una vez completado todo se firma y se envía.

3.1.3.1 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[11].

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.

---

[11] Se puede pensar en soluciones como una fase previa de preparación de un expediente que se le ofrece al ciudadano para que este prepare toda la documentación necesaria desde su casa u oficina, sin llegar a iniciar aún el procedimiento. Los documentos para los cuales haya que efectuar copias (compulsas) electrónicas a partir del papel se podrán completar en una oficina física de la Administración, y firmar y enviar a continuación desde ahí la solicitud directamente o bien desde casa u oficina del trabajo.

Esto puede ser un alivio especialmente cuando en un futuro haya una fuerte interconexión de registros entre las Administración, así un ciudadano aún en caso de tener que utilizar documentos en papel podría beneficiarse de la mayor cercanía de las oficinas de su ayuntamiento para completar un trámite del Estado en ellas, por ejemplo. En cualquier caso, aún queda camino por recorrer para llegar a estas soluciones.

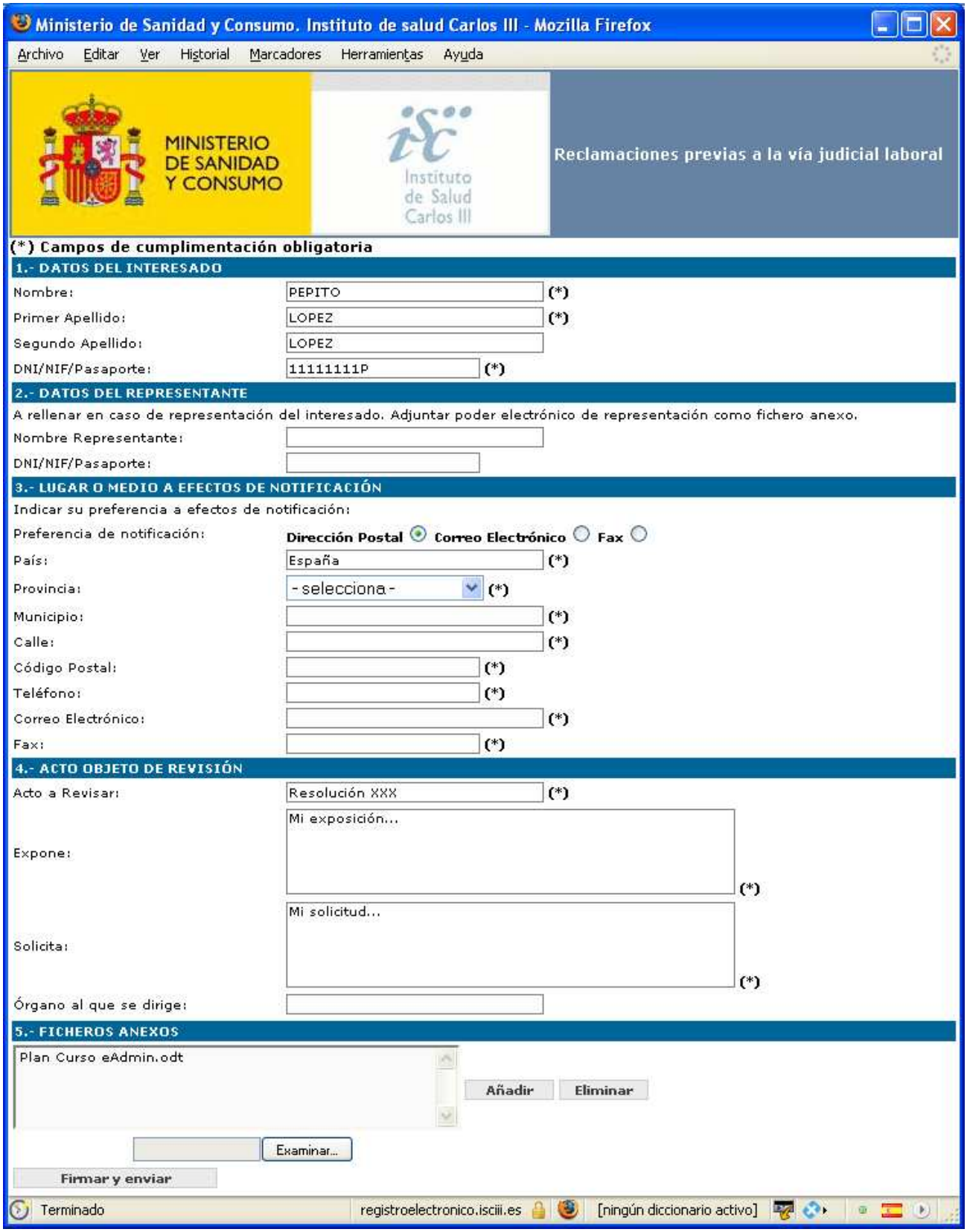


Ilustración 18 – Ejemplo de un formulario típico para iniciar un trámite. En este caso un recurso.

En la **Ilustración 18** 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 obligatorio (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 se requiere expresamente documentos adjuntos con firmados, 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.

3.1.3.2 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 PIN[12] 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 el uso de múltiples firmas. Puede ser el caso, por ejemplo, en solicitudes de ayudas para proyectos I+D dónde ha de firmar todo el equipo científico del proyecto.

En este caso no basta con simples formularios sino que las aplicaciones han de preveer 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 definitiva, 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).

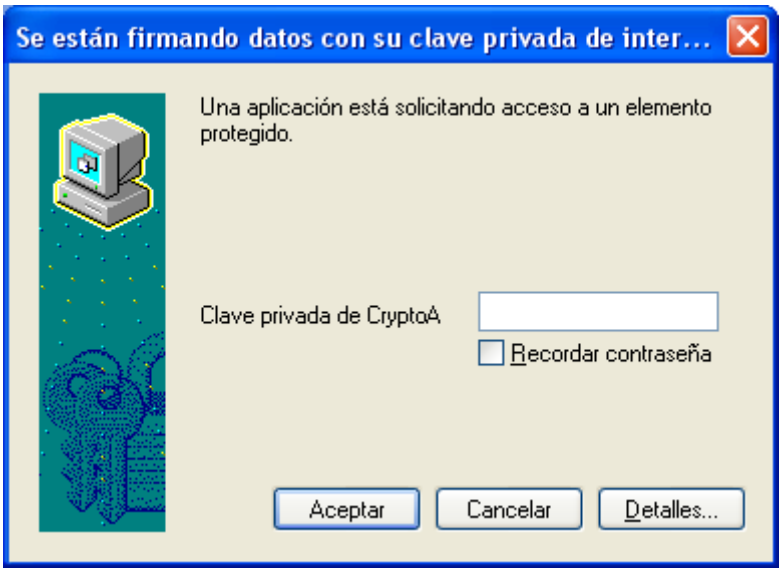


Ilustración 19 – Cuadro de diálogo que visualiza el almacén de certificados de Windows cuando detecta que una aplicación (en este caso el formulario Web) está accediendo a la clave privada del usuario. Ésta ha de introducir de protección de la misma para poder continuar.

[12] Si se han configurado las correspondientes opciones en el almacén de certificados y claves.

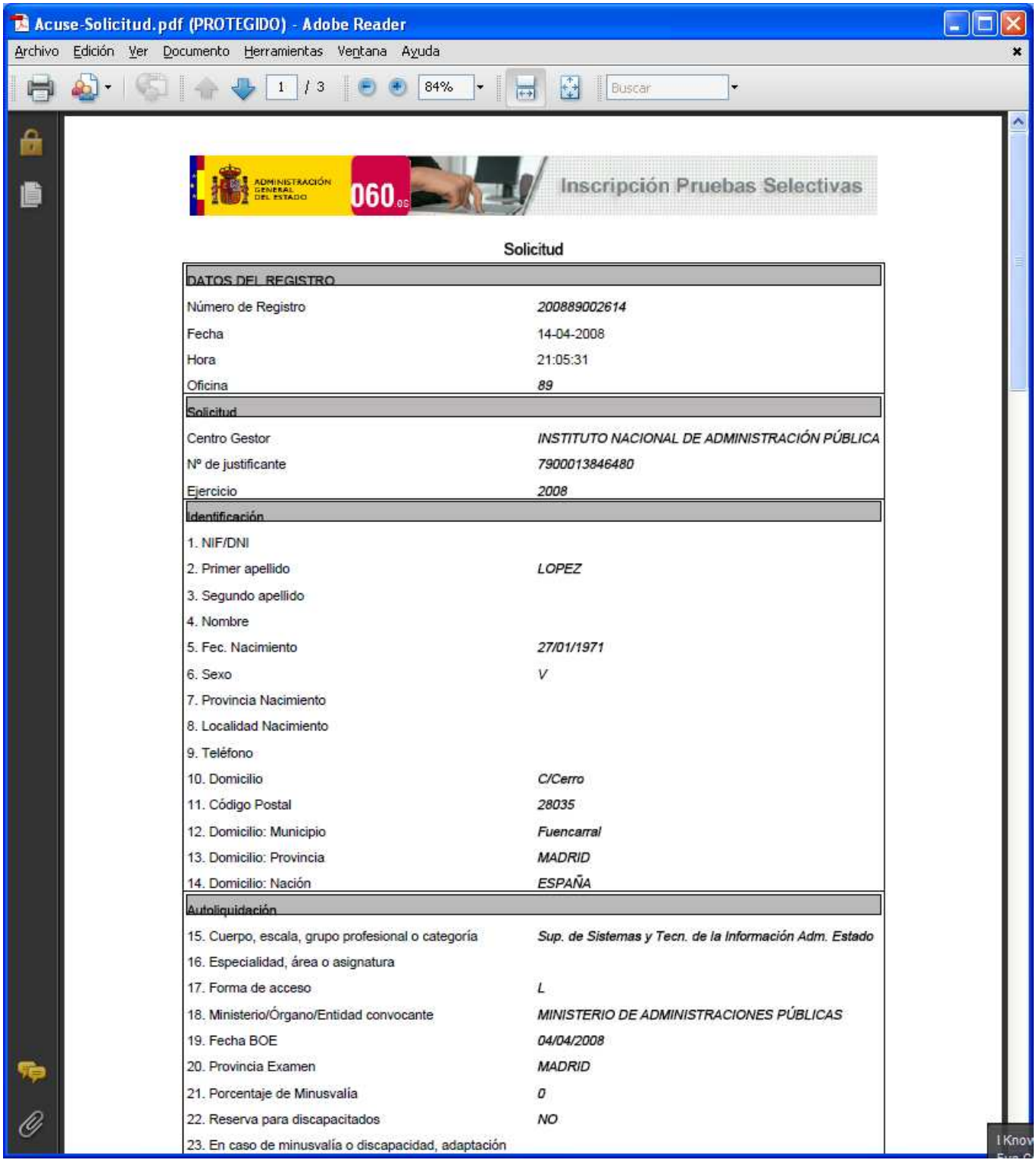
También es peculiar la problemática para los responsables tanto públicos como del sector privado, es decir tanto para los usuario de los servicios de Administración Electrónica como para sus gestores. Estas personas tienen muy poco tiempo disponible y han de firmar a veces decenas de documentos que otra persona les ha preparado previamente en un portafirmas.

En este sentido ya se están usando actualmente **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.

3.1.3.3 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 en este acuse 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.

En la **Ilustración 20** se puede ver un ejemplo de un acuse de recibo real emitido en la inscripción en las oposiciones para el ingreso en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado del Ministerio de Administraciones Públicas.



Acuse-Solicitud.pdf (PROTEGIDO) - Adobe Reader

Archivo Edición Ver Documento Herramientas Ventana Ayuda

1 / 3 84% Buscar

ADMINISTRACIÓN GENERAL DEL ESTADO 060.es Inscripción Pruebas Selectivas

Solicitud

DATOS DEL REGISTRO	
Número de Registro	*200889002614*
Fecha	14-04-2008
Hora	21:05:31
Oficina	*89*
Solicitud	
Centro Gestor	*INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA*
Nº de justificante	*7900013846480*
Ejercicio	*2008*
Identificación	
1. NIF/DNI	
2. Primer apellido	*LOPEZ*
3. Segundo apellido	
4. Nombre	
5. Fec. Nacimiento	*27/01/1971*
6. Sexo	*V*
7. Provincia Nacimiento	
8. Localidad Nacimiento	
9. Teléfono	
10. Domicilio	*C/Cerro*
11. Código Postal	*28035*
12. Domicilio: Municipio	*Fuencarral*
13. Domicilio: Provincia	*MADRID*
14. Domicilio: Nación	*ESPAÑA*
Autoliquidación	
15. Cuerpo, escala, grupo profesional o categoría	*Sup. de Sistemas y Tecn. de la Información Adm. Estado*
16. Especialidad, área o asignatura	
17. Forma de acceso	*L*
18. Ministerio/Órgano/Entidad convocante	*MINISTERIO DE ADMINISTRACIONES PÚBLICAS*
19. Fecha BOE	*04/04/2008*
20. Provincia Examen	*MADRID*
21. Porcentaje de Minusvalía	*0*
22. Reserva para discapacitados	*NO*
23. En caso de minusvalía o discapacidad, adaptación	

Ilustración 20 – Ejemplo de un acuse de recibo emitido en la inscripción un proceso selectivo de empleados públicos. Se han eliminado algunos de los datos personales originalmente presentes en la imagen.

3.1.4 Gestionar certificados y claves privadas

Ya se ha advertido anteriormente la importancia de custodiar las claves privadas para protegerlas del acceso por terceros, el cual podría llevar a la suplantación de la identidad del dueño de la clave. Igualmente conviene custodiar los certificados aunque estos de lo contrario que las claves privadas no son información sensible y se distribuyen para la acreditación de la identidad del poseedor del certificado a terceros.

3.1.4.1 Dar de alta un certificado raíz en el almacén de certificados

El lugar para dar de alta claves privadas y certificados es el almacén de certificados del equipo, como ya fue comentado en otras sesiones el almacén de certificados puede ser el propio del navegador o del sistema operativo.

Así Internet Explorer y otros navegadores como Google Chrome usan el almacén de certificados de Windows, mientras que, por ejemplo, Firefox mantiene su propio almacén. Esto significa que los certificados y claves privadas del almacén de Windows no serán reconocidas por Firefox y que habrá que importarlas por tanto además en el almacén de Firefox.

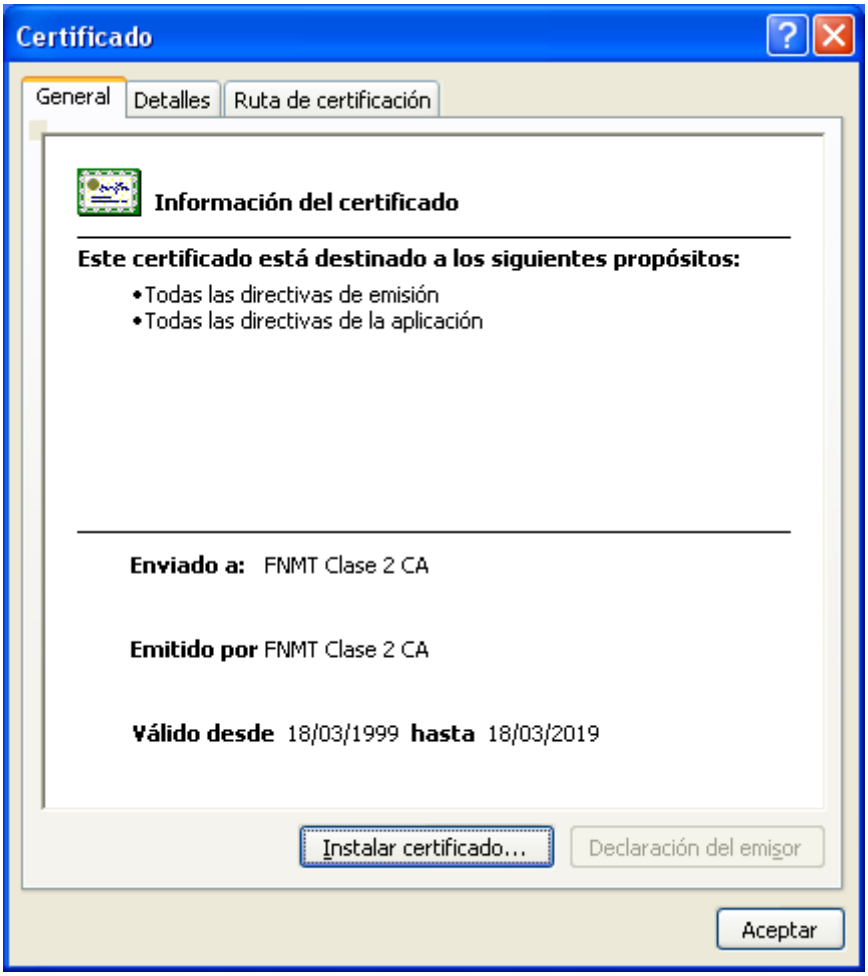


Ilustración 21 – Instalar un certificado en el almacén de Windows. En este caso se ha hecho haciendo doble-click sobre el fichero del certificado y pulsando a continuación el botón "Instalar certificado…" que abrirá un asistente de Windows para su instalación.

