SEGURIDAD EN EL DESARROLLO DEL *SOFTWARE* DE LAS ADMINISTRACIONES PÚBLICAS: UN ESTUDIO JURÍDICO.

Tesis doctoral

María Paz Gil Durán

Directora

Dra. Dª. Mercedes Fuertes López

Catedrática de Derecho Administrativo

UNIVERSIDAD DE LEÓN

2017

Contenido

Figuras

ABREVIATURAS

AA.PP.	Administraciones públicas.
AEAT	Agencia estatal de Administración tributaria.
AENOR	Asociación española de normalización y certificación.
AEMES	Asociación española de sistemas informáticos.
AEPD	Agencia española de protección de datos.
AGE	Administración general del Estado.
ANS	Acuerdo de nivel de servicio.
ASI	Análisis del sistema de información.
ASTIC	Asociación profesional de cuerpos superiores de sistemas y tecnologías de la información de las Administraciones públicas.
ATI	Asociación de técnicos en informática.
ATS	Auto del Tribunal Supremo.
BOC	Boletín oficial de Cantabria.
BOCG	Boletín oficial de las Cortes generales.

BOE	Boletín oficial del Estado.
CA	*Certificate Authority*, autoridad de certificación.
CAPTCHA	*Completely Automated Public Turing test to tell Computers and Humans Apart*, prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos.
CAU	Centro de asistencia a usuarios.
CCN	Centro criptológico nacional.
CEE	Comunidad económica europea.
CEN	*Comité Européen de Normalisation*, Comité europeo de normalización.
CENATIC	Centro nacional de referencia de aplicación de las TIC basadas en fuentes abiertas.
CESAE	Consejo superior de Administración electrónica.
CESE	Comité económico y social europeo.
CIDEC	Centro de investigación y documentación sobre problemas de la economía, el empleo y las cualificaciones profesionales.
CNI	Centro nacional de inteligencia.
CNMV	Comisión nacional del mercado de valores.

COAXI	Comisión Nacional para la Cooperación entre las Administraciones públicas en el campo de los sistemas y tecnologías de la información.
COCOMO	*Constructive Cost Model*, modelo constructivo de costos.
CORA	Comisión para la reforma de las Administraciones públicas.
CP	Ley orgánica 10/1995, de 23 de noviembre, del código penal.
CPP	Contrato de colaboración público privada.
CPU	*Central processing unit*, unidad central de proceso.
CSI	Construcción del sistema de información.
CSV	Código seguro de verificación.
CTT	Centro de transferencia de tecnología.
DEH	Dirección electrónica habilitada.
DGP	Dirección general de policía.
DGS	Desarrollo global de *software*.
DGSeg	Dirección general de seguros.
DGT	Dirección general de tráfico.
DNIe	Documento nacional de identidad electrónico.

DOCE	Diario oficial de las Comunidades europeas.
DoS	*Denial Of Service*, denegación de servicio.
DOUE	Diario oficial de la Unión Europea.
DSI	Diseño del sistema de información.
eAdministración	Administración electrónica.
eID	*Electronic Identity*, identidad electrónica.
eIDAS	Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la directiva 1999/93/CE.
eIDM	*Electronic Identity Management*, gestión de identidad electrónica.
ENECSTI	Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información.
ENISA	*European Network and Information Security Agency*, Agencia europea de seguridad de las redes y de la información.
EIF	*European Interoperability Framework*, marco europeo de interoperabilidad.
ENI	Esquema nacional de interoperabilidad.

ENS	Esquema nacional de seguridad.
ESPRIT	*European Strategic Programme for Research in Information Technologies*, programa estratégico europeo de investigación y de desarrollo en el ámbito de las tecnologías de la información.
ET	Real decreto legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la ley del estatuto de los trabajadores.
ETT	Empresas de trabajo temporal.
EVS	Estudio de viabilidad del sistema.
FJ	Fundamento jurídico.
FNMT	Fábrica nacional de moneda y timbre.
GISS	Gerencia de informática de la seguridad social.
IAE	Impuesto de actividades económicas.
IAS	Implantación y aceptación del sistema.
IDA	*Interchange of Data between Administrations*, intercambio de datos entre Administraciones.
IDABC	*Interoperability Delivery of European e-Government Services to Public Administrations, Businesses and Citizens*, prestación interoperable de

	servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos.
IE	*Internet Explorer*.
IEC	*International Electrotechnical Commission*, Comisión electrotécnica internacional.
IEEE	*Institute of Electrical and Electronics Engineers*, Instituto de ingeniería eléctrica y electrónica.
IEFT	*Internet Engineering Task Force*, grupo de trabajo de ingeniería de Internet.
IGAE	Intervención general de la Administración del Estado.
INAP	Instituto nacional de Administración pública.
INE	Instituto nacional de estadística.
INSHT	Instituto nacional de seguridad e higiene en el trabajo.
INSS	Instituto nacional de seguridad social.
INTECO	Instituto nacional de tecnologías de la comunicación.
IMSERSO	Instituto de mayores y servicios sociales.

ISA	*Interoperability Solutions for European Public Administrations*, soluciones de interoperabilidad para las Administraciones públicas europeas.
ISACA	*Information Systems Audit and Control Association*, asociación de auditoría y control de sistemas de información.
ISM	Instituto social de la marina.
ISO	*International Standards Organization*, Organización internacional de normalización.
ISSS	*Information Society Standardization System*, sistemas de estandarización de la sociedad de la información.
ITSEC	*Information Technology Security Evaluation Criteria*, criterios de evaluación de la seguridad de las tecnologías de la información.
LAE	Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
LCSP	Ley 30/2007, de 30 de octubre, de contratos del sector público.
LEC	Ley 1/2000, de 7 de enero, de enjuiciamiento civil.
LFE	Ley 59/2003, de 19 de diciembre, de firma electrónica.
LGT	Ley 58/2003, de 17 de diciembre, general tributaria.

LOFAGE	Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración general del Estado.
LOPD	Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
LOPJ	Ley orgánica 6/1985, de 1 de julio, del poder judicial.
LORTAD	Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
LRJPAC	Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común.
MAGERIT	Metodología de análisis y gestión de riesgos de los sistemas de información.
MAP	Ministerio de Administraciones públicas.
MINHAP	Ministerio de hacienda y Administraciones públicas.
MSI	Mantenimiento del sistema de información.
MUFACE	Mutualidad de funcionarios civiles del Estado.
NCR	Número de referencia completo.
NSA	*National Security Agency*, Agencia de seguridad nacional norteamericana.

NIST	*National Institute of Standards and Technologies*, Instituto nacional de estándares y tecnologías.
OASIS	*Organization for the Advancement of Structured Information Standards*, Organización para el avance de estándares de información estructurada.
OBSAE	Observatorio de Administración electrónica.
ONTSI	Observatorio nacional de las telecomunicaciones y de la sociedad de la información.
PAe	Portal de Administración electrónica.
PDA	*Personal Digital Assistant*, asistente personal digital.
PEPS	*Pan European Proxy Services*, proxy de servicios pan europeo.
PILAR	Procedimiento informático y lógico de análisis de riesgos.
PIN	*Personal Identification Number*, número de identificación personal.
PKI	*Public Key Infrastructure*, infraestructura de clave pública.
PLCSP	Proyecto de ley de contratos del sector público.
PPT	Pliego de prescripciones técnicas.
PSI	Planificación de sistemas de información.
PYME	Pequeña y mediana empresa.

RA	*Registration Authority*, autoridad de registro.
RAE	Real academia española.
RCM	Real Casa de la moneda.
RCUD	Recurso de casación para unificación de doctrina.
REC	Registro electrónico común.
RFID	*Radio-Frecuency Identification*, identificación por radiofrecuencia.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (reglamento general de protección de datos).
ROI	*Return Of Investment*, retorno de la inversion.
ROSI	*Return Of Security Investment*, retorno de la inversión en seguridad.
RPM	Revista de procesos y métricas de las tecnologías de la información.
RPT	Relación de puestos de trabajo.
SAN	Sentencia de la Audiencia nacional.
SAP	Sentencia de la Audiencia provincial.

S.A.R.A.	Sujetos a regulación armonizada.
SCSP	Sustitución de certificados en soporte papel.
SEPE	Servicio de empleo público estatal.
SMS	*Short Message Service*, servicio de mensajes cortos/simples.
SOA	*Service oriented architecture*, arquitectura orientada a servicios.
SSTS	Sentencias del Tribunal supremo.
STC	Sentencia del Tribunal constitucional.
STIC	Seguridad de las tecnologías de la información y las comunicaciones.
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea.
STS	Sentencia del Tribunal Supremo.
STSJ	Sentencia del Tribunal Superior de Justicia.
SVD	Servicio de verificación de datos.
TDT	Televisión digital terrestre.
TEAR	Tribunal económico administrativo regional.
TECNIMAP	Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas.

TGSS	Tesorería general de la seguridad social.
TI	Tecnologías de la información.
TIC	Tecnologías de la información y las comunicaciones.
TIE	Tarjeta de identidad de extranjeros.
TJUE	Tribunal de Justicia de la Unión Europea.
TREBEP	Real decreto legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la ley del estatuto básico del empleado público.
TRLCSP	Real decreto legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la ley de contratos del sector público.
TSA	*TimeStamp Authority*, autoridad de sellado de tiempo.
TSJ	Tribunal superior de justicia.
VA	*Validation Authority*, autoridad de validación.
VPN	*Virtual Private Network*, red privada virtual.
VV.AA.	Varios autores.
W3C	*World Wide Web Consortium*, Consorcio WWW
WS	*Web Services*, servicios *web*.

1. INTRODUCCIÓN

Las siguientes páginas pretenden poner al descubierto la cara oculta de la Administración electrónica, aquellos aspectos de los que rara vez se oye hablar, desde la óptica de un observador jurídico, no tecnológico, si bien resultará inevitable invocar algunos términos técnicos que, precisamente por su desconocimiento por el ciudadano medio, levantarán barreras a la implantación exitosa de la nueva "Administración sin papeles".

Se ofrece al lector una aproximación inicial a los presupuestos que habilitan la existencia de ese nuevo paradigma desde un triple enfoque, que comienza con un acercamiento somero a los elementos tecnológicos que constituirán los ladrillos con los que construir la Administración electrónica. Le sigue un viaje cronológico a lo largo del camino que ha recorrido el Derecho hasta culminar en el actual marco jurídico europeo y nacional, un conjunto normativo que da forma a ese nuevo edificio que se quiere levantar. Por último, se revisan los aspectos operativos que pueden transformar esa emblemática construcción en una rígida pared contra la que se estrellan los ciudadanos, las empresas del sector privado e, incluso, los propios organismos públicos.

En sus primeros pasos, la Administración electrónica camina firme, dejando huella. Me atrevo a afirmar que va pisándonos a todos según avanza. La interconexión de las bases de datos de los organismos públicos crece y crece, día a día, gestando un enorme monstruo descontrolado. Nadie parece haber analizado la necesidad o el modo de sujetarlo, por lo que

propondré una modificación técnica sencilla que permitiría mantener bajo control a la bestia. Por otra parte, justificaré mi afirmación de que el legislador se ha precipitado al dar el pistoletazo de salida, imponiendo una relación electrónica, en muchos casos obligatoria, cuando las Administraciones públicas son aún incapaces de respetar el principio de neutralidad tecnológica, que les lleva a imponer restricciones indebidas al acceso a la información y a los servicios en función del *software* concreto que el interesado haya deseado instalar en su equipo informático, algo que la jurisprudencia no solo tolera, sino que impone a golpe de sentencia.

Una vez centrado el entorno en que nos movemos, planteo la gran cuestión que despierta mi preocupación. Los empleados públicos se sustituyen, progresivamente, por máquinas, como ha ocurrido reiteradamente desde la revolución industrial en los más diversos campos. Esos ordenadores no piensan, solo obedecen órdenes. Si el acto administrativo es un acto jurídico de voluntad, de juicio, de conocimiento o de deseo dictado por la Administración pública en el ejercicio de una potestad administrativa distinta de la reglamentaria, ¿quién le indica al ordenador cuál es esa voluntad, ese juicio, ese conocimiento o ese deseo?, es decir, ¿quién escribe las órdenes que dan vida al nuevo empleado público electrónico? En mi opinión, sin atisbo de duda, la respuesta ha de ser: la Administración pública que ejercita esa potestad administrativa. Por ello, analizaré las particularidades de los empleados públicos que están capacitados para escribir esos millones y millones de líneas de código y revisaré la situación actual, una realidad innegable por la que se concluye que, frecuentemente, las órdenes que recibe el nuevo empleado público electrónico no las ha escrito la Administración que defiende los intereses generales, sino empresas privadas movidas por un legítimo afán de lucro.

¿Realmente resulta ventajoso recurrir a la externalización del desarrollo del *software* público? En principio, parece que el sector privado tiene mucho que ganar reduciendo el tiempo dedicado a la programación y el número y sueldo de los recursos humanos asignados al proyecto, lo que aumenta el riesgo de que la calidad del *software* se resienta y las distintas dimensiones de la seguridad (autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad) se vean afectadas. Exponer cuáles son los riesgos y cómo pueden impactar puede ayudar a comprender la importancia de mantener el control del *software* que da vida a los ordenadores de nuestras Administraciones públicas. Pero no todo el proyecto que conduce al desarrollo de ese *software* resulta igual de crítico. Por ello, pretendo realizar un acercamiento a cada proceso involucrado, siguiendo la metodología creada por y para las Administraciones públicas, distinguiendo qué tareas podrían externalizarse y cuáles deberían quedar siempre depositadas en las manos de empleados públicos especializados.

Para finalizar, pretendo ilustrar, con algunos ejemplos, los diversos problemas que pueden ponerse de manifiesto por errores informáticos y cómo encararlos.

El tema escogido para esta tesis, la seguridad en el desarrollo del *software* de las Administraciones públicas, desde la óptica jurídica, ha sido poco tratado en la literatura especializada. Son abundantes los estudios técnicos sobre la seguridad del *software* en general, especialmente a nivel internacional, pero he preferido huir de este tipo de texto de forma intencionada, convencida de que escapa del alcance de este trabajo. Junto con la investigación bibliográfica del tema y la experiencia adquirida laboralmente a lo largo de dos décadas dedicadas a desarrollar *software* para el ámbito público, principalmente como funcionaria,

aunque con un breve y muy ilustrativo intermedio al servicio del sector privado, debo agradecer la inestimable ayuda de un grupo de desarrolladores externos que me ha mostrado las dificultades, cuando no imposibilidad, de superar las trabas que encuentran los ciudadanos, las empresas e, incluso, otros organismos públicos, para relacionarse electrónicamente con nuestras Administraciones.

Tras siete meses experimentando cómo se vive la Administración electrónica desde el otro lado, desde la vertiente del gestor público, no del técnico informático, descubro con sorpresa otra realidad que para mí era desconocida. ¿Cómo se puede informatizar la Administración y eliminar el papel con una dotación presupuestaria prácticamente inexistente? El legislador que ha impuesto la Administración electrónica ha olvidado indicarnos cómo vamos a pagarla. Contratos creativos desde el aspecto financiero, como el de colaboración pública privada, parecen tener sus días contados. El problema que me ha preocupado siempre, cómo conseguir una Administración electrónica segura, posiblemente deba ser sustituido por otro reto previo, cómo conseguir una Administración electrónica. Pero eso puede ser objeto de otra tesis doctoral.

2. LOS CIMIENTOS TECNOLÓGICOS DE LA eADMINISTRACIÓN

En su devenir histórico, la actividad administrativa ha evolucionado sin cesar, pero ha sido en los últimos años del pasado siglo XX cuando la investigación científica y los avances tecnológicos en campos como la microelectrónica, la informática y las

telecomunicaciones la han modificado en profundidad[1]. Superando su concepción inicial de mera herramienta, la informática consolida una vigorosa innovación tecnológica comparable a una tercera revolución industrial, donde las máquinas sustituyen a los empleados públicos y la actuación de la Administración se lleva a cabo sin la intervención de una persona física, lo que obliga a cuestionar algunas de las instituciones clásicas del Derecho administrativo[2].

"(…) *la moderna sociedad de la información ha matado a la distancia*" y lo ha hecho con armas tecnológicas, con las tecnologías de la información, que no son inocuas y que, como veremos, generan sus propios riesgos[3]. Pero, gracias a ello, hoy la Administración ofrece sus servicios desde dentro del hogar de los ciudadanos, siempre accesibles en todo lugar y momento[4], sin limitaciones de horarios ni impedimentos por la lejanía geográfica, sin que por las inclemencias del tiempo o la caída de la noche se cuelgue el cartel de "cerrado". El "empleado público electrónico" nos hace olvidar el "vuelva usted mañana" de Mariano José de Larra, nos atiende a horas intempestivas porque, no lo olvidemos, no tiene vida propia, como tampoco tiene amigos íntimos o enemigos manifiestos, parentesco o interés personal en el asunto. La máquina que nos sella la entrada de documentación en el registro telemático, la que resuelve un procedimiento de concurrencia competitiva sin intervención humana, la que calcula nuestros

[1] Aplicamos aquí a la actividad administrativa las afirmaciones que SUSANA RODRÍGUEZ ESCANCIANO dedica a la tecnificación de los procesos productivos en la relación laboral, en su obra de 2015 *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores.*
[2] CANTERO MARTÍNEZ, J. (2011), principio de transparencia, 308-315. A ello se refiere la autora cuando analiza la incidencia de la tecnología en el paradigma de la abstención y recusación en actos administrativos dictados sin intervención humana a través de una mera aplicación informática.
[3] ESTEVE PARDO, J. (2003), ciencia y Derecho, 138.
[4] Sobre la crisis de las nociones de espacio y de tiempo en el que denomina "Derecho público electrónico", *vid*. BERNADÍ GIL, X. (2005), Derecho público.

impuestos o monitoriza nuestras constantes vitales y dispara las alarmas, no piensa[5], se limita a ejecutar las instrucciones que recibe.

Las generaciones más jóvenes no son capaces de imaginar un mundo sin televisión, sin ordenadores o sin Internet, y ninguno de nosotros, probablemente, renunciaría a los estos avances tecnológicos que configuran la vida tal y como hoy la conocemos. Pero hay algo más que no estamos dispuestos a abandonar, la seguridad, que "*se ha constituido en un componente esencial para la calidad de vida*"[6].

Resulta imposible profundizar en el concepto de seguridad informática y de la información sin acercarse antes a la noción de riesgo, especialmente a su componente tecnológico, con la importante carga de complejidad que conlleva, conocida y dominada, aunque no siempre, por los profesionales y expertos del sector[7]. Se trata de un entorno altamente mutable. La época actual se caracteriza no solo por el uso de las tecnologías de la información y las comunicaciones, las TIC, sino por la brusquedad de sus cambios, lo que ha llevado a Gamero Casado a reflexionar sobre una "era de la disrupción" en lugar de la tradicional "era de la información"[8].

La implantación de la Administración electrónica pasa necesariamente por el tratamiento de tres tipos de factores: esos cambiantes aspectos tecnológicos recién aludidos, las

[5] El estudio de las bases de la inteligencia artificial excede de los propósitos de un estudio jurídico. Conforme al estado del arte en esta materia, nuestro "*empleado público electrónico*" es una máquina que no piensa, que se limita a ejecutar las instrucciones que se le proporcionan a gran velocidad.
[6] CASTILLO BLANCO, F.A. (2003), principio de seguridad jurídica, 22.
[7] ESTEVE PARDO, J. (2003), ciencia y Derecho, 147. El autor se refiere concretamente a los riesgos para la salud, aunque su afirmación parece igualmente adecuada para nuestro campo tecnológico.
[8] GAMERO CASADO, E. (2015), mundo en disrupción, 2-3.

bases jurídicas sobre las que se apoya y que le sirven de sujeción, y determinados conceptos operativos[9].

Aunque el instinto nos empuje a pensar que las mayores dificultades para su construcción provienen del elemento técnico, una mirada por las páginas siguientes aportará suficientes motivos para, al menos, cuestionar dicha idea. Los instrumentos tecnológicos son los ladrillos de este nuevo edificio y de su calidad dependerá la solidez del conjunto, pero serán la mente del arquitecto que lo proyecte y las manos artesanas que lo levanten las que alzarán una simple tapia o un rascacielos.

Iniciaremos ese recorrido con una somera aproximación a las materias primas con las que levantar la nueva eAdministración, para continuar revisando el marco jurídico que la regula y los detalles operativos que ralentizan o impulsan su despliegue, con la mirada puesta en detectar la posible incidencia de cada uno de esos factores en la seguridad del *software* que da vida al nuevo "funcionario electrónico".

El ordenador, una de las innovaciones tecnológicas más relevantes de la historia, llega a las Administraciones públicas en el siglo pasado, allá por la década de los sesenta, dando inicio a un proceso de automatización administrativa[10] que, tras una imparable evolución gradual, se ha alejado de aquel incipiente y básico uso como mera máquina de escribir y se ha sumergido masivamente en esa nueva era de la información, la cual, para la Administración pública y para el Derecho administrativo, supone la emergencia de un nuevo conjunto de

[9] GALÁN PASCUAL, C./ MAROTO ILLERA, R. (2013), gobierno electrónico, 23.
[10] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 47 y ss.

actuaciones jurídicas y materiales para las que se ha acuñado la denominación genérica de Administración electrónica[11].

Con aquella informatización inicial comenzó una fase de adquisición, por la Administración, del *software* adecuado para la realización de las tareas administrativas[12], una etapa que nunca puede darse por completada, continuando en la actualidad, puesto que, como acertadamente señala Martínez Gutiérrez, "*la frenética evolución de las tecnologías de la información y la comunicación provoca un proceso de cambio continuo*"[13]. El informe REINA 2016 nos proporciona los indicadores más representativos de la situación y uso de los sistemas y TIC en la AGE, señalando un ascenso del 2,25% con respecto al periodo anterior, mientras que el personal especializado apenas varía[14].

La aparición de Internet y la profusión de terminales entre ciudadanos y empresas, han contribuido a acelerar esa introducción de las TIC en las Administraciones públicas[15]. Como efecto colateral, Internet, al extender los límites de la Administración y cambiar su perímetro, lo ha expuesto[16] a un amplísimo universo de amenazas remotas[17], muchas difícilmente

[11] GAMERO CASADO, E. (2008), era de la información, 30.
[12] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 51.
[13] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 53.
[14] Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2016/Noviembre/Noticia-2016-11-18-Publicacion-del-Informe-REINA-2016.html#.WGVyJ1wbgmM (29 de diciembre de 2016).
[15] ALABAU MUÑOZ, A. (2004), la Unión Europea, 31.
[16] Sería erróneo e ingenuo pensar que una Administración resultaría demasiado pequeña para ser objetivo de ataques cibernéticos. Como muestra, podemos citar al Gobierno de Cantabria, que recibe miles de ataques al año, provenientes de China, Rusia, Estados Unidos o el Estado Islámico. La noticia se ha publicado en la edición digital del periódico El Diario Montañés. http://www.eldiariomontanes.es/cantabria/201605/08/gobierno-blinda-ante-ciberataques-20160507205826.html (19 de mayo de 2016).
[17] MAÑAS ARGEMÍ, J.A. (2003), confianza, 61.

imaginables[18]. A su vez, ha desplegado un gran abanico de posibilidades y unas nuevas exigencias por parte de los ciudadanos hacia sus Administraciones públicas, quienes demandan una transformación notable en la prestación de sus servicios. Ya no es suficiente publicar por Internet lo mismo a lo que antes se accedía por ventanilla. La nueva Administración debe facilitar a los ciudadanos y a las empresas las condiciones adecuadas para que puedan relacionarse con ella de forma telemática, eliminando la necesidad de conocer la estructura administrativa interna, anticipando la información necesaria para la realización de los trámites precisos y ofreciendo la posibilidad de no volver a presentar documentación disponible o accesible por los propios organismos administrativos.

Catalizadora de esa transformación resulta nuestra coyuntura económica, que obliga a buscar modelos más eficientes que colaboren a la contención del gasto[19]. Muestra de esa nueva filosofía es la tramitación electrónica de los procedimientos administrativos, que supuso en 2014 un ahorro estimado de 20.000 millones de euros para empresas, ciudadanos y Administraciones públicas[20].

[18] Los ejemplos disponibles para ilustrar esta afirmación podrían dar lugar a una enciclopedia del cibercrimen. Escogiendo uno de los incluidos en las actas de las V jornadas de estudios de seguridad del Instituto universitario General Gutiérrez Mellado y UNED, celebradas en Madrid el 7, 8 y 9 de mayo de 2013, página 1252, es destacable el descubrimiento, en 2013, de "Octubre Rojo", una red de ciberespionaje dedicada durante seis años antes al robo de información sensible o clasificada de gobiernos y corporaciones privadas, la cual, habiendo establecido conexiones fraudulentas en 55.000 ordenadores, constituye una de las mayores amenazas cibernéticas en Europa y Asia. Dicha red dispone de una compleja estructura compuesta por servidores en 39 países, preferentemente en Alemania y Rusia, y cuenta con 60 dominios y 250 IP diferentes. España representa el 2% de las infecciones producidas.

[19] MONTALBÁN CARRASCO, R. (2013), impulsoras de la transformación, 118.

[20] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO (2015), informe anual 2014, 18.

Para afianzar esta nueva Administración electrónica, es preciso cuidar dos aspectos vitales, concretamente la seguridad y la confianza en ella[21]. Las personas evitamos lo que no nos inspira confianza[22]. La perdemos con facilidad ante una mala experiencia y la recuperamos con creciente dificultad. Se incrementa con la satisfacción de las expectativas y disminuye con las sorpresas negativas. Aunque la confianza es mayor sin fallos, si el producto defectuoso se sustituye por otro impecable con prontitud aún es posible rehabilitarla. Pero, mientras la confianza es algo subjetivo, que recae en el terreno de psicólogos y sociólogos, la seguridad implica connotaciones técnicas que nos llevan al campo de los ingenieros, de los matemáticos, de los físicos… Con una mirada rápida nos acercaremos al extenso mundo de estas ciencias que buscan esa anhelada seguridad.

2.1. LA INGENIERÍA DEL *SOFTWARE*

Se entiende por ingeniería del *software* el establecimiento y uso de principios de ingeniería robustos, orientados a obtener *software* económico que sea fiable, cumpla los requisitos previamente establecidos y funcione de manera eficiente sobre máquinas reales[23]. Lo que no hemos concretado aún es el propio concepto de *software*, el de programa o, descendiendo aún más, el de instrucción. Esbozando su utilidad, nos proporciona unas primeras nociones Peter Norton, el reputado informático conocido por su célebre antivirus, cuando explica didácticamente que todas las computadoras son básicamente similares, operan bajo los mismos

[21] MAÑAS ARGEMÍ, J.A. (2003), confianza, 58-60.
[22] El 45,3% de los usuarios confía mucho o bastante en Internet y tan solo un 1,4% muestra un alto grado de desconfianza, según datos del informe MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO (2015), informe anual 2014.
[23] RODERO RODERO, J.A. (2001), auditoría del desarrollo, 261-262.

principios, están hechas con los mismos componentes básicos y requieren de instrucciones para poder funcionar, las cuales las controlan y les dicen lo que debe hacer[24].

Para la edición 23 del diccionario de la RAE, un programa, conforme a su acepción 12ª, es el "*conjunto unitario de instrucciones que permite a una computadora realizar funciones diversas, como el tratamiento de textos, el diseño de gráficos, la resolución de problemas matemáticos, el manejo de bancos de datos, etc.*". El diccionario recoge también la voz inglesa *software*, la cual define como el "*conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora*". Menos académica pero más visual es la explicación del propio Peter Norton: "*el software hace que la máquina cobre vida*"[25] y consiste en instrucciones que indican a los componentes físicos de la maquina lo que deben hacer. Pero el término *software* no es exactamente un sinónimo de programas, sino que engloba tres componentes, uno de los cuales es, precisamente, el conjunto de programas. A ellos habrá que añadir, en primer término, los datos necesarios para manejar y probar los programas y las estructuras requeridas para mantener y manipular esos datos. La terna se completa con la documentación que describe la operación y el uso del programa[26]. En el mismo sentido, el artículo 96 del real decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la ley de propiedad intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, considera que la expresión "programas de ordenador" comprende su documentación preparatoria, y extiende la misma protección a la

[24] NORTON, P. (2006), introducción a la computación, 3-4.
[25] NORTON, P. (2006), introducción a la computación, 32.
[26] LABORATORIO NACIONAL DE CALIDAD DEL *SOFTWARE* (INTECO) (2009), ingeniería del *software*, 8.

documentación técnica y a los manuales de uso. Por ello, al hablar de seguridad del *software*, es preciso considerarlo en su dimensión más amplia.

Durante años se ha debatido si el desarrollo del *software* es un arte o una ciencia[27]. La belleza y elegancia del código se manifiesta en su fácil lectura y modificación, en su utilidad, flexibilidad, eficiencia… Puede leerse código bello solo por placer, pues el código es capaz de provocar satisfacciones emocionales e intelectuales, pero también dolor al que lo lee[28]. El prestigioso autor de la biblia de los informáticos, "*The Art of Computer Programming*", Donald E. Knuch, afirma que "l*a programación es un arte, porque aplica el conocimiento acumulado al mundo, porque requiere habilidad e ingenio y, sobre todo, porque produce objetos bellos. Un programador que subconscientemente se ve a sí mismo como artista disfrutará de lo que hace y lo hará mejor"*[29].

Protegido como propiedad intelectual[30], el *software* ha sido considerado no patentable en la normativa española. El artículo 4.5 de la nueva ley 24/2015, de 24 de julio, de patentes, excluye específicamente a los programas de ordenador, a las obras artísticas y científicas e, incluso, a los métodos matemáticos, pero en su apartado quinto reabre la polémica con la adición de la cláusula "como tal", que abriría la puerta a la patentabilidad del *software* cuando vaya asociado a algo más. Ello dificulta de forma desmedida la tarea de los

[27] SCHAULL, S.F. (2011), desarrollo de *software*, 7.
[28] Sin duda, dolor de cabeza, una sensación sufrida con excesiva frecuencia por quienes han de mantener el *software* ajeno y que comenta PÉREZ ABELEIRA, M.A. (2006), la belleza del *software*, 60.
[29] KNUTH, D.E. (1974), *Programming as an Art*, 673.
[30] El precitado real decreto legislativo 1/1996 dedica el título VII del libro I – Método, a los programas de ordenador. Aunque protege con derechos de autor los programas y su documentación, deja fuera de esa cobertura tanto las ideas como los principios en los que se basan cualquiera de los elementos de un programa de ordenador, incluso los que sirven de fundamento a sus interfaces.

desarrolladores, obligados a averiguar si las ideas que le van surgiendo durante el proceso están patentadas. En palabras de Richard Stallman, fundador del movimiento por el *software* libre, "*en EE. UU. hay, según creo, cientos de miles de patentes de software, por lo que hacer un seguimiento de ellas sería un trabajo tremendo. De manera que habrá que buscar las patentes pertinentes. Y se encontrará un montón de ellas, pero no necesariamente todas*"[31]. En dos décadas de ejercicio profesional no he conocido a ningún desarrollador que se haya planteado la posibilidad de que el código que estaba programando pudiera estar protegido por patente alguna.

Las licencias son autorizaciones formales de tipo contractual otorgadas por el autor al interesado en realizar actos de explotación del *software*[32]. En función de los derechos que el autor se reserve sobre la obra, suelen clasificarse en dos tipos, ambos presentes en las Administraciones públicas. El primero de ellos, en clara regresión, es el ***software* propietario**. Denominado en ocasiones cerrado, privativo o no libre, es protegido contra la copia, modificación o redistribución, con o sin modificaciones, y habitualmente su utilización requiere el abono de una cantidad económica determinada[33]. Desde la entrada en vigor de la ya derogada LAE, el ciudadano tiene derecho a que la Administración no establezca obstáculos técnicos basados en la incompatibilidad de programas y aplicaciones que no respondan al uso de estándares abiertos, por lo que el recurso al *software* propietario que impida ese acceso solo se concibe con carácter complementario[34]. Habitualmente conserva oculto el código fuente, sin que sea posible acceder a él para saber lo que hace con exactitud, para mejorarlo o adaptarlo a las

[31] http://www.gnu.org/philosophy/danger-of-*software*-patents.es.html
[32] *Vid*. MINHAP (2015), licenciamiento de activos.
[33] INTECO (2012), estudio sobre riesgos de seguridad, 22.
[34] VALERO TORRIJOS, J. (2008), acceso a los servicios, 250.

necesidades propias[35]. A modo de ejemplo, por su tradición en las Administraciones públicas españolas, podemos citar el lenguaje de programación NATURAL asociado a la base de datos ADABAS, sistema propietario de la empresa "*Software* AG", quien ha declarado haber registrado en 2013 la facturación en licencias más alta de toda la historia de la compañía hasta el momento[36]. Los desarrolladores de la Administración pueden programar libremente lo que deseen en lenguaje NATURAL; no pierden esa capacidad por el hecho de tratarse de un *software* propietario. El problema no radica ahí, sino en toda la infraestructura para usarlo, que requerirá pagar las oportunas licencias, en absoluto económicas. Además, se verá limitado a utilizar lo que esa infraestructura le ofrezca, se ajuste a sus necesidades con facilidad o no, sin disponer de más alternativas asumibles. Habida cuenta de la dificultad, muchas veces incluso inviabilidad, de migrar todo el sistema informático a otras soluciones, la Administración puede verse convertida en prisionera de su pasado, condenada a la cautividad tecnológica en el presente y, previsiblemente, en un próximo futuro.

La segunda opción, ampliamente defendida en la actualidad en la Administración pública, es el ***software* libre** (*free software*)[37], denominado así por las libertades de que disfrutan los usuarios del mismo, definidas por *The Free Software Foundation*, distinguiendo las siguientes[38]:

[35] MARTÍNEZ ZORRILLA, D. (2009), *software* libre, 2.
[36] Recuperado de http://www.computerworld.es/negocio/software-ag-obtiene-facturacion-record-de-licencias-en-2013 (29de diciembre de 2016).
[37] No debe confundirse con el *freeware* o *software* gratuito, que es un tipo de *software* en el que la licencia es gratuita.
[38] Recuperado de https://www.gnu.org/philosophy/free-sw.es.html (2 de abril de 2017).

Libertad 0	Ejecutar el programa como se desee, con cualquier propósito
Libertad 1	Estudiar cómo funciona el programa y modificarlo, adaptándolo a las necesidades de cada usuario. Ello requiere el acceso al código fuente.
Libertad 2	Distribuir copias del programa, lo que permite ayudar al prójimo.
Libertad 3	Distribuir copias de sus versiones modificadas a terceros, permitiendo que toda la comunidad se beneficie de las mejoras. Ello también requiere acceso al código fuente.

Por tanto, la diferencia entre *software* libre y propietario es una cuestión de cariz jurídico relacionada con la propiedad intelectual, concretamente con los derechos de autor[39]. Entre sus ventajas se puede destacar el ahorro en la adquisición de licencias, la independencia de los proveedores, la facilidad para adaptar los programas a los requerimientos específicos, la reutilización del código, con los consiguientes ahorros por las economías de escalas, o la posibilidad de acceder al mismo, lo que permite solucionar eventuales errores con agilidad.[40] A su vez, al disponer de su código fuente, facilita la interoperabilidad y fomenta la confianza, por la transparencia de su codificación en vez de la opacidad de una caja negra, así como por su sometimiento al escrutinio de los ciudadanos y de expertos independientes.[41]

[39] MARTÍNEZ ZORRILLA, D. (2009), *software* libre, 3.
[40] GONZÁLEZ CALDERÓN, C./ FERRÁN RIERA, O. (2009). *software* libre, 27-29.
[41] HUERTAS MÉNDEZ, F.A. (2009), elemento de desarrollo, 44-46.

Más compleja resulta la diferenciación entre el *software* libre[42] y el ***software* de código abierto**, apoyado por *Open Source Initiative*. Las diez premisas del código abierto[43], de forma resumida, son las siguientes:

Libre distribución	Gratuito o mediante venta.
Acceso al código fuente	
Trabajos derivados	La licencia debe permitir modificaciones y trabajos derivados, así como su distribución en los mismos términos que la licencia del software original.
Integridad del código fuente del autor	La licencia puede restringir la distribución del código modificado mediante parches, o un nombre o versión diferente.
Sin discriminación de personas o grupos	
Sin discriminación por áreas de trabajo específico	
Distribución de la licencia	Los derechos vinculados al programa deben aplicarse a todos aquellos a quienes se redistribuye, sin necesidad de una licencia

[42] RODRÍGUEZ, G.S. (2008), *software* libre, 175. El autor comenta cómo dentro del movimiento en favor del *software* libre surgió una especialidad distinguida por el término *open source software*, con una ideología diferente de la de su fundador, Stallman, pero que, a ciertos efectos, pueden considerarse sinónimos.
[43] Recuperado de https://opensource.org/docs/osd (2 de abril de 2017).

	adicional.
La licencia no debe ser específica para un producto	Los derechos vinculados al programa no deben depender de que este sea parte de una distribución de software mayor.
La licencia no debe restringir otro software	La licencia no debe establecer restricciones en otro software que se distribuya con él, ni siquiera imponer que todos los demás programas sean de código abierto.
La licencia debe ser tecnológicamente neutral	Ninguna disposición de la licencia puede basarse en cualquier tecnología individual o estilo de interfaz.

Un análisis detallado de la diferenciación entre el *software* libre y el código abierto excede del ámbito de este trabajo. A los efectos que nos ocupan, podrían considerarse sinónimos, hasta tal punto que el ENI, en su glosario de términos, define la "aplicación de fuentes abiertas" como aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios, lo que más bien parece identificarse mucho más con las cuatro libertades que describen al *software* libre que con las diez premisas que caracterizan el *software* de fuentes abiertas.

Las aplicaciones de los organismos públicos declaradas como de fuentes abiertas por la Administración han de permitir ser ejecutadas para cualquier propósito, dar a conocer su

código fuente, modificarse o mejorarse y, por último, redistribuirse a otros usuarios, con o sin cambios, siempre que la obra derivada mantenga estas mismas cuatro garantías[44]. El legislador hace referencia también al uso de estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos, en el artículo 38.5 de la ley 40/2015[45].

El proceso de publicación de código y revisión por todos los internautas que lo deseen puede ayudar a depurar y mejorar el *software* y a luchar contra los ciberatacantes, gracias a la colaboración de la sociedad para descubrir y reparar defectos, aunque puede discutirse la conveniencia de exponer a ojos ajenos el código de las aplicaciones de nuestra Administración, por la posibilidad de poner al descubierto vulnerabilidades cuya publicidad podría suponer riesgos notables. Decantarse por un sí o un no, sin matices, podría resultar precipitado. Aunque la informática se base en ceros y unos, las respuestas a muchas de sus preguntas no pueden contestarse en blanco y negro, sino en una variada gama de tonalidades grises. Cuestiones como si Java es o no *software* libre no son fáciles de responder, pues si determinado *software* libre necesita, por ejemplo, de un compilador o de un intérprete o de una biblioteca que no es libre, presenta una dependencia que limita su libertad[46], por lo que sería necesario pronunciarse sobre cada una de las implementaciones de Java disponibles por separado.

Incluso la variedad en la oferta de *software* libre y la posibilidad de modificarlo a voluntad para ajustarlo a las necesidades concretas de cada instalación, puede causar problemas a la hora de compartir aplicaciones entre diferentes Administraciones. Con muy buena voluntad,

[44] Así se recoge en el artículo 16 del ENI, el cual prevé la aplicación de la licencia pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos.
[45] *Vid*. VALERO TORRIJOS, J. (2008), acceso a los servicios, 249.
[46] *Vid.* www.gnu.org/philosophy/java-trap.es.html

una Comunidad autónoma puede ceder sus aplicaciones a otra de forma gratuita, pero el coste de hacer funcionar ese aplicativo en la receptora puede llegar a ser tan elevado y acarrear tantas vulnerabilidades potenciales que lo convierta en un regalo envenenado, resultando mucho más rentable comenzar el desarrollo desde cero.

Las Administraciones públicas usuarias de *software* libre, al menos sobre el papel, ya no se ven prisioneras de un fabricante, puesto que pueden comparar y escoger el entorno, la infraestructura con la que quieren trabajar, e incluso pueden mejorarla para que se adapte a sus necesidades, lo que no evita la dependencia del proveedor externo que programa sus aplicaciones, quien tiene en su mano un arma poderosa, el poder que le proporciona el conocimiento de ese *software* que únicamente se obtiene al crearlo, como se tratará *infra*. Se estima en 1.100 millones de euros perdidos cada año en el sector público de la Unión Europea por este concepto de cautividad, entendiendo como tal la situación en la que la autoridad pública no puede cambiar fácilmente de proveedor por no disponer de toda la información esencial sobre el sistema para que otro proveedor pueda hacerse cargo del mismo eficientemente[47].

Fuera de la discusión de si es arte o es ciencia, si se usa *software* libre o propietario, queda una verdad incuestionable: tanto el artista como el científico cometen errores. El *software* falla con elevada frecuencia[48]. El autor que nos acompañó a los profesionales del

[47] *Vid*. la comunicación de 2013 de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones contra la dependencia de un proveedor: construir sistemas de TIC abiertos mediante una mejor utilización de normas en la contratación pública, COM/2013/0455 final, descargada de http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52013DC0455&rid=1 (30 de diciembre de 2016).

[48] Constatando una realidad que ni desarrolladores negamos ni puede ser ignorada por los usuarios, algunos se han atrevido a aventurar una cifra de alrededor del 60% de fallos, como recoge la Asociación de técnicos de informática, ATI (2008), en su *Revista española de innovación, calidad e ingeniería del software (REICIS) 4* (2), 8.

sector en nuestros primeros pasos por el mundo de la informática, Roger S. Pressman[49], afirma que los defectos ocultos ocasionan tasas elevadas de fallos al inicio de la vida de un programa, estabilizándose con el tiempo según van siendo depurados los errores, de forma que se aplana la curva que manifiesta la evolución de la tasa de fallos con respecto al tiempo, alcanzando un nivel estable. Sin embargo, durante su vida, el *software* puede (y probablemente debe) sufrir cambios[50], cada uno de los cuales podría provocar un incremento brusco de la tasa de fallos, reflejado en un pico en la curva. Depurando los errores detectados, la tasa de fallos recupera su tendencia a estabilizarse, pero es habitual que, antes de alcanzar de nuevo un nivel estable, sobrevenga otro cambio diferente que vuelve a disparar los errores. Esta actividad cíclica provoca el incremento progresivo del nivel mínimo de la tasa de fallos, que Pressman describe como el "deterioro del *software*" como consecuencia del cambio.

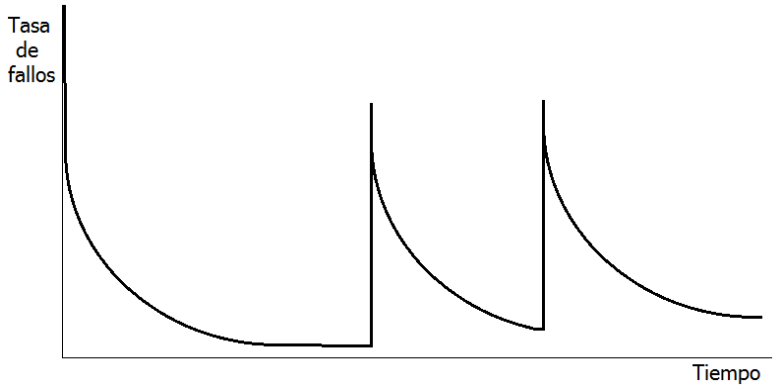

Figura 1: Curva de fallos del *software*

FUENTE: Adaptación de la curva de fallos del *software* incluida en PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 5.

[49] PRESSMAN, R.S. (2010), i*ngeniería del software. Un enfoque práctico*, 4-5.
[50] Señala el autor que muchas veces se solicitan cambios incluso antes de que se disponga de la primera versión.

Clásico en el ámbito de la programación de ordenadores es el estudio que Boehm y Papaccio efectuaron, en 1988, sobre la estimación del coste de la corrección de errores en las diversas etapas del *software*, calculando que la resolución de un error detectado cuando el programa ya está en producción cuadruplica el coste que hubiera supuesto su reparación si se hubiera localizado en fases tempranas[51].

No se puede pretender obtener una demostración formal de la absoluta corrección de un aplicativo, pues la ingeniería del *software* se asemeja más a la medicina que a las matemáticas. La imperfección e impredecibilidad del *software* pertenecen a su naturaleza intrínseca. Un error tan mínimo como la omisión indebida de una coma puede desencadenar un comportamiento totalmente diferente del debido y esperado.[52]

A pesar de conocer la evolución de la curva de fallos, tampoco resulta viable evitar el deterioro del *software* eliminando la ejecución de cambios en la codificación de los programas, a pesar del elevado coste del mantenimiento de las aplicaciones, estimado entre un 60 y un 70% de los recursos del desarrollo total[53]. La ejecución de cambios surge como respuesta a una necesidad. En función de cuál sea esta, el mantenimiento se clasifica en una de las cuatro siguientes modalidades[54]:

---

[51] BOEHM, B.W./ PAPACCIO, P.N. (1988), *Software Costs*, 1466.
[52] *Vid*. GÉNOVA, G., GONZÁLEZ, M.R. Y FRAGA, A. (2007), *Ethical Education in Software Engineering*, 10.
[53] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 656.
[54] Las denominaciones de los distintos tipos de mantenimiento varían entre diferentes autores. Se recoge aquí la clasificación incluida en el documento correspondiente al proceso de mantenimiento de sistemas de información, de la metodología Métrica versión 3, 1.

Correctivo	Reparación de los errores detectados
Evolutivo	Modificaciones necesarias para cubrir la expansión o cambio en las necesidades del usuario
Adaptativo	Cambios a realizar como consecuencia de variaciones en los entornos en los que el sistema opera (configuración del hardware, *software* de base, gestores de bases de datos, comunicaciones…)
Perfectivo	Acciones emprendidas para mejorar la calidad interna de los sistemas, como la reestructuración del código, su definición más clara y la optimización del rendimiento y la eficiencia

Muestra de la indispensable necesidad de mantener el *software* de las Administraciones públicas actualizado, es la problemática surgida con referencia al entorno de ejecución de los *applets* de Java en navegadores *web*[55], que está sufriendo continuas vulnerabilidades de seguridad hasta el punto de convertirse en un peligro que hace desaconsejable su instalación[56]. Navegadores como Chrome[57] ya no lo permiten, lo que ha

[55] Para mayor información puede consultarse la *web* de IBM http://www.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzaj4/rzaj45bejavasecuri ty.htm?lang=es (23 de marzo de 2016).
[56] IDOATE GIL, A./ GARCÍA-MERÁS CAPOTE, T. (2013), práctica de la neutralidad, 6.
[57] Para mayor información se puede consultar la *web* de java https://www.java.com/es/download/faq/chrome.xml (23 de marzo de 2016).

provocado que aplicaciones de nuestras Administraciones públicas[58] hayan dejado de funcionar, casi de un día para otro, pasando a requerir un proceso de mantenimiento que en absoluto resulta sencillo ni inmediato. Pero la necesidad de mantener actualizado el *software* de las Administraciones públicas no tiene su origen únicamente en motivos técnicos como el comentado. La adaptación a los cambios en el ordenamiento jurídico se convierte en una obligación ineludible. A título ilustrativo, cabe señalar las consecuencias sobre las aplicaciones informáticas públicas ocasionadas por el reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la directiva 1999/93/CE, conocido como reglamento eIDAS, el cual entró en vigor el pasado 1 de julio de 2016. A él se unen las modificaciones requeridas por la decisión de ejecución (UE) 2015/1506, la ley 40/2015 de régimen jurídico del sector público y el real decreto 668/2015. Los citados cambios normativos[59] influyen en la plataforma @firma[60] y han desencadenado la actualización de todas las aplicaciones que la utilizan en la medida en que haya podido ser necesario para mantenerlas en funcionamiento[61].

---

[58] *Vid*. JUNTA DE ANDALUCÍA. CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA (2013), plataforma @firma.

[59]Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2016/Marzo/Noticia-2016-03-18-Cambios-en-Plataforma--firma-asociados-al-reglamento-eIDAS-.html (17 de mayo de 2016).

[60] @firma es la plataforma de validación y firma electrónica multi-PKI, que el MINHAP pone a disposición de las Administraciones públicas, proporcionando servicios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva. Recuperado de http://administracionelectronica.gob.es/ctt/afirma#.VzuOdr5WgSk (17 de mayo de 2016). El número de transacciones realizadas con esta plataforma en el año 2015 fue de 291.824.395 operaciones. Recuperado de http://administracionelectronica.gob.es/ctt/afirma/mas#.VzuLjr5WgSk (17 de mayo de 2016).

[61] Los datos que devuelve @firma a las aplicaciones informáticas que invocan sus servicios, en el caso de un certificado europeo no español, variarán en función del prestador de servicios de certificación involucrado en el caso concreto, dificultando el traslado de la información a las pantallas de las propias aplicaciones, lo que no ocurría

Aceptada la indefectible necesidad de mantener el *software* y, con ella, el posible deterioro que vaticina Pressman, es preciso añadir que la crisis del *software*[62] no se limita a la elevada tasa de fallos. La insatisfacción también llega de la mano de la incapacidad de terminar los proyectos a tiempo y dentro del presupuesto planificado, aspecto muchas veces relacionado con una inadecuada gestión y priorización de la demanda, que lleva a asumir múltiples proyectos simultáneamente sin los recursos necesarios, fracasando y causando la pérdida de recursos corporativos. La priorización y evaluación de proyectos basadas en factores como su valor estratégico, valor financiero, riesgo, adecuación a sistemas existentes, tiempo de ejecución, capacidad de la organización y complejidad técnica[63], han de completarse en las Administraciones públicas con otros aspectos intangibles, como los que apuntan en la actualidad las nuevas leyes administrativas, que vienen imponer el procedimiento administrativo electrónico. La gestión de la demanda se vuelve imprescindible y el incumplimiento de la ley se puede dar por garantizado, ante el exceso de trabajo recaído sobre unos recursos humanos y materiales limitados.

---

cuando @firma únicamente validaba certificados de prestadores nacionales. Ahora será habitual encontrar campos nulos donde antes se devolvía información obligatoriamente, mientras que diversos datos útiles se aglutinan sin estructura fija en un solo lugar. Aquellas de nuestras Administraciones públicas que reaccionen antes estas dificultades volviendo la mirada hacia otro lado, admitiendo únicamente certificados españoles bajo la excusa inaceptable de que la presencia de ciudadanos europeos no nacionales es minoritaria, no solo estarán incumpliendo sus obligaciones de forma totalmente irresponsable, sino que únicamente conseguirán retrasar lo inevitable por un breve periodo de tiempo, a costa de un importante daño en la imagen y prestigio de nuestra Administración y en la confianza de la ciudadanía. Los responsables del *software* de las Administraciones públicas deben reaccionar proactiva y diligentemente en el sentido de dar cumplimiento al ordenamiento jurídico.

[62] La crisis del *software*, término acuñado en 1968, es una enfermedad crónica que hace referencia a la imposibilidad endémica de entregar productos *software* dentro del calendario establecido, con la calidad pactada y que no excedan del coste previsto, problema que tratan de afrontar en COLOMO PALACIOS, R./ TOVAR CARO, E./ GÓMEZ BERBIS, J.M./ GARCÍA CRESPO, A. (2007), recomendaciones.

[63] AGUILAR ALONSO, I./ CARRILLO VERDÚN, J./ TOVAR CARO, E. (2008), demanda de TI, 25-26.

Por último, cabe señalar que los defectos del *software*, evidentemente, son un problema no solo en sí mismos, sino que abren la puerta de entrada a los ataques llevados a cabo por aquellos programas dañinos que se conciben específicamente para explotar sus vulnerabilidades, como los independientes gusanos o zombis, o los que necesitan alojarse dentro de otro programa, como trampas, bombas lógicas, caballos de troya o virus. Entre ellos figura un viejo conocidos de los desarrolladores, incluso de los que son empleados públicos, la trampa, como se denomina a una entrada secreta a un programa que elude todos los controles de acceso. Con frecuencia es introducida lícitamente en el *software* por sus programadores, con la intención de facilitar las pruebas y la depuración del código desarrollado de una forma rápida y cómoda[64]. Los problemas surgen cuando ese *software* llega a ponerse en producción sin haber eliminado previamente esa puerta secreta, y se agravan cuando ello ha ocurrido malintencionadamente, pudiendo incluso iniciar la ejecución de un fragmento de código escondido de funcionalidad desconocida, una bomba lógica, o genéricamente *malware*, descrito por INCIBE como "*cualquier tipo de software malicioso o molesto que puede instalarse en los sistemas informáticos para llevar a cabo acciones sin el conocimiento del usuario*"[65]. Coincido con la opinión de William Stallings referente a que, ante la dificultad de instalar controles para detectar trampas, "*las medidas de seguridad deben centrarse en el desarrollo del programa y en las actividades de actualización del software*"[66] y, por ello, en este trabajo, se revisarán las tareas involucradas en la obtención del *software* de las Administraciones públicas desde la óptica de su seguridad. En la actualidad, esos programadores no siempre serán empleados públicos. Es más,

[64] STALLINGS, W. (2004), fundamentos de seguridad en redes, 342-343.
[65] INTECO (2012), desmontando el *malware*.
[66] STALLINGS, W. (2004), fundamentos de seguridad en redes, 343.

puede que ni siquiera hablen nuestro idioma ni pisen nuestro mismo continente. Hace ya más de dos décadas, con las primeras técnicas de *outsourcing*, surge el desarrollo global de *software* (DGS), hoy ya consolidado, que posibilita que las empresas alcancen una disminución de costes intentando mantener el nivel de calidad. Permite contar con desarrolladores localizados físicamente por todo el mundo, que producen *software* a precios más bajos para clientes remotos. Las dificultades versan sobre problemas de comunicación para el intercambio de conocimientos e información, retos en la coordinación de tareas y desafíos en el control de la gestión del proyecto para el cumplimiento de calendario, presupuesto, calidad, estándares…, problemas todos ellos acentuados por la distancia geográfica que, simultáneamente, va asociada a una incómoda diferencia horaria y a una divergencia socio-cultural.[67]

2.2. ALGUNAS TENDENCIAS TECNOLÓGICAS

Las tecnologías de la información y las comunicaciones, las TIC, son un instrumento que ya forma parte de nuestra vida, desempeñando cada vez un papel más significativo. El porcentaje de usuarios de la banca electrónica alcanza el 45%, y se eleva al 53,6% si nos limitamos a las generaciones más jóvenes. La diferencia se incrementa respecto al uso de las redes sociales, enfrentando un 50% de la población en general contra el 90% de esos mismos individuos más jóvenes. Se prevé que estas cifras aumenten en los próximos años de manera notable[68]. Los datos actualizados al pasado verano cifran en un 96,7 % los hogares que cuentan con teléfono móvil y en el 77,8% los que tiene acceso a Internet de banda ancha, pero

[67] VIZCAÍNO BARCELÓ, A./ GARCÍA, F./ PIATTINI, M. (2014), desarrollo global de *software*, 9.
[68] DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (2015), transformación digital, 12.

solo el 49,4% de los ciudadanos utiliza Internet en sus relaciones con las Administraciones públicas[69].

Sobrepasando esa mera función instrumental, las TIC ya no se limitan a facilitar la realización de los procesos tradicionales de manera más rápida y eficiente, sino que se convierten en un presupuesto posibilitador que nos permite abordar procesos que sin ellas no serían ni factibles ni imaginables, adquiriendo así naturaleza estratégica. En la década de los setenta, la Administración española utilizaba las TIC únicamente para automatizar y acelerar sus procesos. En los ochenta se pasó a gestionar con ellas la información, estimada como un activo en sí misma. Cuando se decide aprovechar la capacidad estratégica que ofrecen estas tecnologías para dar respuesta a problemas antes no considerados, es el momento en el cual podemos considerar a la Administración electrónica como la manifestación del proceso de penetración de las TIC en el ámbito público, gracias a la generalización del uso de Internet característica de los noventa y al esfuerzo por reorientar la actividad pública hacia la satisfacción de las necesidades y exigencias de los ciudadanos y de las empresas[70].

Otras nuevas tendencias tecnológicas, como los llamados servicios de computación en la nube (*cloud computing*), la aparición de dispositivos móviles cada vez más inteligentes, la generalización del uso de las redes sociales o la capacidad de análisis de grandes volúmenes de datos (*big data*), confluyen para conformar un nuevo panorama en el que los

[69] MINHAP (2016), leyes 39 y 40, 5.
[70] BARROSO BARRERO, J. (2004), sectores clave, 55-56.

ciudadanos han adquirido nuevos hábitos y expectativas en su relación con las Administraciones públicas[71].

2.2.1. Computación en la nube

El uso del *cloud computing*[72] comienza a generalizarse en la Administración[73], resultando muy atractivo para el desarrollo de políticas públicas estratégicas que exigen alta demanda de recursos tecnológicos en un contexto de crisis económica[74]. Su utilización, cada vez más creciente, plantea desafíos para la efectiva protección de la información, tanto desde la perspectiva de la privacidad de los ciudadanos como por la posibilidad de que autoridades de otros Estados puedan acceder a la información simplemente por encontrarse en servidores de una empresa ubicada en su territorio[75], lo que convierte a la ubicación geográfica de los datos en un elemento fundamental para la confidencialidad y protección de los datos[76]. Definida por el NIST[77] como "*un modelo que permite el acceso a la carta o bajo demanda a todo un conjunto de recursos informáticos como aplicaciones, infraestructura, datos u otros servicios como por ejemplo el almacenamiento de información o el procesamiento de datos recogidos con un mínimo de esfuerzo o de interacción con el proveedor del servicio*", la computación en la nube ha supuesto una auténtica revolución para sus usuarios, al convertir en accesibles los recursos

[71] Introducción al real decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración general del Estado y sus Organismos públicos.
[72] Para un acercamiento más profundo a la computación en la nube orientada en las Administraciones públicas, v*id.* VALERO TORRIJOS, J. (2008), acceso a los servicios, 359-382.
[73] *Vid.* CCN (2014), CCN-STIC-823.
[74] MONTALBÁN CARRASCO, R. (2013), impulsoras de la transformación, 120.
[75] VALERO TORRIJOS, J. (2014), de la digitalización a la innovación tecnológica, 126.
[76] MINHAP (2016), prestación de aplicaciones, 39-40.
[77] Recuperado de http://www.nist.gov/itl/csd/cloud-102511.cfm (15 de mayo de 2016).

informáticos cuya adquisición no puede permitirse, en cualquier momento y lugar en que se halle y con un coste realmente bajo, con la ventaja añadida de la liberación de espacio físico al utilizar recursos informáticos en virtuales[78]. De los distintos modelos de servicios generalmente aceptados, *SaaS*[79] es el más contratado y de mayor interés para nosotros. Denominado "*software* como servicio", proporciona un entorno operativo completo con aplicaciones, administración e interfaz del usuario, en el que el usuario emplea la aplicación contratada sin ocuparse de su instalación, mantenimiento o actualización, que corren a cargo del proveedor del servicio. Una variante de uso también relativamente común corresponde al modelo de "procesos como servicio", donde lo que se proporciona no es simplemente un programa, sino un servicio completo, por ejemplo, la gestión de cobros[80]. Esta modalidad facilitará la reutilización de los recursos informáticos de una Administración informática por otras diferentes, como dispone el artículo 157 de la nueva ley 40/2015, como se verá *infra*.

Beneficios tangibles de la computación en la nube son la reducción de los costes de propiedad y mantenimiento de *hardware* y *software*, acompañada de la independencia de su localización, con ahorro de espacio físico, mejoras en la utilización y eficiencia, una alta escalabilidad y potencia de cálculo, sí como una capacidad de almacenamiento virtualmente ilimitada[81]. En la vertiente opuesta se encuentra la limitación que conlleva la pérdida de conexión a Internet o la baja velocidad de la misma, junto con una fiabilidad cuestionada o las limitaciones de portabilidad de aplicaciones construidas para un servicio de nube a otro

[78] NAVAS NAVARRO, S. (2015), computación en la nube, 5.
[79] *Software as a Service*, del que se prevé que alcance una cuota del 59% delos servicios en la nube en el año 2018.
[80] MINHAP (2016), uso de las herramientas tecnológicas, 14.
[81] AREITIO BERTOLÍN, J. (2010), *Cloud Computing*, 44.

proveedor, añadido todo ello a aspectos mucho más urgentes, como es la carencia de control o los problemas de seguridad y privacidad de datos y programas, a lo que se debe añadir algunos aspectos negativos accesorios, como la dificultad de realizar un adecuado análisis forense o auditorías en caso de necesidad[82]. ENISA recomienda a las Administraciones públicas que decidan iniciar la aventura de subir a la nube que lo hagan adoptando un enfoque escalonado y siempre dejando prevista la opción de una marcha atrás en cada etapa, teniendo en cuenta que la complejidad del entorno introduce variables desconocidas que podrían ser muy difíciles de gestionar[83]. Requieren especial atención los aspectos técnicos y jurídicos a contemplar en la contratación, referentes a conservación de datos, copias de seguridad, niveles de seguridad física y lógica, uso de mecanismos seguros de autentificación, técnicas de cifrado, procedimientos de recuperación, migración y borrado de datos, ubicación física…[84] En relación a la seguridad y confidencialidad de los datos, los riesgos jurídicos aumentan con las transferencias internacionales, cuando las garantías del país donde se ubican no son equiparables a las europeas, no garantizando un adecuado nivel de protección. Habida cuenta de que la mayoría de empresas prestadoras de servicios de computación en la nube son estadounidenses, la sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015 ha agravado el problema ya existente, al invalidar los acuerdos de Puerto Seguro con los Estados Unidos[85].

La consultora Gartner S.A., tras analizar los riesgos de los servicios en la nube, aconseja consensuar con el proveedor quiénes serán los usuarios con acceso a datos sensibles, el

[82] *Vid.* AREITIO BERTOLÍN, J. (2010), *Cloud Computing,* 45-46. El autor enumera exhaustivamente los dieciséis problemas más relevantes presentes en la computación en la nube.
[83] ENISA (2011), toma de decisiones.
[84] FUNDACIÓN TELEFÓNICA (2016), ciberseguridad, 67-69.
[85] GUASCH PORTAS, V./ SOLER FUENSANTA, J.R. (2016), puerto seguro, 331y 342.

sometimiento a auditorías externas y certificaciones de seguridad, la garantía de que los datos en reposo estén correctamente aislados y que los procedimientos de cifrado de la información se realicen por personal experimentado, así como cerrar un acuerdo para que el tratamiento de los datos se subyugue al marco legal del país del suscriptor del servicio. También conviene recabar información sobre la viabilidad de una recuperación completa y el tiempo estimado que necesitará, junto con la garantía de recuperar los datos aún en el caso de que el proveedor sea comprado o absorbido por otro, o bien asegurar la posibilidad de que puedan ser migrados a la nueva infraestructura[86]. En cualquier caso, más que los riesgos conocidos y las precauciones que, como nos advierten, hemos de tomar, quizás debamos preocuparnos por "*los riesgos y carencias normativas que son difíciles de predecir*"[87].

La Comisión deposita grandes esperanzas en la computación en la nube, la cual describe como una industrialización más avanzada de la prestación de servicios informáticos, como "*la informática como servicio de utilidad pública*", comparándola con las centrales eléctricas, que industrializaron el suministro de energía eléctrica[88].

2.2.2. *Big Data*

Superados el *Business Intelligence* (BI) y su minería de datos, habituales a finales del siglo pasado e inicio de este, hoy nos resulta familiar el *Big Data*, macrodatos en nuestro idioma, que aúna datos estructurados con otros que carecen de esta característica, provenientes de la *web*, de cámaras de los móviles, vídeos, redes sociales, sensores de las ciudades,

[86] INTECO-CERT (2011), riesgos y amenazas en *cloud computing*, 16-17.
[87] PIÑAR MAÑAS, J.L. (2011), revolución tecnológica, 34.
[88] COMISIÓN EUROPEA (2012), computación en nube, 4.

conversaciones…, alcanzando un volumen de información que crece exponencialmente, dando lugar a ingentes cantidades que se almacenan abandonando el ordenador personal y trasladándose a la nube, donde se alojan en granjas enteras de computadores para ser tratados con herramientas *software* especiales, capaces de manejar petabytes de información[89]. Son características del *Big Data* las conocidas como "cuatro V" correspondientes a volumen, variedad, velocidad y veracidad, que hacen referencia a cantidades masivas de datos que la organización trata de explotar para mejorar su proceso de toma de decisiones, partiendo de información de diferentes tipos procedentes de fuentes heterogéneas, procesados con la suficiente celeridad esforzándose por conseguir unos datos de alta calidad[90].

Es posible analizar estos ingentes mares de datos, contrastándolos con modelos de comportamiento, para ser capaces de predecir o de aconsejar basándose en ellos. La tendencia actual, por tanto, se centra en el paso de esa gran cantidad de datos (*Big Data*) a aquellos que aporten valor (*Smart Data*), lo que permitirá hacer predicciones, así como recomendaciones más fiables, aunque esos métodos aún no son excesivamente efectivos[91].

Las herramientas de *Big Data* se utilizan, por ejemplo, para la mejora de las ciudades gracias, haciendo un uso más inteligente de los datos en el entorno para lograr una mejor gestión de sus infraestructuras. Conocidas con el nombre de *Smart Cities*, dejan la puerta abierta a una duda: ¿puede estar tranquilo el ciudadano ante el uso de estos datos por potentes

[89] TASCÓN RUIZ, Á. M. (2013), introducción: *Big Data*, 48-49. Es interesante la ilustración del concepto de *petabyte* que nos aporta: en medio petabyte puede almacenarse la grabación de la vida completa de una persona longeva con calidad de alta definición.
[90] PAREDES MORENO, A. (2015), *Big Data*, 42-43.
[91] FUNDACIÓN TELEFÓNICA (2016), sociedad de la información, 80.

herramientas? El periodista digital Mario Tascón defiende la necesidad de alertas de los peligros inherentes[92]. De hecho, no son descartables las actividades de actividades de control e inspección por parte de las Administraciones públicas en un futuro no lejano, apareciendo una nueva amenaza para el derecho de protección de datos de carácter personal de los ciudadanos[93].

2.2.3. Otros servicios

La evolución tecnológica permite acrecentar la provisión de servicios disponibles gracias al incremento del ancho de banda. Las unidades de almacenamiento aumentan en capacidad y disminuyen progresivamente en precio. La introducción de las tecnologías móviles como *Wi-fi*, *bluetooth*, RFID o la mensajería SMS, poco a poco va permitiendo incluir servicios cada vez más complejos, introduciendo un nuevo paradigma *wireless* en la concepción de una nueva eAdministración ubicua y permanentemente accesible, mientras que la TDT permite abrir un nuevo canal de comunicación con todos los ciudadanos, pudiendo llegar incluso a ofrecer servicios administrativos interactivos de tramitación[94].

El incesante desarrollo de las TIC, centrado en el campo del *hardware*, expresó su avance vertiginoso en forma de la tradicional ley de Moore de 1965, que ha venido enunciándose como la predicción de que el número de transistores en un chip se duplica en menos de dos años. Ello ha llevado a Intel a estimar "la *aparición de una nueva tecnología de fabricación aproximadamente cada dos años y la presentación de una nueva microarquitectura de CPU en*

[92] TASCÓN RUIZ, Á. M. (2013), introducción: *Big Data*, 50.
[93] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 394.
[94] FUNDACIÓN TELEFÓNICA (2008), Administración local, 136.

años alternos"[95]. Aunque la miniaturización se acerca a su límite físico[96], se están empleando millones en el estudio de nuevas técnicas, algunas de ellas con fundamento en las ideas propuestas por Paul Benioff, David Deutsch y Richard Feynman en 1982 y, poco después y de forma independiente, por Deutsch, basándose todos ellos en los principios de la física cuántica[97]. Mientras la unidad de información mínima manejada por el ordenador clásico es el bit, que puede representar los valores discretos 0 o 1, el ordenador cuántico maneja qubits, que admiten valores continuos, combinaciones de ambos estados. Con ellos se obtiene una capacidad de realizar operaciones en paralelo o simultáneamente que crece de manera exponencial en relación al número de qubits con los que puede operar el ordenador[98]. Las noticias de los avances en esta dirección nos llegan en forma de un lento goteo[99], no siendo previsible un uso comercial de los ordenadores cuánticos en los próximos años. Incluso así, las profundas innovaciones en la arquitectura de las computadoras están cambiando el papel del *software*, produciendo sistemas sofisticados y complejos que, si bien pueden ofrecer resultados sorprendentes, plantean problemas extraordinarios a quienes se dedican a la construcción del *software*, una de cuyas manifestaciones ha sido la sustitución del programador individual por equipos de especialistas, cada uno centrado en una parte de la tecnología que se requiere para llegar a obtener una aplicación compleja[100]. Se abandonan los grandes sistemas monolíticos y se adoptan

[95] INTEL CORPORATION IBERIA (2009), ley de Moore, 33.
[96] Pavlus, J. (2015). Más allá de la ley de Moore. *Investigación y ciencia*, (466).
[97] Un extraordinario trabajo divulgativo es el publicado con fecha de 3 de junio de 2003 por el que se denominó Grupo de computación cuántica de la Universidad Politécnica de Madrid, que lleva por título *Introducción al modelo cuántico de computación*.
[98] CANTÓN, D. (2014), computación cuántica.
[99] A modo de ejemplo, *vid*. los informes de la Universidad de Yale de los que se informea en la revista *Science* de 27 de mayo de 2016. Recuperado de http://science.sciencemag.org/content/352/6289/1087 (27 de mayo de 2016).
[100] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 3.

arquitecturas como SOA, orientadas a servicios, buscando una respuesta ágil y flexible a las demandas del mercado[101]. El diseño del *software* se vuelve cada vez más modular, con componentes o servicios reutilizables, como los WS (*Web Services* o Servicios *Web*), que pueden hallarse distribuidos por diferentes máquinas conectadas en la red. Una aplicación puede utilizar los servicios ofrecidos por cualquier servidor conectado a Internet. El uso de WS se ha convertido en una cuestión clave para la interoperabilidad[102] entre aplicaciones diferentes. Pueden ser invocados desde cualquier lugar de Internet, con independencia de la plataforma utilizada y del lenguaje de programación empleado[103].

Los entornos fijos cada vez son más heterogéneos, provocando problemas de interoperabilidad, pero es en el ámbito móvil donde más han evolucionado, con gran variedad de teléfonos inteligentes y tabletas. En tal situación, el mantenimiento de la neutralidad tecnológica, como se verá, se dificulta, agravado aún más por las restricciones presupuestarias que la sostenida crisis lleva años imponiendo.

Dejando a un lado aquellos conocimientos que son comunes para cualquier tecnología informática, podría afirmarse que la mitad de lo que hoy necesita conocer un ingeniero del *software* está obsoleto dentro de tres años[104]. La variabilidad tecnológica dificulta

---

[101] ACCENTURE – CENTRO DE ALTO RENDIMIENTO (2008), arquitectura orientada a servicios, 5.
[102] El real decreto 4/2010, de 8 de enero, por el que se regula el esquema nacional de interoperabilidad en el ámbito de la Administración electrónica la define, en su anexo I, como la "*capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos*", reiterando las palabras exactas empleadas en el texto de la LAE.
[103] UNIVERSIDAD DE ALICANTE. DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL. (2012-2013), servicios *Web* y *SOAP*, 4.
[104] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 83, reproduciendo una cita de Steve McConnell publicada en IEEE *Software*.

la estabilidad del *software* y plantea dudas importantes en referencia al modo óptimo de seleccionar a los integrantes del equipo de desarrollo.

2.3. LA CRIPTOGRAFÍA

El diccionario de la RAE, en su 23ª edición, describe la criptografía, del griego κρυπτός kryptós 'oculto' y -grafía, como el "*arte de escribir con clave secreta o de un modo enigmático*". No aclara más la consulta del término criptología, que aparece recogido como el "*estudio de los sistemas, claves y lenguajes ocultos o secretos*". Prosiguiendo la búsqueda, se puede hallar la definición de clave como "*código de signos convenidos para la transmisión de mensajes secretos o privados*" y "*conjunto de reglas y correspondencias que explican un código de signos*". Finalmente, la cuarta acepción de la palabra código se explica como "*sistema de signos y de reglas que permite formular y comprender mensajes secretos*".

Un sencillo ejemplo práctico puede iluminar mejor la idea alrededor de la que giramos. Rumores desmentidos afirman que HAL, el siniestro computador de la película "*2001, una odisea en el espacio*", oculta el nombre del fabricante de ordenadores IBM. Sustituyendo cada letra de la palabra IBM por su anterior en el abecedario, la I pasaría a ser H, la B se cambiaría por la A y la M se convertiría en L, con lo que IBM se transformaría en HAL. Intencionado o no, se trata de un ejemplo de aplicación de la criptografía, en el que se emplea un algoritmo de sustitución de clave -1, similar al utilizado ya por Julio César en los tiempos de la Roma Imperial (él escogió la clave 3, pues sustituía cada letra por la situada 3 posiciones después en el abecedario). Como tributo a este sistema, en la actualidad, cualquier codificación basada únicamente en el desplazamiento de las letras del alfabeto un determinado número de

posiciones se denomina cifrado de César y, obviamente, su uso parece poco seguro salvo, quizá, para la realización de las clásicas "chuletas" escolares.

De las diversas aproximaciones al concepto de criptología, me decanto por aquella que la define como la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave[105] entre un emisor y un receptor a través de un canal de comunicaciones[106]. Esta ciencia se bifurca en dos ramas perfectamente diferenciadas: la criptografía, que se ocupa del proceso de cifrado, y el criptoanálisis[107], que estudia el descifrado o, más exactamente, los ataques contra los criptosistemas.

La filosofía con que los criptógrafos exploraban nuevos métodos ha cambiado radicalmente desde sus inicios, que se remontan hasta el antiguo Egipto[108], cuando la protección efectiva requería mantener oculto el sistema de cifrado. La criptografía moderna da un giro radical en sus planteamientos, exigiendo que el algoritmo informático o modo de funcionamiento del sistema se exponga al conocimiento público y al ataque de los mejores criptoanalistas, para determinar su fortaleza, de forma que ha de mantenerse en secreto únicamente la clave utilizada. Se trata de uno de los principios establecidos en el siglo XIX por Auguste Kerckhoffs en su obra "*La cryptographie militaire*", donde añade, entre otros, la necesidad de que el sistema de cifrado

[105] Partiendo de un mensaje "en claro" y aplicando sobre él el criptosistema escogido, se convierte en un "texto cifrado", también llamado criptograma, a lo que se denomina "mensaje en clave".
[106] Definición de FERNÁNDEZ FERNÁNDEZ, S. (2004), criptografía clásica, 20.
[107] En el programa de TV educativa titulado "*Introducción al criptoanálisis*", emitido el 12 de diciembre de 1998 por TVE2, y accesible desde la página *web* de la UNED http://canal.uned.es/mmobj/index/id/7093 ofrezco unas ideas básicas sobre el criptoanálisis que puede resultar de utilidad para comprender el concepto y los métodos más sencillos de descifrado.
[108] El precitado trabajo de Santiago Fernández nos brinda un detallado y divulgativo viaje por su historia, de interesante lectura.

sea impenetrable en la práctica, así como la sencillez de la clave y la facilidad de memorización y sustitución[109].

Aquella criptografía clásica vino considerándose un arte hasta 1949, año en que el ingeniero y matemático americano Claude Shannon sentó las bases teóricas de la nueva ciencia[110], que llevaron, un cuarto de siglo más tarde, al desarrollo por IBM del estándar comercial americano DES (*Data Encryption Standard*)[111]. Seleccionado por la oficina nacional de estándares norteamericana y afectado por el establecimiento de restricciones a la exportación[112], recibió un fuerte apoyo de la agencia de seguridad nacional de los Estados Unidos, NSA, a pesar (o quizá por ello[113]) de su vulnerabilidad ante los ataques por fuerza bruta[114], consistentes en la prueba de todas las combinaciones posibles de claves, factible por la corta longitud de esta (56 bits), a lo que hay que añadir la existencia de herramientas matemáticas y estadísticas[115] que permiten acortar el tiempo de descifrado, motivos todos ellos que pudieron llevar al departamento de defensa de los Estados Unidos a no utilizar jamás este

[109] GALENDE DÍAZ, J.C. (2006), manuscrito, 54.
[110] CABALLERO GIL, P. (2000), algunos hitos, 405-406.
[111] Sucesores mejorados del criptosistema DES son el triple DES y el AES (*Advanced Encryptíon Standard*).
[112] STALLINGS, W. (2004), fundamentos de seguridad en redes, 59.
[113] Como recoge la periodista REBECCA MACKINNON en la página 110 de la edición digital de su libro *No sin nuestro consentimiento*, el técnico de AT&T en San Francisco, Mark Klein, empleado en sus instalaciones de la calle Folson, importante punto de intercambio de tráfico telefónico y de *e-mail*, filtró en 2003 la construcción, por la NSA (Agencia de seguridad nacional de Estados Unidos), de una sala secreta en esas instalaciones, con el objetivo de dirigir todo el tráfico de *e-mail* y teléfono a su través para ser interceptado y transmitido para su análisis.
[114] STALLINGS, W. (2004), fundamentos de seguridad en redes, 32. El autor explica el ataque por fuerza bruta, que no reviste mayor complicación que la prueba de todas las posibles claves, una detrás de otra, hasta encontrar la correcta. El interés especial de esta cita reside en la comparación de tiempos que tardaría en descubrir la clave un ordenador que pudiera probar un millón de claves por microsegundo. Para una clave de 32 bits, ese tiempo es de dos milisegundos. En cambio, para una clave de 168 bits, ese tiempo se eleva a 5.9×10^{30} años. En cualquier caso, hay que tener en cuenta que los avances tecnológicos van reduciendo progresivamente eso tiempos y lo que hoy es seguro puede no serlo mañana. Por otra parte, hay formas mucho más rápidas de descubrir las claves ajenas. Sugiero la lectura del ejemplo recuperado de la *url* http://www.genbetadev.com/seguridad-informatica/cuanto-tardaria-un-hacker-en-reventar-nuestra-contrasena (4 de agosto de 2016).
[115] CABALLERO GIL, P. (2000), algunos hitos, 406.

sistema[116]. De hecho, en 1998, los periódicos anunciaron la construcción, por menos de 250.000 dólares, de una máquina bautizada como "DES *cracker*", específicamente diseñada para romper el cifrado DES, en un ataque por fuerza bruta que duró únicamente tres días[117]. La protección ante este tipo de ataque exige el incremento de la longitud de la clave. Se considera que una longitud de clave de 128 bits convertiría al algoritmo en inexpugnable por la fuerza bruta[118]. La especificación funcional del protocolo de sustitución de certificados en soporte papel, SCSPv3, utilizada en nuestro país para el intercambio de información de los ciudadanos entre Administraciones públicas, establece el uso de AES (*Advanced Encryptíon Standard*) 128, aunque en determinadas situaciones que requieran una seguridad más elevada, duplica la longitud de la clave utilizando AES 256[119].

Si bien es cierta la existencia de un método de cifrado perfecto, invulnerable, o de seguridad incondicional[120], propuesto por Gilbert S. Vernam[121] y de infalibilidad demostrada por Shannon[122], las exigencias que debe cumplir reducen notablemente su utilidad. Estos requerimientos indispensables imponen que la clave sea al menos tan larga como el texto que se quiere cifrar, se emplee una única vez y sea generada de un modo verdaderamente aleatorio[123]. El sistema de cinta aleatoria es una implementación práctica de este tipo de cifrado, consistente en dos cintas idénticas, una empleada por el emisor en el proceso de cifrado y otra en posesión

[116] PABÓN CADAVID, J.A. (2010), criptografía, 65-66.
[117] STALLINGS, W. (2004), fundamentos de seguridad en redes, 35.
[118] STALLINGS, W. (2004), fundamentos de seguridad en redes, 36.
[119] MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA (2012), especificación funcional, 19.
[120] CCN (2013), CCN-STIC-400, 21.
[121] *Vid.* VERNAM, G.S. (1926), *Cipher Printing Telegraph Systems*, 109-115.
[122] *Vid.* SHANNON, C.E. (1949), *Communication Theory of Secrecy Systems*, 656-715.
[123] FUSTER SABATER, A. (2009), cifrado en flujo.

del receptor, que se utiliza para el descifrado. Su dificultad estriba en la necesidad de un canal de distribución de claves seguro, por lo que su uso regular llega a ser inviable[124]. La colaboración de la física cuántica para soslayar este problema pasa por el envío de la clave utilizando una transmisión fotónica a través de un canal de comunicaciones invulnerable. Esa clave sería utilizada posteriormente para transmitir la información utilizando el método de Vernam en un canal de comunicaciones inseguro[125]. Este es un campo abierto a la investigación que podrá dar frutos en un futuro, pero aún continúan presentándose problemas prácticos que limitan el alcance de la transmisión[126].

El problema de la distribución de claves y su mantenimiento en secreto afecta a los denominados criptosistemas clásicos, también llamados simétricos o de clave secreta, única o privada, caracterizados por emplear la misma clave para cifrar y descifrar o bien por poder deducirse una de la otra.

