IMPULSO AL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN

EL DNI ELECTRÓNICO COMO CATALIZADOR

JOSEFA GARCÍA MESTANZA

Departamento de Economía
y Administración de Empresas.
Universidad de Málaga.

Desde que las TIC, como sector de actividad transversal, y la denominada Sociedad de la Información (SI), como concepto más amplio, se identificaron como elementos determinantes para el avance económico y la mejora de la productividad, los gobiernos desarrollados han venido prestando especial atención a esta nueva dimensión del crecimiento y progreso económico.

Esta fuerte correlación entre gasto en TIC y crecimiento de la productividad llevó a establecer la necesidad de "la creación de una SI para todos" en la Agenda de Lisboa como una de las dimensiones críticas para conseguir incrementar la competitividad de las economías europeas.

En este ámbito, los resultados europeos han sido desiguales. Tomando índices sintéticos, son los países nórdicos, como Dinamarca o Suecia, quienes lideran el desarrollo de la SI en Europa. Detrás de ellos quedan países como Reino Unido, Holanda o Alemania. España se sitúa en las posiciones finales entre los países de la Europa de los 15 y por encima de los nuevos miembros recientemente incorporados (1). En el ámbito mundial nuestro país se sitúa por detrás de los veinte más avanzados. Este grave retraso se agudiza si tenemos en cuenta que su actual patrón de crecimiento no es el propio de una economía avanzada.

Se revelan aspectos significativos de nuestro panorama nacional al desagregar estos índices comparativos. Por ejemplo, poseemos el liderazgo absoluto en disponibilidad de cajeros automáticos y de terminales de punto de venta —lógicamente, esto deriva en una reducida clientela de banca electrónica—; la conectividad a Internet y uso de banda ancha entre las empresas grandes y medianas es comparable a la de cualquier país desarrollado excepto en las micorempresas y autónomos que están muy por debajo; el desarrollo de la Administración Electrónica es relativamente bueno; la actividad de los ciudadanos en comunicación y participación en foros es más que aceptable, a diferencia de la baja posición que ocupamos si atendemos a los indicadores relacionados con el comercio electrónico (Fundación Telefónica, 2007).

Dados estos resultados, y siguiendo las directrices de la Agenda de Lisboa, el Gobierno decidió renovar los

programas en TIC precedentes, Info XXI y España.es, para completar su rango de acción en un nuevo «Plan de Convergencia con Europa» que pretende unirnos a las líneas de desarrollo trazadas en nuestro continente (2). El paraguas que alberga e incorpora estas propuestas es el plan de I+D+i Ingenio 2010, para el periodo 2006-2010.

Uno de los tres programas Ingenio 2010 es el denominado Plan Avanza, el cual se orienta a conseguir la adecuada utilización de las TIC para contribuir al éxito de un modelo de crecimiento económico basado en el incremento de la competitividad y la productividad, la promoción de la igualdad social y regional, la accesibilidad universal y la mejora del bienestar y la calidad de vida de los ciudadanos. A nivel global los objetivos se concretan en que el Gasto TIC sobre el PIB se sitúe en el 7% para el año 2010 (3).

El Plan Avanza se estructura en torno a cinco grandes áreas de actuación:

1] Hogar e inclusión de ciudadanos, donde se desarrollan medidas tendentes a: garantizar la extensión del uso de las TIC en los hogares; aumentar y potenciar la inclusión en éstos; ampliar los ámbitos de participació,n de la ciudadanía en la vida pública.

2] Competitividad e Innovación, con medidas encaminadas a impulsar el desarrollo del sector TIC en España y la adopción de soluciones tecnológicamente avanzadas por las PYMEs españolas.

3] Educación en la Era Digital, incorporando las TIC en el proceso educativo y de formación e integrando a todos los agentes que en él participan.

4] Servicios Públicos Digitales, con medidas que permitan mejorar los servicios prestados por las Administraciones Públicas, aumentando la calidad de vida de los ciudadanos y la eficiencia de las empresas.

5] El nuevo Contexto Digital, con el despliegue de infraestructuras de banda ancha que lleguen a todo el país, genere confianza en ciudadanos y empresas en el uso de las nuevas tecnologías, proporcione mecanismos de seguridad avanzados y promueva la creación de nuevos contenidos digitales.