Cuando se obtiene por primera vez un certificado, generalmente se generará automáticamente el par de claves desde el navegador y se enviará la clave pública al proveedor (CA) al que se solicita el certificado, cuando éste lo expida se descargará e instalará automáticamente en el navegador y/o almacén desde el cual se generaron las claves inicialmente.

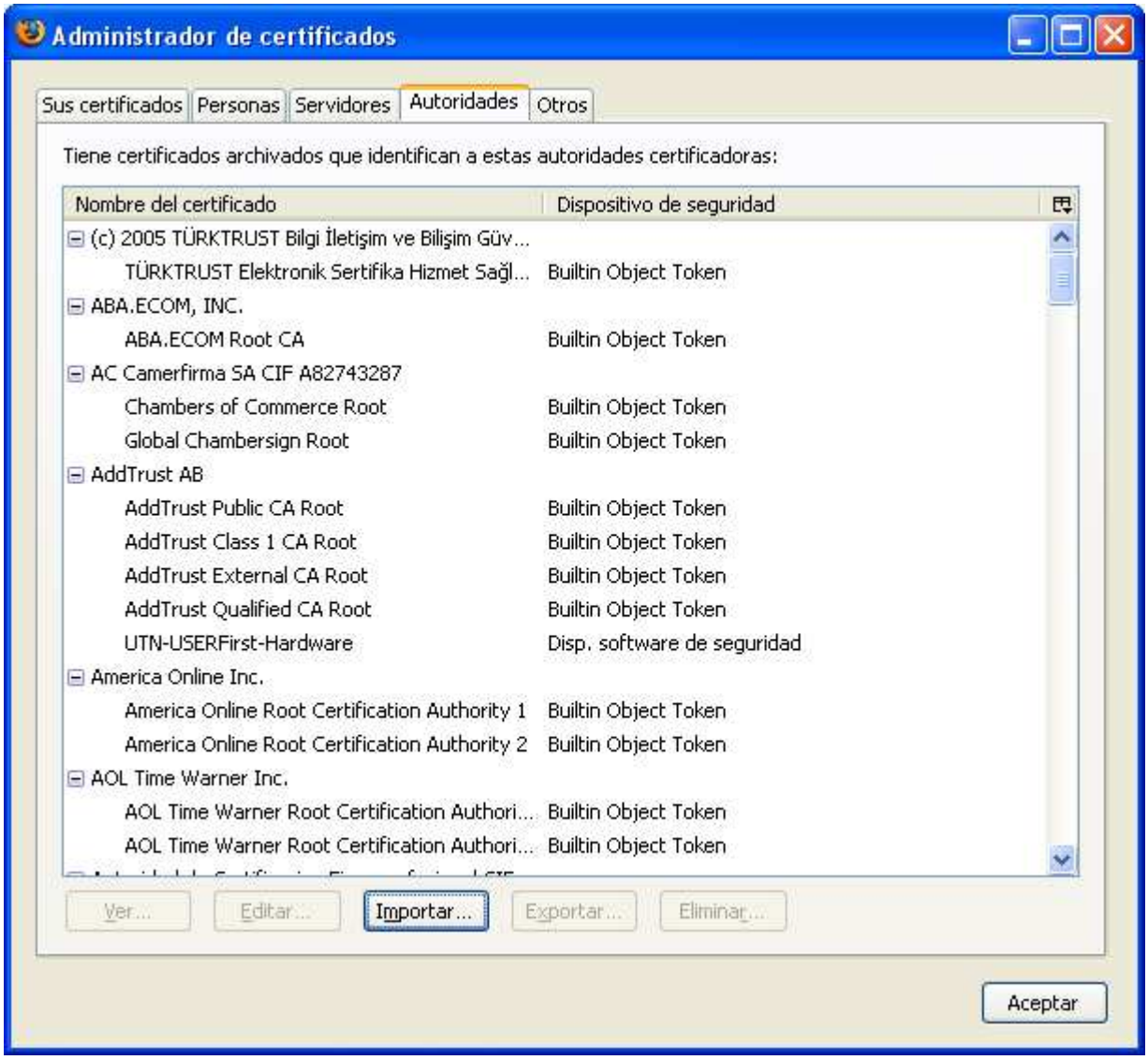


Ilustración 22 – Instalación de un certificado raíz desde el Administrador de certificados de Firefox (menu Herramientas/Opciones/Icono Avanzado/Pestaña Cifrado/Botón Ver certificados). En este caso es necesario importarlo expresamente desde el navegador, ya que Firefox actualmente no usa el almacén de certificados de Windows.

3.1.4.2 Proteger una Clave Privada

Una cuestión sumamente importante en el proceso de importación de la clave privada es su correcta protección mediante un PIN (contraseña).

La manera de cómo se realizan concretamente los pasos para esta protección varia según el almacén usado, pero básicamente se basa en el PIN del fichero con la clave privada (generalmente un fichero con extensión .p12), de modo que al importarla el almacén preguntará por este PIN y sólo si el usuario lo introduce correctamente la importará tal como se puede apreciar en la **Ilustración 23**.

En el caso del almacén de Windows, por ejemplo, se puede apreciar en la **Ilustración 23** también como se ofrecen opciones de seguridad adicionales al usuario tales como habilitar o impedir la exportación de claves privadas y el aviso al usuario del acceso a la clave.

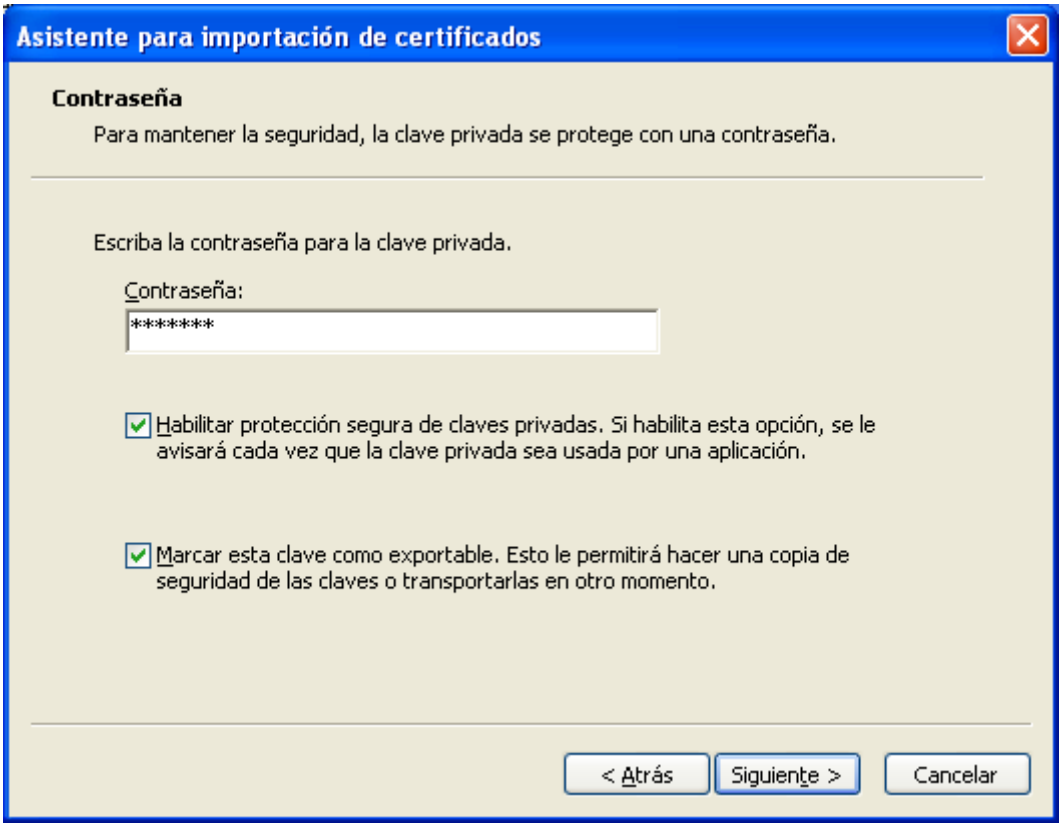


Ilustración 23 – Importación de un fichero de intercambio de información personal .p12 en el almacén de certificados de Windows.

Por otra parte también se puede proteger el uso de la clave para la generación de firmas de modo que en cada acceso a la misma (es decir, para firmar electrónicamente) se pedirá al usuario que introduzca el PIN.

Ilustración 24 – Protección del acceso a la clave privada en el almacén de certificados de Windows.

3.1.4.3 Realizar Copias de Seguridad de un Certificado personal

Una vez instalados la clave privada y certificado personal por primera vez, conviene hacer a continuación una copia de seguridad de los mismos.

Para ello se puede exportar el certificado junto con la clave privada, solo la clave privada o sólo el certificado. Según el almacén a partir del cual se hace la copia (o exportación) se ofrecerán todas o alguna de estas opciones de copia/exportación.

Importante: ya se ha hecho hincapié en la importancia de custodiar con mucho cuidada el fichero .p12 y su PIN de acceso. Desgraciadamente a veces se ven prácticas poco responsables por parte de la misma Administración. Por ejemplo esta utilidad de firma de documentos de la Generalitat Valenciana que pide junto con el documento el fichero .p12 y su PIN al usuario para firmar el documento (es de suponer que lo hace para usarlo luego en el lado servidor para realizar la firma): https://www.tramita.gva.es/rubrica/firmar.html

¡No se le ocurra dar el fichero .p12 y su PIN a nadie, ni siquiera a la Administración!

3.1.5 Firmar un documento

Antes se pudo ver 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.

En los formatos más populares (Word, Excel, PDF, …) es mismo editor del documento incorpora el soporte necesario para firmar un documento. No es objeto del manual entrar en las peculiaridades de cada una de las aplicaciones, pero una vez visto la mecánica general de firma es muy sencillo ya que en las opciones de configuración habrá la correspondiente entrada para la firma digital, y a partir de ahí el comportamiento será similar al de una firma en una aplicación Web: se pedirá al usuario el PIN para el uso de la clave privada y se firmará el documento. Además se guardará el certificado del usuario junto con el documento para que pueda ser consultado por un tercero.

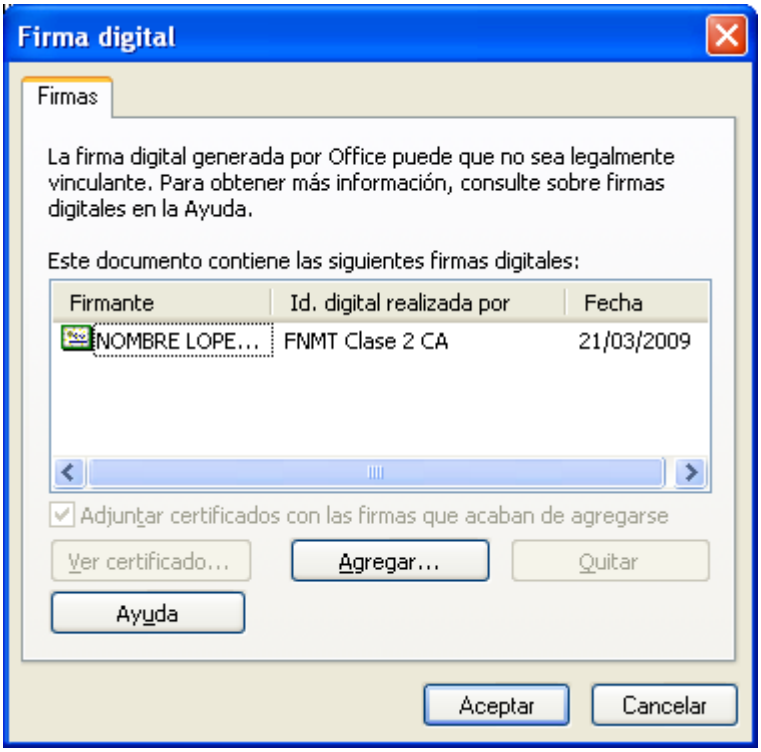


Ilustración 25 – Cuadro de diálogo que muestra Word 2003 para insertar una firma digital en el documento. Se puede apreciar que el documento ya cuenta con una firma que fue creada anteriormente.

Un ejemplo popular sería el editor Word, en este caso se puede añadir una firma digital a través del Menú Herramientas/Opciones/Pestaña Seguridad (versión Word 2003, se usa ésta como ejemplo por ser la más extendida en este momento). Una vez ahí pulsado el botón de "Firmas digitales…" aparece el cuadro de diálogo de la **Ilustración 25**.

Ilustración 26 – Aspectos de la barra de estado de Word 2003 con un documento firmado digitalmente. Se puede reconocer la firma por el icono rojo con forma de sello.

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, **Ilustración 26**. 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).

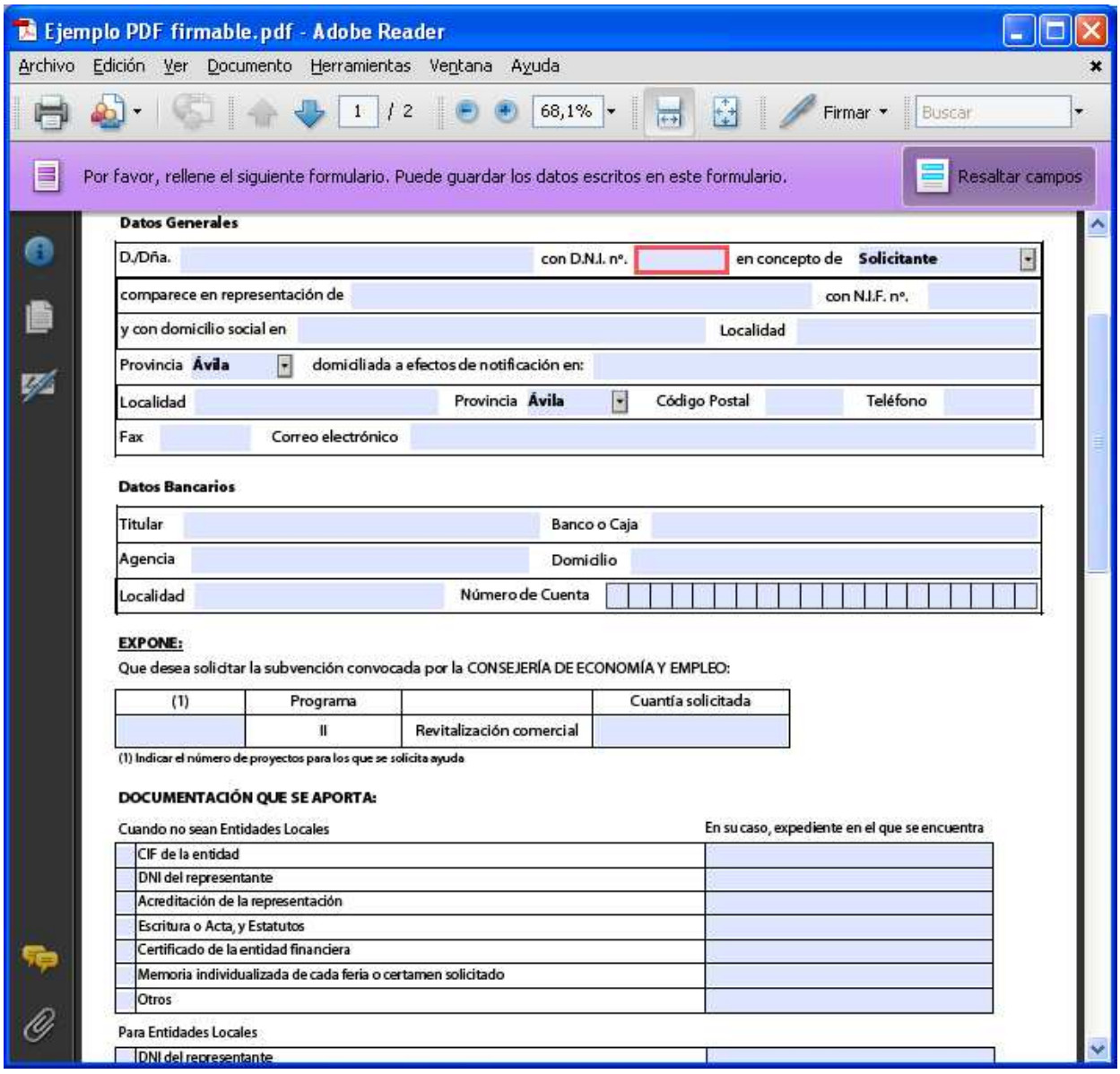


Ilustración 27 – Documento PDF preparado para firma.

