

Mesa redonda

¿La Administración? ¡#eAdministración, por supuesto!

De la seguridad a la ciberseguridad

Evolución de la Administración Electrónica

En el año 1996 se publicó la primera edición del libro *La era de la información. La sociedad en red* escrito por Manuel Castells (1). El citado libro fue el resultado de las investigaciones que el autor inició en 1986.



MARÍA JESÚS CASADO

Responsable de la seguridad de la información de la IGAE.
Ministerio de Hacienda y Administraciones Públicas

Manuel Castells ya se refería a la sociedad de la información, y a su evolución hacia la sociedad conectada, y concebía una nueva economía globalizada: “la integración global de los mercados financieros, el ascenso del Pacífico asiático como el nuevo centro industrial global dominante, la ardua pero inexorable unificación económica de Europa, el surgimiento de una economía regional norteamericana, la diversificación y luego desintegración del antiguo Tercer mundo, la transformación gradual de Rusia y la zona de influencia ex soviética en economías de mercado, y la incorporación de los segmentos valiosos de las economías de todo el mundo a un sistema interdependiente que funciona como una unidad en tiempo real”.

Esta concepción de la sociedad coincide con la realidad actual. Casos tan dispares como la guerra en Siria o la eliminación de la candidatura de Madrid para la organización de los juegos olímpicos de 2020 influyen en el funcionamiento de los mercados financieros y en la economía mundial.

Evolución de la Administración Electrónica

¿Cuál era el nivel de informatización de las Administraciones Públicas del Estado Español en el año 1986? Era muy incipiente pues todavía no se disponía de regulación en esta materia. Sería el año 1992 cuando se aprobó la primera Ley (2) que reconocía la validez administrativa de la información procedente de sus sistemas informáticos. »



Es de justicia mencionar el año 1968 en el que unos gestores intrépidos y con ilusión del extinto Instituto Nacional de Previsión, a los que se les formó en las tecnologías existentes en aquellos años, iniciaron la informatización de los procedimientos de la Seguridad Social. En mi opinión aquél año comenzó la Administración Electrónica.

Su trabajo fue muy fructífero pues aunaban los conocimientos de la gestión con el tecnológico. Estos funcionarios fueron los “analistas informáticos más antiguos”. En el año 1976 se convocaron las primeras oposiciones en las que se pedían conocimientos informáticos, los opositores se examinaban para acceder a la “escala de analistas de la Administración de la Seguridad Social”.

La inscripción y afiliación de trabajadores y empresas conocido como “P20” y las recetas mediante fichas para calcular el gasto sanitario “P29” fueron los primeros procedimientos en informatizarse. La captura de datos comenzó en el año 1972.

Los datos anteriores a 1972 continuaron en soporte papel y su solicitud tenía que realizarse en la calle de

la Coruña (Madrid) y la entrega a los solicitantes tardaba bastante tiempo por la ingente cantidad de legajos.

Antes de acuñarse el nombre de “Gerencia Informática de la Seguridad Social”, la Unidad informática se conocía con el nombre de “Centro de Proceso de Datos de la Tesorería de la Seguridad Social” y tenía la categoría de servicio. En este centro se unieron la informática del Instituto Nacional de Previsión y del Instituto Nacional de la Seguridad Social.

Anterior al año 1988, una empresa o trabajador podía solicitar los datos sobre su vida laboral desde el año 1972 acudiendo a una oficina de la Tesorería General de la Seguridad Social. Personal de la Tesorería registraba la solicitud en un sistema informático y en unos días el peticionario podía pasar a recoger la documentación demandada.

En el año 1988 se dio un paso de gigante cuando en las mismas oficinas, comenzó a realizarse el trámite mencionado en “tiempo real”.

Por lo descrito hasta ahora es por lo que considero el año 1968 el comienzo de la Administración Electrónica en España. Quizás alguno de

los lectores de este artículo conozca una experiencia anterior al año referido.

Se ha recorrido una larga singladura hasta llegar a la Administración Electrónica tal como la entendemos ahora.