Fue en 1976 cuando Whitfield Diffie y Martin Hellman[127] revolucionaron la criptografía introduciendo los criptosistemas asimétricos o de clave pública, caracterizados por el uso de dos claves diferentes e independientes, una de ellas de conocimiento público, mientras que la otra debe mantenerse en secreto. La confidencialidad del mensaje, cifrado con la clave pública que cualquier persona conoce y puede utilizar, queda garantizada al poder ser descifrado únicamente con la clave privada, que se mantiene en secreto y en posesión, únicamente, del

[124] CCN (2013), CCN-STIC-400, 29.
[125] Puede ampliarse información sobre este tema en el programa de TV educativa titulado "Criptografía cuántica", emitido el 18 de octubre de 1998 por TVE2, accesible en la página *web* de la UNED http://canal.uned.es/mmobj/index/id/12240 donde resumo las ideas básicas de la contribución de la física cuántica a la construcción de un canal de comunicaciones invulnerable.
[126] GUILLÉN PINTO, E.P./ NAVARRO GASCA, J.J. (2007), distribución de claves, 71.
[127] DIFFIE, W./ HELLMAN, M.E. (1976), *New Directions*, 644-654.

legítimo titular. Este tipo de criptosistemas asimétricos permiten también garantizar la autenticidad del emisor del mensaje cuando lo cifra utilizando su clave privada, dado que solo él la conoce. Ese mensaje cifrado con la clave privada solo puede ser descifrado con la clave pública correspondiente. De esa forma, si el receptor logra descifrarlo, puede estar seguro de la identidad del emisor. El inconveniente de estos sistemas resulta ser la lentitud del proceso de descifrado, mayor que en los sistemas simétricos[128], por lo que no suele utilizarse para cifrar mensajes de gran volumen[129]. El criptosistema PGP (*Pretty Good Privacy*)[130] de Phil Zimmermann da solución a la lentitud en el descifrado de RSA, cifrando primeramente con IDEA, una derivación del clásico DES, para después cifrar con RSA la clave del mensaje cifrado con el sistema simétrico[131].

El criptosistema asimétrico de uso más generalizado es el RSA, iniciales de sus desarrolladores, Rivest, Shamir y Adleman[132]. Basa su funcionamiento en la complejidad de descomponer grandes números en sus factores primos[133]. Sin embargo, el convencimiento de que el criptoatacante no va a lograr dicha factorización puede proporcionar una sensación de seguridad engañosa, puesto que, como hemos tratado *supra*, la tecnología (y también los

[128] PABÓN CADAVID, J.A. (2010), criptografía, 67.
[129] RIBAGORDA GARNACHO, A./ AREITIO BERTOLÍN, J. (2004), breve panorámica, 9.
[130] En diciembre de 2016 el CCN ha editado una nueva guía con recomendaciones para cifrar y descifrar mensajes y archivos de forma correcta empleando un derivado de PGP conocido como GPG (GNU *Privacy Guard*). Puede descargarse de https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1819-ccn-stic-955b-recomendaciones-de-empleo-de-gpg-1/file.html
[131] PABÓN CADAVID, J.A. (2010), criptografía, 68.
[132] RIVEST, R.L., SHAMIR, A. y ADLEMAN, L. (1977). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Recuperado de http://web.mit.edu/6.857/OldStuff/Fall03/ref/rivest78method.pdf (16 de marzo de 2016).
[133] La fundamentación matemática de este criptosistema no es compleja y puede seguirse detalladamente en SANGRONIZ GÓMEZ, J. (2004), el Sistema RSA, 149-165.

algoritmos[134]) avanzan vertiginosamente, especialmente en velocidad y potencia, de forma que algo que hoy se encuentra dentro de los límites de seguridad computacional[135], podría no estarlo mañana, lo que obliga a aumentar el tamaño de las claves para conservar el nivel de seguridad pretendido[136], algo que habrá que hacer reiteradamente, pues la tecnología no cesa en su progreso. Un criptosistema puede seguir considerándose computacionalmente seguro mientras el coste de romper el cifrado sea más elevado que el valor de los datos protegidos por él o bien el tiempo necesario para lograrlo sobrepase la vida útil de la información[137].

Los criptosistemas de clave pública requieren una infraestructura[138] de publicación y administración de claves práctica y fiable[139], que incluya la certificación de las claves públicas y su validación[140] por parte de las entidades emisoras de los certificados, denominadas autoridades de certificación[141] o prestadores de servicios de certificación. La comprobación de la validación del certificado, incluida su no revocación, puede realizarse de forma interactiva, solicitando esa información a la CA, o en modo diferido, comprobando las

[134] El algoritmo de Shor para un computador cuántico podría llegar a inutilizar el criptosistema RSA, aunque no parece viable a medio plazo. *Vid.* CAICEDO ORTIZ, H.E. (2010), algoritmo de factorización, 352-353.
[135] La denominada seguridad computacional es diferente de la seguridad perfecta o incondicional. Aquella varía con el tiempo, en función del estado de la técnica.
[136] SANGRONIZ GÓMEZ, J. (2004), el Sistema RSA, 163.
[137] STALLINGS, W. (2004), fundamentos de seguridad en redes, 31-32.
[138] Se denomina PKI por sus iniciales en inglés, *Public Key Infrastructure*, o infraestructura de clave pública.
[139] LÓPEZ, J./ MAÑA, A./ MONTENEGRO, J.A./ ORTEGA, J.J. (2000), implementación.
[140] Existen autoridades de validación (VA) que se ocupan de comprobar la validez de certificados electrónicos y también la de las de firmas, debiendo comprobar, en el momento en que se ha generado la firma, el estado de revocación, el periodo de validez y la firma digital de la CA. Si en el momento de realizar la firma el certificado no estaba revocado, no influye en su validez la posible revocación posterior.
[141] También llamadas CAs, iniciales de *Certification Authoritys*.

fechas de validez[142] incluidas en el propio certificado y consultando la más reciente lista de certificados revocados emitida por la entidad.

El adecuado funcionamiento de la infraestructura de clave pública, PKI, requiere depositar nuestra confianza en la autoridad de certificación, CA, que emite el certificado, en el proceso de registro seguido por la autoridad de registro, RA, en la seguridad de los sistemas informáticos de las distintas entidades implicadas en la PKI, en el soporte donde reside el certificado[143], en terceros implicados como son las autoridades de validación, VA, o las autoridades de sellado de tiempo, TSA, y en el propio entorno del usuario, elemento más débil de la cadena[144]. Se nos pide otorgar la misma confianza que, sin reparos, se concede al notariado o al funcionariado que comprueba nuestra identidad con un documento con una fotografía no siempre actualizada.

Son muchos los criptosistemas diferentes propuestos, así como las líneas de investigación abiertas. El motor de estos trabajos de I+D+i en criptografía ya no se reduce a las aplicaciones militares, sino que su uso actual está profundamente arraigado en nuestras vidas diarias, aunque muchas veces no seamos conscientes de ello.

Se espera que las nuevas arquitecturas de la Internet del futuro pongan remedio a los actuales inconvenientes en cuestión de seguridad y privacidad, introduciendo mecanismos

[142] Un certificado se considera expirado cuando está fuera del rango de fechas comprendido entre la de inicio y la de fin de validez, y su uso en un momento temporal fuera de ese rango no tiene implicaciones para su titular.
[143] Es más seguro un soporte *hardware*, como es el del DNI electrónico, que un soporte *software*.
[144] HERNÁNDEZ-ARDIETA, J.L./ GONZÁLEZ-TABLAS, A.I./ RAMOS, B. (2012), repudio.

para gestionar la identidad y la confiabilidad[145]. Las redes de nueva generación, como IPv6, imponen restricciones en cuanto a ancho de banda y recursos de energía, lo que limita los mecanismos de seguridad admisibles, que han de ser mucho más ligeros. Por ello, buscando reducir la longitud de la clave, se están desarrollando novedosas propuestas para la administración de las claves y el proceso de firma y cifrado, con una base matemática centrada en las curvas elípticas e hiperelípticas, que proporcionan un nivel de seguridad equivalente al de los criptosistemas habituales de longitud de clave mayor[146].

Si bien es cierto que el empleo de las comunicaciones cifradas a través de Internet es una dificultad para perseguir delitos de importancia llevados a cabo por el crimen organizado[147], no está exenta de polémica la posibilidad de que los Gobiernos tengan acceso a los mensajes enviados en aras de la defensa de la seguridad pública, algo que puede acercarnos al mundo retratado por George Orwell en su novela 1984. Ese Gran Hermano ha hecho uso en ocasiones de puertas traseras, *backdoors*, diseñadas por los fabricantes de herramientas criptográficas[148] y ocultas en sus productos. Sin perjuicio de que las pruebas obtenidas por estos métodos hayan de ser consideradas ilegales, ello no impide la consecuente destrucción de la confianza de la ciudadanía en los sistemas de cifrado y en el *software* que los sustenta.

Las condiciones básicas para una comunicación segura a través de redes abiertas son la confidencialidad, la integridad, la autenticación y el no repudio[149]. El mantenimiento de la

[145] CASTILLO HOLGADO, A. (2009), innovación tecnológica, 32.
[146] VERA PARRA, N.E./ LÓPEZ, D.A./ MANTA CARO, H.C. (2014), criptografía de curva elíptica, 28.
[147] RUILOBA CASTILLA, J.C. (2006), actuación policial, 57.
[148] PABÓN CADAVID, J.A. (2010), criptografía, 77.
[149] MARCOS MARTÍN, J.L./ BALSELLS TRAVER, M. (2000), génesis y regulación, 33.

confidencialidad de la información no es el único de esos objetivos que pretende cubrir la criptografía. Su utilidad alcanza la pretensión de evitar el repudio interesado[150] de los mensajes y asegurar la integridad de los mismos frente a una hipotética manipulación, así como garantizar la autenticidad de los comunicantes[151], entendiendo por autenticación tanto la identificación, donde el sistema averigua quién es el usuario y comprueba que realmente es él, como el caso más habitual de verificación de la identidad, donde el sistema confirma que es quien dice ser[152].

Durante la transmisión de un archivo, su contenido, o una parte de él, puede alterarse por error, por cortes en la comunicación o por un ataque malicioso. Cuando ese archivo modificado intencionadamente es un programa listo para ser descargado por terceros, el ataque se denomina "troyanización" y puede afectar incluso a páginas oficiales de fabricantes[153] o a las propias Administraciones públicas, quienes no siempre podrían garantizar que su *software* estuviera libre de *malware*. Para resolver el problema, las técnicas criptográficas permiten averiguar si el archivo fue modificado desde su creación, empleando para ello funciones resumen, más conocidas como funciones *hash*, cuyo funcionamiento ha de ser de conocimiento público. Estas funciones transforman un mensaje de cualquier tamaño en otro de longitud fija más pequeña. Ese mensaje más breve recibe el nombre de resumen criptográfico o huella digital. Si junto a un programa listo para descargar se publica su resumen criptográfico, quien lo obtenga puede comprobar si ha sido modificado, calculando el resumen criptográfico y comparándolo con el que debería ser. De este modo puede evitarse la ejecución de *software* que haya podido ser

[150] CCN (2013), CCN-STIC-400, 21.
[151] SANGRONIZ GÓMEZ, J. (2004), el Sistema RSA, 150.
[152] INTECO (2012), guía sobre riesgos y buenas prácticas, 7.
[153] INTECO (2011), cómo comprobar la integridad de los ficheros, 1.

modificado maliciosamente, pues cualquier diferencia indica indefectiblemente que el archivo ha sido alterado[154]. Sin embargo, la coincidencia no garantiza la integridad del *software*, puesto que el atacante que ha manipulado el *software* a descargar también ha podido sustituir la huella digital[155].

Las funciones *hash* han de cumplir un conjunto de requerimientos que le confieren su utilidad, como la irreversibilidad o imposibilidad de que a partir del resumen se pueda obtener el texto original, o el determinismo, es decir, siempre que se aplique una función *hash* concreta a un mensaje determinado se obtendrá el mismo resumen criptográfico. Además, si se produce el cambio de parte del mensaje, aunque sea de un solo bit, la función resumen variará al menos en un 50%, alertando notoriamente de la producción de la modificación indeseada. La función *hash* ha de cumplir además dos condiciones adicionales. La primera consiste en la imposibilidad de generar un mensaje con un resumen criptográfico determinado, salvo utilizando el método de fuerza bruta, es decir, probando con mensajes arbitrarios hasta obtener el resumen criptográfico deseado. El segundo prohíbe la existencia de un método para producir una colisión, es decir, dos mensajes con el mismo resumen (salvo por fuerza bruta)[156].

Es práctica recomendable evitar el almacenamiento de las contraseñas de los usuarios para acceder a determinados sistemas informáticos. En su lugar, lo que se guarda es su resumen criptográfico. De esta forma, cuando el usuario introduce su palabra de paso para

[154] Recientemente se ha absuelto a los acusados del caso "Anonymous" gracias a la demostración de la manipulación de las pruebas digitales lograda mediante la comparación de los códigos *hash* originales con los actuales, confirmando la existencia de diferencias. *Vid.* http://peritoinformaticocolegiado.es/los-acusados-del-caso-anonymous-absueltos-gracias-a-un-peritaje-informatico/

[155] INTECO (2011), cómo comprobar la integridad de los ficheros, 8.

[156] INTECO (2011), cómo comprobar la integridad de los ficheros, 3.

acceder al sistema, se aplica la función *hash* y se compara el resultado con el resumen guardado. Si no coinciden, la contraseña introducida no es correcta y el acceso no será permitido.

Constatado el incesante incremento de los ciberataques contra empresas, que en 2014 se estiman en más de 117.000 cada día, se está intensificando el uso del cifrado de las comunicaciones entre usuarios de en las principales empresas de Internet y se espera que continúe esta tendencia[157].

Conviene rememorar aquí las ideas de Karl Popper que Esteve Pardo nos recuerda[158]: "(…) *la Ciencia no trabaja tanto con certidumbres como con probabilidades. No vayamos a buscar en la Ciencia certidumbres porque posiblemente no nos las dará, nos dará como mucho probabilidades: más probabilidades, altas probabilidades, bajas probabilidades*". La criptografía, en función del algoritmo utilizado, de la longitud de clave…, no nos da, en general, una seguridad total. Para utilizar los algoritmos que ofrezcan una probabilidad de protección más alta, las Administraciones públicas deben escoger entre los que hayan sido acreditados por el Centro criptológico nacional (CCN) para su uso dentro del Esquema nacional de seguridad (ENS), recogidos en la "guía/norma de seguridad de las TIC (CCN-STIC-807) - criptología de empleo en el esquema nacional de seguridad"[159], sin olvidar que la seguridad total, en la práctica, aún no existe.

[157] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO (2015), informe anual 2014, 231-232.
[158] ESTEVE PARDO, J. (2006), Derecho de decisión, 12.
[159] Con respecto a las herramientas de cifrado *software*, puede consultarse la "Guía de seguridad de las TIC (CCN-STIC-437) - herramientas de cifrado *software*" de diciembre de 2007.

2.4. LA FIRMA ELECTRÓNICA

La identidad personal constituye un elemento valioso merecedor de protección jurídica, de especial importancia en el ámbito de la Administración electrónica, donde se debe garantizar que las relaciones entabladas entre los ciudadanos y las Administraciones públicas se llevan a cabo por los legítimos interesados o por sus representantes[160]. La prueba de la identidad en el entorno digital se convierte en un aspecto crítico e indispensable, facilitado por los certificados digitales y la firma electrónica, concepto más amplio que el de firma digital[161], dado que aquella, a diferencia de esta, puede incluir también métodos no criptográficos[162].

La firma digital es la solución que la criptografía ofrece para despejar las dudas sobre la integridad y procedencia de documentos[163]. Pero la firma de un documento de cierta longitud es una operación computacionalmente costosa[164]. Por ello el procedimiento comienza con la obtención del resumen criptográfico, aplicando al documento una función *hash*. Ese resumen es el que realmente se firma con la clave privada, obteniendo lo que se denomina "firma", que suele ser un archivo con extensión SIG o ASC. En ello se basa el concepto de firma digital, en utilizar la clave privada para garantizar que quien envía el mensaje es el titular de la clave pública[165].

---

[160] INTECO (2012), guía sobre riesgos y buenas prácticas, 6.
[161] SORIANO MALDONADO, S. (2001), marco regulatorio general, 79-80. El autor considera el concepto de firma digital como sinónimo de firma electrónica avanzada
[162] INTECO (2012), guía sobre riesgos y buenas prácticas, 24.
[163] CASTILLO RUBÍ, M.A., SANTANA DE LA CRUZ, N., DÍAZ LOBATON, A.M., ALMANZA RODRÍGUEZ, G. Y CASTILLO RUBÍ, F. (2011-2012), teoría de números, 268.
[164] INTECO (2011), cómo comprobar la integridad de los ficheros, 4.
[165] PABÓN CADAVID, J.A. (2010), criptografía, 67.

El envío consta de dos objetos: el documento original y su resumen cifrado. El receptor aplica sobre el documento recibido la misma función *hash*, obteniendo así la función resumen del documento recibido. A su vez, descifra el resumen firmado que ha recibido mediante el uso de la clave pública del firmante. Únicamente tiene que comparar los dos objetos resultantes. Si son diferentes, el documento recibido ha sido alterado y no puede considerar que ha recibido un documento válidamente firmado.

Como puede observarse, con la firma digital no se pretende garantizar la confidencialidad del documento sino la autenticidad de su procedencia y la integridad de su contenido. Recordemos que la confidencialidad se garantiza aplicando la clave pública para el cifrado y la privada para el descifrado, mientras que la autenticidad e integridad se asegura utilizando la clave privada para el cifrado y la pública para el descifrado. De este mismo modo también puede garantizarse el no repudio en origen, es decir, que el emisor de un mensaje firmado electrónicamente no podrá negar[166] a posteriori haberlo enviado[167].

Aspectos como la autenticidad, el no repudio, el estampado de fecha y hora de forma digital[168] y la integridad[169], son aspectos a analizar en los elementos probatorios electrónicos presentados en el proceso judicial.

Si las claves empleadas están asociadas a una persona a través de una autoridad de certificación[170], no solo se garantiza la integridad sino también la identidad del firmante. Es lo

[166] En realidad, veremos casos *infra* en los que sí podría tratar de repudiar ese envío.
[167] LÓPEZ MUÑOZ, J./ MARTÍNEZ NADAL, A./ PATEL, A. (2004), firma electrónica, 3.
[168] La autoridad de sellado de tiempo, TSA, es la que permite añadir un sello de tiempo a la información, es decir, una referencia temporal confiable, firmando digitalmente el conjunto.
[169] PABÓN CADAVID, J.A. (2010), criptografía, 75.

que se conoce como un certificado digital[171], consistente en una certificación por parte de una entidad confiable de que determinada firma criptográfica corresponde a una persona concreta, física o jurídica.

Físicamente, un certificado digital es un fichero de un tamaño de 2 k aproximadamente, expedido por un prestador de servicios de certificación, que contiene la firma de dicho prestador junto con los datos de la persona física o jurídica y su clave pública[172].

Nuestros equipos están preparados para realizar la comprobación de certificados, debiendo haberles indicado previamente cuáles son, según nuestro criterio, las entidades de certificación que consideramos de confianza.

El propio *software* puede ser firmado por el fabricante (por ejemplo, por las Administraciones públicas) permitiendo garantizar así su procedencia.

La especificación funcional del protocolo de sustitución de certificados en soporte papel, SCSP v3, utilizado para intercambiar información de los ciudadanos entre las diferentes Administraciones públicas, dispone que todas las comunicaciones realizadas entre un requirente y un emisor irán firmadas digitalmente para garantizar la autenticación, no repudio e integridad de la información intercambiada, utilizando certificados X509 versión 3 reconocidos y aceptados por @firma para identificar a las máquinas de cada organismo intervinientes en la comunicación,

---

[170] En función del diseño de la infraestructura de clave pública, las autoridades de certificación (CA) pueden estar distribuidas en más de un nivel, en una estructura en árbol, existiendo una CA raíz y tantos niveles intermedios como se haya diseñado, hasta llegar a la CA que emite el certificado del usuario. Cada CA emite los certificados de sus subordinadas, dando lugar así a lo que se denomina cadena de certificación, o conjunto de certificados emitidos desde la raíz hasta el usuario final.

[171] INTECO (2011), cómo comprobar la integridad de los ficheros, 4-5.

[172] ÁLVAREZ HERNANDO, J. (2004), firma electrónica, 7.

emitidos por cualquier autoridad de certificación reconocida tanto por el emisor como por el requirente[173].

Una parte de la ciudadanía aún desconfía del uso de la firma electrónica, a pesar de la existencia de un marco jurídico y tecnológico que apoya, cumpliendo determinados requisitos, su utilización con validez equivalente a la de la firma manuscrita. Se puede apreciar en la sociedad una escisión entre los defensores a ultranza de la versión electrónica y los reacios a su utilización. Probablemente el punto intermedio sea el lugar más adecuado para posicionarse, conociendo las vulnerabilidades de la tecnología de firma electrónica, que pueden minorar notablemente nuestro grado de confianza. Hernández-Ardieta, González-Tablas y Ramos sostienen que "*al contrario de lo que las diversas leyes y estándares fundamentan, la firma electrónica no otorga plenas garantías de no repudio sobre la información firmada*"[174], acompañando su afirmación con una relación detallada de supuestos prácticos susceptibles del repudio del titular de la firma digital. El primer eslabón cuestionable en la cadena que da soporte a la firma es, paradójicamente, la comparecencia presencial ante una autoridad de registro, quien debe comprobar la identidad del solicitante del certificado. El procedimiento utilizado puede variar sustancialmente de una a otra y de él depende la confianza de la relación entre la clave y la real identidad de la persona[175]. No siempre las fotografías de los documentos identificativos guardan una semejanza indiscutible con la imagen actual del solicitante, sin entrar a plantear situaciones difícilmente resolubles como la de los hermanos gemelos idénticos. Sin embargo,

[173] MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA (2011), especificación funcional, 14-15.
[174] HERNÁNDEZ-ARDIETA, J.L./ GONZÁLEZ-TABLAS, A.I./ RAMOS, B. (2012), repudio, 11.
[175] HERNÁNDEZ-ARDIETA, J.L./ GONZÁLEZ-TABLAS, A.I./ RAMOS, B. (2012), repudio, 4.

curiosamente la sociedad no desconfía de la identificación presencial y sí de la electrónica, probablemente porque aquella lleva muchos más años presente en nuestras vidas.

Una vulnerabilidad del sistema, ampliamente reconocida, se centra en el uso de certificados que hayan sido revocados[176] por libre decisión de su titular, porque la clave privada se haya visto comprometida o porque hayan cambiado los datos del mismo (por ejemplo, un certificado de empleado público que haya cambiado de puesto de trabajo o haya pedido la excedencia). Desde el momento de la revocación hasta que dicha información se hace pública y efectiva, transcurre un tiempo en el que el certificado podría ser utilizado ilícitamente. Las listas de certificados revocados se actualizan periódicamente, pero no instantáneamente, siendo habitual un desfase de hasta 24 horas. Durante ese tiempo la VA podría tomar como válido un certificado cuya revocación se está tramitando por la CA. Ello permite que un firmante malintencionado revoque su certificado minutos antes de utilizarlo para firmar, eludiendo así las responsabilidades que hubiera adquirido en dicha operación. Del mismo modo, permite la suplantación de identidad de otro titular, habiéndose apoderado previamente de una clave privada ajena, durante el tiempo de retraso en la tramitación de la revocación que hubiera podido solicitar el afectado. Ello tendría incidencia en operaciones de ejecución inmediata como las transferencias bancarias o el acceso a servicios de pago[177].

[176] HERNÁNDEZ-ARDIETA, J.L./ GONZÁLEZ-TABLAS, A.I./ RAMOS, B. (2012), repudio, 2-3.
[177] HERNÁNDEZ-ARDIETA, J.L./ GONZÁLEZ-TABLAS, A.I./ RAMOS, B. (2012), repudio, 8.

En las incidencias sufridas[178], el elemento más débil de la cadena parece ser claramente el entorno del firmante y, en particular, el compromiso de su clave privada. Los ataques por ingeniería social centran sus esfuerzos en engañar al usuario[179] para realizar determinadas acciones que puedan llevarlo a desvelar su contraseña[180]. Pocas veces se ve a las personas compartir públicamente el número secreto de su tarjeta de crédito, pero muchas no tienen el menor reparo en ceder la contraseña de acceso a distintas aplicaciones informáticas o en instalar su certificado electrónico personal en el ordenador de su secretaria o secretario para que pueda firmar en su lugar. ¡Y cuántas veces el usuario "1234" usa como contraseña "1234", o algo de simplicidad similar! Todas estas actitudes incurren en una incorrecta protección de la clave privada. E incluso, sin pecar de negligencia en la custodia de la clave, puede ocurrir que para su generación se empleen programas inseguros que puedan capturar la clave privada, o que *software* malicioso acceda al almacén de claves del ordenador. La seguridad de la clave también depende del soporte en que se almacene; la clave no puede extraerse de un soporte *hardware*, como es el DNI electrónico, pero sí de un soporte *software*, donde se supedita la seguridad global

[178] Según el estudio sobre la ciberseguridad y confianza en los hogares españoles de ONTSI, p.30, publicado en junio de 2016, correspondiente al período de julio a diciembre de 2016, el 70,5% de los individuos se ha visto afectado en alguna ocasión por algún incidente de seguridad. De ellos, el 87,6% ha recibido *spam* (correos no deseados), el 34,6% ha sido infectado por virus informáticos u otros códigos maliciosos (*malware*), el 9,7% ha perdido el acceso a servicios *on-line* por culpa de ciberataques, el 8,8% ha sufrido pérdidas de información (datos o archivos), al 5,9% le han suplantado su identidad en cuentas de correo electrónico, redes sociales, etc., han accedido sin consentimiento al ordenador u otros dispositivos del 3,9% y lo han perdido o se lo han robado a un 3,4%. Descargado de http://www.ontsi.red.es/ontsi/sites/ontsi/files/ciberseguridad_y_confianza_en_los_hogares_espanoles_junio_2016.pdf (20 de septiembre de 2016).

[179] INTECO (2012), guía sobre riesgos y buenas prácticas, 61.

[180] Como alerta en FUNDACIÓN TELEFÓNICA (2016), ciberseguridad, 2, en muchas ocasiones las contraseñas son lo único que permite acreditar la identidad en las relaciones con las Administraciones públicas, o de los ciudadanos entre sí, o en transacciones económicas,… por lo que la captura de esas contraseñas ha llevado a que se produzcan casos de robo de dinero o de usurpación de la identidad de los usuarios.

de la PKI a la calidad de la contraseña de acceso a ese soporte[181]. Incluso existen prestadores que proporcionan certificados *software* sin ninguna medida de protección que impida el acceso a los mismos por lo que, una vez almacenados en el disco duro del ordenador, cualquiera puede acceder a ellos produciéndose la suplantación de su titular[182].

Resulta altamente recomendable exigir el cambio periódico de contraseñas como medida adicional de seguridad, así como almacenarlas cifradas. La colaboración del usuario para su propia protección pasaría por escoger contraseñas robustas, largas, combinando letras mayúsculas y minúsculas, números y caracteres especiales siempre que estén permitidos, evitando palabras completas y datos personales que facilitarían la tarea del atacante, a lo que hay que añadir la adecuada diligencia en su custodia, sin anotarla en *post-its* pegados en el monitor o guardados en un cajón. No es una práctica segura la de escoger contraseñas iguales para sistemas diferentes puesto que, comprometida una de ellas, ya no permanecerán a salvo las demás[183], a lo que se ha de añadir que la vulnerabilidad de todos ellos será la del sistema más débil.

Existe la posibilidad de que el ordenador firmante contenga *software* malicioso de tipo *keylogger* instalado en él[184], lo que le permitiría averiguar cuáles son las teclas pulsadas por el usuario, descubriendo así la clave introducida.

Los ataques por fuerza bruta consistentes en tratar de averiguar la contraseña del usuario probando todas las posibles credenciales, pueden y deben prevenirse con un adecuado

[181] HERNÁNDEZ-ARDIETA, J.L./ GONZÁLEZ-TABLAS, A.I./ RAMOS, B. (2012), repudio, 7.
[182] BERROCAL LANZAROT, A.I. (2006), la firma electrónica, 430.
[183] INTECO (2012), guía sobre riesgos y buenas prácticas, 54-55.
[184] Las herramientas necesarias se encuentran disponibles en Internet a precios realmente asequibles. Puede encontrarse información al respecto, a modo de ejemplo, en la URL https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf (20 de mayo de 2016).

diseño de las aplicaciones, permitiendo únicamente un número fijo de intentos antes de bloquear el acceso de ese usuario. Habida cuenta de los efectos colaterales provocados al usuario legítimo, al que se impide acceder al aplicativo, existe una posibilidad alternativa de enfrentarse a este tipo de ataque: incorporar un *CAPTCHA* para poder rechazar los intentos de localizar la clave por sistemas automatizados no humanos[185].

Otra clara vulnerabilidad es el libre acceso a las claves en los navegadores *web* donde se permita la firma sin introducir la contraseña cada vez, hábito muy extendido por comodidad, especialmente cuando el volumen de documentos firmados diariamente es elevada. Cualquier usuario de ese equipo podría suplantar al legítimo titular del certificado. El programa que se ejecuta en el ordenador también podría firmar sin que el usuario tuviese conocimiento de que se está haciendo, salvo que esté habilitada la opción de avisar a la persona antes de firmar, pidiéndole confirmación[186].

Existe otra vulnerabilidad aprovechable para lograr que el usuario firme un documento diferente al pretendido. Un *software* malicioso podría estar instalado en el equipo de forma que interfiriese en la elección del documento a firmar, modificándolo o sustituyéndolo por completo. Una contramedida para este ataque pasa por la inclusión de un componente que muestra al firmante el documento que realmente maneja[187].

Existe la posibilidad de insertar código oculto dentro del documento a firmar, de forma que cambie la interpretación o visualización del mismo en función de algún parámetro. El

[185] INTECO (2012), guía sobre riesgos y buenas prácticas, 43-44.
[186] INTECO (2012), guía sobre riesgos y buenas prácticas, 43-44.
[187] INTECO (2012), guía sobre riesgos y buenas prácticas, 43-44.

usuario firma lo que ve en ese momento y, posteriormente, lo que se ve en el documento es algo diferente (el firmante podría haber adquirido un compromiso de pago de 1.000 € y, pasada una determinada fecha u hora posterior a la de la firma, en el documento podría verse la cantidad de 1.000.000 €). Como el contenido del documento no ha cambiado después de firmado, sino que simplemente una macro habría cambiado lo que se visualiza, la firma aparentemente sería válida. La detección de ese código oculto en el momento de la firma es, en la práctica, imposible[188].

A las vulnerabilidades anteriores hay que añadir el posible retardo en el sellado de tiempo, el debilitamiento en la longitud de la clave y los ataques por colisión de funciones *hash*, que permiten al atacante sustituir el documento original por el manipulado manteniendo la validez de la firma realizada. En este último tipo de ataques, es primordial comparar el tiempo que se tarda en encontrar una colisión con el tiempo de validez del documento. Si en un escenario concreto los documentos firmados tienen una validez de horas, el uso de una función *hash* en la que el tiempo necesario para encontrar una colisión sea de días se podría considerar segura[189].

Los ejemplos recién descritos llevarían al ciudadano a repudiar la firma realizada, sumiéndolo en una difícil situación legal.

El DNIe es el dispositivo de autenticación electrónica más extendido en nuestro país[190], distribuido con el objetivo de superar la brecha digital, proporcionando a los ciudadanos

[188] INTECO (2012), guía sobre riesgos y buenas prácticas, 7-8.
[189] INTECO (2012), guía sobre riesgos y buenas prácticas, 9-10.
[190] INTECO (2012), guía sobre riesgos y buenas prácticas, 11.

una firma digital que puedan llevar en su cartera[191], de obligatoria aceptación por todos los sujetos del tráfico jurídico[192].

Incorpora dos certificados, uno para autenticar a su titular y otro para firmar digitalmente, emitidos ambos exclusivamente por el Estado a través de la Dirección general de la Policía nacional[193]. Su utilización requiere su posesión física así como el conocimiento de la contraseña asignada al mismo, que puede ser cambiada por el propio titular, quien demuestra su identidad mediante la lectura de la huella digital en los puntos de actualización existentes en las comisarías, a los que habrá que acudir al menos una vez cada 30 meses para renovar los certificados de la tarjeta. La clave privada está almacenada en el *hardware*, en el microchip, y no puede ser exportada. Su utilización se limita a la autenticación, no siendo imposible emplearlo para cifrar información.

Sin embargo, el uso del DNIe no acaba de generalizarse. En 2013 se produjeron 106.649.275 validaciones de certificados y firmas a través de @firma, pero poco más de un 4% correspondieron al DNIe, exactamente 4.307.123. Del mismo modo, la AEAT recibió el 97% de las declaraciones del IRPF firmadas con un certificado de la FNMT, mientras que la mayoría del 3% restante correspondía al DNIe[194]. No resulta sencillo lograr el funcionamiento de un lector de DNIe en un equipo cualquiera. No solo se requiere poseer ese dispositivo de lectura específico y conseguir que los *drivers* funcionen, sino que se debe introducir el PIN continuamente, saturando

[191] DE QUINTO ZUMÁRRAGA, F. (2006), Documento Nacional de Identidad electrónico.
[192] Sorprendentemente, solo un 19,9 % de los usuarios utiliza certificados digitales de firma electrónica y un 13,5% el DNIe, a lo que hay que añadir que únicamente el 8,8% cifra documentos y datos, según información publicada en MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO (2015), informe anual 2014, 208.
[193] INTECO (2012), guía sobre riesgos y buenas prácticas, 34-35.
[194] Datos obtenidos de la memoria de análisis de impacto del anteproyecto de ley del procedimiento administrativo común de las Administraciones públicas (página 6).

la paciencia del usuario. "*Mientras el ciudadano no pueda insertar el DNI-e en su ordenador y comenzar a trabajar con él directamente, la barrera tecnológica será muy grande (…). Todos los nuevos ordenadores deberían llevar incorporados lectores de tarjetas criptográficas, incluida la del DNI electrónico*"[195]. Habrá que esperar algún tiempo para comprobar los resultados del nuevo DNIe 3.0[196]. Su utilización práctica en las aplicaciones informáticas arrastra, como cualquier otro cambio en el *software* provocado por innovaciones tecnológicas, algunos problemas iniciales que previsiblemente se solventarán, lo que no desmerece el reconocimiento recibido como mejor documento de identidad del año 2016 a nivel europeo[197].

Algunos de los riesgos asociados al proceso de autentificación pueden mitigarse con un diseño seguro de las aplicaciones[198]. Son los desarrolladores y los administradores de los sistemas quienes tienen mayor conocimiento de los riesgos y la seguridad, y a quienes corresponde fijar las condiciones de los procesos de autenticación a programar, debiendo tener en cuenta aspectos como la robustez y complejidad mínima de las credenciales de acceso, el almacenamiento y la transmisión de forma segura y el uso de certificados digitales y firma electrónica[199].

[195] RODRÍGUEZ RICO, J.C. Recuperado de http://www.diariodenavarra.es/noticias/mas_actualidad/cultura/dni_electronico_por_que_funcionado.html (22 de marzo de 2016).
[196] En http://www.dnielectronico.es/PortalDNIe/ pueden consultarse las novedades del nuevo formato.
[197] *Vid*. https://www.dnielectronico.es/PDFs/premio_proyecto_dni3.pdf (accedido el 2 de enero de 2017).
[198] INTECO (2012), guía sobre riesgos y buenas prácticas, 54.
[199] INTECO (2012), guía sobre riesgos y buenas prácticas, 57-58.

El MINHAP ofrece, a todas las Administraciones públicas, la plataforma de servicios de validación y firma electrónica multi-PKI @firma[200] como un servicio de validación de certificados y firmas electrónicas, desacoplado de las aplicaciones, cuyo objetivo es comprobar la validez y no revocación de los certificados utilizados por los ciudadanos, siendo aplicable todos los certificados electrónicos cualificados publicados por cualquier proveedor de servicio de certificación supervisado por el Ministerio de Industria, Turismo y Comercio en España, incluidos los del DNIe. Pero el uso de dichos certificados no convierte automáticamente en seguras a las aplicaciones que los utilizan. @Firma incorpora mecanismos que limitan los riesgos pero, aun así, siguen existiendo otros que hay que prevenir[201]. Entre ellos se incluyen las vulnerabilidades generales de las aplicaciones *web*, susceptibles de ataques por manipulación o falsificación de los valores de los parámetros externos o por ejecución de flujos anormales. Hay que añadir los principales riesgos de los componentes de identificación, que incluyen la autenticación anónima mediante puertas traseras llegadas al entorno de producción, o a través del uso de certificados de prueba proporcionados a los desarrolladores del *software* por las entidades de certificación, la suplantación de identidad por implementaciones defectuosas o el secuestro de sesión[202]. Han de tenerse en cuenta los riesgos específicos del uso del cliente de firma mediante WS y también del uso de la fachada de tickets de @firma, derivados de la manipulación de los parámetros usados en la redirección del navegador y de la alteración en el orden de ejecución del

[200] Información sobre la plataforma de firma @firma disponible en el Portal de Administración electrónica. Recuperado de http://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=afirma#.VvGzj0%20eaISk (2 de enero de 2017).
[201] *Vid*. JUNTA DE ANDALUCÍA. CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA (2012), buenas prácticas.
[202] Sobre la prevención de los ataques que se pueden realizar sobre la gestión de la sesión en páginas web, *vid*. INTECO-CERT (2012), sesiones *web*.

flujo. Por consiguiente, la mayor parte de la seguridad recae sobre los desarrolladores de las aplicaciones.

En relación con @firma, hemos de añadir la enorme dificultad práctica de respetar el principio de neutralidad tecnológica[203], enfrentados a la gran diversidad y dispersión de las tecnologías actuales. Los entornos de ejecución de Java se actualizan cada poco tiempo, pero los trabajos de adaptación requieren varias semanas de pruebas y culminan con la entrega de una nueva versión de las aplicaciones cuando a los usuarios ya no les sirve, por haber migrado, durante la espera, a otra versión de Java más actualizada, entrando en una espiral de mantenimientos evolutivos encadenados que únicamente lleva deterioro del *software* descrito por Pressman que tratamos *supra*. Por experiencia personal, debo sumarme a las palabras de Idoate Gil y García-Merás Capote cuando afirman que "*es completamente imposible acompasar las versiones probadas del producto con el ritmo de actualización de los entornos operativos de los ciudadanos*" [204]. No hace mucho tiempo se hablaba del *miniapplet* de @firma como la gran solución técnica que evitaría los problemas surgidos a consecuencia de la elección de diferentes navegadores o versiones de Java. Hoy, con el *miniapplet* en funcionamiento, la frustración de los usuarios se mantiene inalterada, perdidos en una maraña de dificultades técnicas debidas a la elección de uno u otro navegador, mientras se habla de que la panacea que resolverá todas las dificultades llegará de la mano de AutoFirma[205]. El tiempo les dará o quitará la razón…

[203] *Vid*. LÓPEZ TALLÓN, A. neutralidad tecnológica.
[204] IDOATE GIL, A./ GARCÍA-MERÁS CAPOTE, T. (2013), práctica de la neutralidad, 15.
[205] http://firmaelectronica.gob.es/Home/Empresas/Aplicaciones-Firma.html#autofirma (consultado el 25 de febrero de 2017).

Se retomarán estos aspectos problemáticos recién apuntados en próximos apartados, tras revisar cómo regula nuestro ordenamiento jurídico la firma electrónica.

2.5. CL@VE

Ni los sistemas de firma electrónica basados en certificados, ni tampoco el DNI electrónico que casi todos llevamos en nuestra cartera, parecen haber logrado entrar en la vida cotidiana de la ciudadanía de forma generalizada, algo que parece imprescindible para alcanzar la pretendida extensión de la Administración electrónica. Para permitir la operatividad de los particulares, se ha diseñado el sistema Cl@ve[206], una plataforma común para la identificación, autenticación y firma electrónica, que se ha ideado con la intención de facilitar la operación de los particulares, españoles y extranjeros, ante la Administración, de forma sencilla, unificando y simplificando el acceso electrónico de los ciudadanos a los servicios públicos, permitiendo su identificación ante la Administración mediante el uso de claves concertadas de usuario y contraseña, sin necesidad de recordar claves diferentes para poder acceder a distintos servicios. Aprobado por acuerdo del Consejo de Ministros de 19 de septiembre de 2014[207], sus condiciones de utilización son determinadas por la Dirección de tecnologías de la información y las comunicaciones[208]. Junto a ella, participan en su construcción e implantación y son garantes del sistema la AEAT, la GISS y demás entidades gestoras y servicios comunes de la seguridad social, la DGP y la FNMT-RCM.

---

[206] *Vid*. http://clave.gob.es/clave_Home/clave.html (consultado el 17 de septiembre de 2016).
[207] Resulta recomendable la lectura del acuerdo, publicado en el BOE de 9 de octubre de 2014.
[208] El BOE de 29 de diciembre de 2015 recoge las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema.

Su diseño se basa en la federación de identidades electrónicas, lo que permite que los proveedores de servicios únicamente tengan que integrarse con el denominado "Gestor de identificación", quien será el encargado de establecer las relaciones pertinentes con los distintos sistemas de información.

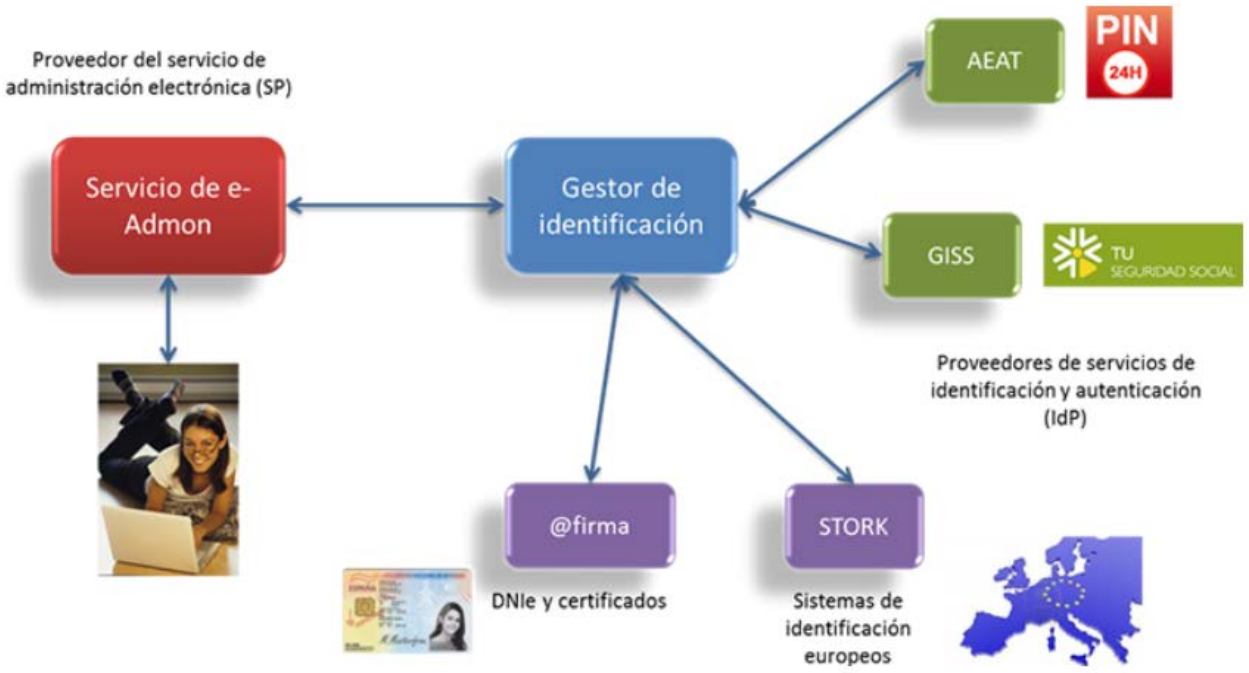

Figura 2: Sistema Cl@ve

FUENTE: http://clave.gob.es/clave_Home/clave/queEs.html

Los ciudadanos que deseen hacer uso de las claves concertadas o de los servicios de firma en la nube deben registrarse previamente, de forma telemática o presencial en cualquiera de las oficinas de los órganos y organismos públicos habilitadas a tal efecto. La forma de registro utilizada será uno de los factores para clasificar el nivel de garantía de identidad y autenticidad asociado, distinguiendo entre el básico, donde los datos los facilita el ciudadano de

forma telemática sin autenticación mediante certificado electrónico reconocido, y el avanzado, donde el ciudadano facilita los datos de forma presencial en una oficina ante un empleado público habilitado al efecto, o de forma telemática, previa autenticación del ciudadano mediante un certificado electrónico reconocido.

A los ciudadanos españoles se les requerirá el DNI en vigor y a los extranjeros la tarjeta de identidad de extranjeros (TIE) o el certificado de ciudadano de la Unión Europea, también en vigor. La posibilidad de registro podrá ser extendida a ciudadanos españoles residentes en el extranjero sin DNI en vigor, mediante la habilitación de procedimientos de verificación de la identidad equivalentes.

En Cl@ve se contemplan dos tipos de sistemas de identificación:

- OCASIONAL o CL@VE PIN: sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios. Se corresponde con el PIN24H de acceso a la AEAT.
- PERMANENTE: sistema de contraseña de validez duradera en el tiempo pero no ilimitada, orientado a usuarios habituales. Se corresponde con el sistema de acceso mediante usuario y contraseña, reforzado con claves de un solo uso por SMS, con los que se accede a los servicios de seguridad social. Con este sistema se permitirá el acceso del ciudadano a la firma en la nube.

Con respecto al acceso a servicios de firma electrónica mediante certificados electrónicos centralizados, el usuario deberá solicitar previa y expresamente su emisión, la cual

se realizará con las mismas garantías de identificación del DNIe. Se requiere que el usuario se haya registrado en nivel avanzado y haya activado su Cl@ve permanente. En el momento de la identificación requerirá una verificación de seguridad adicional mediante un código de un solo uso y validez limitada en el tiempo, recibido por SMS en el teléfono móvil registrado.

El sistema está preparado para incorporar en el futuro, conforme se vayan integrando en el sistema de reconocimiento transfronterizo de identidades electrónicas previsto en la legislación europea, mecanismos de identificación de otros países de la Unión Europea.

Cl@ve garantiza su funcionamiento conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en el ENS, en la LAE y en la normativa de protección de datos, y garantiza la alta disponibilidad del servicio ofrecido.

La Gerencia de informática de la seguridad social (GISS) es responsable de los sistemas de información, las aplicaciones utilizadas y el funcionamiento de Cl@ve permanente, realizando las funciones de identificación y autenticación de usuarios en esta modalidad, para lo que dispone de una copia replicada del fichero de usuarios necesario para verificar la identidad y las garantías de acceso. La seguridad de esas aplicaciones tan delicadas, en relación con el elemento humano que las desarrolla, fuertemente externalizado, será un punto a analizar *infra*.

La ley 39/2015 hace referencia a los sistemas de clave concertada, señalando la posibilidad de que sea admitido como sistema de identificación, lo que recoge específicamente en su artículo 9.2.c), con el tenor de "*Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan*". Por su parte, el artículo 10.2.c), al contemplar los sistemas de firma admitidos por

las Administraciones públicas, se refiere únicamente a "*Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan*". Por lo tanto, parece deducirse del tenor de la ley la prohibición de que los sistemas de clave concertada pueden considerarse como sistemas de firma válidos en ningún término ni condición.

3. LAS BASES JURÍDICAS DE LA eADMINISTRACIÓN

Diversos argumentos apuntan hacia los elementos jurídicos, más que a los tecnológicos y organizativos, como los que condicionan en mayor medida el desarrollo de la Administración electrónica, tanto en el conjunto de la Unión como en cada uno de los Estados miembros.

El ideal utópico de que el ordenamiento jurídico prevea de antemano las situaciones problemáticas que puedan acontecer está notablemente alejado de la realidad. Encarados frente a frente la técnica y su regulación, aunque hayamos afirmado con convicción que aquella no debe marcar el sendero que recorrerá el Derecho, cerraríamos los ojos ante la realidad si no admitiéramos que este reacciona ante los avances científicos y tecnológicos, que van abriendo el camino a recorrer[209].

Reflexiona Piñar Mañas sobre este hecho y nos lleva a plantearnos si, en la situación actual, no es la técnica la que está marcando el rumbo del Derecho, llegando a cuestionar si el contenido de la propia idea de justicia queda condicionado por los avances

[209] Conscientes de esta realidad, el Parlamento europeo y el Consejo se han esforzado en adoptar planteamientos tecnológicamente neutros y abiertos a las innovaciones, "*en razón de la rápida evolución de la tecnología*", como específicamente afirman en el considerando 26 del reglamento eIDAS.

técnicos[210]. Las innovaciones tecnológicas calan en el seno de la sociedad y en la propia actividad administrativa, aquí como fruto de la cláusula del "progreso de la ciencia", incorporación jurídica decimonónica que se mantiene plenamente vigente en la actualidad, imponiendo la incorporación de los adelantos tecnológicos con la necesaria y posterior adaptación normativa dentro del Derecho administrativo[211]. Esas innovaciones técnicas llegan acompañadas de nuevos problemas relacionados con la seguridad informática, que hay que afrontar jurídicamente. Los mensajes pueden ser interceptados, se pueden manipular, es posible negar su validez y la de los documentos electrónicos, existe la posibilidad de acceder a datos personales ilícitamente[212]… Un adecuado marco jurídico puede encauzar estos inconvenientes y mantenerlos bajo control o, al menos, debe intentarlo.

Sin embargo, las nuevas tecnologías no solo afectan al ordenamiento jurídico en cuanto a su contenido, sino que revolucionan incluso la propia forma de entender el Derecho administrativo[213], convertido en la rama del Derecho probablemente más afectada por esta revolución, obligada a enfrentarse con dos retos simultáneos: la adaptación de las Administraciones públicas a esta nueva realidad y la defensa de los derechos del ciudadano, no siempre consciente de los riesgos reales a los que se encuentra expuesto por el mal uso de las nuevas tecnologías por parte del resto de la ciudadanía y de los propios poderes públicos[214].

---

[210] PIÑAR MAÑAS, J.L. (2011), Administración electrónica, 149.
[211] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 56-57.
[212] SALVADOR AYESTARÁN, I. (2001), firma digital, 52.
[213] MARTÍN DELGADO, I. (2009), actuación administrativa automatizada, 354.
[214] BOCANEGRA REQUENA, J.M. Y BOCANEGRA GIL, B. (2011), implantación y régimen jurídico, 27-30. Los autores repasan el día a día de un ciudadano normal, señalando la incidencia de las nuevas tecnologías en su vida y la forma en que le pueden afectar, concluyendo que "*el ciudadano medio, al menos el que vive en una gran ciudad del primer mundo, está absolutamente monitorizado*" y, todo ello, sin entrar en plantearse las actividades de

Acometida con premura, la regulación de la incipiente Administración electrónica ha provocado una explosión normativa en los últimos años, generando un marco regulatorio excesivamente voluminoso[215], complejo y en ocasiones confuso, poco integrador del procedimiento administrativo electrónico con el tradicional y construido sobre este heredando muchos de sus inconvenientes, junto con condicionantes, requisitos y comportamientos no pertinentes en la versión electrónica. Carente de un adecuado análisis de impacto previo, en ciertas ocasiones ha provocado algún incumplimiento de la normativa que aún se mantiene, como es el caso, en nuestro país, de los esquemas nacionales de seguridad e interoperabilidad[216], analizados *infra*.

La problemática descrita no es autóctona ni exclusiva de nuestro país; las soluciones tampoco han de serlo, pero la puesta en funcionamiento de los engranajes de países tan numerosos como heterogéneos, de forma que avancen al unísono en la misma dirección, no resulta una labor sencilla, como veremos a continuación.

3.1. EL EMPUJE DE LA UNIÓN EUROPEA

En cada jurisdicción de los distintos Estados miembros podemos encontrar conceptos legales, requisitos y procedimientos diferentes[217], algo aún más frecuente en relación con las nuevas tecnologías, siempre en incesante y vertiginoso cambio, pero evolucionando a ritmo dispar en cada territorio. Como se verá *infra*, no hay seguridad en ausencia de

organizaciones como la NSA americana. Alertan también del peligro que supondrían estas herramientas informáticas en manos "de *un Hitler o de un Stalin*".

[215] La última versión del Código de Administración electrónica español, disponible para su descarga gratuita en: www.boe.es/legislacion/codigos/ y recuperado el 27 de mayo de 2016, incluía 54 normas y 913 páginas.

[216] GALÁN PASCUAL, C./ MAROTO ILLERA, R. (2013), gobierno electrónico, 27-28.

[217] SALVADOR AYESTARÁN, I. (2001), firma digital, 56.

confidencialidad, sin garantías de autenticidad, con pérdidas de integridad, carente de la disponibilidad adecuada o sin trazabilidad, algo muy difícil de alcanzar si ni siquiera se logra la compatibilidad y la interconectividad a nivel comunitario. Se trata esta de una tarea ardua, complicada con la dificultad de movilizar de forma conjunta a tantos países. No se ha dejado de intentar, una y otra vez, con sucesivos planes, como se verá a continuación, porque la identidad digital del ciudadano no debe encontrar fronteras dentro del territorio de la Unión, ni los sistemas informáticos de los diferentes países pueden dejar de entenderse como si hablaran diferentes idiomas, especialmente en el ámbito público.

Un inconveniente añadido es la atribución de las competencias en materia de organización y funcionamiento de las Administraciones públicas a los propios Estados miembros, a quienes corresponde cualquier decisión relativa a la utilización de las TIC en su seno[218]. Si las instancias de la Unión Europea pretendieran imponer un modelo específico de Administración electrónica, contravendrían el principio de autonomía institucional y procedimental, conforme al cual deben respetar el funcionamiento propio de los Estados miembros[219]. Sin embargo, apoyándose en las posibilidades que ofrecen otras políticas, como las de desarrollo de la sociedad de la información y las telecomunicaciones, investigación y desarrollo tecnológico, redes transeuropeas, desarrollo del mercado interior o de cohesión económica y social[220], las Instituciones europeas sí se han atrevido a establecer un mínimo común, de forma que sus actuaciones resultan cada día más determinantes de la configuración de

[218] ALABAU MUÑOZ, A. (2004), la Unión Europea, 32.
[219] Un análisis pormenorizado del principio referido puede hallarse en el trabajo de Arzoz Santisteban, X. (2013). La autonomía institucional y procedimental de los Estados miembros en la Unión Europea: mito y realidad. *Revista de Administración pública* (191), 159-197.
[220] ALABAU MUÑOZ, A. (2004), la Unión Europea, 32-36.

las diferentes eAdministraciones de los distintos Estados miembros[221]. Juegan en su contra unas actitudes presentes en toda tentativa de cambio, como son la resistencia y el intento de continuar con los procedimientos tradicionales[222].

Las siguientes páginas, aunque densas en sí mismas, resumen someramente los reiterados esfuerzos de las instituciones europeas en su persecución por lograr esos objetivos comunes.

3.1.1. El anciano siglo XX

Volviendo la mirada más de treinta años hacia el pasado, superada la etapa inicial de informatización, la entonces CEE comienza a allanar el camino de la que posteriormente sería una apuesta decidida por las TIC, mediante la aprobación de la **decisión 82/878/CEE**, una de cuyas seis áreas de acción llevaba por denominación "tecnología del programa informático", donde ponía en funcionamiento una serie de proyectos destinados a la creación de *software* común en el marco comunitario, fomentando la colaboración de la industria de las TIC para obtener un método sistemático para el desarrollo común de dichos programas[223].

Simultáneamente, Europa ya era consciente de los riesgos a los que las nuevas tecnologías someten a los derechos de los ciudadanos y, en esa línea, se presentó el **convenio 108**[224] para la protección de las personas con respecto al tratamiento automatizado de datos de

[221] VIDA FERNÁNDEZ, J. (2009), marco normativo comunitario, 59-60.
[222] ORDÓÑEZ SOLÍS, D. (2013), programación, legislación y financiación, 28.
[223] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 68.
[224] Para mayor información sobre el Convenio y su posterior ampliación en 2001, puede consultarse https://www.agpd.es/portalwebAGPD/internacional/Europa/consejo_europa/index-ides-idphp.php (recuperado el 14 de octubre de 2015).

carácter personal[225], del Consejo de Europa, hecho en Estrasburgo el 28 de enero de 1981 y ratificado por España el 27 de enero de 1984, entrando en vigor el 1 de octubre del año siguiente. Se incorpora al Derecho español por la vía del artículo 96 de nuestro Texto fundamental y, a su vez, sirve como criterio de interpretación de los derechos fundamentales, a tenor del artículo 10.2[226]. En él se matiza lo dispuesto explícitamente por nuestra Constitución en su artículo 18.4, no tratando tanto de "limitar" el uso de la informática para garantizar al ciudadano la intimidad personal y el ejercicio de sus derechos, como de "garantizar" el respeto de los derechos fundamentales en relación con la gestión informática de los datos personales, incluyendo el derecho a la vida privada[227].

El convenio establece la obligación, imperativa para cada Parte, de tomar, en su Derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos a la fecha su entrada en vigor, donde destacamos uno con especial incidencia en la obligación de garantizar la adecuada seguridad del *software* de las Administraciones públicas. Nos referimos concretamente a la exigencia de tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no permitida, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

[225] La protección de los datos de carácter personal incluso ha sido recogida en la Carta de los Derechos fundamentales de la Unión Europea de diciembre de 2000 (artículo 8) y en el Tratado de Lisboa, que modifica el Tratado de la Comunidad Europea, cuya entrada en vigor fue en 2009.
[226] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 57.
[227] SANTAMARÍA IBEAS, J.J. (1994), la LORTAD, 268.

A partir de 1984 se suceden los programas ESPRIT[228], RACE[229] y el denominado APLICACIONES TELEMÁTICAS[230], enmarcados dentro de la estrategia comunitaria de investigación y desarrollo en las tecnologías de la información y de las telecomunicaciones. Destaca en nuestra materia, por su preocupación por el desarrollo de la tecnología del *software*[231], el **programa ESPRIT IV**. En el plan de trabajo de ESPRIT[232] se describe el *software* como "*un componente clave de toda una gama de productos y servicios en rápido desarrollo de todos los sectores de la economía europea*" y declara como objetivo general en ese área el de "*garantizar que los profesionales europeos encargados del desarrollo de software de todos los sectores económicos posean las habilidades, capacidad y tecnologías clave necesarias para crear sistemas con uso intensivo de software de gran calidad y pertinencia y responder de manera oportuna a los imperativos y oportunidades del mercado*"[233].

Con la presentación del "Libro blanco sobre crecimiento, competitividad y empleo", en 1993, la Comisión de las Comunidades europeas fijó el **fomento de la sociedad de la información** como una de sus principales propuestas de acción. Tras el sorprendente informe Bangemann, donde no se consideraba relevante la participación del sector público más allá de lo que sería una licitación electrónica, dos años más tarde el "grupo de expertos de alto nivel"

[228] Decisión del Consejo, de 28 de febrero de 1984, referente a un programa europeo de investigación y de desarrollo en el ámbito de las tecnologías de la información (ESPRIT), recuperado de http://www.boe.es/diario_boe/txt.php?id=DOUE-L-1984-80108 (3 de abril de 2016), que fue considerado en los medios informativos de su época como una decisión única en su género, http://elpais.com/diario/1984/02/29/economia/446857212_850215.html, agotó su presupuesto un año antes de su finalización, http://elpais.com/diario/1986/06/19/economia/519516008_850215.html

[229] *Vid.* http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31988D0028&from=ES (recuperado el 3 de abril de 2016).

[230] *Vid.* http://www.rediris.es/difusion/publicaciones/boletin/36-37/enfoque4.html (recuperado el 3 de abril de 2016).

[231] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 74.

[232] *Vid.* http://cordis.europa.eu/pub/esprit/docs/wpespdf.zip (descargado el 27 de mayo de 2016).

[233] *Ibíd*., 11.

contradijo dicha afirmación. Ese mismo sector público antes postergado fue quien abanderó las acciones incorporadas al plan de actuación posterior. El grupo de trabajo 5, encargado del área de temática "Servicios públicos: llevando la Administración cerca de los ciudadanos" llevó a plantear la necesidad de poner en funcionamiento una política específica para la "Administración *on line*" [234].

Las autoridades europeas comienzan a ser conscientes de la importancia de la **interoperabilidad**. La verdadera utilidad de una aplicación informática, como nos indica Gamero Casado, no reside en su uso autónomo, sino en su capacidad de compartir información con otros sistemas, optimizando exponencialmente sus resultados; "*es el mayor paso adelante que se puede lograr en la gestión administrativa, ahorrando cantidades incalculables de tiempo y de dinero a las Administraciones públicas y a los ciudadanos*"[235].

Esa interoperabilidad entre los sistemas de los distintos Estados miembros ha resultado ser un problema trascendental, un objetivo estratégico que ha movido los engranajes comunitarios, actuando en sus distintas dimensiones, no solo técnica[236], sino también organizativa[237], semántica[238] y jurídica[239]. La imposibilidad de que los Estados miembros puedan

[234] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 87-98.
[235] GAMERO CASADO, E. (2009), interoperabilidad, 292-293.
[236] El esquema nacional de interoperatividad, ENI, define la dimensión técnica de la interoperabilidad como la "*relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga*".
[237] Para el ENI es la "*relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan*".
[238] Aparece definida en el ENI como la "*relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación*".
[239] GAMERO CASADO, E. (2009), interoperabilidad, 297. No definida en el ENI, el autor recoge la noción contemplada en el EIF, por la que la interoperabilidad jurídica hace referencia a la "*sincronización adecuada de la*

alcanzar por sí solos ese propósito es lo que otorga legitimación a la Comunidad europea para intervenir en la materia, aun careciendo de competencia específica, con fundamento en el principio de subsidiariedad[240] establecido en el artículo 5 del Tratado de la Unión europea de 7 de febrero de 1992 firmado en Maastricht.

Persiguiendo esa anhelada interoperabilidad, desde el año 1995 se sucedieron los programas[241] IDA (en gestación desde 1991, cuando se argumenta la necesidad de fomentar y coordinar el intercambio de datos entre Administraciones públicas de los distintos Estados miembros)[242], IDA II e IDABC[243].

Afirma Gamero Casado, en materia de interoperabilidad, la extrema utilidad de la licencia pública de la Unión Europea[244], consistente en un contrato de cesión de *software* conforme a la legislación de todos los países miembros y disponible en todos sus idiomas, orientado a promover la reutilización de los programas de Administración electrónica[245]. Desarrollada en el marco de IDABC, esta licencia refuerza la interoperabilidad jurídica "*al adoptar un marco colectivo para la puesta en común del software del sector público*"[246].

---

legislación de un determinado ámbito político para que los datos electrónicos originarios del mismo sean conformes al Derecho aplicable en otros, y se reconozcan recíprocamente cuando ello sea necesario para su utilización en ámbitos distintos del originario". En *Interoperabilidad…*

[240] GAMERO CASADO, E. (2009), interoperabilidad, 304.

[241] MARTÍN GONZÁLEZ, Y. (2009), Unión Europea, 168-169.

[242] ALABAU MUÑOZ, A. (2004), la Unión Europea, 131.

[243] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24147b (recuperado el 2 de abril de 2016).

[244] GAMERO CASADO, E. (2009), interoperabilidad, 332.

[245] GAMERO CASADO, E. (2009), interoperabilidad, 305-306.

[246] Preámbulo de la licencia pública de la Unión Europea, versión 1.1. Recuperado de https://joinup.ec.europa.eu/sites/default/files/eupl1.1.-es_0_0.pdf (3 de enero de 2017).

El "Libro verde sobre información del sector público"[247] incluye los programas IDA y TESS (telemática para la seguridad social) entre los proyectos consolidados en la Unión Europea que posibilitarán la implantación y puesta en funcionamiento de la llamada Administración a distancia[248]. IDA, en particular, promocionó la utilización del *software* libre en las Administraciones públicas[249].

Vigentes los programas IDA e IDABC, el foco de interés de las Administraciones públicas, situado originalmente en el intercambio de datos, fue desplazándose hacia la **prestación de servicios por todo el territorio europeo**; con ello, los servicios telemáticos transeuropeos se convirtieron en servicios paneuropeos de Administración electrónica[250], cuya prestación resulta especialmente compleja por la multiplicidad y heterogeneidad de los sistemas y organizaciones que han de trabajar juntos[251]. Esa noción de Administración electrónica, consistente en la idea de prestar servicios públicos y realizar trámites y procedimientos administrativos por medios electrónicos, informáticos y telemáticos, se importó de Estados Unidos, donde se había bautizado como *e-Government*[252], en 1995, en el seno de la Conferencia ministerial sobre sociedad de la información del G-7 de Bruselas[253].

Ante la necesidad de demostrar la identidad del individuo en sus interrelaciones telemáticas, la recientemente derogada **directiva 1999/93/CE**, del Parlamento europeo y del

[247] ftp://ftp.cordis.europa.eu/pub/econtent/docs/gp_es.pdf (recuperado el 3 de abril de 2016).
[248] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 109.
[249] ALABAU MUÑOZ, A. (2004), la Unión Europea, 152.
[250] AMUTIO GÓMEZ, M.Á. (2006), servicios paneuropeos, 7.
[251] AMUTIO GÓMEZ, M.Á. (2006), servicios paneuropeos, 17.
[252] BOCANEGRA REQUENA, J.M. Y BOCANEGRA GIL, B. (2011), implantación y régimen jurídico, 33. Los autores consideran que la equiparación del concepto del *e-Government* con la eAdministración no resulta adecuada para el Derecho continental europeo.
[253] ALABAU MUÑOZ, A. (2004), la Unión Europea, 99.

Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, fue publicada en el DOCE ya iniciado el año 2000. Vino a facilitar el uso de la firma electrónica y a contribuir a su reconocimiento jurídico, garantizando el correcto funcionamiento del mercado interior[254] y contribuyendo a acortar la distancia que nos separa de los Estados Unidos en el proceso de transformación económica y social a consecuencia de la aplicación de las nuevas tecnologías[255].

Mediante una sucesión de iniciativas y planes de acción se pretendía materializar la aspiración expresada en la denominada **estrategia de Lisboa** de 2000, con una visión para Europa consistente en llegar a ser la sociedad basada en el conocimiento más competitiva del mundo en 2010[256]. Carente de relevancia jurídica inmediata, su fuerza radicaba en el establecimiento de las líneas de actuación que posteriormente se traducirían en medidas concretas[257].

3.1.2. Vislumbrando 2002

Los primeros trabajos encaminados a la implantación de esa ansiada y modélica eAdministración comenzaron en 1999 con la iniciativa *eEurope*[258], presentada en Helsinki, donde se incluye entre las acciones prioritarias a emprender la denominada "Administración pública *on line*", como parte de la política de la sociedad de la información[259].

---

[254] SORIANO MALDONADO, S. (2001), marco regulatorio general, 81.
[255] Aplico aquí a la directiva europea las palabras que dedican a la normativa de firma electrónica europea en MARCOS MARTÍN, J.L./ BALSELLS TRAVER, M. (2000), génesis y regulación, 31-32.
[256] MARTÍN GONZÁLEZ, Y. (2009), Unión Europea, 164.
[257] VIDA FERNÁNDEZ, J. (2009), marco normativo comunitario, 61.
[258] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 99-100.
[259] ALABAU MUÑOZ, A. (2004), la Unión Europea, 59.

La iniciativa se articulaba en una progresión de fases inaugurada con el **plan *eEurope* 2002**, aprobado en el Consejo europeo de Feira de junio de 2000, con la finalidad de alcanzar los objetivos establecidos en el Consejo europeo de Lisboa y la ambición de conseguir los mismos beneficios que una política similar había logrado en Estados Unidos[260], país que nos aventajaba unos diez años en lo referente a la economía del conocimiento[261].

La Comisión ya consideraba la seguridad como una prioridad clave, habida cuenta de que la comunicación y la información se habían convertido en un factor esencial del desarrollo social y económico, considerando crítico el funcionamiento de las redes y los sistemas de información incluso para otras infraestructuras básicas, como son el suministro eléctrico o de agua, constituyendo un requisito previo para el crecimiento del comercio electrónico y para la economía en su conjunto. Era esencial la creación de un clima de confianza en el "entorno en línea" que hiciera disminuir las dudas de los consumidores y de las empresas a la hora de realizar transacciones por vía electrónica, llevando a adoptar nuevos servicios por parte de las Administraciones públicas.

El fomento de una interacción más efectiva y eficaz entre los ciudadanos y la Administración pública conllevaría el intercambio de grandes volúmenes de información de carácter personal, o incluso, confidencial. Por ello, la seguridad era vital para garantizar una utilización eficaz. Las Administraciones públicas, con su modelo de eAdministración, debían ser ejemplos potenciales de soluciones fiables, prever requisitos de seguridad para las TIC y

[260] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 115.
[261] MATÍAS CLAVERO, G. (2005), estrategia de Lisboa, 192.

desarrollar esa cultura de seguridad en su seno, estableciendo políticas adecuadas a esa filosofía, hechas a medida para la institución de que se tratase[262].

Es destacable que la Comisión europea vinculara el impulso de la sociedad de la información con el desarrollo de Internet, dejando a su vez entrever, con el programa IDA, su obsesión por abrir el acceso a la información en manos del sector público al incluir, dentro del objetivo de estimular el uso de Internet, "*la Administración en línea: ofrecer acceso público a los servicios públicos*"[263].

El propósito de este plan se condensaba en la apertura del conjunto de redes de comunicaciones a la competencia, aumentando el número de conexiones a Internet en Europa y estimulando su uso, poniendo un especial énfasis en la formación y la protección de los consumidores[264].

Considerando la confianza del consumidor como un factor clave en el desarrollo del comercio electrónico, *eEurope* 2002 centró su atención en las incipientes modalidades de delincuencia asociadas a las nuevas herramientas tecnológicas[265], destacando el aumento de los perjuicios económicos causados por virus, denegación de servicio, etc., problemas que, unos quince años después, siguen presentes y reforzados en la sociedad de la información actual, en la que la ciberdelincuencia resulta un negocio muy rentable[266].

---

[262] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2001), enfoque político.
[263] ALABAU MUÑOZ, A. (2004), la Unión Europea, 48.
[264] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24226a (recuperado el 30 de marzo de 2016).
[265] *Vid.* http://ciberdelincuencia.org
[266] *Vid.* http://elpais.com/elpais/2016/03/17/opinion/1458242044_459721.html

En *eEurope* 2002 se rechazaba la imposición de soluciones arbitrarias, prefiriendo que el propio mercado determinara el nivel de seguridad adecuado, no sin antes matizar que muchos de los usuarios no eran conocedores de la relativa falta de intimidad de sus transacciones, de los medios disponibles para procurar su protección o de la seguridad de los productos. Señalaba problemas de integración e interoperabilidad de los productos europeos de seguridad con respecto a sistemas operativos, programas y aplicaciones informáticas e incluía, entre las acciones previstas, la de fomentar el desarrollo y la implantación de plataformas de seguridad a base de programas de fuentes abiertas[267] que permitieran una utilización fácil e inmediata ("*plug and play*")[268].

Otra materia que vuelve a estar hoy de ferviente actualidad, la **contratación pública electrónica**, estaba poco extendida en aquellos años, a falta de aclarar su situación legal, necesitada de una importante reforma del procedimiento administrativo. Con esa intención se propuso aprobar dos directivas sobre contratación pública con disposiciones que eliminaran los obstáculos interpuestos y crearan mercados electrónicos para ese tipo de contratación[269].

Los avances en la implantación de la Administración *on line* tienen considerables implicaciones sobre la forma de trabajar de las Administraciones. Requerirán cambios posiblemente difíciles de gestionar, sufriendo restricciones notables en los intentos de desarrollo de los servicios paneuropeos, motivadas por la desigual normativa imperante en los diferentes

[267] Para mayor información sobre *software* libre y *software* de fuentes abiertas, *vid.* http://www.cenatic.es/sobre-el-*software*-libre (recuperado el 3 de abril de 2016) y también el trabajo de CENATIC titulado "Introducción al *software* de fuentes abiertas. Tecnologías libres para personas libres", publicado en *Cuadernos de información tecnológica* y recuperado de http://www.cenatic.es/publicaciones/divulgativas el 3 de abril de 2016.
[268] Plan de acción *eEurope* 2002, 11.
[269] Plan de acción *eEurope* 2002, 18-20.

Estados miembros. La ruta adecuada hacia el éxito pasa por fomentar las mejores prácticas de eAdministración mediante el intercambio de experiencias en toda la Unión, potenciando la utilización de programas de fuentes abiertas y el uso de la firma electrónica en el sector público. Esa novedosa eAdministración debía permitir el acceso electrónico a los servicios públicos, con la puesta a disposición de los ciudadanos de la información pública esencial en línea y la creación de procedimientos administrativos simplificados *on line* para las empresas. Se establecía la obligación para los Estados miembros de garantizar un acceso electrónico generalizado para los principales servicios públicos[270], seleccionados y catalogados en una lista que incluía 12 de ellos para los ciudadanos y 8 para las empresas, inventario que hoy sigue siendo un marco de referencia en el sector[271].

En el terreno normativo, el Parlamento europeo y el Consejo nos dejan su **reglamento (CE) nº 45/2001**, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Creador de la figura del Supervisor europeo de protección de datos, que se encarga de vigilar y controlar el tratamiento de datos que realizan las instituciones y agencias de la Unión del primer pilar, ha llevado también al emplazamiento, en cada institución o agencia, de un encargado de asegurar la aplicación de sus disposiciones[272].

[270] Plan de acción *eEurope* 2002, 21-22.
[271] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 125-126.
[272] NIETO GARRIDO, E. (2014), transparencia y acceso, 73-74.

La seguridad del tratamiento se afronta en su artículo 22, remitiéndose a los conocimientos técnicos existentes y teniendo en cuenta el coste de su aplicación; con esas consideraciones, señala la obligación de poner en práctica las medidas de carácter técnico y organizativo adecuadas para garantizar un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse, especialmente para evitar la comunicación o el acceso no autorizados, la destrucción accidental o ilícita, o cualquier pérdida accidental o alteración, así como cualquier otra forma ilícita de tratamiento.

En 2002, la Unión Europea aprobó un nuevo marco regulador de las comunicaciones electrónicas. Tras su liberalizador predecesor de 1998, vino a regular de modo comprensivo las telecomunicaciones en Europa, con un cambio radical[273] que se refleja en la notable producción de **directivas** en busca de un nivel uniforme de protección en todo el territorio comunitario[274], con intención de avanzar en la eliminación de normas no justificadas por criterios de regulación óptima o de competencia, que pudieran tener efectos contraproducentes sobre la inversión y la innovación, tratando de limitar la regulación

[273] GÓMEZ-BARROSO, J.L./ FEIJÓO GONZÁLEZ, C./ RAMOS VILLAVERDE, S., marco europeo, 918-920.

[274] Directiva 2002/19/CE del Parlamento europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (directiva de acceso); Directiva 2002/20/CE, del Parlamento europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (directiva de autorización); Directiva 2002/21/CE, del Parlamento europeo y del Consejo de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas; Directiva 2002/22/CE del Parlamento europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (directiva de servicio universal); Directiva 2002/58/CE del Parlamento europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre privacidad y las comunicaciones electrónicas) modificada por la directiva 2006/24/CE, del Parlamento europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. La directiva 2009/136/CE del Parlamento europeo y del Consejo, de 25 de noviembre de 2009 modificó las directivas 2002/22/CE y 2002/58/CE.

únicamente a aquellos mercados cuya estructura todavía no permitiera una competencia efectiva entre los operadores[275]. Culminaron en 2002, por tanto, seis normas en las que la idea subyacente era la confianza depositada en las reglas generales de defensa de la competencia, en concreto, una directiva marco, cuatro directivas específicas (de autorización, de acceso, de servicio universal y sobre protección de datos) y una decisión (sobre espectro radioeléctrico)[276].

La legislación española incorporó al año siguiente el "paquete telecom" de directivas de 2002, profundizando así en los principios ya consagrados en la normativa anterior, basados en un régimen de libre competencia, introducción de mecanismos correctores que garanticen la concurrencia de operadores distintos al del antiguo monopolio, protección de los derechos de los usuarios, mínima intervención de la Administración, respeto de la autonomía de las partes y supervisión administrativa de aspectos relacionados con el servicio público, el dominio público y la defensa de la competencia[277]. Tras la experiencia de cuatro años de funcionamiento, se iniciaría un proceso de revisión iniciado a finales de 2007[278].

3.1.3. Nuevo horizonte 2005

Las actividades en materia de Administración electrónica llevadas a cabo por la Comisión hasta el momento se habían caracterizado por su fragmentación y falta de coherencia[279]. Concienciada de que el hito previsto para 2010 no parecía alcanzable, dadas las inercias de la Administraciones, los múltiples intereses involucrados y las posibles insuficiencias

[275] CALVIÑO SANTAMARÍA, N. (2006), regulación y competencia en telecomunicaciones, 68.
[276] GÓMEZ-BARROSO, J.L./ FEIJÓO GONZÁLEZ, C./ RAMOS VILLAVERDE, S., marco europeo, 920-921.
[277] Exposición de motivos de la ley 32/2003, de 3 de noviembre, general de telecomunicaciones.
[278] MARTÍ DEL MORAL, A./ DE LA TORRE MARTÍNEZ, L., servicio público, 356.
[279] ALABAU MUÑOZ, A. (2004), la Unión Europea, 86.

en el diseño del programa, la Comisión europea reformuló y reorientó su estrategia[280]. El plan de acción ***eEurope* 2005**, aprobado por el Consejo europeo de Sevilla en junio de 2002, vino a suceder al que culminaba ese mismo año y que se había dirigido a la extensión de la conectividad a Internet. El nuevo plan se orientó a materializar esa conectividad en un aumento de la productividad económica, con una mejora de la calidad y la accesibilidad de los servicios, basándose en una infraestructura de banda ancha segura disponible para la mayoría de los ciudadanos europeos[281], con el desarrollo del protocolo IPv6[282].

Con todo ello, Europa seguía sin una verdadera política de Administración electrónica, siendo las actuaciones en este campo meros instrumentos para otros objetivos[283].

Consciente de la obligación de mejorar la eficiencia, productividad y calidad de los servicios públicos, restringidos por presupuestos incluso decrecientes, la Comisión[284] vuelve a enfocar su atención en la Administración electrónica, que define como "*el uso de las TIC en las Administraciones públicas, 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*"[285], señalando la necesidad de crear un clima de confianza en la interacción *on line*, generalizar su uso, lograr la interoperabilidad para el intercambio de información e impulsar los servicios paneuropeos.

---

[280] ECHEVARRÍA EZPONDA, J. (2007), gobernanza, 68.
[281] Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24226 (30 de marzo de 2016).
[282] *Vid.* http://www.ipv6.es/es-ES/introduccion/Paginas/QueesIPv6.aspx
[283] ALABAU MUÑOZ, A. (2004), la Unión Europea, 54.
[284] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2003), papel de la administración electrónica, 7.
[285] BOCANEGRA REQUENA, J.M. Y BOCANEGRA GIL, B. (2011), implantación y régimen jurídico, 33-39. Los autores realizan un detallado estudio de las diferentes aproximaciones al concepto de Administración electrónica.

De nuevo se repite la invocación a la imprescindible confianza y el problema de la interoperabilidad, dos constantes reiteradas a lo largo de los años. Para lograr ese entorno de confianza, se ha de garantizar la seguridad de las comunicaciones digitales y la protección de los datos personales, permitiendo al ciudadano su control[286]; para acercarse al sueño de la interoperabilidad, se aprueba el **marco europeo de interoperabilidad, EIF**, vinculante para todos los proyectos financiados con el programa IDABC, vivamente promovido entre los Estados miembros y espontáneamente aceptado por las empresas, conscientes del valor añadido que otorga a sus productos y servicios la acomodación al mismo[287].

La **contratación pública electrónica**, inconclusa, fue una de las principales áreas de mejora que se volvió a contemplar en el nuevo plan de acción, previendo la aprobación de un paquete de directivas que clarificara la normativa comunitaria. Se requería facilitar la entrega de certificados digitales y la disponibilidad de firmas electrónicas en toda Europa, no sin advertir del riesgo de que los certificados no fueran aceptados por igual en las aplicaciones informáticas de todos los países, constituyendo un obstáculo a la participación transfronteriza en la contratación pública electrónica[288].

A pesar de la encendida defensa de la **Administración electrónica**, la Comisión era cauta a la hora de pronosticar los avances en la materia, señalando que podrían pasar años

[286] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2003), papel de la administración electrónica, 14.
[287] GAMERO CASADO, E. (2009), interoperabilidad, 307.
[288] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2003), papel de la administración electrónica, 16-18.

antes de cosechar los beneficios augurados, requiriendo durante el camino a recorrer un vigoroso liderazgo y compromiso político[289].

Aunque los resultados obtenidos en los primeros cinco años de desarrollo de estos planes de acción fueron positivos[290], las reformas de Lisboa resultaron necesarias pero fueron insuficientes; los demás países se movieron incluso con más celeridad en la misma dirección. Los Estados Unidos mantuvieron su adelanto frente a Europa y surgieron países más dinámicos en Asia e Iberoamérica[291].

Una problemática constante y aún no resuelta emana de la falta de homogeneidad entre las distintas Administraciones, incluso en el ámbito del mismo Estado, las cuales no disponen de interfaces comunes ni sistemas de autenticación compatibles, impidiendo la conservación de la identidad digital al cambiar de un sistema a otro, de una Administración a otra, de un Estado miembro a otro. Los problemas estructurales que dificultan la recepción de las nuevas tecnologías por las Administraciones públicas se suman a los otros obstáculos, a lo que debemos añadir la falta de adaptación de las organizaciones y el déficit de capacitación de sus responsables[292].

3.1.4. Panorámica para 2010

Con la trasposición en todos los Estados miembros de la **directiva 2006/123/CE** del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el

[289] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2003), papel de la administración electrónica, 25.
[290] VIDA FERNÁNDEZ, J. (2009), marco normativo comunitario, 70.
[291] MATÍAS CLAVERO, G. (2005), estrategia de Lisboa, 193.
[292] VIDA FERNÁNDEZ, J. (2009), marco normativo comunitario, 72.

mercado interior, se materializan los principales avances en la implantación de la eAdministración. Se trata de una directiva de alcance general cuyo objetivo[293] es la consecución de un auténtico mercado único de servicios, reduciendo o incluso suprimiendo las diversas barreras legales y administrativas, aumentando la seguridad jurídica, disminuyendo cargas administrativas, instaurando la ventanilla única y simplificando y sustituyendo los procedimientos administrativos por su versión electrónica. Toda esta metamorfosis va a transfigurar el modo de actuar de las Administraciones, que proceden a una supresión generalizada de requisitos formales.