Dentro de los editores que gestionan ellos mismo la firma electrónica hay que destacar el caso de los documentos PDF, ya que los usuarios utilizan generalmente el programa gratuito Acrobat Reader de la empresa Adobe para la visualización de los documentos y que es, como dice su nombre, un lector, no un editor. El editor (Adobe Acrobat) lo comercializa Adobe aparte y no es gratuito[13].

Para que un PDF se pueda firmar con Acrobat Reader es necesario preparlo, para lo cual será necesario la versión de coste (Adobe Acrobat) o bien alguna aplicación alternativa capaz de generar un PDF preparado para la firma digital. Muchas veces estos documentos PDF serán del tipo formulario, es decir, tendrán campos a rellenar por el usuario. Estos documentos pueden ser una buena alternativa a la firma de formularios Web.

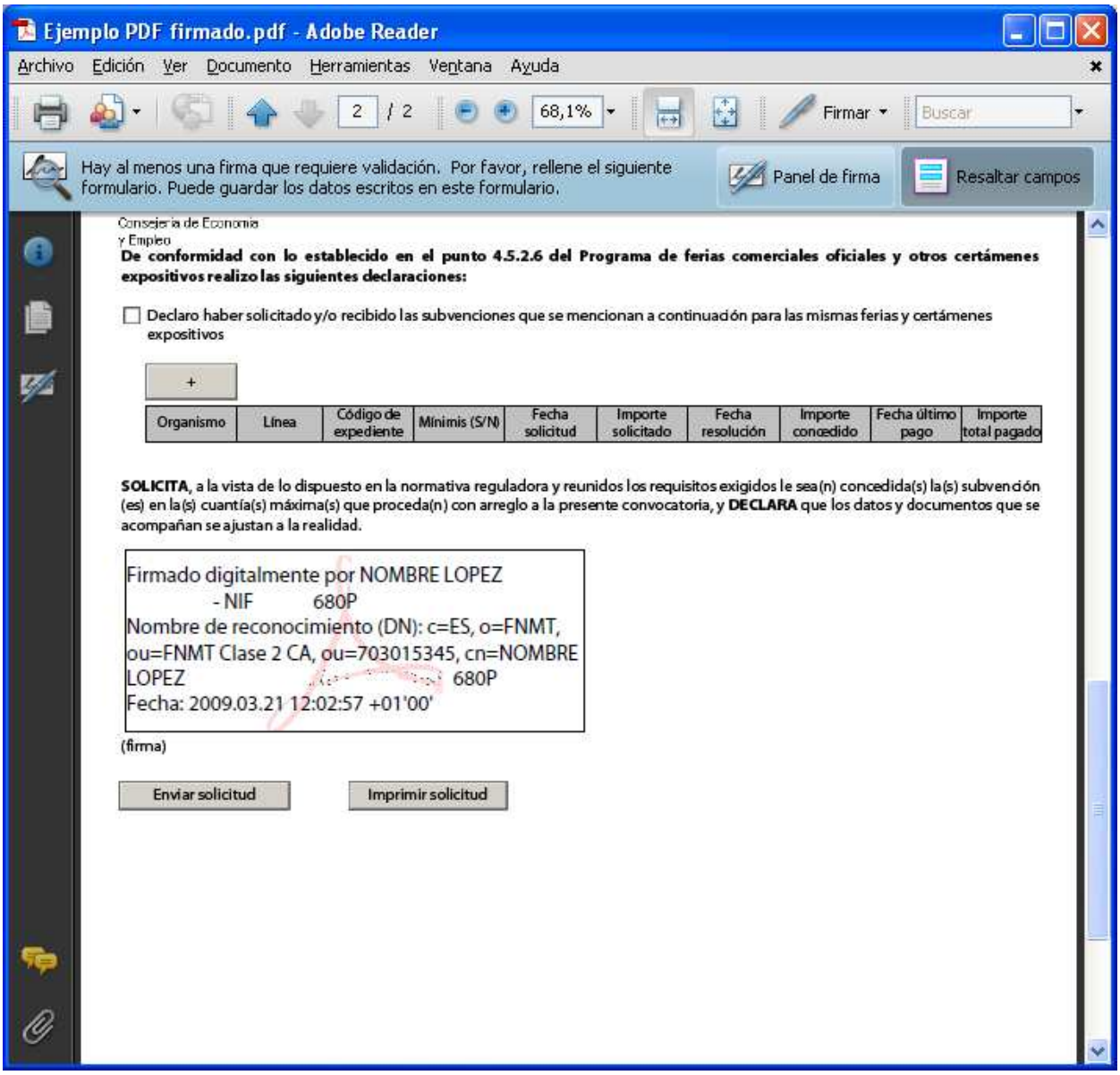


Ilustración 28 – PDF firmado (se han eliminado los datos personales de la firma). Aparte de la firma digital Acrobat Reader ha insertado un gráfico con los datos del firmante.

[13] Existen muchos otros programas que sí son gratuitos, aunque no disponen de una funcionalidad tan amplia como el Adobe Acrobat original. Algunos ejemplos son **PDFCreator** u **OpenOffice**.

Finalmente queda la alternativa general de utilizar una herramienta general de firma electrónica, independiente del formato concreto del documento.

Esta opción es menos cómoda que la gestión de la firma desde el editor, 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.

Un ejemplo es la utilidad **INTECOfirma** que ha desarrollado el **Instituto Nacional de las Tecnologías de la Comunicación** (**Inteco**), esta pequeña utiliza el estándar de firma electrónica **XAdES** en su versión 1.3.2, posiblemente el estándar de firma electrónica más importante en este momento.

XAdES 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. Un ejemplo de su apliación en la administración es el formato estándar de factura electrónica **Facturae**, el cual prevé **XAdES** como formato de firma.

Por sus características se está utilizando principalmente para el manejo de firma electrónica en el backoffice de las aplicaciones de la Administración. De cara al ciudadano, se siguen utilizando en gran medida documentos PDF firmados, fundamentalmente por comodidad para éste.

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.

Ilustración 29 – Pantalla principal de la herramienta de firma electrónica **INTECOfirma** del **Instituto Nacional de las Tecnologías de la Comunicación** (**Inteco**).

Práctica: firmar varios tipos de documentos

Firmar un .PDF preparado para su firma.

Firma un documento .doc, una vez firmado ver qué ocurre si se modifica el documento.

Firmar y recuperar documentos con IntecoFirma, utilizar certificados convencionales y el DNIe, probar la validación online del certificado del DNIe vía OCSP.

3.1.6 Cifrar documentos

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. Este tipo de información lamentablemente se encuentra a veces anotada accesible para todo el mundo, muchas veces en Post-it en el mismo ordenador del trabajador.

Ilustración 30 – Cifrado de un fichero con AxCrypt.

Obviamente esto es una muy mala práctica, especialmente cuando hay alternativas muy buenas para manejar este tipo de información, y hacerlo además muy cómodamente.

En el apartado sobre los fundamentos técnicos de la criptografía ya se expusieron las diferencias entre criptografía simétrica y asimétrica. En la casuística aquí descrita trata de información que normalmente sólo será manipulada por una misma persona, o un grupo muy reducido de personas. Por tanto encaja mejor la criptografía simétrica (con una sola clave).

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** (véase el anexo para más detalles), tiene como ventaja particular que al integrarse con el explorador de Windows resulta especialmente cómoda y rápida de usar. Así con hacer "click" con el botón derecho del ratón sobre el fichero a cifrar sale el menú contextual que se puede apreciar en la **Ilustración 30**.

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.

Volviendo al ejemplo de claves personales, se podría pensar ahora en mantener, por ejemplo, un simple fichero de texto con las diferentes claves y cifrarlo con AxCrypt, usando para el cifrado una clave especial que se memoriza y ya se utilizaría como clave maestra para cualquier información personal sensible.

3.1.7 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 debería ser fácil hacerse con el manejo de cualquier programa de correo electrónico que permita el uso de firmas digitales. Por su popularidad, se repasará un ejemplo concreto del uso de la firma electrónica en Outlook 2003[14].

En primer lugar hay que asignar el certificado a su cuenta de E-mail:

1. Con Microsoft Outlook abierto escoja del menú Herramientas, Opciones. Sale el cuadro de diálogo *"Opciones"* que se puede apreciar en la **Ilustración 31**.
2. En la ventana de Opciones que se abre a continuación, presione sobre la pestaña Seguridad. Cerciórese ahora de que el contenido del cuadro es el que aparece en la **Ilustración 31**.
3. Presione sobre el botón de *"Configuración…"*. Debería aparecer el cuadro de diálogo hijo del anterior rotulado *"Cambiar la configuración de seguridad"* que se aprecia en la ilustración. Presione primero sobre el botón *"Elegir…"* que esta al lado del campo Certificado de firma, y en la ventana que se abre escoja el certificado personal que quiera utilizar de la lista que se despliega[15]. Luego haga 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.

[14] En este ejemplo sólo se discuten firmas digitales basadas en el uso de certificados X.509, existen sistemas alternativos como PGP, pero que en la Administración prácticamente no se usan, y que por tanto no son de interés para este manual.

[15] Importante: Outlook utiliza el almacén de certificados de Windows, por tanto no se reconocerán los certificados que no se encuentren el mismo. Por otra parte, si quiere utilizar el certificado del DNIe, acuérdese de que el mismo debe estar insertado en el lector. Si lo ha insertado después de iniciar Outlook puede ser necesario cerrar y abrir de nuevo Outlook para que reconozca los certificados del DNIe.

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:

Si se han marcado las 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.

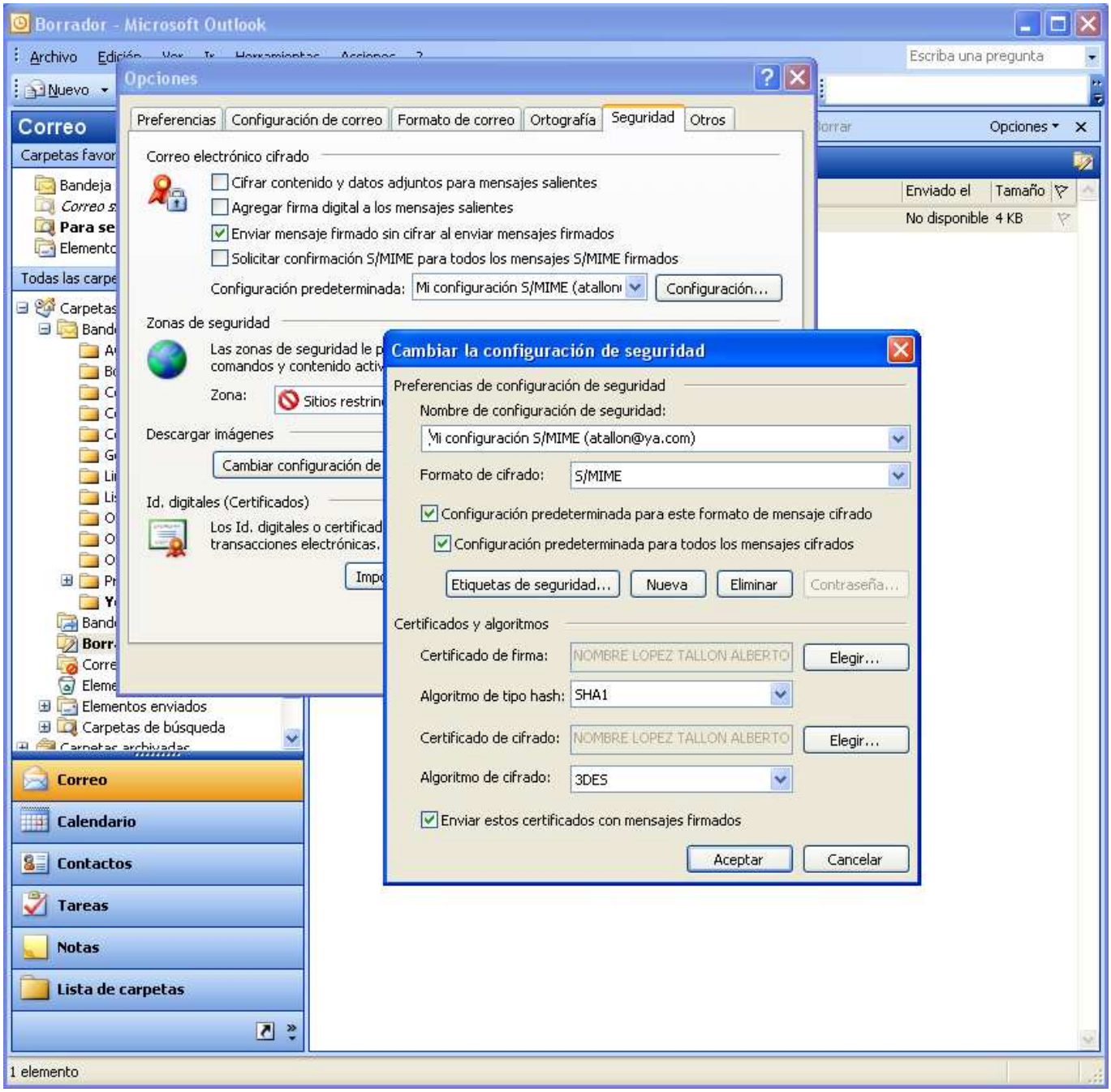


Ilustración 31 – Configuración de firma digital y cifrado en Outlook 2003.

3.1.8 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 correo electrónico debe disponer de la clave pública del destinatario del mensaje.