Este contexto ha abierto una serie de nuevos retos a la sociedad en general y a la española en particular desde el punto de vista de la identificación de los ciudadanos. Para responder a estas nuevas necesidades el Gobierno, desde este Plan, pretende impulsar la identidad digital. La meta es que en el 2010, el 100% de los ciudadanos dispongan del DNI electrónico.

ANTECEDENTES DEL DNI ELECTRÓNICO

El desarrollo de la SI hace necesario buscar nuevas formas de ajustarse a los cambios en las necesidades de la población, a fin de lograr capturar sus beneficios fundamentales para ciudadanos y empresas, tanto en el ámbito económico (incremento de la productividad y de la competitividad) como en el social (reduciendo las diferencias sociales para contribuir a un mayor bienestar). En este proceso una medida emblemática es la implantación del DNI electrónico, que permitirá al ciudadano acreditar su identidad tanto por el canal tradicional (físico) como por el digital.

Los estudios sobre identidad digital, en nuestro país, se remontan a los noventa, destacando, entre otros, el Plan Info XXI y las Recomendaciones de la Comisión Especial de Estudios para el Desarrollo de la Sociedad de la Información, la denominada Comisión Soto, quien, en abril de 2003, para luchar contra las barreras que impedían el pleno desarrollo de la SI, proponía un «golpe de timón» en el que se enmarcaba el desarrollo del DNI electrónico, a fin de que éste diese soporte al conjunto de transacciones electrónicas, ya que mejoraría la seguridad en las mismas e impulsaría el desarrollo de los servicios *on line* de la Administración.

Siguiendo sus directrices estratégicas, en julio de 2003, se diseñó un Plan de Choque para el impulso de la Administración Electrónica, administración.es, dentro del Plan de Actuaciones para el desarrollo de la SI España.es.

A raíz de este Plan, administración.es, en febrero de 2004, el Consejo de Ministros estableció que se comenzara a expedir el DNI electrónico en prueba y se completara la iniciativa de renovación total para el 2007. Pero este proyecto se retrasó por problemas técnicos de compatibilidad entre los certificados digitales de la Fabrica Nacional de Moneda y Timbre (FNMT) y la Seguridad Social.

En julio de 2005 el Gobierno adjudicó el proyecto del DNI electrónico a una unión temporal de empresas formada por Telefónica, Indra y Software AG, que se comprometieron a poner en marcha este proyecto en un plazo máximo de nueve meses. El contrato de adjudicación ascendió a 12 millones de euros e incluía la fabricación de los materiales y los dispositivos para su elaboración y emisión, además de gestionar un cen tro piloto de emisión antes del despliegue en toda España.

Solucionados los problemas técnicos y con retraso de dos años, la expedición del DNI electrónico comenzó en Burgos durante el mes de marzo de 2006,

RECUADRO 1
MECANISMOS INCORPORADOS EN EL DNI ELECTRÓNICO

Seguridad física

El material elegido para su confección, el policarbonato, es más duro que el empleado tradicionalmente, con una duración estimada superior a los diez años, y que no permite combustión alguna por debajo de los 200 grados centígrados, no pudiéndose dividir en láminas, sin provocar su destrucción. Asimismo, se utilizará tinta ópticamente variable, con un hilo de seguridad embebido en el papel, relieves en el plástico y la fotografía impresa estará protegida con los fondos de seguridad. Los datos se grabarán con láser, conteniendo microescrituras con tintas visibles a la luz ultravioleta.

Seguridad administrativa

El Ministerio del Interior acreditará, con carácter exclusivo, los dos certificados del DNI digital: el de autenticación del ciudadano y el de firma digital. De este modo con el nuevo Documento las Fuerzas de Seguridad del Estado tendrán mayor certeza sobre la identidad de los individuos en sitios como aeropuertos u oficinas de la Administración. Además, por razones de seguridad, el ciudadano, de modo voluntario, podrá activar el certificado de firma electrónica en las Oficinas de Expedición.

Seguridad electrónica

Entre sus medidas destacan: un número de identificación único para cada chip, un generador de números aleatorios por hardware verificable internamente, una disposición de elementos optimizada para dificultar el acceso a los componentes, contramedidas para el análisis de fallos diferenciales, alimentación diferencial o de análisis simple de potencia y un blindaje activo con detección de ataques.

donde se desarrolló una experiencia piloto a lo largo de dos meses. Finalizada esta experiencia, se inició su implantación en el resto del territorio nacional.