La tramitación electrónica de los procedimientos administrativos se plantea de forma sistemática y obligatoria, con fecha de realización, novedad que la diferencia de las acciones contempladas en los planes *eEurope*. Se ofrece la oportunidad, no la obligación, de utilizar medios electrónicos durante el procedimiento completo, desde la solicitud hasta la resolución, posibilidad que se dirigirá no únicamente a los nacionales, sino a quienes residan o se encuentren establecidos en otros países miembros, exigiendo a estos Estados que eviten la creación de cargas adicionales y la adopción de soluciones que a largo plazo dificulten la interoperabilidad[294].

2006 supone también el abandono parcial de la estrategia *eEurope*, con la presentación por la Comisión de su **plan de acción sobre Administración electrónica i2010**, destinado a incrementar la eficacia de los servicios públicos, a modernizarlos y a ajustarlos a las necesidades de la población. Entre dichas necesidades, destaca una vez más la disposición de una

[293] VIDA FERNÁNDEZ, J. (2009), marco normativo comunitario, 76.
[294] VIDA FERNÁNDEZ, J. (2009), marco normativo comunitario, 76-78.

identidad digital única con la que poder acceder a todos los servicios, ya sean privados o públicos[295]. La novedad que supone un cambio estratégico más radical es la pretensión de crear un espacio único europeo de la información, coordinando las legislaciones y políticas de los Estados miembros en la materia[296].

La Comisión, con este plan i2010, marca una serie de prioridades y define una hoja de ruta que acelerará la implantación de la Administración electrónica en Europa[297], con el propósito de generar unos beneficios sustanciosos y medibles en 2010, para lo que resulta imprescindible elaborar un marco normativo adecuado en cada uno de los países miembros[298]. Sus grandes objetivos son fortalecer la participación y la adopción de decisiones democráticas y hacer realidad la eficiencia y eficacia, sin dejar atrás a ningún ciudadano, implantando servicios esenciales de gran repercusión, como el 100% de la contratación pública electrónica, estableciendo herramientas clave que permitan un acceso cómodo, seguro e interoperable a los servicios públicos[299].

Reconociendo el trabajo pendiente de desarrollar para conseguir el respeto por las Administraciones públicas de las directrices sobre accesibilidad electrónica de sus páginas *web*, al igual que para avanzar hacia soluciones transfronterizas (especialmente en referencia a la contratación pública electrónica), la Comisión identifica como **herramientas clave** críticas para su impulso la autenticación de documentos digitales, el archivado electrónico y la gestión interoperable de la identidad electrónica para el acceso a los servicios públicos, de forma

[295] SÁNCHEZ GARCÍA, S. (2012), tendencias pan-europeas, 1.
[296] ECHEVARRÍA EZPONDA, J. (2007), gobernanza, 76.
[297] Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24226j (30 de marzo de 2016).
[298] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 142-143.
[299] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2006), acelerar la administración electrónica, 4-5.

respetuosa con los diversos enfoques y soluciones nacionales. Para superar los obstáculos, fomenta el reconocimiento mutuo de las firmas electrónicas entre los distintos países. Con respecto a la interoperabilidad, declara la necesidad de unas especificaciones comunes y unos programas informáticos reutilizables[300].

En el Tecnimap[301] de 2007 se habla del DNIe como un habilitador para el uso de técnicas de identificación seguras y de firma electrónica en nuestro país, y de @firma[302] como catalizador para el desarrollo de servicios de eAdministración seguros, anunciando que, en breve[303], dicha plataforma aceptará otras eIDs europeas[304].

3.1.5. En camino hacia 2020

Nos advierte Linares Gil del riesgo de que nuestras Administraciones públicas se conviertan en "*una moderna y electrónica torre de babel*" si cada una de ellas tiene libertad para admitir sistemas de firma electrónica, al margen del DNIe[305]. El problema se acrecienta a nivel internacional. La interoperabilidad y la identidad transfronteriza continúan siendo retos pendientes para la Unión.

El DOUE de 3 de octubre de 2009 publicó la decisión 922/2009/CE del Parlamento europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de

[300] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2006), acelerar la administración electrónica, 9-10.
[301] Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_lineas_ccoperacion/pae_Tecnimap.html (21 de mayo de 2016).
[302] Recuperado de http://administracionelectronica.gob.es/es/ctt/afirma#.V0AK_75WgSk (21 de mayo de 2016).
[303] Brevedad y aceptación son conceptos abiertos a interpretación. Transcurridos 10 años, en los servicios informáticos de algunas Administraciones públicas comienza ahora a hablarse de la posibilidad de aceptar certificados de prestadores europeos, motivado por la entrada en vigor del reglamento europeo eIDAS, del que hablaremos *infra*.
[304] ÁLVAREZ RODRÍGUEZ, M. (2007), consorcio de AA.PP. europeas STORK.
[305] LINARES GIL, M.I. (2008), identificación y autenticación, 298.

interoperabilidad para las administraciones públicas europeas (ISA), donde se establece, para el período de 2010-2015, el **programa ISA**, relativo a las soluciones de interoperabilidad de las Administraciones públicas europeas que proporcionará, entre otras soluciones comunes y compartidas, la mejora de las herramientas genéricas reutilizables existentes y la creación, el suministro y la mejora de otras nuevas, siempre desde el respeto de los principios de neutralidad[306], apertura, reutilización, seguridad y privacidad y protección de los datos personales.

Seis años más tarde, en el DOUE de 4 de diciembre de 2015, encontramos la decisión (UE) 2015/2240 del Parlamento europeo y del Consejo de 25 de noviembre de 2015, por la que se establece, para el período 2016-2020, un programa relativo a las soluciones de interoperabilidad y los marcos comunes para las Administraciones públicas, las empresas y los ciudadanos europeos (**programa ISA^2**) como medio de modernización del sector público. Consciente de que cada vez es mayor el número de servicios públicos han de convertirse en "digitales por defecto", confirma la necesidad de extremar la eficiencia del gasto público en soluciones de TIC, lo que se facilita aprovechando al máximo la compartición y reutilización de las soluciones desarrolladas, entre las que se encuentran sistemas operativos, aplicaciones e infraestructuras digitales[307]. A estos efectos, el programa ISA^2 fomentará la utilización de una plataforma que permita la difusión de las soluciones disponibles, incluyendo los marcos en

[306] La neutralidad del *software* de nuestras Administraciones públicas con frecuencia no resulta tan satisfactoria como sería de esperar. Con frecuencia las aplicaciones funcionan de forma diferente dependiendo de los navegadores utilizados. A modo de ejemplo, un programa podría no funcionar con Chrome, mostrar una maquetación poco legible con Internet Explorer y funcionar perfectamente con Mozilla Firefox, todo lo cual podría invertirse si se utilizan diferentes versiones de cada uno de los navegadores.
[307] Así se deduce de la definición de "servicios comunes" recogida en su artículo 2.

materia de protección y seguridad, evitando la duplicación de esfuerzos, lo que se materializará, como veremos, en una de las opciones de provisión de *software* para las Administraciones públicas, la referida a la reutilización de las aplicaciones elaboradas o adquiridas por otros organismos.

La estrategia Europa 2020 vuelve a poner el foco de atención en el logro del óptimo desarrollo de la sociedad de la información e incluye, entre sus siete iniciativas clave, la **Agenda Digital para Europa (2010-2020)**, aprobada por la Comisión durante la Presidencia española de la Unión del primer semestre de 2010, con la finalidad de obtener unos beneficios económicos y sociales sostenibles[308] e impulsar la economía europea aprovechando las ventajas del mercado único digital[309]. En ella se señala la fragmentación de ese mercado digital, la falta de interoperabilidad y el incremento de la ciberdelincuencia como importantes obstáculos para el ciclo virtuoso de la economía digital[310], aspectos que ya preocuparon con anterioridad a la Unión. Entre sus retos figuran el desarrollo de la banda ancha, el nuevo diseño del mercado europeo de las telecomunicaciones y el fomento de un entorno amistoso para los consumidores[311].

---

308 http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_lineas_ccoperacion/pae_Cooperacion_Internacional/pae_estrategias_de_administracion_electronica/pae_Ambito_Europeo_-_Sociedad_de_la_Informacion.html#.Vv1TyUdWgSk

309 Sobre el mercado único digital, *vid.* la URL http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_5.9.4.html (recuperado el 3 de abril de 2016).

310 Así se recoge en el considerando 4 del nuevo reglamento eIDAS.

311 Recuperado de http://europa.eu/pol/pdf/flipbook/es/digital_agenda_es.pdf (31 de marzo de 2016).

La Agenda Digital se comprometió a enfrentarse al problema de la cautividad, ayudando a las autoridades públicas a utilizar las normas para promover la eficiencia y reducir la dependencia de proveedores concretos[312].

Con la pretensión de hacer realidad los objetivos imaginados en Malmö, la Comisión publica un nuevo y ambicioso plan de acción sobre Administración electrónica, que establece como prioridades políticas reforzar la posición de ciudadanos y empresas, la movilidad en el mercado único y el alcance de la eficacia y eficiencia, todo ello logrado mediante los habilitadores clave apropiados y las precondiciones legales y técnicas, donde hemos de incluir los ya clásicos interoperabilidad, firma electrónica e identificación electrónica[313]. Si bien el plan i2010 no contemplaba la evolución de las tarjetas identificativas tradicionales hacia las *eID cards*, el nuevo **plan 2011-2015**, incluye como prioridad el establecimiento de sistemas interoperables en los ámbitos de identificación y de autenticación en el territorio de la Unión. Esas tarjetas identificativas electrónicas, entre las que se encuentra nuestro DNIe, son similares a las tradicionales, pero incorporan un chip donde se almacena información identificativa del ciudadano[314].

Todos los países de la Unión han estado desarrollando iniciativas para la gestión de la identidad digital, pero la globalización llega acompañada de inconvenientes también en este terreno. Un ciudadano de un Estado miembro normalmente no puede utilizar su identificación

---

312 Comunicación de 2013 de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones contra la dependencia de un proveedor: construir sistemas de TIC abiertos mediante una mejor utilización de normas en la contratación pública, COM/2013/0455 final, descargada de http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52013DC0455&rid=1 (30 de diciembre de 2016).

313 COMISIÓN EUROPEA (2010), aprovechamiento de las TIC.

314 SÁNCHEZ GARCÍA, S. (2012), tendencias pan-europeas, 2.

electrónica para autenticarse más allá de las fronteras de su propio país, debido a la falta de reconocimiento de los sistemas nacionales en el resto de la Unión, alzando una barrera electrónica que excluye a los prestadores de servicios del pleno disfrute de los beneficios del mercado interior[315]. El DNI físico sigue siendo válido para identificar a un ciudadano español más allá de los límites de nuestro territorio, pero no ocurre lo mismo con el DNIe ni con otros certificados digitales de prestadores nacionales, debido a que los sistemas de gestión de identidad electrónica no son compatibles a nivel paneuropeo[316]. La existencia de diferentes eIDMs en los distintos Estados miembros sigue originando arduos problemas de continuidad transfronteriza de los servicios públicos, por lo que deviene imprescindible el establecimiento de un marco de interoperabilidad sobre la idea de federación de identidad o confianza mutua entre las Administraciones de los países de la Unión en cuestión de métodos de identificación y autentificación. La identidad digital de un usuario, antes administrada por un único proveedor, ahora pasa a ser común a varios, complicando la gestión de su registro, modificación o revocación, aumentando los riesgos de seguridad, las dificultades de incompatibilidad semántica por la disconformidad de sus formatos y los desencuentros entre los diversos sistemas normativos implicados, algunos de los cuales obligan a portar documentos identificativos mientras otros no[317]. Parece indispensable especificar y desarrollar los adecuados sistemas de gestión de identidad, IDMs o eIDMs, entendiendo como tal un conjunto de infraestructuras técnicas y organizativas que permitan la definición, administración y gestión de los atributos relativos a la identidad de los ciudadanos y, con ello, un entendimiento que permita la aceptación

[315] Así lo reconoce el considerando 9 del reglamento eIDAS.
[316] SÁNCHEZ GARCÍA, S./ GÓMEZ OLIVA, A., interoperabilidad pan-europea.
[317] SÁNCHEZ GARCÍA, S. (2012), tendencias pan-europeas, 3-4.

mutua de la identificación digital, con estricto respeto al principio de subsidiariedad por el que cada Estado miembro debe mantener su autonomía y responsabilidad[318].

Respondiendo a la invitación de la Comisión europea por la que insta a las Administraciones públicas a realizar pruebas piloto de interoperabilidad[319] orientadas a proporcionar servicios de eID transfronteriza, el entonces denominado MAP[320] es parte del Consorcio de 21 Administraciones públicas y 8 empresas de 14 países europeos[321] bautizado como STORK[322], o cigüeña, el ave migratoria más común en Europa, que pasa a simbolizar la movilidad de trabajadores y de ciudadanos en general, grandes beneficiados por los avances en materia de eIDM[323]. Conlleva para nuestro país la aceptación de certificados digitales españoles como el DNIe en servicios de eAdministración de otros países[324]. STORK se basa en estudios realizados por IDABC describiendo un modelo federado y tecnológicamente neutral, que soporta múltiples niveles de autenticación. En este modelo se requiere la creación de, al menos, un proveedor de identidad a nivel nacional, que se unen a una red de *proxies* proveedores de servicios, denominados PEPS, cuya función principal es conectar a los proveedores de servicios con los proveedores de identidad en cada país y validar la confianza y seguridad de la información de identidad enviada por estos. Se contempla la posibilidad de que los *proxies* sean

[318] SÁNCHEZ GARCÍA, S./ GÓMEZ OLIVA, A., interoperabilidad pan-europea
[319] *Vid.* ÁLVAREZ RODRÍGUEZ, M. (2007), consorcio de AA.PP. europeas STORK.
[320] Con el nombre actual de MINHAP, es el proveedor nacional de servicios comunes de identificación electrónica y firma a través de su plataforma de servicios de validación y firma electrónica @firma que, entre otros *tokens* o eIDs verifica el DNI electrónico español.
[321] Alemania, Austria, Bélgica, Eslovenia, España, Estonia, Francia, Holanda, Italia, Islandia, Portugal, Luxemburgo, Reino Unido y Suecia.
[322] Acrónimo de ***S****ecure iden****T****ity acr****O****ss bo****R****ders lin****K****ed.*
[323] ÁLVAREZ RODRÍGUEZ, M. (2007), consorcio de AA.PP. europeas STORK.
[324] ÁLVAREZ RODRÍGUEZ, M. (2011), el DNIe español.

nacionales, europeos o incluso que se trate de un modelo mixto en el que coexistan países que confíen en un PEPS nacional y otros en uno europeo[325].

Además del programa ISA, sustituto de IDABC, dedicado a continuar la búsqueda de la interoperabilidad para las Administraciones públicas europeas. Destacables son también otros proyectos como SPOCS (*Simple Procedures Online for Crossborder Services*) para la implantación de ventanillas únicas para servicios transfronterizos y PEPPOL (*Pan-European Public eProcurement On-line*), plan piloto en contratación pública electrónica[326].

Con el objetivo de mejorar la legislación existente sobre firma electrónica y ampliarla con el reconocimiento y aceptación mutuos entre los países miembros "*de los sistemas de identificación electrónica notificados y otros servicios de confianza electrónicos conexos esenciales*"[327], vio la luz el 4 de junio de 2012 en Bruselas, una propuesta de reglamento del Parlamento europeo y del Consejo, publicado dos años después en el DOUE de 28 de agosto de 2014 como **reglamento (UE) 910/2014** del Parlamento europeo y del Consejo de 23 de julio del mismo año, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la directiva 1999/93/CE. Este reglamento, conocido con el nombre de eIDAS, entra en vigor el 1 de julio de 2016, afectando a la normativa básica de identificación y de firma. Su adopción en forma de reglamento lo convierte en el paso más firme que ha dado la Unión para demoler las barreras electrónicas que separan a los ciudadanos europeos.

[325] SÁNCHEZ GARCÍA, S./ GÓMEZ OLIVA, A., interoperabilidad pan-europea
[326] ORDÓÑEZ SOLÍS, D. (2013), programación, legislación y financiación, 27.
[327] Propuesta de reglamento del Parlamento europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Bruselas, 4 de junio de 2012. Recuperado de http://www.ipex.eu (3 de abril de 2016).

Publicado el dictamen favorable del CESE sobre la propuesta en el DOUE de 15 de noviembre de 2012, alaba su planteamiento tecnológicamente neutral y abierto a la innovación, pero lamenta que no haya llegado más lejos al no atreverse a proponer una identificación electrónica *de facto* y *de iure* para una determinada serie de servicios, una eID europea estandarizada que pudieran solicitar todos los ciudadanos de forma voluntaria y que permitiera la armonización de los distintos sistemas nacionales, todo ello desde el respeto de la competencia de los Estados miembros en cuanto a la regulación de la prueba de identidad, así como de los principios de subsidiariedad y proporcionalidad. Por otra parte, consciente de las preocupaciones de las personas en materia de privacidad y seguridad, que se magnifican cuando no se entienden las tecnologías utilizadas, generando un innecesario temor y resistencia, el CESE recomienda que la aplicación del reglamento vaya acompañada de una adecuada campaña informativa.

El reglamento eIDAS establece las condiciones en que los Estados miembros deberán reconocer los sistemas de identificación electrónica de otro país de la Unión, las normas para los servicios de confianza y un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios *web*. Consciente de la vertiginosa mutabilidad tecnológica, adopta un planteamiento declaradamente neutral y abierto a la innovación, con vocación de permanencia y respetuoso con los trabajos de normalización técnica y de desarrollo de los procesos STORK. Así se desprende de su artículo 12 donde, además, se muestra defensor del respeto a la protección de datos de carácter personal,

exigiendo facilitar la aplicación del principio de privacidad desde el diseño y garantizar lo dispuesto en la Directiva 95/46/CE.

De interés en nuestra materia es lo apuntado por el considerando 65, referente a la utilización de los sellos electrónicos para autenticar cualquier activo digital de la persona jurídica, citando como ejemplo los programas informáticos o servidores. También cabe destacar los artículos 27, bajo la rúbrica de "firmas electrónicas en servicios públicos" y 37, titulado "sellos electrónicos en servicios públicos", incidirán plenamente sobre el *software* de nuestras Administraciones, junto con el 45, que incluye los "requisitos de los certificados cualificados de autenticación de sitios *web*". Este nuevo reglamento contempla el uso de pseudónimos en los certificados, indicando que no se debe impedir a los Estados miembros exigir la identificación de las personas de conformidad con el Derecho nacional o de la Unión y estableciendo la obligatoriedad de indicar tal circunstancia claramente en el momento de la firma.

Su entrada en vigor acarrea cambios importantes para los prestadores de servicios de certificación y para las plataformas de firma electrónica como @firma, con repercusiones en las aplicaciones informáticas que las utilizan. Con el reglamento surgen nuevos tipos de certificados y desaparecen otros específicos de la LFE, como el de persona jurídica y el de entidad sin personalidad jurídica, que dejan de renovarse y, en muchos casos, pasan a considerarse certificados no reconocidos/cualificados. El nuevo certificado de firma equivale al anterior de persona física de la LEF. El certificado de sello del reglamento eIDAS tiene similitudes con el de persona jurídica de la LFE, hecha la salvedad de que no lleva asociado a un

custodio o responsable del certificado; con él se puede garantizar el origen e integridad de los datos y autenticar el documento expedido por la persona jurídica o cualquiera de sus activos digitales, incluyendo programas informáticos o servidores. A tenor del artículo 58, cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe aceptarse igualmente la firma electrónica cualificada del representante autorizado, obligación que no se reconoce en sentido inverso. Contempla también un certificado de autenticación *web* con el que vincular el sitio *web* (dominio de Internet) con su titular, ya sea persona física o jurídica, y un certificado no cualificado, sin garantía de que vaya a ser validado, no admitido para su uso como certificado de persona física por la nueva ley 39/2015[328].

A pocas semanas de su entrada en vigor, las Administraciones públicas tuvieron que ultimar las adaptaciones de sus aplicaciones informáticas para que contemplaran las novedades introducidas por el reglamento. Si recordamos la curva de fallos del *software* de Pressman representada en la figura 1, se encontrarían en uno de los picos en que se dispara la tasa de errores. La complejidad aportada por la diversidad de prestadores de servicios de certificación europeos incidirá negativamente en la fiabilidad inicial de las modificaciones programadas. Considero reprochable la actitud de las Administraciones públicas que, pudiendo adaptar sus sistemas, en lugar de afrontar las dificultades que puedan acaecer, opten por no admitir certificados europeos no nacionales, incumpliendo lo dispuesto en el reglamento. En este punto es adecuado traer a colación el considerando 23, conforme al cual "*en la medida en que el presente Reglamento cree la obligación de reconocer un servicio de confianza, solo podrá no reconocerse tal servicio de confianza cuando el destinatario no pueda leerlo o verificarlo por*

[328] GOBIERNO DE ESPAÑA. PLATAFORMA @FIRMA (2016), cambios asociados al reglamento eIDAS, 5.

motivos técnicos sobre los que el destinatario no tenga un control inmediato. No obstante, esta obligación no debe exigir a su vez a un organismo público la obtención del equipo y los programas informáticos necesarios para la legibilidad técnica de todos los servicios de confianza existentes".

Dentro de la estrategia Europa 2020 destaca el papel de la **contratación pública** como uno de los instrumentos pensados para poder alcanzar un crecimiento inteligente, sostenible e integrador[329], mejorando el entorno empresarial, facilitando la innovación y fomentando un uso más generalizado de una contratación ecológica que favorezca la reducción de las emisiones de carbono y el aprovechamiento más eficaz de los recursos, todo ello en conjunción con un uso también más eficaz de los fondos públicos[330]. Se pone así de manifiesto que la contratación pública no es una política abstraída o ajena de las demás políticas públicas, sino que puede ser un medio relevante para cumplir objetivos ambientales y sociales. Fieles a ese enfoque, los principios de la contratación incluyen la garantía del control del cumplimiento de las obligaciones ambientales, sociales y laborales durante la fase de ejecución[331] e incluso antes, en la propia selección del contratista, pues, desde esa perspectiva instrumental de la contratación pública, resulta aconsejable que se exija y valore el cumplimiento de la legislación dela Unión de medio ambiente y de política social[332].

En la implantación de la eAdministración, que tiene carácter fragmentario y sectorial, la contratación pública ha sido uno de los ámbitos en los que la legislación europea

[329] *Vid*. COMISIÓN EUROPEA (2010), crecimiento inteligente.
[330] MORENO MOLINA, J.A. (2015), nuevas directivas, 233-234.
[331] MARTÍNEZ GARCÍA, J./ ELEZ GÓMEZ, A. I. (2015), nuevas directivas, 157.
[332] GIMENO FELIÚ, J.M. (2016), novedades del anteproyecto, 7.

había intentado con anterioridad la modernización a través de las nuevas tecnologías, con las directivas 2004/17/CE y 2004/18/CE[333] y la propuesta, en diciembre de ese mismo año, de un plan de acción para la aplicación del marco jurídico de la contratación pública electrónica[334], fechas en las que la utilización de procedimientos electrónicos tenía carácter facultativo[335]. Es en 2011 cuando deviene obligatorio, al proponer la Comisión un nuevo modelo con tres propuestas, dos de ellas en sustitución de las directivas de 2004 precitadas. Aprobadas por el Parlamento europeo el 15 de enero de 2014[336] y publicadas en el DOUE de 28 de marzo de 2014, su transposición, en general, habría de ser anterior al 18 de abril de 2016. El uso obligatorio de medios electrónicos en la contratación dispone de un plazo significativamente mayor, que finalizará el 18 de octubre de 2018, salvo para centrales de compra, donde deberán estar operativos el 18 de abril de 2017[337]. Esas directivas de cuarta generación son las denominadas "directiva de concesiones" 2014/23/UE, "directiva de contratos" 2014/24/UE y "directiva de sectores especiales" 2014/25/UE, todas ellas de 26 de febrero de 2014. La superación del plazo de transposición sin que se haya producido no solo puede desencadenar la responsabilidad por incumplimiento con posibles consecuencias patrimoniales, sino que implicará que distintos preceptos puedan tener efecto directo y desplazar a nuestra normativa nacional.[338]

Aunque se establece la obligatoriedad de la contratación pública electrónica de forma gradual, en algunos casos hasta avanzado 2018, podemos intuir cierto desánimo en las

[333] ORDÓÑEZ SOLÍS, D. (2013), programación, legislación y financiación, 29.
[334] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2004), *aplicación del marco jurídico*.
[335] ORDÓÑEZ SOLÍS, D. (2013), programación, legislación y financiación, 29-30.
[336] BERNAL BLAY, M. Á. (2014), Entidades locales.
[337] MARTÍNEZ GARCÍA, J./ ELEZ GÓMEZ, A. I. (2015), nuevas directivas, 147.
[338] TRIBUNALES ADMINISTRATIVOS DE CONTRATACIÓN PÚBLICA (1de marzo de 2016), los efectos jurídicos de las directivas, 3-4.

opiniones vertidas en el Observatorio de Contratación Pública. Hace poco más de un año todavía leíamos afirmaciones como "*En España, la contratación pública electrónica no avanza*", echando de menos la existencia de una ley de contratación pública electrónica que desarrollara sus enormes potencialidades, mientras se considera a las directivas "*atrapadas en la maraña de ordenamientos jurídicos diversos*", debiendo abordar los problemas de interoperabilidad de los sistemas informáticos, al construirse la Administración electrónica de forma diferente en cada uno de los países miembros[339].

Al anterior conjunto de directivas ha de añadirse otra destacable en el campo de la eAdministración, la directiva 2014/55/UE relativa a la **facturación electrónica** en la contratación pública[340].

El 6 de mayo de 2015 la Comisión adoptó una **estrategia para completar el mercado único digital**, que comprende una serie de acciones a finalizar antes de que agotar el año 2016. Entre ellas, se incluyen la proposición de normas que faciliten el comercio electrónico transfronterizo, la investigación de la competencia antimonopolio en dicho sector, un análisis exhaustivo de las plataformas *on line*, el refuerzo de la confianza y la seguridad en los servicios digitales en relación con el tratamiento de datos personales, la propuesta de una asociación con la industria de ciberseguridad en el área de las tecnologías y soluciones de seguridad de la red en línea, la promoción de la libre circulación de datos en la Unión, la puesta en marcha de una iniciativa europea de computación en nube, la promoción de prioridades de normas e

[339] BLANCO LÓPEZ, F. (2015), contratación pública electrónica.
[340] MARTÍNEZ GARCÍA, J./ ELEZ GÓMEZ, A. I. (2015), nuevas directivas, 147.

interoperabilidad en ámbitos fundamentales para el mercado único digital[341] y un nuevo plan de Administración electrónica[342].

Con fecha 19 de abril de 2016, a modo de instrumento para unificar esfuerzos, la Comisión publicó su **Plan de Acción sobre Administración Electrónica de la UE 2016-2020**[343], con el objetivo declarado de eliminar los obstáculos digitales que se oponen al mercado único digital y evitar la fragmentación que se puede generar en el contexto de la modernización de las Administraciones públicas. Pretende haber logrado en 2020 prestar unos servicios públicos digitales sin fronteras. Consciente de las diferencias entre las estrategias previas adoptadas para implantar la eAdministración en los distintos Estados miembros, establece una serie de principios que cualquier iniciativa posterior debería respetar, desde un enfoque dinámico y flexible, como viene a ser necesario en un entorno en continuo cambio. Esos principios fundamentales se enuncian como digital por defecto, introducción de la información solo una vez, inclusión y accesibilidad, apertura y transparencia, escala transfronteriza por defecto, interoperabilidad por defecto y, por último, fiabilidad y seguridad integrados en la fase de diseño. Se sigue trabajando en facilitar la plena contratación pública en línea y las firmas electrónicas interoperables. La Comisión señala específicamente que es preciso un mayor esfuerzo por parte de las Administraciones para acelerar el uso de la identificación electrónica y de los servicios de confianza para las transacciones electrónicas en el mercado interior.

---

[341] *Vid*. COMISIÓN EUROPEA (2015), mercado único digital.
[342] Recuperado de http://europa.eu/rapid/press-release_IP-15-4919_es.htm (3 de abril de 2016). *Vid*. texto de la comunicación, en http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
[343] COMISIÓN EUROPEA (2015), *transformación digital.*

Un paso firme en ese refuerzo de la confianza y la seguridad en relación con el tratamiento de datos personales viene dado por el **reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (reglamento general de protección de datos, RGPD). Aplicable a partir del 25 de mayo de 2018, viene a introducir un nuevo modelo de protección de datos para Europa, orientado al uso responsable de la información desde la idea de la responsabilidad proactiva[344].

La utilización de la figura del reglamento, directamente aplicable y obligatorio en todos sus términos, garantiza la uniformidad en el desarrollo, interpretación y cumplimiento en el territorio comunitario[345]. Será necesario revisar el actual ordenamiento jurídico vigente en los diferentes países miembros localizando las adaptaciones que sea necesario realizar, habida cuenta de la obligación de los Estados miembros de eliminar aquellas situaciones de incertidumbre derivadas de la existencia de normas en el derecho interno incompatibles con el europeo, lo que es fuente de ambigüedad e inseguridad jurídica y constituye un incumplimiento de la obligación general de colaboración. "*Esta obligación de depurar el ordenamiento adquiere especial relevancia cuando se trata de normas comunitarias que gozan de aplicación directa y cuya mera entrada en vigor determina la incompatibilidad de las disposiciones internas que las contradigan*"[346]. Con ese objetivo depurativo en mente, pensando en la revisión a realizar *infra* de las disposiciones normativas de nuestro Derecho interno aplicables en la materia, debemos

[344] PIÑAR MAÑAS, J.L. (2016), nuevo modelo europeo de protección de datos, 14.
[345] DAVARA RODRÍGUEZ, M.Á. (2016), comentario de urgencia.
[346] CONSEJO DE ESTADO (2010), cumplimiento, 23-24.

detenernos a estudiar la regulación del consentimiento[347] llevada a cabo por el RGPD, que se inicia en su considerando 32, cuando lo describe como un acto afirmativo claro, libre, específico, informado e inequívoco, y específicamente concluye que "*el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento"*. Continúa el considerando 42 recordando que el responsable del tratamiento ha de ser capaz de demostrar que el interesado ha dado su consentimiento, consciente e informado, matizando que "*el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno*", lo que se recoge en las condiciones del consentimiento de su artículo 7.

En su considerando 78 recuerda la exigencia de adoptar las medidas técnicas y organizativas apropiadas para garantizar lo dispuesto en el propio RGPD, en particular los principios de protección de datos desde el diseño y por defecto, sugiriendo, entre ellas, la reducción al máximo del tratamiento de datos personales y la pseudonimización en un momento tan temprano como sea posible. El artículo 25 afronta esa protección de datos desde el diseño y por defecto y, en su punto segundo, dispone que tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas, algo que, como veremos, parecen incumplir las Administraciones públicas de nuestro país.

Continúa el considerando 78 afirmando la necesidad de alentar a los implicados en el desarrollo, diseño, selección y uso de aplicaciones a que tengan en cuenta el derecho a la

[347] *Vid*. ADSUARA VARELA, B. (2016), el consentimiento.

protección de datos, pero va aún más lejos e indica que también han de asegurarse "*de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones*", todo ello con la debida atención al estado de la técnica, añadiendo, por si hubiera quedado alguna duda, que "*los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos*".

El 19 de julio de 2016 se publica en el DOUE la **directiva (UE) 2016/1148** del Parlamento europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, a fin de mejorar el funcionamiento del mercado interior. A pesar de ser conocida como "directiva sobre ciberseguridad", solo afecta tangencialmente al *software* de las Administraciones públicas, pues se dirige a los operadores de servicios esenciales y los proveedores de servicios digitales. Como señala en su considerando 45, es de aplicación únicamente a las Administraciones públicas que hayan sido identificadas como operadores de servicios esenciales.

3.2. SU ASENTAMIENTO EN ESPAÑA

Condensando la actividad programática y legislativa europea en la materia de los últimos 35 años en una sola frase, podemos sintetizarla como la búsqueda insistente de un nuevo concepto de Administración caracterizada por ser electrónica, *on line*, interoperable, amigable, segura, respetuosa con los derechos fundamentales e implementada por *software* de fuentes abiertas. Descubrir cómo ha enraizado en nuestro país es lo que centrará las siguientes páginas.

En el año 2000, en paralelo con las iniciativas europeas, se desarrolló a nivel nacional la Iniciativa Estratégica para el Desarrollo de la Sociedad de la Información Info XXI,

concretada en el Plan de Acción 2001-2003 "**Info XXI: la Sociedad de la Información para todos**", excesivamente complejo para su gestión y con carencias en cuanto a la coordinación entre los diferentes departamentos y organismos. Buscando un marco normativo favorable a la consecución de los objetivos marcados -una de cuyas grandes líneas es la potenciación de la Administración electrónica a nivel estatal, autonómico y local- se llevan a cabo los trabajos de elaboración de la normativa sobre comercio electrónico, firma electrónica o el plan de dominios de Internet para España[348].

Desde su finalización se sucedieron una serie de iniciativas hasta llegar al programa **España.es 2004-2005**[349], cuyos objetivos fundamentales se orientaron a mejorar la accesibilidad, con una oferta de puntos de acceso público y una formación y promoción adecuadas de las ventajas de la sociedad de la información, al incremento en la productividad y en el crecimiento económico de las PYMES a través de su conexión a Internet, y a un refuerzo de la oferta de contenidos y servicios que favorezca la demanda[350]. Dentro de este programa se enmarca el "plan de choque de la eAdministración", con diecinueve medidas entre las que se incluyen quince grandes servicios electrónicos de alto impacto en la calidad de vida de los ciudadanos[351].

[348] TOMÉ MUGURUZA, B. (2001), INFO XXI, 19-20.
[349] Recuperado de http://www.elmundo.es/navegante/2003/07/11/esociedad/1057923433.html (4 de enero de 2017).
[350] Anexo IX del Plan de Administración electrónica del Gobierno de Aragón, que lleva por título "*Papel de las Tecnologías de la Información y las Comunicaciones en las Administraciones Públicas*", 203.
[351] *Ibíd*., 210.

España, alineada con los objetivos de la Unión Europea con horizonte en la primera década de nuestro siglo, creó el Programa Ingenio 2010[352], que incluía tres planes fundamentales[353]:

- Plan Cenit con el objetivo de aumentar la cooperación pública y privada en I+D.
- Plan Consolider, persiguiendo la excelencia investigadora.
- Plan Avanz@, programa que pretendía alcanzar la media europea en los indicadores de la sociedad de la información, uno de cuyos objetivos fue extender la Administración electrónica poniendo en marcha el DNIe y el registro telemático.

Pensando en la modernización tecnológica para el periodo 2004-2007, el MAP creó el **Plan Conecta**[354], que gira entorno a la Administración electrónica, el rediseño de procesos, la atención multicanal a los ciudadanos, la formación de los empleados públicos y la coordinación y cooperación entre Administraciones. Está integrado por cinco grandes proyectos: Certifica, eDNI, Ciudadano.es, Simplifica y Map en Red[355].

La incorporación de las nuevas tecnologías en las Administraciones públicas presenta desafíos formativos, por la necesidad de hacer frente a la resistencia al cambio y desconfianza de su personal, junto con otros económicos y técnicos, por la complejidad y elevados costes de los desarrollos de los diferentes servicios. Las restricciones presupuestarias

[352] Recuperado de http://www.ingenio2010.es/ (4 de enero de 2017).
[353] SEVILLA ANTÓN, I./ LÓPEZ TEJERA, L., Plan Avanz@.
[354] *Vid.* "*Plan estratégico de modernización CONECTA. Tu Administración en red*", publicado por el MAP en septiembre de 2005.
[355] Anexo IX del Plan de Administración electrónica del Gobierno de Aragón, que lleva por título *Papel de las Tecnologías de la Información y las Comunicaciones en las Administraciones Públicas*, 211.

son un obstáculo para la ejecución de las obligaciones prescritas en un plazo temporal limitado[356]. La magnitud del trabajo a desarrollar puede ilustrarse con el siguiente ejemplo: en 2009, las aplicaciones de la AEAT estaban formadas por más de 400.000 programas que en total contenían más de 160 millones de líneas de código[357].

El 2 de octubre de 2015 el Gobierno aprobó un nuevo plan para acelerar la transformación digital administrativa. Bajo la denominación de "**Plan de transformación digital de la AGE y sus Organismos públicos**", recoge la estrategia TIC para el periodo de tiempo comprendido entre 2015 y 2020. Incluye entre sus objetivos la adopción de una estrategia corporativa de seguridad y usabilidad de los servicios públicos que aumente la confianza en ellos y fomente su uso[358]. Con el convencimiento de que la seguridad es una premisa clave para evitar la desconfianza en el uso de las nuevas tecnologías, considera indispensable abordar la prevención ante posibles ataques y la reducción máxima de posibles riesgos, sin llegar al extremo de que la búsqueda de la seguridad perfecta haga inutilizables las herramientas técnicas, lo que se resume en la aseveración de que "*es necesario alcanzar el equilibrio entre seguridad y usabilidad de los servicios*"[359]. Toda búsqueda de un equilibrio nos lleva inexorablemente a un terreno pantanoso escondido bajo conceptos jurídicos indeterminados y apreciaciones subjetivas al que será imprescindible enfrentarse de forma casuística e individualizada.

[356] CENATIC (2009), fuentes abiertas, 17.
[357] GONZÁLEZ GARCÍA, I. (2009), experiencia de la AEAT, 115.
[358] DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (2015), transformación digital, 9.
[359] DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (2015), transformación digital, 26.

El plan asocia a ese objetivo estratégico una línea de acción con el tenor de "garantizar la seguridad de los sistemas de información de la AGE y sus organismos públicos" enfocada a la aplicación del ENS, que detallaré en un posterior apartado dedicado a las normas técnicas. Lo que sí procede plantear aquí es la reflexión sobre el motivo que ha llevado al legislador a imponer unas exigencias imposibles de llevar a la práctica sin el aumento simultáneo de los recursos económicos y humanos asignados a la implantación de la ambiciosa Administración electrónica por la que apuesta. Como una hipotética explicación, únicamente me vienen a la mente las palabras del recientemente fallecido Eduardo Galeano, que podrían dar algo de claridad a esta cuestión. Opinaba el escritor y periodista uruguayo que "*La utopía está en el horizonte. Camino dos pasos, ella se aleja dos pasos y el horizonte se corre diez pasos más allá. ¿Entonces para qué sirve la utopía? Para eso, sirve para caminar*".

3.2.1. El marco jurídico de nuestra Administración electrónica

3.2.1.1. Los inicios de la modernización

Durante casi un cuarto de siglo, para muchos toda nuestra carrera funcionarial, nos ha acompañado un texto legal que acaba de vivir sus últimos momentos. La **ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común**, ampliamente modificada por la ley 4/1999, ha contribuido enérgicamente a la modernización de nuestras Administraciones públicas, ya que, como expresa el legislador en su exposición de motivos, "*la ley se abre decididamente a la tecnificación y*

modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas".

Así, en su título IV, "De la actividad de las Administraciones públicas", da cumplimiento al mandato constitucional del artículo 105.b)[360] referente al derecho de acceso de los ciudadanos a los archivos y registros administrativos, desarrollándolo con carácter básico e imponiendo la instalación en soporte informático de los registros generales y su integración informática con los restantes registros administrativos. Sin embargo, la disposición adicional segunda, bajo la rúbrica de "Informatización de registros", subordina la efectividad de la incorporación a soporte informático de los mismos al grado de desarrollo de los medios técnicos de que se disponga[361].

La reforma llevada a cabo por la ley 24/2001, de 27 de diciembre, de medidas fiscales, administrativas y del orden social, introdujo la regulación con carácter básico los registros y las notificaciones telemáticos y la incorporación de la disposición adicional decimoctava, aplicable a la AGE, que dotaba de cobertura legal a ciertas prácticas administrativas que obligaban a los ciudadanos a utilizar medios telemáticos en el ámbito tributario y de la seguridad social, promoviendo también el intercambio telemático de

[360] Recuperado de http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=105&tipo=2 (14 de octubre de 2015).

[361] Debemos traer a colación, como señala MARTÍN REBOLLO en sus "*Leyes administrativas*", edición de 2015, la disposición adicional quinta del real decreto ley 8/2011, de 1 de julio, de medidas de apoyo a los deudores hipotecarios, de control del gasto público y cancelación de deudas con empresas y autónomos contraídas por las Entidades locales, de fomento de la actividad empresarial e impulso de la rehabilitación y de simplificación administrativa, la cual dispone para las Comunidades autónomas y las Entidades integradas en la Administración local en las que los registros no se encuentren plenamente incorporados a soporte informático en los términos del precitado artículo 38.3, la obligación de aprobar y hacer públicos los programas y calendarios de trabajo precisos para ello, atendiendo a las respectivas previsiones presupuestarias, en el plazo de seis meses desde la fecha de su publicación en el BOE, 7 de julio de 2011.

información entre Administraciones públicas, en sustitución de las certificaciones acreditativas que deben presentar los interesados en dichos sectores, siempre que se contara con su consentimiento expreso[362]. Con esta reforma se trata de superar el planteamiento inicial de la LRJPAC, más centrada en asegurar la validez de las actuaciones administrativas realizadas a través de la tecnología desde el punto de vista interno, para intentar dotar de seguridad jurídica a las comunicaciones *ad extra* con los ciudadanos, aprovechando la creciente implantación de Internet en esos años y sentando las bases conceptuales en las que se sustentará la regulación que seis años más tarde introduciría la LAE[363].

La LRJPAC abre la posibilidad de emplear medios de notificación distintos a los tradicionales[364] mediante el uso de las nuevas técnicas de transmisión de información, así como la utilización de medios telemáticos para la formulación de solicitudes por parte de los interesados. Sus artículos 38 (registros), 45 (incorporación de medios técnicos[365]), 46 (validez y eficacia de documentos y copias) y 59 (práctica de la notificación) ofrecen un marco jurídico general de referencia para la incorporación sistemática de las tecnologías de la información y de

[362] VALERO TORRIJOS, J. (2007), la nueva regulación legal, 214-215.
[363] VALERO TORRIJOS, J. (2014), de la digitalización a la innovación tecnológica, 120.
[364] El artículo 68 de la ley 24/2001, entre las modificaciones orientadas a impulsar la Administración electrónica, configuró en el artículo 59 de la LRJPAC un nuevo modelo de notificación mediante la puesta a disposición de la actuación correspondiente de manera que los efectos de la notificación se producen bien por el acceso a su contenido bien por el simple transcurso del lapso de diez días desde la puesta a disposición sin que tenga lugar dicho acceso por parte del destinatario.
[365] El artículo 45 de la LRJPAC es desarrollado por el real decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la AGE, ya derogado. Como indica VALERO TORRIJOS en su artículo titulado "Administración pública, ciudadanos y nuevas tecnologías" y publicado en la *revista jurídica de la Región de Murcia* nº 25 (1998), página 22, al limitar su ámbito de aplicación a la AGE, difícilmente puede considerarse que se trate de legislación básica. Los capítulos correspondientes a las notificaciones telemáticas y a los certificados telemáticos no formaban parte del texto original; fueron añadidos posteriormente por el aún vigente real decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

las comunicaciones a las funciones administrativas. Su artículo 45, considerado por el legislador como "*verdadera piedra angular del proceso de incorporación y validación de dichas técnicas en la producción jurídica de la Administración pública y en sus relaciones con los ciudadanos*", apuesta decidida y abiertamente por el empleo de las nuevas tecnologías, al integrar medios y técnicas automatizadas con el reconocimiento formal de su validez. Aunque algunos autores sitúan aquí el nacimiento de la Administración electrónica en España, debemos retrasar ese alumbramiento hasta 1999, cuando fruto del impulso europeo, se comienza a usar el término eAdministración en su sentido actual[366].

Valero Torrijos destaca la ausencia de obligaciones concretas para las Administraciones públicas, por lo que podría verse como un intento por dar reconocimiento legal expreso a la posibilidad de usar medios electrónicos tanto en la propia actividad administrativa como en sus relaciones con los ciudadanos, una pretensión que estima casi testimonial en cuanto a su exigibilidad. Incluso con respecto a la obligación de aprobar los programas y aplicaciones informáticas, no se establecía expresamente ninguna consecuencia a su incumplimiento[367].

Su artículo 53.1 liga la validez del acto administrativo a su ejercicio por el órgano competente y conforme al procedimiento establecido. Cabe preguntarse cómo afecta a esa validez el hecho de que sea una aplicación informática la que exclusivamente decida, es decir, sea ella la que dicte el acto, lo que se analizará *infra*.

La **ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico** viene a incorporar al ordenamiento jurídico español ciertas directivas

[366] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 65-66.
[367] VALERO TORRIJOS, J. (2014), de la digitalización a la innovación tecnológica, 119.

referentes a esa denominada sociedad de la información, como reacción ante la situación de incertidumbre jurídica que provoca el uso de las nuevas tecnologías. Por ello, se esfuerza en proteger los intereses de los destinatarios de servicios para que puedan gozar de garantías suficientes en la contratación de bienes y servicios por Internet, afirma la validez y eficacia del consentimiento prestado por vía electrónica[368] y la equivalencia entre los documentos en soporte papel y los electrónicos a efectos del cumplimiento del requisito de forma escrita, mientras establece un régimen sancionador que autocalifica como "proporcionado pero eficaz". Su sujeción a la normativa de protección de datos se declara explícitamente en los artículos 1, 12 y 19.

El **real decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos**, con la pretensión de impulsar dichas técnicas en la Administración y mejorar así su eficacia, adicionó al real decreto 263/1996 los capítulos correspondientes a las notificaciones telemáticas, certificados telemáticos y transmisiones de datos, con la finalidad de que el intercambio de información entre órganos de la AGE libere al ciudadano de la carga de tener que aportar dichos datos. Añadió también la regulación de los registros telemáticos al real decreto 772/1999, los cuales "*únicamente podrán recibir y remitir solicitudes, escritos y comunicaciones relativas a los trámites y procedimientos que se especifiquen en su norma de creación, no pudiendo, en ningún caso, realizar funciones de*

[368] No podemos ignorar la ligereza con que se presta el consentimiento a través de Internet. En un solo día, 7.500 personas aceptaron vender su alma a una empresa de videojuegos por no leer las condiciones de compra. Recuperado de http://www.elmundo.es/mundodinero/2010/04/20/economia/1271784338.html (25 de mayo de 2016).

expedición de copias selladas o compulsadas de los documentos que se trasmitan junto con la solicitud, escrito o comunicación".

Su disposición final primera, con la rúbrica "requisitos técnicos de los registros y notificaciones telemáticas y prestación del servicio de dirección electrónica única" es desarrollada por la orden PRE/1551/2003, de 10 de junio, vigente hasta el 13 de abril de 2010.

La promulgación de la **ley 58/2003, de 17 de diciembre, general tributaria**, supuso un gran avance al reconocer la automatización de la actuación administrativa o la obtención de imágenes electrónicas de los documentos con idéntica validez y eficacia que el documento origen. Bajo la rúbrica de "utilización de tecnologías informáticas y telemáticas", su artículo 96 dispone la promoción de las técnicas y medios electrónicos, informáticos y telemáticos, recordando que deberá sujetarse a las limitaciones que la Constitución y las leyes. Reconoce la actuación automatizada, garantizando la identificación de los órganos competentes para la programación y supervisión del sistema de información y de los órganos competentes para resolver los recursos que puedan interponerse. Cabe señalar que, en su apartado 4, aún subsiste el requisito de aprobación previa de los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por la Administración tributaria para el ejercicio de sus potestades.

3.2.1.2. Su despegue con la ley de acceso electrónico

El empuje final para propulsar la nueva eAdministración partió de otro texto legal recién llegado ahora al final de su camino, la **ley 11/2007, de 22 de junio, de acceso electrónico**

de los ciudadanos a los servicios públicos, vigente hasta el pasado 2 de octubre de 2016, ley que desaprovechó la oportunidad de definir normativamente el concepto de Administración electrónica, aunque de su articulado se deduce que adopta la elaborada por la Comisión europea[369]. Aunque no se arriesgara a definirla, el legislador había llegado al convencimiento de que su desarrollo seguía siendo insuficiente, debido en buena medida a que las previsiones de los artículos 38, 45 y 59 de la LRJPAC eran facultativas, por lo que la LAE vino empujando, dispuesta a marcar, en palabras de su exposición de motivos, "*un hito trascendental en la construcción de la Administración pública de la sociedad de la información en España*", dando el paso del "podrán" al "deberán", reconociendo el derecho del ciudadano y la obligación correlativa de la Administración, sin que pueda ocasionarse discriminación para los ciudadanos que decidan no utilizar medios electrónicos.

A modo de buque insignia entre los derechos que constituyen el estatuto jurídico del "administrado electrónicamente", encabeza las medidas a implantar la apuntada en el artículo 6.2.b) referente al **derecho del ciudadano a no aportar datos y documentos** que obren en poder de las Administraciones públicas[370], derecho que refleja el cambio hacia un modelo de Administración electrónica de intercambiabilidad total de datos sin intervención directa de órganos ni personal administrativo en los procesos de comunicación[371].

Esta ley precisa que se requerirá el consentimiento del interesado conforme a lo establecido en la LOPD para poder recabar esa información por medios electrónicos, salvo que

[369] MARTÍN DELGADO, I. (2009), actuación administrativa automatizada, 355.
[370] Sobre el derecho a no presentar datos y documentos que ya obren en poder de las Administraciones Públicas, resulta de interés la lectura de VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 278-282.
[371] COTINO HUESO, L. (2015), Administración electrónica, 17.

una norma legal así lo determine o existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados.

A las transmisiones de datos entre Administraciones públicas dedica, con carácter básico, su artículo 9, en el que, con el objetivo de posibilitar el eficaz ejercicio del derecho reconocido en el apartado 6.2.b), obliga a las Administraciones a facilitar a las demás el acceso a los datos relativos a los interesados que obren en su poder en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con la normativa de protección de datos de carácter personal. En su apartado segundo limita la disponibilidad de los datos estrictamente a los requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos, y recuerda la necesidad de cumplir las condiciones establecidas en su artículo 6.2.b).

A este respecto, debemos recordar que el artículo 21 de la LOPD prohíbe, con salvedades, la comunicación de datos entre Administraciones públicas para competencias o materias diferentes. Tampoco es lícita la verificación, sin consentimiento o habilitación legal, de la autenticidad de los datos incluidos en las solicitudes telemáticas formuladas a las Administraciones públicas, prevista por el artículo 11 del real decreto 1720/2007, de 21 de

diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD, artículo finalmente anulado por el Tribunal Supremo[372].

Para Cotino Hueso, que el consentimiento del interesado parezca la condición *sine qua non* para posibilitar el acceso de información de una Administración a otra es un exceso de garantismo, sugiriendo el libre acceso a los datos de otra Administración cuando sea necesario para el cumplimiento de las funciones, al considerarse un interés público relevante, sobre todo cuando la participación del ciudadano en el procedimiento es voluntaria, entendiéndola como una autorización suficiente[373].

Entre **otras obligaciones** establecidas por esta ley, aunque hayan alcanzado menor resonancia entre la ciudadanía, podemos destacar el deber de poner a disposición de los usuarios información por medios electrónicos sobre el estado de tramitación de los procedimientos, o la necesaria admisión de los certificados electrónicos reconocidos en el ámbito de la LFE.

El legislador ya se plantea en la exposición de motivos la cuestión de la privacidad de los datos facilitados en un expediente que, una vez archivados de forma electrónica, pudieran ser utilizados en otro, o por otra Administración, y recalca que la LOPD ya establece su uso únicamente para el fin para el que han sido recabados, no para otro diferente. Reitera también la necesidad de conservar las garantías constitucionales y legales de los ciudadanos derivadas del artículo 18.4 de nuestra Carta Magna, y afirma la vigencia de los

[372] Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo, publicada en el BOE de 26 de octubre de 2010 (página 90214).
[373] COTINO HUESO, L. (2015), Administración electrónica, 18.

derechos fundamentales "*no solo como límite, sino como vector que orienta esta reforma legislativa* (…)".

Refiriéndose al objeto de la ley, dispone el uso de las TIC por las Administraciones públicas de forma que aseguren **la disponibilidad, el acceso, la integridad, la autenticidad y la confidencialidad**[374]. Entre sus finalidades incluye crear las condiciones de confianza en los medios electrónicos, concretando que pretende hacerlo "*estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales*", señalando en particular la intimidad y la protección de datos de carácter personal, garantizando la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos. Y, una vez más, al referirse a los principios generales, vuelve a insistir en que el uso de las TIC tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico. El primer principio al que hace referencia es "*el respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la LOPD, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar*". Se reconoce también el derecho de los ciudadanos a la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones públicas. Pero, consciente de que los derechos no son ilimitados, en el artículo 27.5 invoca el principio de proporcionalidad cuando establece que "*los*

[374] Sorprende cómo el legislador utiliza estas palabras en distintos textos legales con aparente desconocimiento del significado técnico de las mismas. En la LAE incluye la palabra "acceso" entre las tradicionales dimensiones de la seguridad (aspectos que se analizarán *infra*). En la ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, se olvidan de la "autenticidad". En la ley 39/2015 del procedimiento administrativo común de las Administraciones públicas hablan de "seguridad y confidencialidad", es decir, el todo y una de sus partes. Una lectura detenida del ENS resultaría de utilidad para aclarar su utilización técnicamente más adecuada.

requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal".

Su artículo 42.2, de carácter básico, introduce el esquema nacional de seguridad, ENS, explicando que su objeto es "*establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información*", que se regulará en el Real Decreto 3/2010, de 8 de enero, al que nos referiremos en páginas posteriores con detenimiento.

La **disposición final tercera**, también con carácter básico, consideraba el 31 de diciembre de 2009 como fecha límite para que los ciudadanos pudieran ejercer con plenitud sus derechos por medios electrónicos en cualquier procedimiento y actividad de competencia de la Administración. Sin embargo, la modificación operada por la ley 2/2011, de 4 de marzo, de economía sostenible, adicionó un nuevo apartado 5, a cuyo tenor las Comunidades autónomas y las Entidades locales que no cumplan con el cronograma previsto deberán aprobar y hacer públicos los programas y calendarios de trabajo precisos para ello, atendiendo a las respectivas previsiones presupuestarias, con mención particularizada de las fases en las que los diversos derechos serán exigibles por los ciudadanos. No habiendo establecido el legislador las consecuencias de su no publicación, la modificación ha supuesto una vía de escape amplísimamente transitada. Las palabras, siempre sabias y constructivamente críticas, de Valero

Torrijos, se pronuncian sobre ello transcurridos cinco años desde la entrada en vigor de la ley, al analizar sus efectos en el ámbito de la Administración local[375]. Destaca su efecto dinamizador en la apuesta de las autoridades locales por la implantación de los servicios electrónicos, en parte por el carácter básico de la mayor parte de sus preceptos, por lo que resultaban directamente aplicables, y por su flexibilidad, al permitir la adaptación a las particularidades de cada entidad por medio de ordenanzas y al modular el alcance de los derechos de los ciudadanos en función de las disponibilidades económicas y materiales. Sin embargo, lamenta que la crisis económica hubiera provocado o, al menos, servido de excusa inadmisible para dejar inacabados muchos proyectos. Supeditar la implantación de la eAdministración a la existencia de recursos presupuestarios en las Comunidades autónomas y Entidades locales abre la puerta a la discrecionalidad, pues no impide designar recursos a otros objetivos en detrimento del desarrollo de los servicios electrónicos. En cualquier caso, continúa señalando, las Entidades locales siempre pueden beneficiarse de las aplicaciones utilizadas en las Diputaciones provinciales y Comunidades autónomas correspondientes, sin necesidad de establecer convenios al efecto. Y concluye afirmando que la modificación realizada por la ley 2/2011, continúa siendo ineficaz, habida cuenta de que no establece medida o consecuencia alguna por su incumplimiento.

Cotino Hueso apunta la posibilidad de que la no efectividad de los derechos reconocidos a los ciudadanos en el artículo 6.3 de la LAE por los entes locales o autonómicos vulnere el Derecho comunitario, al tratarse de derechos derivados de la trasposición de la directiva de servicios, añadiendo que la vía para lograr su efectivo cumplimiento pasaría por la

[375] VALERO TORRIJOS, J. (2002), la Administración electrónica en el ámbito local.

reclamación por inactividad ante la Administración conforme al artículo 29.1 de nuestra ley jurisdiccional[376].

La LAE acomete la regulación de instituciones polémicas, como el sello de órgano, reflejo de la **actuación administrativa automatizada**[377] que podría tener incidencia negativa en las garantías jurídicas y que lleva a replantear la teoría general del acto administrativo. El sello de órgano quiebra la tradicional concepción del acto administrativo de Zanobini como declaración de voluntad, de juicio, de conocimiento o de deseo, difícilmente encajables en la informática decisional, lo que obliga a replantear los límites que se han de establecer en la construcción y aprobación de los programas y aplicaciones[378], aspecto este que estudiaremos detenidamente *infra*. Dicha aprobación, prevista en los artículos 5 y 9 del derogado real decreto 263/1996, solo subsiste hoy en el ámbito tributario[379]. En cualquier caso, aunque ayuno de publicidad y transparencia, siempre habrá de existir un acto aprobatorio por parte del organismo competente; cuestión diferente será la capacidad y cualificación del empleado público que deba dictar esa aprobación, aspecto también a tratar detenidamente más adelante.

Acudiendo a la definición que la LAE aporta de actuación administrativa automatizada, se refiere a ella como la "*actuación administrativa producida por un sistema de información adecuadamente*[380] *programado sin necesidad de intervención de una persona física en cada caso singular*". La palabra "adecuadamente" abre camino a la inseguridad jurídica, al

[376] COTINO HUESO, L. (2015), Administración electrónica, 9-10.
[377] La actuación administrativa automatizada no es novedosa, puesto que ya venía contemplada, como comentamos *supra*, en la ley general tributaria.
[378] URIOS APARISI, X./ ALAMILLO DOMINGO, I. (2007), límites a la utilización del sello de órgano, 3-7.
[379] Artículo 96.4 de la ley 58/2003, de 17 de diciembre, general tributaria.
[380] El subrayado es nuestro.

desconocer qué cabe entender en dicho concepto. Recordemos que *supra* hemos tratado el tema de los inevitables errores del *software*.

Afirma Piñar Mañas que *"en realidad puede llegar a ser el programa informático y no la Administración el que condicione la decisión adoptada. O si se prefiere, la voluntad de la Administración se expresa a través del filtro del programa informático utilizado"*[381]. Cuando la tecnología se utiliza para sustituir los juicios intelectivos de los empleados públicos y un programa o una aplicación informática pasan a ser los que adoptan las decisiones, se plantean dos aspectos diferentes que resultan claves para determinar la validez final del acto administrativo, la intensidad de la revisión jurisdiccional y, en consecuencia, el derecho a la tutela efectiva de los jueces y tribunales. Por un lado, en cuanto a los puramente formales, se aborda el tema del conocimiento de que, en un determinado procedimiento, se adopta la decisión final de forma automática por un proceso tecnológico. Por otro, procede plantearse la propia legalidad del programa y la aseveración frente al exterior de que cumple con los requisitos necesarios para producir una correcta aplicación del ordenamiento jurídico, aspecto este no especialmente contemplado por la LAE[382].

Para Palomar Olmeda, el papel del citado requisito formal es crucial y no ha sido suficientemente valorado. Afirma que "*el acto administrativo dictado sin tener en cuenta o sin existir la aprobación o la puesta en conocimiento general de las características de la aplicación entra en una crisis de validez radical que solo puede solventarse con la demostración puntual del cumplimiento de los trámites y del acierto – en términos jurídicos- de la decisión adoptada*".

[381] PIÑAR MAÑAS, J.L. (2011), Administración electrónica, 151.
[382] PALOMAR OLMEDA, A. (2009), actuación jurisdiccional, 80.

Sin entrar a analizar la afirmación sobre la crisis de validez radical, sí parece completamente acertado que esa demostración puntual del acierto de la decisión pone punto final a la controversia, y lo hace con independencia de que se trate de una decisión dictada por un empleado público con bolígrafo, papel y calculadora o por una aplicación automática. Continúa Palomar Olmeda afirmando la inversión de la presunción de legalidad, de forma que la Administración se ve compelida a realizar una actividad probatoria de los extremos indicados, sin la cual está en juego la intensidad de la revisión jurisdiccional y de la propia tutela efectiva de los jueces y tribunales, pero afirma que no ocurre cuando la aplicación es conocida públicamente[383].

Martín Delgado revisa los planteamientos doctrinales surgidos recientemente referidos a las dificultades de encajar la total ausencia de intervención humana que caracteriza a la actuación administrativa automatizada con la construcción dogmática del concepto de acto administrativo y la teoría del órgano[384]. Comienza por rememorar al primero en plantear la cuestión, Valero Torrijos, para quien se produce una quiebra del elemento subjetivo que no encaja con la configuración del concepto de órgano administrativo ni con el rigorismo de las normas en cuanto al ejercicio de la competencia por el mismo. Para Delgado García y Oliver Cuello[385] lo que se produce la quiebra del concepto tradicional de acto administrativo como manifestación de voluntad, conocimiento o juicio del órgano administrativo. Palomar Olmeda planteó la posibilidad de reconducir la responsabilidad final del acto administrativo al órgano

[383] PALOMAR OLMEDA, A. (2009), actuación jurisdiccional, 81.
[384] MARTÍN DELGADO, I. (2009), actuación administrativa automatizada, 356-357.
[385] *Vid*. DELGADO GARCÍA, A.M./ OLIVER CUELLO, R. (Mayo-junio, 2006), regulación de la informática decisional.

encargado de aprobar el sistema de información aunque, finalmente, se decantó por imputar la actuación al órgano que tiene encomendado el ejercicio de la competencia. Como excesivamente rigorista cita a Parada Vázquez, quien se muestra inflexible al afirmar que los actos administrativos son manifestaciones de voluntad y las máquinas no la tienen[386]. Para el propio Martín Delgado la actuación administrativa automatizada resulta perfectamente compatible con la teoría del órgano y con el concepto actual de acto administrativo.

El artículo 33 de esta ley deja claro que la gestión electrónica de la actividad administrativa respeta la titularidad y el ejercicio de la competencia, mientras que el 38 requiere que en la resolución de un procedimiento utilizando medios electrónicos se garantice la identidad del órgano competente mediante firma electrónica. Por lo demás, "*la máquina, la herramienta informática, no deja de ser un medio material, como tantos otros, al servicio del titular del órgano*"[387]. Nadie se plantea ninguna de las anteriores cuestiones por el uso de calculadoras por parte de los empleados públicos sino, al contrario, producen más desconfianza las operaciones matemáticas realizadas con lápiz y papel, por ser más susceptibles de contener errores. Los sentimientos de desconfianza o rechazo que, a diferencia de una calculadora, sí produce un ordenador, pueden estar relacionados con el hecho de "no saber lo que hace"[388], pero es preciso

[386] MARTÍN DELGADO, I. (2009), actuación administrativa automatizada, 364.
[387] MARTÍN DELGADO, I. (2009), actuación administrativa automatizada, 361.
[388] En mi opinión personal, salvo en los casos de aplicaciones extremadamente simples y de muy pequeña envergadura, los ciudadanos seguirán sin saber lo que hace el ordenador aunque se les muestre la codificación de los aplicativos. Es más, muchas veces, pasado un tiempo, el propio informático que programó ese código no sabe qué es lo que está haciendo el programa, algo que ocurre especialmente en las aplicaciones monolíticas más antiguas y poco estructuradas. Por ello, el esfuerzo requerido para modificar un programa que ya está en producción, muchas veces desarrollado por personas ajenas, es altamente costoso y considerablemente arriesgado, disparándose, como indica *supra* la figura 1, la tasa de errores tras cada modificación del *software*. Por ello, funcionalmente, considero que la opción óptima pasa por encomendar los desarrollos informáticos a empleados públicos que conservarán con

recordar que la actuación administrativa automatizada es, por definición, la producida por un sistema "adecuadamente programado", por lo que no se produce quiebra alguna del elemento subjetivo ni del concepto tradicional de acto administrativo. A estos efectos, un sistema informático adecuadamente programado no se diferencia de una calculadora o de una máquina de escribir, no desvirtúa la voluntad del órgano competente; el acto administrativo producido será nulo o anulable en los mismos casos contemplados por los artículos 62 o 63 de la LRJPAC, con independencia de si se ha producido o no a través de una actuación administrativa automatizada, procediendo la abstención y recusación cuando sea el caso.

Se abre la puerta a la posible nulidad de los actos administrativos producidos mediante su utilización de un *software* no programado adecuadamente, conforme al supuesto del artículo 62.1.e). No solo es preciso analizar cuándo puede considerarse que la programación es o no adecuada, sino que será necesario evaluar si esa inadecuación equivale a prescindir total y absolutamente del procedimiento legalmente establecido.

El diccionario de la RAE define el infinitivo "adecuar" como "adaptar algo a las necesidades o condiciones de una persona o de una cosa" y el adjetivo "adecuado" como "apropiado para alguien o algo", mientras que "apropiado" es definido como "ajustado y conforme a las condiciones o a las necesidades de alguien o de algo". La búsqueda de criterios para determinar la posible inadecuación de los programas informáticos de las Administraciones públicas será más productiva si se realiza tras haber examinado las diferentes tareas implicadas en la obtención del *software*.

---

mayor probabilidad el conocimiento detallado de la programación y podrán reaccionar, en caso necesario, con rapidez y mayor seguridad.

Conforme al artículo 38.2, podrán adoptarse y notificarse resoluciones de forma automatizada en aquellos procedimientos en los que así esté previsto, de donde deriva que la norma reguladora de cada procedimiento deberá incluir una habilitación específica. Comparten la opinión de que es necesaria una habilitación normativa previa Martín Delgado, Linares Gil y Palomar Olmeda[389].

Su artículo 39 prevé, en caso de actuación automatizada, la obligación de establecer previamente el órgano u órganos competentes para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente, así como el órgano que debe ser considerado responsable a efectos de impugnación. Este artículo nos lleva a plantear algunos importantes interrogantes… Quien defina las especificaciones, quien programe el *software* y quien mantenga las aplicaciones, quien audite el sistema o el código fuente, ¿ha de ser necesariamente un órgano administrativo? ¿Puede externalizarse? Volvemos a remitirnos aquí al desarrollo de las respuestas afrontado *infra*. Y, habida cuenta de que este artículo no es básico, ¿cómo afecta a las Comunidades autónomas?

Como concluyen Urios y Alamillo, la situación nos lleva "(…) *al necesario establecimiento de controles jurídicos sobre la programación de los sistemas de tramitación que hagan uso del sello, para evitar posibles desviaciones informáticas de poder*"[390]. En mi opinión, esa afirmación debe extenderse a todos los programas informáticos de las Administraciones públicas que, de manera directa o indirecta, incidan en la esfera jurídica de los ciudadanos.

[389] MARTÍN DELGADO, I. (2009), actuación administrativa automatizada, 373.
[390] URIOS APARISI, X./ ALAMILLO DOMINGO, I. (2007), límites a la utilización del sello de órgano, 11.

La automatización de las actuaciones administrativas viene siendo una realidad desde hace décadas, careciendo de una disciplina legal específica hasta la llegada de la LAE, donde el legislador no entra a establecer requisitos, garantías o límites aunque, como señala Valero Torrijos[391], no se puede ignorar la exigencia de respeto del ejercicio competencial recogida en el artículo 33. A diferencia del derogado real decreto 263/1996, la LAE no contiene previsión alguna sobre la obligatoriedad de dar publicidad a los programas utilizados. Añade el mismo autor[392] una valoración negativa por lo que considera una clara regresión para las garantías del ciudadano y de la propia actividad administrativa, al derogar la obligación de aprobar previamente a su uso los programas y aplicaciones informáticas, así como difundir públicamente sus características[393], sustituyendo la garantía de transparencia y responsabilidad que proporcionaba la aprobación expresa por acto administrativo o por norma jurídica y su difusión por una mera referencia a la necesidad de conocer previamente el órgano competente a efectos técnicos[394]. Si bien es cierto que, conforme a los principios de transparencia y de legalidad, es generalizada la opinión doctrinal de que ha supuesto una pérdida de garantías, debo defender la primacía del principio de seguridad. "*Es necesario tener en cuenta que, por la propia naturaliza de la materia, la exposición detallada de los proyectos, iniciativas, herramientas, trabajos realizados, etc. debe someterse a la lógica prudencia y, en consecuencia, evitar ofrecer*

[391] VALERO TORRIJOS, J. (2007), la nueva regulación legal, 234-235.
[392] VALERO TORRIJOS, J. (2009), las garantías jurídicas, 26-27.
[393] En mi opinión, la publicación de las características de los programas y aplicaciones sí resulta adecuada, en cualquier caso. Lo que considero cuestionable es la publicación del código, habida cuenta de que puede proporcionar información que facilite los ciberataques, especialmente en programas antiguos desarrollados con unos estándares de calidad poco exigentes.
[394] La obligación de aprobación previa aún subsiste en el ámbito tributario, a tenor del artículo 96.4 de la ley general tributaria.

información que pudiera en sí mismo constituir un riesgo para la organización"[395]. La exposición pública del código fuente de las aplicaciones informáticas difícilmente va a proporcionar información de utilidad a la ciudadanía, en general carente de conocimientos necesarios para comprenderla[396]; sin embargo, existe el riesgo de que pueda resultar preocupantemente provechosa para los ciberatacantes. Son muchas las aplicaciones informáticas en cuyo código está escrita directamente la contraseña de acceso, una práctica totalmente inadecuada pero relativamente frecuente, y no siempre fácilmente evitable. Una aplicación informática es solo una herramienta, nada más. Los criterios que ha de aplicar para resolver son los mismos que se aplicarían manualmente; el resultado ha de ser el mismo que se obtendría resolviendo manualmente y, si no es así, debe recurrirse el acto como se recurriría si se hubiera resuelto manualmente.

La publicidad del código fuente, no imprescindible para lograr la seguridad jurídica, sí puede ser perjudicial para la seguridad informática. Sin embargo, su publicación resulta decisiva para posibilitar la libre reutilización del *software* en otras Administraciones

[395] TORRES CARBONELL, J.J. (2009), el papel de la seguridad, 233. El autor realizó esta afirmación, que comparto plenamente, siendo Subdirector general de Tecnologías de la Información y de las Comunicaciones de la Dirección general de Servicios y Coordinación Territorial del Ministerio de economía y hacienda.

[396] Tras haber ejercido durante más de 20 años como desarrolladora de *software* para diferentes Administraciones públicas, considero que no supondría para mí ninguna dificultad técnica ocultar en el código fuente las instrucciones necesarias para favorecerme personalmente. Y, en función del tamaño de la aplicación informática, sería casi imposible de detectar incluso si se realizara una auditoría. Téngase en cuenta que hay aplicaciones informáticas que incluyen varios miles de módulos, muchos de los cuales pueden contener a su vez miles de líneas de código, que no siempre se ejecutan secuencialmente, sino que van saltando de uno a otro módulo en función de condiciones que se determinan dinámicamente. Y, por supuesto, mi NIF no aparecería en ninguna de ellas, pues se construiría también dinámicamente cuando se diesen determinadas condiciones que solo yo conocería. Partiendo de esta premisa, ¿tiene capacidad el órgano competente para aprobar la aplicación desarrollada cuando, muchas veces, ni los propios informáticos somos capaces de saber qué hace un programa?

públicas[397]. El ENI obliga a ello, tanto para las aplicaciones ya finalizadas como para las que sigan en desarrollo, buscando el beneficio de una mejor eficiencia. Los organismos que tengan intención de cumplir su obligación, deberán asegurarse de que el código no contenga información cuya publicación ponga en riesgo sus sistemas, como credenciales del tipo usuario y contraseña, algo que, para aplicaciones antiguas desarrolladas en una época de menor rigor, podría requerir cierto esfuerzo. Indirectamente, por tanto, la publicación del código podría desembocar en una mejora en la calidad del *software*.

La LAE introduce en su tenor el principio de **neutralidad tecnológica**[398], garantizando la independencia del ciudadano en cuanto a su elección entre las diferentes alternativas tecnológicas disponibles. En palabras de Boix Palop, "*se trata, en sentido estricto, de garantizar que los medios tecnológicos empleados por el ciudadano o que éste tenga a su disposición tengan un efecto neutro en la tramitación del procedimiento*"[399]. Sin embargo, su loable intención cocha frontalmente con la realidad tecnológica y con la limitación de los recursos públicos, por lo que difícilmente se materializa en el *software* implementado por nuestras Administraciones. En los entornos tecnológicos escogidos por los usuarios converge una abundante variedad de productos que da lugar a miles de combinaciones posibles que obligan a las Administraciones públicas a "*realizar un esfuerzo gigante para dar cabida a esa*

[397] Esta publicación no debe abrirse necesariamente a la ciudadanía. Es posible restringir esa información a personal de las Administraciones públicas debidamente identificado.
[398] El mantenimiento de la neutralidad tecnológica es una exigencia legal ineludible que, en determinados aspectos relacionados con la programación del *software*, resulta inviable conseguir. Por ello, debo puntualizar que estas dificultades que comento son referidas la neutralidad del *software* de las Administraciones públicas, algo totalmente independiente de la neutralidad de Internet. Con respecto a este aspecto, *vid*. FUERTES LÓPEZ, M (2014), neutralidad en la red.
[399] BOIX PALOP, A. (2010), previsiones en materia de neutralidad, 311. *Vid*. también el trabajo del mismo autor (2007), la neutralidad tecnológica.

heterogeneidad"[400], convirtiendo en inabordable cualquier proyecto de Administración electrónica que pretenda cumplir estrictamente con el principio de neutralidad tecnológica, máxime cuando los múltiples organismos en distintos Ministerios, Comunidades autónomas, Diputaciones provinciales, Entidades locales, etc. trabajan de forma independiente en el desarrollo de aplicaciones informáticas destinadas a dar respuesta a las mismas o muy similares necesidades públicas. Parece imprescindible una actuación coordinada de todas ellas, así como el establecimiento de modelos colaborativos tipo forja que favorezcan el uso de *software* libre[401]. Si un importante obstáculo para alcanzar la neutralidad tecnológica es la falta de recursos, humanos principalmente, y la opción de ampliarlos no es presupuestariamente viable, habremos de optimizarlos, repartiendo los trabajos a ejecutar entre los efectivos disponibles, en lugar de dedicar a diferentes equipos (estatales, autonómicos o incluso locales) a resolver la misma tarea.

Siguiendo a Valero Torrijos, Cotino Hueso señala los potenciales problemas de la presentación de escritos y comunicaciones sometidos a plazo a través de registros electrónicos, lamentando que, si bien se ha afirmado el derecho a la ampliación del plazo de presentación ante caídas o disfunciones del servidor en periodos importantes, este derecho no ha sido regulado, añadiendo entre los aspectos problemáticos la indefinición del artículo 28.3 de la LAE al respecto de las notificaciones electrónicas, donde no aclara la noción de "imposibilidad técnica o material del acceso" que evita que pueda tenerse por rechazada[402]. En general, el autor propugna el reconocimiento de garantías específicas frente a la actuación administrativa automatizada o, en general, soluciones ante situaciones de error de las aplicaciones, configurando una presunción

[400] IDOATE GIL, A./ GARCÍA-MERÁS CAPOTE, T. (2013), práctica de la neutralidad, 1.
[401] IDOATE GIL, A./ GARCÍA-MERÁS CAPOTE, T. (2013), práctica de la neutralidad, 12-13.
[402] COTINO HUESO, L. (2015), Administración electrónica, 12.

favorable para el ciudadano que interactúa electrónicamente, un principio *in dubio por actionem* electrónico[403].

El **real decreto 1671/2009**, de 6 de noviembre, viene a desarrollar parcialmente la LAE. En su introducción, nos recuerda cuáles son los principios considerados estratégicos por el legislador, a saber, la más plena realización de los derechos reconocidos en la LAE con garantía de que no resultan afectados otros bienes constitucionalmente protegidos, como pueden ser la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros, y el establecimiento de un marco flexible en la implantación de los medios de comunicación, cuidando los niveles de seguridad y protección de derechos e intereses previstos en nuestro ordenamiento jurídico, todo ello con el objetivo de evolucionar sin impedir la pervivencia de técnicas preexistentes, facilitando la implantación y adaptación de las actuales y sin dificultar la incorporación en el futuro de nuevas soluciones y servicios.

Dispone su artículo 20 la posibilidad de que la AGE y sus organismos públicos vinculados o dependientes utilicen sistemas de CSV de documentos en el desarrollo de actuaciones automatizadas, vinculando al órgano u organismo y, en su caso, a la persona firmante, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente. También se adentra en el mundo de los certificados electrónicos destinados al personal a su servicio en el artículo 22, limitando su uso al desempeño de las tareas propias de su puesto de trabajo o para relacionarse con las Administraciones públicas cuando estas lo admitan. Si bien establece un contenido mínimo que

[403] COTINO HUESO, L. (2008), derechos del ciudadano, 133.

incluye nombre y apellidos del titular, así como su DNI o número de identificación de extranjero, su apartado 4 hace referencia a una novedosa excepción, el "certificado electrónico de empleado público con pseudónimo"[404], apropiado para acciones por medios electrónicos que afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización. Si bien no está pensado para ocultar la identidad de empleadas públicas víctimas de violencia de género que se hayan acogido a la posibilidad que les brinda el artículo 82 del TREBEP, entendemos perfectamente subsumible entre las causas que justifican su utilización.

El uso de los certificados públicos con pseudónimo también está motivando aún adaptaciones en las aplicaciones informáticas de las Administraciones públicas (recordemos que el real decreto 668/2015, de 17 de julio, otorga un plazo de doce meses para realizar las adaptaciones técnicas necesarias).

Cabe preguntarse si cualquier funcionario podría negarse, basándose en la normativa reguladora de protección de datos, a utilizar un certificado electrónico de empleado público en el que aparezca su nombre y su número de DNI. La AEPD resolvió dicha cuestión en el expediente TD/01638/2013, dictando la resolución número R/02699/2013, de la cual reproducimos aquí la conclusión: "*En consecuencia, el certificado de firma electrónica de empleado público sobre el que solicita la cancelación es una herramienta puesta a su disposición por el organismo para el que presta servicios para su identificación como*

[404] El artículo 22.4, vigente desde el 19 de julio de 2015, es de nueva introducción, en virtud del apartado tres del artículo único del real decreto 668/2015, de 17 de julio, por el que se modifica el real decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

trabajador de dicho organismo y de la Administración general del Estado, siendo, por ello, una condición obligatoria en su relación laboral". La nueva ley 39/2015 viene a despejar cualquier duda estableciéndolo específicamente en su artículo 14.2.e).

La **ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio**, conocida como "ley paraguas", junto con la **ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la ley 17/2009,** denominada "ley omnibus", incorporan a nuestro ordenamiento jurídico la directiva de servicios, adecuando nuestra normativa a los principios de la norma europea, de forma que "*trasladan el profundo cambio que comienza a producirse en el modo de entender la relación de la Administración con los ciudadanos y las empresas, impulsando la modernización de las AA.PP. para responder a las necesidades de empresas y consumidores*".[405]

El artículo 42 de la LAE hace referencia a dos instrumentos técnicos imprescindibles para el logro de los objetivos marcados por la normativa examinada, lo que ha llevado a publicar dos reales decretos en la misma fecha, 8 de enero de 2010. El primero de ellos, el **real decreto 3/2010, regula el esquema nacional de seguridad** en el ámbito de la Administración electrónica, ENS. El segundo instrumento es el **real decreto 4/2010, por el que se regula el esquema nacional de interoperabilidad** en el ámbito de la Administración electrónica, ENI. Debido a su carácter técnico, relegaremos su estudio al capítulo correspondiente.

[405] MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA (2011), prácticas de referencia, 6.

3.2.1.3. El acceso a la información pública

El preámbulo de la **ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno** remarca el potencial de las nuevas tecnologías para posibilitar el acceso del ciudadano a la información pública disponible, entendiendo como tal los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones. La regulación y garantía de ese derecho de acceso, previsto ya en leyes preexistentes, es uno de los objetivos de este texto legal, el cual viene a solventar deficiencias reiteradamente manifiestas, como la restricción a documentos contenidos en procedimientos administrativos ya terminados o las limitaciones en su práctica. El legislador ha configurado el derecho de acceso a la información como un principio de actuación de las Administraciones, no como un derecho fundamental en sí mismo, postura defendida por Piñar Mañas[406].

La ley configura un derecho de acceso limitado solamente cuando exista una justificación debida a la propia naturaleza de la información o por colisión con otros intereses protegidos, debiendo en tales casos realizar una ponderación entre el interés salvaguardado con la limitación y el interés público en la divulgación. En particular, podría plantearse con frecuencia un conflicto con la protección de datos personales, problema aclarado por la ley

[406] El autor, reconociendo que el legislador ha optado por la interpretación contraria, nos aporta poderosos argumentos que apoyan la defensa de su apreciación del derecho al acceso a la información como derecho fundamental en PIÑAR MAÑAS (2014), transparencia, 45-51.

estableciendo los mecanismos de equilibrio necesarios[407]. Habida cuenta de que ni el derecho al acceso a la información ni el de protección de datos son ilimitados, se ha de alcanzar ese equilibrio entre ambos[408], valorando las circunstancias de cada caso concreto, ponderando los intereses de las partes implicadas y aplicando el principio de proporcionalidad[409], huyendo de generalizaciones. En caso de que la limitación no afecte a la totalidad de la información, prevé la concesión de un acceso parcial previa omisión de la información afectada, salvo que de ello resulte una información distorsionada o que carezca de sentido, en cuyo caso se indicaría qué parte ha sido omitida.