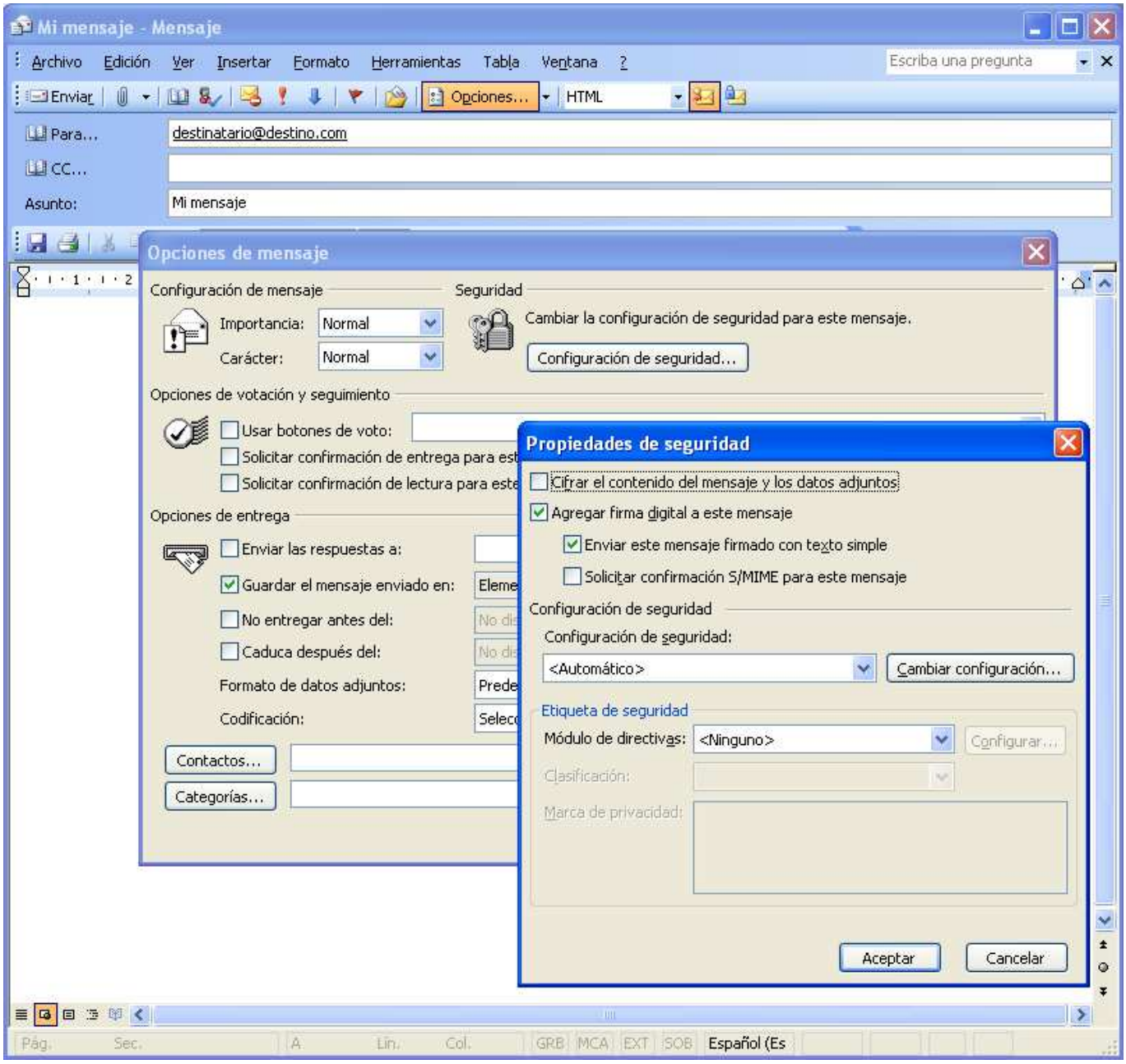


Ilustración 32 – Configuración individual de un mensaje de correo electrónico en Outlook 2003 para enviar como cifrado (hay que habilitar la opción de "Cifrar el contenido del mensaje y los datos adjuntos", en la imagen está aún deshabilitada).

Para ello hay diferentes posibilidades, una es recibir la clave pública 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.

Para ello se siguen los pasos siguientes:

1. Cree el mensaje de correo electrónico y adjunte los archivos que desee como de costumbre.
2. Presione sobre el botón *"Opciones…"* y en la ventana que se abre a continuación presione sobre el botón *"Configuración de seguridad…"*. Habilite la opción de "Cifrar el contenido del mensaje y los datos adjuntos".
3. Presione el botón de Aceptar y luego sobre el botón de Cerrar.
4. Presione sobre el botón de Enviar.

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 típicos.

3.2.1 Estamos usando 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 usando los servicios de Administración Electrónica.

Por tanto no es extraño que a un usuario se le pase la renovación aunque el proveedor de servicios de certificación (o 'prestador' como lo llama la **Ley 59/2003**) suele avisar por correo electrónico u otros medios con bastante antelación a los usuarios.

En este caso generalmente el sitio Web al que estamos accediendo deberá estar preparado para diagnosticar este problema y reportarlo al usuario, de todos modos 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 dar mensajes genéricos de error con el certificado, decir que el usuario no posee un certificado válido.

Por otra parte, por si esto fuera poco, el comportamiento concreto depende también del almacén de certificados. Así, por ejemplo, una vez más hay diferencias entre el almacén de Windows (que usan las aplicaciones de Windows como Internet Explorer, Word, Outlook, etc.) y el almacén de Firefox.

El almacén de Firefox permite utilizar certificados caducados y será por tanto el sitio quien detectará (o deberá detectar) que el certificado del usuario ha expirado, sin embargo, el almacén de Windows aunque puede albergar certificados caducados, incluso importarlos, no permite utilizarlos si encuentra que ha expirado su periodo de validez.

Queda por tanto como conclusión que ante cualquier anomalía con respecto al certificado de usuario que ocurra al intentar acceder a una Web que lo requiera se comprueba que este se encuentra en el almacén que corresponde y vigente.

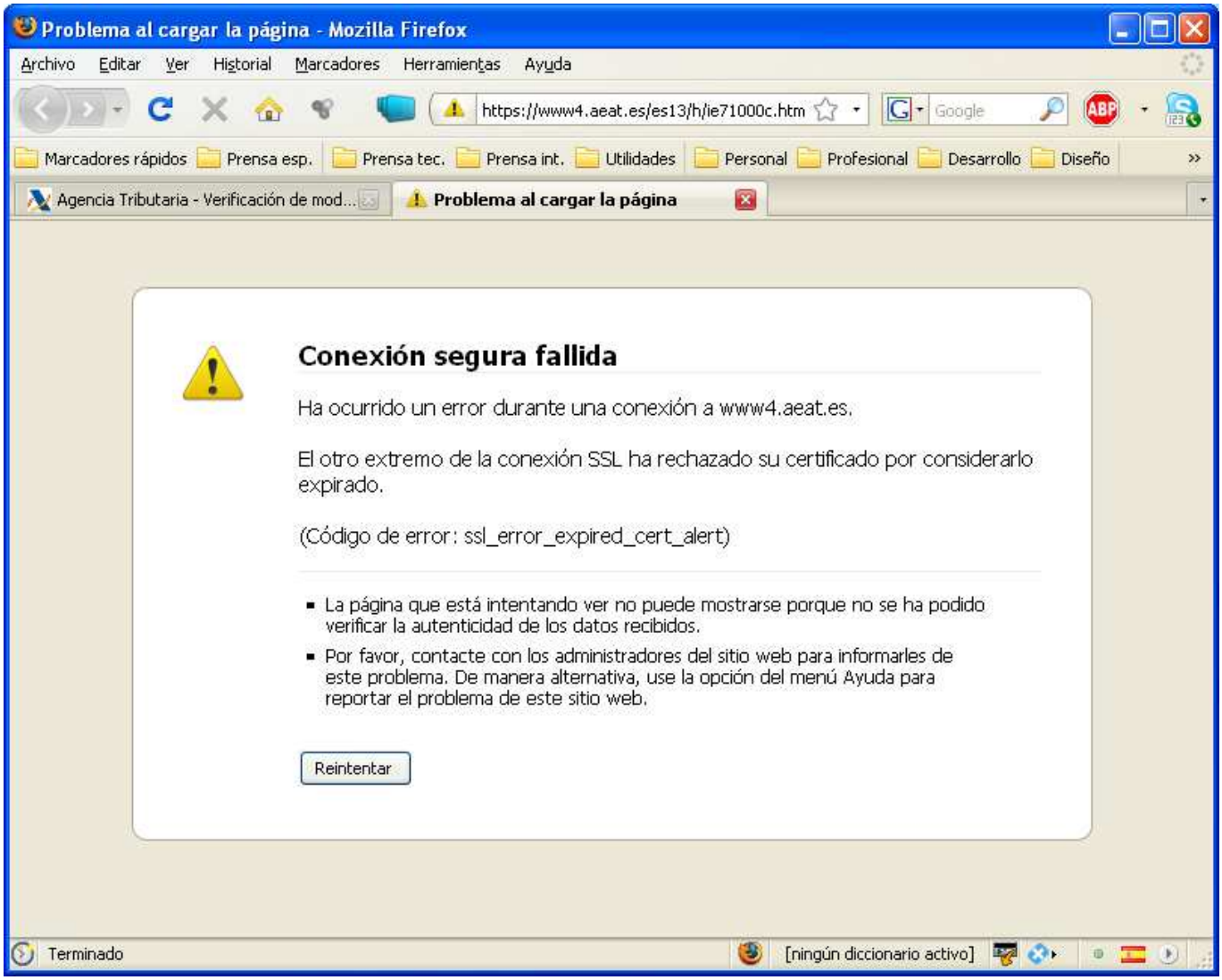


Ilustración 33 – Intento de acceso a la oficina virtual de la AEAT con un certificao caducado con Firefox. El mismo intento con Internet Explorer provocaría un comportamiento diferente: la Web reaccionaria como si el usuario no dispusiera de un certificado.

3.2.2 El sitio Web (sede electrónica) del organismo usa un certificado que nuestro Navegador no reconoce

Algunas veces puede suceder que al acceder a algún sitio Web éste 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 y lo conocido y/o 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 con tranquilidad 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 le sería completamente inservible.

Ilustración 34 – Aviso de Firefox al encontrarse con un certificado de servidor que no recnonce.

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 aconsejan no entrar en el sitio[16]. Según el fabricante, los navegadores pueden ofrecer también mecanismos específicos de tratar el problema de los sitios cuyo certificado no se reconoce.

En el caso de Firefox, por ejemplo, existe la posibilidad de dar de alta una "excepción de seguridad" que consiste en dar de alta el certificado presentado por el sitio Web en una "lista blanca" de certificados tolerados aunque se desconozca su CA.

[16] Siempre y cuando se trata de una versión razonablemente actual del navegador, las versiones muy antiguas no suelen avisar por defecto de esta situación.

En cualquier caso esta práctica entraña riesgos, puede ser tentadora por su comodidad, pero por esa misma razón puede inclinar al usuario a bajar la guardia y confiar en sitios que no son seguros. Sólo se debe emplear cuando se está 100% seguro de saber a dónde se está accediendo, y mejor aún es no usarla nunca.

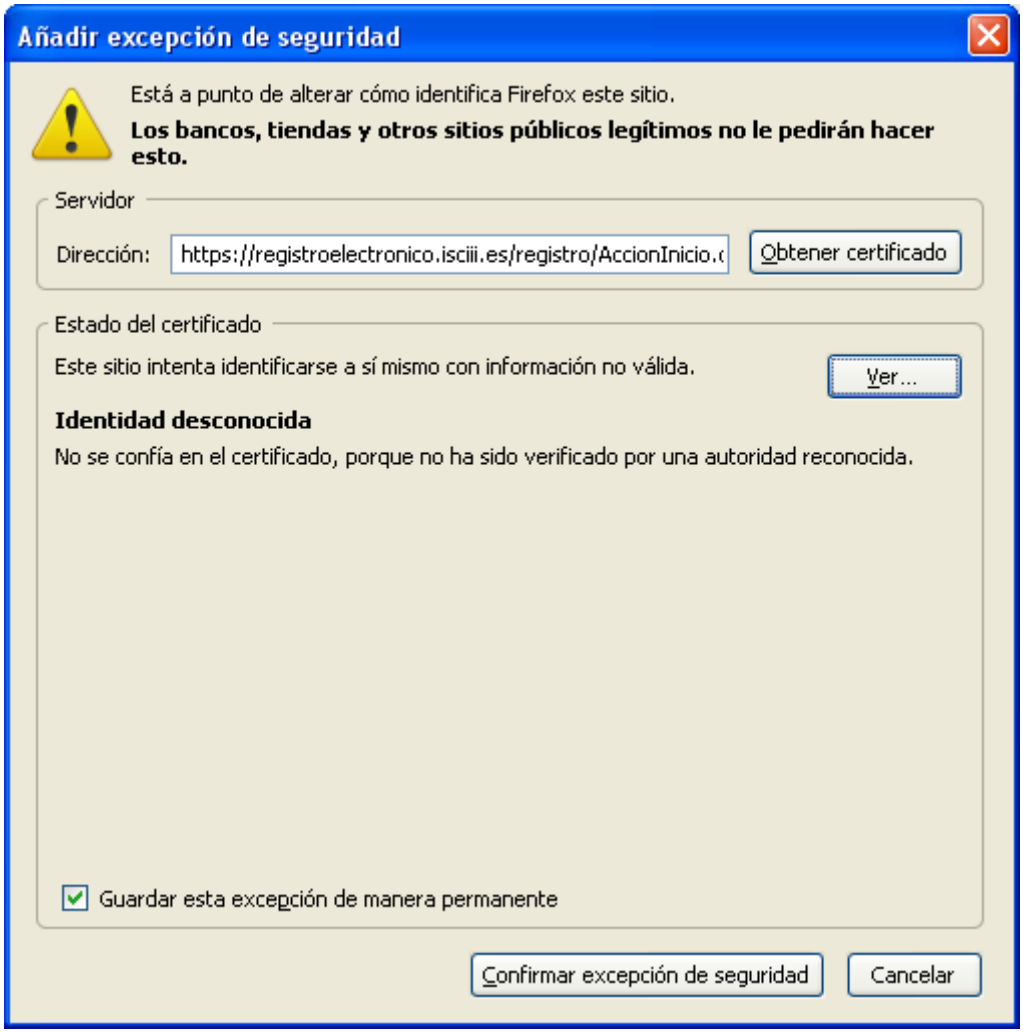


Ilustración 35 – Firefox muestra este diálogo si se hace click sobre el enlace "O añadir una excepción…" de la Ilustración 16 y se siguen los pasos para añadir una excepción. De este modo el navegador guarda el certificado del sitio al que se está accediendo para identificarlo en futuras ocasiones como certificado de confianza. Ojo, nótese que esto es distinto a incorporar el certificado raíz de la CA de ese certificado en el almacén de certificados.

Se puede concluir para estos casos que si se da el caso y se trata de un sitio en al que se prevé acceder con cierta frecuencia hacerse con su certificado en instalarlo. En general estos sitios ofrecerán sus certificados para su descarga en su Web. En cualquier caso que cerciorarse de tener la absoluta certeza de que se está accediendo al sitio que es (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.

Los mecanismos como las excepciones de seguridad de Firefox pueden ser útiles, pero hay que utilizarlos con cuidado, ya que invitan a la práctica imprudente de darlos de alta sin mayores garantías y la próxima vez el usuario (u otro usuario) percibirá al sitio como uno seguro cuando quizás no lo sea.

3.2.3 El Usuario no dispone de un certificado digital

Este caso es relativamente fácil de identificar, ya que el usuario se le mostrará el aviso pertinente. No obstante, como ya fue mencionado, puede ser que en realidad sí dispone de un certificado, pero que este haya caducado.