Se ha pasado de la presentación en soporte papel de los requisitos que los ciudadanos debían cumplir para relacionarse con la Administración, a la gestión automatizada de los citados requisitos evitándoles desplazamientos y con el ahorro de tiempo que ello supone.

Se han ido cubriendo etapas cuyos resultados han sido los pilares que han sustentado la realización de otras etapas, y sus consiguientes resultados, hasta llegar a una Administración Electrónica sólida.

Alguno de los pilares a destacar son los siguientes:

- Consideración de la validez administrativa de la información proporcionada por los sistemas informáticos.
- Concepción primigenia de la seguridad (3) de la información procedente de los sistemas electrónicos.
- Habilitación (4) a la Fábrica Nacio-

nal de Moneda y Timbre-Real Casa de la Moneda, para la prestación de servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de las comunicaciones de las Administraciones Públicas y los Organismos Públicos, a través de técnicas y medios electrónicos, informáticos y telemáticos.

- Establecimiento (5) de un cauce jurídico apropiado que, adaptándose plenamente a la normativa vigente sobre firma electrónica y en el marco del artículo 45 de la Ley 30/1992 y del Real Decreto 263/1996, permita una pronta y mejor implantación de los servicios necesarios para garantizar la seguridad, validez y eficacia a través de medios electrónicos, informáticos y telemáticos.

- Regulación (6) de la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado.

- Toda la legislación vigente en el momento de escribir este artículo.

La normativa que reconoce al ciudadano el derecho a relacionarse electrónicamente con las Administraciones Públicas regula dos aspectos complementarios y a la vez con intereses contrapuestos que requieren establecer un equilibrio entre ellos: son la funcionalidad y la seguridad (7).

De la seguridad a la ciberseguridad

La Administración Electrónica estaría huérfana si sólo se centrara en el cambio de la regulación de los procedimientos administrativos para que, al mismo tiempo, se puedan prestar los mismos del modo tradicional y, además, electrónicamente.

En el preámbulo de la Ley 11/2007, el espíritu del legislador deja constancia de que “una ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas se justifica en la creación de un marco jurídico que facilite la extensión y utilización

de estas tecnologías. Y el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. La desconfianza nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías”. Es decir, si al ciudadano no se le transmite confianza, en vano trabajan las Administraciones Públicas. Eso quiere decir que ni la funcionalidad debe prevalecer sobre la seguridad ni viceversa.

Estonia y el ataque informático que sufrió el 1 de mayo de 2007 ilustran la necesidad de que funcionalidad y seguridad deben ir juntas.

Estonia (8) es un país que ha apostado por el uso intensivo de las Tecnologías de la Información y se ha convertido en un Estado totalmente informatizado. Todos los ciudadanos disponen de un dispositivo físico de identificación similar al Documento Nacional de Identidad Español. Con ese dispositivo pueden pagar impuestos, votar, obtener préstamos, etc. En el Consejo de Ministros se utiliza información proporcionada por los sistemas informáticos, no se utiliza el soporte papel.

El ataque citado anteriormente fue diseñado y dirigido contra un objetivo concreto: Estonia. Fue realizado por hackers desde Rusia y se desconoce el móvil real que lo inspiró, pero sí se conoce el suceso que lo desencadenó. El ataque se llevó a cabo utilizando una técnica muy conocida y de uso muy extendido (ataque de denegación de servicio) que, como consecuencia, paralizó el país pues no sólo afectó a los servicios prestados electrónicamente a los ciudadanos sino también

La normativa que reconoce al ciudadano el derecho a relacionarse electrónicamente con las Administraciones Públicas regula dos aspectos complementarios y a la vez con intereses contrapuestos que requieren establecer un equilibrio entre ellos: son la funcionalidad y la seguridad

a entidades financieras, agencias de prensa, etc. El ataque duró tres días y finalizó cuando los hackers lo abandonaron.

Como puede apreciarse, el espacio físico ha dejado paso al espacio virtual creándose una nueva cultura “la cultura de la virtualidad real” cada vez más extendida, aunque con niveles de desarrollo muy distintos según los países.