No obstante, en la FNMT hacía ya tiempo que estaban disponibles las unidades de Tarjeta Criptográfica, el Cryptokit, que fue el embrión del DNI digital. De aspecto prácticamente igual al de una tarjeta de crédito de un banco, se distribuye junto con un lector que permite conectar la tarjeta con el ordenador personal, y certificar así la identidad del usuario cuando esté navegando y realice operaciones *on line*.

EL DNI ELECTRÓNICO

El modelo de DNI electrónico propuesto acredita la identidad personal de su titular y permite la firma electrónica de documentos, por lo que posee las mismas funciones que el actual, con la firma física, pero ampliándolas a la red (4).

El soporte de este Documento es una tarjeta de policarbonato, que sigue el estándar ISO-7816-1, semejante a una tarjeta de crédito, con el mismo tamaño y color que el DNI actual, aunque la foto se desplaza hacia la derecha, la firma pasa a la parte inferior e incluye un chip informático en la parte izquierda.

Este chip (5) contiene los mismos datos que aparecen en la tarjeta —datos personales, fotografía, firma y huella dactilar digitalizadas— junto con los certificados de autenticación y de firma electrónica —el de autenticación impide que la personalidad del firmante sea suplantada y el de firma electrónica reconocida protege la información enviada a través de un medio telemático— no incluyendo ningún otro tipo de dato diferente —sanitarios, fiscales o de tráfico—.

De este modo, para autentificarse el usuario o firmar digitalmente documentos electrónicos se requerirá un lector de tarjeta que cumpla el estándar ISO-7816 (con dispositivo integrado en el teclado externo, conectado vía USB o a través de interfaz PCMCIA) y un software que puede descargarse vía Internet (tanto el CSP, para entornos de Microsoft Windows, como el PKS#11, para entornos Linux, Unix o Mac, podrán obtenerse en la dirección www.dnielectronico.es/descargas/) en cada ordenador personal (Intel —a partir de Pentium III— o tecnología similar).

Así, para operar con el nuevo Documento a través de la red se deberá introducir éste en un lector de tarjetas, previamente conectado al PC. El usuario se conecta al servidor web de un prestador de servicios (Administración, empresa...), quien le presenta su certificado (para comprobar que realmente se ha conectado con quien desea hacerlo) y le indica que la conexión es segura. El terminal del usuario y el servidor web se intercambian las claves públicas para iniciar una comunicación segura. Cuando el servidor web requiera la firma electrónica del usuario, éste accederá a su certificado de firma a través de la clave privada y cumplimentará los datos solicitados por el servidor. Tras la comprobación del contenido del documento, lo firma digitalmente. A continuación se envía el documento, la firma y el certificado de usuario al prestador de servicios, quien, a través del Servicio de Validación, comprueba que los certificados no han sido suspendidos ni revocados.

Este Documento incorpora mecanismos de seguridad tanto físicos como administrativos o electrónicos para evitar su falsificación, e, incluso, algunos requieren un análisis de laboratorio (Recuadro 1).

La expedición y entrega del nuevo Documento se hace en el momento de su solicitud —el tiempo ronda los 15 minutos— en cualquiera de los centros de emisión repartidos por todo el país —prácticamente todas las provincias lo emiten— eliminando los plazos de espera existentes hasta hace unos meses —entorno a una semana— y el número de visitas a la Oficina de Expedición —de dos a una—.

A finales de 2007, cerca de tres millones de ciudadanos ya disponían del DNI electrónico, y los trabajos se centraron en estudios sobre su uso y en los perfiles de protección para su utilización como dispositivo seguro de creación de firma digital en plataforma PC y TDT (6).

A finales de 2008, con más de siete millones de ciudadanos con el DNI electrónico, los trabajos fueron encaminados a la creación de varios macrocentros a nivel nacional para la expedición de este Documento, a su compatibilidad en dispositivos que funcionan con códigos abiertos, a Sistema de Gestión y Monitorización del Servicio (metodología ITIL) y a sistema de gestión de espera (Ministerio del Interior, 2008) (7).