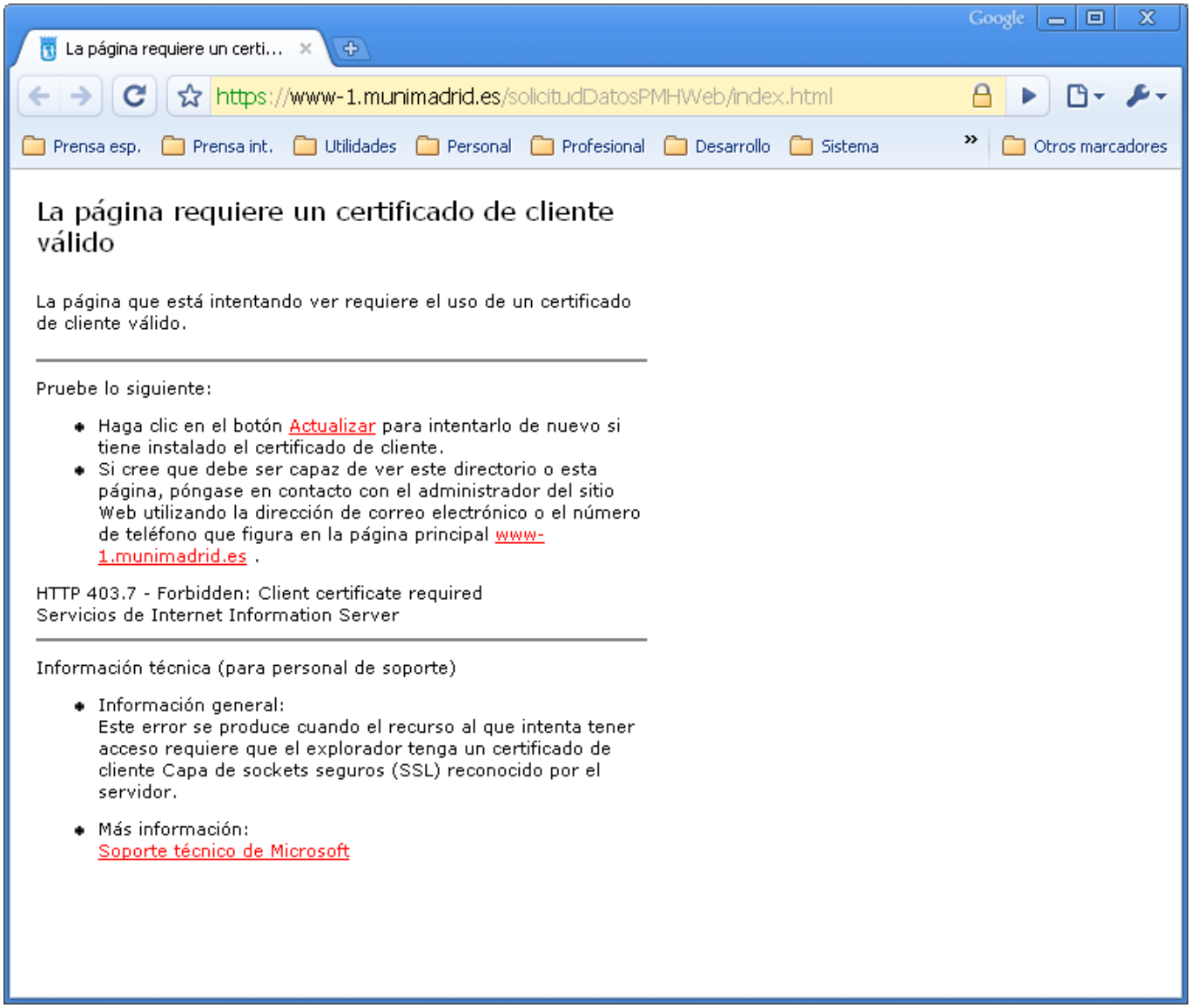


Ilustración 36 – Pantalla que muestra Google Chrome al acceder a un sitio que solicita un certificado de usuario cuando éste no dispone de ninguno.

3.2.4 Problemas con el navegador al acceder a una Web que requiera el uso de certificados

Es relativamente frecuente que el usuario experimente algún problema técnico con el navegador. Un ejemplo típico son insuficientes permisos para la descarga de un control **ActiveX** en Internet Explorer (un tipo de componente que descargan algunas Webs para realizar la firma digital en el navegador).

Las sedes electrónicas suelen ofrecer guías para la correcta configuración del navegador, en el caso de Agencia Tributaria, por ejemplo, se encuentra aquí: http://www.aeat.es/aeat/aeat.jsp?pg=ayuda/faq/es_ES

Segunda Parte: Aspectos Jurídicos

4. ELEMENTOS DE ADMINISTRACIÓN ELECTRÓNICA

Para que sea posible una Administración electrónica se necesitan una serie de de elementos tecnológicos sobre los cuales apoyar sus servicios, a veces se hace referencia a ellos como **elementos habilitantes**.

Por otra parte, el Ministerio de Administración Públicas está ofreciendo un gran número de estos elementos como **servicios horizontales** al resto de las Administraciones a través de la **red SARA**, lo cual les permitirá ofrecer más rápidamente y con menos coste servicios de Administración electrónica, especialmente en el caso de pequeños organismos con escasos recursos.

Estos elementos son en definitiva conceptos administrativos "de siempre" que se llevan al terreno de las TIC. Los ejemplos quizá más emblemáticos son la firma electrónica y los registros electrónicos. La **Ley 11/2007** ha dado una vuelta de tuerca más definiendo nuevos elementos como, por ejemplo, el expediente electrónico y la **sede electrónica**.

Los usuarios de Administración electrónica se encontrarán con estos elementos en sus relaciones con la Administración Pública, y aunque son conceptos relativamente nuevos ya forman parte de la jerga administrativa y conviene por tanto conocerlos bien.

4.1 El Documento Electrónico y la Copia Electrónica

El anexo de definiciones de la **Ley 11/2007** define el concepto de **documento electrónico**:

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

Por tanto un documento electrónico sería cualquier tipo de documento informático de los que habituales en el día a día de una oficina, ya sea un documento Word, una hoja Excel, un PDF, o incluso un documento .txt escrito con el Notepad de Windows.

El **artículo 29** hace referencia al uso de documentos electrónicos en la Administración Pública:

> ***Artículo 29. Documento administrativo electrónico.***
>
> *1. Las Administraciones Públicas podrán emitir validamente por medios electrónicos los documentos administrativos a los que se refiere el **artículo 46** de la **Ley 30/1992**, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen **una o varias firmas electrónicas** conforme a lo establecido en la Sección III del Capítulo II de la presente Ley.*
>
> *2. Los documentos administrativos incluirán **referencia temporal**, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.*
>
> *3. La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar **servicios de sellado de tiempo**.*

Por otra parte, según el **artículo 3, apartado 6** de la **Ley 59/2003, de Firma electrónica**:

> *6. El documento electrónico será soporte de:*
>
> *a) **Documentos públicos**, por estar **firmados electrónicamente** por funcionarios que tengan legalmente atribuida la facultad de dar **fe pública**, **judicial**, **notarial o administrativa**, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.*
>
> *b) **Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos** en el ejercicio de sus funciones públicas, conforme a su legislación específica.*
>
> *c) **Documentos privados**.*
>
> *7. Los documentos a que se refiere el apartado anterior tendrán el valor y la **eficacia jurídica** que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.*

Información para responsables de proyectos de Administración Electrónica

Para que un documento electrónico pueda cumplir con los requisitos de la Ley 11/2007 tiene que cumplir una serie de requisitos. Estos requisitos no se especifican como tal expresamente en la ley, pero derivan de las previsiones legales como la **conservación** de los documentos electrónicos o la **neutralidad tecnológica** y uso de **estándares**:

- El **formato** del documento debe ser **independiente del dispositivo** de manera que el documento pueda ser accedido por cualquier usuario ahora o en el futuro.
- **No debe depender de cualquier software o dispositivo** cuya evolución futura desconocemos y debe estar basado en estándares. Es fácil imaginar, por ejemplo, un recurso contencioso-administrativo, donde el documento tiene que presentarse ante el juez y éste tiene que poder acceder a él con facilidad.
- Debe ser un formato **autocontenido** de manera que toda la información necesaria para representar el contenido de documento se encuentre en el propio documento, y no sea preciso acceder a contenidos externos que quizá en el futuro no estén disponibles.
- **Autodocumentado**. Toda la información para localizar el documento, catalogarlo, etc. Esté contenida en el propio documento, y no almacenada en recursos externos.
- El **formato** del documento debe estar publicado para que en un futuro sea posible acceder a él.
- No debe tener **restricciones** como contraseñas que comprometan su acceso en el futuro.

Esto quiere decir en primer lugar que el documento electrónico no se puede implementar, por ejemplo, mediante registros en una base de datos. Es decir, un formulario de solicitud que firme un ciudadano no puede almacenarse como una estructura de tabla con los campos de los formularios almacenados en los correspondientes campos de la tabla.

En primer lugar una estructura de este tipo ya no sería susceptible de firmarse electrónicamente, pero además, al depender completamente del sistema se perdería la capacidad de utilizarlo propiamente como un documento.

Un ejemplo de referencia para posibles implementaciones que se puede citar es el nuevo **BOE Electrónico**: En este caso se usa por la facilidad para el usuario el formato **PDF/A-1ª ISO 19005-1**, diseñado expresamente para la conservación a largo plazo de documentos electrónicos. Otros formatos alternativos son **XAdES/CAdES**, aunque tienen el inconveniente de ser más difíciles de usar por los ciudadanos.

No obstante estos últimos suelen ser habituales en el archivo de documentos por parte de la Administración. Es decir, un formulario como el antes mencionado es habitual que se almacene y firme utilizando **XAdES**/**CAdES**, sin embargo de cara al ciudadano será más deseable emitir documentos en un formato **PDF/A**, por ejemplo.

La **Ley 11/2007** también prevé la posibilidad de realizar copias electrónicas de los documentos electrónicos lo no sería muy sorprendente si no fuera que lo permite además en formatos diferentes al original.

Sin embargo quizás la novedad legal más importante en relación de las copias es la posibilidad de incorporar documentos en papel digitalizados como copias auténticas, incluso llegando al extremo de poder destruir los originales en papel. Esto abre la puerta a mantener un expediente íntegramente electrónico.

> ***Artículo 30. Copias electrónicas.***
>
> *1. Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, **manteniéndose o no el formato original**, tendrán inmediatamente la consideración de **copias auténticas** con la eficacia prevista en el **artículo 46** de la **Ley 30/1992**, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico 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.*
>
> *2. 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** siempre que se cumplan los requerimientos y actuaciones previstas en el **artículo 46** de la **Ley 30/1992**, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.*

*3. Las Administraciones Públicas podrán obtener **imágenes electrónicas** de los documentos 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**.*

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

*5. Las copias realizadas en soporte papel de 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.*

Por otra parte, si el lector ha prestado atención observará que el apartado 2º consagra el concepto de **compulsa electrónica**, la cual es fundamental soportarla ya que en la práctica los procedimientos difícilmente serán 100% electrónicos puesto que en la práctica hoy por hoy será casi siempre necesario incorporar documentos emitidos originalmente en papel por terceras partes en los procedimientos electrónicos.

Un precedente muy importante a la compulsa electrónica de la Ley 11/2007 ha sido la **Orden ITC/1475/2006**, de 11 de mayo, sobre utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria, Turismo y Comercio.

Esta orden desarrolla el concepto de compulsa electrónica más a fondo que la Ley 11/2007, aunque con la limitación obvia de un ámbito legal reducido al Ministerio de Industria, Turismo y Comercio. Es de esperar que el próximo reglamento de desarrollo de la Ley 11/2007 aborde estos extremos sentando así una base común para todas las Administraciones Públicas.

A nivel europeo hay que destacar especialmente la norma **MoReq2** (**ISO 15489**). El **Mo**delo de **Req**uisitos para la gestión de documentos electrónicos de archivo incide especialmente en los requisitos funcionales de la gestión de documentos electrónicos de archivo mediante un **sistema de gestión de documentos electrónicos de archivo** (**SGDEA**). La especificación se ha concebido de forma que pueda aplicarse en todas las organizaciones públicas y privadas que deseen, y será es el modelo de referencia a seguir por las Administración de la **Unión Europea** dentro de su iniciativa **IDABC** (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens).

4.2 Archivo Electrónico (Archivo Legal)

Artículo 31. Archivo electrónico de documentos.

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

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

*3. 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**.*

El archivo electrónico de documentos es otro aspecto clave. En este caso hay que destacar especialmente una dificultad a la que el **artículo 31** no se refiere expresamente: la conservación de documentos electrónicos durante periodos de tiempo largos con todas las garantías de autenticidad e integridad.

El problema que se plantea es el siguiente: los certificados asociados a las firmas electrónicas de los documentos que garantizan su autenticidad e integridad, e identifican al firmante tienen una duración limitada en el tiempo (según la **Ley 59/2003** máximo 4 años).

¿Qué ocurre por tanto si hay que utilizar un documento de este tipo después de que el certificado del firmante haya expirado y por tanto ya no es válido?

Por otra parte, las tecnologías avanzan continuamente. Las técnicas criptográficas utilizadas actualmente se consideran 100% seguras, de hecho no se conocen casos en las cuales hayan podido ser violadas mediante ataques informáticos.

¿Pero dentro de 30 años, con una tecnología mucho más avanzada, esto seguirá igual?

Retomaremos las respuestas en el apartado de **Firma Longeva de Documentos**.

4.3 El Expediente Electrónico

El expediente electrónico es uno de los conceptos claves que introduce la **Ley 11/2007**, en el **artículo 32** define su naturaleza:

> ***Artículo 32. Expediente electrónico.***
>
> *1. El expediente electrónico es el **conjunto de documentos electrónicos** correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.*
>
> *2. El **foliado** de los expedientes electrónicos se llevará a cabo mediante un **índice electrónico**, firmado por la Administración, órgano o entidad actuante, según proceda. Este índice garantizará la **integridad** del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.*
>
> *3. 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.*

4.4 Firma Electrónica, Sello Electrónico y Sede Electrónica

Recordemos la definición del **artículo 3** de la **Ley 59/2003, de Firma Electrónica**:

> ***Artículo 3. Firma electrónica, y documentos firmados electrónicamente.***
>
> *1. 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.*
>
> *2. 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 que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su **exclusivo control**.*
>
> *3. Se considera **firma electrónica reconocida** la firma electrónica **avanzada** basada en un **certificado reconocido** y generada mediante un **dispositivo seguro de creación de firma**.*
>
> *4. 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.*
>
> *5. [...]*

El **apartado 8** del **artículo 3** (según redacción modificada por la **Ley 56/2007**) dice que:

> *8. El soporte en que se hallen los **datos firmados electrónicamente** será admisible como **prueba documental en juicio**. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una **firma electrónica avanzada** basada en un **certificado reconocido**, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un **dispositivo seguro de creación de firma electrónica**.*
>
> *La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.*
>
> *Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.*
>
> *9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.*
>
> *10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.*

Por otra parte la **Ley 11/2007** a partir de aquí introduce una serie de conceptos nuevas para el ámbito de la Administración Pública. Cabe destacar en primer lugar el concepto de **sello electrónico**, que no es otra cosa que una firma electrónica institucional. Es decir, identifica a la institución, no a un empleado público.

> ***Artículo 18. Sistemas de firma electrónica para la actuación administrativa automatizada.***
>
> *1. Para la **identificación** y la **autenticación** del ejercicio de la **competencia** en la **actuación administrativa automatizada**, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:*
>
> *a. **Sello electrónico** de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.*
>
> *b. **Código seguro de verificación** vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la **integridad** del documento mediante el acceso a la sede electrónica correspondiente.*
>
> *2. Los certificados electrónicos a los que se hace referencia en el apartado 1.a incluirán el **número de identificación fiscal** y la **denominación** correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.*
>
> *3. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.*
>
> ***Artículo 19. Firma electrónica del personal al servicio de las Administraciones Públicas.***
>
> *1. Sin perjuicio de lo previsto en los artículos 17 y 18, 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, de acuerdo con lo dispuesto en los siguientes apartados.*
>
> *2. 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.*
>
> *3. La firma electrónica basada en el **Documento Nacional de Identidad** podrá utilizarse a los efectos de este artículo.*

Finalmente conviene reseñar también la nueva posibilidad de sustituir el tradicional tablón de anuncios o edicto por la publicación en la sede electrónica.

> ***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.*

4.4.1 Comprobación de la Firma Electrónica

Como se ha visto anteriormente una firma electrónica viene avalada por un certificado del firmante y una de las comprobaciones básicas en cualquier sistema es verificar la validez de este certificado. Pero además hay que comprobar la firma electrónica en sí, es decir, que el código resumen cifrado del documento firmado coincide con lo que debería ser.