Nos encontramos ante el espacio virtual o ciberinfinito o ciberespacio. El concepto “ciberespacio” se men- »

cionó por primera vez en el relato *Johhny Mnemonic* escrito por William Gibson en el año 1981. Una vez más, términos utilizados en las Tecnologías de la Información y de las Comunicaciones (TICs) proceden de la ficción. También procede de la ficción el término Metaverso incluido en la novela *Snow Crash*, escrita por el autor Neal Stephenson y publicada en el año 1992.

De igual modo que el espacio virtual ha derivado a la palabra ciberespacio, el término seguridad ha evolucionado a la palabra ciberseguridad de cuño relativamente reciente.

En el año 2012 (9) me preguntaron sobre si la ciberseguridad era una cuestión de futuro. Mi respuesta fue: “La ciberseguridad es una realidad, no es una cuestión de futuro. Ya está impactando en el sector público por la obligatoriedad de prestar el máximo número de servicios electrónicamente y por la implementación de las medidas previstas en el Esquema Nacional de Seguridad en un tiempo limitado que requiere aumentar la inversión, la formación del personal dedicado a la seguridad y un mayor foco en la concienciación de los empleados públicos en un marco presupuestario de austeridad. A todo ello se añade la evolución de los vectores de ataque hacia el uso de técnicas más sofisticadas y las nuevas tendencias en el ámbito tecnológico como el uso extendido de dispositivos móviles y el cloud computing”.

La Unión Europea, mediante una comunicación conjunta del Parlamento Europeo, del Consejo, del Comité Económico y Social Europeo y del Comité de las Regiones, ha aprobado y publicado la Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto y protegido.

Esta comunicación tiene por objeto defender los valores esenciales de la Unión Europea tanto en el mundo físico como en el digital, así como

proteger los derechos fundamentales de los ciudadanos europeos.

El Consejo de Ministros del 31 de mayo de 2013 aprobó la Estrategia (10) de Seguridad Nacional que ha sido el resultado de revisar y actualizar la Estrategia de Seguridad Nacional aprobada en 2011 por el anterior ejecutivo.

Dicha Estrategia se considera una “cuestión de estado” por lo que el primer paso de su implementación ha sido la creación (11) del Consejo de Seguridad Nacional presidido por el Jefe del Estado su Majestad el Rey Don Juan Carlos. La primera reunión del Consejo se celebró el 11 de julio de 2013.

La Estrategia hace referencia al ciberespacio y a la ciberseguridad, cuyo objetivo es “garantizar el uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques”.

Del párrafo anterior se infiere que una de las prioridades de la Estrategia es garantizar el uso seguro (seguridad) de las redes y de los sistemas de información (funcionalidad), prioridad que afianza la reiterada afirmación que he realizado a lo largo del presente artículo: “la funcionalidad y la seguridad han de ir de la mano”. No se puede concebir la Administración Electrónica como servicios, sino como “servicios seguros” de manera que estén garantizadas la integridad, confidencialidad y disponibilidad de los mismos y se inspire confianza a los ciudadanos. *

NOTAS

- (1) La sociedad en red. Alianza Editorial.
- (2) Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (artículo 45).
- (3) Real Decreto 263/1996, por el que

se regula las técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

(4) Artículo 81 de la Ley 66/1997, de 30 de diciembre, de las medidas fiscales, administrativas y del orden social.

(5) Real Decreto 1317/2001, de 30 de noviembre, que desarrolla el artículo 81 de la Ley 66/1997.

(6) Real Decreto 772/1999, de 22 de junio, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

(7) Artículo 42.b de la Ley 11/2007, desarrollado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

(8) Gedeon programmes. Odissea. Avec la participation de FRANCE 5. Et de Planete.

(9) Revista SIC, número 100, junio 2012 (especial SIC 100).

(10) Estrategia de seguridad nacional: un proyecto para todos”.

(11) Consejo de ministros celebrado del 31 de mayo de 2013.