Según palabras del propio Director General para el Desarrollo de la SI (Ciervo, 2008) hasta ahora se ha trabajado en el lanzamiento del DNI electrónico tanto desde el punto de vista de despliegue de infraestructuras, como de la adaptación de servicios y la sensibilidad de la ciudadanía. Para esta legislatura, el principal objetivo es la generalización de su uso y el desarrollo de aplicaciones para su uso público y privado, a través de la prestación de servicios atractivos y seguros para ciudadanos, empresas y entidades locales.

RETOS Y OPORTUNIDADES DEL DNI ELECTRÓNICO EN LA SOCIEDAD DE LA INFORMACIÓN

El DNI electrónico, además de la utilidad convencional tradicional, permite actuar en las redes de comunicación públicas y privadas, respaldando a su propietario al garantizar la integridad del documento firmado, el no repudio de éste y la autenticidad de origen, mientras que al receptor de un correo electrónico o de un pedido en una tienda de Internet le permite saber quién está realmente al otro lado. Aunque, en ningún caso garantiza que se tengan fondos en el banco y tampoco contiene aplicaciones de monedero electrónico —simplemente supone un otorgamiento de fe a un documento de la Red—.

Una persona con este DNI podrá, por ejemplo, efectuar trámites completos con las Administraciones Públicas (renovar sin salir de casa el pasaporte, pagar impuestos, tasas o multas, presentar reclamaciones, solicitar licencias de importación o exportación, certificados de empadronamiento o de la Seguridad Social, comprobar el saldo de puntos del carnet de conducir...), realizar compras firmadas (compra-venta de valores, de bienes inmuebles...), votar, matricularse en centros públicos o privados, firmar contratos y documentos notariales, utilizar de forma protegida el ordenador personal, participar en una conversación por Internet con la certeza de que el interlocutor es quien dice ser, efectuar transacciones bancarias *on line* o de comercio electrónico seguras...

Además, gracias a su chip, la policía podrá reconocer a sus usuarios desde un simple teléfono móvil o PC de bolsillo y determinar su autenticidad sin tener que llamar a la central. Incluso, este documento podría sustituir a las tarjetas de identificación electrónica que llevan los empleados en algunas empresas. El problema de fondo que subyace en este Documento, tanto político como filosófico, será trazar la frontera entre privacidad y seguridad. Por ello, probablemente, éste seguirá siendo un documento de identificación y no de control.

En el ámbito Judicial, hasta ahora, el principal problema en las comunicaciones a través de la red ha sido la identidad de las partes que interactuaban. Con la emisión del nuevo Documento digital y la creación y aprobación de los «Terceros de Confianza», se podrá solventar este problema. El DNI electrónico permitirá asegurar que la persona es realmente quien dice ser, y la entidad certificadora podrá actuar a modo de «notario virtual».

En principio los beneficios derivados de su uso son muchos e importantes. Este proyecto ha sido valorado positivamente por la Asociación Nacional de Empresas de Internet y el Consejo Superior de las Cámaras de Comercio, Industria y Navegación a través de su Foro de Firma Electrónica al estimar que favorecerá el comercio al incrementar la seguridad y la confianza en las transacciones *on line*.

No obstante, las críticas tampoco se han hecho esperar. Por ejemplo, la Asociación de Internautas y la Comisión de Libertades Informáticas manifestaron que no se debía despachar la regulación del DNI electrónico en dos artículos de la Ley 29/2003 de firma electrónica (8), ya que se requeriría una Ley Orgánica específica por afectar directamente a derechos fundamentales, además de criticar la imposición por decreto de su puesta en marcha sin ningún tipo de debate político ni social previo (9).

RECUADRO 2
MARCO LEGAL BÁSICO DEL NUEVO DNI

- ✓ Directiva 1999/93/CE del Parlamento Europeo y del Consejo por el que se establece un marco comunitario para la firma electrónica.
- ✓ Ley 59/2003 de Firma Electrónica.
- ✓ Ley Orgánica 15/1999 de protección de datos de carácter personal.
- ✓ Real Decreto 1553/2005 que regula la expedición del DNI y sus certificados de firma electrónica.

De otro lado, la seguridad del nuevo Documento se convierte en una cuestión clave. Mientras que la pérdida o sustracción del DNI tradicional no supone un riesgo grave para el usuario, ya que normalmente requiere su presencia al ser autentificado mediante la firma y la fotografía, en el DNI electrónico la seguridad se ve comprometida al poder usarse por un tercero sin consentimiento o conocimiento del titular.