En algunos casos la herramienta asociada al formato utilizado incorpora herramientas de comprobación. Es el caso, por ejemplo, de documentos PDF. Un documento PDF firmado electrónicamente será reconocido por el lector de Adobe, el Acrobat Reader, y se podrá comprobar fácilmente la validez de la firma. Sin embargo este es un caso especial porque el propio formato PDF ya prevé mecanismos para incorporar una firma embebida y ofrece la funcionalidad de validación.

Sin embargo, en otros casos (un simple documento txt, por ejemplo) el formato no incorpora ninguna previsión para la firma y es necesario el uso de una herramienta de comprobación de firmas.

En el ámbito pública el Ministerio de Administraciones Públicas ofrece un servicio online (VALIDe) a través del cualquier los funcionarios pueden validar la firma electrónica de cualquier documento. Actualmente este servicio está limitado a los empleados pública, pero está en proyecto ampliarlo a los ciudadanos.

4.4.2 Firma Longeva de Documentos

En el apartado de **Archivo Electrónico (Archivo Legal)** ya se hizo referencia al problema que supone la limitación en el tiempo de los certificados asociados a las firmas electrónicas para el archivo y validación a largo de periodos de tiempo largos.

Existen diferentes soluciones pero la más habitual es un **sellado de tiempo**[17] periódico que no es otra cosa que una firma digital que incluye además información sobre el momento en el tiempo en el que se efectúo. De este modo con un sellado periódico de los documentos archivados y firmados se confirma y mantiene su validez acreditando que en el momento de sellado la firma fue válida. Al hacerlo periódicamente se van manteniendo estas garantías en el tiempo. Los sellos en el tiempo actuarán en definitiva como **evidencias electrónicas**.

Este mecanismo se conoce como **firma longeva** y suele ser frecuente emplear el formato **XAdES-A** (archivado) para ella.

4.5 Registro Electrónico

El Registro Electrónico es quizás el elemento de Administración Electrónica por excelencia. Permite interactuar electrónicamente con el correspondiente organismo para la presentación de escritos, solicitudes y comunicaciones relativas a los procedimientos administrativos especificados en su orden de creación y publicados en su sede electrónica.

Para utilizar el Registro Electrónico es necesario disponer de un DNI Electrónico u otro certificado digital reconocido incluido en la lista de certificados admitidos, así como cumplir con el resto de requisitos técnicos.

Dado el peso que tiene esta figura dentro de la Administración Electrónica se reproduce la **Sección I** del **Capítulo III** de la **Ley 11/2007** que los regula en su totalidad:

> ***Artículo 24. Registros electrónicos.***
>
> *1. Las Administraciones Públicas crearán **registros electrónicos** para la **recepción** y **remisión** de **solicitudes**, **escritos** y **comunicaciones**.*
>
> *2. 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.*
>
> *3. 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.*
>
> *4. En el ámbito de la Administración General del Estado se automatizarán las oficinas de registro físicas a las que se refiere el **artículo 38 de la Ley 30/1992**, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, a fin de garantizar la **interconexión** de todas sus oficinas y posibilitar el acceso por medios electrónicos a los **asientos registrales** y a las **copias electrónicas** de los documentos presentados.*
>
> ***Artículo 25. Creación y funcionamiento.***
>
> *1. Las **disposiciones de creación** de **registros electrónicos** se publicarán en el **Diario Oficial** correspondiente y su texto íntegro deberá estar disponible para consulta en la **sede electrónica** de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el **órgano o unidad responsable** de su gestión, así como la **fecha** y **hora oficial** y los días declarados como **inhábiles** a los efectos previstos en el artículo siguiente.*
>
> *2. En la sede electrónica de acceso al registro figurará la **relación actualizada** de las **solicitudes**, **escritos** y **comunicaciones** a las que se refiere el apartado 2.a) del artículo anterior que pueden presentarse en el mismo así como, en su caso, la posibilidad de presentación de solicitudes, escritos y comunicaciones a los que se refiere el apartado 2.b) de dicho artículo.*
>
> *3. 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**.*

[17] El sellado de tiempo es un servicio con un amplio abanico de aplicaciones. Es muy conveniente, por ejemplo, en transacciones comerciales o en actos públicos en los que el momento del acto es esencial. El servicio lo proporciona generalmente una tercera entidad de confianza que actúa como **autoridad de sellado de tiempo (TSA)**.

*4. Podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación, siempre que cumplan los **estándares de formato** y **requisitos de seguridad** que se determinen en los **Esquemas Nacionales de Interoperabilidad** y de **Seguridad**. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.*

Artículo 26. Cómputo de plazos.

*1. Los registros electrónicos se regirán a efectos de cómputo de los **plazos** imputables tanto a los interesados como a las Administraciones Públicas por la **fecha y hora oficial de la sede electrónica** de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su **integridad** y **figurar visible**.*

*2. Los registros electrónicos permitirán la presentación de solicitudes, escritos y comunicaciones **todos los días del año** durante las **veinticuatro horas**.*

3. A los efectos del cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.

4. El inicio del cómputo de los plazos que hayan de cumplir los órganos administrativos y entidades de derecho público vendrá determinado por la fecha y hora de presentación en el propio registro o, en el caso previsto en el apartado 2.b del artículo 24, por la fecha y hora de entrada en el registro del destinatario. En todo caso, la fecha efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el escrito, solicitud o comunicación.

5. Cada sede electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquella, los días que se considerarán inhábiles a los efectos de los apartados anteriores. En todo caso, no será de aplicación a los registros electrónicos lo dispuesto en el artículo 48.5 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

4.6 Notificaciones electrónicas

Este Servicio permite al ciudadano o a la empresa recibir todas las notificaciones procedentes de las administraciones públicas en un buzón asociado a su **Dirección Electrónica Única (DEU)**, que es una dirección electrónica especial en Correos, diferente a una cuenta de correo electrónico convencional.

La recepción de las notificaciones es confidencial y segura, enviando además al ciudadano mediante un correo electrónico habitual un aviso de recepción de notificación. El ciudadano puede elegir, para cada procedimiento, si desea ser notificado de forma electrónica.

Hay que tener en cuenta que según el **artículo 28.3** de la **Ley 11/2007** tras 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** (se hará constar en el expediente, especificándose las circunstancias del intento de notificación y se tendrá por efectuado el trámite siguiéndose el procedimiento).

Sin embargo en una notificación convencional por la vía papel ante una notificación fallida se harían intentos por otras vías alternativas (tablón de edictos del Ayuntamiento, boletines, etc.) dando lugar en la práctica a un plazo considerable más largo ante una incidencia en la notificación.

4.7 Pago Electrónico

La pasarela de pagos (MAP-AEAT) 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.

La manera de realizar el pago es algo particular; permite pagar a través de cargo en cuenta o tarjeta del ciudadano, devolviendo el resultado de la operación. Si todo ha ido correctamente, se recibe el Número de Referencia Completo (NRC) ó identificador electrónico del pago.

Ese NRC se indicará normalmente en el trámite que implica el pago, es decir, será un campo a rellenar en la correspondiente solicitud que luego se firma y envía.

4.8 La Factura Electrónica

La facturación electrónica es un equivalente funcional de la factura en papel y consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos.

Existen tres condicionantes principales para la realización de e-Factura:

- Se necesita un formato electrónico de factura de mayor o menor complejidad (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros)
- Es necesario una transmisión telemática (tiene que partir de un ordenador, y ser recogida por otro ordenador).
- Este formato electrónico y transmisión telemática, deben garantizar su integridad y autenticidad a través de una firma electrónica reconocida.

Para homogenizar estos aspectos técnicos se ha desarrollado la **Orden PRE/2971/2007**, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares.

En esta orden se crea el formato de factura electrónica **facturae**, junto con la previsión de compatibilidad en futuras con normas como UBL (Universal Business Language).

Facturae define fundamentalmente las tecnologías de firma a utilizar en las facturas y una estructura en XML que éstas deben cumplir.

Por otra parte hay que destacar también las previsiones que hacen la **Ley 56/2007** de Medidas de Impulso de la Sociedad de la Información y **Ley 30/2007** de Contratos del Sector Público.

En el caso de la primera se pueden destacar los siguientes puntos:

- Obligatoriedad para sector público en los términos establecidos en Ley de Contratos.
- Plan de generalización de la factura-e en el plazo máximo de 9 meses … promoviendo la interoperabilidad.
- Normas sobre formatos estructurados y no restrictivos por el Mityc y el Meh en 6 meses, de acuerdo con organizaciones de estandarización globales. Esto se ha traducido en el formato **facturae**.
- Adaptación a lenguas oficiales.
- Aplicación al tratamiento y conservación de los datos necesarios para la facturación electrónica lo dispuesto en la LOPD.

Hay que destacar además especialmente las medidas en relación con las empresas que presten servicios al público en general de especial trascendencia económica[18]:

- Obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica. Afecta a comunicaciones electrónicas, banca, seguros, agua, gas, electricidad, agencias de viaje, transporte viajeros, comercio al por menor.
- Consulta del historial de facturación.

De la **Ley 30/2007** hay que destacar especialmente los siguientes aspectos:

[18] Es decir, banca, suministro de agua, gas, electricidad, transportes, etc.

- Se autoriza al Ministro de Economía y Hacienda para aprobar, previo dictamen del Consejo de Estado, las normas de desarrollo de la disposición adicional decimonovena que puedan ser necesarias para hacer plenamente efectivo el uso de medios electrónicos, informáticos o telemáticos en los procedimientos regulados en esta Ley.
- En el plazo máximo de un año desde la entrada en vigor de la Ley, el Ministro de Economía y Hacienda aprobará las normas de desarrollo necesarias para hacer posible el uso de las facturas electrónicas en los contratos que se celebren por las entidades del sector público Estatal.
- Transcurridos tres meses desde la entrada en vigor de las normas a que se refiere el apartado anterior la presentación de facturas electrónicas será obligatoria en la contratación con el sector público estatal para las sociedades que no puedan presentar cuenta de pérdidas y ganancias abreviada.
- Por Orden conjunta de los Ministros de Economía y Hacienda y de Industria, Turismo y Comercio, se extenderá progresivamente la obligatoriedad del uso de las facturas electrónicas para otras personas físicas y jurídicas en función de sus características y el volumen de su cifra de negocios. En todo caso, transcurridos dieciocho meses desde la entrada en vigor de las normas a que se refiere el apartado anterior, el uso de la factura electrónica será obligatorio en todos los contratos del sector público estatal.
- El Consejo de Ministros, a propuesta de los Ministros de Economía y Hacienda y de Industria, Turismo y Comercio, adoptará las medidas necesarias para facilitar la emisión de facturas electrónicas por las personas y entidades que contraten con el sector público estatal, garantizando la gratuidad de los servicios de apoyo que se establezcan para determinadas empresas.

TERCERA PARTE: PERSPECTIVAS DE LA ADMINISTRACIÓN ELECTRÓNICA

5. LOS SERVICIOS HORIZONTALES E INSTITUCIONES DE ADMINISTRACIÓN ELECTRÓNICA

5.1 El Portal del Ciudadano 060

La **Red 060** es una iniciativa del Ministerio de Administraciones Públicas (MAP) 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.

5.1.1 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.

5.1.2 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.
- 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.

5.1.3 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.

5.2 El Portal del DNIe

En España el DNIe se expide desde marzo del año 2006. El nacimiento del DNI electrónico responde a la necesidad de otorgar identidad personal a los ciudadanos para su uso en la nueva Sociedad de la Información, en particular en sus relaciones con las Administraciones Públicas, además de servir de impulsor de la misma.

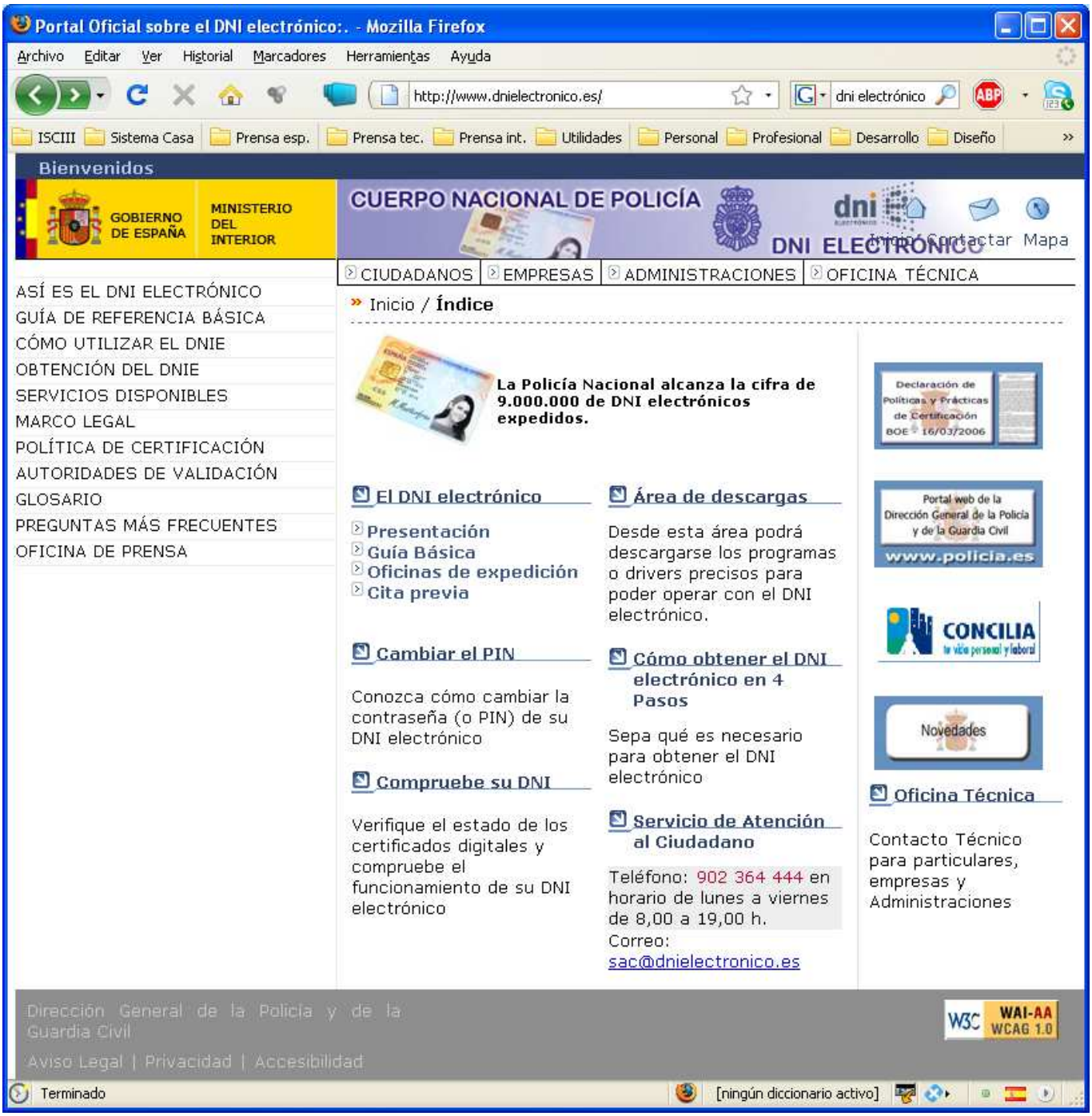


Ilustración 37 – Portal del DNI electrónico.

De hecho se espera que el DNIe sea el elemento clave para conseguir un acceso uso masivo de los servicios electrónicos de la Administración, una como efecto arrastre una mayor inmersión de los usuarios y las empresas en los servicios de la sociedad de la información.

Ese valor estratégico que se otorga al DNIe dentro de las políticas públicas actuales se ha visto reflejado, entre otras cosas, en la creación de un portal que aglutina toda la información relevante, herramientas y diversos documentos y guías para facilitar a los ciudadanos su uso. El portal se encuentra en: http://www.dnielectronico.es/

5.3 La Fábrica Nacional de Moneda y Timbre

Actualmente la FNMT es uno de los protagonistas más importantes en la Administración Electrónica.

Ilustración 38 – Página principal de la FNMT.