Todo ello no será necesario si previamente se efectúa la disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

El informe 0178/2014 del gabinete jurídico de la AEPD da respuestas a una consulta sobre la interacción de esta nueva ley y la normativa reguladora de la protección de datos personales. Analiza la confidencialidad de las calificaciones en un proceso de concurrencia competitiva, apoyándose en la doctrina de la Audiencia nacional, la cual, en su sentencia de 26 de abril de 2012 de la sección primera de la Sala de lo contencioso administrativo, considera los

---

[407] Aunque aún no hemos revisado la normativa de protección de datos de carácter personal, adelantamos aquí que, al tratarse de una norma de rango legal, es de aplicación el artículo 11.2.a) de la LOPD, a tenor del cual el consentimiento del interesado para la comunicación de sus datos no preciso cuando la cesión esté autorizada en una ley.

[408] Continúa PIÑAR MAÑAS en el texto citado analizando la relación entre el acceso a la información y la protección de datos, citando una nutrida referencia a la jurisprudencia europea, en las páginas 51-57.

[409] La STC 207/1996 de 16 de diciembre de 1996, recuerda que, *"para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".*"

principios de publicidad y transparencia esenciales como garantizadores del principio de igualdad, concluyendo la prevalencia del principio de publicidad sobre la protección de datos y señalando que "(…) *debemos concluir que no es exigible el consentimiento de aquellas personas que participen en un procedimiento de concurrencia competitiva para el tratamiento de las calificaciones obtenidas en dicho procedimiento y ello como garantía y exigencia de los demás participantes para asegurar la limpieza e imparcialidad del procedimiento en el que concurren"*. La sentencia parte de que no existe expresamente exención al régimen de tratamiento de datos personales referente a la garantía de transparencia de los procesos competitivos, por lo que llega a su conclusión recurriendo a la ponderación de los intereses en conflicto. Ahora bien, debemos plantearnos la siguiente cuestión: si la participante en el proceso de concurrencia competitiva fuese una mujer víctima de violencia de género, por ejemplo, una empleada pública acogida a la movilidad del artículo 82 del TREBEP, ¿puede considerarse justificable la publicación de su nombre, apellidos y DNI en Internet, o sería suficiente publicar su puntuación?

Afirma la memoria de análisis de impacto del proyecto de real decreto que la norma no produciría efectos sobre los gastos públicos y sobre los presupuestos generales del Estado y que, a tenor de su disposición adicional única, las medidas contenidas no podrían suponer incremento de dotaciones, retribuciones o gastos de personal[410]. Debemos interpretar, por tanto, que los diversos portales de transparencia que proliferan por las Administraciones públicas, han de ser desarrollados necesariamente por el personal informático a su servicio, en

[410] Recuperado de http://www.mpr.gob.es/otai/Documents/MAIN_Reglamento_Transparencia.pdf (30 de mayo de 2016).

detrimento del resto de tareas que se les pudiera asignar. Ya indicamos *supra* que la inadecuada gestión de la demanda, que lleva a asumir múltiples proyectos simultáneamente sin los recursos necesarios, es una de las causas de la crisis del *software*.

3.2.1.4. Las nuevas leyes administrativas

El 2 de octubre del pasado año 2015, el BOE alumbró dos hermanas siamesas[411], las leyes 39 y 40/2015, que parecen dar el paso definitivo para implantar la eAdministración en nuestro país, gracias a un enérgico impulso de la llamada "Administración sin papeles", tanto en su funcionamiento interno como en sus relaciones con la ciudadanía. Con ellas, la Administración electrónica deja de ser regida por una ley especial para insertarse en el mismo corazón, en el cuerpo principal del Derecho administrativo básico común[412]. Para el OBSAE, estas dos normas "*suponen una gran revolución administrativa, fruto de una sociedad cambiante y de un nuevo entorno presidido por la eficacia, la eficiencia y la innovación tecnológica, que requieren de una correlativa adaptación de la Administración*"[413].

De los nuevos textos legales de 2015 se desprende realmente esa preocupación, casi obsesiva, por la mejora interna del funcionamiento en aras de lograr la eficiencia y economía administrativa, y su abrumadora inquietud por la Administración electrónica, que lleva al legislador a incorporar importantes innovaciones al respecto en unas leyes que, por lo demás, son continuistas en su planteamiento[414]. Pero no era necesario este importante cambio normativo, ni

[411] CHAVES GARCÍA, J.R. (2 de octubre de 2015), siamesas administrativas.
[412] GAMERO CASADO, E. (2016), panorámica.
[413] MINHAP (2016), leyes 39 y 40, 1-2.
[414] CASARES MARCOS, A. (2016), novedades, 66-67.

su separación en dos textos legales[415], para despertar la nueva era de la Administración electrónica. Hubiera bastado dictar una ley específica sobre la materia acompañada de un plan estratégico de implantación progresiva de su contenido[416] y de una dotación presupuestaria adecuada que lo soporte.

Su publicación ha generado una fuerte avenida de tareas informáticas a completar en un breve plazo[417], sin perjuicio de que se pueda aprovechar, adaptar o reutilizar el trabajo ya avanzado en años anteriores. La reforma sancionada por la nueva ley 39/2015 dispone la electronificación absoluta del procedimiento administrativo[418] y el tiempo previsto para ello es escaso. La celeridad con que se han de preparar las soluciones informáticas para alcanzar ese objetivo temporal no puede relajar el estricto cumplimiento de las garantías establecidas para la defensa de derechos fundamentales y, entre ellos, el de protección de datos de carácter personal. Informática y Derecho han de caminar de la mano, teniendo siempre en mente la máxima de que algo "técnicamente posible" no siempre será "jurídicamente lícito", recordando de nuevo que la informática la que debe ajustarse a la normativa, no el Derecho quien debe recoger en sus disposiciones las soluciones informáticas implantadas, por muy efectivas que resulten ser.

Nos advierte Piñar Mañas sobre la potencialidad de las nuevas herramientas, mucho más poderosas que las anteriores, para controlar a los ciudadanos gracias a la obtención,

---

[415] Para GAMERO CASADO (2016), se trata de un problema de calidad normativa con un claro deterioro de la seguridad jurídica, por la dificultad de predecir en qué lugar sistemático se regula cada cuestión, llegando a calificar el nuevo esquema como de caótico.
[416] FERNÁNDEZ RODRÍGUEZ, T. R. (2015), notificaciones electrónicas, 362.
[417] De conformidad con su disposición final 7ª, la ley 39/2015 entrará en vigor al año de su publicación en el BOE, salvo las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la Administración y archivo único electrónico, que producirán efectos a los dos años de la entrada en vigor de la ley.
[418] CASARES MARCOS, A. (2016), novedades, 75.

intercambio y tratamiento de información de todo tipo, y nos alerta de la posibilidad de "*ser utilizadas sin manifestaciones externas aparentes, pero con resultados inimaginables*"[419]. Esa tecnología ya está aquí. Llegó con suavidad, sin llamar demasiado la atención, pero arraigó con fuerza gracias a los grandes beneficios que aportaba en cuanto a comodidad y celeridad, para la Administración y para los administrados, y ahora crece cada día sin descanso (un 24% durante el pasado año y cerca del 50% en este último)[420]. Como añade Piñar Mañas, no podemos olvidar que "*tan posible es con ellas conseguir una Administración transparente como convertirla en esencialmente opaca*"[421].

La **ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas**, junto con la ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, viene a sustituir, entre otras, a nuestra LRJPAC. Se trata de una reforma del ordenamiento jurídico que, además de innovarlo en la dirección favorable a la implantación real y efectiva de la Administración electrónica, y de dar solución al problema de la dispersión normativa, separa las relaciones "*ad extra*" y "*ad intra*" en dos leyes diferentes que marcarán el futuro administrativo. A esta ley 39/2015 le corresponde ocuparse de la regulación de los derechos y garantías mínimas que corresponden a todos los ciudadanos en relación con la actividad de las Administraciones, como señala el legislador en su introducción, aunque cuesta apreciar esa defensa en temas como la notificación por vía electrónica. "*Inaceptable*

[419] PIÑAR MAÑAS, J.L. (2011), Administración electrónica, 148.
[420] Cifras proporcionadas por el subdirector general de impulso de la Administración digital y servicios al ciudadano del Ministerio de Hacienda y Administraciones públicas, MINHAP, Aitor Cubo Contreras, en su intervención en la primera mesa redonda denominada "Una Administración sin papel" de la I jornada sobre las nuevas leyes administrativas celebrada durante los días 16 y 17 de noviembre de 2015.
[421] PIÑAR MAÑAS, J.L. (2011), Administración electrónica, 148.

absolutamente" son las palabras que más repite la doctrina para esta regulación, que transforma lo que antes era una garantía para los interesados en una pesada carga, obligando al ciudadano a recorrer todas las sedes electrónicas en busca de una posible notificación[422].

Una de las manifestaciones de esa innovación es la separación entre identificación y firma electrónica, simplificando los medios para acreditar una u otra. De ordinario se requerirá la identificación del ciudadano, exigiendo la firma electrónica cuando deba acreditarse la voluntad y consentimiento del interesado. Además de los sistemas de identificación y firma contemplados en el tenor de la ley, también será admisible cualquier otro que las Administraciones públicas consideren válido, en los términos y condiciones que se establezcan. Añade el legislador en la introducción que se admitirán como sistemas de identificación cualquiera de los sistemas de firma admitidos, así como sistemas de clave concertada y cualquier otro que establezcan las Administraciones públicas, y nos recuerda "*la obligación de los Estados miembros de admitir los sistemas de identificación electrónica notificados a la Comisión europea por el resto de Estados miembros, así como los sistemas de firma y sello electrónicos basados en certificados electrónicos cualificados emitidos por prestadores de servicios que figuren en las listas de confianza de otros Estados miembros de la Unión Europea* (…)". Como comentamos con anterioridad, la actitud de algunas Administraciones públicas de ir retrasando la modificación de sus aplicaciones informáticas a tal efecto, peca de irresponsable y únicamente logrará posponer lo inevitable, a costa de una pérdida de imagen de nuestras Administraciones en el exterior.

[422] FERNÁNDEZ RODRÍGUEZ, T. R. (2015), notificaciones electrónicas, 364-367.

La ley muestra la preocupación por la seguridad informática, aunque adolece del cierto rigor que sería esperable en un texto posterior a la publicación del ENS, que se manifiesta en su artículo 13.h) cuando hace referencia a la protección de datos personales exigiendo "*la seguridad y confidencialidad de los datos recogidos en sus ficheros, sistemas y aplicaciones*", olvidando que la confidencialidad no es algo ajeno a la seguridad, sino que es una de sus dimensiones, como veremos más adelante. En esta reiteración podemos intuir la intención del legislador de remarcar la importancia de la protección de los datos de carácter personal, que vuelve a poner de manifiesto en su artículo 16.

Aunque la ley no cita explícitamente otra de las dimensiones de la seguridad que analizaremos con posterioridad, la trazabilidad, parece deducirse del tenor de su artículo 17.2, donde, al respecto del archivo de documentos electrónicos, obliga a preservarlos en un formato que permita garantizar su autenticidad, integridad, conservación y consulta con independencia del tiempo transcurrido desde su emisión, permitiendo el cambio de formato y/o soporte que lo haga accesible desde diferentes aplicaciones, en clara referencia a los servicios de custodia digital. El mismo artículo, en el punto siguiente, invoca al ENS en relación con los medios o soportes en que se almacenen documentos, añadiendo una curiosa sucesión de términos: integridad, autenticidad, confidencialidad, calidad, protección y conservación.

Su **artículo 28** contempla la posibilidad de sustituir la aportación de documentos al procedimiento administrativo por uno de entre tres posibles modos de recabarlos de forma electrónica, concretamente a través de sus redes corporativas o mediante consultas a las plataformas de intermediación de datos o a través de otros sistemas electrónicos habilitados al

efecto. El precepto presenta una redacción algo confusa[423]. Tras leerlo repetida y detenidamente, vamos a partir de la idea de que utiliza las expresiones "consultar", "recabar" y "obtener" en calidad de sinónimos. Distingue entre documentos elaborados por las Administraciones públicas (punto 2º) y documentos aportados anteriormente a las Administraciones públicas por los interesados (punto 3º).

- Para los documentos elaborados por la Administración, en un primer momento exige el consentimiento expreso del interesado para poder realizar la consulta pero, acto seguido, se contradice y admite el consentimiento presunto, a falta de oposición expresa o ley especial que requiera consentimiento expreso.

- Para los documentos aportados con anterioridad por el interesado, ya directamente admite el consentimiento presunto con las mismas salvedades del apartado previo. Pero, a diferencia del anterior, añade el deber de información previa de los derechos en materia de protección de datos "*en ambos casos*", aparentemente refiriéndose a las dos salvedades, lo que lleva al contrasentido de que no sea necesario informar de sus derechos a quien autoriza presuntamente (quien podría hacerlo por ignorar sus derechos), pero sí al que se niega expresamente (quien parece conocerlos muy bien). Por ello, aplicando el principio *in dubio por libertate*, parece más adecuada la interpretación de que "ambos" son, por un lado, quienes autoricen aunque sea presuntamente y, por otro, la salvedad, la cual incluye tanto la oposición expresa como la existencia de esa ley especial. Sin embargo, esta interpretación parece demasiado forzada, por lo que cabe plantearse qué motivó el cambio de redacción

[423] GIL DURÁN, M.P. (2016), derecho de control, 132-133.

entre el artículo 42.3 del anteproyecto y el 28.3 del proyecto de ley, en el que se introdujo la frase "*debiendo, en ambos casos, ser informados previamente de sus derechos en materia de protección de datos de carácter personal*". Consultando el informe del anteproyecto elaborado por el gabinete jurídico de la Agencia española de protección de datos, vemos en su página 14 que recoge la necesidad de modificar el tenor del párrafo segundo proponiendo la siguiente redacción:

"*Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá ser informado de la documentación requerida, indicando (…)*"

Por lo tanto, parece razonable concluir que la expresión "*en ambos casos*" se refiere a los datos o documentos no exigidos por la normativa y a los que hayan sido aportados anteriormente. De ser correcta esta suposición, la redacción final del precepto ha sido muy poco afortunada.

En este punto, debemos pararnos a pensar cómo casa la presunción de consentimiento salvo oposición expresa o ley especial aplicable que requiera consentimiento expreso, establecida en dos ocasiones en el artículo 28, con el tenor del RGPD, donde, como ya vimos, se exigía como condición de validez del consentimiento que se tratase de una acción afirmativa, aclarando en el considerando 32 que el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. En mi opinión, la ley 39/2015 debe ser modificada. Los modelos de documentos diseñados a partir de la presunción de consentimiento, en los que

aparezca una casilla para que el interesado pueda marcar su oposición, diseñados a tenor de lo dispuesto en el artículo 28 e implantados a la entrada en vigor de la nueva ley, obligando a modificar el *software* en dos ocasiones: una para ponerlos en producción y otra para retirarlos si finalmente resulta ser incompatible con lo dispuesto en el RGPD. Todo ello, recordemos, lleva asociado un incremento en la tasa de errores del *software* que se refleja en la figura 1 recogida *supra*.

La **ley 40/2015, de 1 de octubre, de régimen jurídico del sector público** recoge las disposiciones que regulan el funcionamiento interno de cada Administración y las relaciones entre ellas, entre las que preceptúa el uso de medios electrónicos que aseguren la interoperabilidad y seguridad de los sistemas y garanticen la protección de los datos de carácter personal[424]. Prevé algo similar al el uso del certificado de empleado público con pseudónimo en el artículo 43.2 e incluye en el 44.4 la obligación de garantizar, también y en todo caso, la seguridad de los entornos cerrados de comunicaciones y la protección de los datos que se transmitan en ellos.

En el capítulo IV del título III, la ley examina las relaciones electrónicas entre las Administraciones. Recuerda la utilidad del ENI y del ENS y contempla diversos aspectos de las transmisiones de datos entre Administraciones públicas. Indica que se debe facilitar el acceso de las demás Administraciones a los datos relativos a los interesados que obren en su poder,

[424] El legislador ha utilizado en este artículo 3.2 una loable redacción, elegante y rigurosa. Hace referencia a la interoperabilidad y a la seguridad, ambas reguladas por los respectivos esquemas nacionales, incluyendo una especial llamada de atención al cumplimiento de la normativa de protección de datos personales. De esta forma cubre todas las dimensiones de la seguridad sin reiterar, olvidar ni inventarse ninguna, defectos a los que ya estamos acostumbrados y que ya hemos hecho constar en varias ocasiones. Desgraciadamente no ha mantenido el mismo criterio en el resto del texto, por ejemplo, en su artículo 46.3, en el 155...

especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios que proporcionen las máximas garantías de seguridad[425]. Pero no puede hacerse libremente, sino cumpliendo la normativa reguladora de la protección de datos de carácter personal, y limitándose estrictamente a los requeridos a los interesados por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia conforme a la normativa reguladora de los mismos.

Debemos llamar la atención de un aspecto novedoso en el artículo 41.1. La nueva ley modifica la definición de "actuación administrativa automatizada", que ahora pasa a ser "*cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público*". Comparándola con la definición anterior, se aprecia que desaparece la exigencia de que esté adecuadamente programada. Con la nueva ley, la actuación administrativa automatizada no perderá tal calificación por el hecho de que el *software* sea defectuoso. Además, suscita la reflexión el concepto de intervención directa. Si se incluye en el *cron*[426] la ejecución de un programa en modo *batch*[427] nocturno que calcule el importe a abonar en determinado concepto a un conjunto numeroso de ciudadanos, estaríamos ante una actuación administrativa automatizada. ¿Pierde tal carácter si ese mismo programa se ejecuta de forma *on-line* cuando un empleado público pulsa el icono llamado "Calcular"? Intuitivamente,

[425] El legislador, como acabamos de comentar, añade las palabras "integridad y disponibilidad"; con "seguridad", que lo englobaría todo.
[426] A través del *cron* se programa la ejecución de un conjunto de tareas de forma desatendida, sin intervención humana.
[427] Modo de ejecución desatendida, por lotes, sin intervención humana, conceptualmente opuesto al modo de ejecución *on-line*.

parece que pulsar un botón no tiene transcendencia suficiente para destruir su naturaleza de actuación administrativa automatizada. ¿Y si ha sido un empleado público el que ha desarrollado íntegramente el programa que se ejecuta? ¿No sería una intervención mucho más directa que pulsar un botón?

El artículo 41.2 reproduce textualmente el tenor del 39 de la LAE, que sigue obligando a establecer previamente el órgano u órganos competentes, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Ciertamente, hace referencia literal al "órgano u órganos", sin incluir el calificativo de "administrativos", lo que podría dar entrada a las empresas del sector privado. Sin embargo, sí emplea la calificación de "competentes" y, recordemos, "*la competencia es irrenunciable y se ejercerá por los órganos administrativos que la tengan atribuida como propia, salvo los casos de delegación o avocación, cuando se efectúen en los términos previstos en ésta u otras leyes*"[428]. Pero únicamente "*podrán delegar el ejercicio de las competencias que tengan atribuidas en otros órganos de la misma Administración, aun cuando no sean jerárquicamente dependientes, o en los Organismos públicos o Entidades de Derecho Público vinculados o dependientes de aquellas*"[429]. Cabe preguntarnos dónde encajan aquí las empresas del sector privado. Evidentemente, tampoco encajan en la avocación, limitada por el artículo 10 a órganos superiores o al órgano delegante. Por tanto, el artículo 41.2 impide a las empresas del sector privado, en el caso de actuación administrativa automatizada:

- la definición de las especificaciones,

[428] Artículo 8.1 de la ley 40/2015.
[429] Artículo 9.1 de la precitada ley.

- la programación,
- el mantenimiento,
- la supervisión y
- el control de calidad y,
- en su caso, la auditoría del sistema de información y de su código fuente.

Aquí reside la importancia de la nueva definición del artículo 41.1. En el momento en que una aplicación informática incluya un acto o una actuación realizada íntegramente por el programa sin intervención directa del empleado público, ese aplicativo no podrá ser externalizado.

3.2.1.5. La protección de datos de carácter personal

Que las TIC han venido para quedarse[430] es una realidad que nadie desea ni puede cambiar. La sociedad actual, incluyendo a las propias Administraciones públicas, se ha transformado de forma tal que las nuevas generaciones no pueden imaginar la existencia sin Internet. Pero, como todo crecimiento vigoroso corre el riesgo de ser descontrolado, necesita una adecuada guía para lograr un desarrollo equilibrado y productivo. Con anterioridad no hemos podido evitar hacer alusión, en diferentes momentos, a la protección de datos personales,

[430] Aplicamos aquí a las TIC la elocuente expresión de COTINO HUESO, L. (2008), derechos del ciudadano, 119.

íntimamente ligada con los variados temas que hemos ido comentando. Este puede ser un buen momento para detenerse a estudiar monográficamente la normativa que la regula[431].

La **Constitución española de 1978**, igual que otros textos contemporáneos y territorialmente próximos[432], como el portugués de 1976 o la ley federal alemana de 1977, ya reflexionaba sobre el potencial peligro de las técnicas informáticas, por su incidencia en la vida de los ciudadanos. En su artículo 105.b), referente al derecho de acceso a archivos y registros administrativos, matizaba su exclusión cuando la información que de ellos pudiera recabarse afectara, en otros, a la intimidad de las personas[433.] Pero es en el artículo 18.4 donde el constituyente manifestaba su recelo ante las nacientes nuevas tecnologías y las subordinaba al ejercicio de los derechos por parte de la ciudadanía, un recelo con cierto carácter premonitorio, pues en la década de los setenta no se disponía de la tecnología actual, no se trataban los ingentes volúmenes de datos que se manejan hoy día, ni las facilidades para distribuirlos de forma instantánea eran las mismas que ahora, motivos por los que parece razonable que no podamos encontrar en el Texto constitucional específicamente reconocido el derecho a la protección de datos. Tampoco se prevé su inclusión, pues la rigidez de nuestra Constitución origina importantes dificultades para su modificación; aún no se ha logrado el consenso requerido para la inclusión de un nuevo derecho fundamental.

---

[431] Para una información más exhaustiva, puede consultarse el código de protección de datos de carácter personal recuperado de http://www.boe.es/legislacion/codigos/codigo.php?id=055_Proteccion_de_Datos_de_Caracter_Personal&modo=1 (31 de mayo de 2016).

[432] Ya más alejado de nuestras fronteras podemos referir la americana *Privacy Act* de 1974.

[433] Para mayor información sobre su desarrollo legal y excepciones a su obligatoriedad, *vid.* http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=105&tipo=2 (recuperado el 14 de octubre de 2015).

Hoy en día, los poderes públicos, para llevar a cabo las funciones que la propia Constitución les encomienda, recogen, almacenan y procesan de forma masiva e ineludible los datos personales de millones de ciudadanos. Esa enorme cantidad de información, recogida a una escala cada vez más amplia de bases de datos, da una información fragmentaria pero múltiple de perfiles relativos a las personas[434].

La elaboración de perfiles no requiere una gran complejidad técnica y sí puede resultar notablemente perjudicial en manos de empresas aseguradoras o empleadoras[435]. Entre sus utilidades se encuentra el *marketing* relacional, en auge, que se basa en el tratamiento masivo de grandes cantidades de datos buscando conseguir del mayor número posible de perfiles de las personas para conocer sus patrones de conducta, a fin de identificar las necesidades de los clientes de forma individual[436]. Con esos perfiles, con esa información elaborada, se posibilita la toma de decisiones sobre ellas, así como el análisis y la predicción de sus preferencias, comportamientos y actitudes[437].

Con ese espíritu preventivo, el constituyente disponía la remisión a la ley para limitar[438] el uso de la informática como garantía del honor y la intimidad personal y familiar de los ciudadanos y del pleno ejercicio de sus derechos. Dicha reserva legal, por afectar a derechos

[434] PÉREZ VELASCO, M.M. (2006), intercambio de datos, 45-46.
[435] FUNDACIÓN TELEFÓNICA (2016), ciberseguridad, 62-63. Recuerda lo sencillo que resulta establecer perfiles de las personas a partir de los *likes* de *Facebook*, comentando la existencia de estudios que refieren la posibilidad de predecir con ello la localización de una persona con 80 semanas de anticipación y un 80% de fiabilidad.
[436] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 271.
[437] Considerando 24 del RGPD.
[438] SANTAMARÍA IBEAS, J.J. (1994), la LORTAD, 262. El autor parece apreciarse una aparente predisposición negativa del constituyente español, al no hablar de "regular", sino de "limitar" el uso de la informática. Si bien este autor califica de criticable dicho prejuicio, hoy, casi cuatro décadas después, los niveles de injerencia de las TIC en nuestras vidas parecen confirmar la justificación de dichos temores.

fundamentales, ha de entenderse referida a ley orgánica, a tenor del artículo 81.1 de nuestra Carta Magna. Lo que no se especifica son los métodos para ejercer esa limitación, por lo que queda al arbitrio del legislador orgánico la forma de garantizar el derecho de autodeterminación informativa.

La enérgica incursión de las nuevas tecnologías durante las últimas décadas ha forzado la reacción del ordenamiento jurídico, diseñando un conjunto legislativo con frecuencia incompleto, lo que ha exigido a la jurisprudencia la siempre difícil tarea de colmar las lagunas que surgían cada vez que la técnica se adelantaba a la norma, hambrienta de actualización.

La **ley orgánica 1/1982, de 5 de mayo, de protección civil del honor, la intimidad personal y familiar y la propia imagen**, no llegaba a abordar el desarrollo del artículo 18.4 de forma autónoma; hace referencia a los aparatos de grabación y detección de conversaciones, pero no al tratamiento de datos personales. Su enfoque se basa en la protección final del honor, intimidad y propia imagen como derechos tradicionales, problemas que sí preocupaban a la sociedad española del momento, que aún no había tomado conciencia del nuevo derecho emergente.

El derecho a la autodeterminación informativa fue construido a partir de la sentencia del Tribunal constitucional federal alemán de 15 de diciembre de 1983, en la que se parte del derecho general de la personalidad recogido en el artículo 2.1 de la ley fundamental de Bonn y se llega a la configuración de un derecho a decidir cuándo y bajo qué límites revelar situaciones referentes a la propia vida, de lo que se deriva la necesidad de proteger jurídicamente

el uso informático de datos personales, no por su carácter privado, sino por el peligro que supone su utilización[439].

Hasta 1992, España fue uno de los pocos países de Europa occidental que no contaba con una disciplina jurídica en la materia. Cuando las Cortes generales afrontaron este desarrollo legislativo, no tuvieron que inventar nada, obtuvieron sobrada inspiración del abundante Derecho comparado, además de ajustarse a las disposiciones del convenio 108, en cumplimiento del mandato constitucional del artículo 10.2. La tardanza en dar ese paso solo pudo deberse a "*una falta de conciencia de la entidad del problema que aquí subyace*"[440].

El Estado español viene a cumplir sus compromisos internacionales en la materia y el mandato del constituyente, con la promulgación de nuestra primera ley de protección de datos, la **ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal**, LORTAD, desarrolladora del artículo 18.4 de nuestra Norma Suprema, que mantendrá su vigencia hasta el 14 de enero de 2000, fecha en que es derogada y sustituida por la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, LOPD.

La LORTAD declara tener por objeto la limitación del uso de la informática (misma expresión aparentemente negativa que la recogida en el precitado artículo 18.4) y de otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

[439] BRU CUADRADA, E. (2007), mecanismos jurídicos, 81.
[440] MURILLO DE LA CUEVA, P.L. (1998), autodeterminación informativa.

Cabe preguntarse por qué se tardó catorce años en dotar a nuestro ordenamiento jurídico de un desarrollo normativo del artículo 18.4. Como sugiere de la Quadra-Salcedo, "*tal vez lo explique el escaso desarrollo todavía de la informática y la telemática en nuestro país; o que la preocupación principal consistía en el desarrollo de los derechos fundamentales clásicos que hasta esa fecha habían sido negados por la Dictadura*"[441].

Este texto legal se aplica a los datos de carácter personal que figuren en ficheros automatizados, tanto públicos o privados, alcanzando incluso al uso posterior y no automatizado de los mismos, cuando están registrados en soporte físico susceptible de tratamiento automatizado[442.] Quizá su publicación fue un poco precipitada, adelantándose a la directiva 95/46/CE que ya estaba en preparación y que obligaría, por tanto, a adaptar la nueva ley poco tiempo después de su nacimiento, para incluir en su ámbito de aplicación a los ficheros no automatizados[443].

A pesar de las múltiples excepciones en su ámbito de aplicación, la LORTAD viene a poner punto final a la escasez y dispersión de la regulación existente en aquel momento, con importantes lagunas en el ordenamiento jurídico que generan indefensión[444]. Sorprende la claridad con la que el legislador de 1992 intuye el peligro que conlleva la recolección,

[441] DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T. (2015), LORTAD, 31.
[442] Conviene recordar que la LORTAD va ligada a la limitación del uso de la informática dispuesto por el precitado artículo 18.4 constitucional, lo que motiva la pretensión de congruencia entre la Norma fundamental y su desarrollo legislativo, que se refleja en que el ámbito de aplicación ha de estar ligado al uso de ordenadores, es decir, se aplica a los ficheros automatizados o, al menos, a ficheros con tratamiento automatizado posterior.
[443] DE LA QUADRA-SALCEDO plantea, entre los motivos de esa posible precipitación, el nacimiento en la conciencia de nuestra sociedad de la importancia de ese nuevo derecho al ir generalizándose el uso de la informática y la telemática, e ir surgiendo situaciones litigiosas relacionadas con ello. Añade también como razón el compromiso internacional del Estado español de adaptarse a las exigencias del Convenio 108.
[444] SANTAMARÍA IBEAS, J.J. (1994), la LORTAD, 269.

almacenamiento, tratamiento y distribución de datos aislados que, coherentemente enlazados[445], pueden conducir a la elaboración de un perfil de la personalidad del individuo no siempre acertado pero que, en todo caso, debería mantenerse reservado a su esfera privada. Así lo expresa en su exposición de motivos, cuando advierte de la posibilidad de que los más diversos datos puedan ser compilados, permitiendo así acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que pertenecen a la esfera privada de las personas, así como dibujar un determinado perfil o configurar una determinada reputación o fama. Por ello, el legislador sitúa su foco de atención en el *software* que procesa los datos almacenados, que son susceptibles de configurar el perfil del individuo si llegan a conectarse entre sí, a la vez que manifiesta su convencimiento de que dicho perfil puede ser valorado para las más diversas actividades, no solo privadas, sino también públicas.

Este texto legal comparte con el convenio 108 los principios de protección de datos, aunque la LORTAD es más estricta cuando dispone que los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades "distintas" de aquellas para las que los datos hubieran sido recogidos (el convenio solo rechaza las finalidades incompatibles).

Hoy nos queda, en recuerdo de esta ley, la Agencia de protección de datos de la cual fue creadora, ente estatal de derecho público independiente de las diferentes Administraciones, que tiene atribuidas distintas potestades administrativas de naturaleza

[445] Este tema ya se refleja en la literatura con gran éxito de ventas, como es el caso de la novela "El círculo" de DAVE EGGERS, de 2014, que retrata una asfixiante sociedad a la que nos veríamos abocados si se realizase un tratamiento masivo de datos aislados en ausencia total de limitaciones legales.

ejecutiva, a las que añadir cierta capacidad normativa[446]. Ante ella es posible reclamar las actuaciones contrarias a esta normativa, en la forma que reglamentariamente se determine, procediendo la interposición de recurso contencioso-administrativo contra sus resoluciones.

La consideración de la protección de los datos de carácter personal como derecho fundamental llegó de la mano de la jurisprudencia. Una serie de sentencias de amparo, entre las que podemos citar la STC 94/1998 viene a respaldar a un sector de la doctrina que defendía la existencia de un derecho fundamental autónomo, independiente del derecho a la intimidad, que permita controlar el flujo de información personal, pertenezca o no ese ámbito de la intimidad. Las STCs 290 y 292 de 2000 ya afirman que es un derecho que tiene su propia sustantividad. Hoy día, no cabe duda de tal naturaleza, reforzada por el nuevo RGPD[447].

La denominación que se da a este nuevo derecho parece no estar cerrada todavía. Se le ha llamado "derecho a la libertad informática". En otras ocasiones ha recibido el nombre de "*habeas data*", cuando en realidad esta expresión refleja más bien un instrumento puesto a su servicio. También ha sido llamado "derecho a la autodeterminación informativa", pero tampoco parece convencer, lo mismo que la expresión "derecho a la protección de datos". Lo que subyace en el fondo es la garantía de la privacidad. Como indica de la Quadra-Salcedo, "*me parece que no hemos encontrado todavía el nomen iuris que le cuadre*"[448].

En virtud de la habilitación de desarrollo reglamentario prevista en la disposición final primera de la LORTAD, se dicta el **real decreto 1332/1994, de 20 de junio, por el que se**

[446] BERNADÍ GIL, X. (2005), Derecho público, 222.
[447] PIÑAR MAÑAS, J.L. (2016), nuevo modelo europeo de protección de datos, 15 y 16.
[448] Expresión empleada en su intervención en la jornada de celebración, por la Agencia española de protección de datos, de los 20 años de protección de datos en España.

desarrollan determinados aspectos de la ley orgánica 5/1992, vigente hasta el 19 de abril de 2008. Encontramos en él una definición de "datos de carácter personal" más detallada que la ofrecida por los instrumentos jurídicos vistos hasta ahora: "*toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable*". Destaca en su texto la referencia al bloqueo de datos del artículo 16 y la concepción como personalísimos de los derechos de acceso a los ficheros automatizados, de rectificación y de cancelación, sin perjuicio de la actuación a través de representante legal del afectado que se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

Con la publicación del **real decreto 994/1999, de 11 de junio, por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal**, vigente hasta el 19 de abril de 2008, se lleva a cabo el desarrollo de lo dispuesto en los artículos 9, sobre seguridad de los datos [449], y 43.3.h[450] de la LORTAD. Tras esos casi siete años de anhelada espera, este reglamento vino a configurar tres niveles de medidas de seguridad mínimas exigibles en función de la mayor o menor necesidad de garantizar la confidencialidad[451] y la integridad de la información. Lejos de establecer un

[449] Establece la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos personales, remitiendo a un posterior desarrollo reglamentario la especificación de los requisitos y condiciones exigibles.
[450] Considera infracción grave el mantenimiento de ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad determinadas reglamentariamente.
[451] De ninguna forma debe entenderse que el nivel de seguridad bajo equivale a no dotar de una protección adecuada a la información o a los servicios, por las pocas repercusiones que pueda tener la ocurrencia de un incidente de seguridad. Pongamos un ejemplo… En un sistema de gestión de personal pueden almacenarse los cursos de formación de los empleados públicos, la cual parece ser una información inocente, que a alguien inexperto en

documento meramente teórico, se logró elaborar un referente práctico que permitiría a los responsables guiarse en la adopción de las medidas necesarias. Su fin era establecer las medidas técnicas y organizativas necesarias para garantizar la seguridad de los ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

La **ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal**, que deroga la LORTAD, adaptó nuestro ordenamiento a lo dispuesto por la directiva 95/46/CE del Parlamento europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Lo que en principio pretendía ser un cambio sencillo, derivó en un proceso complejo que, como lamenta de la Quadra-Salcedo[452], dejó una ley ayuna de toda exposición de motivos.

En su objeto ya apreciamos una diferencia con su predecesora. Mientras la LORTAD buscaba limitar el uso de la informática, la LOPD parece deshacerse de esa visión

---

protección de datos podría parecerle poco digna de la adopción de las medidas necesarias para asegurar su confidencialidad. Esa persona podría pensar, muy acertadamente, que el mantenimiento de esos cursos en un sistema informático permite, con un relativamente pequeño esfuerzo y en un brevísimo tiempo, generar de forma automática los certificados de méritos generales de miles de funcionarios. Hasta aquí tendríamos un uso legítimo y altamente productivo de la información y del sistema informático. Pero… ¿sería igual de legítimo ejecutar un proceso que genere un listado de los empleados públicos que han realizado el curso titulado "Excel", "Gestión de personal" y "Procedimiento administrativo"? ¿Y si cambio la pregunta de "Excel" por "*Data Warehouse*"? ¿Y si sigo así sucesivamente hasta averiguar qué cursos tengo que incluir como méritos en un concurso para que la plaza la consiga la persona que yo quiero que la obtenga? Estaríamos utilizando la informática para eludir los principios constitucionales de igualdad, mérito y capacidad en el acceso al empleo público.
Por ello, no basta con que la persona que acceda a la información esté autorizada para acceder a ella. También ha de tener una justificación legítima para acceder a ella. Pero si no existe un procedimiento de revisión de los accesos y sus motivos, ¿quién va a controlarlo? ¿Acaso el Juez de lo contencioso administrativo va a pedir el registro de accesos? ¿Por qué motivo iba a pedirlo? ¿Cómo puede el perjudicado demostrar la desviación de poder a la hora de "diseñar" el concurso a medida?

[452] QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T. DE LA. (2015), LORTAD, 27.

negativa de las TIC y, apreciando su potencial, pretende garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Por ello, es de aplicación a los datos de carácter personal registrados en cualquier soporte físico, incluso papel, no requiriendo ya que se trate de ficheros automatizados. Se independiza así del uso de la informática que motivó el surgimiento de su predecesora LORTAD.

La ley nos ofrece una serie de definiciones unificadoras de conceptos entre las que incluye la noción de "datos de carácter personal", considerando como tal cualquier información concerniente a personas físicas identificadas o identificables, añadiendo que se considerará un "fichero" a todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Ambas definiciones nos resultarán imprescindibles más adelante, para poder analizar la legalidad de algunas aplicaciones informáticas públicas en uso en nuestro país, estudio en el que invocaremos también el artículo 4.1, que contiene una regla reiteradamente invocada en informes y jurisprudencia: "*Los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*". Cuando los datos se recojan directamente del interesado, este puede negarse a proporcionarlos cuando no le parezcan pertinentes o adecuados o los considere excesivos para la finalidad para la que se recaban, decisión que va íntimamente ligada a su derecho a la información en la recogida de

datos. La ley añade además que los datos no podrán utilizarse para otros fines incompatibles con aquellos para los que fueron recogidos, siendo cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, no pudiendo conservarse en forma que permita la identificación del interesado durante un período superior al necesario para sus fines.

El tratamiento requiere el consentimiento inequívoco del afectado, salvo que por ley se disponga otra cosa o se den unas ciertas situaciones, entre ellas, la recogida para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias[453] o que se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

Destacable también es el artículo 6.4: "*En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, este podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable de fichero excluirá del tratamiento los datos relativos al afectado.*"

La ley reconoce el derecho de oposición, incorporado por primera vez en la directiva 95/46/CE del Parlamento europeo y del Consejo, pero ha recibido numerosas críticas

[453] La redacción de este artículo se mejoró en el reglamento de desarrollo, al especificar que esas competencias debían serle atribuidas por una norma con rango de Ley o una norma de derecho comunitario. Aquí hemos de señalar el procedimiento de declaración de infracción de Administraciones públicas AP/00024/2015, instruido por la AEPD a la Consejería de educación, cultura y deporte de la Junta de Andalucía, por incluir en una página *web* de libre acceso nombres y apellidos de empleados públicos destinados en un instituto de enseñanza secundaria sin haber recabado previamente su consentimiento inequívoco.

por su insuficiencia, al no definir en qué consiste, cuestión resuelta al publicar el reglamento que la desarrolla.

Un estudio sobre seguridad e informática no puede dejar de llamar la atención sobre el artículo 9 de la LOPD, rubricado como "seguridad de los datos", referente a la obligación de "*adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos*", en cuyo segundo apartado incluye específicamente la seguridad de los programas.

La LOPD dedica su artículo 11 a la comunicación de datos, solo posible, salvo disociación, para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, requiriendo el previo consentimiento del interesado salvedad hecha de los casos enumerados en su apartado 2, donde podemos destacar la autorización legal de la cesión. Ese consentimiento, que será revocable, será nulo cuando el interesado ignore la finalidad a que se destinarán o el tipo de actividad del cesionario. Este artículo será de aplicación a los accesos automatizados pues, como señala Valero Torrijos, nos vemos obligados a equiparar el acceso automatizado a una simple cesión o comunicación, habida cuenta de la falta de adaptación normativa a esa específica realidad tecnológica[454].

La disposición adicional cuarta modifica el artículo 112.4 de la ley general tributaria para excepcionar la necesidad de consentimiento en la cesión de datos objeto de

[454] VALERO TORRIJOS, J. (2008), acceso a los servicios, 276.

tratamiento a efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal. En este ámbito tampoco será de aplicación la cesión del artículo 21.1 de la LOPD.

De total aplicabilidad en la contratación de servicios de desarrollo de *software* para las Administraciones públicas es el artículo 12, que regula el acceso a los datos por cuenta de terceros, donde se establece que no se considera comunicación de datos cuando dicho acceso es necesario para la prestación de un servicio al responsable del tratamiento y se detallan diversos aspectos prácticos en relación con su ejecución.

Resulta imprescindible señalar aquí el artículo 21, rubricado como "comunicación de datos entre Administraciones públicas", en virtud del cual los datos de carácter personal recogidos o elaborados por la Administración para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o que versen sobre materias distintas salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. El inciso «*cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso*» fue declarado nulo por la STC 292/2000[455].

Si bien el RGPD europeo no ha puesto fin a nuestra LOPD, sí se verá parcialmente desplazada, exigiendo su modificación. En su considerando 8, la norma europea

[455] http://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf

prevé la posibilidad de que los Estados miembros incorporen a su normativa nacional, por razones de coherencia y claridad, elementos de la misma.[456]

Al igual que la LOPD, el **real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999**, tiene por finalidad afrontar los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales, lo que intenta completando las carencias detectadas durante los ocho años que transcurrieron entre la publicación de ambos y aportando un conjunto de definiciones que permiten entender los conceptos más técnicos en materia de protección de datos[457]. Con su publicación se derogan los reales decretos 1332/1994 y 994/1999, así como todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en él.

El reglamento será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, automatizado o no, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Sin embargo, establece una preocupante excepción en su artículo 2.2, donde establece que no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. Dado que este artículo plantea una excepción a la obligación de protección de datos, debe interpretarse en sentido estricto y de

[456] PIÑAR MAÑAS, J.L. (2016), nuevo modelo europeo de protección de datos, 16.
[457] La AEPD ha publicado un conjunto de guías, a modo de ayuda, para promover el adecuado cumplimiento de la LOPD y de este Reglamento que la desarrolla. Entre ellas figura la guía para la protección de datos en las relaciones laborales.

modo restrictivo, por lo que en cualquier fichero que contenga datos adicionales a los citados se encontrará plenamente sometido a la LOPD. Como indica la AEPD en su informe 78/2008, no están excluidos del ámbito de aplicación de la ley los ficheros en los que se incluya el DNI, al no ser necesario para el mantenimiento del contacto empresarial.

De especial interés para los casos de contratos de servicios informáticos realizados por las Administraciones públicas son los artículos 20 y 21, que contemplan las relaciones entre el responsable y el encargado del tratamiento[458] y la posibilidad de subcontratación, 82 "encargado del tratamiento", 83 "prestaciones de servicios sin acceso a datos personales" y 86 "régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento".

El artículo 34 de este real decreto viene a paliar la laguna dejada por la LOPD al no definir qué se entiende por derecho de oposición, regulando su ejercicio en el artículo que le sigue.

De especial interés es el título VIII, "De las medidas de seguridad en el tratamiento de datos de carácter personal", donde las clasifica en tres niveles: básico, medio y alto. Por defecto, se aplicarán las medias de nivel básico, añadiendo otras cuando se cumpla alguna de las circunstancias que obligan a elevar el nivel de protección, a tenor de lo establecido en el artículo 81. Las medidas incluidas en cada uno de esos niveles tienen la condición de mínimos exigibles.

[458] El tratamiento de datos por cuenta de terceros se regula en el artículo 12 de la LOPD.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Los ficheros temporales o copias de documentos creados exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81, y serán borrados o destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación.

En el artículo 88 se contempla detalladamente el documento de seguridad que debe elaborar el responsable del fichero o tratamiento, donde se recogerán las medidas técnicas y organizativas acordes a la normativa de seguridad vigente, que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

Señala Valero Torrijos la falta de rigor con que sus previsiones se han aplicado en el ámbito de las Administraciones públicas, relacionándolo con el hecho de que el incumplimiento de las obligaciones legales no pueda ser sancionado económicamente, añadiendo que tampoco se sanciona con la invalidez, al menos en los casos más graves, las decisiones administrativas adoptadas por medio del incumplimiento[459].

Finalmente, cabe reseñar la **STJUE de 24 de noviembre de 2011**, que resuelve la cuestión prejudicial planteada por nuestro Tribunal Supremo relativa a la interpretación del artículo 7.f) de la directiva 95/46/CE. En ella se reconoce el efecto directo de dicho artículo y se subraya la necesidad de realizar una ponderación entre el interés legítimo de quien vaya a tratar

[459] VALERO TORRIJOS, J. (2014), de la digitalización a la innovación tecnológica, 121.

los datos y los derechos fundamentales de los ciudadanos afectados, para poder determinar en cada caso concreto cuál prevalece.

La **ley 15/2014, de 16 de septiembre, de racionalización del sector público y otras medidas de reforma administrativa**, al prever la utilización preceptiva del BOE para la publicación de actos administrativos con plenos efectos, mediante la reforma del artículo 59.5 LRJPAC, no ha tenido en cuenta las implicaciones que tiene la difusión de información administrativa referida a la protección de los datos personales de los ciudadanos, incluso a pesar de que la decisión del TJUE sobre el derecho al olvido[460] de 13 de mayo de 2014[461] (asunto C-131/12)[462]. Este derecho se orienta a evitar que ciertos episodios obtengan una difusión permanente en la *web*, permaneciendo de manera atemporal en los motores de búsqueda, ocasionando un perjuicio gratuito una vez producido el efecto de publicidad administrativa y transcurridos los periodos de recursos. Se concreta en la facultad de solicitar la cancelación de esos datos.[463]

Durante los días 16 y 17 de noviembre de 2015 tuvieron lugar las jornadas sobre **las nuevas leyes administrativas, 39 y 40/2015**, en el Instituto nacional de Administración pública, INAP. Los vídeos de las diferentes intervenciones se encuentran disponibles en la mediateca de su página *web*, www.inap.es. El subdirector general de impulso de la Administración digital y servicios al ciudadano del MINHAP intervino en la primera mesa

[460] VALERO TORRIJOS, J. (2014), de la digitalización a la innovación tecnológica, 123.
[461] *Vid*. LÓPEZ PORTAS, M.B. (2015), derecho al olvido, 143-175.
[462] Para conocer la normativa relacionada con este derecho, se ha elaborado un código del derecho al olvido disponible en la URL http://www.boe.es/legislacion/codigos/codigo.php?id=094_Codigo_del_Derecho_al_Olvido&modo=1 (recuperado el 31 de mayo de 2016).
[463] SUÁREZ VILLEGAS, J.C. (2014), el derecho al olvido, 35-36.

redonda, denominada “Una Administración sin papel”, donde dedicó parte de su entusiasta ponencia a la plataforma de intermediación de datos. Sin dejar de reconocer públicamente el meritorio trabajo realizado por él y por su equipo para hacer realidad, en todas las Administraciones de nuestro país, la implantación de la Administración electrónica de forma racional, optimizada y organizada, es el momento de señalar un punto de su discurso que, personalmente, me transmite preocupación por la posible falta de control por los ciudadanos de sus propios datos personales, en particular la descripción de la plataforma de intermediación como “*un sitio donde se comunican todos los datos de todas las Administraciones públicas para que sean recogidos por otras*”, cuyo uso se describe de la siguiente forma: “*Cualquier dato que necesite para mi procedimiento administrativo, miro a ver si está en la plataforma. Si está en la plataforma, no se lo pido al ciudadano, lo uso directamente*.” Se podría entender que, por la limitación del tiempo asignado a su ponencia, ha prescindido de añadir que antes verifica que tiene el consentimiento para realizar tal consulta o que no consta la oposición del ciudadano. Sin embargo, transmite cierto desasosiego que pueda extenderse la tendencia a olvidar esa comprobación[464].

Por su repercusión en la esfera jurídica de los ciudadanos, dedicaremos un apartado a estudiar detenidamente esta plataforma más adelante.

3.2.1.6. La regulación de la firma electrónica

La nueva concepción del servicio público que subyace bajo la denominación de eAdministración debe superar el obstáculo que supone la distancia física. La gestión de la

[464] GIL DURÁN, M.P. (2016), derecho de control, 134-135.

identidad es uno de los pilares que sostiene la eAdministración y la técnica nos proporciona herramientas para dar solución a esa problemática proporcionando la confianza requerida. "Confianza" no es solo una palabra cuya presencia inunda páginas, es mucho más que eso, es la base sobre la que se edifica la Administración electrónica y, para obtenerla, es preciso dotarse de un marco normativo adecuado que haga desaparecer la inseguridad jurídica que acompaña, con frecuencia, al vertiginoso desarrollo de las nuevas tecnologías.

Si bien la Administración tributaria o la CNMV ya hacían uso de la firma electrónica en sus actividades, la primera regulación jurídica con un ámbito de aplicación general llegó con el **real decreto ley 14/1999, de 17 de septiembre, sobre firma electrónica**, vigente hasta el 20 de marzo de 2004. Publicada adelantándose tres meses a la directiva europea en la materia, España mostró así su decisión de ponerse en cabeza de los países miembros[465]. Duramente criticada por el procedimiento y el momento de su aprobación, su desarrollo incompleto llevó como consecuencia su escasa aplicación y pobre utilidad real[466].

Su objetivo era fomentar el uso de esta nueva técnica para incrementar la seguridad en la transmisión de información y, con ello, aumentar la confianza de los potenciales usuarios, ya se tratara de ciudadanos, empresas o las propias Administraciones públicas, e impulsar así el avance en nuestro país de la sociedad de la información que Europa insistentemente reclamaba. La necesidad de proporcionar una adecuada seguridad jurídica de la que se carecía hasta ese momento se utilizó como justificación de la urgencia de su publicación. Se consideraba que el sector empresarial español podía prestar un servicio de certificación de

[465] MARCOS MARTÍN, J.L./ BALSELLS TRAVER, M. (2000), génesis y regulación, 31.
[466] BERROCAL LANZAROT, A.I. (2006), la firma electrónica, 399.

suficiente calidad, para lo cual era preciso establecer un régimen jurídico que le fuera aplicable, previendo la acreditación voluntaria de prestadores de servicios de certificación mediante sistemas regulados por normas objetivas, razonables y en ningún caso discriminatorias[467].

Se pretendía potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aportara confianza en la realización de transacciones electrónicas en redes abiertas, como Internet. El citado real decreto ley incorporó al ordenamiento público español 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.

En desarrollo de este real decreto ley se promulgó la **orden de 21 de febrero de 2000** por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, aún vigente, y posteriormente el **real decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la ley 66/1997**, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, en materia de prestación de servicios de seguridad por la FNMT-RCM, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones públicas[468], también vigente, que no debe interpretarse como una asignación en exclusiva de la prestación de dichos servicios a la FNMT, habida cuenta del régimen de libre concurrencia imperante en el sector.

[467] *Vid.* sumario del real decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.
[468] *Vid*. ARENILLA SÁEZ, M. (2011), crisis y reforma, 182-183.

2003 acaba su andadura trayéndonos una nueva regulación que viene a reforzar esa ansiada seguridad jurídica y la consecuente confianza por parte de la ciudadanía, en un momento en que era palpable su necesidad[469]. Se trata de la **ley 59/2003, de 19 de diciembre, de firma electrónica**, cuya exposición de motivos resalta la nociva repercusión de ese manifiesto recelo en el desarrollo de la Administración electrónica. El texto legal completa, actualiza y sustituye el marco establecido en el real decreto ley 14/1999, con la intención de dinamizar el mercado de la prestación de servicios de certificación. Sin embargo, no derogó el artículo 81 de la ley 66/1997, que recoge un régimen específico para la FNMT-RCM, lo que sirvió para dotarla de un estatuto prevalente discordante con el principio de libre prestación de servicios en que se basa la directiva europea, aspecto no resuelto hasta 2007[470].

La nueva ley cambia sutilmente la definición de firma electrónica, pasando a considerarla como "*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*". Algo tan corriente como una contraseña en un sistema de autenticación que requiera usuario y *password*, es una firma electrónica, al igual que un PIN, un nombre al pie de un correo, la combinación de una pregunta-respuesta, todos ellos de complejidad tan escasa como la seguridad que proporcionan, lo que plantea dudas sobre su valor probatorio sobre la autenticación o identificación del firmante[471].

[469] El artículo del Diario de León de fecha 30 de junio de 2003 resulta muy ilustrativo de la problemática del momento. Recuperado de http://www.diariodeleon.es/noticias/sociedad/descubierto-agujero-seguridad-electronico-fabrica-moneda_88660.html (9 de abril de 2016).
[470] VALERO TORRIJOS, J. (2014), de la digitalización a la innovación tecnológica, 120-121.
[471] BERROCAL LANZAROT, A.I. (2006), la firma electrónica, 406.

La ley establece una especialidad dentro de las firmas electrónicas, que denomina "avanzada" y que no solo posibilita identificar al firmante sino que, además, "*permite detectar cualquier cambio ulterior de los datos firmados*", utilidad cuya importancia ya se ha comentado. Pero no es suficiente con ello para que la firma se considere avanzada. También se exige que esté "*vinculada al firmante de manera única y a los datos a que se refiere*". Hasta el 30 de junio de 2015 la ley añadía otro requerimiento para considerar la firma electrónica como avanzada, que fuera "*creada por medios que el firmante puede mantener bajo su exclusivo control"*. Sin embargo la nueva redacción[472] lo ha sustituido por "*creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control*". El legislador ha introducido un concepto jurídico indeterminado en la definición, que abre una puerta a la inseguridad jurídica.

A su vez, la ley introduce una novedad con respecto a su predecesora, cual es la distinción de una especialidad dentro de las firmas electrónicas avanzadas, que denomina "reconocida"[473] y define como "*la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*". Se deduce, por tanto, que el uso de un certificado reconocido no necesariamente implica que la firma por él generada sea reconocida[474].

[472] Nueva redacción creada por el apartado uno de la disposición final cuarta de la ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social.
[473] BERROCAL LANZAROT, A.I. (2006), la firma electrónica, 418. Señala la autora que nos encontramos ante una novedad más formal que sustantiva, pues simplemente se crea una nueva categoría de firma a la que otorga un *nomen iuris*, al que asocia un concepto contenido en la norma preexistente.
[474] *Vid*. JUNTA DE ANDALUCÍA. CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA (1 de marzo de 2012), avanzada y reconocida.

La noción de certificados reconocidos la proporciona la misma ley en su artículo 11, definiéndolos como los "*expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten*". El concepto de dispositivo seguro de creación de firma lo encontramos en el artículo 24, donde se recogen un mínimo de exigencias de obligado cumplimiento, redactadas de nuevo recurriendo a conceptos jurídicos indeterminados como "asegurar razonablemente" o "seguridad razonable".

Esta firma electrónica reconocida, cumplidora de todos los requisitos exigidos, es la que el legislador equipara funcionalmente con la firma manuscrita en el artículo 3.4. Sin embargo, la firma electrónica realizada con un determinado tipo de certificado electrónico reconocido, podría ser o no una firma electrónica reconocida, en función de si el usuario final ha decidido utilizar o no un dispositivo seguro de creación de firma. En el caso del DNIe, el dispositivo siempre será el propio carné, mientras que con un certificado *software* exportable la decisión queda en manos de su titular, originando una importante inseguridad jurídica.

Coincido plenamente con Francisco J. García Mas[475] en su advertencia contra la manera grandilocuente en que se proclama que este tipo de firma garantiza la identidad del firmante. Aclara que esa identidad no queda asegurada al cien por cien, pues el titular de la firma puede no haber sido quien ha firmado[476], sino un tercero. Valero Torrijos señala la dificultad

[475] Opinión de GARCÍA MAS recogida por BERROCAL LANZAROT, A.I. (2006), la firma electrónica, 420.
[476] La firma electrónica, a diferencia de la manuscrita, realmente no es "personal e intransferible".

para demostrar el uso ilícito del certificado, que, en muchos casos, se puede convertir en una *probatio diabolica*.[477]

A modo de ejemplo García Mas señala la posibilidad de que el titular haya dado el PIN de acceso a alguien voluntariamente[478], lo haya extraviado o haya sido observado o copiado por personas ajenas. Plantea la posibilidad de asumir o no responsabilidades por parte del titular de la firma, quien, por su falta de diligencia, podría tener arrogarse las consecuencias de la utilización de la firma por un tercero, pero, de forma rigurosa, no se podrá considerar prestado el consentimiento en el contrato que pudiera haber sido firmado. Manifiesta que se podría pedir que asuma las responsabilidades del mismo, o alegar que existe un principio general en la firma electrónica sobre asunción de lo que se firma, pero insiste en que nunca se podrá considerar que efectivamente ha prestado el consentimiento.

En relación con las aplicaciones informáticas que requieren firmas, en los artículos 24.2 y 25.2. se define el dispositivo de creación/verificación de firma como un programa o sistema informático que sirve para aplicar los datos de creación/verificación de firma. Es sencillo deducir la importancia de controlar la seguridad del desarrollo del *software* de las Administraciones públicas en esta materia, viendo la enumeración de requerimientos que un código incorrectamente programado podría no cumplir, conforme al artículo 24.3.a) y d). Ese programa o sistema informático seguro de creación de firma debe garantizar que los datos

[477] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 92-93.

[478] Con una frecuencia mucho mayor de lo que cabría esperar inicialmente, se reciben llamadas solicitando modificaciones en el *software* por problemas a la hora de intentar firmar digitalmente una secretaria (el uso del femenino es intencionado, pues refleja la realidad observada) usando el certificado del alto cargo para el que trabaja. Tras la negativa a modificar las aplicaciones para que faciliten la suplantación (aunque sea consentida) y cuestionada dicha práctica, la explicación recibida siempre es una de estas dos: "*el directivo no tiene tiempo para firmar tanto documento*" o bien "*mi jefe no se lleva bien con los ordenadores*".

utilizados para la generación de dicha firma pueden producirse solo una vez, asegurando razonablemente su secreto[479], y que el dispositivo utilizado no altera los datos o el documento que deba firmarse, ni impide que este se muestre al firmante antes del proceso de firma[480].

De un modo análogo, a tenor del artículo 25.3, el programa o sistema informático seguro de verificación de firma debe garantizar que los datos utilizados para verificar dicha firma corresponden a los mostrados a la persona que la verifica, que esta verificación se realiza de forma fiable, que su resultado se presenta correctamente, que la persona que verifica la firma electrónica puede establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados, que se muestran correctamente tanto la identidad del firmante o su pseudónimo como el resultado de la verificación, y que se verifican de forma fiable la autenticidad y la validez del certificado electrónico correspondiente, pudiendo detectar cualquier cambio relativo a su seguridad.

El cumplimiento de todas esas garantías, imprescindibles para la validez de la firma electrónica, pasa por las manos del personal informático que desarrolla esas aplicaciones. La nueva LFE ha eliminado la presunción legal de su cumplimiento[481], a pesar de las dificultades que puede suponer su acreditación, prácticamente imposible en ocasiones. Dicha modificación, aunque de consecuencias incómodas, parece razonable dada la tendencia a la privatización de los

[479] Es fácil imaginar el mal uso que se podría dar a esos datos si se guardasen y reutilizasen o divulgasen sin conocimiento del interesado.
[480] Si la persona no puede ver lo que firma, este proceso constituiría un salto al vacío. De hecho, la creencia de que el programa no cambia internamente los datos utilizados para la firma o el propio documento a firmar ya constituye un acto de fe, puesto que el usuario no tiene la certeza de que ello sea así. El buen funcionamiento de la Administración electrónica requiere confianza, puede llamarse fe si se prefiere, en la creencia de que las Administraciones públicas utilizan un *software* seguro. Esa seguridad es la que queremos analizar en este trabajo.
[481] Antes contenida en el artículo 3.1 del real decreto ley 14/1999.

sistemas de certificación y el riesgo de dotar de los mismos efectos a sistemas públicos y privados[482]. La exposición de motivos de la ley vincula el "*mayor protagonismo a la participación del sector privado en los sistemas de certificación*" con la "*eliminación de las presunciones legales*". Esa desconfianza patente del legislador debe llevarnos también a cuestionar el masivo desplazamiento hacia el sector privado del desarrollo del *software* de las Administraciones públicas, un *software* al cual proporcionamos nuestro PIN sin saber, realmente, qué hace internamente con él, si lo almacena "para mejor ocasión", si lo usa para firmar el documento que nos muestra u otro diferente que no llegamos a ver, a modo de "cheque en blanco"…

Cabe destacar el artículo 28 de esta ley, referente al reconocimiento de la eficacia de los dispositivos seguros de creación de firma expedidos en otros Estados miembros, donde es posible reconocer la influencia de la constante búsqueda de la interoperabilidad y la defensa del mercado electrónico transfronterizo en la Unión, descrita *supra*, que también se refleja en el tenor del artículo 4.2. Esta ley, anterior al reglamento eIDAS, ya apuntaba en esa dirección, pero deberá ser actualizada a la normativa europea que acaba de entrar en vigor.

Resultó innovadora en su momento la consideración del DNI electrónico como certificado electrónico reconocido y, por ello, de uso equiparable a la firma manuscrita. De su normativa específica, el **real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica**[483], resulta poco conocido el artículo 1.4, que establece el diferente uso potencial del DNIe en

[482] BERROCAL LANZAROT, A.I. (2006), la firma electrónica, 440.
[483] Modificado por el real decreto 869/2013

función de la edad y de la capacidad de obrar. En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado, sin la posibilidad de firmar.

3.2.1.7. Otros desarrollos normativos

El completo marco legal y operativo descrito a nivel europeo y estatal se ha ido completando con el desarrollo de normas propias de las Administraciones autonómicas y locales, encaminado a cumplir o desarrollar las directrices normativas existentes, dando respuesta a los nuevos derechos y obligaciones en materia de Administración electrónica[484].

No se puede olvidar la influencia de la normativa de contratos sobre la Administración electrónica, habida cuenta del frecuente recurso a la externalización[485] del desarrollo del *software*. En todo contrato administrativo interviene, por definición, una parte privada, pero, a diferencia de lo que ocurre en los contratos entre particulares, presididos por la autonomía de la voluntad, dichos contratos administrativos están ligados al interés general y justifican ciertas prerrogativas de la Administración, con alcance aquilatado por la jurisprudencia y la legislación[486]. Esa normativa, que regula la contratación pública en aras a la consecución

[484] Ministerio de política territorial y Administración pública (2011). *Op. cit* p 7.
[485] La externalización viene a constituir una vía intermedia entre la prestación directa y la privatización, como señala Carles Ramió en su trabajo de 2009 titulado "Teoría y práctica del fenómeno de la externalización", en C. Ramió (Coord.), *La colaboración público-privada y la creación de valor público* (p. 57). Colección_Estudios. Serie Gobierno Local, 14. Diputación de Barcelona.
[486] MELIÁN GIL, J.L. (2013), prerrogativas de la Administración, 14-17.

efectiva, eficiente y libre de corrupción de la prestación demandada, tiene como punto de partida el Derecho comunitario[487].

La normativa sobre contratación pública de nuestro país tradicionalmente se ha visto sumida en un continuo proceso de cambio que origina cierta inseguridad jurídica[488], proceso aún inacabado. España debía incorporar a su ordenamiento jurídico el último paquete de directivas europeas sobre contratación en el plazo fijado a tal efecto, el 18 de abril de 2016, obligada en cuanto al logro del resultado final, no en cuanto a la forma o medios para alcanzarlo. Sin embargo, la trasposición no se logró, a pesar de que se iniciaron los trabajos preparativos incluso ante de la aprobación de dichas directivas, llegando a completar la elaboración de las nuevas leyes y su tramitación administrativa. La disolución de las Cortes generales en octubre de 2015 detuvo su tramitación parlamentaria[489], aún más retrasada por la repetición de las elecciones el 26 de junio de 2016. Conforme a la jurisprudencia del TJUE, expirado el plazo de transposición sin que se haya completado, los particulares podrán invocar ante nuestra jurisdicción nacional el efecto directo de aquellas disposiciones suficientemente claras y precisas que establezcan una obligación no sujeta a excepción o condición.

El proyecto de ley de contratos del sector público, PLCSP, viene a cumplir la obligación de transponer dos de las tres nuevas directivas, concretamente la directiva de concesiones y la de contratos.

---

[487] GIMENO FELIÚ, J.M. (2010), mecanismos de control, 519.
[488] GIMENO FELIÚ, J.M. (2010), mecanismos de control, 522.
[489] JUNTA CONSULTIVA DE CONTRATACIÓN ADMINISTRATIVA DEL ESTADO. Resolución de 16 de marzo de 2016.

3.2.2. Sus repercusiones sobre la ciudadanía en materia de protección de datos de carácter personal[490]

La interconexión de bases de datos públicas aporta comodidad al ciudadano, dado que se le ahorra la presentación de datos o documentos que ya estén a disposición de la Administración, pero ello se puede convertir en un perjuicio, por la posibilidad de que esa ingente cantidad de información de que disponen los organismos públicos se interconecte permitiendo no solo obtener perfiles, sino que llegue a sustituir el control de la propia información personal por un control de la Administración sobre los individuos[491].

El modo en que el *software* de la Administración lleve a la práctica el contenido de la normativa es decisivo para materializar el respeto del ordenamiento jurídico o bien forzarlo hasta que encaje con las conveniencias públicas[492].

Decididos a hacer realidad el derecho de los ciudadanos a no aportar datos y documentos que obren en poder de las Administraciones públicas, y sin duda inmersos en la idea de facilitar la generalización del uso de la eAdministración por el público en general, los poderes legislativo y ejecutivo avanzan al unísono en la dirección adecuada, dando los primeros pasos, con firmeza, hacia la implantación de una plataforma de intermediación de datos. Esa senda arranca con el real decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la AGE y de sus

[490] *Vid*. GIL DURÁN, M.P. (2016), derecho de control, 135-144.
[491] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 645-646.
[492] El siguiente caso real y la propuesta de una mejora técnica para solventar sus deficiencias han sido publicados en (2016) "El derecho de control de los datos personales en la plataforma de intermediación de la nueva eAdministración", *Revista de privacidad y Derecho digital* (5), 109-146.

organismos públicos vinculados o dependientes, habilitando un medio de verificación de los datos de identidad denominado SVDI[493] (sistema de verificación de datos de identidad) que entra en funcionamiento con la publicación de la orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al mismo en los procedimientos para cuya tramitación sea imprescindible acreditar, de modo fehaciente, datos personales incorporados a los documentos de identidad de los ciudadanos, debiendo contar con el consentimiento del interesado para la utilización concreta de dicho sistema.

El ciudadano que se acerca a las dependencias administrativas frecuentemente manifiesta su satisfacción por evitarle la molestia de aportar una fotocopia de su documento de identidad, lo que sustituye sin el menor esfuerzo por la plasmación de una cruz en la correspondiente casilla de autorización de la consulta telemática. El empleado público normalmente corrobora la complacencia, agradecido de no tener que recoger y almacenar más papel del estrictamente necesario. En ambos casos, la utilización del SVD ha sido masivamente aceptada por ciudadanos y empleados públicos como una mejora considerable en la tramitación de los procedimientos administrativos, a la luz de la comodidad y celeridad que la acompañaban.

Sin embargo, en la práctica diaria, el procedimiento es manifiestamente defectuoso, afirmación que realizo desde mi experiencia personal, íntimamente convencida de que no se trata de un caso puntual. El ciudadano se acerca a la ventanilla con una, o con unas cuantas, solicitudes ya rellenas, en las que aparece marcada la casilla de autorización de la

[493] Según cálculos de las instituciones europeas, esa supresión supondría el ahorro de unos 7 millones de horas anuales que los ciudadanos dedican a realizar trámites, como indicaba diez años atrás el MINHAP en su nota de prensa, recuperada de la *url* http://www.seap.minhap.es/web/prensa/actualidad/noticias/2006/04/2006_04_28.html (23 de enero de 2016).

consulta de los datos del documento de identidad, y el empleado público que presta servicio en la ventanilla recoge su solicitud, y todas las demás aunque sepa que no son de la persona allí presente, sin requerir en ningún momento su identificación para comprobar que quien ha marcado la casilla de autorización es verdaderamente el interesado. En la práctica diaria se está accediendo a datos personales de ciudadanos sin saber si ellos lo han autorizado realmente o no. Un papel con una cruz y una firma no comprobada, entregada por un desconocido en un mostrador de un organismo público no garantiza la validez jurídica de esa autorización. E, incluso así, se consulta. Debo manifestar por ello mi convencimiento de que el sistema se ha puesto en marcha con unas graves carencias de formación y concienciación del personal al servicio de las Administraciones públicas.

Si bien es cierto que el acceso a los datos identificativos de la persona sin su autorización real podría considerarse que adolece de repercusiones de importancia en la vida privada del afectado, en modo alguno puede defenderse la misma argumentación en el caso de la supresión de la exigencia de aportar el certificado de empadronamiento como documento probatorio del domicilio y residencia, implantada con la publicación simultánea del real decreto 523/2006. En esta ocasión, se sustituye el certificado por una consulta al sistema de verificación de datos de residencia, SVDR, donde se requiere igualmente el consentimiento del interesado. Este sistema entró en funcionamiento con la publicación de la orden PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al mismo.

A lo largo de diez años de trabajo, el SVD ha evolucionado de forma continuada, añadiendo nuevos cedentes de información. Los denominados “servicios intermediados” requieren la mediación de la plataforma del MINHAP, que ha de funcionar como un nodo de interoperabilidad, prestando servicios de interconexión técnica, organizativa y jurídica. Conocida como “plataforma de intermediación de datos”, hoy permite a las Administraciones públicas consultar y comprobar por medios electrónicos los datos de los ciudadanos obrantes en otras múltiples Administraciones, evitando que el interesado tenga que aportar los documentos acreditativos de los mismos.

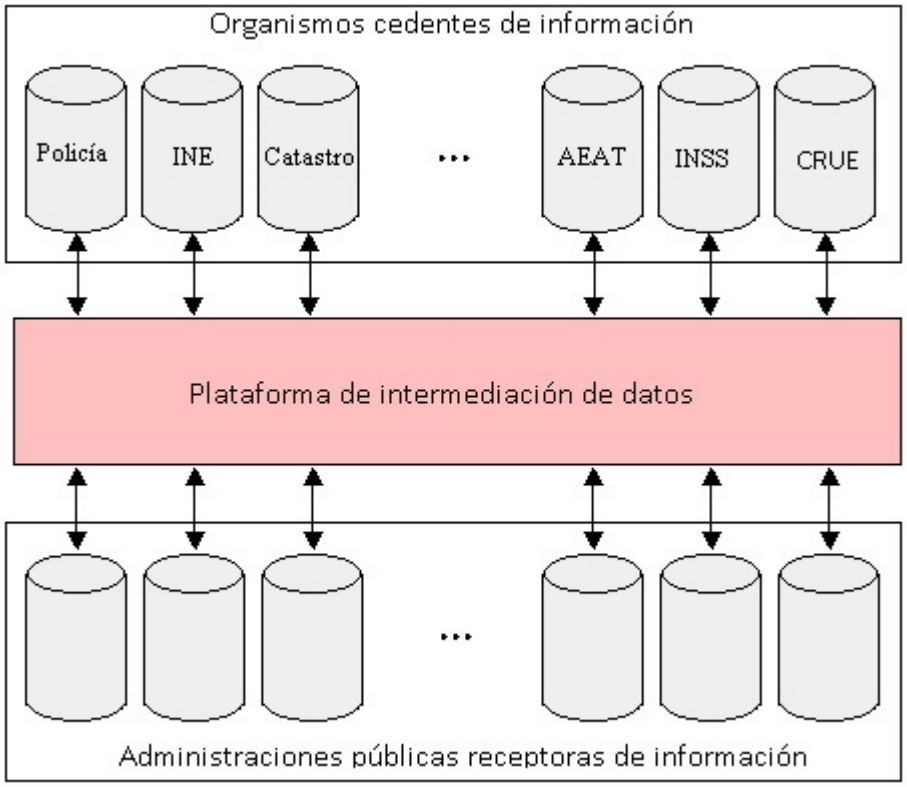

Figura 3: Modelo de intermediación

FUENTE: Elaboración propia basada en la comunicación sobre la Plataforma de intermediación de las jornadas sobre tecnologías de la información para la modernización de las Administraciones Públicas (Tecnimap) de 2010, adaptada al catálogo de SCSP de marzo de 2017.

En marzo de 2017, el catálogo de los "servicios intermediados" de verificación y consulta de datos SCSP incluye los siguientes:

- Consulta de datos de identidad, de la Dirección general de la policía.

- Verificación de datos de identidad, de la Dirección general de la policía.
- Consulta de datos de conductores, de la DGT.
- Consulta de datos de vehículos, de la DGT.
- Consulta y verificación de residencia con fecha de la última variación, del INE.
- Consulta y verificación de residencia con fecha de la última variación para finalidades distintas a la supresión del volante de empadronamiento, del INE.
- Verificación de datos de residencia (ámbito), del INE.
- Consulta de títulos no universitarios, por documentación o por datos de filiación, del Ministerio de educación.
- Consulta de títulos universitarios, por documentación o por datos de filiación, del Ministerio de educación.
- Consulta de la condición de estar becado, del Ministerio de educación.
- Consulta de datos catastrales, de la Dirección general del catastro.
- Consulta de certificación de titularidad, de la Dirección general del catastro.
- Consulta de bienes inmuebles, de la Dirección general del catastro.
- Obtención de descriptiva y gráfica, de la Dirección general del catastro.
- Obtención de documento CSV, de la Dirección general del catastro.
- Consulta de situación actual de desempleo, del SEPE.

- Consulta de importes actuales, del SEPE.
- Consulta de importes por periodo, del SEPE.
- Consulta de estar inscrito como demandante de empleo a fecha actual, del SEPE.
- Consulta de estar inscrito como demandante de empleo a fecha concreta, del SEPE.
- Estar al corriente de pago con la AEAT para contratos con las Administraciones públicas (con incumplimientos), de la AEAT.
- Estar al corriente de pago con la AEAT para autorización de licencias de transporte (con incumplimientos), de la AEAT.
- Estar al corriente de pago con la AEAT para subvenciones y ayudas (con incumplimientos), de la AEAT.
- Estar al corriente de pago con la AEAT para permisos de residencia y trabajo para extranjeros (con incumplimientos), de la AEAT.
- Estar al corriente de pago con la AEAT genérico (con incumplimientos), de la AEAT.
- Nivel de renta, de la AEAT.
- Consulta de estar al corriente de pago con la seguridad social, de la TGSS.
- Consulta de estar dado de alta en la seguridad social a fecha concreta, de la TGSS.
- Consulta del grado y del nivel de dependencia, del IMSERSO.

- Consulta de las prestaciones del registro de prestaciones sociales públicas, incapacidad temporal y maternidad, del INSS.
- Consulta de nacimiento, del Ministerio de Justicia.
- Consulta de matrimonio, del Ministerio de Justicia.
- Consulta de defunción, del Ministerio de Justicia.
- Consulta de inexistencia de antecedentes penales por datos de filiación, del Ministerio de Justicia.
- Consulta de inexistencia de antecedentes penales por delitos sexuales por datos de filiación, del Ministerio de Justicia.
- Consulta de inexistencia de antecedentes penales por documentación, del Ministerio de Justicia.
- Consulta de inexistencia de antecedentes penales de delitos sexuales por documentación, del Ministerio de Justicia.
- Consulta de entidades aseguradoras y reaseguros, de la DGSeg.
- Consulta de mediadores de seguros y corredores de reaseguros, de la DGSeg.
- Consulta de planes y fondos de pensiones, de la DGSeg.
- Consulta de datos de solvencia requeridos para participar en concursos públicos, de la DGSeg.

- Consulta de datos sobre el IAE, del Gobierno de Navarra.
- Consulta de datos sobre el IAE, del Gobierno del País Vasco.
- Consulta de datos de residencia legal, del MINHAP.
- Estar inscrito en el registro central de personal, del MINHAP.
- Comunicación del cambio de domicilio, del MINHAP.
- Consulta de firmas para legalización diplomática de documentos públicos extranjeros, del Ministerio de asuntos exteriores.
- Consulta de subsistencia de poderes notariales, del Consejo general del notariado.
- Consulta de copia simple de poderes notariales, del Consejo general del notariado.
- Consulta de notarios y notarías, del Consejo general del notariado.
- Consulta de subsistencia de administradores de una sociedad, del Consejo general del notariado.
- Certificado de afiliación, de MUFACE.
- Certificado individual de abonos, de MUFACE.
- Certificado de prestaciones de pago único recibidas, de MUFACE.
- Consulta de datos de afiliación, de MUFACE.
- Consulta de datos individual de abonos, de MUFACE.
- Consulta de datos de prestaciones de pago único recibidas, de MUFACE.

- Certificado de consulta de calificaciones para pruebas de conocimientos constitucionales, del Instituto Cervantes.
- Consulta de datos del fichero de titularidades financieras (por interviniente), de la Comisión de prevención de blanqueo de capitales.
- Consulta de datos del fichero de titularidades financieras (por producto), de la Comisión de prevención de blanqueo de capitales.
- Consulta de auditorías de consultas realizadas del fichero de titularidades financieras, de la Comisión de prevención de blanqueo de capitales.
- Consulta corriente de pago para ayudas, para Comunidades autónomas.
- Consulta corriente de pago para contrataciones, para Comunidades autónomas.
- Relación de Comunidades autónomas disponibles para corriente de pago.
- Relación de Comunidades autónomas disponibles para discapacidad.
- Relación de Comunidades autónomas disponibles para familia numerosa.
- Relación de Comunidades autónomas disponibles para permisos de explotación marisquera.
- Relación de universidades disponibles para datos de matrículas.

Esta plataforma de intermediación da respuesta a una necesidad ineludible, la de proporcionar un intercambio de información inmediato y sencillo entra las distintas Administraciones públicas de nuestro país. En 2015 se realizaron 53.596.776 de transmisiones de

datos en el sistema[494]. Su ámbito de aplicación potencial abarca más de 8.000 organismos de todas las Administraciones públicas, ya sea estatal, autonómica o local, y pone a su disposición datos de unos 38 millones de ciudadanos mayores de 18 años[495]. En 2014 se estima que llevó a ahorrar 180 millones de euros[496].

Las consultas a esos servicios se pueden realizar de dos modos diferentes:

- El primero consiste en el acceso por un empleado público autorizado mediante un cliente *web*, de modo que "*cuando conectamos con un servidor web desde nuestro navegador, el servidor nos devuelve la página web solicitada, que es un documento que se mostrará en el navegador para que lo visualice el usuario, pero es difícilmente entendible por una máquina. Podemos ver esto como web para humanos*"[497]. Es el empleado público el que consulta la información y la usa como considere.

- El segundo modo de acceso consiste en una consulta automatizada invocando *Web Services*, WS, desde la aplicación informática que gestione el trámite que requiere la aportación de esos datos, de una forma transparente para el ser humano. "*Los Servicios Web ofrecen*

[494] Boletín de indicadores del Observatorio de Administración electrónica de 29 de enero de 2016.
[495] Los datos que se comentan a continuación han sido obtenidos de la *web* de la Dirección general de fondos comunitarios y del Portal de Administración electrónica https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2015/Marzo/Noticia-2015-03-31-nota-tecnica-intermediacion-ccaa.html (10 de enero de 2016).
[496] Puede consultarse una estimación de ahorros e incremento de gastos por la implantación generalizada de la plataforma de intermediación de datos en las páginas 62 y ss. de la memoria de análisis de impacto normativo del anteproyecto de ley del procedimiento administrativo común de las Administraciones públicas, recuperada de http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_10/spl_101/pdfs/2.pdf (12 de febrero de 2016).
[497] UNIVERSIDAD DE ALICANTE. DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL. (2012-2013), servicios *Web* y *SOAP*, 4.

información con un formato estándar que puede ser entendido fácilmente por una aplicación. En este caso estaríamos ante una web para máquinas"[498].

Ya sea una aplicación informática o una persona física quien requiera la información, con anterioridad el responsable del órgano administrativo habrá tenido que solicitar el acceso a la plataforma de intermediación, aportando una autorización, debidamente justificada[499], para cada usuario y/o aplicación que pretendan obtener acceso al sistema. Una vez concedido el permiso, esa aplicación o ese empleado público podrán conectarse al sistema para consultar los datos de cuantos ciudadanos deseen, es decir, lo que se les autoriza es el uso de uno o varios servicios concretos (por ejemplo, el de identidad, residencia y discapacidad), no el acceso a los datos de una persona concreta.

En las Comunidades autónomas y en las Entidades locales, existirá un responsable que velará por las condiciones y normas de buen uso del servicio entre los usuarios de su Administración autorizados a acceder[500], sin perjuicio de que el control del cumplimiento de la normativa deba ser realizado por autoridades independientes. A ese respecto, la LOPD configura a la Agencia de protección de datos como ente de derecho público que actúa con plena independencia de las Administraciones públicas en el desempeño de sus funciones y otorga a los

[498] UNIVERSIDAD DE ALICANTE. DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL. (2012-2013), servicios *Web* y SOAP, 4.
[499] Si la necesidad de realizar la consulta se ampara en una norma legal, deberá reflejarse la norma habilitante y su finalidad en la solicitud de acceso al servicio.
[500] Información extraída del punto 5 (requisitos de confidencialidad) de las condiciones técnicas y funcionales del sistema de intermediación de datos entre Administraciones públicas, anexas al modelo de acuerdo temporal de prestación de servicios de Administración electrónica del MINHAP a los Ayuntamientos.

funcionarios que practican la inspección el carácter de autoridad pública en el ejercicio de sus funciones[501].