Incluso, la seguridad basada en el oscurantismo del hardware tecnológico no es una garantía absoluta, puesto que las tarjetas se pueden criptoanalizar teniendo los recursos adecuados, y cada día aparecen medios más sofisticados. Y es que, las firmas manuscritas son complicadas de falsificar, mientras que una clave, una vez conocida, puede ser introducida por cualquiera.

O también, puede que se filtre la información y a partir de ahí manipular o crear circuitos que emulen el funcionamiento de estos dispositivos. Si se lograra clonar los DNI o se rompieran los sellos criptográficos, no sería necesario disponer de las tarjetas originales, lo que dificultaría la detección del fraude.

El hecho de que no se informen o conozcan fallos de seguridad no significa que no existan, e incluso, que no se estén explotando con éxito por los delincuentes.

También, cuando se da de alta su utilización en la red, se da como un «todo», y no por servicios. Si el usuario pudiera activar o desactivar en el tiempo las operaciones que desea, o establecer un límite en la cuantía de las mismas, se minimizarían los posibles ataques, y en el supuesto caso de fallo de seguridad, su uso estaría limitado a una serie de acciones previamente definidas por su usuario.

Por ello, al tener más usos y funciones que el DNI actual, se aumentarán considerablemente los ámbitos de aplicación, el interés por el producto y sus funcionalidades y, paralelamente, las áreas con un riesgo potencial para los ciudadanos.

Otro punto débil indirecto puede derivar del lugar desde el que se realicen las operaciones. En ocasiones, estas tarjetas se usarán en ámbitos no controlados, como el hogar o en instalaciones no vigiladas, en los que cabe la posibilidad de coacción o amenaza. Si no se garantiza algún tipo de seguridad al respecto, pueden ser bastantes los casos en los que se obligue al titular a hacer un uso del DNI mediante intimidación, máxime con el aumento de los casos de malos tratos que existen.

Además, se han de tener en cuenta las limitaciones de los usuarios a la hora de establecer y recordar las contraseñas de seguridad.

Otro problema que puede afectar a su extensión y uso es el hecho de que no sea universal. Cuando se pretendía que este documento fuese crucial para actuar en las redes de comunicaciones públicas y privadas, acreditando la identidad del usuario y posibilitándole para firmar digitalmente, no se contemplaba que su uso estuviese limitado al estado español.

En este terreno se está avanzando bastante. Por ejemplo, en el Plan de Acción eEuropa 2005, el programa IDABC, para el periodo 2005-2009, se trabaja en el intercambio electrónico de datos entre Administraciones en la UE, la interoperabilidad de los mismos y su normalización (10). Incluso, diez de éstos países preparan ya la digitalización del documento nacional de identidad: Bélgica, Finlandia, Italia, Holanda... En Bélgica ya se expide de manera oficial (11), aunque a diferencia del documento español no incorpora los datos biométricos de identificación, y en Finlandia se dispone de este sistema desde diciembre de 1999. No obstante, a pesar de que su Documento sirve para realizar gestiones con la Administración, como documento de viaje y desde junio de 2004 como identificación para la Seguridad Social, no ha sido todo lo exitoso que se esperaba (Heichlinger, 2007).

De hecho, el éxito de este Documento electrónico no dependerá sólo de la creación de un sistema que garantice la seguridad de las comunicaciones electrónicas sino también de que este sistema vaya acompañado de las facilidades de uso que permitan su aplicación generalizada.

En este caso concreto, la estandarización adquiere un papel clave en tanto que facilita la creación de nuevos servicios. Es una realidad contrastada que

cuando un servicio electrónico funciona, en tiempo y forma, y está asentado, su uso crece exponencialmente en breve plazo.

No obstante, siempre que se establezca un sistema de gestión basado en el DNI electrónico debe haber un procedimiento alternativo tradicional, para que su uso mayoritario no suponga un problema a los usuarios que tengan menos recursos, una reducida capacitación técnica o simplemente, no lo quieran utilizar en su faceta electrónica. A este respecto, el artículo 9, apartado 2, del RD 1553/2005, establece que la activación de la utilidad informática de este Documento (identificación electrónica de su titular y la capacidad de realizar la firma electrónica de documentos) tiene carácter voluntario.