A pesar de que en España ya existen decenas de prestadores de servicios de servicios de certificación, el liderato de la Fabrica Nacional de Moneda y Timbre es tal que se puede considerar casi un monopolio de facto en la expedición de certificados electrónicos, si dejamos al margen el caso particular del DNIe. Esto se debe fundamentalmente al tiempo que lleva prestando el servicio y la expedición gratuita de certificados para personas físicas.

5.4 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 si y 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.

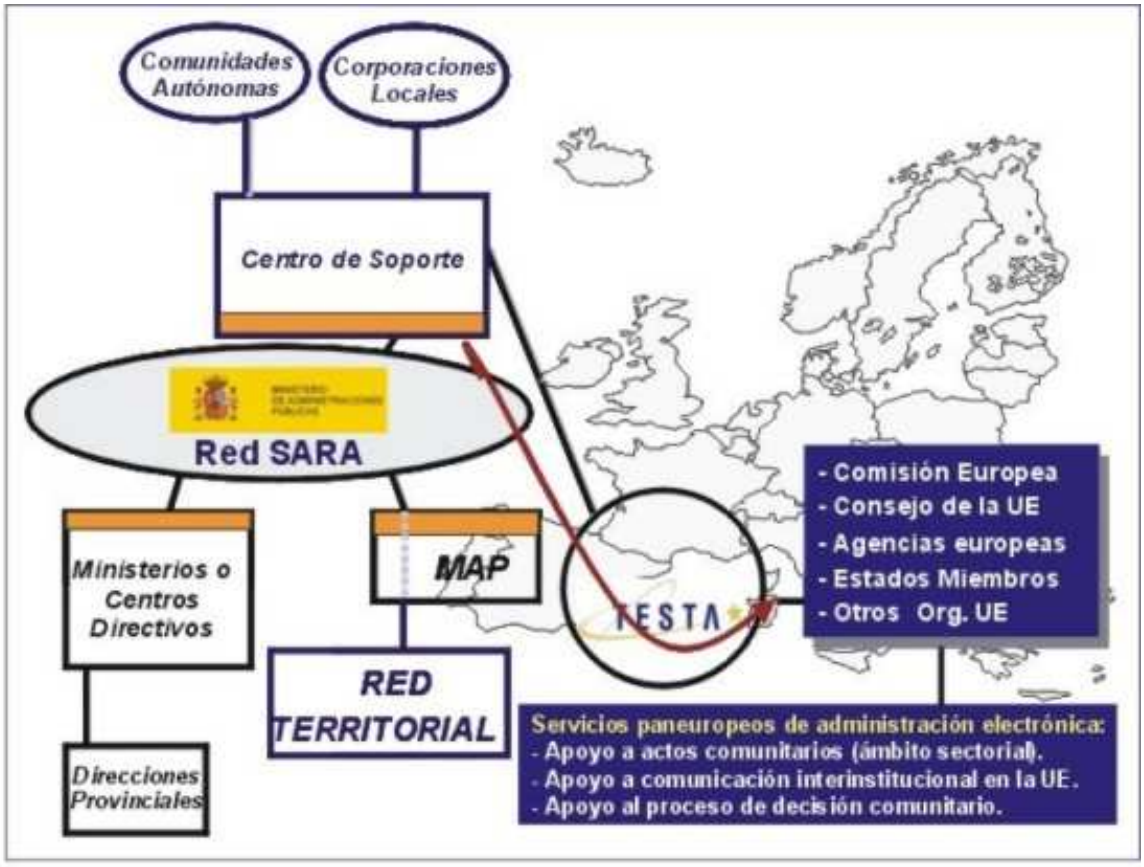


Ilustración 39 – Estructura de la red SARA.

Por otra parte se pretende facilitar con es 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 **sTESTA** 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.

5.5 El Consejo Superior de Administración Electrónica

El Consejo Superior de Administración Electrónica es el órgano colegiado adscrito al Ministerio de Administraciones Públicas, 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 creados 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. INTERNET E INNOVACIÓN EN LA ADMINISTRACIÓN PÚBLICA

La Administración Electrónica, aunque se suele asociar principalmente 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.

Resulta especialmente interesante 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.

6.1 El Concepto de Web 2.0

El término, **Web 2.0** fue acuñado por **Tim O'Reilly**[19] en **2004** 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** o las **folcsonomías**, que fomentan la colaboración y el intercambio ágil de información entre los usuarios.

Los propulsores 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 y una sofisticada organización avala la calidad de los mismos evitando actos de vandalismo y que la información sea lo suficientemente 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 consigue a su vez que actos aislados malintencionados no lleguen a prosperar.

Muchos de los contenidos de este documento han sido tomados de la Wikipedia aprovechando que se encuentran bajo la **Licencia de documentación libre de GNU**[20] que permite su libre copia y redistribución. Por otra parte la redacción de este documento ha servido para realimentar estos artículos ampliándolos a su vez con el material elaborado por el autor sobre estas materias. De hecho muchas veces la dinámica ha sido mejorar/ampliar el artículo original de la Wikipedia y una vez terminado este trabajo copiar los contenidos en este documento, de modo que la ampliación de los contenidos de la Wikipedia no ha supuesto prácticamente ningún esfuerzo adicional.

Se ha creado en definitiva una dinámica en la que tanto este documento como la Wikipedia han salido beneficiados, lo que constituye un buen ejemplo de los beneficios de la filosofía Web 2.0

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**[21] y actualmente no pocas voces sostienen que ésta incluso ha sido superada por la Wikipedia[22], aparte de que la supera ampliamente en cantidad y detalle de artículos (En enero del 2009 la Wikipedia en inglés contiene 2.700.000 artículos frente a 500.000 de temas en la Enciclopedia Británica).

[19] Fundador de O'Reilly Media, una compañía muy popular por sus libros y publicaciones en torno al mundo del software open source.

[20] Términos de la licencia: http://www.gnu.org/copyleft/fdl.html

[21] Fuente: http://www.nature.com/nature/journal/v438/n7070/full/438900a.html

[22] Fuente: http://www.enriquedans.com/2007/07/wikipedia-mas-fiable-que-la-encyclopædia-britannica.html

Práctica: editar un artículo en la Wikipedia

El ejercicio propuesto consiste en que en grupo se escoja uno a varios artículos de la Wikipedia en español sobre materias en las que tengan interés y conocimiento. Seria deseable que las materias escogidas versen sobre temas relacionados con la Administración Pública. También es válido, incluso preferible, crear artículos nuevos.

A continuación los alumnos deberán darse de alta en la Wikipedia como usuario, y a partir de ahí editar alguna parte de los artículos escogidos con el fin de mejorarla.

Hay que destacar que esto es una práctica real, es decir, una contribución real a la Wikipedia.

6.2 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 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. Para dar una orientación más concreta sobre el significado de este concepto se reproduce un fragmento del artículo de blog en http://vozyvoto.es/2007/12/11/los-rasgos-de-la-administracion-20/:

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**.

6.3 Blogs

En los últimos años se ha forjado poco a poco una importante **blogosfera** en el ámbito de la Administración Pública, con muchas decenas de blogs, tanto generalistas como especializados en determinados ámbitos. En el Anexo de este libro se listan algunos a modo de ejemplo y un directorio blogs, **K-Government**, a través del cual se pueden localizar fácilmente los blogs más relevantes.

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.

Ilustración 40 – Entrada del blog del sitio de Barack Obama en el que Obama presenta una carta de agradecimiento a todos aquellos que lo apoyaron en la presentación de su presupuesto a las cámaras.

En definitiva ofrece una fuente de información única para los empleados públicos y afines que les conecta de una manera mucho más activa en la vida de 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. Esperemos por tanto que a medio plazo se puedan convertir también en una fuente de información valiosa para el público en general y fomentar en los medios unos debates sobre la Administración y la Función pública más cualificados de los que se publican actualmente.

Las características quizás más diferenciadoras de estos blogs frente a los medios tradicionales de difusión (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.

6.3.1 Blogs y Política

Aunque supone desviarse algo del ámbito de este libro, 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 Diez** en el caso de España. En el caso de Obama, aparte de ser un reconocido "fan" de las nuevas tecnologías, ha encontrado un canal adicional a través del cual reforzar de manera muy eficaz su campaña y hacerla más atractiva para determinados segmentos de público.

En el caso de Rosa Diez quizás haya que destacar más que la Web fue un canal alternativo a las campañas tradicionales que ha permito al partido articular y difundir una campaña con una inversión muy reducida que llegó a un número de personas que con las limitaciones económicas propias de un partido joven seguramente no se podría haber conseguido ni de lejos por las vías tradicionales.

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. Por otra parte, permite al ciudadano conocer mejor el pensamiento del político en cuestión y decidir con mayor criterio si se sienten identificados con él o no.

Actualmente ya existe un buen número de blogs de este tipo, con diferentes grados de actividad. Es fácil localizarlos vía buscadores como Google, una lista que puede servir como referencia se puede encontrar aquí: http://www.alianzo.com/es/top-blogs/country/spain/politicos

Por su carácter 2.0 estos blogs son una vertiente más de conceptos como **e-Participación** o **e-Democracia** que poco a poco se están forjando gracias a las nuevas tecnologías y prometen en general mejoras de la calidad de los sistemas democráticos, más democracia en definitiva. ¿Cuándo ciudadanos a pie han podido discutir de tu a tu cuestiones económicas, políticas o sociales con políticos de primer nivel?

Hay muchos ejemplos, uno reciente que permite ver este fenómeno es el artículo de **Jordi Sevilla** titulado *"El problema no son los políticos"*, http://blog.jordisevilla.org/2009-03-31/el-problema-no-son-los-politicos/, que en el momento de la redacción de este libro ya había suscitado más de 30 respuestas de los Internautas.

Ilustración 41 – Blog de Jordi Sevilla.

6.3.2 Herramientas para la creación de un Blog

Las herramientas se clasifican, principalmente, en dos tipos: aquellas que ofrecen una solución completa de alojamiento, gratuita (como **Freewebs**, **Blogger** y **LiveJournal**), y aquellas soluciones consistentes en software que, al ser instalado en un sitio Web, permiten crear, editar y administrar un blog directamente en el servidor que aloja el sitio (como es el caso de **WordPress** o de **Movable Type**).

Este software es una variante de las herramientas llamadas **Sistemas de Gestión de Contenido** (**CMS**), y muchos son gratuitos. La mezcla de los dos tipos es la solución planteada por la versión multiusuario de WordPress (**WordPress MU**) a partir de la cual se pueden crear plataformas como **Rebuscando.INFO**, **Wordpress.com** o **CiberBlog.es** o ***Blog total**.

En el Anexo se encuentra un listado de diversas herramientas.

6.4 Wikis

El término "Wiki" procede del Hawaiano y significa "rápido" y eso es exactamente lo que caracteriza a las Wikis: ser un medio rápido 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**. 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 relativamente poco control 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[23].

6.4.1 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, los valores y 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.

[23] La clave está en el hecho de que son muchísimos menos los usuarios mal-intencionados, de modo que si se produce un ataque de vandalismo, éste es detectado y eliminado rápidamente por los demás usuarios. No obstante, se han dado casos que aún a pesar de tener una corta duración han conseguido hacer daños, como ha ocurrido con determinados casos de difamación personal de algunos personajes públicos. Este tipo de casos han suscitado debates sobre si se debe mantener o no el carácter tan abierto de la colaboración en la Wikipedia, por el momento, se mantiene.

En ese sentido el uso de las Wiki 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.

6.4.2 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**, http://www.wikanda.es, una Wiki especializada en todo que gira en torno a esta Comunidad autónoma o la **Madripedia**, http://www.madripedia.es, promovida por el **Ayuntamiento de Madrid**. Otro ejemplo es el portal **e-Catalunya**, http://ecatalunya.gencat.net, una iniciativa de la **Generalitat de Cataluña** para impulsar la sociedad del conocimiento en esta Comunidad.

De todos modos quizás la referencia en cuanto a Wikis accesibles al público más importante aún sea la propia Wikipedia que ya 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 el la documentación de procedimientos de trabajo o la documentación, manuales, howto's, etc. de las aplicaciones corporativas.

6.4.3 Herramientas para la creación de Wikis

Una ventaja más de las Wikis es el hecho de que las principales herramientas de Wikis son gratuitas y de código abierto para su implementación, de modo que la puesta marcha de una herramienta de este tipo no presenta prácticamente barreras de entrada como lo puede ser el pago de licencias, etc. Por otra parte son sencillas de instalar y utilizan tecnologías y productos ampliamente difundidos como PHP, Java, MySQL o Postgresql.

Quizás la referencia más popular sea la herramienta **MediaWiki**. MediaWiki es un motor para wikis bajo licencia **GNU**, programado en **PHP**. A pesar de haber sido creado y desarrollado para Wikipedia y los otros proyectos de la fundación Wikimedia, ha tenido una gran expansión a partir de 2005, existiendo gran número de wikis basados en este software que nada tienen que ver con dicha fundación. La mayoría de ellos se dedican a la documentación de software o a temas especializados. Puede ser instalado sobre servidores Web Apache o IIS y puede usar como motor de base de datos MySQL o PostgreSQL.

En el Anexo se listan varias herramientas de Wiki.

6.5 Redes Sociales

Las **redes sociales** en Internet son en este momento probablemente en fenómeno Web 2.0 que con más fuerza se está desarrollando y el más generalista y popular. Una red social es una estructura social 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, relaciones sexuales, 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 **200 millones** de usuarios en la actualidad según sus propias estadísticas. Muchas Universidades norteamericanas han declarado que 2008 será el último año en que publiquen sus anuarios de estudiantes, un clásico en estas instituciones, puesto que las redes sociales han jubilado a los mismos.

En España la primera red social es actualmente **Tuenti**, puesta en marcha a finales del 2006, con una cifra de usuario que según la fuente oscila entre 3,5 y 5 millones de usuarios en marzo del 2009.

Estos dos ejemplos anteriores se orientan 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. ¿Qué agenda tradicional puede competir con esto?

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 por ejemplo, formular consultas a otros profesionales, difundir presentaciones profesionales, realizar sondeos de opinión, recavar 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.

6.5.1 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 ya sean 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.

Las redes sociales son por tanto un complemento muy interesante a los directorios de profesionales, tales como el portal **Funciona** de la Administración General del Estado que proporcionan una información que por su naturaleza no se pueden realizar con aplicaciones intra-organizativas como lo es Funciona.

6.5.2 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.

Tradicionalmente, los candidatos a la presidencia de Estados Unidos han obtenido fondos para sus campañas a través de corporaciones y donaciones particulares, que tienen un límite de 2.000 dólares. El primer candidato que recurrió a las donaciones a través de Internet fue Howard Dean, que en el año 2004 obtuvo 27 millones de dólares a través de este canal.

Es de sobra conocida la dura batalla que se ha presentado en las primarias del Partido Demócrata entre Obama y **Hillary Clinton**. Ésta, poseedora de más experiencia y mejores contactos, se había asegurado para su bando las grandes donaciones a su partido en el momento en que Obama entró en la disputa preelectoral.

Ante esta desventaja inicial, Obama se vio en la necesidad de encontrar un modo alternativo de recaudar fondos para su bando. Contrató a **Cris Hughes**, uno de los dos fundadores de Facebook, para que dirigiera su campaña online. Ésta se ha basado en la interacción y la participación de los usuarios, a través de enlaces, blogs, vídeos, recomendaciones, grupos, etc.

Ilustración 42 – Página para la comunicación de noticias sobre el PlanE en Twitter.

Finalmente, Obama ha conseguido **264 millones** de dólares en donaciones, frente a los **88,2 millones** del que será su rival, el republicano McCain. Obama es incluso el primer candidato que rechaza fondos públicos para financiar su campaña. Cabe destacar que casi la mitad de esa cantidad se ha recaudado con donaciones inferiores a 200 dólares, lo cual demuestra la mucha gente que ha sido movilizada.