El cesionario indica los datos de identificación de la persona concreta a consultar. Si es suficiente para identificar de forma única al ciudadano, a través de la plataforma de intermediación del MINHAP, el cedente le proporciona los datos pertinentes.

Para realizar la consulta concreta de los datos de una determinada persona mediante este sistema, será preciso contar con su consentimiento previo, fehaciente e informado, salvo que una norma de rango de ley lo autorice. El ciudadano, antes de consentir, debe ser conocedor no solo de que se va a acceder a sus datos personales, sino también de que tal acceso se materializará mediante el uso de la plataforma de intermediación.

A tenor del artículo 3.h) de la LOPD, se entiende por consentimiento "*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*". Especifica su artículo 6 la necesidad de consentimiento inequívoco para el tratamiento, salvo que la ley disponga otra cosa. Hemos de recalcar la palabra "informada" y traer a colación el artículo 5 que, bajo la rúbrica de "derecho de información en la recogida de datos" impone la obligación de suministrar una información previa, expresa e inequívoca de la existencia del fichero o tratamiento y, también, de los destinatarios de la información.

[501] En la relación de puestos de trabajo de la Agencia española de protección de datos, figuran 11 puestos de inspector/a de datos, 23 de inspector/a instructor/a y 9 de subinspector/subinspectora de datos. Incluso si se dedicaran únicamente a inspeccionar las transmisiones de datos entre Administraciones públicas, no parece una plantilla suficiente para controlar la licitud de 40.000.000 de consultas de datos personales anuales, cifra que no dudamos que se haya sobrepasado en 2015 y que, previsiblemente, irá aumentando de forma espectacular en los años venideros

Técnicamente, el sistema no comprueba si existe ese consentimiento, por lo que la plataforma de intermediación pone datos de millones de ciudadanos al alcance de miles de empleados públicos que no tienen, y la inmensa mayoría no tendrán jamás, ningún interés legítimo en ellos. Como garantía jurídica, el sistema de intermediación dispone de un módulo de auditoría donde quedan registradas todas las consultas realizadas, incluyendo la identidad del solicitante y la fecha. A esa información de auditoría solo puede acceder el personal de la Administración debidamente autorizado y acreditado.

Resulta cuestionable el cumplimiento del principio de seguridad del artículo 9 de la LOPD. No parece que un acceso generalizado a los datos de los ciudadanos por parte de los empleados públicos concuerde con lo que se entiende por "*adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su (…) tratamiento o acceso no autorizado (…)*". Al menos se echa en falta la adecuada formación y concienciación de los empleados públicos orientada a evitar el posible uso ilegítimo del sistema, el acceso no autorizado a datos de carácter personal. El conocimiento de la problemática, de las posibles repercusiones en la esfera individual de los afectados y de la normativa en materia de protección de datos personales es, diez años después, aún una tarea pendiente y de tal importancia que los cursos deberían ser obligatorios, igual que lo son los de prevención de riesgos laborales.

El mismo concepto de uso ilegítimo es el que aplica la Junta de Andalucía en su página *web*, refiriéndose a SCSP, cuando afirma que "*se considerará como uso irregular o indebido la consulta de datos relativa a interesados concretos cuyas solicitudes o expedientes no*

se encuentren tramitándose en los procedimientos, trámites o servicios autorizados o de aquellos sobre los que no conste su consentimiento expreso"[502]. Y, en la misma línea, Troncoso nos recuerda que "*los accesos indebidos no provienen únicamente de terceras personas ajenas a la organización sino también de empleados de la propia Administración pública*"[503].

La plataforma de intermediación permite que el empleado público autorizado a usar un determinado servicio (por ejemplo, el servicio de consulta de grado y nivel de dependencia) pueda acceder no solo a la información del ciudadano cuya solicitud tiene ante sí y que ha autorizado dicha consulta, sino también a los datos de cualquier otra persona, quien no solamente no ha prestado su consentimiento sino que, además, no sospecha de que la información sobre su domicilio o grado y nivel de dependencia está siendo vista por alguien. Esa carencia de información deja inermes a los ciudadanos, quienes desconocen qué Administraciones públicas pueden almacenar datos sobres sus personas. En esas condiciones, "*menos aún pueden conocer y prevenir o perseguir el uso desviado o la diseminación indebida de tales datos, incluso aunque le causen lesiones en sus derechos o intereses legítimos*"[504].

Los datos de más de 38.000.000 de ciudadanos están expuestos ante miles de empleados públicos que puede acceder a ellos por los más variados motivos imaginables: curiosidad malsana, relajación de las más elementales normas de seguridad (bloquear los equipos

[502] Página *web* de la Junta de Andalucía, https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/supresiondecertificadosensoportepapel (16 de enero de 2016).
[503] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 682.
[504] Fragmento extraído del FJ 4º de la STC 254/1993, donde el Máximo Intérprete de la Constitución alerta de los peligros del uso incontrolado de los datos de carácter personal y de la carencia de información suficiente. Esta sentencia fue pionera en esgrimir el artículo 18.4 de nuestra Norma fundamental, al resolver un recurso de amparo en el que dicho Tribunal debió determinar si el Convenio del Consejo de Europa sobre protección de datos personales surte efecto directo o interpretativo.

cuando se va a ausentar, custodiar adecuadamente las contraseñas, orientar los monitores de forma que no sean vistos por terceras personas…), manipulación (como la falsificación de una firma en una solicitud que presenta alguien que dice haberse olvidado el DNI y autoriza la consulta de sus datos de identidad), sobornos (la información es poder y el poder se paga bien), extorsión (como el caso del maltratador que busca a su pareja huida y no se detendrá hasta localizarla, utilizando cualquier opción a su alcance)…

Incluso ocurre con buena intención, en un exceso de diligencia, cuando el empleado público se ofrece amablemente a mirar los datos en el ordenador cuando el ciudadano ha olvidado traer su DNI, sin pensar que si esa persona no es quien ha dicho ser, está accediendo a datos personales sin el permiso del interesado. Otro caso real es el de un ciudadano que se persona y entrega en una oficina pública una solicitud propia y otra de su pareja, firmadas de forma manuscrita. Sin pedir ningún documento acreditativo (porque ambos han marcado la casilla indicando que autorizan la consulta electrónica), recaban sus datos de identidad y de residencia por ordenador a través del sistema de verificación y consulta de datos. Si ya es indebido hacerlo con la persona que está allí presente sin pedir su identificación[505], con la teoría de que si se la piden, ¿para qué necesitan acceder a datos que ya están en el DNI?, peor es que además accedan a los datos de la pareja, delante del individuo y permitiendo que los vea… Perfectamente podría haber averiguado así dónde vive un perseguido por un grupo terrorista o

[505] Recordemos de nuevo que el Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes afecta exclusivamente a la exigencia de aportar fotocopia del DNI y no a la obligación de identificación de quien comparece ante la Administración pública. Puede resultar aparentemente incoherente, pero es preciso que el interesado enseñe el DNI original al empleado público, antes de que este pueda acceder al servicio de verificación de datos de identidad.

una víctima de violencia de género, que huyen y se ocultan escondiéndose de sus perseguidores. Se trata de un supuesto que, desgraciadamente, se da en la realidad; el cambio del lugar de trabajo y residencia huyendo de un perseguidor es un caso real contemplado, por ejemplo, en el artículo 82 del TREBEP, que permite la movilidad de por razón de violencia de género o por violencia terrorista, para hacer efectivo el derecho de la víctima a la protección real y efectiva.

Permitir ese libre acceso confiando únicamente en que el empleado público consultará solo datos de ciudadanos que hayan consentido, es una acción peligrosa conforme a los conceptos básicos del Derecho penal[506], donde el juicio de peligro coincide con un juicio de previsibilidad objetiva *ex ante*, realizado por una persona inteligente, colocada en la posición del autor, en el momento del comienzo de la acción y teniendo en cuenta todas las circunstancias del caso concreto cognoscibles por la persona inteligente, más las conocidas por el autor (saber ontológico) y la experiencia común de la época sobre los cursos causales (saber nomológico). Si la producción del resultado aparece como no absolutamente improbable, la acción es peligrosa.

Los autores y responsables de una plataforma de intermediación reconocida con el premio al servicio público de la ONU[507] en 2014, entre otros[508], sin duda cumplen el estándar de personas inteligentes. Sobre las circunstancias conocidas por su autor no podemos pronunciarnos pero bastaría unas pocas visitas a las oficinas públicas para observar a cuántos ciudadanos que

[506] CEREZO MIR, J. (2002), peligro abstracto, 49.
[507] La noticia se ha publicado en el Portal de Administración electrónica, http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2014/Mayo/Noticia-CTT-2014-05-28-SVD-UNPSA-2014.html#.Vxf3sUdWgSk (20 de abril de 2016).
[508] En el informe del OBSAE que lleva por título "La visión de nuestra Administración electrónica fuera de España", fechado en abril de 2014, se publicita la plataforma de intermediación de datos como referente de buenas prácticas galardonada por el Instituto europeo de Administración pública, EIPA, con un certificado de mejor práctica en la categoría nacional en los premios europeos del sector público, EPSA, añadiendo que, además, es un referente para el programa ISA.

presentan solicitudes que incluyen la marca de autorización no se les exige identificarse con el original del documento de identidad, a pesar que el propio código penal castiga en sus artículos 197 y 198, entre otros casos, al empleado público que "*sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*".

Por tanto, habida cuenta de que, *ex ante*, no es absolutamente improbable que alguien acceda a los datos sin el consentimiento del interesado, el peligro es una cualidad inherente a la acción y ha de concluirse que dejar ese libre acceso a miles de personas es peligroso. No debemos cometer el error de olvidar la naturaleza del ser humano: accederá a esa información porque no hay nada que se lo impida. Expresado en palabras de la periodista Rebecca MacKinnon, "*la cuestión fundamental de la democracia es que el poder, cuando no tiene obstáculos, puede conducir a abusos por parte de cualquier persona o grupo de personas con la oportunidad para ejercerlo*"[509]. Por ello, es preciso eliminar la posibilidad.

El documento sobre la Administración en línea, adoptado el 8 de mayo de 2003 por el denominado "grupo de trabajo sobre protección de datos del artículo 29", expone que la autoridad de protección de datos española consideró, en su momento, que el proyecto de reglamento para la promoción de la Administración en línea cumplía los requisitos de la

[509] MACKINNON, R. (2012), libertad en Internet, 34.

normativa de protección de datos de carácter personal, al exigir el consentimiento de los afectados previamente a la transferencia electrónica de los datos entre Administraciones, promulgándose así el real decreto 209/2003[510], de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos. Sin discrepar de esta decisión, no comparto el funcionamiento de la plataforma al permitir la posibilidad real y efectiva de accesos no consentidos.

El mismo documento recoge la postura del Reino Unido, quien publicó en 2002 un informe titulado «*Privacy and data sharing: the way forward for public services*» donde presenta la interconexión como algo aparentemente promovido por el desarrollo de la Administración en línea y las perspectivas de los ciudadanos en este ámbito, pero insistiendo en la necesidad igualmente importante de sus expectativas en cuanto a la protección de la vida privada y considerando, por tanto, la conveniencia de equilibrar las interconexiones (y la supuesta mejora que conllevan en los servicios de la Administración) y la protección de los usuarios en relación con el tratamiento de sus datos personales. Indica también que la búsqueda

[510] Añade algunos artículos al real decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la AGE. Entre los artículos adicionados podemos destacar el 13 que, bajo la rúbrica de "*Sustitución de certificados en soporte papel*", permitía su remplazo por certificados telemáticos o por transmisiones de datos siempre que el interesado lo autorizara o una norma de rango legal lo dispusiera, con estricta sujeción a lo dispuesto en la normativa de protección de datos. En la misma línea el artículo 15 hace referencia a las transmisiones de datos.
El real decreto 263/1996 ha sido derogado por el real decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Este dedica su artículo 2 a las transmisiones de datos y documentos entre órganos y organismos de la AGE con ocasión del ejercicio reconocido por el artículo 6.2.b) de la LAE. En él, se remite a los esquemas nacionales de interoperabilidad y de seguridad. A su vez, se establece la obligación de informar al ciudadano expresamente de que el ejercicio del derecho a no aportar datos o documentos que obren en poder de las Administraciones públicas implica el consentimiento, revocable, para que sean recabados. Indica también que el derecho se ejercitará de forma específica e individualizada para cada procedimiento concreto.

de este equilibrio pasaría, obligatoriamente, por analizar las ventajas que se espera obtener con la interconexión, la posible existencia de algún enfoque alternativo que permita alcanzar el mismo objetivo, los riesgos y costes de la interconexión y las garantías que se podrían precisar para gestionar esos riesgos.

El "grupo de trabajo sobre protección de datos del artículo 29", con respecto al control del usuario de sus datos personales, recoge la postura de países como España o Irlanda, en los que las autoridades de protección de datos consideran que los ciudadanos deben poder mantener bajo control sus datos personales en todas las fases del procedimiento administrativo, que deben ser informados de los intercambios y que estos pueden requerir su consentimiento. Sin embargo, la autoridad irlandesa recomienda que se dé a los ciudadanos una oportunidad de consentir su inclusión en el nuevo sistema y que se les informe acerca de los fines y usos de la base de datos central, oportunidad que no se nos ha otorgado en España, puesto que nuestros datos están, sin nuestra autorización, disponibles en el sistema de intermediación para los usuarios que deseen apropiarse de ellos. Nuestro consentimiento a la recogida y tratamiento de los datos personales que existen hoy en día en las distintas bases de datos de la Administración pública no implica en modo alguno el consentimiento a su cesión[511] ni a ser incluidos en un sistema de interconexión que pone a disposición de miles de empleados públicos nuestra información, por si acaso en alguna ocasión decidimos reutilizarla. Más de 38.000.000 de ciudadanos estamos en él, nos guste o no, lo que nos lleva a preguntarnos si no se está

[511] FJ 13º de la STC 292/2000 de 30 de noviembre de 2000, que resuelve el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

incumpliendo el derecho de "(…) *oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención*"[512].

Analizándolo, la primera cuestión a plantearse es si este sistema de interconexión es, todo él en su conjunto, un fichero. Acudiendo a la definición jurídica que contempla la normativa de protección de datos de carácter personal, de conformidad con el artículo 3.b) de la LOPD un fichero es "*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*". Luego es posible concluir que el sistema de intermediación de datos se trata de un fichero, jurídicamente hablando. Por tanto, si nuestros datos están en este fichero, en este sistema de interconexión, sin nuestro consentimiento, nuestros derechos han sido incumplidos, salvo que consideremos que existe una habilitación legal implícita, en cuyo caso entraría en juego el artículo 34.a) del reglamento de desarrollo de la LOPD, conforme al cual el afectado tiene derecho a que no se lleve a cabo el tratamiento de sus datos de carácter personal como consecuencia de la concurrencia de un motivo legítimo y fundado[513], referido a su concreta situación personal, derecho que el actual diseño de la plataforma no parece otorgarnos.

Conviene recordar la meritoria aclaración del concepto de cesión aportada por Troncoso Reigada, para quien la revelación de datos personales a terceros es una cesión o

[512] FJ 5º de la STC 292/2000 de 30 de noviembre de 2000.

[513] Podría ser el caso real de la funcionaria víctima de violencia de género que, sabiendo que su exmarido saldrá de la cárcel dentro de seis meses e inmediatamente volverá a intentar matarla, huye sin dejar rastro, trasladándose a trabajar al otro extremo del país gracias a la movilidad que le ofrece el artículo 82 del texto refundido del Estatuto básico del empleado público. Lo último que desearía esta mujer es que su nueva residencia esté accesible para los ojos de miles de personas. Y, lo peor, es que ella no se enterará de que su nueva dirección ha sido consultada hasta que se encuentre frente a frente e indefensa con su agresor. De poco le valdrá a ella, en ese caso, que la persona que consultó sus datos sea sancionada con posterioridad.

comunicación, cualquiera que sea la forma de poner a disposición esos datos, incluyendo la interconexión, la consulta o la publicación. Señala específicamente que no es preciso que el cesionario esté identificado y tampoco que lleve a cabo un tratamiento posterior, como es la recogida, grabación o conservación de la información, aclarando que ello permite considerar como cesión la publicación de información personal en Internet. *"Bastaría que potencialmente los cesionarios pudieran llevar a cabo distintos tratamientos de información personal –recogida, grabación, conservación, interconexión, transferencias –, aunque no lo lleven a cabo finalmente*."[514]

Coincido en la apreciación de que el cedente ha consumado la cesión de datos en el momento en que los pone a disposición de un tercero, con independencia de que dicho tercero los consulte o no. Y la plataforma de intermediación posibilita precisamente eso, que los datos personales de más de 38.000.000 de ciudadanos sean puestos a disposición de miles de empleados públicos, accedan a ellos o finalmente no lo hagan, materialicen o no la recogida. El protocolo de sustitución de certificados en soporte papel, SCSP, tal y como está ideada la plataforma de intermediación, parece incumplir la normativa de protección de datos personales ya desde el principio, por su propio diseño, fundamentado en la libre disponibilidad de los datos para quien tenga acceso al servicio y quiera recogerlos. La existencia de una norma que impide acceder a ellos sin consentimiento no impide que, en la realidad, se acceda a ellos sin consentimiento. Debemos recordar que no basta con eso, que el artículo 9 de la LOPD obliga a "*adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad*

[514] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 500-501.

de los datos de carácter personal y eviten su (…) *tratamiento o acceso no autorizado* (…)", no solo las organizativas, también las técnicas.

Señala Valero Torrijos que, por la intensificación de los intercambios de información, será necesario contemplar conceptos como la interoperabilidad, no solo desde la perspectiva técnica y organizativa, sino que habrán de reforzarse desde el prisma jurídico. En particular, especifica que los niveles de protección que ofrece el Derecho han de proyectarse en el diseño de las aplicaciones y el funcionamiento de los sistemas de información[515]. El Derecho ofrece unos niveles de protección, en principio, suficientes. Ahora corresponde proyectarlo en el diseño de la plataforma.

La propuesta técnica que planteo como alternativa es sencilla tecnológica y funcionalmente. Se basa en el presupuesto de que el ciudadano es el dueño de los datos, algo que contradice el enfoque del que partió la plataforma en sus inicios, filosofía reflejada en varios documentos enviados al Tecnimap de 2010[516], disponibles en el portal de Administración electrónica PAe, donde podemos comprobar que se considera dueño de los datos al organismo que los custodia[517]:

- "*Para los casos donde sea indispensable la fehaciente justificación de dichos datos, estos documentos se sustituyen por una consulta a la Plataforma de Intermediación, que obtendrá dichos datos de los "**dueños y custodios** de los mismos", como por*

[515] VALERO TORRIJOS, J. (2014), de la digitalización a la innovación tecnológica, 125.
[516] Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_lineas_ccoperacion/_pae_Tecnimap/pae_TECNIMAP_2010_Zaragoza/pae_COM_2010-Eficiencia_y_sostenibilidad.html#.VxkRCEdWgSk (21 de abril de 2016).
[517] La negrita es nuestra.

ejemplo la Dirección General de la Policía en el caso de la Información de Identidad (…)".

- "*Para constatar la veracidad de los datos, el sistema se comunica con los "**dueños/custodios**" de los datos* (…)".
- "*Recepción de la respuesta generada por el **Organismo dueño de los datos*** (…)".

Sin embargo, hoy día parece pacífica la afirmación de que el verdadero dueño de los datos personales es la propia persona afectada. Aparentemente, los responsables de la plataforma de intermediación no han tomado conciencia de que los datos no son de los cedentes, ellos solo son los custodios, por lo que en el modelo de intermediación está ausente la figura del verdadero propietario de la información, el ciudadano. Afirma Troncoso Reigada que "(…) *la declaración de los ficheros facilita que el responsable tome conciencia de que esa información no le pertenece, sino que corresponde a las personas, auténticas dueñas de sus datos personales*"[518]. En la misma línea, la comisaria europea de Justicia, Vera Jourova, valedora de una nueva legislación europea de protección de datos, afirma que "*Nuestros datos son nuestra identidad y debemos ser dueños de ella*"[519].

Pérez Velasco planteó, hace ya una década, el uso de cuentas administrativas personalizadas como solución técnica y organizativa a analizar, proponiendo diferentes escenarios, como el de "*una especie de caja fuerte virtual que contiene los datos personales de los usuarios y que está ubicada en un portal de la Administración, pero en una zona neutra e*

[518] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 297.
[519] Recuperado de http://internacional.elpais.com/internacional/2015/12/16/actualidad/1450284367_569200.html (16 de enero de 2016).

inaccesible para esta" donde el usuario podría facilitar la transferencia de los mismos de una administración a otra, pudiendo llegar a estar incluso "*bajo el control directo del usuario, en forma de una tarjeta, o sobre su ordenador*", o emular lo que en Francia se denomina "la casa del servicio público virtual", donde el usuario efectúa puntualmente mandatos precisos como recoger y facilitar ciertas informaciones, realizar transacciones o ejecutar órdenes[520].

La propuesta técnica que planteo para dar cumplimiento al artículo 9 de la LOPD precitado se basa en la misma filosofía y aprovecha la plataforma actual, pero parte de premisa de que el dueño de los datos es el ciudadano y, por ello, debemos permitir que los guarde "bajo llave".

Únicamente se requiere crear un fichero de lo que se podrían denominar "interruptores". Cada ciudadano podría conectarse a una página *web* de la Administración con su DNIe o certificado electrónico y, simplemente, escoger ON/OFF para abrir o cerrar la puerta por la que entran y salen sus datos, del mismo modo que cerrando la llave de paso del suministro que hay en la entrada de su casa es capaz de cortar el agua en toda su vivienda, en previsión de posibles fugas. Con la llave cerrada no hay agua en toda la casa, no se accede a sus datos por ningún empleado público a través de ninguno de los servicios de consulta existentes. Cuando desee permitir el acceso, vuelve a ponerlo a ON.

[520] PÉREZ VELASCO, M.M. (2006), intercambio de datos, 50-51.

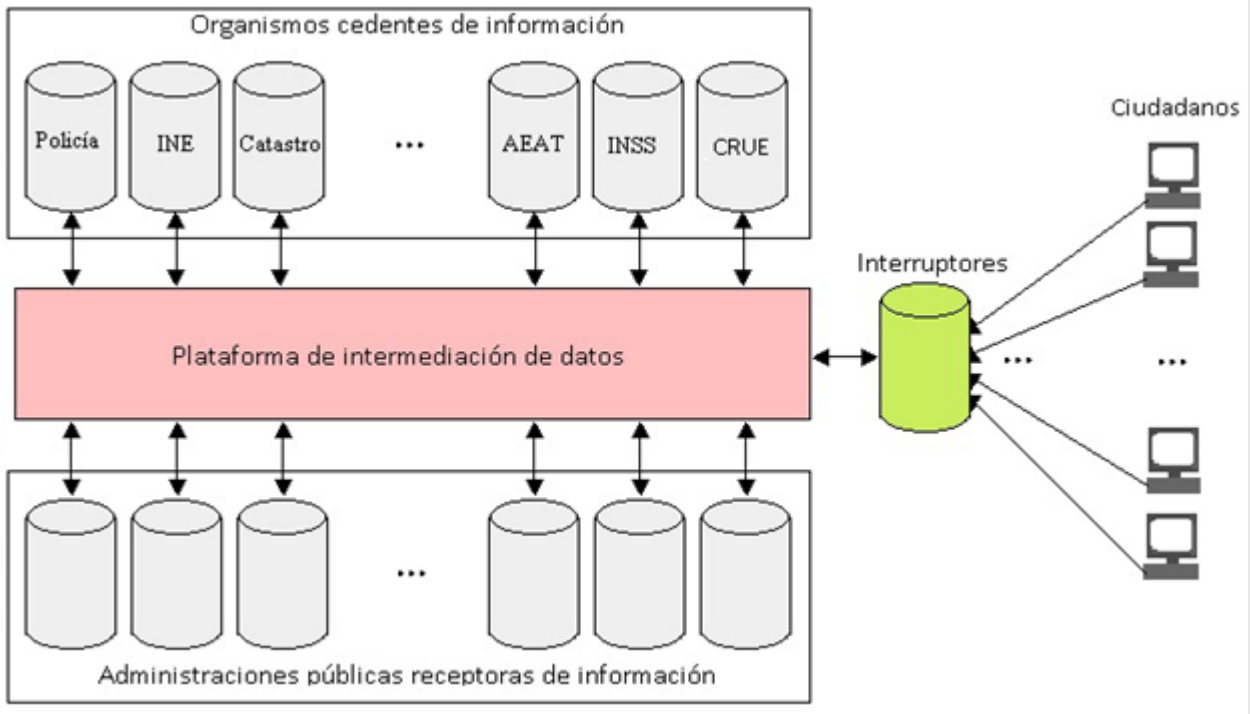

Figura 4: Modelo de intermediación propuesto

FUENTE: elaboración propia.

Ahora que, con origen en el artículo 8 de la Carta de derechos fundamentales de la Unión Europea, todas las políticas de la Unión se orientan a la protección de los datos de carácter personal frente a la utilización de los sistemas informáticos, es el momento de adelantarnos e incluir en este esquema al verdadero dueño del dato y materializar su derecho al control y disposición que la jurisprudencia reconoció hace ya casi un cuarto de siglo, en el FJ 7º de la STC 254/1993, al aseverar que "(…) *la garantía de la intimidad adopta hoy un contenido positivo en*

forma de derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático[521] *(habeas data*[522]*)*".

SCSP y la plataforma de intermediación de datos, en su configuración actual, no ofrecen las debidas garantías, puesto que no previenen los accesos indebidos, aspecto de vital importancia al que podemos aplicar el FJ 6º de la STC 292/2000, en el que el Máximo Intérprete de la Constitución se refiere al poder de disposición garantizado por el derecho a la protección de datos: "*Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información*". La plataforma actúa como fuente de información sin las debidas garantías y no previene el riesgo de acceso indebido.

Tampoco parece ajustarse al tenor del artículo 9.2 de la LAE (trasladado al 155.2 de la ley 40/2015) en el que regula las transmisiones de datos entre Administraciones públicas y establece que "*la disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones* (…)". Se entiende por

[521] La expresión "datos insertos en un programa informático" fue muy poco afortunada y se ha transmitido así hasta la actualidad. Podría entenderse tal referencia en el viejo siglo XX, cuando no era extraño encontrar datos incrustados dentro del código fuente de los programas pero, en la actualidad, tal conducta debe rechazarse como una muy mala práctica de programación. Por ello, debemos interpretar la precitada expresión "programa informático" como equivalente a fichero, archivo, banco de datos electrónico, almacén de datos, *data warehouse* o a cualquiera de sus sinónimos.

[522] La denominación de este derecho aún no parece decidida, habiendo sido bautizada como *habeas data*, derecho a la autodeterminación informativa, derecho a la protección de datos, libertad informática o derecho a la garantía de la privacidad. Como señaló DE LA QUADRA-SALCEDO en la jornada de celebración, por la Agencia española de protección de datos, de los 20 años de protección de datos en España, "*me parece que no hemos encontrado todavía el nomen iuris que le cuadre*".

disponibilidad la disposición de los servicios a ser usados cuando sea necesario[523], considerando que se da una carencia de la misma cuando se produce una interrupción del servicio. Otra definición de la disponibilidad es la de propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren[524]. ¿Puede decirse que SCSP, SVD o la plataforma limitan la disponibilidad a los datos requeridos? En absoluto. Con SCSP, a través de la plataforma, la disponibilidad es de 24 x 7 [525], salvo interrupciones en su funcionamiento que pudieran producirse ocasionalmente. Y pone a disposición de los cesionarios autorizados todos nuestros datos, todos los días, todas las horas del día. SCSP no tiene en la menor consideración el hecho de que ninguna Administración requiera o no nuestros datos de grado o nivel de dependencia, por ejemplo, porque no hayamos solicitado nada relacionado con ello, le da igual, ahí están nuestros datos de dependencia para que cualquier empleado público con acceso al servicio de consulta correspondiente pueda verlos si, por el motivo que sea, decide consultarlos.

No debemos confundir ceder con acceder. Se cede aunque no se acceda. Mantenemos, por tanto, que la cesión de nuestros datos se ha realizado en el mismo momento en que un empleado público es autorizado a usar un servicio de consulta, con independencia de que, de forma efectiva, descargue o no nuestra información. Pero, incluso admitiendo que no fuera así y que la cesión no se tuviese por realizada hasta que el tercero lee la información, el ciudadano

[523] MAGERIT 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, libro 1, 9. No hemos escogido MAGERIT para aclarar el concepto de disponibilidad por azar, sino porque su uso está específicamente recomendado en las órdenes PRE/3949/2006 y PRE/4008/2006 por las que se establece la configuración, características, requisitos y procedimientos de acceso al sistema de verificación de datos de identidad y de residencia.
[524] MAGERIT 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, libro 2, 15.
[525] 24 horas diarias durante los 7 días de la semana.

siempre tiene derecho a ser informado de la cesión. Sin embargo, la misma no se le notifica. Desconocemos cuáles y cuántos de nuestros datos han sido accedidos a través de la plataforma. Y, sin saberlo, es imposible ejercer el derecho a oponerse a su posesión y a su uso.

Con respecto al módulo de auditorías integrado en la plataforma de intermediación, al que únicamente puede acceder determinado personal de las Administraciones públicas, debemos manifestar que nos parece insuficiente. Incluso suponiendo que en cada Comunidad autónoma o cada Entidad local se habilite a un empleado público para realizar la oportunas comprobaciones, estamos dejando el control de la existencia de consentimiento fehaciente en manos de la propia Administración pública. Incluso contando con la colaboración, dedicándose en exclusiva (exclusividad que obligaría a abandonar el resto de sus tareas), de los inspectores y subinspectores de la Agencia española de protección de datos[526] (45 según recoge su RPT[527]) y de sus homólogas autonómicas, es imposible comprobar siquiera un porcentaje aceptable de los millones de transferencias realizadas, con la dificultad añadida de que la supresión de la presentación de la fotocopia del DNI impide comprobar la autenticidad de la firma manuscrita que pueda constar en el consentimiento.

La filosofía de la plataforma de intermediación se orienta no a prevenir el riesgo, sino a sancionar el acceso indebido, pero los mecanismos preventivos de ese acceso indebido son inexistentes y los instrumentos reactivos son ineficaces; no resulta suficiente que en las escasas ocasiones en que se revisa el motivo de un empleado público para acceder a un determinado

[526] Sin entrar a analizar las dudas que se plantean sobre la independencia real y efectiva de la Agencia española de protección de datos, me limitaré a admitirla sin cuestionarla.
[527] Recuperado de http://www.agpd.es/portalwebAGPD/LaAgencia/rrhh/common/retribuciones/RPT_2016.pdf (4 de abril de 2017).

dato, la presentación de un documento con la casilla de autorización marcada constituya justificación bastante, sin requerir la comprobación de la autenticidad de la firma o la ratificación del consentimiento por el ciudadano. Rudolf von Ihering nos recuerda por qué la Justicia sostiene en una mano la balanza y en la otra una espada con la que hacer efectivo el Derecho. "*La espada, sin balanza, es la fuerza bruta, y la balanza sin la espada, es el derecho en su impotencia; se complementan recíprocamente; y el derecho no reina verdaderamente, más que en el caso en que la fuerza desplegada por la justicia para sostener la espada, iguale a la habilidad que emplea en manejar la balanza*"[528].

Analizados los anteriores aspectos, solo cabe recordar la aseveración jurisprudencial[529], a cuyo tenor, al privar a la persona de las facultades de disposición y control sobre sus datos personales, se le priva también de su derecho fundamental a la protección de datos, teniendo en cuenta que "*se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección*"[530].

Como reclamaba el informe "*Privacy and data sharing: the way forward for public services"* del Reino Unido citado anteriormente, habría que analizar la existencia de algún enfoque alternativo que permita alcanzar el mismo objetivo. La postura de la autoridad de protección de datos irlandesa recomendando dar a los ciudadanos la oportunidad de consentir su inclusión en el nuevo sistema nos parece adecuada, aunque con variaciones.

[528] RUDOLF VON IHERING, la lucha por el derecho.
[529] STC 292/2000 de 30de noviembre de 2000, FJ 10º.
[530] STC 11/1981 de 8 de abril, FJ 8º.

Para que la sociedad sea consciente de la existencia de la plataforma y la posibilidad de abrir y cerrar la llave de paso, el interruptor, será imprescindible informar adecuadamente a los ciudadanos[531]. Como recomienda la autoridad irlandesa, "*dicha información ha de ser lo suficientemente precisa como para que las personas puedan entender realmente los riesgos potenciales que conlleva la transmisión de sus datos y las consecuencias que ésta podría inducir. Sin tal información, el consentimiento personal sería ilusorio, pues no habría ninguna razón justificada para rechazar la comunicación de los datos frente al argumento de la simplificación de los procedimientos administrativos*"[532]. Actualmente, no hemos encontrado ninguna información sobre la plataforma, SCSP o SVD, que advierta que los datos del ciudadano los pueden ver miles de empleados públicos y/o aplicaciones sin que la persona afectada llegue a enterarse.

Esta propuesta admite una mejora que aumenta levemente la complejidad y notablemente la usabilidad. Consiste en colocar un interruptor para cada uno de los servicios existentes o que puedan llegar a existir. Continuando con nuestro símil, ahora estaríamos refiriéndonos a situar una llave de corte de agua en cada aseo o cuarto de baño y en la cocina. Si se quiere prevenir una posible fuga, no hace falta cortar el agua de toda la casa; basta con cerrar la llave allá donde consideremos conveniente. Por ejemplo, podría tener activas (ON) las consultas de datos de identidad de la Dirección general de la policía, de títulos universitarios del

[531] En la noticia sobre el intercambio de datos entre Administraciones públicas publicada en el Portal de Administración electrónica, consultada el 23 de enero de 2016, no se encuentra mención alguna en relación a los riesgos potenciales. Puede leerse la misma en la url https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2013/Marzo/pae_Noticia_2013-03-04_Nota_tecnica_marzo_2013.html#.V6zVga02tsk

[532] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2003), documento de trabajo, 17.

Ministerio de educación y de matrimonio del Ministerio de Justicia, y desactivadas (OFF) todas las demás.

En cualquiera de las dos opciones (interruptor único o conjunto de interruptores), además de la posibilidad de escoger entre ON/OFF, el ciudadano deberá poder rellenar, opcionalmente, su dirección de correo electrónico o su número de teléfono móvil, para que le sea notificada cualquier transferencia de datos inmediata y automáticamente, por *e-mail* o mediante mensaje de texto. Este aviso es coherente con el RGPD, en cual, en su considerando 87, señala que debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación al interesado. A estos efectos, es preciso recordar que la AGE ya cuenta con una plataforma de mensajería, SIM (sistema integral de mensajería), mantenida por el propio MINHAP y puesta a disposición de todas las Administraciones públicas, que permite a las aplicaciones incluir capacidades de gestión de correos electrónicos y SMS[533]. Esta es una buena ocasión para utilizar su propia plataforma, proporcionando un servicio plenamente orientado al beneficio del ciudadano y, simultáneamente, publicitar su existencia posibilitando la extensión de su uso por los distintos organismos públicos, de forma que estos integren en su funcionamiento diario algo tan práctico que ya se ha convertido en habitual en entidades financieras, comercios, agencias de transportes, servicios veterinarios…

[533] Información recuperada de http://administracionelectronica.gob.es/ctt/sim#.VrDdS1lqRaU (el 7 de febrero de 2016).

Con estos cambios se implementa el derecho de control y disposición del ciudadano sobre sus datos de carácter personal. Permite materializar el derecho de oposición, pudiendo escoger libremente si desea posibilitar que sus datos se pongan o no a disposición de las restantes Administraciones públicas utilizando la plataforma de intermediación de datos. En caso de que haya decidido seleccionar el ON, cada vez que alguien efectúe una transferencia de información, recibirá el correspondiente aviso por correo electrónico o móvil, haciéndose efectivo su derecho a ser informado de la cesión. En el caso de tratarse de un acceso que el ciudadano haya consentido, la notificación no tendrá mayor trascendencia pero, si se trata de un acceso indebido, al ser avisado de inmediato, podrá tomar las medidas que considere oportunas, entre ellas denunciar la cesión ante la Agencia de protección de datos con pretensión de que sea incoado un expediente disciplinario al empleado público que ha ejecutado la consulta. Esta colaboración de los ciudadanos en la defensa del Derecho concuerda con la defendida por Ihering cuando asevera que "*El derecho es trabajo sin descanso, y no solamente el trabajo de los poderes públicos, sino también el de todo el pueblo.* (…) *Todo hombre que lleva en sí la obligación de mantener su derecho toma parte en ese trabajo nacional, y contribuye en lo que puede a la realización del derecho sobre la tierra*"[534]. Permite, por tanto, lo que jurisprudencialmente se pretendía, que es: conocer y prevenir o perseguir el uso desviado o la diseminación indebida de los datos. Estamos seguros de que los accesos indebidos disminuirán drásticamente ante la perspectiva de que el afectado conozca de inmediato su ocurrencia y reaccione adecuadamente, logrando así la consecución real y efectiva de la protección de nuestros datos personales, gracias a la colaboración generalizada de la ciudadanía, en el

[534] RUDOLF VON IHERING, la lucha por el derecho.

convencimiento de que "*resistir a la injusticia es un deber del individuo para consigo mismo, porque es un precepto de la existencia moral, es un deber para con la sociedad, porque esa resistencia no puede ser coronada con el triunfo, más que cuando es general*"[535].

Entiendo que la modificación propuesta es factible y necesaria, habida cuenta de que la Administración debe buscar la máxima eficacia del derecho fundamental de protección de datos de carácter personal, aplicando el principio *in dubio por libertate*[536] (en caso de duda a favor siempre del sentido más favorable para la existencia y garantía de un derecho fundamental).

Es preciso recordar que solo por ley pueden establecerse limitaciones a un derecho fundamental, debiendo ser, en todo caso, respetuosas con su contenido esencial, sin instaurar restricciones que lo hagan impracticable o tornen ineficaz la garantía que la Constitución le otorga[537]. Cualquier limitación legal a un derecho fundamental debe respetar, además, el principio de proporcionalidad[538]. A mi juicio tal propuesta es idónea, pues posibilita la consecución del objetivo (que no es otro que permitir al ciudadano no presentar determinados datos si consiente su consulta por medios electrónicos). En este momento no se advierten otras medidas menos gravosas o lesivas para lograrlo, luego cumple con el criterio de necesidad, y el sacrificio del derecho que pudiera implicar siempre será menor que el producido por el sistema

[535] RUDOLF VON IHERING, la lucha por el derecho.
[536] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 110.
[537] STC 292/2000 de 30 de noviembre de 2000, FJ 11º.
[538] Puede consultarse la STC 207/1996, la cual nos recuerda los requisitos que conforman la doctrina del Máximo Intérprete de la Constitución sobre la proporcionalidad, consistente en que la medida limitativa del derecho fundamental esté prevista por la Ley, que sea adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo. Para un estudio con mayor profundidad resulta de interés el libro titulado "El principio de proporcionalidad y los derechos fundamentales. El principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculante para el legislador", obra de Carlos Bernal Pulido.

existente, por lo que, si el modelo de intermediación cumple el criterio de proporcionalidad estricta, el modificado también lo hará.

Debemos por ello concluir que, al existir una propuesta menos gravosa, el modelo actual incumple el criterio de necesidad exigido por la jurisprudencia para considerar aceptables las medidas limitativas de derechos fundamentales.

La decisión de implantar la solución sugerida correspondería al Director de Tecnología de la Información y de las Comunicaciones del MINHAP, en virtud de sus competencias[539] para diseñar el uso común de servicios TIC, para definir directrices técnicas y de gobernanza, para implantar y dirigir proyectos para el uso de medios y servicios generales comunes y obligatorios para toda la AGE y sus organismos públicos, para diseñar, implantar y gestionar los medios y servicios necesarios para facilitar el acceso electrónico de los ciudadanos a los servicios públicos y para colaborar en el desarrollo de políticas de seguridad en el ámbito de la Administración electrónica.

Solo desde esta Dirección podrá realizarse una estimación precisa del tiempo de desarrollo requerido para implementar la solución propuesta, en virtud del estado de sus recursos técnicos y humanos, pero podría aventurarse que, en caso de no poder realizarse con medios propios, bastaría licitar un contrato de servicios menor con plazo de ejecución de tres meses.

El ENI no requiere adaptación para implantar la solución propuesta, habida cuenta de que la modificación sugerida viene a dar cumplimiento al mandato de su artículo 8, a cuyo

[539] La información sobre sus competencias se puede recuperar de la URL http://www.minhap.gob.es/es-ES/El%20Ministerio/Organigrama/CVs/Paginas/DirecciondeTecnologiasdelaInfomacionydeComunicaciones.aspx (12 de marzo de 2016).

tenor las condiciones de seguridad aplicables deberán resultar conformes a los principios, derechos y obligaciones contenidos en la normativa de protección de datos de carácter personal. En cualquier caso, sí resultaría conveniente la adopción de una nueva resolución de la Secretaría de Estado de Administraciones públicas para adecuar la norma técnica de interoperabilidad de protocolos de intermediación de datos[540].

El catálogo de servicios de la Administración electrónica[541] de 2014 incluye, en su página 15, entre los servicios disponibles para los ciudadanos, a la plataforma de intermediación de datos. Su último párrafo alaba las ventajas que proporciona al ciudadano y a la Administración. Este sería un lugar adecuado para advertir del riesgo denunciado en este trabajo e incluir una URL, http://controlarmisdatos.redsara.es por ejemplo, donde cada ciudadano pueda indicar los servicios que desea habilitar o deshabilitar, así como la dirección de correo electrónico o el número de teléfono móvil donde prefiere ser informado de los accesos realizados a sus datos personales.

Allá donde hemos leído u oído hablar de SVD, SCSP o la plataforma de intermediación de datos, comprobamos que se promociona como una herramienta para satisfacer las necesidades de los ciudadanos, con el objetivo de liberarlos de la necesidad de presentar documentos que les son requeridos. Sin embargo, no son las necesidades y prioridades de la

[540] En el BOE del 26 de julio se publicó la Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de protocolos de intermediación de datos. En ella se define los roles de los agentes que participan en los intercambios intermediados de datos y se establecen las condiciones relativas a los procesos de intercambio intermediado de datos a través de la plataforma del Ministerio de Hacienda y Administraciones públicas, MINHAP, que ha sido premiada por la ONU en dos ocasiones, en reconocimiento a los avances en Administración electrónica.

[541] Disponible para su descarga en el Portal de Administración electrónica, en la URL http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2014/Julio/Noticia-CTT-2014-07-24-Catalogo-servicios-Ae-DGMPIAE.html#.VuM4eEeaJfc (11 de marzo de 2016).

sociedad lo buscado, sino las conveniencias de la actuación administrativa. Entendemos perfectamente aplicables las palabras de Valero Torrijos, "*no se han aprovechado las posibilidades de la tecnología para convertir a los ciudadanos, destinatarios de los servicios electrónicos, en auténticos coprotagonistas de la gestión administrativa*"[542].

La difusión de la medida propuesta a través de la inclusión de una leyenda y una URL en el catálogo no parece suficiente en el caso de las mujeres perseguidas por sus parejas o exparejas. Para dar debido cumplimiento al artículo 18 de la ley orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género, sería necesario informar específicamente a las mujeres afectadas por esta lacra social de la posibilidad técnica de deshabilitar la utilización de los servicios de la plataforma de intermediación, impidiendo así el acceso a sus datos personales, especialmente a la localización de su residencia actual.

La falta de medios electrónicos por parte de los interesados podría poner en riesgo la utilidad de la solución propuesta, especialmente en las generaciones pre-Internet. En previsión de este problema, el artículo 12 de la ley 39/2015, ya prevé la asistencia por funcionarios públicos en lo referente a identificación y firma electrónica.

En la actualidad, ya existe un servicio que permite consultar las transmisiones de datos de un ciudadano realizadas mediante cualquiera de los servicios disponibles en la plataforma de intermediación de datos. También existe otro que permite obtener los justificantes PDF de dichas transmisiones. Suponemos que pueden ser utilizados en la carpeta ciudadana, para que cada uno de nosotros pueda consultar las transmisiones que se han realizado de sus datos

[542] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 40-41.

personales hasta este momento, pudiendo actuar en consecuencia[543]. Recordemos que "(…) *ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin*"[544].

Se puede poner en duda, sin embargo, la tenencia de un conocimiento suficiente por parte de la ciudadanía; dudamos de que sea consciente siquiera de la existencia de una plataforma de intermediación y, mucho menos, que se plantee solicitar la información pertinente sobre lo que se ha consultado con ella; más cuestionable aún es que la ciudadanía conozca la disponibilidad de una carpeta ciudadana. En consecuencia, se estima necesario promover una campaña informativa en la que se expliquen no solo los pros, sino también los contras, como sugería la autoridad irlandesa, y se envíe de oficio a cada ciudadano la información relativa a las cesiones realizadas de sus datos hasta la fecha, dejando a la voluntad de cada persona la posibilidad de solicitar esa información periódicamente, mientras esos servicios de consulta de las transmisiones no estén accesibles directamente para el propio ciudadano[545], debidamente identificado con su DNIe o certificado digital, materializando así el derecho de acceso[546], inmediato y sin la limitación legal de obtener como máximo uno cada doce meses.

---

[543] Realizada una prueba de dichas consultas en la carpeta ciudadana, el resultado fue nulo, a pesar de que se ha utilizado el servicio de consulta de datos de domicilio. Puede interpretarse como que el programa informático está en pruebas o no funciona aún correctamente.

[544] FJ 6º de la STC 292/2000 de 30 de noviembre de 2000.

[545] Somos conscientes de que requeriría un esfuerzo especial de refuerzo de la seguridad, dado que esos informes abandonarían la red SARA.

[546] El legislador orgánico, consciente de que la premisa indispensable para cualquier reclamación o rectificación es saber qué información sobre sus personas almacenan las distintas Administraciones públicas, recoge el derecho de acceso a los datos, a su procedencia y a las comunicaciones de los mismos previstas o realizadas. Aunque se limita el ejercicio de este derecho, salvo excepciones, a una vez cada doce meses, debemos plantearlos la legitimidad de esta restricción a los derechos fundamentales en el momento actual. El legislador de 1999 pudo entender que esta limitación era idónea, necesaria y proporcionada, requisitos imprescindibles para la licitud de tal medida. Sin embargo, en 2016, el empleo de técnicas informáticas para el acceso a la información almacenada nos lleva a

Como la imaginación no tiene límites, nos preguntamos… ¿por qué no implementar las modificaciones necesarias para que el ciudadano pueda utilizar también el resto de los servicios? No serían las Administraciones públicas las que se intercambiaran la información, sino que sería el propio ciudadano quien la obtuviera de manera inmediata y la pudiera aportar junto a su solicitud, si ese fuera su deseo.

Salvando el escollo técnico de mejorar la seguridad para que la información pueda circular manteniendo la confidencialidad fuera de la red SARA, no imaginamos una forma mejor de materializar el derecho de control del uso y disposición de los datos de carácter personal por parte de los ciudadanos.

El modelo de intermediación permite grandes ahorros y mejora el servicio público en cuanto a la eficacia y eficiencia de la actividad administrativa, es cierto, contribuyendo indudablemente y de forma espectacular a la implantación de la Administración electrónica. "(…) *no podemos olvidar que la informática ha desempeñado, y sin duda seguirá desempeñando, un indudable avance en el desarrollo humano, solo queda encauzar adecuadamente los medios que ofrece para evitar que pueda volverse contra la persona*"[547]. Conscientes por tanto de su utilidad pero temerosos ante su mal uso, no se pretende eliminar los grandes bancos de datos en poder de las Administraciones públicas ni la interconexión que los posibilita, sino someter su utilización a la normativa de protección de forjada jurisprudencialmente, de forma consecuente con lo expuesto en el considerando 7 del RGPD,

---

plantear la conveniencia de una revisión legislativa orientada no solo a modificar esa acotación temporal, sino también a facilitar al ciudadano el acceso telemático inmediato a los datos registrados en ficheros de titularidad pública.

[547] ÁVILA RODRÍGUEZ, C.M. (2012), vida privada, 178.

conforme al cual las personas físicas deben tener el control de sus propios datos personales, reforzando la seguridad jurídica y también práctica.

Analizado el conflicto de esta solución informática con el derecho fundamental a la protección de datos de carácter personal, ofrecemos soluciones técnicas, factibles y relativamente simples, que puedan situarnos allá donde se encuentra el punto de equilibrio entre las distintas posturas enfrentadas, aplicando el principio de proporcionalidad, sopesando las ventajas para el servicio público y su incidencia en el derecho fundamental afectado. Como señala Martín Rebollo, la eficacia no puede obtenerse a cualquier coste, porque el precio que nunca se puede pagar es el de la garantía; eficacia y garantía han de caminar juntas[548].

3.2.3. Consecuencias para los obligados a usar medios electrónicos del incumplimiento del principio de neutralidad tecnológica

En páginas anteriores he justificado el incumplimiento del principio de neutralidad tecnológica en el desarrollo del *software* de las aplicaciones de nuestras Administraciones públicas, no por menospreciar su importancia, sino por la imposibilidad de alcanzarla con los recursos limitados de que se dispone. También se ha expuesto la enorme dificultad que puede suponer lograr que el equipo del ciudadano funcione adecuadamente para usar la eAdministración de manera exitosa, lo que Gamero Casado describe de una forma magníficamente acertada al decir que "*Incluso usuarios avanzados en el manejo de las TICS padecen graves dificultades para completar los trámites exigidos en los procedimientos. Debido a restricciones del sistema (tamaño o formato de los ficheros), a problemas de*

[548] MARTÍN REBOLLO, L. (1992), vigencia y limitaciones, 32-33.

interoperabilidad, y a otros motivos, a veces no logran completar el trámite en el plazo previsto"[549]. El mismo autor denuncia la implacable jurisprudencia[550] que condena a los obligados a relacionarse con la Administración por medios electrónicos cuando no logran hacerlo en plazo "*aun cuando haya constancia probatoria de que intentó la presentación electrónica sin lograrla, e incluso de que, a la vista de ello, realizó el trámite en plazo de manera presencial*"[551].

Es preciso recordar el artículo 4.i) de la derogada LAE, por el que la utilización de las TIC había de garantizar la independencia en la elección de las alternativas tecnológicas por los ciudadanos. Hoy es el artículo 11.1.b) del ENI el que establece que los servicios electrónicos y las aplicaciones puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas han de ser visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

Por ello, en mi opinión, el obligado a relacionarse con la Administración por medios electrónicos que no logre realizar el trámite por utilizar versiones de navegadores (incluso de uso generalizado como Chrome, Mozilla Firefox o Internet Explorer) incompatibles con aplicaciones como la plataforma @firma (utilizada por muchas Administraciones públicas), o por versiones de Java no recientes o, paradójicamente, por versiones de Java demasiado nuevas, ha cumplido sobradamente con su deber intentándolo sin éxito. Es la Administración la

[549] GAMERO CASADO, E. (2016), panorámica.
[550] La implacable jurisprudencia a la que hace referencia es la SAN 872/2011 de 10 de febrero de 2011, cuyos fundamentos jurídicos (y, sobre todo, técnicos) estimo interesante desgranar a continuación.
[551] GAMERO CASADO, E. (2016), panorámica.

que ha incumplido su obligación de respetar la neutralidad tecnológica, justificadamente por la carencia de medios humanos, materiales y técnicos, pero la ha incumplido. Los tribunales han de apreciar este hecho y no repercutir al ciudadano, inocente e indefenso, las consecuencias de las carencias públicas. Sin embargo, nuestra jurisprudencia parece desconocer el principio de neutralidad tecnológica y fallar en su contra, a pesar de que toda restricción indebida en el acceso a los contenidos y servicios ofrecidos por medios electrónicos podría dar lugar a la correspondiente responsabilidad patrimonial[552].

La sentencia de la Audiencia nacional 872/2011, de 10 de febrero de 2011, desestima el recurso contencioso administrativo interpuesto por la representación procesal de la Comunidad autónoma de La Rioja, quien no fue capaz de presentar una solicitud utilizando medios electrónicos, decidiendo entregarla el último día del plazo en las oficinas de Correos. Este es el primer punto que llama la atención. La recurrente es una Administración pública y, como indica la sentencia, "*las entidades interesadas (Organismos Oficiales) necesariamente han de contar con un elevado grado de implantación y uso de las tecnologías de la información y la comunicación*". Por tanto, si un organismo oficial no ha sido capaz de lograrlo, ¿resulta lícito obligar a ciudadanos y a empresas a utilizar unos medios electrónicos que ni la propia Administración consigue emplear con éxito?

La recurrente describe el problema indicando que "*en el momento de introducir la contraseña maestra de la Consejera, para remitir la solicitud, solo aparecía una página que se estaba cargando, sin que se visualizara nada más ni terminara de cargarse*". Esta explicación no

[552] VALERO TORRIJOS, J. (2008), acceso a los servicios, 249.

es en absoluto un caso aislado. Es, en lo esencial, la misma que he oído en decenas de ocasiones en un periodo de tiempo inferior a dos años y, sin ir más lejos, he podido vivirla la semana pasada, estando presente cuando una empresa intentaba acceder con certificado al registro electrónico de una Administración pública. Ocurre con bastante frecuencia, sin que las aplicaciones indiquen al usuario, en general, qué puede estar ocurriendo.

Podemos leer en el FJ2 que "(…) *se tramitó la solicitud de instalación de la maquina* (sic) *virtual Java en la Consejería de Servicios Sociales, necesaria para la ejecución del programa Avanza 2008, comprobándose la correcta ejecución del mismo* (…)" y "*el Servidor de la Comunidad Autónoma funcionaba perfectamente y la firma electrónica se encontraba correctamente instalada. Por lo que probablemente el problema técnico estaba en el Ministerio, por una posible saturación de su servidor*". Se deduce fácilmente de estos dos fragmentos que la recurrente, una Administración pública, daba "palos de ciego" en su búsqueda de una solución para un problema que desconocía y del que aún estaba muy lejos de acercarse. ¿Cómo se puedes esperar, por tanto, que un ciudadano medio sepa lo que le está ocurriendo y cómo resolverlo?

En el FJ4 se recoge el informe de la Subdirectora general para la sociedad digital, que se refiere al *log*[553] de la aplicación, diciendo que "*El registro electrónico guarda el rastro de los intentos fallidos de transmisión y de sus posibles causas... se averiguó que no había rastro de ningún intento que correspondiese a la solicitud de la Consejería de Servicios Sociales*

[553] De los registros de *log* se hablará *infra*, en el capítulo correspondiente al análisis de riesgos. Por el momento, basta con indicar que se trata de un fichero en el que se van guardando trazas de lo que ocurre con la aplicación, las cuales pueden ser analizadas con posterioridad.

del Gobierno de La Rioja". Esta afirmación de la Subdirectora es, como mínimo, discutible. Efectivamente, el registro electrónico guarda rastro de los intentos fallidos de transmisión y, sí, también es cierto que entre ellos no figuraba el del Gobierno de La Rioja. El matiz reside en que el registro electrónico solo guarda los intentos fallidos de transmisión que han llegado a contactar con la aplicación y han fallado, pero no recoge aquellas tentativas malogradas que ni siquiera han llegado a establecer contacto, como le ocurrió a La Rioja. Explicándolo con una burda comparación, sería diferente llamar con un móvil a una persona que ha olvidado su teléfono en el coche, que intentar hacer esa misma llamada pero no lograrlo porque el móvil se nos ha quedado sin batería. En el primer caso, el destinatario verá que tiene una llamada perdida. En el segundo caso, nunca sabrá que alguien intentó hablar con él. En resumen, el registro electrónico solo guarda rastro de algunos intentos fallidos, de aquellos que llegan a establecer conexión. La Subdirectora conocía ese matiz, pues continúa diciendo que "*Esto significa, salvo prueba en contrario, que el solicitante pudo haber rellenado su solicitud pero no llegó a conectar con el registro electrónico* (…)". Efectivamente, eso es lo que ocurrió, se intentó, pero no se logró.

Continúa el informe señalando que "*para que pudiésemos aceptar que su intento de envío era válido, había que comprobar que el fallo en la transmisión fuera imputable al funcionamiento del registro telemático del MITYC, y no al interesado, para lo que nos debían mandar el mensaje de error* (…)". Resulta algo difícil enviar un mensaje de error que la aplicación no da. Al menos podría mostrar un aviso al usuario, antes de comenzar el intento, explicando que si en determinado tiempo máximo no se logra completar el proceso, las causas pueden ser debidas a no utilizar tal navegador, o tal o cual versión de java, etc. En este caso, "*el*

Gobierno de la Rioja admitió que el error se había producido porque habían utilizado para la transmisión un equipo informático que no tenía incorporado el certificado de firma electrónica de la titular de la Consejería en el navegador de Internet". Parece bastante obvio que para utilizar un certificado electrónico, hay que tener un certificado electrónico. Igual ya no lo es tanto el hecho de que, para utilizar un certificado electrónico desde un navegador, hay que tener el certificado electrónico instalado en ese navegador concreto, no siendo suficiente tenerlo en otro (o lo que es peor, en un ordenador diferente). Si algo tan sencillo como esto ha impedido que una Administración pública fuese capaz de enviar una solicitud a través de un registro electrónico, ¿qué cabe esperar del ciudadano corriente, de las empresas del sector privado o del presidente de mi comunidad de vecinos[554]?

Prosigue el informe afirmando que "*en las páginas Web del Ministerio se publica información suficiente para poder utilizar los programas para cumplimentar las solicitudes*". Pero si un organismo público no es capaz de entender cómo se usa un certificado electrónico, ¿cómo se espera que la ciudadanía pueda entender cómo escoger las versiones adecuadas de los navegadores admisibles y no otros, y cómo cambiar su versión de java en función de la que necesite la aplicación que va a utilizar, que puede ser incompatible con la que le pide otra Administración pública con la que también tenga obligación de relacionarse? ¿Entenderán lo que tienen que marcar en el panel de control de java para que se logre desplegar el *applet* o el

[554] Gamero Casado señalaba ya, cuando la ley era solo un anteproyecto, la problemática a la que se iban a enfrentar las comunidades de propietarios, condenadas a dejar la administración a un profesional especializado. *Vid*. GAMERO CASADO, E. (2016), panorámica.

miniapplet de firma electrónica? ¿O más bien conseguirán llegar a "*niveles exasperantes de frustración*"[555]?

Mientras la neutralidad tecnológica de las aplicaciones públicas no nos lleve a una mejora importante en su usabilidad, la Administración debería poner a disposición de los obligados a relacionarse con ella por medio electrónicos un servicio de asesoramiento técnico avanzado[556], capaz de resolver todas las dificultades que se puedan presentar, algo realmente complejo, así como habilitar espacios de acceso público con diferentes equipos ya configurados para asegurar la compatibilidad con las distintas aplicaciones que el usuario requiera, y asistencia personal *in situ* para su uso.

3.2.4. La privación del trámite de subsanación

Señalaba *supra* un aspecto novedoso de la nueva ley 40/2015, sutilmente escondido en su artículo 41.1. La actual definición de "actuación administrativa automatizada", que ahora pasa a ser "*cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público*", ha hecho desaparecer la exigencia de que ese *software* estuviese "adecuadamente programado".

Nos encontramos ante un concepto jurídico indeterminado complejo de definir, habida cuenta de que el *software* siempre contiene errores, como se explicó *supra*. Incluso en el caso de que el programador hubiera producido un código totalmente libre de fallos, el defecto

[555] GAMERO CASADO, E. (2009), interoperabilidad.
[556] Recordemos que la nueva ley precisamente excluye de asistencia a los obligados a relacionarse con la Administración por medios electrónicos.

podría provenir de la especificación de requisitos, como ocurre con los programas que no están preparados para permitir la subsanación de solicitudes debido a un análisis incorrecto del proceso a informatizar. Citando la STSJ de Cantabria 862/2009, entre otras, "*la progresiva espiritualización del Derecho pugna con el empleo de fórmulas sacramentales de cuya perfecta cumplimentación, sin posibilidad alguna de rectificación o subsanación, dependa el ejercicio mismo de los derechos. El empleo de impresos estereotipados,* ***de procesos informáticos***[557] *y de mecanismos, en suma, encaminados a facilitar la actividad de la Administración y a gestionar masivamente procedimientos que afectan a numerosos interesados, tal como sucede en los procedimientos de concurrencia competitiva, no pueden convertirse en una trampa saducea para los ciudadanos*".

Cuando el ciudadano que pretende presentar una solicitud por vía electrónica desconoce algún dato que el programa informático exige cumplimentar obligatoriamente, no podrá continuar si no lo introduce, no podrá grabar ni enviar en plazo por vía telemática, con lo que tampoco le será posible ejercer su derecho de subsanación, todo porque el diseño del programa no tiene en cuenta las exigencias legales[558]. Este supuesto, no contemplado expresamente en la legislación anterior, se regula ahora por el artículo 68.4 de la ley 39/2015, viniendo a consumar la privación del trámite de subsanación instaurada *de facto* durante la vigencia de la LAE, si bien de forma ambigua. La Administración puede establecer un modelo obligatorio de solicitud en un procedimiento concreto (artículo 66.6 de la misma ley), pero ello no le autoriza a imponer datos o requisitos no previstos en la normativa de aplicación. Si un

[557] La negrita es nuestra.
[558] PIÑAR MAÑAS, J.L. (2011), revolución tecnológica.

formulario electrónico incurre en esa ilegalidad, no permitiendo continuar por considerar obligatorio un dato no exigido por la normativa aplicable, ante esta clara restricción de derechos que impide la presentación en plazo, Gamero Casado entiende que el trámite de presentación se debe considerar subsanable en tanto que la Administración no depure el formulario y suprima las exigencias obligatorias que rebasan las previsiones normativas.[559]

Personalmente considero más acertado culminar con éxito la presentación electrónica del formulario dentro del plazo establecido, rellenando todos los datos indebidamente exigidos por la Administración. En aquellos campos destinados a contener caracteres alfanuméricos, el ordenador probablemente aceptará como válida cualquier respuesta diferente a espacios en blanco, como "--", o bien ".", o incluso "NO OBLIGATORIO" o "NO APLICA", o su versión reducida "N/A". Si la información pedida de forma indebida es un correo electrónico, la máquina probablemente aceptará algo similar a "NOOBLIGATORIO@EMAIL.ES". En el caso de campos numéricos, puede servir de ejemplo, real y reciente, la solicitud de admisión al programa de doctorado, en la que se exigía la introducción de la nota media numérica obtenida en los estudios que dan acceso a dicha titulación. El cálculo de ese dato es imposible cuando la carrera se terminó en 1994, cuando no constaba en el expediente nota media alguna, ni siquiera nota numérica de cada asignatura, ni número de créditos de cada una. La solución rápida pasa por introducir 5,0 (valor mínimo admisible) y grabar la solicitud, abriendo así la posibilidad de subsanarla posteriormente. La opción de presentarla en papel, a tenor del precitado artículo 68.4 y de una rígida jurisprudencia, está abocada al contencioso-administrativo y, probablemente, al fracaso.

[559] GAMERO CASADO, E. (2016), panorámica.

4. EL ELEMENTO OPERATIVO EN LA eADMINISTRACIÓN

Los elementos operativos u organizacionales, frecuentemente olvidados al elaborar las normas[560], pueden dificultar una implantación exitosa de la Administración electrónica. Para Gamero Casado, el verdadero reto de la interoperabilidad no está en sus dimensiones técnica ni semántica, sino en la organizativa y jurídica[561]. Para Baño León, más que en la ley, es en la normativa técnica y en la capacidad de accesibilidad del *software* donde más se arriesgan las garantías de los particulares en la eAdministración, afirmando que los programas han de permitir un manejo simple la información, que ha de ser fácilmente accesible e inteligible por cualquier persona que sepa leer y escribir[562].

Agrupando en tres grandes áreas conceptuales los elementos operativos que inciden en la implantación de la Administración electrónica, la primera englobaría la inercia, la resistencia al cambio y falta de incentivos, presentes tanto en el personal al servicio de las Administraciones públicas como la ciudadanía, empresas y profesionales incluidos. Un segundo bloque trataría la escasez de formación en las distintas partes implicadas, para finalizar con un tercer grupo que abarque dos aspectos íntimamente ligados como son la seguridad y la confianza.[563]

Al margen de los aspectos señalados, la implantación de la Administración electrónica puede verse condicionada por la carencia de los medios necesarios para su puesta en marcha, problema agudizado especialmente en las Entidades locales de menor tamaño.

[560] DE MIGUEL MOLINA, M. (2010), Nueva Gestión Pública, 134.
[561] GAMERO CASADO, E. (2009), interoperabilidad, 299.
[562] BAÑO LEÓN, J.M. (2015), reforma del procedimiento.
[563] GALÁN PASCUAL, C./ MAROTO ILLERA, R. (2013), gobierno electrónico, 33-35.

4.1. CARENCIA DE LOS MEDIOS NECESARIOS

La transformación completa del procedimiento administrativo tradicional en un procedimiento administrativo electrónico, a fecha de hoy, habiendo entrado ya en vigor la mayoría de los preceptos de las nuevas leyes 39 y 40/2015, no deja de ser un anhelo. No se puede ignorar la disparidad entre la realidad cotidiana (en muchos casos carente de medios personales y técnicos suficientes y adecuados) y la aspiración de avanzar en la generalización e imposición del uso de medios electrónicos[564]. "*El plano de irrealidad en el que se han movido los redactores de la ley*"[565] choca frontalmente con el quehacer diario del funcionario rodeado de grandes columnas de archivadores repletos de papel, que recorre pasillos flanqueados por estanterías rebosantes, mientras fantasea en cómo, con un presupuesto de 20.000 € para desarrollos informáticos, puede pretender transformar en electrónicos las decenas de procedimientos administrativos diferentes que figuran inventariados en su servicio. Nuestras nuevas y ambiciosas leyes administrativas no han venido de la mano del necesario acompañamiento presupuestario, a pesar de que "*el cambio de la red de procedimientos, trámites y formas, requerirá costes e inversiones ingentes en medios físicos así como recursos humanos especializados*"[566]. Por tanto, la efectividad de la reforma viene condicionada por contemplar unas asignaciones presupuestarias que permitan poner en marcha el conjunto de medidas

[564] CASARES MARCOS, A. (2016), novedades, 96.
[565] GAMERO CASADO, E. (2016), panorámica.
[566] CHAVES GARCÍA, J.R. (2016), nuevos forjados.

previstas en los nuevos textos legales[567]. Hasta el momento, se puede afirmar que la Administración electrónica en nuestro país es una realidad a "medio construir"[568].

4.2. INERCIA, RESISTENCIA AL CAMBIO O FALTA DE INCENTIVOS

Valero Torrijos identifica este aspecto como el que, con frecuencia, resulta ser el principal inconveniente para la efectiva aplicación de las tecnologías, y lo describe como "*inercias y hábitos de una práctica administrativa excesivamente burocratizada*", afirmando que acaba constituyendo una rémora de las iniciativas reformistas, máxime cuando presentan un trasluz tecnológico[569].

La presencia de ese elemento tecnológico, en ciertos individuos, añade un problema adicional, una reacción que puede incluso desembocar en una afección psicológica en la que la salud mental del trabajador sufre deterioros importantes. Conocido como tecnoestrés o **estrés tecnológico**, puede derivar de una falta de adaptación a la técnica derivada de una incorrecta estrategia de implantación, centrada en las máquinas y no en sus usuarios, sin participación activa de los destinatarios y carente de un proceso gradual de introducción[570].

El *software* puede ser diseñado de forma que minimice ese impacto negativo en los usuarios. Con ese objetivo, el anexo del real decreto 488/1997, de 14 de abril, sobre

[567] QUINTANA DAIMIEL, A. (2015), análisis preliminar.
[568] DAVARA FERNÁNDEZ DE MARCOS, L./ DAVARA RODRÍGUEZ, M.A. (2016), novedades.
[569] VALERO TORRIJOS, J. (2009), las garantías jurídicas, 19. El mismo autor también afirma la deliberada perpetuación de esas inercias y hábitos de trabajo con un exceso regulatorio asistemático, lo que ha dificultado el desarrollo del potencial innovador de las TIC, en VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 54.
[570] RODRÍGUEZ ESCANCIANO, S. (2015), control empresarial, sección 4.1.

disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización, en su apartado 3.b), establece que el programa habrá de ser fácil de utilizar y deberá, en su caso, poder adaptarse al nivel de conocimientos y de experiencia del usuario, que se puede materializar, conforme a la guía técnica[571] del INSHT, en los siete principios generales aplicables a las técnicas de diálogo que describe la norma UNE-EN-ISO9241.10: adaptación a la tarea, autodescriptibidad, controlabilidad, conformidad con las expectativas del usuario, tolerancia a los errores, aptitud para la individualización y facilidad de aprendizaje.

Habida cuenta de que el estrés puede provenir de la dificultad de adaptación del trabajador a los nuevos sistemas, el INSHT contempla unas estrategias preventivas que pasan por proporcionar una información adecuada sobre los cambios y sus consecuencias que evite las reticencias motivadas por el miedo, formar en el uso de las nuevas tecnologías para mitigar la tecnofobia y la tecnoansiedad, involucrar a los propios empleados en la selección e implantación de las herramientas, redefinir el puesto de trabajo, diseñarlo desde las perspectivas de ergonomía, usabilidad y amigabilidad, desarrollar equipos de trabajo dedicados específicamente a los problemas que pueda generar la implantación de las modificaciones y crear un ambiente de apoyo a la implantación de las innovaciones tecnológicas[572]:

La **incentivación**[573] de los empleados y de los organismos públicos puede llevarse a cabo haciéndolos partícipes de la construcción del nuevo modelo, de forma que se sientan parte

[571] INSTITUTO NACIONAL DE SEGURIDAD E HIGIENE EN EL TRABAJO, evaluación y prevención, 34.
[572] RODRÍGUEZ ESCANCIANO, S. (2015), control empresarial, sección 4.2.
[573] GALÁN PASCUAL, C./ MAROTO ILLERA, R. (2013), gobierno electrónico, 33 y ss.

de la solución, no ajenos a ella, de forma que sus esfuerzos contribuyan al logro del éxito de la innovación tecnológica. Un estímulo para los organismos que puede contribuir a la culminación del proceso de forma adecuada puede ser la asignación de distintivos de conformidad, cumplimiento o excelencia. Sin embargo, el modo más productivo de incentivar a la ciudadanía, incluyendo tanto particulares como profesionales o empresas, pasa por el incremento de la rapidez y de la sencillez en la realización de los trámites.

La posibilidad de incluir incentivos económicos por la utilización de las nuevas tecnologías es una cuestión no pacífica, habida cuenta de la débil línea que separa ese estímulo económico al uso de medios electrónicos de la discriminación de los ciudadanos que no gozan de la misma facilidad para enfrentarse exitosamente con los avances técnicos[574]. A tenor del artículo 4.b) de la ya derogada LAE, se ha de respetar el principio de igualdad, de forma que el uso de medios electrónicos no implique restricciones o discriminaciones para los ciudadanos que se relacionen con la Administración por medios no electrónicos, dejando a salvo las medidas dirigidas a incentivar la utilización de aquellos. En mi opinión, sí se podría producir discriminación al incentivar económicamente el uso del canal electrónico a sabiendas de que las generaciones no nativas digitales, especialmente las de mayor edad, habitualmente no se encuentran en condiciones técnicas ni psicológicas óptimas para emprender esa aventura. Lo que para los jóvenes presenta un gran atractivo, para ellos resulta una actividad tortuosa y, me atrevo a decir, imposible de culminar con éxito. Muchos de ellos no saben utilizar un cajero automático,

[574] GALÁN PASCUAL Y MAROTO ILLERA no aprecian discriminación alguna en la aplicación de este tipo de medidas en la página 35 de su trabajo antes citado. Su interpretación se apoya en un reparto de los beneficios asociados a la disminución del coste del trámite realizado, interpretando que una parte debe recaer en el ciudadano que ha motivado ese ahorro.

viven en soledad y sobreviven con una pensión limitada, pero no tienen opción a un ahorro económico que sí se ofrece a las generaciones más jóvenes. La nueva ley 39/2015, con sus artículos 13.b) y 12.2, viene a resolver el problema previendo la asistencia a los interesados en el uso de medios electrónicos en su relación con la Administración. Así, si no disponen de los medios electrónicos necesarios, su identificación o firma electrónica puede ser válidamente realizada por un funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello, tras proceder a su identificación y a la obtención de su consentimiento expreso, quedando constancia para los casos de discrepancia o litigio. Del mismo modo, Galán y Maroto, consideran como incentivo el dictar la obligatoriedad de la tramitación electrónica para los casos en que se cumplan las condiciones adecuadas; en caso contrario, afirman que se pueden potenciar los servicios habilitados.

Pero el derecho de asistencia en el uso de los medios electrónicos encierra en sí mismo un grave problema de discriminación, al relegar a los obligados por el deber de comunicarse electrónicamente con la Administración[575], grupo ampliable reglamentariamente[576]. Tal previsión constituye una discriminación negativa carente de todo fundamento y justificación inadmisible[577].

Una muestra de la inercia que dificulta una transformación tan radical como la constituida por el paso a la tramitación digital es la dificultad en la **reasignación de los efectivos**

[575] MENÉNDEZ SEBASTIÁN, E.M. (2016), nuevas Leyes, 29.
[576] FERNÁNDEZ RODRÍGUEZ, T. R. (2015), notificaciones electrónicas, 364-365. El autor cuestiona con dureza la carga que se puede imponer a los ciudadanos por una norma reglamentaria en aras de beneficiar únicamente a la Administración.
[577] GAMERO CASADO, E. (2016), panorámica.

de las Administraciones públicas. La Administración, como indica Gamero Casado[578], es una estructura tremendamente rígida, y puede llegar a encontrarse con efectivos sobrantes en determinadas áreas que será necesario asignar a nuevos puestos de trabajo. La LAE ya parecía consciente de ello, a tenor de su disposición adicional tercera, donde prevé la elaboración, tras su entrada en vigor, de un plan de implantación que incorpore la estimación de los recursos económicos, técnicos y humanos precisos para su adecuada aplicación, algo que debería haberse realizado con anterioridad a la publicación de la ley[579].

Por último, no puede ignorarse el **elevado coste económico** que supone la implantación de la Administración electrónica como un gran factor de retardo en su materialización. Es preciso dotar a las Administraciones públicas de los equipos informáticos adecuados para el correcto desempeño de sus tareas, los cuales, en un breve espacio de tiempo, habrán quedado obsoletos y requerirán su renovación. A su vez, será necesario desarrollar el *software* adecuado para llevar a cabo este ambicioso objetivo, lo que requiere programas específicos "*que son extraordinariamente costosos y complejos de mantener y actualizar*".[580]

4.3. ESCASEZ DE FORMACIÓN

Los trabajadores, por lo general, prefieren comprender el porqué de las cosas, reaccionando con resistencia y rechazo a lo que les es impuesto[581]. Una adecuada preparación redunda en la disminución de la resistencia al cambio.

[578] GAMERO CASADO, E. (2008), era de la información, 32.
[579] DE MIGUEL MOLINA, M. (2010), Nueva Gestión Pública, 136.
[580] GAMERO CASADO, E. (2008), era de la información, 32.
[581] CARRASCO NÚÑEZ, Á. (2013), conceptos de seguridad informática, 114.

Instrumentos como el ENS disponen la formación del personal de forma que se garantice su conocimiento efectivo[582]. La formación del personal de la Administración especialista en el campo de la seguridad de las TIC está encomendada al CCN adscrito al CNI (Centro nacional de inteligencia)[583]. Pero, a pesar de la importancia de los conocimientos imprescindibles en este ámbito, no es esta la carencia de formación que parece frenar la implantación de la eAdministración. La propia LAE es consciente de que una gran parte del éxito o fracaso de la implantación de la Administración electrónica está directamente relacionada con la forma en que los empleados públicos perciban el cambio y colaboren con él, requiriendo un esfuerzo en formación y en obtención de nuevas habilidades, y así se muestra en su artículo 33[584]. Afirma Valero Torrijos que la aplicación práctica de la LAE requiere un cambio radical en la formación de su personal "*de manera que las inercias e intereses creados no terminen por frenar las posibilidades de modernización* (…)"[585]. A pesar de la necesidad de atemperar adecuadamente el coste de la formación, "*solo un empleado público debidamente formado es capaz de asumir con decisión sus responsabilidades y su papel en el desenvolvimiento del procedimiento*"[586]. En el mismo sentido, la propia ley lo prevé en su disposición adicional segunda, bajo la rúbrica de "formación de empleados públicos", entre otras materias, de la utilización de medios electrónicos, la seguridad de los mismos o la protección de datos de carácter personal, pero la restringe al ámbito de la AGE. Para Martínez Gutiérrez, se trata de una

[582] Disposición adicional segunda.
[583] Así se ha dispuesto en el artículo 2.2.b) del real decreto 421/2004, de 12 de marzo, por el que se regula el Centro criptológico nacional. A modo de ejemplo, puede verse la resolución de 7 de junio de 2016 del INAP, por la que se convocan acciones formativas en materia de seguridad de las TIC, en colaboración con el CCN, publicada en el BOE de 9 de junio de 2016.
[584] AGUILAR ROS, R./ PALOMAR OLMEDA, A. (2011), procedimiento electrónico, 650-651.
[585] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 119.
[586] GALÁN PASCUAL, C./ MAROTO ILLERA, R. (2013), gobierno electrónico, 36.

propuesta interesante a la vez que deficiente, por vincular únicamente a la AGE, dado su carácter no básico, y por no precisar los instrumentos concretos mediante los cuales promover esa efectiva formación[587], la cual debería extenderse a todas las Administraciones públicas[588].

El TREBEP reconoce como derecho individual del empleado público la formación continua y la actualización permanente de sus conocimientos y capacidades profesionales; a su vez, también lo contempla como instrumento de planificación de los recursos humanos de las Administraciones públicas, necesaria para la consecución de la eficacia y eficiencia. Para lograrlas, es imprescindible la formación profesional continua de todos los empleados públicos, así como su reciclaje profesional. Esa necesidad se ha vuelto "*más imperiosa dada la rápida evolución de los conocimientos y de las tecnologías de la información y de las comunicaciones y, con ello, de los requerimientos de la Administración a sus empleados*".[589]

Tanto el INAP[590] como distintos centros de formación de empleados públicos han incluido en su oferta formativa una amplia variedad de cursos correspondientes al área de nuevas tecnologías, junto con algunos otros versados sobre protección de datos, novedades legislativas, etc. Sin embargo, es mi opinión personal que el aprendizaje efectivo, directamente relacionado con el grado de interés, no puede asegurarse siquiera con las pruebas de aprovechamiento, salvo honrosas excepciones. La formación reglada, puntuable en concursos de traslados, podría

[587] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 371.
[588] DE MIGUEL MOLINA, M. (2010), Nueva Gestión Pública, 135.
[589] Resolución de 9 de octubre de 2013, de la Secretaría de Estado de Administraciones públicas, por la que se publica el acuerdo de formación para el empleo de las Administraciones públicas de 19 de julio de 2013, publicada en el BOE de 21 de octubre de 2013.
[590] *Vid.* http://www.inap.es/formacion-en-tic (accedido el 21 de enero de 2017).

provocar una asistencia interesada en algo diferente al aprendizaje. Sin perjuicio de su mantenimiento, la aplicación de técnicas como el *mentoring* en las Administraciones públicas podría obtener mejores resultados. De amplia aplicación en entornos empresariales y consistente en la guía del trabajador por su "mentor", aumenta la motivación de los empleados, reduce la tasa de movilidad laboral, mejora la capacidad de liderazgo, conduce a una mayor capacidad de adaptación, incrementa el interés en compartir conocimientos y la capacidad para enfrentarse a la toma de decisiones con mayor garantía[591]. El trabajo en equipo da la oportunidad de compartir el saber que, de otro modo, se perdería con la jubilación o con los traslados del personal. La experiencia acumulada de un compañero ayuda a avanzar sin tener que partir de cero, permitiendo su puesta al día[592]. Pero la interacción directa entre dos empleados públicos podría resultar una forma excesivamente lenta de transmisión del conocimiento. "*Una Administración con tantos empleados públicos es rica en experiencias de buenas prácticas que deben ser trasladadas a otras unidades*" y la Administración electrónica contribuye a la gestión de ese conocimiento, creando redes de *benchmarking* [593].

El procedimiento administrativo electrónico supone un paso atrás en la protección de los datos de carácter personal, en opinión de Parra y Campanillas[594], la cual subscribo. Es posible que los empleados públicos, en término medio, conozcan la normativa, pero no parecen haberla interiorizado. Un trabajador concienciado y motivado podría influir en su entorno

[591] COLOMO PALACIOS, R./ TOVAR CARO, E./ GÓMEZ BERBIS, J.M./ GARCÍA CRESPO, A. (2007), recomendaciones
[592] MARTÍN MORENO, F. (2013), experiencia profesional, 58-59.
[593] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 573.
[594] PARRA SÁEZ, S./ CAMPANILLAS CIAURRIZ, J. (2010), procedimiento administrativo electrónico, 816-817.

sensiblemente más que todos los cursos reglados que se pudieran impartir a la misma audiencia. No se trata tanto de una cuestión de formación como de concienciación.