CONCLUSIONES

El sector de los contenidos digitales está llamado a convertirse en uno de los protagonistas de la revolución digital del futuro, ya que su tendencia de crecimiento en volumen de negocio se ha afianzado en los últimos años en todos los países desarrollados (Cierco, 2008).

A este respecto, nuestro país sigue presentando un avance muy desigual entre ciudadanos, empresas y Administraciones en los distintos elementos de la cadena de valor y existen problemas de oferta de infraestructuras y de servicios y contenidos de utilidad como problemas de demanda.

El DNI electrónico puede actuar como catalizador en el desarrollo de esta SI al incidir sobre la escasa percepción de la utilidad y del potencial de las nuevas tecnologías como impulsoras de la productividad, la competitividad y de la mejora de la calidad de vida de los ciudadanos y empresas, así como sobre la reducida oferta de servicios y contenidos que puedan ser considerados de utilidad e interés por los usuarios (12).

Los datos expuestos a lo largo de este artículo obligan a pensar que la implantación del DNI electrónico, como facilitador del acceso generalizado de los ciudadanos a la nuevas tecnologías, ya es una realidad en nuestro país aunque hace falta alcanzar una masa crítica de usuarios que utilicen y demanden los nuevos servicios para apreciar el verdadero efecto de este Documento en la sociedad española. No obstante, el hecho de que se extienda su uso dependerá de la evolución de un conjunto de factores integrados como son el incremento de la tecnología, el desarrollo de una buena organización orientada desde la Administración, una legislación adecuada, la cooperación interadministrativa, el desarrollo de aplicaciones privadas, la participación ciudadana y el cambio cultural (13).

NOTAS

[1] Nuestro indicador de convergencia respecto a la Unión, a finales de 2006, fue del 84,1%.

[2] Hemos de tener en cuenta que la UE no se encuentra a la cabeza del mundo en el desarrollo de la SI.

[3] El Presidente del Gobierno propuso en el debate de investidura la ampliación del periodo de vigencia de este Plan hasta 2012, actualizando sus objetivos y actuaciones para adecuarlos a los nuevos retos que nos presenta la sociedad en red del siglo XXI.

[4] El DNI electrónico tiene suficiente valor, por sí sólo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo (Art. 2, RD 1553/2005), e incorpora a las características del DNI tradicional las nuevas funciones de firma electrónica de documentos (Ley 59/2003).

[5] El chip electrónico posee tres partes accesibles en lectura: una pública ?sin restricciones? que refleja el certificado de la autoridad de certificación de producción y las claves públicas del ciudadano; una privada ?a través de password o datos biométricos? que contiene claves privadas del ciudadano, el certificado de firma y el certificado de autenticación; y, una zona de seguridad ?mediante la utilización del PIN y procedimiento de acceso a disposición de la Administración? con los datos biométricos, los datos de filiación contenidos en el soporte físico y el número de serie del soporte.
El PIN es la contraseña que protege las claves privadas y permite activarlas en las aplicaciones que generan firma electrónica. Este PIN, que originalmente se entrega en un sobre ciego, puede ser cambiado por otro a elección del ciudadano.

[6] Al DNI electrónico le correspondió el 32,95 % del presupuesto ejecutado en 2007 del Plan Avanza (47,6 MME) (Red.es, 2008).

[7] A la fecha de finalización de este artículo aún no se ha publicado la distribución por tipo de actuaciones del presupuesto ejecutado en 2008 del Plan Avanza.

[8] Artículos 15 y 16 de la citada Ley (BOE nº 304, de 20 de diciembre). La base legal para la construcción de la presente Ley es la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica.

[9] Esta realidad se puso de manifiesto en las enmiendas formuladas a esta Ley en el Congreso (casi 250) y en el Senado (289).

[10] Ver eEurope Smart Card Charte Prof. of concept and holistic solution. eEpoch Projet (proyectos de cooperación europeo de interoperabilidad y seguridad en los sistemas de identidad digital) e-ID and the Information Society in Europe (http://www.eepoch.net/) ó Interoperable European Electronic Identities (http://www.id.ee/porvoo5/?show=1).

[11] Según el Ministerio del Interior de ese país, para finales de este año se prevé que el 100% de los ciuda-

danos belgas de más de 12 años tendrán ya la nueva tarjeta.