Aunque sin llegar a estos extremos en España el uso de redes sociales en política también empieza a prosperar, algunos ejemplos son el caso de **Patxi López** o **Rosa Diez** con cuentas en **Facebook**, **Tuenti** y **Twitter** en las elecciones autonómicas del 2009.

Una variante curiosa del uso de las redes sociales es la página[24] en Twitter creada la comunicación de las medidas del **PlanE**[25] del Gobierno a los usuarios de esta red. De este modo no es necesario que los usuarias 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.

6.6 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 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**[26] 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", por un valor muy superior al presupuesto para publicidad de la compañía anunciante.

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.

Algunos afirman que el término marketing viral fue acuñado originalmente por el capitalista de **riesgo Steve Jurvetson** en 1997 para describir la práctica de varios servicios libres de correo electrónico (como Hotmail) de añadir su propia publicidad al correo saliente de sus usuarios; aunque el primero en escribir sobre este tipo de marketing viral fue el crítico **Douglas Rushkoff** en 1994 en su libro *"Media Virus"*. La hipótesis es que si esa publicidad llega a un usuario "sensible" (es decir, interesado en el producto ofrecido por Hotmail, el correo gratuito), ese usuario "se infectará" (es decir, se dará de alta con una cuenta propia) 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.

[24] http://twitter.com/medidas

[25] http://www.plane.gob.es/

[26] Astroturfing es un 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. Es objetivo es crear la impresión de una manifestación pública e independiente sobre políticos, grupos políticos, productos, servicios, eventos, etc. Los astroturfers intentan orquestar para ello acciones protagonizadas por individuos aparentemente diversos y geográficamente distribuidos, tanto a través de actuaciones explícitas como más subliminales e incluso ocultas.

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: impulsa a los usuarios de un producto servicio específico a contárselo a sus amigos. Esa es una recomendación "boca a boca" positiva.

6.6.1 Aplicaciones y Ventajas de Marketing Viral en la Administración Pública

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 a través de los nuevos servicios electrónicos está cambiando radicalmente y para mejor 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 dónde 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 será 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 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 menos 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 vimos su 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 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 enviar un crear un video 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 aquí: http://obamain30seconds.org/

Por otra parte el diseño de la Web personal de Obama, http://www.barackobama.com, 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:

- 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

En España, uno de los pocos ejemplos de marketing viral en el sector público, es la iniciativa desarrollada por el Ayuntamiento de Burgos, concretamente el área de Juventud, que ha utilizado técnicas de marketing viral como acción de captación de nuevos teléfonos de jóvenes a los que enviar información de las actividades organizadas por la concejalía.

En la **Ilustración 43** se puede ver el mensaje utilizado por el Ayuntamiento con el que anima a los jóvenes a que reenvíen este mensaje a sus amigos. En el mensaje se menciona el procedimiento para que estos últimos se incorporen al sistema de información municipal.

Ilustración 43 – Mensaje SMS difundido en una acción de marketing viral en el ayuntamiento de Burgos[27].

Es un ejemplo como se ha utilizado un medio muy afín (el móvil) al público objetivo (jóvenes menores de 30 años) para crear una campaña que por medios tradicionales seguramente habría sido mucho menos eficaz y más cara.

[27] Fuente: http://movilaapp.blogspot.com/2007/08/marketing-viral-en-el-ayuntamiento-de.html?showComment=1187590380000

6.7 Crowdsourcing

Tras el término de **crowdsourcing**, acuñado por el escritor **Jeff Howe** y el editor **Mark Robinson** de la revista tecnológica **Wired** se encuentra la sencilla idea de sustituir el trabajo de grupos profesionales especializados mediante la participación masiva de voluntarios y la aplicación de principios de autoorganización.

Aunque ésta no es una idea nueva, se está volviendo bastante popular y ha sido aplicada por empresas como **Boeing**, **Dupont** o **Procter & Gamble**, que buscan solucionar sus problemas de forma masiva a través de iniciativas como por ejemplo **InnoCentive**[28].

La idea es otro ejemplo de nuevos modelos de negocio que nacen a raíz de los principios de la Web 2.0. La importancia del crowdsourcing radica en definitiva en que con este modelo colaborativo es posible que una gran cantidad de participantes entusiastas puedan realizar el trabajo de un grupo de profesionales experimentados.

Un ejemplo de la vida política española fue la campaña del Partido Popular en las elecciones generales del 2008: El candidato del PP vio las ventajas del crowdsourcing y en su Web *Hola, soy Mariano Rajoy* pedía voluntarios para diseñar sus vídeos electorales.

Lo que destaca de esta iniciativa del Partido Popular es la puesta en escena[29]: se muestra una reunión de maitines de la cúpula del partido donde va llegando Mariano Rajoy, Ana Pastor, Gabriel Elorriaga, Pío García Escudero, Jorge Moragas y Sandra Moneo. Finalmente, Elorriaga dice que falta alguien, y en ese momento Rajoy dice que lo va a llamar. Lo que sucede es que Rajoy llama al teléfono de la persona que se ha metido en la web, que recibe el siguiente mensaje: *"Hola, soy Mariano Rajoy, ¿dónde te has metido? Te estamos esperando, pero si no puedes llegar, yo lo que te pido es que nos mandes tus ideas a mi página web. Un saludo y un fuerte abrazo"*.

[28] InnoCentive, fundada por la farmaceutica Lilly, es una compañía de "innovación abierta" que acepta como encargos la resolución de problemas de I+D en un amplio abanico de campos como ingeniería, TIC, modelos de negocio, matemáticas, química, etc. A partir de ahí los problemas se publican como "desafíos" para que sean solucionados por voluntarios que se ofrezcan para ello. A aquellos que aporten la mejor solución para el problema se les da un premio que oscila típicamente entre 10.000 y 100.000 dolares.

[29] El vídeo se puede ver aquí: http://www.youtube.com/v/bTW_G2En0U8&rel=1

ANEXO

1. SITIOS DE REFERENCIA

1.1 Sobre Seguridad

- **Inteco**: http://www.inteco.es
- **Kriptópolis**: http://www.kriptopolis.org
- **Hispasec**: http://www.hispasec.com/
- **Red.es / Red Iris**: http://www.red.es

1.2 Información sobre Criptografía

- **Advanced Encryption Standard (AES)**: http://es.wikipedia.org/wiki/AES
- **XML Advanced Electronic Signature (XAdES)**: http://es.wikipedia.org/wiki/Xades

1.3 Relativos a Administración Electrónica

- **Portal 060**: http://www.060.es/
- **Portal del DNI electrónico**: http://www.dnielectronico.es/
- **Portal Factura-e**: http://www.facturae.es/
- **Moreq2**: http://www.moreq2.eu/

1.4 Blogosfera sobre la Administración Pública en general y Administración Electrónica

- **K-Government, Agregador de Blogs sobre Administración Pública**: http://www.k-government.com/2008/02/07/los_blogs_de_la_blogosfera_pblica_espaola/
- **Sociedad Conectada. Voz y Voto. Reflexiones sobre Tecnología, Sociedad y Administración Pública**: http://vozyvoto.es/
- **I-public@. Reflexiones sobre administración pública inteligente**: http://i-publica.blogspot.com/
- **Administraciones en Red**: http://eadminblog.net/
- **eFuncionario**: http://efuncionario.com/
- **Sociedad en Red**: http://www.sociedadenred.info/
- **Openpropolis:** http://www.openpropolis.com/

1.5 Utilidades de Criptografía

Utilidad	Descripción y URL
TrueCrypt	Aplicación para la creación de unidades virtuales cifradas. Aparte de la capacidad de crear unidades virtuales como si fueran discos físicos destacan especialmente las funcionalidades orientadas para impedir que el usuario pueda ser extorsionado: http://es.wikipedia.org/wiki/TrueCrypt
AxCrypt	Utilidad para el cifrado de ficheros: http://www.axantum.com/AXCRYPT/
KeePass	Utilidad para almacenar claves de acceso y otra información sensible de un modo sencillo. Dispone además de complementos como la integración con el navegador Web, etc. : http://keepass.info/
Validador de firmas	Validador de firmas online: http://www.signaturevalidator.com/
Aplicación de firma electrónica	Una aplicación en Java que permite firmar cualquier documento electrónicamente. Es necesario un registro previo, pero la aplicación es gratuita: https://www.inteco.es/Seguridad/DNI_Electronico/Firma_Electronica_de_Documentos/

2. HERRAMIENTAS

2.1 Blogs

Utilidad	Descripción y URL
Blogger	Servicio de **Google** para crear y publicar un blog de manera fácil. El usuario no tiene que escribir ningún código o instalar programas de servidor o de scripting. Blogger acepta para el hosting de los blogs su propio servidor (Blogspot) o el servidor que el usuario especifique (FTP o SFTP): http://www.blogger.com
Wordpress	WordPress fue creado a partir del desaparecido b2/cafelog y se ha convertido junto a Movable Type en el CMS más popular de la blogosfera. Las causas de su enorme crecimiento son, entre otras, su licencia, su facilidad de uso y sus características como gestor de contenidos. Otro motivo a considerar sobre su éxito y extensión, es la enorme comunidad de desarrolladores y diseñadores, que se encargan de desarrollarlo en general o crear plugins y themes para la comunidad (que ascendían a 2524 y 1320 respectivamente en julio de 2008). Servicio de posting de blogs Wordpress.com: http://wordpress.com/ Descarga de la herramienta para posting propio: http://wordpress.org/
Más...	Listado de software para blogs: http://en.wikipedia.org/wiki/Weblog_software

2.2 Wikis

Utilidad	Descripción y URL
MediaWiki	MediaWiki es un motor para wikis bajo licencia GNU, programado en PHP. A pesar de haber sido creado y desarrollado para Wikipedia y los otros proyectos de la fundación Wikimedia, ha tenido una gran expansión a partir de 2005, existiendo gran número de wikis basados en este software que nada tienen que ver con dicha fundación. La mayoría de ellos se dedican a la documentación de software o a temas especializados. http://www.mediawiki.org/wiki/MediaWiki/es
Más...	Listado de software para Wikis: http://es.wikipedia.org/wiki/Software_para_wikis

3. LIBROS

Libro	Descripción y URL
Wikinomics	**Wikinomics: How Mass Collaboration Changes Everything** (ISBN 1591841933) es un libro escrito por Don Tapscott y Anthony D. Williams publicado por primera vez en diciembre del 2006. Explorar como algunas compañías en el siglo 21 han utilizado la "colaboración masiva" y la tecnología open-source tal como las Wikis para su éxito.

	El libro describe el cambio que está provocando la **Wikinomia** (una nueva economía donde se aplican los conceptos descritos en el libro), donde los consumidores llegan a ser **prosumidores**, puesto que no sólo consumen los servicios, sino que también los producen. http://wikinomics.com/book/
The Long Tail	La larga estela o larga cola (en el original en inglés The Long Tail) fue una expresión acuñada por Chris Anderson en un artículo de la revista Wired de Octubre de 2004 para describir determinados tipos de negocios y modelos económicos tales como Amazon.com o Netflix. Lo hizo a partir de un texto publicado por Clay Shirky, uno de sus redactores. El término larga cola se utiliza normalmente en estadística en relación con distribuciones de riqueza o con el uso del vocabulario. Internet y el entorno digital han cambiado las leyes de distribución y las reglas del mercado. La reducción en el coste de almacenamiento y distribución que permiten las nuevas tecnologías, hace que no sea ya necesario focalizar el negocio en unos pocos productos de éxito, en los superventas. Hay que darse cuenta de que ahora existen dos mercados: uno centrado en el alto rendimiento de pocos productos y otro, nuevo y todavía no familiar, basado en la suma o acumulación de todas las pequeñas ventas de muchos productos, que puede igualar o superar al primero. Son el antiguo mercado de masas y el nuevo nicho de mercados, representados por la cabeza y la cola de la conocida gráfica de distribución estadística. Este concepto se aplica también muy bien a la naturaleza de la Web 2.0, los blogs, Wikis, etc. La Web 2.0 se trata de conectar personas, no ordenadores, como también escribió Kevin Kelly en un famoso artículo en la revista Wired: We are the machine. Las redes sociales por supuesto no son sólo blogs, también recogen el fenómeno de Facebook, My Space o Linkedin, poniendo en contacto a millones de personas a través de Internet. Traducción del artículo original de Chris Anderson: http://babalum.wordpress.com/2006/10/12/la-larga-estela-el-fin-de-pareto/ Blog de Chris Anderson: http://www.thelongtail.com/ Libro **The Long Tail: Why the Future of Business Is Selling Less of More (ISBN 1-4013-0237-8)**: http://books.google.com/books?id=O2k0K1w_bJIC&printsec=frontcover

4. ENLACES VARIOS

- Libro sobre la blogosfera hispana, *"La Blogosfera hispana: Pioneros de la Cultura Digital"*: http://www.fundacionorange.es/areas/25_publicaciones/publi_253_9.asp
- Artículo interesante sobre digitalización certificada y compulsa electrónica: http://inza.wordpress.com/2008/03/06/digitalizacion-certificada-y-compulsa-electronica/
- El documento electrónico en la oficina judicial: http://noticias.juridicas.com/articulos/60-Derecho%20Procesal%20Civil/200902-12457898653256.html
- Presentación sobre el uso de el uso de Wikis en la empresa: http://docs.google.com/PresentationEditor?id=dgf869jf_6hn8sbm
- Discusión interesante sobre pormenores de la generación de claves privadas: http://www.kriptopolis.org/sobre-la-generacion-de-claves
- Wikanda: http://www.wikanda.es
- El presidente de la era Internet: http://blogs.publico.es/dominiopublico/919/el-presidente-de-la-era-internet/
- Como diferenciarse en LinkedIn: http://micarreralaboralenit.wordpress.com/2009/01/15/diferenciarse-en-linkedin/
- Explicación gráfica del éxito de recaudación de la campaña de Obama: http://www.xplane.com/obama/XPLANED_Obama_Fundraising.pdf
- Explicación de la estrategia de Marketing viral de Barack Obama: http://www.themccainobamavirals.com/2008/10/top-5-barack-obamas-viral-marketing.html

- Ejemplos del uso de tecnologías Web 2.0 en la Administración: http://eadminblog.net/post/2008/05/25/uso-de-tecnologias-20-en-la-administracion-publica-ejemplos-cercanos

5. TERMINOLOGÍA RELATIVA A LA FIRMA ELECTRÓNICA

Término	Definición
Poseedor de claves	Posee dos claves criptográficas matemáticamente relacionadas. Una **privada** secreta y una **pública** que puede dar a conocer.
Firma electrónica	Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, *"conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante."*
Firma digital	Operación criptográfica realizada sobre un documento con la clave privada de su **único** poseedor.
Verificación de firma	Operación criptográfica inversa, realizada únicamente con la clave pública del firmante. Permite detectar cualquier alteración del documento.
Identificación del firmante	Puede hacerse durante la verificación de la firma cuando conocemos **inequívocamente** a quien pertenece la clave pública.
Certificado digital	Estructura de datos que contiene la clave pública de un usuario junto con sus datos de identificación. Nombre y DNI. Los emiten los **Prestadores de Servicios de Certificación** y sirven para verificar las firmas e identificar al firmante.
Datos de creación de firma	Clave privada de un titular.
Datos de verificación de firma	Clave pública de un titular.
Certificado electrónico de firmante	Documento que vincula unos datos de **verificación de firma** a un firmante.
Certificado reconocido	Certificado que contiene los datos que marca la ley y es emitido por un Prestador de Servicios de Certificación que cumple las obligaciones legales establecidas para la comprobación de la identidad del titular, fiabilidad y garantías.
Dispositivo seguro de creación de firma	Dispositivo que sirve para aplicar los datos de creación de firma y posee una serie de garantías de seguridad. Según las normas técnicas de la UE, una tarjeta inteligente con certificación de seguridad EAL4+ se considera un DSCF.
Firma electrónica reconocida	Firma electrónica creada por medios que el firmante puede mantener bajo su **exclusivo control** y generada mediante un Dispositivo Seguro de Creación de Firma. Jurídicamente tiene el mismo valor que la firma manuscrita.