Un caso problemático asociado a la falta de formación, al que Valero Torrijos considera de especial trascendencia, es la efectiva supervisión por parte de la Administración del funcionamiento de las aplicaciones informáticas, particularmente en los casos de actuación automatizada. Denuncia que en demasiados casos esa fiscalización no se lleva a cabo, en ocasiones por la carencia de la formación necesaria para realizar las comprobaciones oportunas[595]. He defendido la imposibilidad de que el personal administrativo realice esa fiscalización debido a su carencia de formación técnica, convencida de que unos pocos cursos de informática no le aportan el conocimiento requerido. Pero más preocupante es la falta de formación del personal técnico al servicio de las Administraciones públicas, quienes, en principio, parecen idóneos para asumir esa función. Un desarrollador funcionario, con dilatada experiencia en programación con lenguajes como Cobol o Natural, difícilmente puede certificar la adecuación a los requerimientos de una aplicación informática programada en Java. La rápida evolución de los entornos tecnológicos puede conducir a ese problema; recordemos la afirmación de que la mitad de lo que hoy necesita conocer un ingeniero del *software* estará obsoleto en tres años.

La ausencia de la formación adecuada por parte de la ciudadanía también levanta una barrera a la implantación exitosa de la Administración electrónica. Contemplada en la exposición de motivos de la LAE es, junto con la falta de recursos económicos y

[595] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 70.

estadísticamente asociada a ella, causa de la brecha digital. Las campañas formativas en el campo de las nuevas tecnologías constituyen un ataque directo a esa brecha. La ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, ya consciente de ello, pretende potenciar las iniciativas de formación en las TIC[596]. Pero no basta con realizar acciones de divulgación; para logra una cultura de ciberseguridad se requiere una ingente labor formativa especializada para todos los sectores de la sociedad.[597]

La Fundación Telefónica, en su estudio de 2016 titulado "*Ciberseguridad, la protección de la información en un mundo digital"*[598], confirma la existencia de una cierta inercia en el comportamiento de los internautas en relación a la seguridad, al mantener hábitos de autoprotección desfasados, más propios de épocas en las que la conexión a Internet era algo puntual y las tecnologías estaban restringidas a actividades muy concretas, por lo que se considera imprescindible una adecuada concienciación y formación sobre los peligros que acechan y la forma de enfrentarse a ellos.

La imposibilidad de acceder a los servicios de Administración electrónica puede deberse a los más diversos motivos ajenos al ciudadano y conocidos por las Administraciones públicas[599], que sumirán al usuario en la desesperación, incluso tratándose de informáticos

[596] FERNÁNDEZ RODRÍGUEZ, J.J./ SANJURJO RIVO, V.A. (2010), acceder o no, 264-282.
[597] TOMÁS MORALES, S. DE. (2014), capacitación especializada, 15.
[598] TOMÁS MORALES, S. DE. (2014), capacitación especializada, 14.
[599] *Vid*. DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA, *MiniApplet*, 97-99. Allí declara un conjunto de problemas conocidos, como los errores al firmar ficheros mayores de 4 *megabytes*, la no aparición de los certificados de las tarjetas CERES en el diálogo de selección de certificados desde Mozilla Firefox en Windows, el bloqueo del *applet* con el navegador Mozilla Firefox y DNIe que provoca que no se muestre el diálogo de selección de certificados (se desbloquea al retirar el DNIe del lector), la no detección en ocasiones de la inserción o extracción del DNIe u otra tarjeta inteligente, situaciones en las que el *applet* no detecta ningún certificado bajo Mozilla Firefox y ocasiones en las que el *miniApplet* no permite la firma de archivos PDF con ciertos certificados.

profesionales. Las dificultades también pueden obedecer a problemas en la configuración del equipo del usuario[600], que requieren, para su resolución, una formación importante de la que carece la mayor parte de la ciudadanía, como disponer de la información sobre las versiones de los navegadores que son incompatibles con los *applets* de firma[601], las versiones del navegador o de Java que es necesario tener instaladas[602], lo que hay que añadir en la lista de excepciones de sitios de la pestaña de seguridad del panel de control de Java o cómo configurar los valores de seguridad de la pestaña denominada "avanzado", también del panel de control de Java. Incluso así, aún puede ser necesario añadir una excepción con la ruta del servidor de firma en la pestaña "servidores" del administrador de certificados.

Si la neutralidad tecnológica fuese una realidad, en lugar de un objetivo teórico imposible de alcanzar a fecha actual, el uso de la firma electrónica, quizá – aunque me permito dudarlo – no supondría una gran dificultad para la mayoría de la población, sin perjuicio de que debamos preocuparnos por un grupo nada despreciable de ciudadanos que, ya sea por edad o por educación, no están en condiciones de afrontar un cambio de las proporciones que supone la eAdministración diseñada por nuestras nuevas leyes[603]. Pero, en la actualidad, conseguir configurar un equipo en nuestros hogares o empresas que permita el uso satisfactorio de las aplicaciones públicas no siempre es sencillo[604]. El gran problema es su obligatoriedad, ampliada

[600] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 73.
[601] A fecha 22 de enero de 2017, Chrome no soporta *applets;* de Mozilla Firefox son compatibles las versiones entre v31.0 y v39.0; en Internet Explorer lo admite en las versiones v.7 o superiores.
[602] A fecha 22 de enero de 2017, es preciso contar con la versión 7 de Java o superior aunque, en ocasiones, ha sido necesario instalar una versión de 32 bits de Java.
[603] FERNÁNDEZ RODRÍGUEZ, T. R. (2015), notificaciones electrónicas, 363.
[604] En ocasiones, hasta puede ser inviable. Algunas Administraciones públicas hacen uso de aplicaciones que no admiten las versiones más recientes de Java, mientras que otras precisamente exigen la utilización de versiones más

de manera extraordinaria por la nueva ley 39/2015, a pesar de que son muchos los que no disponen de los conocimientos ni de los medios necesarios para entablar relaciones electrónicas, a lo que se añaden los problemas de usabilidad que suscitan muchas plataformas[605].

4.4. SEGURIDAD Y CONFIANZA

No puede ignorarse que la utopía de la seguridad total en un sistema informático es una meta inalcanzable[606], máxime cuando los recursos humanos y materiales para intentar obtenerla son finitos[607]. La seguridad es un compromiso que se basa en el equilibrio entre lo que cuesta recuperarse de los ocasionales incidentes y lo que gastaremos en protección y prevención[608]. Es preciso emplear esos recursos adecuadamente para lograr, a su vez, un equilibrio[609] entre la productividad que las tecnologías de la información otorgan a la

modernas. La disponibilidad de más de un ordenador en el hogar, cada uno configurado de forma diferente, es una carga excesiva para el ciudadano.

[605] GAMERO CASADO, E. (2016), panorámica.

[606] El propio Centro criptológico nacional (CCN) admite esa idea como punto de partida inicial y nos exhorta a prepararnos para que los incidentes de seguridad nos afecten en la menor medida posible, como indica en la página 96 de su guía/norma de seguridad de las TIC que lleva por título "Manual STIC" (CCN-STIC 400 versión 1.1) de fecha mayo de 2013.

[607] Puede obtenerse toda la información al respecto en el detallado informe REINA de 1 de enero de 2015, donde se recogen los indicadores más representativos de la situación y uso de los sistemas y tecnologías de la información y comunicaciones en la Administración del Estado. En su introducción nos recuerda que la Comisión de estrategia TIC realiza la recogida de "información de los recursos tecnológicos, humanos, económicos y de contratación relacionados con las tecnologías de la información" y publica en el Portal de Administración Electrónica (PAe) informes periódicos presentando los resultados de estos estudios.

[608] *Si no inviertes en seguridad corres un alto riesgo*. (2013). Instituto nacional de ciberseguridad, INCIBE. Recuperado de https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/si_no_inviertes_en_seguridad_corres_un_alto_riesgo (28 de febrero de 2016).

[609] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 279. El autor llama la atención sobre el siempre difícil equilibrio entre los derechos de los ciudadanos y la actividad de la Administración, señalando que esta se hace más poderosa gracias a las tecnologías de la información, lo que obliga a que el poder administrativo esté limitado, juridificado.

Administración y el máximo respecto a los derechos de los ciudadanos, con total sujeción al ordenamiento jurídico[610].

En la búsqueda de ese equilibrio en el seno de las propias Administraciones públicas, es frecuente el enfrentamiento entre el personal técnico, que persigue la efectividad práctica priorizando la solución técnica óptima sobre las "molestas" ataduras legales[611], y el jurídico, que impone el Derecho sobre la tecnología[612]. Convencidos de que la falta de reivindicación de la primacía del Derecho sobre la tecnología pone en riesgo los cimientos en los que se asienta nuestro modelo constitucional[613], los pocos profesionales técnicos que defendemos la sujeción al Derecho resultamos, como mínimo, "incómodos"[614]. Pero, sin duda, ese es el papel que esperamos hoy del Derecho administrativo, que se posicione a la vanguardia de los cambios, en lugar de supeditarse a ellos, que no vaya al remolque de las necesidades regulatorias, sino que se anticipe[615].

Para llegar a establecer dónde se sitúa el adecuado punto de equilibrio entre seguridad y productividad, es necesario realizar estudios cuantitativos de costes y beneficios, teniendo en cuenta que las Administraciones públicas no pueden olvidar valorar aspectos

[610] J.L. PIÑAR MAÑAS reflexiona sobre si la técnica está al servicio del Derecho o si es este el que está al servicio de aquella en el capítulo Revolución tecnológica y nueva Administración con el que abre la obra que él mismo dirige, *Administración electrónica y ciudadanos*, (páginas 25-39).
[611] Como indica el libro I – Método, de MAGERIT 3.0 en su página 11, "*hasta el mejor plan de seguridad se vería seriamente hipotecado sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria a las medidas, o tienen la percepción de pasarse el día "luchando contra las [absurdas] medidas de seguridad"*.
[612] Nos recuerda PIÑAR MAÑAS las palabras de LORENZO MARTIN RETORTILLO, "*la técnica no tiene por qué arrumbar al Derecho*", lo que, como añade, no siempre se cumple. En PIÑAR MAÑAS, J.L. (2011), revolución tecnológica, 27.
[613] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 397.
[614] Como sugiere LANGDON WINNER en su obra "La ballena y el reactor", encajaríamos en lo que los propios colegas describirían como "*maniáticos peligrosos y radicales*".
[615] GAMERO CASADO, E. (2015), mundo en disrupción, 1.

intangibles[616]. Volvemos a preguntarnos si el sector privado, movido por sus propias razones económicas, puede tomar decisiones en materia de seguridad del *software*, planteándonos la posibilidad de establecer una reserva funcionarial[617] a determinadas tareas del desarrollo de especial trascendencia pública.

El reglamento eIDAS destaca desde sus primeros considerandos la importancia que la creación de un clima de confianza en el entorno *on line* supone para el desarrollo económico y social[618]. Esa confianza tiene un importante papel en la configuración de las percepciones y de las respuestas de la sociedad ante los riesgos tecnológicos[619]. La exposición a los ciberataques no solo provoca elevados costes económicos, sino la pérdida de la confianza de los ciudadanos en estos sistemas que, en la actualidad, resultan críticos para el funcionamiento de la sociedad, como afirma la Estrategia de Seguridad Nacional de 2013.[620]

La confianza en la actuación racional, libre y fundada de los otros actores públicos y privados sería la situación ideal que no sentimos en la realidad cotidiana, la cual nos demuestra la necesidad de tomar medidas y articular principios que disciplinen el funcionamiento de las

---

[616] Nutridos ejemplos de valores intangibles pueden encontrarse en el artículo "El capital intelectual en el sector público" de BOSSI QUEIROZ, FUERTES CALLÉN y SERRANO CINCA. Los autores señalan el predominio de los objetivos cuantificables en el sector privado, ligados a la obtención de rentabilidad, a aumentar el valor de mercado de la empresa y a la obtención de beneficios. Sin embargo, los objetivos de las Administraciones públicas son frecuentemente no monetarios e incluyen aspectos como el grado de satisfacción de los ciudadanos sobre los servicios públicos y la calidad del servicio o su percepción de los usuarios.

[617] CANTERO MARTÍNEZ, J. (2013), criterios para la clasificación. La autora destaca que el legislador básico estatutario ha señalado algunos criterios básicos para la distinción de ambos colectivos, funcionarios y laborales, que nos conducen al terreno de los conceptos jurídicos indeterminados cuya concreción final se relega al posterior desarrollo legal que se realice para cada ámbito territorial.

[618] DAVARA FERNÁNDEZ DE MARCOS, L./ DAVARA RODRÍGUEZ, M.A. (2016), novedades.

[619] Según el estudio sobre la ciberseguridad y confianza en los hogares españoles de ONTSI, página 56, publicado en junio de 2016, en el segundo semestre de 2015, un 44% de los usuarios encuestados tiene mucha o bastante confianza en Internet, un 42,4% tiene suficiente confianza, mientras que el 13,6% afirma tener poca o ninguna confianza.

[620] AMICH ELÍAS, C./ VELÁQUEZ ORTIZ, A.P. (2014), la ciberdefensa y sus dimensiones, 60.

instituciones, para posibilitar y garantizar a los ciudadanos la fiabilidad de ese comportamiento, específicamente del poder público[621]. Dichas instituciones han adquirido el deber de proteger al público frente a diversos riesgos, incluso se podría decir que se legitiman ejerciendo esta función, por lo que la confianza en ellas para regular o controlar efectivamente los riesgos y tecnologías se suele considerar un factor esencial de su aceptabilidad.[622] Los técnicos y científicos han dispuesto los instrumentos necesarios, y así lo reconoce la LAE en su exposición de motivos, pero la generalización de la sociedad de la información, además del impulso recibido por parte de las Administraciones públicas, depende "*de la confianza y seguridad que genere en los ciudadanos* (…)". El primer escollo que encuentra la eAdministración en este camino puede ser el escepticismo de los juristas, de letrados de los organismos públicos, quienes no acaban de confiar en la suficiencia de esos instrumentos y tienden a entorpecer la efectiva implantación alegando impedimentos legales. De forma similar, la desconfianza de los ciudadanos en general, afirma Gamero Casado, solo se vence "*con prudencia y perseverancia en las acciones públicas*"[623].

En este sentido, la LAE declara entre sus fines el de la creación de las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, especialmente los relacionados con la intimidad y la protección de datos de carácter personal.

[621] CASTILLO BLANCO, F.A. (2003), principio de seguridad jurídica, 22.
[622] SOLÁ, R./ PRADES, A./ ESPLUGA, J./ REAL, M. (2009), confianza, incertidumbre y percepción social, 162-166.
[623] GAMERO CASADO, E. (2008), era de la información, 32-33.

Entre los colectivos que se muestran más recelosos se encuentran las personas mayores de cierta edad, el segmento de población menos acostumbrado al uso de Internet. Si bien es cierto que con su utilización va creciendo la confianza, esta se pierde de nuevo tras sufrir experiencias negativas, como los ataques por virus. En el extremo opuesto en cuanto a experiencia, aparecen los informáticos profesionales y los que se dedican laboralmente a la sociedad de la información, quienes, sin embargo, suelen ser muy desconfiados, pues son conocedores de la complejidad y debilidades implicadas[624] y sabedores del riesgo que un mal *software* puede suponer. Cantero Martínez relaciona la confianza con la publicación del código de esas aplicaciones informáticas[625], aspecto ya comentado *supra*.

Los constantes incidentes de seguridad de los que informan los medios de comunicación no ayudan a la generación de un clima de seguridad. En cualquier caso, tanto la confianza como la seguridad son sensaciones subjetivas, de carácter relativo, depende de nuestra percepción de cada situación concreta[626]. No se puede identificar seguridad con confianza. Ribagorda Garnacho, en una comparación muy acertada, recuerda como el medio de transporte estadísticamente más seguro, el avión, produce reacciones muy diversas entre los ciudadanos, que van desde la total confianza hasta el terror más absoluto a pesar de reconocer lo infundado de su temor[627]. Pero, a mayor seguridad, parece razonable esperar mayor nivel de confianza en la ciudadanía. Por ello, es preciso determinar conceptualmente qué es la seguridad y cómo

[624] ROIG BATALLA, A. (2009), intimidad y Administración electrónica, 735.
[625] CANTERO MARTÍNEZ, J. (2011), principio de transparencia, 320-321.
[626] MIRALLES LÓPEZ, R. (2009), modelos de evaluación, 751-753.
[627] RIBAGORDA GARNACHO, A. (2011), aspectos técnicos, 717.

incrementarla, lo que nos lleva directamente al terreno de las normas técnicas objeto del siguiente capítulo.

4.5. DIFICULTADES ESPECÍFICAS DE LAS ENTIDADES LOCALES DE MENOR TAMAÑO

Algunos puntos críticos de carácter interno condicionan la expansión de la eAdministración en las Entidades locales; se trata de los recursos humanos y materiales, los aspectos de carácter institucional y de cultura organizativa, y algunos problemas asociados al componente político de la toma de decisiones[628].

Las restricciones presupuestarias constituyen el principal problema a la hora de implantar las soluciones tecnológicas. La complejidad en la tramitación de las partidas plurianuales que, con frecuencia, son necesarias para los proyectos TIC, y las prioridades de los políticos, que no ven un retorno rápido de estas inversiones, obstaculizan la llegada de la eAdministración. La inexistencia de un departamento de informática con personal adecuadamente preparado para la implantación y posterior operación y mantenimiento, habitual en municipios con una población inferior a 20.000 habitantes, o su diversa o inadecuada ubicación en el organigrama de la entidad, acrecienta esas dificultades. Las iniciativas de cesión y de reutilización de *software*, si bien son de interés, llevan asociados problemas de escalabilidad y evolución de las aplicaciones. Sería más conveniente que esas Entidades locales de menor

[628] CRIADO GRANDE, J.I. (2004), usos y recursos, 300.

tamaño recibieran servicios adaptados a sus necesidades que puedan mantener sin necesidad de contar con personal especializado, en lugar de recibir tecnología que no puedan mantener[629].

En septiembre de 2016 se ha publicado una guía, editada por el MINHAP, orientada a facilitar el cumplimiento de las obligaciones introducidas por las nuevas leyes administrativas en materia de Administración electrónica a las Entidades locales[630].

5. NORMAS DE NATURALEZA TÉCNICA

En su resolución de 7 de mayo de 1985, el Consejo decidió introducir un "nuevo enfoque" en materia de armonización técnica y normalización, respaldado en el mismo año por el Libro blanco de la Comisión sobre la realización del mercado interior. Ponen de manifiesto la necesidad de superar las barreras impuestas por la existencia de diferentes reglamentaciones y normas técnicas de los diversos países miembros. Ese nuevo enfoque se fundamenta en el principio básico del reconocimiento mutuo de las normativas nacionales con objetivos equivalentes (considerando como tal a aquellas que compartan finalidad, aunque difieran en los medios para alcanzarla), de forma que la armonización legislativa a nivel comunitario es excepcional y se restringe a los casos restantes. Simultáneamente, se generalizó el uso de la técnica de armonización comunitaria basada en el reenvío a normas, que supone el abandono de la pretensión de regular directa y exhaustivamente todas las cuestiones, limitándose a recoger las exigencias esenciales[631]. El propio reglamento eIDAS invoca a normas y especificaciones

[629] FUNDACIÓN TELEFÓNICA (2008), Administración local, 233-234.
[630] MINHAP. (2016), uso de las herramientas tecnológicas.
[631] ÁLVAREZ GARCÍA, V. (1999), la normalización industrial, 356-359.

técnicas en numerosas ocasiones; entre ellas y a modo de ejemplo, su artículo 7.d, donde leemos "(…) *que el Estado miembro que efectúa la notificación garantice que los datos de identificación de la persona que representan en exclusiva a la persona en cuestión se atribuyen de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente* [632](…)".

El real decreto 1337/1999, de 31 de julio[633], por el que se regula la remisión de información a la Comisión europea y a determinados organismos de normalización, en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información, aporta un conjunto de definiciones clarificadoras a la hora de distinguir entre conceptos que podrían resultar inicialmente confusos. Basándose en ellas, podemos caracterizarlas esquemáticamente de la siguiente forma:

- **Especificación técnica:**
  - descripción que figura en el documento en el que se definen las características requeridas de un producto;
  - es un concepto general asumido por:
    - ✓ la normalización técnica, de carácter voluntario;
    - ✓ la reglamentación técnica, de carácter obligatorio;

[632] El subrayado es nuestro.
[633] La directiva 98/34/CE, a la que hace referencia el presente real decreto, ha sido derogada por el artículo 10 de directiva (UE) 2015/1535 del Parlamento europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

- ✓ los pliegos de condiciones generales de la contratación privada o pública[634].

- **Norma técnica:**
  - no es una norma jurídica[635];
  - es una especificación técnica aprobada por un organismo reconocido de actividad normalizadora internacional, europeo o nacional,
  - puesta a disposición del público para su aplicación repetida o continua,
  - de observancia no obligatoria,
  - consensuada, elaborada con la participación de las partes interesadas (fabricantes, usuarios y consumidores, laboratorios, administración, centros de investigación, etc.)[636].

- **Reglamento técnico:**
  - especificaciones técnicas u otros requisitos o disposiciones relativas a los servicios, incluidas las disposiciones administrativas que sean de aplicación,
  - de cumplimiento obligatorio, ya sea *de iure* o *de facto*;
  - el real decreto recoge una relación con algunos ejemplos de reglamentos técnicos *de facto*, concretamente:

[634] MOLES I PLAZA, R.J. (2001), Derecho y calidad, 70.
[635] MOLES I PLAZA, R.J. (2001), Derecho y calidad, 67.
[636] Este último punto se recoge en el documento MINISTERIO DE LA PRESIDENCIA (2010), normalización, 4.

a. Las disposiciones legales, reglamentarias o administrativas de un Estado miembro que remitan:

   - ✓ a especificaciones técnicas, a otros requisitos o a reglamentos relativos a los servicios, o
   - ✓ a códigos profesionales o de buenas prácticas que a su vez se refieran a especificaciones técnicas, a otros requisitos o a reglamentos relativos a los servicios, y cuya observancia confiere una presunción de conformidad a las prescripciones fijadas por dichas disposiciones.

b. Los acuerdos voluntarios de los que sean parte contratante los poderes públicos y cuyo objetivo sea el cumplimiento, por razones de interés general, de las especificaciones técnicas u otros requisitos, o de reglamentos relativos a los servicios, con exclusión de los pliegos de condiciones de los contratos públicos.

c. Las especificaciones técnicas u otros requisitos, o los reglamentos relativos a los servicios relacionados con medidas fiscales o financieras que afecten al consumo de productos o a la utilización de servicios, fomentando la observancia de dichas especificaciones técnicas u otros requisitos o reglamentos relativos a los servicios.

Las normas europeas son documentos de carácter voluntario que están llamadas a desempeñar un importante papel de apoyo a la estrategia 2020 para un crecimiento inteligente, sostenible e integrador, para lo que han de estar rápidamente disponibles, para garantizar la

interoperabilidad entre los servicios y las aplicaciones en el ámbito de las TIC; de lo contrario, dada la rápida evolución de las tecnologías, podrían quedar obsoletas incluso antes de ser adoptadas[637].

Por su carácter facultativo, el incumplimiento de la norma técnica nunca será sancionable, al no existir tampoco posibilidad de infracción; sin embargo, ha sido creada con la intención de alcanzar un elevado grado de uso, lo que constituye la base del denominado "derecho blando"[638].

En materia de las TIC son muy numerosos los organismos normalizadores dedicados a establecer los estándares a utilizar tanto por el sector público como por el privado, como son IEEE, W3C, OASIS o IEFT[639]. En el ámbito internacional, ISO es el organismo encargado de la normalización en todos los sectores de la técnica salvo en el campo eléctrico y electrotécnico, reservado para IEC. Cada país puede aportar un único organismo de normalización para integrarse en ambos. En España, es AENOR quien asume la responsabilidad internacional en ISO y en IEC. En Europa, el organismo que centraliza las actividades de normalización en materia de las TIC es CEN/ISSS.[640]

Son tres los tipos de normas que afectan a la Administración electrónica[641]:

- Normas semánticas: marcan el formato de los mensajes de intercambio definiendo un vocabulario común entre las dos partes que se comunican.

[637] COMISIÓN EUROPEA (2011), visión estratégica.
[638] MOLES I PLAZA, R.J. (2001), Derecho y calidad, 69-70.
[639] FUNDACIÓN TELEFÓNICA (2008), Administración local, 144.
[640] MINISTERIO DE LA PRESIDENCIA (2010), normalización, 4.
[641] FUNDACIÓN TELEFÓNICA (2008), Administración local, 145-146.

- Normas técnicas: de más bajo nivel que las anteriores, hacen referencia a temas diversos. En ellas se desarrolla con todo detalle los que los informáticos y el resto de personal técnico (nunca los ciudadanos) han de conocer para implementar el código que sustentará lo establecido por la norma administrativa[642]. A modo de ejemplo podemos citar las que determinan lo que se incluye en un certificado digital, o la estructura y modo de acceso de las listas de revocación.

- Normas de técnicas de gestión: tienen relación con el uso de las técnicas en el procedimiento administrativo. Sirve como ejemplo la regulación de la notificación electrónica.

En ocasiones, el legislador se enfrenta al desconocimiento del tema a regular. La intervención de comités científicos en la elaboración de las normas jurídicas, ya sean leyes o reglamentos, aporta una mejora objetiva de la calidad de la producción normativa, a través de una transformación subjetiva de sus fuentes de producción[643], lo que resulta ser una de las razones que genera desconfianza en la participación de dichos órganos. Esa intervención puede introducir demasiadas reglas tecnificadas, expresiones de ciencia o técnica o expresiones ambiguas[644].

En las ocasiones en que el tenor de la norma no pormenoriza todos los aspectos minuciosamente, será necesario completarla y, en ese sentido, el cumplimiento de la LAE ha requerido el desarrollo de un amplio conjunto de normas técnicas, allá donde no entra al

[642] FUNDACIÓN TELEFÓNICA (2008), Administración local, 281.
[643] MONTORO CHINER, M.J. (2003), seguridad jurídica, 338.
[644] MONTORO CHINER, M.J. (2001), técnica legislativa, 157.

detalle[645]. En España, estas normas de organismos estandarizadores, como AENOR, no son asimilables a actos administrativos, a diferencia de lo que ocurre en otros países cercanos, como Francia, donde sí son equiparables[646].

La referencia a normas técnicas privadas desde una norma jurídica tradicionalmente despierta el interés del jurista, especialmente en el ámbito del Derecho administrativo. La legitimidad de esas normas técnicas proviene del consenso en su adopción entre la comunidad científica, por lo que se plantea un problema cuando dichas normas, elaboradas por organismos[647] diferentes de las instancias políticas y de las Administraciones públicas, "*sobrepasan su propio espacio adquiriendo eficacia frente a terceros y ganando relevancia pública*".[648] Por la técnica de la remisión, habitual en el Derecho técnico y en el ambiental, el contenido de esas normas elaboradas por organizaciones privadas adquiere la validez y eficacia propia de la norma jurídica. Mediante estas cláusulas remisoras, principalmente usadas en normas reglamentarias, se garantiza una constante adaptación de la norma jurídica al estado de la técnica, evitando el desfase de la reglamentación. La norma técnica tiene, entonces, un carácter completivo de la jurídica[649]. Pero el reenvío dinámico de una norma jurídica a otra técnica, en su versión actual o futura, plantea serias reservas, por la pérdida de control sobre lo que a ella se incorpora, convirtiendo la norma jurídica remitente en una

[645] FUNDACIÓN TELEFÓNICA (2008), Administración local, 281.
[646] TARRÉS VIVES, M. (2003), normas técnicas, 159-160.
[647] Estos organismos de normalización se configuran habitualmente como entidades privadas sin ánimo de lucro.
[648] TARRÉS VIVES, M. (2003), normas técnicas, 156-158.
[649] TARRÉS VIVES, M. (2003), normas técnicas, 170-171.

norma en blanco o de contenido movible, dotando en la práctica al organismo privado con una potestad reglamentaria/legislativa no admisible constitucionalmente[650].

Más adecuada resulta la remisión indirecta a través de una "cláusula técnica", que invoca, de forma genérica, al estado de la técnica y de los conocimientos científicos, mejor tecnología disponible y otros conceptos jurídicos indeterminados similares. Con ello, el legislador renuncia a elaborar detalladamente la reglamentación técnica que, de otro modo, pronto devendría obsoleta aunque, con ello, introduce un componente valorativo o discrecional[651].

Las diferentes series de normas desarrolladas por los organismos de estandarización en materia de seguridad[652] de la información y del *software* sin duda son de gran utilidad, en ocasiones imprescindibles, para cualquier proyecto de desarrollo de aplicaciones. Centrándose en las previstas específicamente para su uso en las Administraciones públicas, la

[650] TARRÉS VIVES, M. (2003), normas técnicas, 178-179.
[651] TARRÉS VIVES, M. (2003), normas técnicas, 180-183.
[652] Podemos destacar la serie de normas ISO/IEC 27000, que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, o la UNE 71504, la cual ofrece una metodología de análisis y gestión de riesgos para los sistemas de información. Centradas en el ámbito de la criptografía, en MINISTERIO DE LA PRESIDENCIA, normalización, 13-15, destaca la ISO/IEC 18014 referente a los servicios de fechado electrónico, ISO/IEC 18033 sobre algoritmos de cifrado, ISO/IEC 10118 para funciones *hash*, ISO/IEC 9796 en relación a esquemas de firma digital que incorporen funcionalidades de autenticación e integridad, ISO/IEC 9798 para la autenticación de entidades, ISO/IEC 15946 para criptografía basada en curvas elípticas, ISO/IEC 11770 respecto a gestión de claves, ISO/IEC 13888 para sistemas de no repudio, ISO/IEC 15408 referente a los criterios de evaluación de la seguridad de las tecnologías de la información, ISO/IEC 18045 respecto a la metodología de evaluación de la seguridad e ISO/IEC TR 15446, que proporciona orientación para la producción de perfiles de protección.

normalización en materia de seguridad de las TIC se materializa en variados instrumentos técnicos (ENS, PILAR[653], MÉTRICA, MAGERIT…)[654].

5.1. EL ESQUEMA NACIONAL DE INTEROPERABILIDAD

La búsqueda de la interoperabilidad ha sido una constante durante años. Protagonista del real decreto 4/2010, de 8 de enero, en él se la define con las mismas palabras empleadas por la LAE, "*capacidad de los sistemas de información y de los procedimientos a los que dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos*". Martínez Gutiérrez lo reconduce hacia la idea de compatibilidad, refiriéndose al uso de estándares tecnológicos para garantizar la conectividad de equipos, plataformas o aplicaciones[655]. Gamero Casado lo equipara a "*un proceso de normalización que permite a un programa o sistema informático compartir la información con otros programas y sistemas y establecer comunicaciones con ellos*", destacando el ahorro de recursos económicos, temporales y humanos que logra tanto para la ciudadanía como para las propias Administraciones públicas[656].

Calificado por el mismo autor como "*un modelo vinculante, rígido y centralizado, algo sin precedentes en el panorama comparado y que sitúa a España en la vanguardia de las políticas de interoperabilidad*"[657], el real decreto regula el ENI en el ámbito de la

[653] Como explica en la página 284 de "*Las TIC en la Administración local del futuro*", la herramienta PILAR (procedimiento informático-lógico para el análisis y la gestión de riesgos) es de uso exclusivo para nuestras Administraciones públicas, requiere una licencia gratuita para su uso y sigue la metodología MAGERIT.
[654] MINISTERIO DE LA PRESIDENCIA, normalización, 6-7.
[655] MARTÍNEZ GUTIÉRREZ, R. (2011), cooperación y coordinación, 670.
[656] GAMERO CASADO, E. (2009), interoperabilidad, 292-294.
[657] GAMERO CASADO, E. (2009), interoperabilidad, 328.

Administración electrónica, dando cumplimiento a lo dispuesto por el artículo 42.1 de la LAE, conforme al cual habría de contener "*el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad*". El mismo tenor se reproduce de forma exacta en el artículo 156.1 de la ley 40/2015.

El legislador español trata de asegurar la interoperabilidad mediante la vía de la cooperación interadministrativa en un plano de igualdad, a diferencia del modelo italiano basado en un sistema de coordinación[658] donde la AGE impondría a las Administraciones autonómicas y locales sus normas de estandarización obligatorias respecto al diseño de aplicaciones, plataformas y programas[659].

El ENI se ocupa de las dimensiones organizativa (referida a la capacidad de colaboración para alcanzar los logros mutuamente acordados[660]), semántica (por la que la información intercambiada es interpretable de forma automática y reutilizable, normalmente gracias a las transmisiones de los datos mediante ficheros XML[661] con un formato previamente acordado) y técnica (a través del uso de estándares abiertos[662] que garanticen la independencia en

[658] En referencia a la diferenciación entre los principios de coordinación y de cooperación, Martínez Gutiérrez nos remite al estudio de la STC 214/1989, de 21 de diciembre.
[659] MARTÍNEZ GUTIÉRREZ, R. (2011), cooperación y coordinación, 673-676.
[660] GAMERO CASADO, E. (2009), interoperabilidad, 296.
[661] GAMERO CASADO, E. (2009), interoperabilidad, 296.
[662] En el Tecnimap de Murcia 2004 se presentó la comunicación titulada "El marco europeo de interoperabilidad. Recomendaciones de la industria de las tecnologías de la información y comunicación", cuyo autor, HUGO LUEDERS, destaca en la página 7 la importancia de distinguir los estándares abiertos del código fuente abierto. Mientras este último es un tipo de acuerdo de licencia que permite a los desarrolladores determinadas libertades para construir sobre el código fuente existente, los estándares abiertos hacen referencia a un tipo de marco técnico que acordado por las distintas compañías para asegurar una mayor interoperabilidad de sus productos.

la elección, la adaptabilidad al progreso y la no discriminación de los ciudadanos por razón de su elección tecnológica[663]). Contempla también los estándares e independencia en la elección de las alternativas tecnológicas, de las infraestructuras y servicios comunes, la reutilización, la interoperabilidad de la firma electrónica y de los certificados y de la conservación a lo largo del tiempo de los documentos electrónicos, remitiendo al ENS en cuanto a los aspectos de seguridad y cerrando su articulado con una llamada a la actualización permanente "*en paralelo al progreso de los servicios de Administración electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que le apoyan*".

Su disposición adicional primera enumera las normas técnicas de interoperabilidad[664] a desarrollar, de obligado cumplimiento para las Administraciones públicas[665], entre las que figuran las referentes al documento electrónico, la digitalización de documentos, el expediente electrónico, la política de firma electrónica y certificados de la Administración y los protocolos de intermediación de datos. Además, podemos encontrar dos guías de gran utilidad para la reutilización de aplicaciones informáticas.

Las normas técnicas de interoperabilidad[666] desarrollan un conjunto de aspectos técnicos sobre los cuales se consideró necesario entrar en un nivel de detalle y extensión excesivos para ser incluidos en el propio real decreto y, en ocasiones, con unas necesidades de

---

663 http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Esquema_Nacional_de_Interoperabilidad.html (23 de mayo de 2016).

664 http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#.V9Ugnq02tc0 (recuperado el día 11 de septiembre de 2016).

665 Como señala Gamero Casado, estas normas técnicas no se corresponden con las categorías generales dela normalización industrial, pues son reglas de obligado cumplimiento. Interoperabilidad y administración electrónica: conéctense, por favor (p. 329).

666 Siete de ellas publicadas en el BOE de 30 de julio de 2011.

actualización periódica que hacían inadecuada su inclusión en él[667]. En su elaboración han venido participando más de 200 expertos de ámbitos como el jurídico, las TIC o archivos, procedentes de la AGE, Comunidades autónomas, Corporaciones locales y Universidades, con la colaboración de Justicia[668].

De forma semejante a lo que observaremos en el ENS al referirse a la seguridad, el ENI también considera la interoperabilidad como un proceso integral en el que la debilidad de un sistema la determina su punto más frágil, que habitualmente es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Gamero Casado señala la extraordinaria importancia de incluir cláusulas administrativas particulares la exigencia a los desarrolladores de *software* de respetar las determinaciones en materia de interoperabilidad.[669]

Sin embargo, es preciso tener en cuenta que la información, hasta los datos más anodinos, puede ser analizada, disgregada, recompuesta y combinada para conseguir otra diferente a la que le sirvió de base[670]. Sin negar las virtudes de la interoperabilidad, hemos de alertar del riesgo que puede suponer la interconexión de diferentes bases de datos que puedan trabajar al unísono, permitiendo configurar perfiles de las personas[671].

Desde la óptica del desarrollo del *software* de las Administraciones públicas, la interoperabilidad resulta necesaria tanto para la transferencia de tecnología como para la

[667] AMUTIO GÓMEZ, M.Á. (2012), normas técnicas, 127-128.
[668] AMUTIO GÓMEZ, M.Á. (2012), normas técnicas, 144.
[669] GAMERO CASADO, E. (2009), interoperabilidad, 332.
[670] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 47.
[671] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 229-230. El autor alerta de este peligro también al referirse a bases de datos con información biométrica.

reutilización de aplicaciones de otras Administraciones públicas, en beneficio de una mayor eficiencia[672], como se verá. En este momento, basta con apuntar que, a la hora de seleccionar los estándares que van a ser utilizados por las Administraciones públicas, conforme al artículo 11 del ENI, ha de tenerse en cuenta su potencial de reutilización y la posibilidad de su implementación bajo diversos modelos de desarrollo de aplicaciones.

5.2. EL ESQUEMA NACIONAL DE SEGURIDAD

Para Molina Mateos, la seguridad cibernética es un bien jurídico que adquiere una dimensión institucional y supraindividual, cuyo objeto jurídico de protección inmediato es la seguridad colectiva. Añade que el desarrollo del ciberespacio se configura como un bien de alto valor que requiere seguridad como elemento imprescindible y necesita protección jurídica[673]. En nuestro ordenamiento jurídico y en el ámbito de las Administraciones públicas, el esquema nacional de seguridad afronta ese reto de acercarse al nuevo mundo tecnológico y, como indica su título, a su seguridad. Guardando paralelismo con el ENI, el objeto del ENS, previsto en el artículo 42.2 de la LAE, reiterado en el 156.2 de la ley 40/2015 y regulado por el real decreto 3/2010, consiste en el establecimiento de la política de seguridad en la utilización de medios electrónicos, entendiendo como tal el conjunto constituido por los principios básicos y los requisitos mínimos que permitan una protección adecuada de la información. Inspirado en la LAE, durante su elaboración se ha tenido en cuenta la normativa reguladora de materias como la protección de datos personales, la Administración electrónica, la firma electrónica, el DNIe…

[672] Preámbulo del real decreto 4/2010, de 8 de enero, por el que se regula el esquema nacional de interoperabilidad en el ámbito de la Administración electrónica, ENI.
[673] MOLINA MATEOS, J.M. (2015), aproximación jurídica, 8-11.

El ENS fue modificado[674] por el real decreto 951/2015, de 23 de octubre, al objeto de reforzar la protección frente a las ciberamenazas mediante una eficaz adecuación del mismo a la rápida evolución experimentada por las tecnologías y adecuarlo a la normativa europea, en particular al reglamento eiDAS, y a la nacional, en especial a los principios generales de la ley 40/2015.

En su introducción, el ENS declara su finalidad de crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Continúa indicando que persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Para ello, requerirá ser desarrollado y perfeccionado en paralelo a la evolución de los servicios.

Su Anexo IV nos ofrece la definición de seguridad de las redes y de la información, diciendo que se trata de "*la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y*

674 http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2015/Octubre/Noticia-2015-10-23-Aprobada-actualizacion-del-Esquema-Nacional-de-Seguridad.html#.V27D7DU2tsk

sistemas ofrecen o hacen accesibles", definición que ya parece encaminarnos hacia las que serán las "dimensiones" básicas de la seguridad, entre las que es poco habitual citar la trazabilidad.

El ENS enfoca la seguridad como un proceso integral que aúna todos los elementos técnicos, humanos, materiales y organizativos, excluyendo cualquier actuación puntual o tratamiento coyuntural, mientras centra su máxima atención en la concienciación de las personas que intervienen en el proceso y en sus responsables jerárquicos, para que "*ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad*". Contempla de forma conjunta medidas de prevención, detección y recuperación, las primeras orientadas a reducir la posibilidad de que las amenazas lleguen a materializarse, y las otras dos a atajar a tiempo los incidentes de seguridad. Considera distintas líneas de defensa y múltiples capas de seguridad, constituidas por medidas de naturaleza organizativa, física y lógica, reevaluadas y actualizadas periódicamente, justificadas y proporcionales al riesgo que traten de mitigar.

La consideración de la seguridad como función diferenciada lleva a distinguir entre el responsable de la información (aquel que determina los requisitos de la información tratada), el responsable del servicio (quien establece los requisitos de los servicios prestados) y, por último, el responsable de seguridad (quien ha de tomar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios). Específicamente dispone que la responsabilidad de la seguridad de los sistemas de información ha de estar diferenciada de la responsabilidad sobre la prestación de los servicios. Será la política de seguridad, obligatoria para todos los órganos superiores de las Administraciones públicas, la que detalle las

atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos. Sin embargo, esa obligatoriedad no existe en las empresas del sector privado. El INE aporta un dato preocupante para 2015: casi el 30% de las empresas con, al menos, 250 empleados, carece de una política de seguridad establecida. El porcentaje se eleva al 50% en el caso de empresas de 50 a 249 empleados, y continúa creciendo al disminuir el tamaño de la organización, hasta llegar al 90% en el caso de las empresas con menos de 10 empleados[675]. Consultando en el INE las empresas con actividad principal (grupos CNAE93) 722, correspondiente a "consulta de aplicaciones informáticas y suministro de programas de informática", en el año 2009 (último dato disponible), el 92,38% de ellas corresponde a menos de 10 empleados y otro 5,56% no alcanza los 50. Es decir, una aplastante mayoría de empresas suministradoras de *software* carece de política de seguridad, algo que, para las Administraciones públicas, sugiere la conveniencia, o más bien la obligación, de exigir en la contratación de servicios de desarrollo que los proveedores cuenten con ella.

El personal relacionado con la información y los sistemas ha de aplicar los principios de seguridad en el desempeño de su trabajo. Debe ser formado, estar informado de sus obligaciones en cuanto a la seguridad y ser supervisado para verificar el seguimiento de los procedimientos establecidos. Las normas de seguridad concretarán el significado y alcance del uso seguro del sistema.

De especial transcendencia es la exigencia de identificación única de cada usuario que acceda al sistema, recogida en el artículo 14.4, a los efectos de poder exigir

[675] FUNDACIÓN TELEFÓNICA (2016), ciberseguridad, 16.

responsabilidades. Ha de saberse en todo momento quién recibe derechos de acceso, de qué tipo son y quién ha realizado cada actividad, lo que permitirá, como ordena el artículo 23, el registro de las actividades de cada usuario, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa, todo ello con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y conforme a la normativa de protección de datos. La importancia de obtener y conservar estos registros de actividad será evidente *infra*, tras analizar el caso juzgado en la STSJ de Madrid 1140/2015, sala de lo contencioso, de fecha 30 de enero de 2015, desfavorable para un trabajador a quien le han desaparecido casi ocho años de cotización, a pesar de poder probar su existencia en el fichero en numerosas ocasiones anteriores.

El ENS establece la necesidad de que se diseñen y configuren los sistemas de forma que se garantice la seguridad por defecto, señalando unos requisitos que difícilmente podrán lograrse, salvo que desarrollen a medida. Por ello, este será un aspecto a tener en cuenta a la hora de comenzar los trabajos de obtención de un nuevo *software* o al redactar los pliegos de prescripciones técnicas para los contratos de servicios a licitar.

Por último, hay que señalar la necesidad de garantizar la protección de la información almacenada o en tránsito en entornos inseguros como equipos portátiles, asistentes personales (PDAs), dispositivos periféricos, soportes y comunicaciones sobre redes abiertas o con cifrado débil.

Su artículo 29 prevé la elaboración de unas guías de seguridad TIC por parte del CCN, muy útiles y detalladas, con un nivel técnico elevado. A su vez, dispone la aprobación por el MINHAP de unas instrucciones técnicas (al menos las inventariadas en la disposición adicional 4ª), obligatorias para todos los organismos públicos, en las que se tendrán en cuenta las normas armonizadas a nivel europeo que resulten de aplicación, habiéndose publicado las dos primeras (informe de estado de la seguridad y conformidad con el ENS) en el BOE de 2 de noviembre de 2016.

Como principal deficiencia del ENS cabe citar la ausencia de consecuencias expresas de su incumplimiento, salvedad hecha de la medida cautelar de posible retirada de información o de servicios en sistemas de categoría alta. Quizá el temor de una posible paralización de los servicios públicos ha guiado tal omisión[676]. Sin embargo, esa permisividad podría cambiar próximamente en aquellos casos que afecten a la protección de datos de carácter personal, gracias al RGPD europeo, cuyo artículo 83.7 abre la puerta a la posibilidad de habilitar la imposición de multas administrativas a autoridades y organismos públicos[677].

5.2.1. Dimensiones de la seguridad

El concepto de seguridad, referido al ámbito de las TIC, parece tener unos perfiles borrosos. Ya se ha comentado en diferentes ocasiones cómo el legislador utiliza palabras como seguridad, confidencialidad, disponibilidad, integridad, no repudio, autenticidad… con un criterio dudoso. Por ello, resulta encomiable la elaboración del ENS a la hora de clarificar estas

[676] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 184.
[677] PIÑAR MAÑAS, J.L. (2016), nuevo modelo europeo de protección de datos, 16.

nociones, esfuerzo realizado con el fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas y de poder establecer la categoría de estos. La determinación del nivel de seguridad de cada una de las dimensiones y, en consecuencia, de la categoría del sistema, indicará las medidas que, como mínimo, habrá que implementar. Es importante en los proyectos de la eAdministración que esa valoración se realice en el momento en que se diseña la aplicación, permitiendo así la denominada *Privacy By Design*, no con posterioridad[678]. Por ello, el responsable del tratamiento ha de revisar la metodología empleada para asegurarse de que se cumplen los principios de privacidad desde la fase de diseño, sin requerir que se deban añadir controles tardíos al producto o al servicio[679].

Distingue el ENS cinco dimensiones a tener en cuenta para valorar los sistemas: autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad. Todas ellas son partes de un mismo todo y, en su conjunto, conforman el concepto genérico que entendemos como seguridad.

5.2.1.1. Autenticidad/autenticación

El ENS define la autenticidad como la "*propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos*".

[678] TRONCOSO REIGADA, A. (2011), la Administración electrónica, 270.
[679] CARPIO CÁMARA, M. (2016), seguridad del tratamiento, 345.

Coincide textualmente con la utilizada en MAGERIT 3.0[680], extraída de la norma UNE 71504:2008.

A tenor de las explicaciones ofrecidas por la guía 803, a la hora de valorar un sistema, el nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica[681]. Hemos de recordar aquí el principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones públicas a través de medios electrónicos, reconocido por la LAE en su artículo 4.h), principios que ahora la ley 40/2015 invoca en su preámbulo y exige para la sede electrónica.

El CCN nos recuerda que no debería acceder a un sistema quien no hubiera sido autorizado para ello, aspecto importante cuando se tiene que garantizar la privacidad de los datos gestionados por la propia Administración pública. Garantizar los procesos de autenticación y control de acceso constituye otras de las máximas de la seguridad, recordando que han de verse como una garantía para la protección de la información, no como una incomodidad. Sin embargo, la autenticación no se limita al control de accesos. Existen otros aspectos, como la segregación de funciones o la implementación de mecanismos de bloqueos, abarcados por esta dimensión, íntimamente relacionada con la trazabilidad, pues sin poder saber quién ha realizado una determinada actuación sería imposible remediar situaciones o establecer responsabilidades[682].

[680] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 16.
[681] CCN (2011), CCN-STIC-803, 6.
[682] CCN (2014), CCN-STIC-850A, 12-13.

De las 75 medidas de seguridad contempladas por el ENS, 50 de ellas afectan a la autenticidad[683]. Si bien inventariar cada una en estas líneas no aportaría mayor utilidad, sí parece adecuado mencionar dos de ellas, llamadas “mecanismo de autenticación” y “protección de la autenticidad y de la integridad”.

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Figura 5: Mecanismo de autenticación

Fuente: BOE de 4 de noviembre de 2015, 104255.

Como indica la figura 5, las exigencias de la medida de seguridad “**mecanismo de autenticación**” son mayores cuanto más elevado sea el nivel de seguridad requerido.

De forma genérica, el ENS permite usar como factores de autenticación, solos o combinados, los siguientes[684]:

– "algo que se sabe": contraseñas o claves concertadas.

– "algo que se tiene": componentes lógicos, como los certificados *software*, o dispositivos físicos (*tokens*).

– "algo que se es": elementos biométricos[685].

[683] Puede consultarse la tabla publicada en el BOE de 4 de noviembre de 2015, 104250-104252.
[684] La determinación de los mecanismos concretos a utilizar en cada sistema, en función de su nivel, excede del ámbito del ENS y, conforme a lo dispuesto en su artículo 29, se desarrolla en las guías CCN-STIC, elaboradas por el Centro criptológico nacional.

Para proporcionar credenciales[686] de autenticación a los usuarios, han debido de identificarse y registrarse previamente de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración, mediante la presentación física del usuario y verificación de su identidad ante un funcionario habilitado para ello o de forma telemática, ya sea DNIe o certificado electrónico cualificado o bien utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos que estén contemplados en la normativa de aplicación.

En sistemas de nivel bajo, en principio se admite cualquier mecanismo de autenticación sustentado en un solo factor. En el caso de "algo que se sabe" (contraseñas o claves concertadas), han de aplicarse unas reglas básicas de calidad, aunque no es raro que se incumplan incluso en sistemas de nivel alto. El mero hecho de que una Administración pública adquiera un paquete comercial diseñado y destinado para gestionar datos personales clasificados como de nivel alto por la LOPD, en un sistema de categoría alta según en ENS, en el cual se admiten como credenciales válidas el nombre de usuario "1234" con contraseña "1234", pone de manifiesto un total desconocimiento en materia de seguridad, pero aún resulta más preocupante que los usuarios de esa aplicación realmente utilicen tales nombres y contraseñas, lo que ya

[685] JAVIER y TERESA AREITIO analizan las técnicas biométricas en el trabajo titulado "Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación. En la página 52 realizan un breve recorrido por las tecnologías biométricas, como el iris, voz, geometría de la mano, rostro o huella dactilar, medidas del cráneo, termografía facial, patrón de venas de las manos, lóbulos de la oreja, exploración de la retina, huella de la mano, firma manuscrita, dinámica de introducción de teclas sobre un teclado, pigmentación y desarrollo de las uñas, forma de andar o de gesticular, reflectividad óptica de la piel, ADN... Resulta interesante también la lectura del artículo de Diego Alejandro Álvarez sobre la "identificación biométrica en gemelos" de 2014 y la comparativa ofrecida por RedIRIS entre algunas de estas técnicas, en la URL https://www.rediris.es/cert/doc/unixsec/node14.html (6 de julio de 2016). A su vez, el CCN ha dedicado una de sus guías a este tema, "Guía de seguridad de las TIC (CCN-STIC-490) - dispositivos biométricos de huella dactilar" de diciembre de 2007.

[686] El ENS denomina credenciales a las instancias del factor o los factores de autenticación que se utilicen en el sistema.

revela la inmensa necesidad de formar y concienciar a los empleados públicos. Dado que tal paquete comercial no se puede modificar y adaptar a las necesidades de nuestros organismos públicos, al no tratarse de *software* desarrollado a medida, si el usuario pone en peligro la confidencialidad de la información por incumplir las normas básicas de calidad de las contraseñas, la sanción disciplinaria parece ser la única medida que se puede adoptar.

Establece el ENS, en esta medida de seguridad, que las credenciales se activarán una vez estén bajo el control efectivo del usuario, se mantendrán bajo su control exclusivo y se cambiarán con una periodicidad adecuada a lo establecido en la política de seguridad y a la categoría del sistema concreto. El control exclusivo implica el uso individual, no la utilización de la misma clave por todo el personal de un determinado departamento. Pero, suponiendo que existiese alguna razón imperiosa que obligara a compartir una clave entre varios trabajadores, como puede ser el agotamiento del número de licencias disponibles, debería ser inmediatamente cambiada tan pronto como una de esas personas abandone el equipo de trabajo. Especial gravedad presenta este punto cuando el uso de la clave compartida se realiza por un equipo de desarrolladores de *software* externo a la Administración, donde es habitual el desfile constante de programadores que son contratados por la empresa adjudicataria del servicio y que la abandonan por diferentes motivos algún tiempo después. La problemática descrita culmina cuando dentro del propio *software* destinado a las Administraciones públicas figuran escritos usuarios y contraseñas de otros servicios, que rara vez llegan a cambiarse. Los desarrolladores que abandonan la empresa se van con el conocimiento del funcionamiento del programa, de las claves de acceso al código y de las contraseñas de otros sistemas, unos conocimientos muy útiles

para aquel en quien habite una vocación latente de *hacker*, para quien un acuerdo de confidencialidad[687] no supondrá ningún impedimento para sus ilegales intenciones.

El ENS establece la obligación del usuario de reconocer su recepción y el conocimiento y aceptación de las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el compromiso de informar de forma inmediata en caso de pérdida. Continúa estableciendo el ENS que las credenciales se retirarán y serán deshabilitadas cuando la persona, equipo o proceso que autentican termine su relación con el sistema.

Para los sistemas de nivel medio, el ENS exige la utilización de, al menos, dos factores de autenticación. Para el supuesto en que uno de ellos sea "algo que se sabe" refuerza la exigencia rigurosa de calidad y renovación. Dispone además que las credenciales hayan sido obtenidas tras un registro previo presencial o telemático, en este caso usando certificado electrónico cualificado o bien mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Para los sistemas de nivel alto, dispone la suspensión de credenciales tras un periodo definido de no utilización. Para el empleo de "algo que se tiene", se requerirá el uso de elementos criptográficos *hardware* usando algoritmos y parámetros acreditados por el CCN. Las

[687] El apéndice VI del documento “CCN-STIC-821- Normas de Seguridad en el ENS. Acuerdo de confidencialidad para terceros. NP50” lo considera como una garantía formal por duración indefinida y un compromiso de los terceros de que la información a la que pudiera tener acceso no va a ser divulgada más allá de los usos previstos para ella.

credenciales deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+	++

Figura 6: Protección de la autenticidad y de la integridad

Fuente: BOE de 4 de noviembre de 2015, 104261.

La medida de seguridad "**Protección de la autenticidad y de la integridad**" se incluye dentro del bloque correspondiente a las comunicaciones y afecta a ambas dimensiones. Su importancia la pone de manifiesto Troncoso Reigada cuando señala que la implantación de medidas de seguridad que garanticen la conservación de la información administrativa e impidan su alteración (indebida, se entiende) "*es imprescindible para la tutela de los derechos y el normal funcionamiento de la actividad administrativa, ya que no es posible asumir la validez de un documento administrativo si no se encuentra garantizada su autenticidad y su integridad*"[688].

Se admite cualquier mecanismo de autenticación previsto en la normativa aplicable. En el supuesto de utilización de claves concertadas, cuando el nivel sea medio o alto respectivamente, han de aplicarse exigencias medias o altas en cuanto a su calidad. Para el nivel bajo se debe asegurar la autenticidad del otro extremo de un canal antes de intercambiar información, así como prevenir la alteración de la información, la inyección de información

[688] TRONCOSO REIGADA, A. (2011), la Administración electrónica, 268.

espuria y el secuestro de sesión, garantizando su detección y activando los procedimientos preestablecidos.

Para el nivel medio ha de emplearse un acceso por VPN cuando la comunicación discurra por redes fuera del propio dominio de seguridad, empleando algoritmos acreditados por el CCN.

Para el nivel alto se valorará positivamente el empleo de dispositivos *hardware* en el establecimiento y utilización de la VPN. El ENS dispone el uso de productos certificados cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a ISO/IEC 15408 u otras de naturaleza y calidad análogas, y cuyos certificados estén reconocidos por el ENECSTI[689].

En ocasiones, puede resultar adecuado compatibilizar la acreditación de la identidad en la relación electrónica con la confidencialidad y la preservación de la intervención del ciudadano, en ciertos ámbitos como la presentación de quejas, sugerencias, peticiones… Para ello puede ser de gran utilidad práctica el uso de los nuevos certificados con pseudónimo[690] (aunque, como señala la AEPD, el pseudónimo no es equivalente a la anonimización, puesto que el pseudónimo siempre es reversible[691]).

[689] Puede encontrarse información sobre el ENECSTI en la URL http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_evaluacion_y_certificacion_de_la_seguridad/pae_Seguridad_Evaluacion_Esquema_Nacional.html (10 de julio de 2016).
[690] COTINO HUESO, L. (2008), derechos del ciudadano, 211.
[691] AEPD (2014), guía para una evaluación de impacto, 15.

5.2.1.2. Integridad

Introduciendo el tema con un supuesto real, lo que parece ser una pérdida de autenticidad y/o de integridad de la información albergada en los ficheros de la Administración, posteriormente detectada y reparada, llevó a que el 20 de mayo de 2011, el Juzgado de instrucción número 3 de Marbella condenara por sentencia firme a un ciudadano como autor de un delito contra la seguridad vial, contemplado por el artículo 384 del CP, tras conducir su vehículo sin que legalmente pudiera hacerlo, debido a la pérdida total de sus puntos y, por ello, de la vigencia de su permiso de conducción. Casi dos años más tarde, la Jefatura provincial de tráfico de Málaga emitió una certificación reconociendo que, como consecuencia de errores informáticos, el afectado hacía perdido puntos de forma improcedente, por lo que, en el momento del supuesto delito, conducía legalmente habilitado para ello. La sentencia fue anulada en procedimiento de revisión por la sala de lo penal del Tribunal Supremo cuatro años después de haber sido dictada[692].

El ENS define la integridad como la "*propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada*", coincidente con la utilizada en MAGERIT 3.0[693] y extraída de la norma ISO/IEC 13335-1:2004.

La guía 803 indica que el nivel de seguridad requerido en el aspecto de integridad depende de las consecuencias que tendría su modificación por alguien que no está autorizado para ello[694].

[692] STS 3168/2015 de 10 de Julio de 2015.
[693] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 15.

Sin embargo, al concepto de integridad se le asocian frecuentemente otras interpretaciones, no necesariamente incompatibles. Un encargado de seguridad podría añadir a esa definición las palabras "*sin ser descubierto*". En cambio, el administrador de la base de datos suele asociar el concepto de integridad a la exigencia de que los datos sean precisos, válidos y coherentes. Quien diseñe el modelo de datos entenderá por integridad la existencia de tablas con claves primarias únicas no nulas, es decir, la ausencia de duplicados en el conjunto de datos y la presencia de una clave con la que acceder de forma exclusiva a cada una de las entidades. El experto en la materia que se ha informatizado podría identificar la integridad de los datos como la comprobación de que la relación entre las distintas entidades se ajusta a lo previsto en las reglas de negocio. Para el proveedor, la integridad se establece en la etapa de diseño de la base de datos mediante la aplicación de un conjunto de reglas y procedimientos estándar, se mantiene mediante rutinas de validación y verificación de errores y se evidencia por la ausencia de datos alterados entre dos actualizaciones del mismo registro[695]. Todas son visiones diferentes referidas a la misma cuestión.

La medida de protección "mp.com.3", llamada "**Protección de la autenticidad y de la integridad**", comentada en el apartado anterior, afecta también, como su propia denominación indica, a la dimensión de integridad.

Un aspecto con frecuencia olvidado es la integridad del *software*, de los ficheros que lo contienen. Analizando si su contenido ha cambiado desde su creación, ya sea por error, por cortes en la comunicación, por inyección de código malicioso… podría tratar de determinar

[694] CCN (2011), CCN-STIC-803, 6.
[695] GELBSTEIN, E. (2011), la integridad.

si se mantiene la integridad del mismo. Incluso en entornos de código abierto con código fuente accesible, la revisión de este para saber si ha sido alterado es un procedimiento inadecuado en la práctica, a consecuencia del tamaño de los programas. Por tanto, es posible que el *software* a descargar, incluso de páginas de las propias Administraciones públicas, haya sido alterado y no esté libre de *malware*. Para comprobar la integridad de los ficheros puede recurrirse a funciones *hash*, firma digital y uso de certificados[696], ya comentados.

Durante años los empleados públicos, carentes de soluciones informáticas que resolviesen sus necesidades operativas, han venido sobreviviendo al quehacer diario mediante el uso de herramientas ofimáticas, como las populares hojas de cálculo Excel o bases de datos Access, obteniendo, en muchas ocasiones, auténticas aplicaciones informáticas sobre las que sustentar su negocio. Las primeras representan un gran riesgo para la integridad de la información, y ambas incumplen incluso las previsiones más básicas establecidas por el ENS. Sin embargo, un simple vistazo a los equipos de las diferentes oficinas públicas, nos lleva a estimar en miles el número de estas soluciones informáticas, lo que representa un importante problema presupuestario y operativo. La adaptación de los sistemas informáticos de las Administraciones públicas al ENS puede y debe llevar como consecuencia la desaparición de ese tipo de herramientas ofimáticas, disparando así la necesidad imperiosa de contratar a empresas de servicios para desarrollar aplicaciones sustitutivas, al verse desbordados los recursos humanos informáticos internos disponibles, generando unos gastos imposibles de satisfacer y obligando, por tanto, a los distintos organismos a incumplir el ENS, a trasladar sus Excel o Access fuera de la red corporativa o a dejar de prestar el nivel de servicio requerido. Surge también la cuestión de

[696] INTECO (2011), cómo comprobar la integridad de los ficheros.

a quién le corresponde solucionar el problema, que suele pasar de mano en mano buscando dónde ser resuelto, vagando desde el empleado público que gestiona los datos, salpicando al usuario que creó la hoja de cálculo, aterrizando en el departamento de informática para, finalmente, convertirse en una molesta cuestión que planea sobre todos ellos en su conjunto[697].

Ataques contra la integridad intencionados son cada día más frecuentes, poniendo en evidencia que el ser humano sigue siendo el punto más débil de la seguridad. Un virus puede infectar nuestros equipos por impericia o inconsciencia, pero también el *malware* puede llegar hasta ellos intencionadamente, escondiendo bombas lógicas en el código de los programas por parte de aquellos que están encargados de programarlos. Se consideran como un ataque a la integridad de los datos las modificaciones no autorizadas de sistemas operativos, la introducción de puertas traseras en las aplicaciones o cambios no consentidos en las tablas de las bases de datos, en la información almacenada en los entornos de producción o en la configuración de la infraestructura[698].

La responsable de la protección de la integridad es la unidad de negocio, no el departamento de informática (tampoco si este es un servicio externo). Entre las tareas indispensables se encuentra el mantenimiento actualizado de los privilegios de acceso. El ENS considera la integridad como afectada por las medidas de seguridad del marco operacional correspondiente al control de acceso comprendidas entre la “op.acc.2” y “op.acc.7” (requisitos de acceso, segregación de funciones y tareas, proceso de gestión de derechos de acceso, mecanismo de autenticación, acceso local y acceso remoto).

[697] GELBSTEIN, E. (2011), la integridad, 2.
[698] GELBSTEIN, E. (2011), la integridad, 3.

Constituye un riesgo importante no suprimir los permisos ostentados por un empleado una vez que ha finalizado su prestación de servicios en esa unidad o en esa actividad. El peligro se incrementa cuando el trabajador dispone de libre acceso a los datos de producción y al código fuente, como es habitual en el personal informático. "*Cuando un usuario está en condiciones de omitir los procedimientos de control de cambios, existe el riesgo de que se produzcan daños serios*"[699]. Si ese personal informático además es personal externo, ese riesgo se encuentra fuera de control.

5.2.1.3. Confidencialidad

La ley 39/2105, en su artículo 13.h), reconoce el derecho de las personas a la confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones públicas. El ENS define esa confidencialidad como la "*propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados*", literalmente coincidente con la contemplada por MAGERIT 3.0[700], extraída de la norma UNE-ISO/IEC 27001:2007. Sin duda es una interesante definición que lleva a cuestionar el funcionamiento de la plataforma de intermediación de datos, donde se pone a disposición de miles de empleados públicos la información de millones de ciudadanos que no les han autorizado a disponer de ella.

[699] GELBSTEIN, E. (2011), la integridad, 4.
[700] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 15.

El nivel de seguridad requerido en el aspecto de confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información[701].

Como máxima perseguida por el ENS, la confidencialidad establece un conjunto muy variado de medidas que aplicarán condicionantes para la salvaguarda de los datos, impidiendo que personas no autorizadas puedan acceder a ellos, dando así forma a la última barrera de protección que se aplicará para garantizar la seguridad de un sistema frente a un atacante. Los mecanismos empleados van desde la propia salvaguarda de la contraseña que se almacena de forma no legible, a la implementación de protocolos que emplean cifrado, como HTTPS, alternativa a protocolos inseguros por el envío en claro como el propio HTTP. El CCN[702] advierte de la necesidad de cambiar estos mecanismos con el paso del tiempo, recordando que, aunque se hable de algoritmos de cifrados o protocolos seguros, no todos son tan fiables como se diseñaron en un principio[703].

dimensiones	C		
nivel	bajo	medio	alto
	No aplica	aplica	+

Figura 7: Protección de la confidencialidad

Fuente: BOE de 4 de noviembre de 2015, 104260.

[701] CCN (2011), CCN-STIC-803, 6.
[702] CCN (2014), CCN-STIC-850A, 13.
[703] Para consultar los algoritmos que pueden emplearse y los que no, hay que recurrir a la *guía CCN-STIC-807 sobre Criptología de empleo en el Esquema Nacional de Seguridad*.

La medida denominada "**protección de la confidencialidad**" se aplica al nivel medio y, con mayores exigencias, al nivel alto. En el nivel medio requiere el empleo de VPN cuando la comunicación discurra por redes fuera del propio dominio de seguridad, así como el uso de algoritmos acreditados por el CCN. Para el nivel alto se prefiere la utilización de dispositivos *hardware* en el establecimiento y utilización de la VPN y el empleo de productos certificados cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a ISO/IEC 15408 u otras de naturaleza y calidad análogas, y cuyos certificados estén reconocidos por el ENECSTI.

El ENS incluye más medidas de seguridad que afectan a la confidencialidad, entre ellas la mayor parte del bloque de "control de acceso" y otras individuales como "criptografía", "borrado y destrucción", "calificación de la información", "cifrado", "limpieza de documentos"… Incluso un error de programación puede provocar la pérdida de confidencialidad con importantes consecuencias. Con fecha 12 de junio de 2013 se desestimó el recurso interpuesto por una compañía telefónica ante la sanción impuesta por la AEPD por haber comunicado a uno de sus clientes, al entrar en el portal *web* para ver sus propias facturas, las correspondientes a terceros, emitidas a nombre de otras personas, donde figuraban nombre y apellidos, dirección completa, NIF y número de cuenta bancaria parcialmente anonimizada, así como líneas y tarifas contratadas, consumos, SMS enviados y llamadas efectuadas, persistiendo el problema durante casi cinco meses desde que la compañía tuvo conocimiento de los hechos. La empresa alegó que los datos erróneamente mostrados no eran reales, sino creados al azar por un error informático. La sala de lo contencioso de la Audiencia nacional consideró probada la

cesión de datos personales reales, un fallo informático diferente del que alegaba la compañía, y confirmó la sanción de 12.000 € de multa[704].

Es importante recordar que el ENS y la normativa de protección de datos de carácter personal no son excluyentes, sino complementarios. La aplicación de las medidas de seguridad previstas en el ENS no excusa la implantación de las previstas por la LOPD y sus normas de desarrollo. La jurisprudencia interpreta el artículo 9 de la LOPD como una obligación de resultado consistente en la implementación de esas medidas de seguridad de forma que resulten efectivas[705].

5.2.1.4. Disponibilidad

En el ámbito de la conducción de vehículos a motor, un ciudadano recurrió una denuncia por circular sin haber contratado el seguro obligatorio de responsabilidad civil. Sin embargo, en la fecha de la denuncia, su seguro se encontraba en vigor, no estando disponible esa información a consecuencia de un fallo informático[706].

El ENS define la disponibilidad como la "*propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren*". Este tenor coincide literalmente con la descripción utilizada en MAGERIT[707], extraída de la norma UNE 71504:2008.

[704] SAN 2723/2013 de 12 de junio de 2013, sala de lo contencioso.
[705] FJ4. de la Sentencia de la Audiencia nacional 4419/2011, sala de lo contencioso, de 6 de octubre de 2011, entre otras.
[706] Sentencia del Juzgado contencioso administrativo n° 1de Lleida 320/2016 de 15 de marzo de 2016.
[707] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 15.

El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita[708]. Pero la disponibilidad no debe entenderse en términos absolutos, sino que se considerará compatible con la producción de breves interrupciones requeridas por motivos técnicos y anunciadas con la suficiente antelación[709].

El CCN describe la disponibilidad como "*uno de los pilares fundamentales para garantizar el objetivo estipulado para la Administración pública: ofrecer un servicio*", concluyendo que, ante las adversidades han de darse las condiciones para que el servicio pueda seguir ofreciéndose, señalando que las medidas serán más amplias y necesarias según aumente en criticidad el servicio prestado[710].

La valoración de la disponibilidad es absolutamente casuística. Para determinadas informaciones o servicios, es posible que no se generen daños apreciables por una interrupción que se prolongue a lo largo de varios días, mientras que para otros podría desencadenarse una situación crítica en cuestión de minutos[711].

Las consecuencias de la indisponibilidad del servicio o de la información pueden repercutir muy perjudicialmente en el ciudadano. Las coyunturas imaginables serían innumerables e incluirían fallos en el *software*, caída de los servidores, problemas en las redes de transmisión,…

[708] CCN (2011), CCN-STIC-803, 6.
[709] VALERO TORRIJOS, J. (2008), acceso a los servicios, 245.
[710] CCN (2014), CCN-STIC-850A, 11-12.
[711] *Vid.* "El valor de la interrupción del servicio" en la página 26 del libro I – Método, de MAGERIT 3.0.

La seguridad informática con frecuencia camina de la mano de la seguridad jurídica. Afirma Cotino Hueso que el derecho a la relación electrónica implica la seguridad jurídica del ciudadano en esa relación. El principio *in dubio pro* administrado podría dirigir la respuesta en casos polémicos no afrontados aún por el legislador, donde el ciudadano vea frustrada su confianza legítima en la interactuación electrónica. Continúa recordando el mismo autor cómo Valero Torrijos se pronuncia en el mismo sentido, llegando a afirmar el derecho a la ampliación del plazo de presentación respectivo cuando confluyan dos circunstancias: imposibilidad de la presentación imputable en exclusiva a la Administración e indisponibilidad del servicio prolongada durante una parte considerable del periodo o acontecida el último día del plazo concedido[712].

El CCN recuerda la exigencia de implementar procedimientos ante contingencias, sin limitarse solo al establecimiento de soluciones tecnológicas, y cita, en una enumeración no exhaustiva, algunas de las medidas de seguridad aplicables, como el dimensionamiento de los servicios, el usos de sistemas, medios, instalaciones y personal alternativos, la gestión de copias de seguridad, la vigilancia de las condiciones de mantenimiento del suministro eléctrico o la protección frente a incendios o inundaciones[713].

A medio camino entre la integridad y la disponibilidad, es habitual leer en la prensa[714] noticias referentes a la solicitud de un rescate[715] por descifrar la información de los

[712] COTINO HUESO, L. (2008), derechos del ciudadano, 155-156.
[713] CCN (2014), CCN-STIC-850A, 11-12.
[714] A modo de ejemplo puede leerse esta noticia del pasado año 2015 recuperada de http://ccaa.elpais.com/ccaa/2015/03/13/madrid/1426272342_374007.html (4 de julio de 2016).
[715] *Vid*. informe del CCN titulado "*CCN-CERT ID-24/16 Ransom.CryptXXX*" disponible en https://www.ccn-cert.cni.es/informes/informes-de-codigo-danino-id.htm (28 de septiembre de 2016).

discos duros de equipos infectados por *ransomware*, un tipo de *software* malintencionado que restringe el acceso a nuestra propia información, lo que, al menos, resulta molesto para los particulares y puede desencadenar graves consecuencias para las empresas afectadas[716]. Quizás el ejemplo modélico de indisponibilidad encajaría mejor con lo denominado "denegación de servicio" (*DoS, Denial Of Service*), un ataque informático producido sobre la fuente de los datos o contra el canal de transmisión, que provoca la interrupción del acceso a un servicio a sus usuarios legítimos[717]. Las consecuencias pueden llegar a ser muy graves, en función de la criticidad del servicio suspendido (imaginemos hospitales, centrales nucleares[718], estaciones eléctricas, aeropuertos…).

En materia de seguridad del *software*, es importante diseñar aplicaciones y servicios de modo tal que opongan la mayor resistencia a los ataques de *DoS*, evitando vulnerabilidades[719] que puedan ser explotadas a tal efecto. Las recomendaciones del CCN advierten que debe cuidarse la implementación de funciones pesadas y controlar su ejecución, analizar los algoritmos empleados, así como controlar el número de ejecuciones y el paso de parámetros[720].

[716] FUNDACIÓN TELEFÓNICA (2016), ciberseguridad, 15.
[717] CCN (2013), CCN-STIC-820, 6.
[718] *Vid*. el artículo titulado "*Las centrales nucleares desatienden el riesgo de ataques informáticos*", publicado en El País con fecha 6 de octubre de 2015, disponible en http://tecnologia.elpais.com/tecnologia/2015/10/05/ actualidad/ 1444058435_765864.html (26 de septiembre de 2016).
[719] INTECO (2012), guía sobre riesgos y buenas prácticas, 6. Define la vulnerabilidad como una debilidad que puede ser 'activada' de forma accidental o intencionadamente, como un factor de riesgo interno de un elemento expuesto a una amenaza de ser susceptible a sufrir un daño y de encontrar dificultades en recuperarse posteriormente.
[720] CCN (2013), CCN-STIC-820, 35. Describe diez vulnerabilidades del *software* que deben ser evitadas para minimizar las posibilidades de sufrir este tipo de ataques.

dimensiones	D		
nivel	bajo	medio	alto
	No aplica	aplica	+

Figura 8: Protección frente a la denegación de servicio

Fuente: BOE de 29 de enero de 2010, 45.

El ENS ha dedicado a esta vulnerabilidad concreta una medida de seguridad específica, "mp.s.8", denominada "**protección frente a la denegación de servicio**", que afecta exclusivamente a la disponibilidad y se aplica en el nivel medio y, en mayor medida, en el alto. Para nivel medio establece medidas preventivas y reactivas frente a ataques de *DoS*, planificando y dotando al sistema de capacidad suficiente para atender a la carga prevista con holgura y previendo el despliegue de aquellas tecnologías que puedan prevenir los ataques conocidos. Para el nivel alto requiere el establecimiento de sistemas de detección de los ataques de *DoS* y de procedimientos de reacción a los mismos, impidiendo también el lanzamiento de dichos ataques se realicen desde las propias instalaciones perjudicando a terceros.

El ENS dispone otras medidas de seguridad que afectan a la disponibilidad, en exclusiva o no, como el bloque denominado "continuidad del servicio" o las medidas "cnergía eléctrica", "protección frente a incendios", "copias de seguridad (*backup*)"…

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Figura 9: Medios alternativos

Fuente: BOE de 29 de enero de 2010, 45.

La medida de seguridad "mp.s.9", denominada "**medios alternativos**", exigida solo para el nivel alto, pretende garantizar la existencia y disponibilidad de dichos medios alternativos, sujetos a las mismas garantías de protección que los medios habituales, para prestar los servicios en el caso de que fallen.

Fallos informáticos de terceras partes pueden ocasionar grandes problemas en la relación de los ciudadanos con las Administraciones públicas. El recurso a una hipotética falta de disponibilidad del servicio bancario no impidió que, el 22 de diciembre de 2010, el TEAR en Illes Balears desestimara la reclamación presentada contra el acuerdo, dictado por el Administrador tributario de la Agencia tributaria de las Illes Balears, que confirmaba el recargo por presentación extemporánea de una autoliquidación de la tasa fiscal sobre el juego correspondiente a diciembre de 2007, por un importe de 9.460,81 €. La reclamante reconoció la presentación extemporánea a causa de un error técnico y a dificultades en el sistema operativo de la entidad bancaria, error informático que no pudo acreditar. Como indica la sentencia[721], "*su condición de sujeto pasivo del impuesto determina su responsabilidad frente a la Hacienda*

[721] STSJ de las Illes Balears 17/2013 de 9 de enero de 2013, sala de lo contencioso.

Pública, sin perjuicio de sus relaciones con la entidad bancaria colaboradora si es que un fallo en su sistema informático fue la causa de la presentación e ingreso tardíos", como señala el artículo 17.4 de la LGT, por el que los elementos de la obligación tributaria no se ven alterados por actos entre particulares. Cabe meditar sobre la afirmación del FJ1 conforme a la cual "*sería de responsabilidad de la demandante no haber actuado con la diligencia debida y no dejar para el último día el cumplimiento de sus obligaciones tributarias, con la asunción del riesgo que ello pueda conllevar*" y preguntarse si la conclusión hubiera sido la misma si el mal funcionamiento hubiera provenido de la Administración o hubiera afectado a sus sistemas informáticos, por ejemplo, impidiendo el funcionamiento de sus pasarelas de pagos.

Si bien es cierto que los actos o convenios de los particulares no pueden alterar la posición del sujeto pasivo y los demás elementos de la obligación tributaria, ni surtir efectos ante la Administración, en el ámbito sancionador, en el que la responsabilidad es personal, rige el principio de culpabilidad, por lo que es preciso atender a las circunstancias concretas de cada caso y, en caso de sanción, motivarla adecuadamente.[722]

5.2.1.5. Trazabilidad

Una empresa de tasaciones y valoraciones fue sancionada, entre otras, con una multa de 45.000 € prevista en el artículo 10.a) de la ley 26/1988, de 29 de julio, sobre disciplina e intervención de las entidades de crédito, por presentar deficiencias en la organización administrativa, técnica o de personal en los procedimientos de control interno, lo que incluye las exigencias mínimas de administradores o profesionales titulados. En particular, se detectan

[722] STSJ de Cataluña 2073/2012 de 23 de febrero de 2012, sala de lo contencioso.

problemas de trazabilidad puestos de manifiesto en la coincidencia entre validador y tasador en, al menos, 136 tasaciones revisadas, deficiencia que la propia empresa reconoció, achacando su existencia a un error informático en el uso de las claves.[723]

El ENS define la trazabilidad como la "*propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad*", definición coincidente con la utilizada en MAGERIT 3.0[724], extraída de la norma UNE 71504:2008. La guía elaborada por el CCN para valorar las dimensiones de la seguridad y categorizar el sistema explica que, con respecto a la trazabilidad, el nivel requerido se obtiene en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha modificado o ha accedido a una cierta información. Para determinar el nivel necesario, plantea algunas preguntas sobre el grado en que la incapacidad para rastrear un acceso a la información impediría o dificultaría la capacidad de subsanar un error o la persecución de un delito o si facilitaría la comisión de estos[725].

Explica el CCN que, ante una incidencia, es preciso poder determinar lo que ha pasado para aplicar las medidas correctoras adecuadas, para lo que será necesario disponer información. El ENS establece los procedimientos y mecanismos a emplear para que ello resulte factible. "*Los mecanismos empleados para garantizar la trazabilidad ofrecerán capacidad analítica a los especialistas de tal forma que podrán operar en modo preventivo o reactivo, según demande la necesidad*". La aplicación de la trazabilidad requiere medidas diversas, como

[723] SAN 2025/2013de 7 de mayo de 2013, sala de lo contencioso.
[724] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 16.
[725] CCN (2011), CCN-STIC-803, 6 y 10.

procesos de identificación y control de acceso, segregación y cumplimiento de funciones, mecanismos de autenticación, accesos locales y remotos, registros de la actividad de los usuarios o empleo de marcas de tiempo. Pero, como hace constar el CCN, no es suficiente garantizar la existencia y disponibilidad de los registros, también se ha de asegurar su integridad, descansando su validez en la confirmación de que no han sido alterados, por lo que múltiples dimensiones de seguridad se aplican sobre una misma medida para lograr cumplir su propósito"[726]. El ENS establece la obligación de retener las cuentas de los usuarios durante todo el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas, tiempo denominado "periodo de retención".

Al comentar *infra* la STSJ de Madrid 1140/2015, sala de lo contencioso, de fecha 30 de enero de 2015, sobre la pérdida de casi ocho años de cotización de un trabajador, reiteraré estas ideas, cuestionando el cumplimiento de las medidas de seguridad, en particular las incluidas en el marco operacional de control de acceso, que brevemente resumo a continuación.

				op	Marco operacional
Dimensiones afectadas	Básica	Media	Alta	op.acc	Control de acceso
Autenticidad y trazabilidad	aplica	aplica	aplica	op.acc.1	Identificación
Integridad, confidencialidad, autenticidad y trazabilidad	aplica	aplica	aplica	op.acc.2	Requisitos de acceso
Integridad, confidencialidad, autenticidad y trazabilidad	No aplica	aplica	aplica	op.acc.3	Segregación de funciones y tareas
Integridad, confidencialidad, autenticidad y trazabilidad	aplica	aplica	aplica	op.acc.4	Proceso de gestión de derechos de acceso
Integridad, confidencialidad, autenticidad y trazabilidad	aplica	aplica +	aplica ++	op.acc.5	Mecanismo de autenticación
Integridad, confidencialidad, autenticidad y trazabilidad	aplica	aplica +	aplica ++	op.acc.6	Acceso local *(local logon)*
Integridad, confidencialidad, autenticidad y trazabilidad	aplica	aplica +	aplica +	op.acc.7	Acceso remoto *(remote login)*

Figura 10: Control de acceso

Fuente: BOE de 4 de noviembre de 2015, 104250.

(convenciones adaptadas por la autora para aumentar la legibilidad)

[726] CCN (2014), CCN-STIC-850A, 14.