[12] De ahí que se torne fundamental el hacer partícipes a los ciudadanos de las ventajas de su utilización y la Administración Pública ha de liderar este proceso.

[13] Aunque escasas comienzan a surgir las primeras iniciativas en el sector empresarial para dinamizar la relación comercial con sus clientes. Por ejemplo, Caja Madrid permite la realización de operaciones en los cajeros automáticos con el DNI electrónico ampliando los servicios y operaciones disponibles.

BIBLIOGRAFÍA

CIERVO, D. (2008): "Entrevista a D. David Cierco", *revista-ays.com,* nº 25, septiembre, en http://www.revista-ays.com/DocsNum25/PersAAPP/Cierco.pdf (Consultada el 21 de noviembre de 2008).

COMISIÓN DE LIBERTADES E INFORMÁTICA (2006): «Según la Comisión de Libertades e Informática la Ley de Firma Electrónica tiene importante defectos técnicos», en http://www.madridpress.com/home/DetallNews.jsp?id=19590&static=0 (Consultada el 22 de noviembre de 2006).

CONSEJO SUPERIOR DE LAS CÁMARAS DE COMERCIO, INDUSTRIA Y NAVEGACIÓN (2006): *Foro de firma electrónica,* a través de su Foro de Firma Electrónica, Camerfirma, en http://www.camerfirma.com (Consultada el 22 de noviembre de 2006).

DIRECTIVA 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, Diario Oficial de las Comunidades Europeas, de 19 de enero de 2000.

FÁBRICA NACIONAL DE MONEDA Y TIMBRE, FNMT (2008): *Obtenga el certificado de usuario con su DNI, en* http://www.cert.fnmt.es (Consultada el 22 de noviembre de 2008).

FUNDACIÓN TELEFÓNICA: *La sociedad de la información en España 2007,* http://www.telefonica.es/sociedaddelainformacion/html/informes_home.shtml (Consultada el 22 de noviembre de 2008).

HEICHLINGER, A. (2007): «Las TIC en la Administración Pública Europea: El auge del gobierno electrónico», *Boletic*, septiembre-octubre, en:
http://www.astic.es/Asociacion/DetallesBoletic/Documents/Boletic43/opinion/opinion_2.pdf (Consultada el 21 de noviembre de 2008).

INFORMATIVOS.NET (2008): *Valoración de la Ley de Firma Electrónica,* en;
http://informativos.net/notampliada.asp?idNoticia=41861 (Consultada el 22 de noviembre de 2008).

INICIATIVA I2010 (2008): *Preparar el futuro digital de Europa. Revisión intermedia de la iniciativa i2010 (Informe anual sobre la sociedad de la información 2008),* Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 17 de abril, Bruselas: http://mastertv.files.wordpress.com/2008/10/i2010-informe-2008.pdf, también en http://www.csi.map.es/csi/pdf/i2010_ar_2008_en.pdf y en http://ec.europa.eu/information_society/eeurope/i2010/mid_term_review_2008/index_en.htm (Consultada el 21 de noviembre de 2008).

LEY 59/2003, de 19 de diciembre, de firma electrónica. BOE nº 304, de 20 de diciembre de 2003,
http://www.setsi.mcyt.es/legisla/internet.htm (SETSI-LEY 59/2003).

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.

MINISTERIO DEL INTERIOR (2008): *DNI electrónico*, en http://www.dnielectronico.es (Consultada el 23 de noviembre de 2008).

PLAN DE CHOQUE PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA, Ministerio de Ciencia y Tecnología y Ministerio de Administraciones Públicas, 8 de mayo de 2003.
http://www.astic.es/eAdministracion/Documents/PlanChoque.pdf (Consultada el 21 de noviembre de 2008).

PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 13 de mayo de 1998 por la que se establece un marco común para la firma electrónica, Comisión de las Comunidades Europeas COM(1998) 297 final, 98/0191 (COD).

REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

RECOMENDACIONES DE LA COMISIÓN ESPECIAL DE ESTUDIOS PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN (2003): *Aprovechar la Oportunidad de la Sociedad de la Información en España*, de 1 de abril, Madrid.

RED.ES (2008): *Memoria de actividades 2007*, en http://www.red.es/publicaciones/articles/id/2214/memoria-actividades-2007.html (Consultada el 22 de noviembre de 2008).