Todas las medidas de seguridad del marco operacional englobadas bajo la denominación genérica de "**control de acceso**", con código "op.acc", afectan, entre otras, a la dimensión de la trazabilidad. Cubren el conjunto de actividades preparatorias y ejecutivas para gestionar los accesos a un recurso, para la realización de una acción dada por parte de una determinada entidad, usuario o proceso. El control de acceso implantado buscará la ponderación entre la comodidad de uso y la protección de la información, inclinándose hacia la comodidad en los sistemas de nivel bajo y decantándose hacia la protección en los de nivel alto. Ese control parte de unos principios establecidos bajo la premisa de que todo acceso está prohibido salvo concesión expresa, que la entidad ha de quedar identificada singularmente, que el uso de los recursos ha de estar protegido, que se habrá definido previamente a qué necesita acceder cada entidad, con qué derechos y bajo qué autorización, que la identidad de la entidad deberá quedar suficientemente autenticada y que debe controlarse tanto el acceso local como el remoto. A todo ello es preciso añadir que los encargados de autorizar, usar y controlar el uso han de ser personas diferentes. Afirma el ENS que cumpliendo todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización.

Encontramos otras tres medidas más en el real decreto que afectan en exclusiva a la dimensión de la trazabilidad, concretamente la "op.exp.8" y la "op.exp.10" dentro del marco operacional y la medida de protección "mp.info.5".

dimensiones	T		
nivel	bajo	medio	alto
	aplica	+	++

Figura 11: Registro de la actividad de los usuarios

Fuente: BOE de 4 de noviembre de 2015, 104264.

La primera de ellas, denominada "**registro de la actividad de los usuarios**", pretender registrar el uso del sistema, ya sea un acceso exitoso o un intento fallido, para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Figura 12: Protección de los registros de actividad

Fuente: BOE de 29 de enero de 2010, 30.

La segunda, llamada "**protección de los registros de actividad**", se aplica únicamente en el nivel alto de seguridad. El ENS prohíbe la modificación y eliminación de esos registros por personal no autorizado, fijando los mismos requisitos para las copias de seguridad que pudieran existir. Dispone la protección de los registros del sistema, determinando el periodo de retención de los registros y asegurando la fecha y hora de forma inequívoca mediante sellos

de tiempo. Precisamente los "**sellos de tiempo**" es la tercera de las medidas citadas, desarrollada *infra*.

En ocasiones no resulta viable la asignación individualizada de credenciales de uso estrictamente personal e intransferible, debido a las características del servicio. En esos casos excepcionales, debe quedar identificada singularmente cada persona y momento en que se haga uso de dichas credenciales, habilitando los mecanismos oportunos que permitan contar con un listado permanentemente actualizado de los accesos, permitiendo así que la trazabilidad quede garantizada[727].

5.2.2. Medidas de seguridad

En el ámbito de la eAdministración, la seguridad de la información y, por tanto, de las aplicaciones informáticas que la gestionan, es una garantía del cumplimiento de los principios de calidad y exactitud. La implantación de medidas de seguridad es una garantía de la disponibilidad de la información administrativa y de su conservación, a la vez que evita la alteración de la documentación obrante en sus ficheros, ya sea aportada por los ciudadanos o elaborada por la Administración[728]. Dichas medidas aparecen indicadas en el anexo II del ENS, debiendo ser aplicadas para dar cumplimiento a los requisitos mínimos exigibles. Son definidas como un "*conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad*". Entre ellas, se

[727] Así se contempla en la orden PRE/57/2016, de 14 de septiembre, por la que se regulan las condiciones sobre seguridad de la información y de los sistemas de información a incorporar en los pliegos de cláusulas administrativas particulares y de prescripciones técnicas en la contratación pública de la Administración de la Comunidad autónoma de Cantabria, publicada en el BOC de 30 de septiembre de 2016.
[728] TRONCOSO REIGADA, A. (2011), la Administración electrónica, 268.

incluyen medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación. El ENS las agrupa según una clasificación diferente, en tres bloques llamados marco organizativo, marco operacional y medidas de protección.

Para determinar las medidas de seguridad a aplicar, es preciso tener en cuenta los activos que constituyen el sistema, la categoría del mismo conforme a lo previsto en el artículo 43 y las decisiones que se adopten para gestionar los riesgos identificados. En el caso particular de manejar datos de carácter personal, se aplicará la normativa de protección de datos, sin perjuicio de los requisitos establecidos en el ENS. Las medidas, aunque tengan la condición de mínimos exigibles, como indica el 27.3, son ampliables a criterio del responsable de seguridad, teniendo en cuenta el estado de la tecnología, la naturaleza de la información o servicios protegidos y el riesgo a que están expuestos.

Entre los requisitos mínimos establecidos encontramos el correspondiente a la profesionalidad, que alcanza al personal de organizaciones externas que provean a las Administraciones públicas de servicios de seguridad, a quienes se les exigirá, de manera objetiva y no discriminatoria, una cualificación y unos niveles idóneos de gestión y madurez en los servicios prestados. Se tratará *infra* la forma de valorar la experiencia del equipo de desarrollo en las licitaciones. Las guías de seguridad elaboradas por el CCN, previstas en el artículo 29 del ENS, establecen el requisito de estar en condiciones de exhibir la correspondiente “declaración de conformidad” con el ENS (para sistemas de categoría básica) o la “certificación de conformidad” (voluntario salvo para las categorías media y alta), utilizando los mismos procedimientos que los exigidos para las entidades públicas. La notificación de esa obligación a

la empresa contratada es responsabilidad de las entidades públicas contratantes, quienes podrán solicitar en todo momento los informes de autoevaluación o auditoría correspondientes, al objeto de verificar la adecuación e idoneidad[729].

El ENS obliga a que la seguridad de los sistemas sea atendida, revisada y auditada por personal cualificado, dedicado e instruido, recibiendo la formación específica necesaria para garantizar la seguridad de las TIC de la Administración. El CCN ha elaborado la guía "CCN-STIC-808 – Verificación del cumplimiento de las medidas en el ENS" que sirve como herramienta para el trabajo de campo del auditor.

Al objeto de cumplir los principios básicos y requisitos mínimos establecidos, se aplican las medidas de seguridad indicadas en el anexo II del real decreto, proporcionales a las dimensiones de seguridad relevantes en el sistema a proteger y a la categoría del mismo, la cual se determina valorando el impacto que, sobre la organización, tendría un incidente de seguridad, según su repercusión en la capacidad para alcanzar los objetivos pretendidos, proteger los activos a su cargo, cumplir sus obligaciones diarias de servicio, así como respetar la legalidad vigente y los derechos de las personas. Ese impacto se evalúa de forma independiente en cada dimensión.

5.2.2.1. Medidas de seguridad para servicios externos

Entre las medidas de seguridad contempladas en el ENS dentro del denominado "marco operacional" se incluye un bloque dedicado a los servicios de empresas o trabajadores externos, aplicable entre otros a las organizaciones proveedoras de *software*.

[729] CCN (2015), CCN-STIC-809, 10.

El ENS afirma, al utilizar servicios externos, la delegación se limita a las funciones, añadiendo que la organización mantiene su responsabilidad en cuanto a los riesgos en que se incurre, en la medida en que impacten sobre la información manejada y sobre los servicios finales prestados.

Dimensiones afectadas	Categorías afectadas			Medidas de seguridad	
	Básica	Media	Alta		
				op.ext	Servicios externos
Cualquiera	No aplica	aplica	aplica	op.ext.1	Contratación y acuerdos de nivel de servicio
Cualquiera	No aplica	aplica	aplica	op.ext.2	Gestión diaria
Disponibilidad	No aplica	No aplica	aplica	op.ext.9	Medios alternativos

Figura 13: Medidas de seguridad para servicios externos

Fuente: BOE de 4 de noviembre de 2015, 104251.

(convenciones adaptadas por la autora para aumentar la legibilidad)

La medida "**contratación y acuerdos de nivel de servicio**", exigible para las categorías media y alta por igual, afecta a cualquiera de las dimensiones de la seguridad. Consiste en establecer contractualmente, con anterioridad a la utilización de los recursos externos, las características del servicio prestado y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio y las consecuencias de su incumplimiento.

Cuando se audite el cumplimiento de esta medida, se podría comprobar si el análisis de riesgos realizado previamente identifica los asociados a la intervención del proveedor externo y si existe de un procedimiento documentado de pasos previos a la contratación, donde

se requiera que el proveedor detalle las características del servicio a prestar y manifieste la satisfacción de los requisitos de servicio y seguridad requeridos y aprobados previamente, que se defina lo que se considera calidad mínima y las consecuencias de su incumplimiento y que se establezcan las funciones, obligaciones y responsabilidades de cada parte[730].

La segunda medida, denominada "**gestión diaria**", es exigible para las categorías media y alta por igual, afectando a cualquiera de las dimensiones de la seguridad. Será especialmente importante en los contratos de mantenimiento del *software* de las Administraciones públicas. Requiere establecer un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, un procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado, así como el mecanismo y los procedimientos de coordinación tanto para llevar a cabo las tareas de mantenimiento de los sistemas afectados como para actuar en caso de incidentes y desastre.

Aspectos auditables son el procedimiento de gestión de incidencias del servicio externo, que ha de ser coherente con el genérico, así como la existencia de un procedimiento documentado que defina la frecuencia de las mediciones del cumplimiento de las obligaciones de servicio, indicando su responsable y el protocolo de actuación en caso de incumplimiento o degradación en la calidad acordada. El auditor consultará el cumplimiento de los mecanismos y los procedimientos de coordinación previstos para llevar a cabo las tareas de mantenimiento[731].

[730] CCN (2011), CCN-STIC-808, 46. Sorprendentemente, la guía no prevé su aplicación a la disponibilidad, ni para la medida "op.ext.1" ni para la "op.ext.2".
[731] CCN (2011), CCN-STIC-808, 47.

La medida "**medios alternativos**"[732], afecta solo a la disponibilidad y es exigible únicamente para el nivel alto. Su función es la provisión del servicio en caso de indisponibilidad de los medios contratados, con las mismas garantías de seguridad previstas para los medios habituales. A la hora de licitar un contrato de servicios[733] de desarrollo de una nueva aplicación informática para la Administración, rara vez se plantea qué hacer cuando el *software* no es entregado satisfactoriamente en el plazo prefijado más allá de establecer penalizaciones. No es frecuente ofrecer alternativas al uso del aplicativo cuya puesta en producción se retrasa. El ENS, con esta medida, parece consciente de la importancia que ello puede tener en casos de nivel alto (imaginemos qué podría haber ocurrido si el 1 de enero de 2000 no se hubiese dispuesto de un *software* adecuadamente depurado en centrales nucleares, aeropuertos, hospitales…).

5.2.2.2. Medidas de protección de las aplicaciones informáticas

Las medidas de protección se centran en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. Uno de esos activos es el *software*.

[732] Existen dos medidas diferentes con el nombre de "medios alternativos" que no deben confundirse. Una de ellas se sitúa entre las medidas operacionales de servicios externos y la otra entre las dedicadas a la protección de las comunicaciones.

[733] Con referencia a los contratos informáticos, *vid*. MENÉNDEZ SEBASTIÁN, E.M. (2009), contratos de servicios del sector público, 188-208. En particular, a tenor del artículo 9.3.b) del TRLCSP, los programas de ordenador desarrollados a medida para las Administraciones públicas son objeto de contratos de servicios.

Dimensiones afectadas	Categorías afectadas			Medidas de seguridad	
	Básica	Media	Alta		
				mp.sw	Protección de las aplicaciones informáticas
Cualquiera	No aplica	aplica	aplica	mp.sw.1	Desarrollo
Cualquiera	aplica	aplica +	aplica ++	mp.sw.2	Aceptación y puesta en servicio

Figura 14: Medidas de protección de las aplicaciones informáticas

Fuente: BOE de 4 de noviembre de 2015, 104252.

(convenciones adaptadas por la autora para aumentar la legibilidad)

La primera medida de protección de las aplicaciones informáticas lleva por denominación "**desarrollo de aplicaciones**" y es exigible por igual para las categorías media y alta, afectando a cualquier dimensión de la seguridad. En ella se obliga a contar con un entorno de desarrollo diferente y separado del de producción (también llamado real o de explotación), además de vetar en este la existencia de herramientas o datos de desarrollo. A su vez, establece que las pruebas anteriores a la implantación o modificación no se realicen con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Si bien es cierto que la separación de entornos de trabajo aísla la explotación de los riesgos del desarrollo[734], hasta el punto de que muchas veces llega a existir un tercer entorno en medio, separándolos aún más[735], la conveniencia o no de disponer de herramientas al servicio de los desarrolladores en las máquinas de producción es un tema nada pacífico (incluso se discute el propio privilegio de acceso de los informáticos a este entorno). Aunque, sobre el papel,

[734] NOVOA BERMEJO, J.A. (2001), auditoría de técnica de sistemas, 354.
[735] Este nuevo entorno se denomina de preexplotación o preproducción.

se plasmen las buenas intenciones sobre la separación de entornos, la realidad frecuentemente se impone, especialmente cuando no se puede disponer de una copia de los datos reales en desarrollo y se convierte en imprescindible que un informático entre en producción a manipular datos para solventar problemas que, de otro modo, no se podrían reparar. Es el momento de buscar el equilibrio entre la seguridad y el cumplimiento de las obligaciones asumidas por la Administración. En ese sentido afirma MAGERIT 3.0 que "*a fin de que estas actividades cuajen en la organización, es imprescindible que la seguridad sea mínimamente intrusiva: que no dificulte innecesariamente la actividad diaria ni hipoteque alcanzar los objetivos de productividad propuestos*"[736]. Una protección tal que impida a la Administración ejercer las funciones que tiene encomendadas por el artículo 103 del texto constitucional debe ser rechazada.

El ENS dispone la aplicación de una metodología de desarrollo reconocida que tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida, trate específicamente los datos usados en pruebas, permita la inspección del código fuente e incluya normas de programación segura. Además, obliga a incluir mecanismos de identificación y autenticación, y de protección de la información tratada, así como generar y tratar pistas de auditoría.

Aspectos auditables son la existencia de un inventario de servidores que identifique a qué entorno da servicio cada uno, o la de herramientas de compilación en producción. Con respecto al seguimiento de una metodología, es de utilidad comprobar la

[736] MINHAP. MAGERIT 3.0, libro I – Método, 11.

existencia de la documentación cuya generación está prevista en la misma, así como su cobertura extensiva a los aspectos de seguridad. La guía del CCN pone como ejemplo la metodología Métrica v3, la misma sobre la que incidiremos *infra*. El auditor podría verificar la inexistencia de datos reales en el entorno de desarrollo, salvo que se cuente con autorización expresa, así como consultar el diseño de un desarrollo y confirmar la disponibilidad de una política o normativa documentada que prevea mecanismos de identificación y autenticación y de protección de la información[737].

Sorprende que la guía 808 del CCN propone la verificación de una acción no prevista en el ENS. A pesar de que este no dispone una aplicación superior y específica para la categoría alta, la guía sugiere, en su página 77, la verificación de la aplicación de un procedimiento de inspección de código documentado, previendo la consulta de uno de esos informes. En cualquier caso, ya se trate de un error de la guía o de una carencia accidental del ENS, esta inspección de código podría ser la alternativa a la exposición pública del código fuente de las aplicaciones informáticas, tan demandada por la doctrina. Ahora bien, cabe preguntarse quién sería el encargado de efectuar esta inspección. Si este trabajo se encarga a una empresa externa, podría cuestionarse la fiscalización de la actividad de la Administración por parte del sector privado. Si esa misma empresa externa es la autora del código desarrollado e inspeccionado, aunque se trate de diferentes personas físicas, el procedimiento parece totalmente inadecuado.

[737] CCN (2011), CCN-STIC-808, 75-76.

La segunda medida de protección de las aplicaciones informáticas se denomina "**aceptación y puesta en servicio**". Afecta a todas las dimensiones y se exige de forma más intensa según se incrementa la categoría. Antes de la puesta en producción del nuevo *software*, deben comprobarse una serie de puntos:

- Categoría básica: se constatará que se cumplen de los criterios de aceptación en materia de seguridad, cerciorándose de que no se deteriora la de otros componentes. Las pruebas han de realizarse en un entorno de pre-producción, sin utilizar datos reales salvo que pueda asegurarse el nivel de seguridad correspondiente. El auditor podría valorar la evidencia documental del plan de pruebas de los aspectos comentados, ejecutado con constancia de sus resultados sobre un entorno aislado, no utilizando datos reales salvo que cuente con las garantías adecuadas. La guía 808 del CCN recomienda la consulta de la metodología Métrica v3[738].

- Categoría media: se analizarán las vulnerabilidades y realizarán pruebas de penetración o *hacking* ético, simulando ser un atacante. El auditor podría consultar el análisis, así como la resolución de los problemas detectados[739].

- Categoría alta: se observará también la coherencia en la integración en los procesos y se considerará la oportunidad de realizar una auditoría de código fuente. El auditor podría investigar los resultados obtenidos y, en caso de no haberse realizado la revisión del código fuente, podría comprobar los motivos por los cuales se ha tomado esta decisión[740]. En todo

[738] CCN (2011), CCN-STIC-808, 77.
[739] CCN (2011), CCN-STIC-808, 78.
[740] CCN (2011), CCN-STIC-808, 78.

caso, es preciso tener en cuenta que la auditoría completa del código fuente puede ser de un coste prohibitivo[741], tanto en esfuerzo como en dinero, por lo que se centrará únicamente en los puntos identificados como críticos.

5.2.2.3. Medidas de protección de la información

El *software* de las Administraciones públicas ha de satisfacer todos los requerimientos que permitan implantar en la práctica las medidas de protección de la información en evitación de que un funcionamiento inadecuado la ponga en riesgo. Consciente de ello, Valero Torrijos muestra su preocupación por la conservación y accesibilidad futura de los documentos y los expedientes electrónicos, no solo en relación con los certificados y la firma electrónica, sino también por la necesidad de disponer en todo momento de aplicaciones y programas compatibles con los utilizados inicialmente para generar los documentos[742]. En el mismo sentido se manifiesta Cotino Hueso, quien muy visualmente lo describe como "*la espada de Damocles que se ciñe sobre la información electrónica*"[743]. Por ello, toda migración del sistema informático deberá ser efectuada de forma que garantice la autenticidad, disponibilidad y utilidad de los registros almacenados[744]. Así lo recoge el legislador en el artículo 17.2 de la nueva ley 39/2015 y en el 46.2 de la ley 40/2015, refiriéndose específicamente al acceso desde diferentes aplicaciones. Ambos artículos, en sus respectivos apartados 3, invocan el cumplimiento de las garantías previstas en la legislación de protección de datos, ya previsto por el ENS.

[741] CCN (2013), CCN-STIC 804, 62.
[742] VALERO TORRIJOS, J. (2009), las garantías jurídicas, 27.
[743] COTINO HUESO, L. (2008), derechos del ciudadano, 208.
[744] JARAUTA SÁNCHEZ, J. (2007), cadena de confianza, 6.

Dimensiones afectadas	Categorías afectadas			Medidas de seguridad	
	Básica	Media	Alta		
				mp.info	Protección de la información
Cualquiera	aplica	aplica	aplica	mp.info.1	Datos de carácter personal
Confidencialidad	aplica	aplica +	aplica +	mp.info.2	Calificación de la información
Confidencialidad	No aplica	No aplica	aplica	mp.info.3	Cifrado
Integridad y autenticidad	aplica	aplica +	aplica ++	mp.info.4	Firma electrónica
Trazabilidad	No aplica	No aplica	aplica	mp.info.5	Sellos de tiempo
Confidencialidad	aplica	aplica	aplica	mp.info.6	Limpieza de documentos
Disponibilidad	aplica	aplica	aplica	mp.info.9	Copias de seguridad *(backup)*

Figura 15: Medidas de protección de la información

Fuente: BOE de 4 de noviembre de 2015, 104252.

(convenciones adaptadas por la autora para aumentar la legibilidad)

La medida denominada "**datos de carácter personal**" se aplica por igual a todas las categorías y afecta a todas las dimensiones. Dispone la aplicación cumulativa de lo dispuesto en el propio ENS y de la LOPD y en la normativa de protección de datos de carácter personal, en su caso.

Es preciso hacer notar la diferencia entre las categorías básica, media y alta contempladas por el ENS, conceptualmente distintos de los niveles de seguridad exigibles a los ficheros y tratamientos por el artículo 80 del RLOPD, también llamados básico, medio y alto, pero no necesariamente coincidentes.

El auditor de esta medida podría comprobar la existencia de un procedimiento documentado para identificar los datos susceptibles de ser calificados como personales, la declaración del fichero ante la AEPD y el cumplimiento de la normativa aplicable[745].

La medida denominada "**cifrado**" afecta únicamente a una de las dimensiones de la seguridad, a la confidencialidad, y obliga a su utilización únicamente cuando el sistema sea considerado de categoría alta, lo que no impide su uso voluntario en las categorías inferiores pues, a tenor del artículo 27.3, las medidas tienen la condición de mínimos exigibles, pudiendo ser ampliados. La información solo estará en claro mientras se esté haciendo uso de ella, no durante su almacenamiento ni transmisión.

El auditor podría comprobar aspectos como la existencia de una política o normativa documentada que contemple el cifrado de ficheros, directorios, discos virtuales o bases de datos, así como de la información transmitida. También podría verificar que se dispone de un procedimiento documentado que determina cómo cifrar correctamente los datos en función de su clasificación y del medio en el que se almacena. Igualmente será una evidencia de cumplimiento la existencia tanto de información realmente cifrada como de mecanismos para aplicar dicho procedimiento, como GnuPG, TrueCrypt, VPN IPSec, etc[746].

La medida "**firma electrónica**" se debe aplicar con más intensidad según se va elevando el nivel, afectando a la seguridad y a la autenticidad, al tratarse de un instrumento capaz de permitir la comprobación de la procedencia, y la integridad, ofreciendo las bases para evitar el repudio.

[745] CCN (2011), CCN-STIC-808, 78.
[746] CCN (2011), CCN-STIC-808, 80-81.

- Para el nivel bajo el ENS acepta cualquier tipo de firma electrónica previsto en la legislación vigente.
- En el nivel medio, cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos han de ser cualificados. Los algoritmos y parámetros empleados estarán acreditados por el CCN. El ENS exige que la firma electrónica pueda ser verificada y validada durante todo el tiempo que sea necesario para que la Administración pueda realizar su actividad. Cuando la Administración firme documentos electrónicamente, debe anexar la información necesaria a los efectos de que se pueda verificar y validar en cualquier momento. Cuando recabe documentos firmados por el administrado, ha de verificar y validar la firma recibida en el momento de la recepción.
- En el nivel alto ha de usarse firma electrónica cualificada, con sistemas, productos o equipos que hayan superado una evaluación conforme a normas europeas o internacionales (ISO/IEC 15408 u otras de naturaleza y calidad análogas). Sus certificados deben estar reconocidos por el ENECSTI. Los criterios exigibles se detallarán mediante una instrucción técnica de seguridad.

Conforme a lo dispuesto por el artículo 27.5, son admisibles otros mecanismos de firma electrónica sujetos a derecho incorporando medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio.

Son aspectos a auditar la existencia y el cumplimiento de una política de firma electrónica y de un procedimiento en el que quede constancia de los documentos que requieren capacidad probatoria, así como la realización de la firma de los mismos, la existencia de un

inventario de algoritmos criptográficos acreditados utilizados y las posibles autorizaciones de los responsables para el uso de productos no seguros o no certificados. También se debe constatar que el certificado y los datos de verificación y de validación y, en su caso, el sello de tiempo, acompañan a las firmas. En el nivel alto habría que verificar el uso de certificados reconocidos y de dispositivos seguros de verificación de firma[747].

La medida llamada "**sellos de tiempo**" afecta únicamente a la trazabilidad. El ENS exige su aplicación únicamente para el nivel alto. Los sellos de tiempo prevendrán la posibilidad del repudio posterior, por lo que son de utilidad en la información susceptible de ser utilizada como evidencia electrónica en el futuro.

En el proceso de sellado de tiempo se recurre a un tercero de confianza conocido como "Autoridad de sellado de tiempo", un prestador de servicios de certificación que emite sellos con fecha y hora oficial según establece el real decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del real instituto y observatorio de la Armada como laboratorio depositario del patrón nacional de tiempo y laboratorio asociado al Centro español de metrología[748].

El recurso a ese tercero de confianza es lo que diferencia principalmente a un sello de tiempo de una simple marca de tiempo generada por una aplicación informática cualquiera. Además, comparando las definiciones de ambos conceptos aportadas por el ENI en su glosario de términos, un sello de tiempo siempre incluye fecha y hora, mientras que una marca de tiempo podría incluir únicamente la fecha, algo que no se adapta a una de las novedades introducidas por

[747] CCN (2011), CCN-STIC-808, 82-83.
[748] PUNZÓN MORALEDA, J./ SÁNCHEZ RODRÍGUEZ, F. (2010), sellado de tiempo, 716-717.

la ley 39/2015, como es el cómputo de plazos administrativos por horas, declarando hábiles las veinticuatro horas del día, algo coherente con el contexto electrónico.

Para lograr el propósito pretendido con el sellado, es necesario tratar los datos pertinentes para la verificación posterior de la fecha con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad. Los sellos de tiempo serán renovados periódicamente mientras la información aún sea necesitada por el proceso administrativo. Se emplearán "sellos cualificados de tiempo electrónicos" acordes con la normativa europea, así como productos certificados[749] o servicios externos admitidos.

Se fechan electrónicamente los documentos cuya fecha y hora de entrada o de salida debe acreditarse fehacientemente, así como las firmas cuya validez deba extenderse por largos periodos o así lo exija la normativa aplicable; alternativamente se pueden utilizar formatos de firma avanzada que incluyan fechado[750].

El trabajo del auditor pasa por la comprobación de la existencia de procedimientos documentados para identificar y establecer el tiempo de retención de la información, para fechar electrónicamente y para validar fechados. También puede verificar el sellado de aquellos documentos cuya fecha y hora de entrada o salida debe acreditarse fehacientemente, y constatar el tratamiento seguro que permita comprobar posteriormente la fecha. Otras evidencias de cumplimiento podrían ser que se contemple alternativamente el uso de formatos de firma avanzada que incluyan fechado, la existencia de un procedimiento para identificar la duración del

[749] Para más información, consúltese la medida del marco operacional “op.pl.5”, denominada “componentes certificados”.
[750] CCN (2013), CCN-STIC 804, 68.

sello de tiempo en función del periodo requerido por el proceso administrativo al que da soporte o la constatación de que los sellos de tiempo que lo requerían han sido renovados conforme al procedimiento[751].

Habida cuenta de que el principal desafío planteado por las garantía tecnológicas de los documentos electrónicos es la necesidad continua de actualización ante la evolución de los riesgos de seguridad[752], aplicando las medidas analizadas, las plataformas de custodia de documentos electrónicos completan el ciclo de vida de los documentos firmados, refirmándolos de forma preprogramada y automatizada conforme a las políticas establecidas, con el fin de mantener su validez en el tiempo[753].

5.2.2.4. Medidas de protección de los servicios

Entre las medidas de protección de los servicios, la segunda es aplicable a las aplicaciones informáticas.

[751] CCN (2011), CCN-STIC-808, 84.
[752] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 227.
[753] JARAUTA SÁNCHEZ, J. (2007), cadena de confianza, 6.

Dimensiones afectadas	Categorías afectadas			Medidas de seguridad	
	Básica	Media	Alta		
				mp.s	Protección de los servicios
Cualquiera	aplica	aplica	aplica	mp.s.1	Protección del correo electrónico
Cualquiera	aplica	aplica	aplica +	mp.s.2	Protección de servicios y aplicaciones web
Disponibilidad	No aplica	aplica	aplica +	mp.s.8	Protección frente a la denegación de servicio
Disponibilidad	No aplica	No aplica	aplica	mp.s.9	Medios alternativos

Figura 16: Medidas de protección de los servicios

Fuente: BOE de 4 de noviembre de 2015, 104252.

(convenciones adaptadas por la autora para aumentar la legibilidad)

Denominada "**protección de los servicios y aplicaciones *web***", atañe a los subsistemas mediante los cuales se publica información en la red. Afecta a cualquiera de las dimensiones del mismo modo en los sistemas de categoría básica y media, y más intensamente en los categorizados como altos. Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a ella obviando la autenticación, en particular evitando que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado, previniendo ataques de manipulación de URL y de manipulación de fragmentos de información almacenada en el disco duro del visitante de una página *web* a través de su navegador, a petición del servidor de la página, conocido como *cookies*. Además, debe prevenirse los ataques de inyección de código, los intentos de escalado de privilegios y los ataques de *cross site scripting*[754]. Igualmente, se prevendrán ataques de manipulación de programas o dispositivos,

[754] *Vid.* https://www.incibe.es/glossary/empresas/diccionario/XSS_Glosario

conocidos como *proxies*[755], que realizan una acción en representación de otros, y sistemas especiales de almacenamiento de alta velocidad o *cachés*.

Las evidencias a buscar por el auditor se basan en la comprobación de la existencia y cumplimiento de políticas o normativas documentadas sobre diversos aspectos relacionados con la medida concreta, como la especificación de las medidas de seguridad con que deben contar los servidores *web* a tenor de lo identificado en el análisis de riesgos, o si se determina desde la etapa de diseño la imposibilidad de acceder a la información sin la autenticación requerida, o se marca el protocolo de acceso a utilizar impidiendo que se utilice otro, o si se usan mecanismos para impedir ataques de manipulación de URL, o si se protegen las *cookies* frente a su manipulación, o existen mecanismos para impedir ataques de inyección de código, intentos de escalado de privilegios, ataques de *cross site scripting*, manipulación de *proxies* o de *cachés*. Resulta de utilidad también comprobar la realización de auditorías de seguridad y pruebas de penetración[756].

Habida cuenta de que el real decreto no puede profundizar en temas tan técnicos, su artículo 29 ha previsto la colaboración del CCN mediante la elaboración de sus guías de seguridad para las TIC. La propia guía 808 de verificación del cumplimiento del ENS recomienda al auditor la utilización de otras tres guías más específicas: la CCN-STIC-504 para la configuración segura de *Internet Information Services* 6.0, la CCN-STIC-671 para la

[755] *Vid*. CCN (2014), CCN-STIC-660.
[756] CCN (2011), CCN-STIC-808, 89-91.

configuración segura de servidores *web* Apache y la CCN-STIC-672 como guía de seguridad de Tomcat[757].

5.2.2.5. Medidas de gestión de personal

La gestión de los recursos humanos presenta una importante incidencia sobre la seguridad del *software* de las Administraciones públicas, pues el ser humano es el eslabón más débil de la cadena que sostiene esa seguridad. En ocasiones la amenaza está dentro de la propia organización, son los propios empleados, que cuentan con acceso a información privilegiada y son capaces de aprovechar procedimientos internos de seguridad descuidados y de moverse por los sistemas de la organización sin dejar rastro. Muchos permiten a compañeros utilizar sus credenciales, comprometiendo el sistema. La "ingeniería social" por parte de intrusos maliciosos busca acceso al sistema a través de cualquier truco imaginable para conseguir que un usuario legítimo comparta sus contraseñas.

Tanto los usuarios como el personal de las TIC son una importante fuente de errores. Por parte de los usuarios, se producen por la introducción de datos equivocados o por no seguir las instrucciones adecuadas para el procesamiento los datos y uso del sistema, mientras que los informáticos, intencionadamente o no, pueden dar lugar a errores de *software* al diseñar y desarrollar nuevos programas o mantener los ya existentes.

La creciente complejidad y el tamaño de los programas, junto con las demandas de entrega en el plazo fijado, han contribuido al incremento de los defectos del *software* y a sus vulnerabilidades. Un programa relativamente pequeño, de varios cientos de líneas, puede

[757] CCN (2011), CCN-STIC-808, 90-91.

contener decenas de decisiones que conducen a cientos o incluso miles de diferentes caminos. Y las aplicaciones importantes son, por lo general, muchos más grandes; contienen incluso millones de líneas de código que hacen imposible probar o revisarlo por completo o eliminar todos los defectos. Cada año se identifican miles de vulnerabilidades. En 2011, Symantec identificó 70 en el navegador Chrome, alrededor del 50 en Safari y Firefox, y otros 50 en Internet Explorer, algunas de las cuales fueron críticas[758].

El ENS dedica un bloque de medidas a la "Gestión de personal", aunque no específicamente dedicado a personal informático.

Dimensiones afectadas	Categorías afectadas			Medidas de seguridad	
	Básica	Media	Alta		
				mp.per	Gestión del personal
Cualquiera	No aplica	aplica	aplica	mp.per.1	Caracterización del puesto de trabajo
Cualquiera	aplica	aplica	aplica	mp.per.2	Deberes y obligaciones
Cualquiera	aplica	aplica	aplica	mp.per.3	Concienciación
Cualquiera	aplica	aplica	aplica	mp.per.4	Formación
Disponibilidad	No aplica	No aplica	aplica	mp.per.9	Personal alternativo

Figura 17: Medidas de gestión de personal

Fuente: BOE de 4 de noviembre de 2015, 104251.

(convenciones adaptadas por la autora para aumentar la legibilidad)

La primera de estas medidas, "**caracterización del puesto de trabajo**", afecta a todas las dimensiones de la seguridad y es de obligado cumplimiento en los sistemas de categoría media o alta, sobre los que se aplica del mismo modo. Dispone la definición de las

[758] LAUDON, K.C./ LAUDON, J.P. (2014), *Management Information Systems*, 335- 338.

responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad basándose en el análisis de riesgos, indicando los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad. Obliga a tener en cuenta dichos requisitos en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.

El auditor que evalúe el cumplimiento del ENS puede examinar, de nuevo, las políticas y normativas documentadas, en busca de la caracterización de cada puesto de trabajo en materia de seguridad, donde se definan las responsabilidades de cada uno y los requisitos del ocupante del puesto, verificando que esos requerimientos se exigen realmente en el proceso de provisión, incluyendo la comprobación de los antecedentes. El auditor podrá revisar quién ostenta cada puesto y sus referencias[759].

Lo dispuesto en esta medida del ENS, en el caso de la Administración pública, parece empujar a la revisión y actualización de las RPTs en materia de seguridad. En las empresas del sector privado que pretendan obtener la declaración o certificación de conformidad con el ENS, sería necesario disponer de algún instrumento similar.

La medida denominada "**deberes y obligaciones**" afecta a todas las dimensiones de la seguridad y se aplica por igual en cualquiera de las tres categorías de sistemas. Dispone que se informe a cada persona de los deberes y responsabilidades de su puesto en materia de seguridad, especificándole las medidas disciplinarias a que haya lugar, cubriendo tanto el periodo

[759] CCN (2011), CCN-STIC-808, 58-59.

de desempeño como el posterior a la finalización del mismo, tiempo en el que subsistirá el deber de confidencialidad.

El ENS también contempla al personal contratado a través de un tercero, disponiendo que se han de establecer los deberes y obligaciones del personal y de cada parte, así como el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

El auditor revisará la política o normativa documentada comprobando si se especifica la forma de informar al empleado y de recabar su aceptación explícita y firmada, consultando los documentos ya rubricados. En caso de externalización podría ser útil la revisión del contrato. Se puede considerar como evidencia que exista un procedimiento documentado que defina la resolución de incidentes relacionados con el incumplimiento de las obligaciones por parte del personal del tercero, así como la identificación de una persona de contacto para la resolución de este tipo de incidentes[760].

La guía 808 de verificación del cumplimiento contempla de forma separada la dimensión de confidencialidad en la categoría media, particularidad que no aparece en el ENS, donde se considera la misma aplicación para las tres categorías. Lo que la guía sugiere al auditor para la categoría media es la comprobación de la existencia de un acuerdo de confidencialidad firmado.[761]

[760] CCN (2011), CCN-STIC-808, 59-60.
[761] CCN (2011), CCN-STIC-808, 60.

La medida que lleva por nombre "**concienciación**", afecta a todas las dimensiones y se aplica por igual en todas las categorías. Contempla la realización de las acciones necesarias para concienciar regularmente al personal sobre su papel y responsabilidad para lograr los niveles exigidos de seguridad y, en particular, el recordatorio periódico de la normativa de seguridad relativa al buen uso de los sistemas, la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado, así como el procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

A pesar de que el ENS no establece diferencias en su aplicación a los sistemas de distintas categorías, la guía 808 sí lo hace. Sugiere al auditor la comprobación de los requisitos de ejecución y la existencia de un procedimiento documentado que indique quién es el responsable de la elaboración del plan de concienciación, su periodicidad y contenido. Para los sistemas de categoría media, se analiza la financiación, para lo cual cabría comprobar que en el procedimiento documentado consta el cálculo de los recursos necesarios para su ejecución regular. Para los sistemas de categoría alta, la guía añade la comprobación de que cada persona ha recibido y seguido el plan de concienciación, lo que se evidenciaría con la existencia de registros donde quede constancia de esa asistencia[762].

Dado que el mayor problema que afecta a la seguridad de la información normalmente proviene de las personas, la formación y la concienciación del personal se convierten en objetivos fundamentales a perseguir. Se implementará un programa de

[762] CCN (2011), CCN-STIC-808, 60-61.

concienciación en seguridad, dirigido directamente al usuario. Para INCIBE, es el eslabón más importante en relación con la ciberseguridad, pues la fuga de información tiene "*un componente social y humano muy importante*". Sostiene que detrás de ese tipo de incidente "*se esconden motivaciones personales, económicas, daño a la imagen de la organización o simples errores, entre otras*"[763].

Un adecuado programa de concienciación debe aclarar cómo proteger los activos, explicar por qué es importante proporcionar esa protección y cómo convertir a los usuarios en la primera barrera interpuesta ante los peligros que acechan. Es preciso hacerles comprender que la seguridad no es únicamente responsabilidad del personal informático y de otros expertos en la materia, y que resulta imprescindible incluir ciertos buenos hábitos en su actividad diaria. "*La seguridad debe considerarse como parte de la operativa estándar, no como algo añadido al trabajo habitual, siendo fundamental la incorporación de la seguridad a la actividad laboral*"[764]. Por tanto, en íntima relación con la anterior, se incluye la medida de protección "**formación**" del personal, de forma regular, en las materias que requieran para el desempeño de sus funciones, especialmente en lo referente a configuración de sistemas, detección y reacción a incidentes y gestión de la información en cualquier tipo de soporte, cubriendo al menos las actividades de almacenamiento, transferencia, copias, distribución y destrucción.

De nuevo la guía 808 muestra discrepancias con el ENS. No contempla la dimensión de disponibilidad como una de las afectadas por la medida de protección, y establece comprobaciones diferentes para los sistemas de categoría baja y media. Sugiere al auditor la

[763] INCIBE (2015), una fuga de información, 3.
[764] CCN (2013), CCN-STIC-400, 18.

verificación de la existencia de un plan de formación donde figure el responsable de su elaboración, las necesidades formativas de cada puesto, la planificación en la impartición y la frecuencia con la que debe actualizar. Habría que revisar también la extensión su cobertura. Para los sistemas de categoría media, prevé comprobar si existe constancia de la ejecución del plan formativo y la valoración dada al mismo[765].

La medida denominada "**personal alternativo**" solo afecta a la disponibilidad y se aplica de forma obligatoria únicamente al nivel alto. Consiste en garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en ausencia del personal habitual, quienes han de estar sometido a las mismas garantías de seguridad.

El auditor puede tomar como evidencia la existencia de un procedimiento documentado que identifique qué personas pueden suplir al personal habitual, que estén localizables y conozcan los procedimientos necesarios[766].

Por último, hemos de incluir en esta revisión de medias de seguridad útiles en el ámbito del desarrollo del *software* de las Administraciones públicas algunas medidas de protección del bloque operacional dedicado a la explotación.

5.2.2.6. Medidas de seguridad de explotación

[765] CCN (2011), CCN-STIC-808, 61-62.
[766] CCN (2011), CCN-STIC-808, 62-63.

Dimensiones afectadas	Categorías afectadas			Medidas de seguridad	
	Básica	Media	Alta		
				op.exp	Explotación
Cualquiera	aplica	aplica	aplica	op.exp.1	Inventario de activos
Cualquiera	aplica	aplica	aplica	op.exp.2	Configuración de seguridad
Cualquiera	No aplica	aplica	aplica	op.exp.3	Gestión de la configuración
Cualquiera	aplica	aplica	aplica	op.exp.4	Mantenimiento
Cualquiera	No aplica	aplica	aplica	op.exp.5	Gestión de cambios
Cualquiera	aplica	aplica	aplica	op.exp.6	Protección frente a código dañino
Cualquiera	No aplica	aplica	aplica	op.exp.7	Gestión de incidentes
Trazabilidad	aplica	aplica+	aplica ++	op.exp.8	Registro de la actividad de los usuarios
Cualquiera	No aplica	aplica	aplica	op.exp.9	Registro de la gestión de incidentes
Trazabilidad	No aplica	No aplica	aplica	op.exp.10	Protección de los registros de actividad
Cualquiera	aplica	aplica+	aplica+	op.exp.11	Protección de claves criptográficas

Figura 18: Medidas de seguridad de explotación

Fuente: BOE de 4 de noviembre de 2015, 104250-104251.

(convenciones adaptadas por la autora para aumentar la legibilidad)

La medida denominada "**configuración de seguridad**" hace referencia a la configuración de los equipos, extensible también a las aplicaciones informáticas, especialmente cuando dispone que, previamente a su entrada en operación, se retirarán cuentas y contraseñas estándar y se aplicará la regla de "mínima funcionalidad", es decir, se proporcionará la requerida para que la organización alcance sus objetivos y ninguna otra, desactivando aquellas funciones que no sean de interés, resulten no necesarias o sean inadecuadas al fin que se persigue. Se aplicará la regla de "seguridad por defecto", en el sentido de que las medidas de seguridad serán respetuosas con el usuario y lo protegerán, salvo que se exponga conscientemente a un riesgo. El ENS establece un uso natural seguro para los casos en que el usuario ni siquiera haya consultado el manual de utilización.

La medida llamada "**gestión de cambios**" es de cumplimiento obligado para los sistemas de categoría media y alta, a los que se aplica por igual. Se debe mantener un control continuo de los cambios realizados. Antes de poner en producción una nueva versión se debe comprobar su correcto funcionamiento en un equipo que no esté en el entorno de producción. Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Además, será necesario determinar si los cambios son relevantes para la seguridad del sistema; los que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.

El auditor puede comprobar si se dispone de un procedimiento documentado que indique la frecuencia y motivos de los cambios, la aprobación del responsable, la documentación asociada a las modificaciones, las pruebas de seguridad del sistema tras el cambio y la retención de una copia del componente previo por un tiempo preestablecido. También puede comprobar si dicho procedimiento contempla la ventana de tiempo en que el cambio afecta en menor medida a los servicios relacionados, realizándose en dicho periodo si se estima oportuno[767].

Una empresa de servicios financieros dedicada a la venta de automóviles fue sancionada con 40.001 € por incluir los datos de uno de sus clientes en un fichero de morosos, de forma automática, manifestando haber sido ocasionado por un error informático[768]. Si fue así, un cambio incorrecto llegó hasta el entorno de explotación, manifestándose en la producción de un incidente de seguridad.

[767] CCN (2011), CCN-STIC-808, 37-38.
[768] SAN 1419/2012 de 22 de marzo de 2012, sala de lo contencioso.

La medida de seguridad llamada "**gestión de incidentes**" es de aplicación obligatoria por igual a los sistemas categorizados como de nivel medio o alto. Se entiende por incidente de seguridad al conjunto de uno o más eventos de seguridad no planificados que presentan una probabilidad significativa de comprometer las operaciones y amenazar a la seguridad corporativa. Para afrontarlos, debe disponerse de un proceso integral, dando una respuesta correcta, ágil y proporcional, reduciendo al mínimo su impacto y la frecuencia de repetición[769].

El proceso ha de incluir procedimientos para reportar los eventos de seguridad y debilidades (detallando los criterios de clasificación y el escalado de la notificación), para adoptar medidas urgentes (incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros), para asignar recursos para investigar las causas, analizar las consecuencias y resolver el incidente, para informar a las partes interesadas, internas y externas, para prevenir la repetición del incidente, para incluir en los procedimientos de usuario la identificación y forma de tratar el incidente y, por último, para actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

El ENS se detiene especialmente en la gestión de incidentes que afecten a datos de carácter personal, recordando que se ha de tener en cuenta también lo dispuesto en la LOPD y sus normas de desarrollo.

El auditor podrá comprobar la existencia de ese procedimiento, su contenido y su aplicación en incidentes anteriores, así como la asignación de recursos para investigar las causas

[769] CCN (2013), CCN-STIC-400, 96-97.

y consecuencias, y resolver el incidente. También puede verificar si ese procedimiento está alineado o coordinado con el procedimiento de gestión de incidencias de la LOPD[770].

La medida denominada "**registro de la actividad de los usuarios**" afecta únicamente a la trazabilidad. El ENS establece su aplicación obligatoria en todos los sistemas, en mayor intensidad conforme aumenta al incrementarse el nivel. Las aplicaciones informáticas registrarán la actividad de los usuarios, tanto las exitosas como los intentos fracasados, guardando el detalle de quién la realiza, cuándo y a qué información accede, incluyendo también las operaciones realizadas por operadores y administradores con permisos especiales sobre el sistema. A través del análisis de riesgos se determina qué actividades registrar y con cuánto detalle. En sistemas de categoría baja se guardarán los registros de actividad en los servidores. En los de nivel medio se revisarán informalmente los registros de actividad buscando patrones anormales. En el nivel alto se dispondrá de un sistema automático de recolección de registros y correlación de eventos, una consola de seguridad centralizada.

Entre las evidencias a estudiar por el auditor figuran el detalle de los mecanismos a utilizar para mantener el reloj del sistema en hora y la presencia de herramientas para analizar los registros en busca de actividades fuera de lo normal. También puede consultar si los mecanismos de registro almacenan los accesos a la configuración del sistema de forma que los propios operadores y administradores no puedan modificarlos, y los intentos exitosos y los

[770] CCN (2011), CCN-STIC-808, 39-41.

accesos fracasados. La guía 808 recomienda al auditor la consulta de otra guía, la dedicada a las herramientas de análisis de ficheros de *log*, CCN-STIC-434[771].

La medida llamada por el ENS "**registro de la gestión de incidentes**"[772] se aplica a las categorías media y alta por igual. Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, guardando el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente. También se grabará toda evidencia susceptible de sustentar o hacer frente a una demanda judicial, o pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o facilite la persecución de delitos. El ENS establece el recurso a asesoramiento legal especializado para determinar la composición y detalle de esas evidencias. Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

El auditor puede comprobar la existencia de evidencias documentales de los registros generados durante la gestión de incidencias, así como que se ha recurrido a asesoramiento legal en la determinación de la composición y el detalle, y que se han seguido sus recomendaciones. Puede consultar si el personal responsable de estas actividades conoce el procedimiento y dispone de los medios para ponerlo en práctica[773].

5.2.3. Normas de seguridad

El Centro criptológico nacional, a través de su "Guía de seguridad (CCN-STIC-821) - Esquema nacional de seguridad - Normas de seguridad", de abril de 2013, viene a

[771] CCN (2011), CCN-STIC-808, 41-42.
[772] La guía 808, en su página 42, lo bautiza como "registro de la gestión de incidencias".
[773] CCN (2011), CCN-STIC-808, 42-43.

proponer a nuestras Administraciones públicas una relación de "normas de seguridad" que se ajustan a la previsión del ENS, real decreto donde se insta a los organismos públicos a desarrollar, publicar y hacer valer normas de carácter interno para incrementar el nivel de seguridad. Como resalta la propia guía, esa necesidad de completar el marco normativo aparece prevista en artículos como el 14.3, sobre gestión de personal, donde explicita que "*el significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad*", o con diversos tenores en el 18 (adquisición de productos de seguridad), 21 (protección de información almacenada y en tránsito), 23 (registro de actividad), 34 (auditoría de la seguridad), 37 (prestación de servicios de respuesta a incidentes de seguridad en las Administraciones públicas), disposición adicional tercera (comité de seguridad de la información de las Administraciones públicas), etc.

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Figura 19: Normativa de seguridad

Fuente: BOE de 29 de enero de 2010, 19.

Entre las medidas de seguridad incluidas en el marco organizativo se incluye la denominada "**normativa de seguridad**", que afecta a todas sus dimensiones y se aplica a todas las categorías, básica, media y alta, por igual. Esta medida establece la obligación de disponer de

una serie de documentos que describan el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido y la responsabilidad del personal con respecto al cumplimiento o violación de estas normas, especificando derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

La precitada guía 821 subraya la habilitación a los organismos de las Administraciones públicas para promover su propia normativa interna y de relación con terceros, señalando cómo se alienta en varias medidas de seguridad del ENS, entre las que cita, a modo de ejemplo, la de requisitos de acceso [op.acc.2], deberes y obligaciones [mp.per.2], concienciación [mp.per.3], formación [mp.per.4] y protección del correo electrónico (*e-mail*) [mp.s.1].

Es el artículo 29 del ENS el que encarga al CCN la elaboración y difusión de las guías STIC, pero es en el 37 donde establece que ofrecerá normas, instrucciones, guías y recomendaciones para aplicar el ENS y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración y, en cumplimiento de este mandato, incluye en la guía 821 algunos modelos de normas de seguridad que pueden (no imperativamente) ser utilizadas por los organismos de las Administraciones públicas. Entre esas normas queremos destacar, por su incidencia en la externalización del desarrollo del *software*, el apéndice IV, titulado “Normas para trabajar fuera de las instalaciones del organismo. NP30”, el VI, denominado “Acuerdo de confidencialidad para terceros. NP50” y el VII, llamado “Modelo de contenido de buenas prácticas para terceros. NP60”.

6. ANÁLISIS DE RIESGOS EN LAS ADMINISTRACIONES PÚBLICAS

Cabe aplicar las palabras de Esteve Pardo[774], "*En materia de riesgos el Derecho debe actuar en cierto modo contra sí mismo, debe hacerse reflexivo*". Se trata de unos riesgos cuyo origen se materializa en la tecnología que vertebra las sociedades modernas, una tecnología que, como continúa afirmando, "*cumple con el Derecho, reconocida por el Derecho y, en muchos casos, incentivada por el Derecho*". No se trata de analizar los riesgos de actividades ilegales, sino los que acompañan a las TIC al servicio de las propias Administraciones públicas.

"*Las TIC hacen surgir el **riesgo** (y el mito) del Gran Hermano orwelliano que todo lo controla y todo lo ve, sumiendo a la intimidad y a la seguridad en una utopía (si bien es cierto que ello es una interpretación un tanto hiperbólica que desconoce que los avances también traen consigo nuevos mecanismos de **defensa** de la vida privada y no sólo instrumentos agresivos con la misma)*"[775]. Riesgo y defensa, dos palabras enfrentadas que vienen a resumir la situación de los sistemas informáticos de nuestras Administraciones públicas, a las que dedicamos las próximas páginas.

Las TIC, en sí mismas, no son un riesgo; lo es su mal uso, que puede derivar en desconfianza e inseguridad. Resulta básico saber dónde está realmente la amenaza para poder articular adecuadamente las medidas de defensa[776].

Cada cambio que tiene lugar en una organización lleva asociados unos riesgos inherentes, que pueden derivar hacia algo totalmente inocuo o potencialmente desastroso. En

[774] ESTEVE PARDO, J. (2003), ciencia y Derecho, 141.
[775] FERNÁNDEZ RODRÍGUEZ, J.J./ SANJURJO RIVO, V.A. (2010), acceder o no, 263 (la negrita es nuestra).
[776] MIRALLES LÓPEZ, R. (2009), modelos de evaluación, 752.

previsión de ello, las empresas tratan de aumentar su grado de resiliencia, para resistir las perturbaciones que las pudieran zarandear y regresar a su estado de calma original cuando estas hayan cesado[777].

La noción de riesgo tiene entrada en nuestra estrategia de ciberseguridad. Entre sus principios rectores figura el de "proporcionalidad, racionalidad y eficacia", que recoge la necesidad de "*gestionar los riesgos derivados del uso de la tecnología de forma dinámica, equilibrando oportunidades y amenazas, asegurando la proporcionalidad en las medidas de protección adoptadas, que habrán de ser elementos habilitantes de la confianza y no trabas al desarrollo de nuevos servicio*". Su objetivo IV consiste en la sensibilización de ciudadanos, profesionales, empresas y Administraciones públicas españolas ante los riesgos derivados del ciberespacio, con el convencimiento de que la gestión eficaz de los mismos requiere de una sólida cultura de ciberseguridad que incluya el conocimiento de las herramientas para la protección de información, sistemas y servicios[778].

Esa sensibilización en la materia con la que se quiere impregnar el ambiente podría comenzar con la difusión de cuatro axiomas de la era cibernética que convendría que la sociedad interiorizara[779]:

- No existen sistemas informáticos 100% seguros y probados, solo sistemas cuyos fallos aún no han sido descubiertos.

[777] MARTÍN ROMERAL, L./ TORRES GALLEGO, Á. (2008), riesgos tecnológicos, 14.
[778] PRESIDENCIA DEL GOBIERNO (2013), estrategia de ciberseguridad nacional, 16-23.
[779] CARO BEJARANO, M.J. (2013), peligros tecnológicos, 199.

- Cualquier dispositivo con *software* basado en el comportamiento del usuario puede ser manipulado para hacer cosas que sus creadores no tenían previstas.
- Cualquier dispositivo conectado a una red puede verse comprometido por un tercero.
- La ciberseguridad es un problema que ninguna organización, pública o privada, puede resolver por sí sola.

La criticidad del ciberespacio ante las vulnerabilidades hace que su protección y el aumento de su capacidad de resistencia y recuperación se conviertan en aspectos vitales que potenciar, junto con el fortalecimiento de la legislación y el fomento de la colaboración público-privada[780], cuya intensificación es una de las características más destacadas de la implantación de la Administración electrónica[781]. La postura expectante de quien teme a los problemas confiando en que nunca acontezcan no parece productiva. Se necesita presentar una actitud proactiva, no solo reactiva, lo que requiere una solución integral que englobe seguridad lógica y física, y también el aumento de los recursos humanos y económicos[782], algo que en momentos de crisis y restricciones presupuestarias no parece muy factible. Teniendo en cuenta esas dificultades financieras, se torna si cabe más importante priorizar los riesgos identificados, categorizarlos, decidiendo cuáles deben ser abordados, aceptando dócilmente la premisa de que nunca se dispondrá de tiempo ni de recursos suficientes para afrontar todos ellos[783].

[780] CARO BEJARANO, M.J. (2013), peligros tecnológicos, 195.
[781] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 360.
[782] CARO BEJARANO, M.J. (2013), peligros tecnológicos, 202.
[783] MARTÍN ROMERAL, L./ TORRES GALLEGO, Á. (2008), riesgos tecnológicos, 17.

El ENS, dentro de las medidas contempladas dentro del marco operacional, dedica un subconjunto a la planificación. La primera de ellas, "op.pl.1", lleva por denominación "**análisis de riesgos**".

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	++

Figura 20: Análisis de riesgos

Fuente: BOE de 29 de enero de 2010, 20.

El análisis de riesgos afecta a todas las dimensiones de la seguridad y a todas las categorías, pero las exigencias del ENS se endurecen según va elevándose esta última. Mientras en la categoría básica es suficiente con realizar un análisis informal en lenguaje natural, en el que se identifiquen los activos más valiosos del sistema, las amenazas más probables con las salvaguardas que protegen de ellas y los principales riesgos residuales, en la categoría media ese análisis ha de ser semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Para la categoría alta se exige la realización de un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que cubra la identificación y valoración cualitativa de los activos más valiosos del sistema, la identificación y cuantificación de las amenazas posibles y de sus vulnerabilidades habilitantes, identificación y valoración de las salvaguardas adecuadas y, finalmente, la identificación y valoración del riesgo residual.

Si bien el análisis de riesgos procede realizarlo cuando así lo disponga directa o indirectamente la normativa aplicable, nada obsta su elaboración cuando se estime conveniente para la protección responsable de los activos de la organización[784].

6.1. INTRODUCCIÓN A MAGERIT 3.0

El artículo 13 del ENS, bajo la rúbrica de "Análisis y gestión de los riesgos", ha previsto, para cada organización que desarrolle e implante sistemas TIC, la realización de su propia gestión de riesgos, empleando alguna metodología reconocida internacionalmente.

El CSAE ha elaborado la metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT, con la intención de conocer y poder gestionar aquellos riesgos que acompañan al uso de las TIC, pretendiendo que sea aplicada en nuestras Administraciones públicas. Aunque se trata de una metodología perteneciente al MAP, cualquier organización que trabaje con información y sistema informáticos puede estar interesada en su uso, para lo que no requiere autorización previa[785].

Las ventajas de su utilización se deducen del tenor del artículo 6 del ENS, conforme al cual el análisis y la gestión de riesgos, que deben mantenerse permanentemente actualizados, son una parte esencial del proceso de seguridad que nos permite el mantenimiento de un entorno controlado, donde se minimicen los riesgos hasta niveles aceptables, mediante el despliegue de medidas de seguridad. A la determinación de esos niveles que se consideran aceptables se llega buscando un punto de equilibrio en el que sopesen la naturaleza de los datos y

[784] MINHAP. MAGERIT 3.0, libro I – Método, 18.
[785] INTECO (2008), guía avanzada sobre gestión de riesgos, 55.

sus tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad aplicables. La realización del análisis y la gestión de riesgos, conforme al artículo 11 del ENS, irá íntimamente ligada a la política de seguridad y, en función de los resultados obtenidos, permitirá establecer los requisitos mínimos aplicables que, incluso, podrán ser inexistentes allá donde no existan riesgos significativos.

MAGERIT parte de un concepto de riesgo[786] definido como la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios. Declara como objetivos directos[787] la concienciación de los responsables de la existencia de riesgos y de la necesidad de gestionarlos, la proposición de un método sistemático para analizar aquellos que se deriven del uso de las TIC, así como la ayuda para descubrir y planificar el control de los mismos. A su vez, sirve de piedra angular de los procesos de evaluación, certificación, auditoría[788] y acreditación que formalizan la confianza que merece el sistema[789].

El análisis de riesgos engloba las siguientes tareas[790]:

MAR.1 – Caracterización de los activos.

MAR.11 – Identificación de los activos.

MAR.12 – Dependencias entre activos.

[786] MINHAP. MAGERIT 3.0, libro I – Método, 9.
[787] MINHAP. MAGERIT 3.0, libro I – Método, 8.
[788] El propio esquema nacional de seguridad y la normativa de protección de datos de carácter personal exigen la realización de auditorías periódicas, que partirán del análisis de riesgos realizado a los sistemas de información.
[789] MINHAP. MAGERIT 3.0 , libro I – Método, 14.
[790] *Vid*. MINHAP. MAGERIT 3.0, libro I – Método, 36-45.

MAR.13 – Valoración de los activos.

MAR.2 – Caracterización de las amenazas.

MAR.21 – Identificación de las amenazas.

MAR.22 – Valoración de las amenazas.

MAR.3 – Caracterización de las salvaguardas.

MAR.31 – Identificación de las salvaguardas pertinentes.

MAR.32 – Valoración de las salvaguardas.

MAR.4 – Estimación del estado de riesgo.

MAR.41 – Estimación del impacto.

MAR.42 – Estimación del riesgo.

La documentación finalmente obtenida tras la realización del análisis de riesgos contiene un "modelo de valor" donde se detallan los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada una, un "mapa de riesgos" que describe las amenazas significativas sobre cada activo caracterizadas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo, una "declaración de aplicabilidad" que recoge las contramedidas que se consideran apropiadas para defender el sistema de información, una "evaluación de salvaguardas" existentes, calificadas según su eficacia para reducir el riesgo que afrontan, un "informe de insuficiencias o vulnerabilidades" que incluye el detalle de las salvaguardas necesarias pero ausentes o insuficientemente eficaces y

un “estado de riesgo” donde describe el impacto y riesgo para cada activo frente a cada amenaza. Esta documentación es un fiel reflejo del estado de riesgo y de las razones por las que no es aceptable. Es fundamental entender las razones que llevan a una valoración determinada para que el proceso de gestión de riesgos esté bien fundamentado. Dicho proceso partirá de esas valoraciones para atajar el riesgo o reducirlo a niveles aceptables[791].

En su apartado de “consejos prácticos”, MAGERIT recomienda ciertas protecciones basadas en las amenazas esperadas para la Administración electrónica. Dice así: “*registre cuidadosamente quién hace qué en cada momento pues se enfrentará a incidencias con los usuarios, teniendo que determinar quién tiene razón y quién paga los perjuicios. También habrá quien quiera usar sus servicios sin tener derecho a ello (fraude).*

Lo que se puede necesitar, es necesario, y parte de las responsabilidades del responsable de seguridad es disponer de la información correcta cuando haga falta”[792]. Se trata de un interesante párrafo que no parece haberse aplicado en la reciente STSJ de Madrid 1140/2015, sala de lo contencioso, de fecha 30 de enero de 2015 que se verá *infra*.

Las guías de MAGERIT parten de un criterio de máximos, requiriendo su adaptación al sistema concreto a que se aplique. Resulta recomendable emprender una aproximación iterativa, descendiendo progresivamente en cada vuelta, alcanzando cada vez mayores detalles[793]. Describen un proceso, conforme a las normas ISO 31000, que parte de la determinación del contexto, examinando parámetros y condicionantes externos e internos,

[791] MINHAP. MAGERIT 3.0, libro I – Método, 45-46.
[792] MINHAP. MAGERIT 3.0, libro I – Método, 96.
[793] MINHAP. MAGERIT 3.0, libro I – Método, 13.

obligaciones propias y contraídas, relaciones con otras organizaciones… La identificación posterior de los riesgos busca una relación de los posibles puntos de peligro. Su análisis pretende calificar los riesgos identificados, revisando sus consecuencias con un análisis cuantitativo u ordenando su importancia relativa mediante un enfoque cualitativo. La evaluación de los riesgos traduce las consecuencias a términos de negocio, permitiendo tomar decisiones respecto a qué riesgos se aceptan y cuáles no, y en qué circunstancias aceptarlo o bien trabajar en su tratamiento.[794] El enfoque cualitativo evalúa el nivel de riesgo de seguridad de un sistema informático mediante el uso de distintas encuestas, entrevistas y cuestionarios técnicos. Se requiere la preparación de diferentes escenarios para analizar si se compromete la seguridad, con el fin de ilustrar la vulnerabilidad de la organización a los ataques. El enfoque cuantitativo asigna un valor numérico absoluto a los activos, amenazas, vulnerabilidades y contramedidas. La identificación exacta de los riesgos y la justificación de costos/beneficios de las contramedidas son fundamentales para la construcción de una buena estrategia de mitigación de riesgos[795].

MAGERIT menciona la importancia de tener siempre en mente que los sistemas de información han de ser soporte de la productividad de la organización, por lo que "*es absurdo un sistema muy seguro pero que impide que la organización alcance sus objetivos*", debiendo buscar el equilibrio entre seguridad y productividad[796].

El CCN ha desarrollado la herramienta PILAR, "procedimiento informático-lógico para el análisis de riesgos", al objeto de dar soporte a ese análisis de riesgos de sistemas

[794] MINHAP. MAGERIT 3.0, libro I – Método, 20.
[795] BISTARELLI, S./ FIORAVANTI, F./ PERETTI, P. (2006), *defense trees*.
[796] MINHAP. MAGERIT 3.0, libro I – Método, 20.

de información siguiendo la metodología MAGERIT. Se trata de una herramienta capaz de calcular calificaciones de seguridad siguiendo los epígrafes de normas *de iure* o *de facto* de uso habitual, entre ellas UNE-ISO/IEC 27002:2009 (sistemas de gestión de la seguridad), el real decreto 1720/2007 (datos de carácter personal) y el propio real decreto 3/2010 (ENS).

6.2. VALORACIÓN DE LOS ACTIVOS

Todo sistema de información cuenta con dos ingredientes esenciales: la información que maneja y los servicios que presta. Esos elementos primarios son los que marcan los requisitos de seguridad para todos los demás componentes del sistema. Junto a esos activos esenciales habrá otros, entre los que, únicamente a modo ilustrativo, podemos citar las claves criptográficas, el equipamiento informático (*hardware*), las redes de comunicaciones, los soportes de información, el equipamiento auxiliar, las instalaciones, el personal… y las propias aplicaciones informáticas. Sin embargo, refiriéndose precisamente a estas, al *software*, MAGERIT[797] puntualiza su significado, aclarando que las considera un activo en sí mismas en el sentido de "*tareas que han sido automatizadas para su desempeño por un equipo informático*", pero no en el sentido de código fuente (desde este último punto de vista, las incluye dentro del apartado de "datos", de interés comercial, es decir, como un activo esencial).

MAGERIT aborda la valoración de los activos[798], considerando como tal, conforme a la norma UNE 71504:2008, al componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización,

[797] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 10.
[798] MINHAP. MAGERIT 3.0, libro I – Método, 25-27.

lo que incluye información, datos, servicios, aplicaciones, equipos, comunicaciones y recursos humanos, físicos y administrativos. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo, lo que incluirá aspectos como el gasto de reposición englobando adquisición e instalación, coste de mano de obra, pérdida de ingresos por lucro cesante, capacidad de operar (denominando así a la confianza de los usuarios y proveedores, cuya disminución se traduce en una pérdida de actividad o en peores condiciones económicas), sanciones por incumplimiento de la ley o de posibles obligaciones contractuales, menoscabos en otros activos propios o ajenos, daño a personas, deterioros en el medio ambiente…[799]

No siempre es posible traducir a cifras dinerarias la valoración, especialmente cuando afecta a conceptos abstractos, intangibles, como la credibilidad de la organización. Una valoración cualitativa permite posicionar el valor de cada activo en un orden relativo respecto de los demás, frecuentemente planteando las escalas como "órdenes de magnitud", con el inconveniente de que no se pueden sumar valores, algo que se realiza con naturalidad en las estimaciones dinerarias y que permite elaborar estudios cuantitativos de costes y beneficios.

6.3. AMENAZAS

La norma UNE 71504:2008 las describe como toda causa potencial de un incidente que puede producir daños a un sistema de información o a una organización, pudiendo tener un origen natural, provenir del entorno industrial, nacer de defectos en las aplicaciones (lo

[799] Para ampliar la información referente a los criterios de valoración, puede consultarse MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 19-23.

que se suele denominar “vulnerabilidad”) o ser causada por las personas de forma accidental o deliberada[800].

La degradación mide el daño causado por un hipotético incidente y suele describirse como una fracción del valor del activo, siendo habitual utilizar expresiones como “totalmente degradado” o “degradado en una pequeña fracción”. Cuando las amenazas son intencionales, probablemente no será suficiente saber cuál es la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se malogra, pues el atacante puede causar muchísimo daño incidiendo sobre una pequeña proporción escogida detenidamente de forma selectiva. La probabilidad de ocurrencia presenta mayor complejidad para su determinación, siendo usual expresarla y modelarla cualitativamente por medio del uso de alguna escala nominal[801].

Se denomina “impacto” a la medida del daño sobre el activo derivado de la materialización de una amenaza, y “riesgo” a la medida del daño probable sobre un sistema. En ausencia de salvaguardas, conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia[802].

La identificación exhaustiva de amenazas, para cada activo y para cada dimensión de la seguridad, podría parecer casi imposible en principio. Ayuda contar con la experiencia pasada y, complementariamente, disponer de un catálogo de amenazas. MAGERIT, consciente

[800] MINHAP. MAGERIT 3.0, libro I – Método, 27.
[801] MINHAP. MAGERIT 3.0, libro I – Método, 28. El texto ofrece algunos ejemplos de escalas de probabilidad que podrían servir de modelo.
[802] *Vid*. MINHAP. MAGERIT 3.0, libro I – Método, 28-31, para profundizar en los conceptos de impacto y de riesgo.

de tal dificultad, al igual que otras metodologías, propone la utilización, en una primera aproximación, de su "catálogo de elementos", permitiendo así un acercamiento inicial que posteriormente se podrá mejorar. La técnica denominada “árboles de ataque” consiste en idear escenarios similares a dramatizaciones de cómo un atacante se enfrentaría a nuestros sistemas, planteando diferentes situaciones según el perfil técnico del atacante y sus recursos técnicos y humanos[803].

La valoración de las amenazas no resulta tarea sencilla, especialmente en relación a los errores humanos, aunque el recurso a la experiencia facilita aquilatar valores realistas. La complejidad aumenta al tratar con ataques deliberados, los cuales dependen en gran medida de la suerte. Sin embargo, una serie de factores permiten agudizar el peligro de la amenaza, tal y como indica MAGERIT en su apartado de “consejos prácticos”, donde identifica los siguientes motivos de agravación:

- Sencillez técnica, en el sentido de no requerir grandes conocimientos especializados por parte del atacante. Esta facilidad cada día es más frecuente, gracias a las herramientas que, a tal efecto, pueden adquirirse por Internet a precios irrisorios[804].
- Bajo coste, por no suponer para el atacante grandes inversiones en equipos tecnológicos. La potencia de cálculo necesaria se sustituye de forma barata, apropiándose de la capacidad de cálculo de un número enorme de equipos ajenos conectados a la red, haciendo que trabajen para el atacante.

[803] MINHAP. MAGERIT 3.0, libro I – Método, 93.
[804] *Vid*. disponibilidad y precios de algunas de esas herramientas en “*North American Underground: The Glass Tank*”, de WILHOIT Y HILT, *Trend Micro Incorporated*, 2015.

- Rentabilidad económica elevada, por posibilitar grandes beneficios que desemboquen en el enriquecimiento del atacante.
- Importante satisfacción no económica, entendida como la consecución de grandes beneficios no dinerarios para el atacante, entre los que se incluye el prestigio personal o su mayor autoestima. MAGERIT añade una coloquial frase repleta de sentido como consejo para quien desee mantener alejados a los ciberatacantes: "*por lo que más quiera, evite los retos y jamás alardee de que su sistema de información es invulnerable: no lo es y no tiene gracia que se lo demuestren*".
- Existencia de un mal ambiente de trabajo que siembra empleados descontentos y recoge su venganza a través de los sistemas, simplemente para causar daño.
- Mala relación con los usuarios externos, quienes se desquitan a través de los sistemas que utilizan[805].

MAGERIT 3.0 proporciona un inventario no exhaustivo de errores o fallos de origen humano, diferenciándolos en accidentales o intencionados. Algunos guardan una íntima relación con el desarrollo del *software*, los cuales paso a comentar.

6.3.1. Con origen humano accidental

MAGERIT 3.0 incluye, dentro de su inventario no exhaustivo, una lista de errores o fallos no intencionados de origen humano accidental[806]. Puede seleccionarse en esa lista, a

[805] MINHAP. MAGERIT 3.0, libro I – Método, 93.
[806] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 33-39.

modo de ejemplo, los que previsiblemente presentan una relación más cercana con la seguridad del desarrollo de las aplicaciones.

6.3.1.1. [E.3] Errores de monitorización (*log*)

Los *logs* son ficheros que contienen información referente a las actividades realizadas mediante sistemas informáticos. Los desarrolladores de las aplicaciones pueden grabar en ellos toda la información que consideren de utilidad, como accesos de usuarios, fallidos o no, errores producidos en la aplicación, rastros que indican el orden en que se han ejecutado las sentencias, valores contenidos en un determinado momento por diferentes variables, mensajes de aviso, etc. Su utilidad es indudable a la hora de intentar reproducir la casuística que ha llevado a que se produzca un determinado suceso, normalmente asociado a funcionamientos inesperados.

Los ficheros de *log* son especialmente útiles en la detección de intrusos, ya que su revisión posterior puede detectar problemas no descubiertos en tiempo de ejecución, lo que significa que los atacantes, teóricamente, no tendrán tiempo para perfeccionar su ataque y volver a intentarlo[807].

Los *logs* suelen ser ficheros de texto muy voluminosos, por lo que se utilizan herramientas para facilitar su análisis y/o tratamiento.

Además de los ficheros de *log* descritos, que sirven para controlar la actividad del propio sistema informático, es necesario registrar la actividad de los usuarios, en cumplimiento

[807] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 5-6.

del artículo 23 del ENS, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar las actividades indebidas o no autorizadas.

Los errores no intencionados de monitorización consisten en un inadecuado registro de actividades, debido a la inexistencia de anotaciones que deberían haber sido realizadas, asientos incompletos o erróneamente fechados, registros incorrectamente atribuidos,... Una programación inadecuada de las aplicaciones y un deficiente juego de pruebas puede ser su origen.

Los errores en los *logs* afectan a la integridad de la información y repercuten en la trazabilidad. Un funcionamiento inadecuado podría provocar, a modo de ejemplo, que no se registrasen los accesos a las historias clínicas, o a los datos puestos a disposición de empleados públicos a través de la plataforma de intermediación de datos, o que no se pueda averiguar cómo han desaparecido años de cotización de la vida laboral de un trabajador. Este último ejemplo, real, se analizará *infra*.

En casos concretos, los errores de monitorización podrían afectar a la confidencialidad. El código del programa podría contener, por ejemplo, una sentencia de *logging* que realice un registro en un fichero de *log* del contenido de los elementos que se han ido añadiendo a la base de datos, entre los cuales podría encontrarse el valor devuelto por la función *getPassword*(), que es la contraseña en texto plano (no criptografiada) proporcionada por el usuario y asociada a su cuenta[808]. Grabando ese valor en el *log*, se ha violado la privacidad del usuario y se ha atentado contra la confidencialidad. Cualquiera que revise ese *log* tendría acceso

[808] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 44.

a su contraseña. Y si el usuario ha pecado de inocencia, teniendo todas las contraseñas de sus sistemas idénticas, sus credenciales habrán sido descubiertas en su totalidad, permitiendo, además, la fuga de información de otros sistemas diferentes.

6.3.1.2. [E.4] Errores de configuración

Afectan a la integridad de los datos de configuración. MAGERIT lo describe como una introducción de tales datos erróneos, explicando, a su vez, que prácticamente todos los activos dependen de esa configuración, diligencia realizada por el administrador, quien introduce los privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

Un error típico que genera un problema particularmente delicado surge por almacenar una contraseña en texto plano en un fichero de configuración. Cualquier usuario que tenga permisos de lectura sobre ese fichero tendrá acceso al recurso protegido por esa *password*, lo que facilita enormemente el trabajo de un atacante. Las buenas prácticas dictaminan que una contraseña nunca debe ser almacenada en texto plano[809].

Las mismas apreciaciones podemos hacerlas para la escritura de las credenciales de acceso en claro dentro del código de los programas, agravado por el hecho de que podrán ser vistas por todos los programadores, muchas veces incluso desarrolladores pertenecientes a servicios externos a la organización. *"Las contraseñas escritas directamente en el código fuente pueden comprometer la seguridad de un sistema de una manera que puede no ser fácilmente*

[809] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 20.

remediable"[810]. De ahí deriva mi preocupación personal por la publicación del código de las aplicaciones que masivamente reclama la doctrina.

6.3.1.3. [E.15] Alteración accidental de la información

Limitándonos al entorno de programación de aplicaciones, es difícil encontrar a un desarrollador que pueda afirmar, con sinceridad, no haber alterado accidentalmente los datos de algún fichero o del propio *software*. La manipulación del código de un programa no está garantizada ante los errores humanos. El alcance de los daños derivados del mismo podrá variar, desde ser inapreciable hasta llegar a provocar efectos catastróficos. Imaginemos, a modo de ejemplo, la modificación accidental y errónea del grupo sanguíneo de un paciente antes de que se le practique una transfusión. Un caso real aúna aspectos de confidencialidad y de trazabilidad en referencia al cambio de una dirección de correspondencia en los ficheros de una compañía de gas natural, que resultó sancionada con una multa de 50.000 € por enviar al domicilio de otra persona tres facturas de la denunciante. La empresa alegó que si la modificación del domicilio de envío no la realizó la interesada, la alteración de esa información tuvo que deberse necesariamente de un fallo informático. La Audiencia nacional confirmó la sanción sin necesidad de entrar en los aspectos informáticos de la situación[811].

6.3.1.4. [E.18] Destrucción de información

Podría considerarse un caso particular del anterior. Si a fin de mes la aplicación que genera las nóminas de los millones de pensionistas de nuestro país descubriera que los

[810] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 47-48.
[811] SAN 2264/2013 de 10 de mayo de 2013, sala de lo contencioso.

números de las cuentas bancarias a las que ha de realizar las transferencias no contienen información alguna, las protestas serían masivas.

6.3.1.5. [E.19] Fugas de información

En un estudio realizado en 2010 por *WhiteHat Security*, el 64% de los sitios *web* examinados presentaba una vulnerabilidad relacionada con fugas de información[812], si bien no separa porcentajes en función de su origen accidental o intencionado.

MAGERIT lo describe como "*revelación por indiscreción, incontinencia verbal, medios electrónicos, soporte papel, etc.*".

Cuando la fuga afecta a información del sistema, puede revelar datos que ayuden a un adversario a conformar el sistema y concebir un plan de ataque.[813]

Se produce una violación de la privacidad, muchas veces ilegal, cuando información privada de los usuarios, introducida en la aplicación, se escribe en una localización externa[814]. Un ejemplo consiste en grabar la contraseña del usuario en el fichero de *log*.

Un error simple de programación al comprobar las credenciales del usuario podría dar acceso indebido a datos que deberían guardarse en secreto.

Una vulnerabilidad de las aplicaciones informáticas, bastante conocida en relación al control de acceso, es la referida a la fijación de sesión. En estos casos, una aplicación autentica a un usuario sin validar previamente la sesión existente, dando continuidad a la utilización de la

[812] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 8.
[813] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 46.
[814] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 44.

sesión asociada ya previamente con el usuario, permitiendo que el atacante tenga acceso a la sesión autenticada, materializando así la fuga de información.

6.3.1.6. [E.20] Vulnerabilidades de los programas

Un caso real de explotación maliciosa de fallos del *software* tuvo lugar durante los días 16, 18 y 19 de febrero de 2015, en los que se produjeron 26 errores en la mecanización de códigos en el sistema informático de determinada empresa. Esas erratas consistieron en la introducción de un carácter o espacio en blanco en el código correspondiente. El *software* del sistema no era capaz de reconocerlo, malinterpretando su significado de forma que provocaba el envío de pedidos a clientes a los que no correspondía y la emisión de albaranes diferentes a los que deberían haberse emitido. Todos esos códigos incorrectos fueron grabados por el mismo usuario. La sentencia[815] concluyó que esa introducción de información se llevó a cabo utilizando un medio de difícil detección, apreciable solo con un estudio muy exhaustivo de los pedidos, lo que permite considerar no la existencia de una equivocación del trabajador, sino una conducta premeditada dirigida a perjudicar el correcto suministro a los principales clientes de las piezas fabricadas. En este caso, un usuario malintencionado explotó una vulnerabilidad accidental.

MAGERIT denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza o, más detalladamente, a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Por tanto, son vulnerabilidades todas las ausencias o ineficacias de las medidas pertinentes para salvaguardar el valor propio o acumulado sobre un activo, empleando a veces el término “insuficiencia” para resaltar el hecho

[815] STSJ del País Vasco 467/2016 de 2 de febrero de 2016, sala de lo social.

de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza[816].

La idea de "vulnerabilidad de los programas *software*", que ha salpicado páginas anteriores, es definida por MAGERIT como defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar, aunque afecta también a las dimensiones de disponibilidad y confidencialidad[817].

Las buenas prácticas de programación[818] se orientan a disminuir la cifra de vulnerabilidades asociadas al aplicativo. El desarrollador, para ir cerrando huecos, ha de ponerse siempre en el lugar de un atacante que busca de resquicios descubiertos, y pensar que toda entrada es potencialmente maliciosa, por lo que deberá tratar de minimizar la superficie de ataque, mantener la seguridad por defecto (*security by default*), controlar el estado en que queda la aplicación en caso de fallo, no permitir que la seguridad descanse únicamente sobre la ocultación del código, mantener la simplicidad de las instrucciones, probar adecuadamente comprobando que no aparece ningún efecto colateral, prevenir la inyección de código SQL,… Sin embargo, no se puede garantizar ni el rigor en la creación de la aplicación, ni la profesionalidad en su uso, como tampoco es factible inmunizar al ser humano contra el cansancio o el estrés. Son de esperar equivocaciones y omisiones involuntarias[819].

[816] MINHAP. MAGERIT 3.0, libro I – Método, 35.
[817] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 37.
[818] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 3-7.
[819] MADURGA OTEIZA, J.M. (2001), auditoría de aplicaciones, 446.

6.3.1.7. [E.21] Errores de mantenimiento / actualización de programas

Afecta a las aplicaciones (*software*) en sus dimensiones de integridad y disponibilidad. MAGERIT lo describe como defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. En aquellos casos en que los programas sean de desarrollo propio o subcontratado, podría producirse el mismo problema. En cualquier caso, no son extraños los errores en el *software*. Una conocida entidad bancaria fue sancionada con 2.000 € por una infracción del artículo 6.1 de la LOPD, tipificada como grave[820]. El envío de publicidad se debió a una circunstancia excepcional de mal funcionamiento de su sistema informático, que no reconocía a los clientes que habían expresado su voluntad de no recibirla cuando su inclusión en la "lista Robinson" se hubiese producido el mismo día que se había dado de alta en un plan de pensiones de la entidad, incidencia que fue corregida inmediatamente después de la reclamación del afectado. Dicho fallo puede producirse con una única letra incorrecta dentro de un voluminoso programa[821], un error típico vivido por la inmensa mayoría de los desarrolladores en algún momento. De las muchas excusas sobre fallos informáticos alegadas en los tribunales y no demostradas, este caso es perfectamente entendible y, en mi opinión, real, lo que no basta para evitar la sanción. Ya sean tristemente ciertos o alegremente inventados, buscando una excusa fácil para una situación desesperada, las alegaciones de mal funcionamiento de las aplicaciones

[820] Sanción confirmada por la SAN 1926/2012 de 27de abril de 2012, sala de lo contencioso.

[821] A modo de ejemplo, en el lenguaje de programación NATURAL, el operador LT significa “menor que” y el operador LE equivale a “menor o igual”. Utilizar uno en lugar de otro al comparar dos fechas ya podría producir ese error que costó a la entidad bancaria la multa de 2.000 €. Este ejemplo puede ilustrar la facilidad con la que se puede provocar un problema importante y la dificultad de localizar el fallo antes de que se produzca, aunque se establezcan controles o se contraten los servicios de un auditor previamente a la puesta del programa en explotación.

utilizadas por los ciudadanos o por las empresas son abundantes, especialmente en el ámbito tributario o en el campo de la protección de datos, situaciones ante las cuales nuestros tribunales reiteran que "*son muchas las sentencias en que se ha insistido en que los errores informáticos no son suficientes para eliminar la antijuridicidad de las conductas sancionadas*"[822].

El 7 de marzo de 2012, en relación con una subvención, la AEAT certificó que la solicitante no se hallaba al corriente de sus obligaciones tributarias, lo que llevó a la Dirección general de economía a emitir un informe desfavorable a la concesión, denegándose la misma. El 30 de octubre del mismo año, la AEAT aportó los certificados que acreditaban su equívoco como consecuencia de un error informático en la emisión telemática del certificado negativo. A tenor de la normativa reguladora del recurso extraordinario de revisión, se solicitó dictamen al Consejo consultivo autonómico, el cual consideró los nuevos certificados como documentos de valor esencial para la resolución del asunto que, aunque posteriores, evidencian el error de la resolución recurrida, estimando por ello el recurso.[823]

Otros muchos errores informáticos de las aplicaciones utilizadas en las Administraciones públicas han llegado a nuestros tribunales. El éxito o fracaso del recurrente normalmente va ligado a la habilidad del defensor y a los pasos seguidos con anterioridad en el proceso administrativo. En cualquier caso, a modo ilustrativo de la incidencia que puede presentar un *software* con deficiencias, podemos citar algunos ejemplos, como la certificación errónea de méritos en procesos de selección o provisión debido a fallos en los programas de

[822] SAN 1787/2016 de 25 de febrero de 2016, sala de lo contencioso.
[823] Dictamen nº 103/13 de 20 de marzo de 2013, del Consejo consultivo de la Comunidad de Madrid.

gestión de personal[824], la incorrecta ordenación de las bolsas de sustituciones que conllevan contrataciones indebidas[825], la grabación incorrecta de los puestos pedidos por un funcionario en su solicitud de participación en un concurso de traslados[826], abono de salarios no proporcionales al trabajo realizado[827]o con complemento de jornada partida improcedente[828], diagnóstico erróneo de inmunodeficiencia por VIH por haber incurrido en error informático la transcripción en la codificación del diagnóstico[829], sustitución de una matrícula por la de otro vehículo en un pliego de cargos[830]…

6.3.1.8. [E.24] Caída del sistema por agotamiento de recursos

Afecta a la disponibilidad de servicios, equipos informáticos (*hardware*) y comunicaciones, y se describe como una carencia de recursos suficientes que provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Las aplicaciones pueden presentar vulnerabilidades causadas por no liberar adecuadamente los recursos del sistema, lo que podría llegar a provocar la denegación de servicio al agotar el *pool* de recursos[831]. Dejar un valor *maxOccurs* sin límite en un esquema XML también puede conducir a un agotamiento de recursos y a una denegación del servicio[832].

[824] SAN 1884/2007 de 18 de abril de 2007, sala de lo contencioso.
[825] STSJ de Andalucía 3617/2010 de 2 de marzo de 2010, sala de lo contencioso.
[826] SAN 4449/1998 de 10 de noviembre de 1998, sala de lo contencioso.
[827] STSJ de Galicia 2004/2009 de 8 de abril de 2009, sala de lo contencioso.
[828] STSJ del País Vasco 2497/2008 de 14 de octubre de 2008, sala de lo contencioso.
[829] STSJ de Cataluña 7077/2006 de 3 de julio de 2006, sala de lo contencioso.
[830] STSJ de Extremadura 343/2005 de 25 de febrero de 2005, sala de lo contencioso.
[831] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 36-42.
[832] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 21.

Sin entrar en mayores detalles técnicos, basta comentar que la programación inadecuada del *software* puede inutilizar los recursos *hardware*. Problemas por el funcionamiento inadecuado en situaciones de alta concurrencia también han llegado a nuestros tribunales[833], suponiendo la resolución del contrato y la restitución de más de 60.000 €.

6.3.1.9. [E.28] Indisponibilidad del personal

Lo describe MAGERIT como la ausencia accidental del puesto de trabajo por enfermedad, alteraciones del orden público, guerra bacteriológica,...

Es práctica relativamente habitual disponer de un único especialista en una determinada materia, provocado quizá por el exceso de carga de trabajo y la falta de recursos humanos. Ante su indisponibilidad, se pueden plantear serias dificultades. Si, además, ese trabajador es un empleado de una empresa externa, se genera una dependencia altamente problemática.

6.3.2. Con origen humano deliberado

MAGERIT 3.0 incluye también una lista no exhaustiva de ataques intencionados de origen humano, es decir, fallos deliberados causados por las personas, de los cuales algunos vienen relacionados con la seguridad del desarrollo de las aplicaciones de manera más directa.

[833] Sentencia de la Audiencia Provincial de Pontevedra 2132/2014 de 2 de octubre de 2014.

6.3.2.1. [A.3] Manipulación de los registros de actividad (*log*)

Del mismo modo que entre los fallos no deliberados se contemplaba los errores de monitorización de los *logs*, es necesario señalar ahora la posibilidad de su manipulación intencionada, algo, por lo general, relativamente sencillo y que afecta a los registros de actividad en cuanto a su integridad, pero con repercusión en la trazabilidad, dado que, cuanto más susceptible sea a la manipulación, menores serán sus efectos probatorios.

La inseguridad se potencia en los casos de antiguos empleados con conocimientos sobre los sistemas de seguridad, especialmente si son informáticos, ya que esa información les permite sustraer, atacar o destruir los datos más vulnerables y los *logs* de actividad[834]. Ya se comentó *supra* la problemática que representan los empleados que abandonan la empresa de servicios yéndose con el conocimiento del entorno y con las claves de acceso.

6.3.2.2. [A.4] Manipulación de la configuración

MAGERIT advierte que prácticamente todos los activos dependen de su configuración y esta responde a la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Todo queda en su mano y, por ello, tiene a su alcance el control del sistema. Señala como activo afectado los registros de actividad[835], algo que parece erróneo. Debemos entender que el activo afectado es el conjunto de datos de configuración.

[834] RUILOBA CASTILLA, J.C. (2006), actuación policial, 60-61.
[835] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 40.

La manipulación malintencionada de la configuración afecta a la integridad, confidencialidad y disponibilidad.

6.3.2.3. [A.5] Suplantación de la identidad del usuario

Puede afectar a la confidencialidad, autenticidad e integridad.

Explica MAGERIT que, con la suplantación, el atacante disfruta de los privilegios del suplantado para sus fines propios, pudiendo ser perpetrada por personal interno, por personas ajenas a la organización o por personal contratado temporalmente.

Martín Delgado admite la práctica de cesión de claves a terceros y la posibilidad de suplantación, matizando su complejidad técnica y, por ello, minimizando el riesgo. Incluso partiendo de dicha premisa, defiende la relación más directa entre el firmante y la firma electrónica que con su equivalente versión manuscrita, sabiendo que cualquiera puede intentar imitar esta última, mientras que son pocas personas las capacitadas para realizar la misma operación con la firma digital[836].

6.3.2.4. [A.6] Abuso de privilegios de acceso

Afecta a la confidencialidad, integridad y disponibilidad. MAGERIT describe la problemática diciendo que "*cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas*"[837].

[836] MARTÍN DELGADO, I. (2008), identificación y autenticación, 324-325.
[837] MINHAP. MAGERIT 3.0, libro II – Catálogo de elementos, 41.

Un estudio realizado en 2014 por Oracle[838] concluye que el 65% de los encuestados tienen miedo a los ataques internos, al 54% le preocupa el abuso de los privilegios de acceso por parte del personal de tecnologías de la información, sorprendentemente casi coincidente con la cifra de los que muestran su preocupación por los códigos maliciosos o virus (53%).

6.3.2.5. [A.8] Difusión de *software* dañino

Afecta a las dimensiones de disponibilidad, integridad y confidencialidad y al tipo de activo correspondiente a las aplicaciones (*software*). MAGERIT lo describe como la propagación intencionada de virus, espías (*spyware*), gusanos, troyanos, bombas lógicas, etc.

En defensa de los sistema informáticos de las Administraciones públicas, el real decreto 1671/2009 permite que los registros electrónicos rechacen los documentos electrónicos que les sean presentados que contengan código malicioso o dispositivo susceptible de afectar a la integridad o seguridad del sistema.

En referencia al desarrollo o a la adquisición de productos que puedan ser inseguros, es preciso incluir el problema de las puertas traseras comentado *supra*. Como comenta Caro Bejarano "*otro problema que se plantea con la externalización de la producción de dispositivos electrónicos es la falta de garantía sobre los mismos, ya sea el hardware y/o el*

[838] Recuperado de https://www.oracle.com/es/corporate/pressrelease/2-19189.html (18 de julio de 2016).

software puede esconder puertas traseras que permitan el acceso remoto con total desconocimiento del usuario que adquiere ese dispositivo"[839].

Los programas de desarrollo propio y los subcontratados tampoco están necesariamente libres de código dañino. Podemos encontrar puertas traseras (también llamadas trampas) que permiten acceder sin pasar los procedimientos de seguridad. Son utilizadas de forma legítima por los programadores en el entorno de desarrollo, pero nunca deberían llegar al entorno de producción, donde se convierten en una seria amenaza que, si está bien implementada, resulta muy difícil de detectar incluso sabiendo positivamente que la trampa existe, por lo que "*las medidas de seguridad deben centrarse en el desarrollo del programa y en las actividades de actualización del software*"[840].

Un programador puede incluir en el código, por ejemplo, una bomba lógica, un fragmento introducido dentro de algún programa legítimo que está preparado para "explotar" cuando convergen ciertas condiciones[841]. Por ejemplo, en una fecha determinada coincidente con un mes en el que se abone la paga extra, podría ordenarse desviar un 1% de la nómina de cada pensionista de la seguridad social a determinadas cuentas bancarias, sin que tal movimiento aparezca en ninguno de los listados de comprobación ni de cuadre.

[839] CARO BEJARANO, M.J. (2013), peligros tecnológicos, 208.
[840] STALLINGS, W. (2004), fundamentos de seguridad en redes, 342-343.
[841] STALLINGS, W. (2004), fundamentos de seguridad en redes, 344. El autor cita como ejemplo el de Tim Lloyd, cuya bomba lógica provocó a su empresa más de diez millones de dólares y fue condenado a indemnizarla con solo dos millones.

6.3.2.6. [A.11] Acceso no autorizado

La LOPD identifica como amenaza el acceso no autorizado, disponiendo la obligación de aplicar las salvaguardas adecuadas al estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos[842]. El RLOPD impone, entre las medidas de seguridad de nivel medio, el establecimiento de un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Esta amenaza afecta a la confidencialidad e integridad. El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, normalmente aprovechando un fallo del sistema de identificación y autorización.

También puede producirse aprovechando una vulnerabilidad del programa mediante inyección de código SQL. Para evitarlo, las buenas prácticas de programación recomiendan no confiar en la interfaz de usuario para restringir los valores que pueden ser enviados, sino implementar en la aplicación y en la capa de base de datos un control de acceso que tenga en cuenta el usuario realmente autenticado[843].

6.3.2.7. [A.13] Repudio

Afecta a los servicios y a los registros de actividad, en su dimensión de integridad, impactando de modo indirecto en la trazabilidad. Lo describe MAGERIT como la negación *a posteriori* de actuaciones o compromisos adquiridos en el pasado, y explica las

[842] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 490-491. El autor señala la mayor adecuación de este artículo, en tanto que establece la aplicación de medidas técnicas acordes al estado de la tecnología, a los ficheros automatizados.
[843] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 12-13.

diferencias entre el repudio de origen (se desmiente el haber enviado el mensaje), el de recepción (afirma no haberlo recibido) y el de entrega (negación de haber recibido un mensaje para su entrega a otro).

Se trata de una cuestión de carácter jurídico en la que el Derecho establece una fuerte presunción en virtud de la cual el firmante no puede negar el resultado de la autenticación por medios telemáticos, invirtiendo la carga de la prueba y obligando a quien asegure no haber firmado en tales términos la demostración de su afirmación[844], algo que probablemente no será sencillo.

En el caso particular de las entidades bancarias, el no repudio se garantiza por la incorporación del número de referencia completo (NRC) que se emplea, por ejemplo, como justificante de pago electrónico[845].

6.3.2.8. [A.15] Modificación deliberada de la información

Consiste en la alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Identificada como amenaza por la LOPD, resulta imprescindible adecuar las garantías que impidan la alteración de cada uno de los datos o documentos individualmente considerados y del conjunto de todos ellos, considerado como una unidad lógica dotada de una secuencia temporal, cuya integridad y autenticidad han de ser aseguradas[846].

[844] MARTÍNEZ GUTIÉRREZ, R (2011), identificación y autenticación, 424.
[845] LINARES GIL, M.I. (2008), identificación y autenticación, 308.
[846] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 99.

El problema se potencia en los casos de antiguos empleados con conocimientos sobre los sistemas de seguridad, especialmente si son informáticos, pudiendo más fácilmente sustraer, atacar o destruir los datos.

Es de reseñar la acertada opinión de Valero Torrijos al respecto del uso de las nuevas tecnologías para impedir la alteración de los documentos, extensible a otras acciones como la acreditación de las circunstancias temporales en que se generan o el acceso a la información. Señala que, a causa de las facilidades que permite la tecnología, podría darse una cierta apariencia de garantía y cumplimiento que, sin embargo, no obedezca a la realidad, en el caso de que las medidas técnicas limiten su virtualidad simplemente al plano teórico. Por ello, considera imprescindible el refuerzo del cumplimiento efectivo y, sobre todo, la exigencia de cumplir las normas técnicas que aseguren tales extremos[847].

6.3.2.9. [A.18] Destrucción de información

Consiste en la eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

6.3.2.10. [A.18] Divulgación / revelación de información

Hemos de incluir aquí también la revelación de datos sensibles sobre la propia aplicación informática, como comentarios en el código fuente, rutas y nombres de archivos, nombres de servidores, *strings* de conexión o mensajes de error no capturados procedentes de

[847] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 146-147.

capas inferiores, lo que proporcionaría información útil para los atacantes[848], motivo por el cual manifiesto mi reticencia a la publicación del código de los programas implantados en las Administraciones públicas.

En referencia a la información propiamente dicha, nos recuerda Troncoso Reigada cómo la divulgación o revelación de datos personales afecta a otros derechos fundamentales, más allá del propio derecho a la protección de datos. Así, señala la negativa influencia sobre el derecho a la vida y a recibir una adecuada asistencia sanitaria, pues la pérdida, alteración o no disponibilidad de la historia clínica perjudica la propia asistencia médica, y su publicación daña la confianza médico-paciente de forma que puede llevar a ocultarle información ante la perspectiva de que llegue a ser conocida. El mismo autor comenta la vulneración del derecho a la libertad sindical en determinados tratamientos indebidos del dato de la cuota sindical, y también el de la libertad ideológica y religiosa si no se protege adecuadamente la información de ideología, religión o creencias[849].

Probablemente las mayores incertidumbres que se plantean ante el riesgo de divulgación de información están relacionadas con la computación en la nube. Muchos componentes de los sistemas de información quedan así fuera del control directo de la organización. La gestión de riesgos es el proceso de identificarlos y valorarlos, realizando los pasos necesarios para reducirlos a un nivel asumible. Los sistemas *cloud* públicos requieren, al igual que los tradicionales, que los riesgos sean gestionados a lo largo de su ciclo de vida. Valorar y gestionar riesgos en sistemas que utilizan servicios de *cloud computing* presenta la

[848] SEGURINFO 2013, aplicaciones más seguras, 38.
[849] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 37-38.

dificultad de confirmar que los controles de seguridad están implementados correctamente y cumplen con los requisitos, por lo que es preciso plantearse el grado de control que la organización está dispuesta a delegar en el proveedor para que sea él quien implemente los controles necesarios para la protección de los datos y las aplicaciones de la organización, así como las pruebas de su efectividad. Si el nivel de confianza baja por debajo de las expectativas y la organización no puede aplicar medidas correctivas, esta debe decidirse entre la aceptación de un riesgo mayor o el rechazo del servicio[850].

6.3.2.11. [A.22] Manipulación de programas

Afecta a la confidencialidad, integridad y disponibilidad de aplicaciones (*software*). Se describe como alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza, como podría ser un trato preferente para el NIF del programador a la hora de calcular su nómina, participar en un procedimiento público de concurrencia competitiva, revisar su declaración del IRPF…

No es improbable que un empleado descontento cometa errores voluntariamente. Tampoco es imposible que un trabajador sucumba a la tentación del fraude perfecto si considera mínima la posibilidad de ser descubierto conociendo adecuadamente el sistema, la organización y los controles[851].

Una importante entidad bancaria sufrió los efectos de un error informático que propició unas rentabilidades desproporcionadas, de más del 1000 %, al movilizar planes de

[850] INTECO-CERT (2012), sesiones *web*, 21.
[851] MADURGA OTEIZA, J.M. (2001), auditoría de aplicaciones, 447.

previsión asegurados, entre noviembre de 2014 y octubre de 2015[852]. Quizá no se trató de una manipulación voluntaria del programa, sino accidental. En cualquier caso, sí parece haber sido voluntario el aprovechamiento que algunos empleados hicieron de ese código defectuoso.

De forma claramente intencionada, el 24 de abril de 2014 se puso en producción un desarrollo informático de *Business Intelligence* que simula una curva natural de llamadas atendidas de forma que, en lugar de presentar un número mínimo de cero llamadas, muestra un valor arbitrario configurable en función de distintos parámetros. El cliente, la empresa pública ADIF, solo puede ver los datos facilitados por esa aplicación, una información absolutamente viciada, elaborada para cuadrar de forma acorde con la facturación que se va a enviar al cliente, en la que incide el número de llamadas atendidas. A lo largo de dos años y medio, se facturaron 2.469.030 llamadas inventadas, lo que supone un incremento de un 31,7%, y ha supuesto la cantidad de 1.127.521 € de más, en lo que se describe como "*una maquiavélica estrategia de manipulación de datos*" que no solo perjudica al cliente, la empresa pública, sino también a la propia empresa desarrolladora, que desconoce las acciones efectuadas por personas de su confianza. El programa malicioso no estaba pensado para subsanar errores, sino simplemente enfocado a la manipulación de datos, incrementando aleatoria pero voluntariamente el número de llamadas atendidas que, conforme a las previsiones del contrato, quedaba corto e impedía la obtención de las comisiones deseadas.[853]

[852] STSJ de Castilla la Mancha 2291/2016 de 15 de septiembre de 2016, sala de lo social.
[853] STSJ de Madrid 8908/2016 de 22 de julio de 2016, sala de lo social.

6.3.2.12. [A.24] Denegación de servicio

Afecta a la disponibilidad de servicios, equipos informáticos y redes de comunicaciones. Se explica por la carencia de recursos suficientes, lo que provoca la caída del sistema cuando la carga de trabajo es, intencionadamente, desmesurada.

Ya sea premeditada o accidental, la denegación de servicio puede acarrear consecuencias muy negativas a la ciudadanía. Cita Valero Torrijos, a modo de ejemplo, las repercusiones que tendría este problema si acaeciese el último día del plazo en un procedimiento de concurrencia competitiva de selección de contratistas[854]. Troncoso Reigada trae a colación el perjuicio sobre el derecho a recibir la adecuada asistencia sanitaria ocasionado por la falta de disponibilidad de las historias clínicas, recordando la declaración por la Agencia de protección de datos de la Comunidad de Madrid de la comisión de una infracción grave llevada a cabo por un centro sanitario que, por indisponibilidad de su sistema de información, impidió que un pediatra consultara la historia clínica de un menor inmigrante en régimen de acogimiento[855].

6.3.2.13. [A.28] Indisponibilidad del personal

Afecta a la disponibilidad del personal interno. Se describe como la ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos,...

[854] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 80.
[855] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 681.

6.3.2.14. [A.29] Extorsión

Descrito como la presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido, resulta fácil imaginar al perseguidor de la mujer víctima de violencia de género, en un intento de localizarla, extorsionando a cualquier empleado público con acceso a la plataforma de intermediación de datos.

6.3.2.15. [A.30] Ingeniería social (picaresca)

Se describe como el abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

The European Network and Information Security Agency alerta del espionaje corporativo desarrollado por ingeniería social, que se realiza a través de las personas que pertenecen a una corporación, grupo o empresa, como pueden ser sus trabajadores, y que, a su vez, son miembros de redes sociales, denunciando que estos pueden, con absoluta ignorancia, proporcionar información muy útil y valiosa[856].

6.4. SALVAGUARDAS

Se definen las salvaguardas o contramedidas como aquellos mecanismos tecnológicos o procedimientos que reducen el riesgo. Dado el amplísimo abanico de posibilidades donde elegir, es adecuado proceder a una criba inicial basada en su aplicabilidad, seleccionando únicamente aquellas relevantes en función del tipo de activo a proteger, dimensiones de seguridad afectadas, amenazas a neutralizar y posible existencia de salvaguardas

[856] OROZCO PARDO, G. (2012), vida privada, 150.

alternativas, dejando sin aplicar aquellas cuyo empleo no se justifique por ser manifiestamente desproporcionadas para el riesgo a proteger. La protección prestada por las salvaguardas abarca diferentes tipos: prevención, disuasión, eliminación, minimización de impacto, corrección, recuperación, monitorización, detección, concienciación o administración[857].

6.5. GESTIÓN DE LOS RIESGOS

Resulta habitual que recursos humanos del sector privado escriban las instrucciones[858] que controlan el comportamiento de nuestro "empleado público electrónico", cuya actuación puede afectar a unos pocos sujetos concretos o incluso a millones de ciudadanos indeterminados en un grado difícilmente imaginable. Con las instrucciones precisas, un individuo podría no existir para la Agencia tributaria mientras que otro podría convertirse en un peligroso preso fugado en busca y captura. En determinadas circunstancias, el registro telemático podría no funcionar justo el último día del plazo para presentar solicitudes, nuestra historia clínica podría mostrarse en la pantalla de cualquier internauta y toda la información sobre nuestros estudios académicos podría desaparecer de los ficheros públicos. Una simple mirada a nuestro alrededor pone de manifiesto que confiar ciegamente en la bondad de la programación implementada por empresas del sector privado, movidas por consideraciones económicas, es un error que puede acarrear consecuencias importantes[859]. Adicionalmente, es preciso ser consciente

[857] MINHAP. MAGERIT 3.0, libro I – Método, 31-34.
[858] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 193. El autor señala la posibilidad de que las aplicaciones no hayan sido diseñadas por personal técnico de la Administración, sino por la entidad privada seleccionada mediante un previo procedimiento contractual.
[859] Una prestigiosa empresa internacional, Volkswagen, instaló versiones de *software* trucado en más de 11 millones de vehículos para alterar las pruebas de emisiones de gases, recuperado de http://www.lavanguardia.com/economia/20151018/54437291884/volkswagen-fabrico-varias-versiones-*software*-alterar-emision-gases.html (25 de febrero

de que el *software* de las Administraciones públicas ha de considerarse también objetivo de la delincuencia organizada y blanco para acciones de espionaje o de sabotaje con origen en otros países, esperando un crecimiento de estas actividades en los próximos años, debido al bajo coste que supone la guerra cibernética frente a los gastos armamentísticos tradicionales[860].

La gestión de riesgos no se plantea la obtención de un riesgo cero, simplemente porque este no existe[861]. La imposibilidad del riesgo cero, más que un mero dato técnico, es una afirmación explícita de nuestros tribunales, tanto nacionales como europeos, por lo que el papel de las instancias públicas no es su eliminación, sino la determinación del riesgo permitido, el que consideran aceptable[862].

Con la información obtenida mediante el análisis de riesgos pueden adoptarse las oportunas decisiones referentes a su gestión, que necesariamente vendrán condicionadas por diversos factores, entre los que figuran la gravedad del impacto y/o del riesgo, las obligaciones a las que esté sometida la organización por ley, por reglamentos sectoriales o por contrato. Dentro del margen de maniobra que aún reste, puede pasar a considerar ciertos impactos intangibles como aspectos reputacionales o de imagen pública, política interna (tales como sus capacidades de contratar al personal idóneo, retener a los mejores, soportar rotaciones de personas, ofrecer una carrera profesional atractiva, etc.), relaciones con los proveedores (donde se puede incluir su capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, o de obtener trato prioritario, etc.), relaciones con los clientes o usuarios (capacidad de retención, de incrementar la

de 2016). Sus efectos nocivos se evalúan en el artículo La salud pública ante el caso Volkswagen. (2015). *Revista de Salud Ambiental de la Sociedad Española de Sanidad Ambiental (SESA) 15*(2), 148-149.

[860] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO (2015), informe anual 2014, 232.

[861] ESTEVE PARDO, J. (2003), ciencia y Derecho, 147.

[862] ESTEVE PARDO, J. (2014), contractualización, 1231.

oferta, de diferenciarse frente a la competencia, etc.), relaciones con otras organizaciones (capacidad de alcanzar acuerdos estratégicos, alianzas, etc.), nuevas oportunidades de negocio (como formas de recuperar la inversión en seguridad) o acceso a sellos o calificaciones reconocidas de seguridad.

Finalmente, a cada riesgo significativo se le habrá asignado una calificación de entre las siguientes:

- CRÍTICO: requiere atención urgente.
- GRAVE: requiere atención.
- APRECIABLE: puede ser objeto de estudio para su tratamiento.
- ASUMIBLE: no se van a tomar acciones para atajarlo. Señala MAGERIT que se trata de una opción arriesgada que no debe ser tomada sin prudencia o justificación, pudiendo venir motivada por el hecho de que el impacto o riesgo residuales sean asumibles o porque el coste de las salvaguardas oportunas sea desproporcionado en comparación al impacto y riesgo residuales[863].

Ahora bien, hay que diferenciar dos papeles diferentes en la gestión de riesgos, de contenido diferenciado, encomendados a distintos poderes. El poder científico, legitimado por el conocimiento experto y especializado, asume las funciones de información, dictamen y valoración de los riesgos, pero el poder decisorio ha de corresponder a las instancias públicas que

[863] MINHAP. MAGERIT 3.0, libro I – Método, 47. En las páginas siguientes comenta con más detalle la opción de aceptación del riesgo, de interesante lectura.

lo tengan atribuido, en último término, por determinación constitucional[864]. Aunar el conocimiento experto y la legitimación para decidir en unos mismos individuos, pertenecientes a cuerpos de empleados públicos especializados al servicio de la Administración, "*definida por su vocación de servicio al interés general y su necesaria imparcialidad*"[865], difícilmente puede arrastrar consecuencias más perjudiciales que depositar una confianza ciega sobre personal técnico del sector privado movido por sus propios intereses económicos.

6.6. ESTUDIOS COSTE/BENEFICIOS

Durante los últimos años la necesidad ha obligado a las Administraciones públicas a priorizar, a pensar en lo que es o no es prescindible, a esforzarse por conservar lo que se debe mantener y a sopesar a qué se debe renunciar. El análisis coste-beneficio ha sido una técnica por lo general ausente en la Administración española hasta fechas recientes, con la llegada de la ley de economía sostenible[866].

Irremediable, la protección frente a la inseguridad arrastra unos gastos que, en paralelo al incremento de nuestras necesidades, van creciendo. Es preciso adquirir *hardware* y licencias, costear el mantenimiento y retribuir a quienes asuman la formación de administradores y usuarios. Unos usuarios formados y concienciados en las políticas de seguridad pueden hasta llegar a reducir las necesidades de inversión, al permanecer vigilantes y reportar información directa sobre los incidentes en momentos tempranos[867].

[864] ESTEVE PARDO, J. (2003), ciencia y Derecho, 142.
[865] CASTILLO BLANCO, F.A. (2003), principio de seguridad jurídica, 55.
[866] RIVERO ORTEGA, R. (2011), simplificación administrativa, 117.
[867] CARRASCO NÚÑEZ, Á. (2013), conceptos de seguridad informática, 114.

Como veremos *infra*, al hablar del estudio de viabilidad de un sistema de información, el análisis coste/beneficio ayudará a la hora de valorar la necesidad y oportunidad de acometer la realización de un proyecto y, en su caso, comparar y seleccionar la alternativa más beneficiosa, y estimar los recursos que van a requerirse para completar el proyecto en el plazo indicado[868].

El cálculo de costes no suele ser una tarea sencilla, pues no ha de limitarse únicamente a los imputables de forma directa, como el valor de los bienes afectados o el salario de los trabajadores que han visto impedida su labor diaria, sino que ha de abarcar también los indirectos, como la pérdida de reputación y confianza, las campañas orientadas a recuperar en lo posible la buena imagen, el tiempo gastado en vencer la reticencia de los usuarios, la utilización de otros medios para interactuar con la institución, los gastos legales acarreados por reclamaciones, denuncias o indemnizaciones… Habrá que poner en la balanza la inversión en los riesgos más graves frente al coste de asumir el riesgo. "*Generalmente, todas las instituciones tienen más que ganar que perder en invertir en seguridad y máxime si la gente está concienciada*".[869]

MAGERIT 3.0 parte de la afirmación de que no debe invertirse en salvaguardas más de lo que pueda valer lo que se desea proteger (valor que no necesariamente estará calculado como una cifra de dinero).

[868] MAP. Métrica V3. Técnicas y prácticas, 6.
[869] CARRASCO NÚÑEZ, Á. (2013), conceptos de seguridad informática, 114.

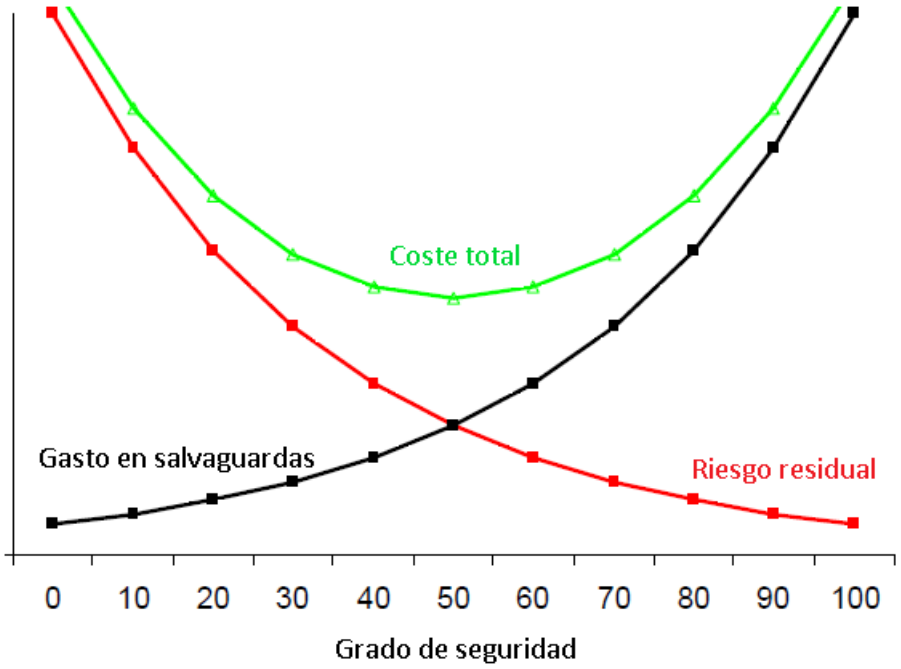

Figura 21: Relación entre el gasto en salvaguardas y el riesgo residual

Fuente: MAGERIT 3.0 libro I - Método

Esta curva teórica[870] indica que el riesgo, también interpretable como "coste de la inseguridad" (curva roja), disminuye muy rápidamente en cuanto se gasta una pequeña cantidad en salvaguardas (curva negra), motivo por el cual esa inversión resulta muy rentable. Nos encontramos en la zona izquierda de la gráfica; lo que esa parte refleja es que la inversión en unas medidas básicas de seguridad provocan un descenso importante del riesgo, por lo que son inexcusables.

[870] En la práctica de la vida diaria, los escenarios son más complejos, entrando a analizar simultáneamente muchas combinaciones de medidas de salvaguarda.

Sin embargo, en la zona derecha de la gráfica, cuanto más se intenta acercarse a la seguridad total, al riesgo cero, los gastos en salvaguardas se disparan desmesuradamente y se vuelven inasumibles, convirtiendo la seguridad total en inalcanzable. En ese extremo derecho, una enorme inversión en salvaguardas apenas se ve reflejada en una disminución observable del riesgo.

Si sumamos el coste de los gastos en salvaguardas (curva negra) con el coste que pueda derivar de la inseguridad, del riesgo (curva roja), obtenemos el coste total para la organización (representado por la curva verde). Podemos observar que hay un punto donde el coste total alcanza su valor mínimo, en un punto intermedio, un punto de equilibrio entre lo que se arriesga y lo que se invierte en defensa. Ese sería el punto al que habría que tender si el estudio fuera puramente cuantitativo, es decir, si la única consideración fuese económica[871].

En un estudio puramente cualitativo o en uno mixto, es preciso atender a los aspectos intangibles, como los reputacionales, argumentos de competitividad, obligaciones de cumplimiento normativo, motivos relacionados con la capacidad de operar y razones de productividad[872]. Será necesario buscar un punto de equilibrio, eligiendo una combinación de medidas que sea asumible[873].

La lista de aspectos valorables a la hora de realizar un análisis coste/beneficios en la eAdministración es larga y, con seguridad, no exhaustiva. Desde la óptica del ciudadano, se

[871] MINHAP. MAGERIT 3.0, libro I – Método, 50-51.
[872] En su página 87 cita otros textualmente, como la credibilidad o buena imagen (claramente subsumibles dentro de los aspectos reputacionales), el conocimiento acumulado, la independencia de criterio o actuación, la intimidad de las personas (una clara obligación de cumplimiento normativo) y la integridad física de las personas.
[873] MINHAP. MAGERIT 3.0, libro I – Método, 53.

percibe un ahorro costes de los servicios públicos y una mejora de su calidad de vida. Para las empresas, se reducen los gastos asociados a los servicios públicos, eliminando el papeleo y acortando el tiempo de espera. Los empleados públicos necesitarán dedicar menos tiempo a tareas rutinarias y dispondrán de más tiempo para la interacción especializada cara a cara en la atención al público.

Las herramientas para el cálculo del retorno de la inversión, ROI, ayudan a justificar ante la dirección de la organización los desembolsos efectuados[874]. En el ámbito de la seguridad informática, esas herramientas, aquí bautizadas como ROSI, pretenden calcular el ahorro logrado a consecuencia de evitar incidentes de seguridad, lo que se ajustaría a la siguiente operación:

ROSI[875] = [(Ganancia – Coste) / Coste]

Dentro del marco de la Comisión para la Reforma de las Administraciones Públicas (CORA) se constituyó un grupo de trabajo al objeto de diseñar una metodología para el análisis coste/beneficios de los proyectos, del que resultó escogida ARCAS, que constituye un instrumento para estimar la conveniencia de desarrollar futuros proyectos de administración electrónica, seleccionando y priorizando los que aporten al ciudadano mayores ahorros, a la vez que permite concienciar a los propios gestores del papel crucial que desempeña la eAdministración en el contexto actual[876].

[874] AUDISEC (2008), retorno de inversión, 3-7.
[875] ENISA (2012), *Security Investment*, 2.
[876] Recuperado de http://administracionelectronica.gob.es/ctt/arcas/infoadicional#.V4j7iDU2tsk (15 de julio de 2016).

6.7. TRATAMIENTO DEL RIESGO

El riesgo y su tratamiento pueden desencadenar importantes repercusiones políticas, pues no se limitan a proporcionar una descripción técnica de la situación, sino que orientan la toma de decisiones. 1969 abrió el debate sobre el llamado "riesgo aceptable" a raíz de un artículo publicado en la revista *Science* donde se presentaba un estudio sobre la aceptabilidad social de distintas fuentes de riesgo y se desarrollaba un método de evaluación del nivel aceptado en relación con los beneficios producidos por la tecnología[877].

La duda que se plantea es qué hacer frente a riesgos que se consideran no aceptables. La metodología MAGERIT 3.0 plantea diversas posibilidades: eliminación, mitigación, compartición y financiación.

Normalmente la **eliminación** de la fuente de riesgo es una opción adecuada únicamente para activos que no afecten a la información o a los servicios esenciales de la organización, por cuanto constituyen su misión. En el caso de componentes no esenciales, se podría plantear la eliminación de cierto tipo de activos empleando otros en su lugar o, también, barajar la posibilidad de reordenar la arquitectura del sistema de forma que se altere el valor acumulado en ciertos activos expuestos a grandes amenazas. Cita MAGERIT, a modo de ejemplo, la segregación de redes y el desdoblamiento de equipos para atender a necesidades concretas alejando lo más valioso de lo más expuesto. Tras la eliminación, se requiere rehacer el análisis de riesgos[878].

[877] PRADES LÓPEZ, A./ ESPLUGA TRENC, J./ HORLICK-JONES, T. (2015), riesgos tecnológicos, 399-402.
[878] MINHAP. MAGERIT 3.0, libro I – Método, 53.

La **mitigación** del riesgo implica la reducción de la degradación causada por la amenaza (acotar el impacto) o, alternativamente, la disminución de la probabilidad de que esa amenaza se materialice. En cualquiera de los dos casos es preciso ampliar o mejorar el conjunto de salvaguardas, repitiendo después el análisis para verificar que realmente el estado de riesgo de la organización ha disminuido[879]. Esta técnica se enfrenta al problema frontalmente y busca soluciones. A modo de ejemplo, ante el riesgo que supone la elevada rotación del personal desarrollador, la mitigación busca reducir el movimiento de dichos efectivos, buscando sus causas (pobres condiciones laborales, salario bajo…), evitando las que están bajo su control (mejora de las condiciones, subida de retribuciones…), desarrollar técnicas que aseguren la continuidad cuando los efectivos se vayan, organizar equipos de trabajo en los que cada actividad se disperse entre más de una persona, asignar un miembro de personal de respaldo a cada técnico crítico), etc. Como la mitigación, al igual que la gestión de la calidad, conlleva costes (respaldar a cada técnico crucial cuesta dinero) se debe recurrir de nuevo al análisis coste-beneficio. Si para un proyecto grande se pueden detectar entre 30 y 40 riesgos diferentes, y para cada uno se identifican entre 3 y 7 formas de manejarlo, la gestión de riesgos se convierte en un proyecto en sí mismo, que va a requerir la adaptación de la ley de Pareto al desarrollo del *software*, por el que, como el 80% de los problemas se producen por el 20% de los riesgos, a estos habrá que asignar la prioridad más alta.[880]

La **compartición** ha venido denominándose tradicionalmente “transferencia del riesgo”, pudiendo ser parcial o total. Se distinguen dos formas básicas de compartir riesgo. El

[879] MINHAP. MAGERIT 3.0, libro I – Método, 53-54.
[880] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 649-651.

cualitativo se comparte por medio de la externalización de componentes del sistema, repartiendo responsabilidades. El cuantitativo se comparte por medio de la contratación de seguros. En ambas opciones cambia el conjunto de componentes del sistema o su valoración, por lo que será preciso realizar un nuevo análisis del sistema resultante[881]. Ante los problemas de seguridad del *software* de las Administraciones públicas, pasarle las repercusiones económicas a un tercero, como puede ser a una aseguradora que indemnice los daños, en principio, no es la respuesta que cabe esperar de la Administración, además de que puede producirse un "deslizamiento sutil" debido a la carencia de repercusiones económicas de importancia. Así, al principio la Administración debía indemnizar por causar daños al funcionar mal, tarde o nunca, pero al carecer de costes excesivos, puede llegar a que acepte pagar a cambio de no tener que cambiar sus pautas de conducta[882].

La **financiación** consiste en la reserva de fondos, a veces llamados "de contingencia", realizada por la organización cuando acepta un riesgo, para el caso de que este se concrete y deba responder de sus consecuencias. También puede ser parte de los contratos de aseguramiento. Normalmente esta opción no modifica nada del sistema, por lo que no requiere repetición del análisis de riesgos disponible[883], pero tampoco parece ser la mejor solución para los problemas de seguridad del *software*.

[881] MINHAP. MAGERIT 3.0, libro I – Método, 54.
[882] *Vid*. MARTÍN REBOLLO, L. (1992), vigencia y limitaciones, 54.
[883] MINHAP. MAGERIT 3.0, libro I – Método, 54.

7. EL DESARROLLO DEL *SOFTWARE*

Íntimamente relacionados aunque conceptualmente diferentes, las nociones de seguridad del *software* y de seguridad de la información no son intercambiables, lo que no impide que la optimización de una de ellas desemboque en una manifiesta mejoría de la otra. Asegurar el *software* abarca el producto en todos sus aspectos, trascendiendo hasta su proceso de desarrollo, mientras que el objetivo de la seguridad de la información radica en la protección de las aplicaciones ya desarrolladas, vistas como un simple activo más, sin buscar soluciones a los problemas de seguridad que actualmente afectan al *software*[884].

Ante la perspectiva de desarrollar un programa, es necesario conocer, desde sus inicios, las restricciones que se han de implementar por motivos de seguridad. Todo intento de encajarlas después dentro de un diseño preexistente provocará cambios que podrían desencadenar vulnerabilidades, elevar en gran medida el coste y retrasar el plazo de entrega, todo ello suponiendo el escenario más favorable en el que no se produzcan incompatibilidades con requisitos, conflictos que, de producirse, si se hubieran previsto desde el principio, hubieran sido estudiados en busca de la mejor forma de superarlos[885]. Todo ello se sintetiza en la afirmación de MAGERIT de que la seguridad debe estar embebida en el sistema desde su primera concepción[886], con el objetivo de conseguir que el producto sea seguro durante su explotación, lo que obliga a tomar en consideración el proceso utilizado para su desarrollo, los factores humanos implicados, con sus habilidades y conocimientos, las prácticas organizacionales declaradas e

[884] TOVAR, E., CARRILLO, J., VEGA, V. Y GASCA, G. (2006), desarrollo de productos, 62-63.
[885] ROSADO, D.G./ BLANCO, C./ SÁNCHEZ, L.E./ FERNÁNDEZ-MEDINA, E./ PIATTINI VELTHUIS, M. (2010), la seguridad, 205.
[886] MINHAP. MAGERIT 3.0, libro I – Método, 77.

instauradas que deben respetarse y aplicarse, así como una rigurosa validación y verificación de cada uno de los productos obtenidos[887], comprobando que cumple con los estándares y requisitos de seguridad instaurados[888].

En el caso particular del *software* crítico, utilizado para controlar sistemas potencialmente peligrosos, la implementación de las características de seguridad y dependabilidad puede resultar muy costosa. Requiere que los desarrolladores demuestren determinados conocimientos especiales, que las organizaciones planifiquen roles independientes para asumir el desarrollo, verificación, validación y evaluación de la seguridad, así como la utilización de determinadas herramientas y precauciones para la reutilización del *software*.[889]

Durante ese proceso de desarrollo, se encuentran en la ingeniería del *software* los criterios metodológicos que guían el camino hasta la obtención de un producto final de calidad, con un enfoque científico, pero sin olvidar los principios[890], casi filosóficos, que iluminan y enriquecen ese trayecto, entre los que considero destacables los siguientes:

- **Las personas y el tiempo no son intercambiables**: por lo general, duplicar el número de programadores no reduce el plazo de entrega a la mitad, como se verá *infra*.
- **Documentar es primordial**: la memoria humana es muy volátil y resulta accesible a un único individuo. Los recuerdos se conservan y comparten mucho mejor si se registran sobre un soporte más duradero, como el papel o los discos. Sin embargo, es preciso mantener la

[887] Se verá *infra* cómo la interfaz de seguridad de Métrica V3 indica el modo de afrontar este aspecto con detenimiento.
[888] TOVAR, E., CARRILLO, J., VEGA, V. Y GASCA, G. (2006), desarrollo de productos, 67-68.
[889] RODRÍGUEZ DAPENA, P. (2009), *software* crítico, 43-46.
[890] LABORATORIO NACIONAL DE CALIDAD DEL *SOFTWARE* (INTECO) (2009), ingeniería del *software*, 18-19.

documentación actualizada; su existencia desfasada no solo es inútil, sino altamente perjudicial. Los errores en la documentación pueden ser tan devastadores para la aceptación del programa como los habidos en cualquiera de los otros dos componentes del *software*: los datos y el código fuente[891].

- **Después de probar, hay que probar y probar**: es conveniente realizar pruebas adicionales por personas diferentes, alguna de ellas, a ser posible, carente de conocimientos previos sobre la funcionalidad implementada por el programa. La idea de que una prueba exitosa es aquella que no detecta ningún error es totalmente equivocada. Las pruebas se diseñan para localizar errores, alcanzan su objetivo cuando los encuentran y fracasan cuando no lo logran[892], pues estarán dejando pasar fallos a producción que acabará localizando el usuario. En la misma línea, podemos añadir otro de los principios del desarrollador del *software*: **haz que los errores los encuentre un colaborador, no un cliente**.

- **Las mejoras y modificaciones hay que introducirlas con cuidado**: la máxima "si funciona, no lo toques" se ha levantado sobre cimientos empíricos. No requiere un seguimiento ciego, pero tampoco debe ser menospreciada. Es preferible aderezar las modificaciones con una buena dosis de prudencia.

- **La entropía del *software* es creciente**: la física nos enseña que la entropía tiende a crecer, que el orden se disipa en la aleatoriedad, no al contrario[893]. No vemos en la vida diaria que el

[891] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 431.
[892] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 95-96.
[893] HERNÁNDEZ ROJAS VALDERRAMA, R./ RIVAS TOVAR, L.A. (2008), complejidad, 137.

caos muestre una tendencia a ordenarse. Tampoco lo hace el código de un programa, el cual sufre la llamada indefectible de la ley de la entropía creciente.

- **La gente es la clave del éxito**: esta es una afirmación repetida por los responsables de equipos dedicados a la ingeniería del *software* pero, con frecuencia, contradicen sus palabras con sus acciones, descuidando los aspectos relacionados con su personal[894]. Aunque pueda sostenerse, en la mayoría de las profesiones, que la consecución de las metas propuestas descansa sobre los trabajadores, pocas ocupaciones laborales se caracterizarán por un porcentaje de trabajo intelectual tan alto[895], unido a un riesgo de error difícilmente detectable tan elevado y con consecuencias potenciales tan graves. La necesidad de formación y preparación del informático rara vez es cuestionada. Sin embargo, la motivación del desarrollador adquiere un valor primordial que, normalmente, se desvela como un aspecto ampliamente desatendido. Afirma Pressman algo fácil de comprobar en el trabajo diario: "*un proceso de software, sin importar cuán bien se conciba, no triunfará sin personal de software talentoso y motivado*"[896]. No es extraño detectar, con solo una mirada, el descontento en el ámbito laboral público, ni la masificación de las factorías del *software* del sector privado, algo preocupante si se tiene en cuenta que la programación es una tarea laboral en la que un simple punto y coma marca la diferencia entre el éxito y el fracaso[897].

[894] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 556-557.
[895] *Vid*. MENÉNDEZ SEBASTIÁN, E.M. (2009), contratos de servicios del sector público, 208. La autora nos recuerda que la realización de un programa de ordenador a medida cuenta con todas las características para ser considerado como un contrato de servicios de prestaciones intelectuales.
[896] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 688.
[897] *Siete señales que indican que nunca serás un buen programador*. Descargado de http://blog.capacityacademy.com/2015/04/20/7-senales-indican-nunca-seras-buen-programador/ (14 de agosto de 2016).

Esa falta de motivación va íntimamente relacionada con otro de los principios de la ingeniería del *software*: **la gente necesita sentir que su trabajo es apreciado**.

- **Primero hazlo correcto, luego hazlo rápido**: la obtención de un buen trabajo irremediablemente consume un mínimo de tiempo que no se puede reducir. Por debajo de esa duración crítica, el resultado no será el correcto.

- **Nunca dejes que tu jefe o cliente te convenza para hacer un mal trabajo**: es este, sin duda, un interesante principio difícil de hacer valer en una empresa privada, y que requiere un carácter muy fuerte al empleado público que se sienta suficientemente motivado para defenderlo. Cuando el mantenimiento de la familia depende del sueldo del trabajador privado, o la promoción del empleado público guarda más relación con sus amistades y contactos personales que con la calidad de su trabajo, ambos obedecerán las órdenes sin cuestionarlas.

Los códigos de ética profesional pueden ayudar al logro de un comportamiento ético en la profesión y a mostrar a los desarrolladores su cualidad de personas libres con una responsabilidad no transferible a otros. El de ACM/IEEE, fundado en la humanidad del ingeniero *software*, resume en ocho principios sus valores nucleares[898]:

1. Actuar de modo acorde con el interés público.
2. Favorecer los intereses de su cliente y empleador.
3. Garantizar un elevado nivel de calidad en sus productos.

[898] GÉNOVA, G., GONZÁLEZ, M.R. Y FRAGA, A. (2007), *Ethical Education in Software Engineering*, 14.

4. Mantener la integridad e independencia en sus juicios profesionales.
5. Adoptar un planteamiento ético en la gestión de los proyectos.
6. Fomentar la integridad y reputación de la profesión.
7. Ser honestos con sus colegas y apoyarlos.
8. Procurar una formación continua durante toda la vida para sí mismos.

Todas las metodologías aplicables y todos los principios interiorizados no van a cambiar una realidad: *"El software es una empresa difícil. Muchas cosas pueden salir mal y, francamente, muchas con frecuencia lo hacen"*[899]. Pressman confirma lo que informáticos y usuarios hemos aprendido con la experiencia diaria y, por ello, nos exhorta a estar preparados, a comprender los riesgos y tomar medidas proactivas para evitarlos o, al menos, manejarlos. Es consciente de que lo habitual en los equipos de desarrollo de *software* es trabajar en "modo bombero", siguiendo una estrategia reactiva, enfrentándose a los riesgos del proyecto cuando se materializan, "apangando fuegos". Las consecuencias derivadas de tales prácticas son fácilmente imaginables: el plazo de entrega se retrasa, los costos aumentan y la calidad disminuye. Los riesgos más habituales en el propio proceso de desarrollo del *software* se ven potenciados por factores como su complejidad y tamaño, la ambigüedad en las especificaciones, la incertidumbre técnica y la tecnología punta[900].

Junto a los riesgos genéricos que amenazan a todo proyecto de *software*, existen riesgos específicos que afectarán al caso concreto y que podrían ser previstos por quienes tengan

[899] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 640.
[900] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 641-642.

clara comprensión de la tecnología, del personal y del entorno particular del *software* a construir. Sin carácter exhaustivo, pueden citarse aspectos tan frecuentes como la estimación del tamaño significativamente a la baja, la resistencia de los usuarios finales al nuevo sistema, la fijación de una fecha de entrega apretada, el cambio de los requisitos especificados por el cliente, la insatisfacción de las expectativas depositadas en esa tecnología, la inexperiencia de los desarrolladores, una alta rotación del personal…[901]

7.1. LA INADECUADA GESTIÓN DE LA DEMANDA

En todas las empresas que han alcanzado una cierta dimensión existe un departamento de informática, del que no se puede prescindir, que devora enormes y crecientes cantidades de dinero. Los avances informáticos que se hacen realidad en las distintas secciones de la empresa despiertan en el resto de la organización un ansia consumista de servicios, junto con algunos destellos de envidia. Ya se comentó *supra* que una inadecuada gestión de la demanda puede llevar a la asunción de múltiples proyectos simultáneamente sin los recursos necesarios, lo que se ha identificado como una de las causas de la crisis del *software*. La sobrecarga disminuye si la ubicación del departamento de informática está suficientemente alta en la jerarquía y cuenta con la masa crítica adecuada para disponer de autoridad y operar con independencia del resto de la empresa.[902]

Es primordial informar al usuario del coste, temporal y económico, que suponen sus peticiones y sus cambios de requerimientos o de opinión.

[901] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 642-646.
[902] RAMOS ESCOBOSA, J.M. (2001), auditoría de la Dirección, 217.

Una alternativa factible a plantearse es la posibilidad de cobrar esos servicios de forma real, recaudando esos costes del resto de departamentos de la organización, algo que, allá donde se implanta, suele convertirse en un tema delicado, especialmente a la hora de fijar el precio de transferencia o coste interno que el departamento de informática repercute al resto. En cualquier caso, ese reparto ha de ser justo, ecuánime y consistente, incluir únicamente los conceptos adecuados para su cálculo y no sobrepasar los precios de mercado para servicios similares[903].

7.2. LOS PARTICIPANTES EN EL DESARROLLO DEL *SOFTWARE*

Si bien podemos entender que a nuestro "empleado público electrónico" no le resulta aplicable la institución de la abstención o recusación por su ejecución de actos administrativos automatizados, Martín Delgado nos recuerda, con gran acierto, que es la programación del sistema informático la que determina el contenido de esa actuación automatizada[904], trasladando al órgano que asume esa tarea el deber constitucional de objetividad de las Administraciones públicas. Esta objetividad, predicada de la Administración, trasciende a los elementos personales de la organización administrativa, a los empleados públicos[905]. Sin embargo, el personal técnico informático de las Administraciones públicas es manifiestamente insuficiente para acometer y mantener los distintos proyectos[906], situación agravada en el

[903] RAMOS ESCOBOSA, J.M. (2001), auditoría de la Dirección, 223-225.
[904] MARTÍN DELGADO, I. (2009), actuación administrativa automatizada, 375.
[905] ARIAS MARTÍNEZ, M. A. (2011), principio de objetividad, 185.
[906] Resulta recomendable la lectura de la descripción de la situación aportada por el Director del Centro de Administración de Recursos y Gestión de Adquisiciones y Gerente Adjunto de la Gerencia de informática de la seguridad social (GISS), FRANCISCO JAVIER SANTAMARÍA ZAPATA, en su artículo "Los recursos humanos en la Informática de la seguridad social", publicado en el monográfico sobre la GISS de la revista BoleTIC 44,

momento actual por el decidido empuje recibido por la Administración electrónica, lo que nos impone una dependencia no deseada y excesiva de empresas externas, movidas siempre por sus intereses económicos particulares.

Aunque los puestos de trabajo relacionados con el desarrollo del *software* pueden recibir múltiples nombres diferentes, en la práctica, muchos son equivalentes entre sí. La metodología Métrica V3 a revisar *infra*, de forma genérica, define cinco perfiles en los que puede encajar cualquiera de los participantes, denominados directivo, jefe de proyecto, consultor, analista y programador[907]. Cabe hacer una crítica a este modelo de roles participantes en el desarrollo del *software* establecido por Métrica V3; no contempla la participación de expertos legales en ninguno de los procesos[908]. En consecuencia, a la hora de determinar los requisitos de la aplicación a desarrollar, reunido el personal informático con los usuarios expertos, con frecuencia estos últimos reclaman la inclusión en los formularios electrónicos de datos no exigidos por la normativa aplicable, de forma que se producen situaciones como las tratadas supra en referencia a la privación del trámite de subsanación[909].

El concepto de personal directivo para Métrica V3 agrupa a un conjunto variado de empleados, denominados comité de dirección, comité de seguimiento, directores de usuarios y usuarios expertos. Todos ellos comparten unas características comunes, como son su elevado

---

noviembre-diciembre de 2007, de la Asociación profesional de cuerpos superiores de sistemas y tecnologías de la información de las Administraciones públicas, ASTIC.

[907] MAP. Métrica V3. Participantes, 1.

[908] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 207.

[909] Debo insistir aquí en que el reproche de tal situación no ha de dirigirse a los informáticos. Los programadores no tienen ningún interés en incluir más o menos datos en el formulario, ni en hacerlos o no obligatorios. Son los usuarios quienes pretenden conseguir tanta información adicional como les sea útil para facilitar su trabajo. Por ello, la intervención de expertos legales resolvería tal problema.

nivel en la organización contratante (en nuestro caso, la Administración), el conocimiento de los objetivos estratégicos, del negocio, del entorno y de la organización, junto con la autoridad para validar y aprobar cada uno de los procesos realizados durante el desarrollo.[910]

Dentro del perfil de jefe de proyecto, Métrica V3 incluye no solo al propiamente dicho, sino también a los responsables de implantación, mantenimiento, operación, sistemas, seguridad y calidad. El perfil del consultor incluye al del mismo nombre, al consultor informático, al consultor de las tecnologías de la información, al especialista en comunicaciones, al técnico de sistemas y al técnico de comunicaciones. El perfil analista agrupa al analista propiamente dicho, junto con el administrador de la base de datos, los equipos de arquitectura, formación, implantación, operación, seguridad, soporte técnico y proyecto y al grupo de aseguramiento de la calidad. El perfil programador se limita al mismo. La inmensa variedad de trabajos asumidos por estos cuatro perfiles genéricos tienen una característica común, consistente en que, conforme a lo especificado por Métrica V3, en ningún momento aparecen restringidos al personal de la organización administrativa[911]. Por ello, resulta imprescindible revisar todas las actividades y tareas que pueden realizar, desde la óptica de sus implicaciones jurídicas, para poder deducir si debe restringirse a empleados públicos, lo que se revisará *infra* con detenimiento, tratando de alcanzar la suficiente profundidad como para ser capaces de responder a tan interesante cuestión, pero sin hundirnos demasiado en un abismo de tecnicismos. Antes de ello, conviene esbozar unas pinceladas sobre la generalidad del personal desarrollador.

[910] MAP. Métrica V3. Participantes, 2.
[911] *Vid*. MAP. Métrica V3. Participantes

La efectividad de cualquier equipo de desarrollo de *software* requiere una organización orientada a maximizar las habilidades y capacidades de sus integrantes, aunque resulta habitual que el líder no cuente con esa mezcla justa de habilidades que le permitan motivar al personal a producir a su máxima capacidad, organizar, alentar la creatividad, diagnosticar y resolver los conflictos técnicos y organizativos más relevantes, asumir el control cuando sea necesario, recompensar la iniciativa y el logro sin castigar la asunción controlada de riesgos, mantener el control en situaciones de alto estrés y construir equipo (comprendiendo las señales, verbales o no, y reaccionando ante las personas que las envían)[912].

En momentos relajados, en los que los plazos de entrega no pendan sobre las cabezas como espada de Damocles, el *mentoring* es una práctica a fomentar, la cual proporcionará no solo un incremento de conocimientos técnicos difícil de obtener por otros caminos, sino también un mayor disfrute en el entorno laboral, una socialización del puesto de trabajo y la satisfacción personal de compartir y de aprender, algo que procuraría a las organizaciones una mayor motivación de los empleados, menores tasas de movilidad laboral y un incremento en la capacitación individual y global del equipo[913], a lo que se añadiría la ventaja de disponer de un respaldo ante el riesgo de que el personal especializado en un tema se vea imposibilitado repentinamente para prestar sus servicios.

Alejadas quedan estas ideas de una realidad individualista, en la que cada cual guarda el conocimiento bajo llave y se encierra en su torre de marfil. La irrupción de la

[912] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 557-559.
[913] COLOMO PALACIOS, R./ TOVAR CARO, E./ GÓMEZ BERBIS, J.M./ GARCÍA CRESPO, A. (2007), recomendaciones, 2-4.

inteligencia emocional en el ámbito empresarial ha supuesto mejoras en la producción de los programadores que alcanzan hasta un 1272%[914]. La influencia de la motivación en la productividad de los programadores se ha estudiado desde hace años, concluyéndose que disponer de trabajadores motivados es fuente de buenos resultados[915].

7.2.1. La estimación de los recursos humanos necesarios

El cálculo exacto del esfuerzo requerido para desarrollar cualquier proyecto informático es excesivamente complejo y depende de factores inciertos o desconocidos, aunque las técnicas existentes proporcionan un valor aproximado que puede resultar suficiente y la experiencia extraída de la realización de proyectos similares anteriores resulta de utilidad.[916]

Viendo que el incremento innecesario del tamaño del grupo puede arrastrar efectos negativos y siendo conscientes de que los recursos humanos son el factor más influyente en la determinación de los costes totales, al tratarse de actividades con gran necesidad de capital humano, es preciso estimar adecuadamente el personal a dedicar al proyecto. Ese cálculo no es una tarea sencilla[917], por lo que son múltiples las técnicas de estimación que tratan de predecir el esfuerzo requerido para completar el desarrollo del *software* sin desviaciones de costes y de tiempo.[918]

---

[914] COLOMO PALACIOS, R./ TOVAR CARO, E./ CARRILLO VERDÚN, J. (2004), factor humano, 27.
[915] HERNÁNDEZ-LÓPEZ, A./ COLOMO PALACIOS, R./ GARCÍA CRESPO, Á. (2011), productividad, 52.
[916] MAP. Métrica V3. Gestión de proyectos, 2.
[917] Sin referirse específicamente a los contratos de servicios de desarrollo de aplicaciones informáticas, MENÉNDEZ SEBASTIÁN, E.M. afronta la que describe como "*difícil tarea de cuantificar los trabajos intelectuales*" en (2009), contratos de servicios del sector público, 533-539.
[918] HERNÁNDEZ-LÓPEZ, A./ COLOMO PALACIOS, R./ GARCÍA CRESPO, Á. (2011), productividad, 44.

A pesar de que no todas las técnicas de estimación tienen en cuenta factores como la experiencia y el estilo de programación (como las basadas en el análisis de los Puntos Fusión sugeridas por Métrica v3)[919], en mi opinión, son circunstancias que propician los retrasos y aumento de costes. Siguiendo COCOMO II, una evolución del modelo de estimación de costes COCOMO de Boehm, se pueden identificar seis aspectos relacionados con el personal que es necesario tener en cuenta[920]:

- Capacidad de los analistas.
- Capacidad de los programadores.
- Continuidad del personal.
- Experiencia en la aplicación.
- Experiencia en la plataforma.
- Experiencia con el lenguaje y las herramientas.

Cuando el trabajo sea realizado por los propios empleados públicos, la información sobre su capacidad, continuidad y experiencia concretas estará disponible para su valoración, o resultará fácilmente accesible, en el momento de estimar los recursos necesarios y los costes asociados, algo inviable en el momento de licitar un contrato de servicios para el desarrollo del *software* por empresas externas.

[919] MAP. Métrica V3. Técnicas y prácticas, 83.
[920] COLOMO PALACIOS, R./ TOVAR CARO, E./ CARRILLO VERDÚN, J. (2004), factor humano, 30.

La **experiencia** del equipo con el lenguaje y las herramientas específicas[921], en la aplicación[922] y en la plataforma concreta[923], resulta fácilmente verificable, en especial aquella que haya sido adquirida en la propia Administración en la que el empleado público presta sus servicios, siendo habitual su valoración como mérito en los concursos de funcionarios o incluso exigible como formación específica.

Si bien es imposible garantizar la **continuidad** del equipo, pudiendo finalizar por circunstancias sobrevenidas imposibles de prever, es presumible un elevado grado de estabilidad en el desempeño de los puestos de trabajo informáticos de las Administraciones públicas, no solo por la inamovilidad en la condición de funcionario, sino por la escasez de destinos alternativos en los que pueda prestar servicio el personal técnico fuera del área informática. La continuidad del empleado público en el puesto concreto obtenido por concurso se vincula en el TREBEP con la evaluación del desempeño, nada sencilla y poco materializada en la práctica.

Más compleja sin duda resultará la valoración de la **capacidad** de analistas y programadores, habida cuenta de la dificultad de establecer incluso lo que se entiende por capacidad, un concepto indeterminado que la Administración puede dotar de contenido dentro de

---

[921] Un ejemplo donde se exige como formación específica es "*experiencia demostrable en programación con lenguajes Cobol, Natural, C, etc., conocimientos de sistemas operativos (Unix, VSE, etc.) y en particular del entorno operativo del Gobierno de Cantabria, conocimientos en metodología de análisis y programación, capacidad de comunicación y aptitud para formar personas*", extraído del BOC extraordinario de 8 de enero de 2015, 352.

[922] Puede verse el BOC extraordinario de 31 de julio de 2009, 135, donde se valora como mérito "*experiencia en la coordinación, explotación y mantenimiento de la aplicación informática del Sistema Integrado de Gestión de Personal y Nóminas para el Personal Docente no Universitario de la Consejería de Educación. (0,09 puntos por mes)*".

[923] A modo de ejemplo, se valora como mérito "*experiencia en sistemas operativos (UNIX, VSE, etc.) y en particular del entorno operativo del Gobierno de Cantabria (0.09 puntos por mes*)", extraído del BOC de 17 de enero de 2006, 706.

un amplio margen de libertad (STC 50/1986)[924]. La edición 23 del diccionario de la RAE la describe como la "cualidad de capaz", lo que nos remite a este último vocablo, definido en su tercera acepción como "apto, con talento o cualidades para algo". Acercándonos un poco más al ámbito de la sociedad del conocimiento, es posible distinguir entre diferentes, pero muy próximos, conceptos. Así las "actitudes" son fundamentos conscientes, y los "conocimientos" son las bases necesarias para entender lo que se pretende, concluyendo que las "capacidades" son las condiciones suficientes para alcanzar el éxito, relacionadas con el talento (que debe ser desarrollado y retenido en la organización) y vinculadas al logro de altos rendimientos[925].

Los seis aspectos considerados en COCOMO II, resumidos como continuidad, mérito y capacidad, parecen adaptarse al empleo público con suma facilidad, coincidiendo con los principios constitucionales de aplicación en el acceso a la función pública, los cuales prolongan su vigencia a lo largo de la vida funcionarial, haciéndose patentes en los sistemas de provisión de puestos de trabajo y en el sistema de carrera administrativa y de promoción interna. La Administración tiene la posibilidad de escoger a los mejores analistas y programadores disponibles en el mercado laboral a través de la oferta de empleo público. Puede y debe diseñar los procesos selectivos siguiendo un criterio objetivo, de forma que su contenido se adecue a las funciones o tareas a desempeñar (artículo 55.2.e del TREBEP). Los requisitos de acceso han de responder única y exclusivamente a los principios de mérito y capacidad[926], sin que el grado de detalle en su definición pueda llegar a determinar a personas concretas e individualizadas (STC

[924] GARCÍA GARCÍA, M.J. (2008), principios constitucionales, 134.
[925] BUENO CAMPOS, E./ MERINO MORENO, C. (2007), creación de empresas, 4-5.
[926] *Vid*. PARADA VÁZQUEZ, R. (2015), empleo público, 455-457, donde el autor señala mérito y capacidad, regularidad y eficiencia de los servicios públicos y neutralidad de la Administración como causas eficientes de la implantación de la moderna burocracia.

269/1994) y siempre prevaleciendo la capacidad sobre el mérito, de modo que, en los concursos-oposición, no se pueda tener en cuenta los méritos acreditados cuando no se ha superado el mínimo de capacidad exigido (STC 67/1989)[927].

Por ello, la consideración de la capacidad, experiencia y continuidad del equipo de desarrollo integrado por empleados públicos, previsiblemente proporcionará estimaciones de recursos, costes y plazos bastante acertadas, sobre todo cuando se disponga de información detallada de proyectos anteriores similares con los que poder comparar el que se está valorando.

Sin embargo, los retrasos[928] son una constante en los proyectos informáticos, también en el ámbito público. Uno de los principios de la ingeniería del *software* citado *supra*, el referido a que las personas y el tiempo no son intercambiables, permite deducir que una inadecuada estimación de los recursos humanos requeridos para desarrollar el *software* acarreará problemas por incumplimiento de plazos con certeza. Un proyecto que se puede realizar en doce meses con un único programador no se podrá realizar en un mes empleando a doce programadores. Cada programador añadido, en términos netos, produce menos que el anterior, hasta llegar un momento en que añadir uno más es contraproducente[929].

[927] GARCÍA GARCÍA, M.J. (2008), principios constitucionales, 129-141.
[928] Hay que tener en cuenta que el incumplimiento del plazo de entrega no siempre es imputable al contratita. Los informáticos necesitan la colaboración de los usuarios expertos, por ejemplo para definir los requerimientos y para probar el *software*. La falta de disponibilidad de los usuarios, ya sea por desidia, por sobrecarga de trabajo, por rechazo a la informatización o por cualquier otro motivo imaginable, repercutirá negativamente en el plazo de entrega, sin que por ello se pueda imputar el retraso a la empresa desarrolladora.
[929] KRUGMAN, P.R./ WELLS, R./ OLNEY, M.L. (2008), fundamentos de economía, 167.

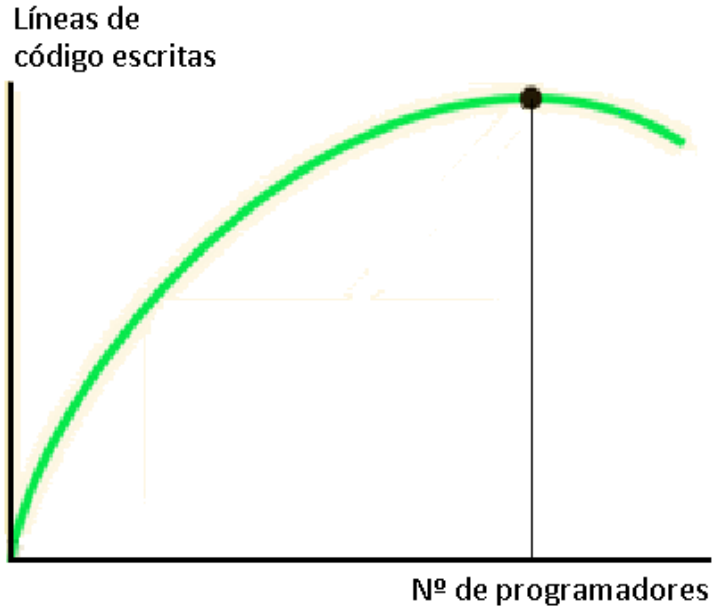

Figura 22: Productividad de los programadores de un proyecto

Fuente: KRUGMAN, P.R./ WELLS, R./ OLNEY, M.L. (2008), fundamentos de economía

Por ello, un retraso en el calendario, generalmente no se soluciona agregando más programadores. De hecho, suele introducir más demoras, debido a que la incorporación tardía de desarrolladores al proyecto resta tiempo a los ya existentes, que se ven obligados a asumir su formación, al menos en todo lo referente al aplicativo concreto que se está desarrollando. Ese tiempo de instrucción no lo emplean los veteranos en avanzar en el proyecto[930]. Conforme a lo establecido en el artículo 212 del TRLCSP, pueden establecerse en los pliegos penalidades para la demora en la entrega del *software* o, incluso, proceder a la resolución del contrato. En mi opinión, esto puede desencadenar un pernicioso efecto colateral, en concreto, la pérdida de

[930] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 624.

calidad. La duración del desarrollo del *software* y su calidad aumentan o disminuyen simultáneamente. El contratista siempre preferirá disminuir la calidad antes que sobrepasar el plazo de entrega, teniendo en cuenta que los defectos pueden no detectarse hasta haber finalizado el periodo de garantía y, en caso de no ser así, podrá afrontar su resolución durante la duración de la misma sin tener que sufrir penalidades por incumplimiento.

7.2.2. Aspectos destacables en gestión de personal

Habida cuenta de que la calidad de los recursos humanos se contagia a los sistemas de información desarrollados por ellos, la gestión del personal se convierte en un factor crucial a controlar. La revisión de los aspectos estudiados a tal efecto por un auditor informático puede aportar la claridad que ilumine el camino correcto a seguir a la hora de intentar mejorar la calidad y seguridad del *software* actuando sobre el personal que ha de desarrollarlo. Esos puntos a comprobar por el auditor son los siguientes:[931]

1. Objetividad en la selección del personal: debe valorarse la formación, la experiencia y los niveles de responsabilidad asumidos anteriormente en la cobertura de vacantes en el departamento de informática, incluyendo la promoción interna, la búsqueda directa de personal externo, utilización de empresas de selección de personal o de trabajo temporal…

2. Evaluación regular del desempeño: ha de valorarse su rendimiento basándose en estándares establecidos a los que añadir las responsabilidades específicas del puesto de trabajo concreto. Con esa intención, el TREBEP pretende incrementar la cualificación y motivación de los empleados públicos midiendo su rendimiento, valorando su conducta y

[931] RAMOS ESCOBOSA, J.M. (2001), auditoría de la Dirección, 221-223.

reflejando esos resultados directamente en sus retribuciones, en la progresión en su carrera profesional, etc., algo que no parece carente de dificultades. Entre ellas, cabe señalar la consecuente conflictividad a causa de la disconformidad con las evaluaciones recibidas y las dificultades para establecer la fijación de los parámetros a medir, los cuales necesariamente diferirán en función del puesto de trabajo concreto que ocupe el empleado evaluado, siendo necesario realizar un ingente trabajo de individualización de los parámetros a valorar[932]. Aplicado a los desarrolladores de *software*, podría contabilizarse el número de líneas de código generado por cada persona, lo que desencadenaría una preocupante proliferación de comentarios innecesarios dentro de los programas, fragmentación de cada instrucción en múltiples partes separadas por retornos de carro innecesarios e inconvenientes… También podría controlarse el número de programas codificado por cada empleado, quienes pasarían a dividir cada módulo en otros muchos de tamaño diminuto y disminuirían radicalmente el tiempo empleado en realizar las pruebas necesarias. Podría medirse el número de errores descubiertos, con lo que el programador inmediatamente tenderá a ocultarlos. En ingeniería del *software* se utilizan continuamente las más diversas métricas de productividad y de calidad con propósito de estimación, planificación y mejora, lo que proporciona beneficios significativos. Sin embargo, su utilización para la evaluación del desempeño choca frontalmente con algunas de las máximas a tener en cuenta en la administración de proyectos *software*, concretamente:

- ✓ "*No usar métricas para valorar a los individuos*".
- ✓ "*Nunca usar métricas para amenazar a los individuos o a los equipos*".

[932] ALMEIDA CERREDA, M. (2009), evaluación del desempeño, 119-120.

- ✓ "*No considerar "negativos" los casos de métricas que indiquen un área problemática*", pues simplemente son un indicio para mejorar el proceso[933].

Por otra parte, uno de los defectos reiterados que el Magistrado Jose Ramón Chaves detecta en las distintas experiencias de evaluación del desempeño examinadas, y que describe como "*el que tiene padrino se bautiza*", consiste en que el superior jerárquico informe de manera informal y propicie una valoración del desempeño del puesto de trabajo, determinando así el abono del complemento de productividad o influyendo en la adjudicación de uno u otro puesto de trabajo[934]. Eso, que puede ser reprochable en cualquier puesto de trabajo, arrastra una consecuencia importante en el ámbito del desarrollo de aplicaciones, como es la reformulación de uno de los principios básicos de la ingeniería del *software* detallados *supra*, "nunca dejes que tu jefe o cliente te convenza para hacer un mal trabajo", el cual pasará a redactarse ahora como "el jefe siempre tiene la razón".

3. Formación de los empleados: ha de determinarse su necesidad en función de su experiencia, puesto de trabajo, responsabilidad, desarrollo futuro personal y evolución tecnológica de la instalación, llevándose a la práctica de una manera planificada y ordenada. Además del calendario de cursos, de la descripción de cada uno de ellos y de los métodos y técnicas de enseñanza, hay que asegurarse de que los mismos sean consistentes con los conocimientos, experiencia y responsabilidades asignadas al personal, así como con la estrategia tecnológica marcada para los sistemas de información. Una nutrida colección de cursos sobre

[933] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 571-574.
[934] Recuperado de https://delajusticia.com/2015/02/26/evaluacion-del-desempeno-de-los-funcionarios-milonga-y-necesidad/ (18 de agosto de 2016).

programación avanzada en un lenguaje que el empleado no utiliza en su puesto de trabajo ni tiene la posibilidad de practicar con asiduidad, podría abultar el currículo del desarrollador incluyendo materias que realmente no domina.

4. Existencia de procesos para la promoción del personal que tengan en cuenta el desempeño profesional. En la cara opuesta de la moneda se detectan volúmenes importantes de rotación de personal, acompañados de altos niveles de absentismo laboral y de una cifra de proyectos con plazo y/o presupuesto sobrepasados estadísticamente elevada, todos ellos indicios de problemas en de liderazgo o de falta de motivación. Sin embargo, la promoción mediante el cambio de puesto de trabajo puede resultar complicada cuando la RPT no dispone de suficientes vacantes, situación que, como se verá *infra*, puede desencadenar graves problemas incluso en organismos medianamente voluminosos como es la GISS[935]. En los servicios informáticos de menor tamaño, como los de la Administración local o los de pequeñas Comunidades autónomas, el problema puede agudizarse al disponer de menos puestos de mayor nivel. Tratándose de una estructura de reducidas dimensiones, donde la progresión mediante la ocupación de puestos de mayor nivel es difícil de encauzar y lleva a muchos funcionarios a ver frustradas sus legítimas expectativas de mejora[936], cabría plantearse una peculiar modalidad de carrera administrativa, innovación apuntada por el TREBEP y calificada por Parada Vázquez como "la carrera de los inmóviles"[937], la carrera horizontal, basada, a la par, en no cambiar de puesto de trabajo y en desarrollar subjetivamente competencias a través del desempeño de aquel, valorando la trayectoria y actuación profesional del empleado público, la calidad de sus trabajos,

[935] *Vid.* SANTAMARÍA IBEAS, J.J. (1994), la LORTAD,
[936] ARROYO YANES, L.M. (2012), carrera profesional, 102.
[937] *Vid*. PARADA VÁZQUEZ, R. (2015), empleo público, 508.

los conocimientos adquiridos, el resultado de las evaluaciones de desempeño…, introduciendo así un factor de motivación personal.[938]

5. Establecimiento de controles de rotación de personal con el objetivo de asegurar que ni el cambio de puesto de trabajo de los desarrolladores ni la finalización de sus contratos laborales lleguen a afectar a la seguridad informática, para lo cual deberán existir procedimientos que inhabiliten las credenciales de acceso a locales y sistemas informáticos con efectividad inmediata, como contempla el ENS en sus medidas.

7.2.3. Los cuerpos TIC de las Administraciones públicas

La Administración es una organización profesional[939] que, conforme al artículo 103.1 de nuestra Constitución de 1978, sirve con objetividad los intereses generales, definidos por nuestro ordenamiento jurídico, con sometimiento pleno a la ley y al Derecho, aunque los nombramientos por razones de estricta confianza política merman las garantías de imparcialidad[940] y transparencia. El apartamiento de los fines vinculados a la utilidad pública o al interés social de la colectividad resulta tan fiscalizable por los tribunales como la comisión de

[938] FUENTETAJA PASTOR, J.Á. (2009), carrera horizontal, 63-70.
[939] *Vid*. PARADA VÁZQUEZ, R./ FUENTETAJA PASTOR, J. (2016), Derecho de la función pública, 394-398. Con aguda crítica, los autores cuestionan los patéticos intentos de mejorar la deteriorada imagen del empleo público mediante enumeración de deberes y códigos de conducta, calificados como "*una retahíla de obviedades morales*" incapaz de producir un efecto motivador significativo. Coincido plenamente con su interpretación del que podría ser el auténtico problema, cuando señalan que "*si en la provisión de los niveles de dirección de las empresas privadas se siguiesen los criterios que de ordinario se utilizan en el sector público para nombrar a los dirigentes de los organismos públicos, la inmensa mayoría de ellas no se libraría de la quiebra*".
[940] *Vid*. PARADA VÁZQUEZ, R./ FUENTETAJA PASTOR, J. (2016), Derecho de la función pública, 402. Resaltan los autores el deber de actuar con imparcialidad, igualitariamente y sin discriminación, conforme al artículo 14 de nuestra Carta Magna, con un comportamiento fundamentado en consideraciones objetivas al margen de cualquier otro factor.

una ilegalidad[941]. Por ello, en muchos casos, esas garantías esenciales estriban en la intervención de un funcionario o de un órgano colegiado que carezcan de vínculos clientelares y tengan garantizada la inamovilidad[942]. La asunción de los principios éticos[943] por los funcionarios es garantía de calidad en la prestación de los servicios públicos[944]. En nuestro país, esos funcionarios gozan de unas fuertes garantías de inamovilidad en el empleo y en el puesto de trabajo, que permite una defensa contra las habituales tentativas de politización del empleo público, aunque existe poco espacio real para el desarrollo profesional individual y se detecta una menguada productividad que encarece los servicios públicos. Hay que añadir la práctica inexistencia de una planificación estratégica de los recursos humanos que conduce a desajustes. Merecería la pena abordar las reformas necesarias pendientes para mantener un servicio público suficiente y de calidad, fomentando la profesionalidad frente a la politización, la flexibilidad frente a la rigidez, la planificación frente a improvisación y la valoración de méritos y estímulos adecuados frente a una concepción estática e igualitarista del empleo público. Pero, ante el déficit público, se opta por congelar su oferta y reducir la tasa de reposición de efectivos, de forma drástica y prácticamente indiscriminada, poniendo en riesgo la continuidad de algunos servicios.[945] Entre ellos, los cuerpos TIC también han sufrido esos recortes, justo cuando se quiere poner en marcha, sin camino de retorno, un proyecto tan necesitado de informáticos como es la Administración electrónica.

---

941 TOLIVAR ALAS, L. (2008), el personal de la Administración, 10.
942 SÁNCHEZ MORÓN. (2011), captura del empleo público, 72-73.
943 *Vid*. GARCÍA MEXÍA, P.L. (2001), ética pública, 131-168.
944 CARRO FERNÁNDEZ-VALMAYOR, J.L. (2010), ética pública, 14.
945 SÁNCHEZ MORÓN, M. (2011), empleo público en España, 20, 21y 27.

Afirma Esteve Pardo que la complejidad alcanzada por la tecnología imposibilita que los cuerpos de funcionarios tengan el conocimiento y control de sus posibles riesgos, añadiendo que, en la mayor parte de los sectores, es prácticamente imprescindible la colaboración de técnicos y expertos externos, quienes están en la vanguardia de la innovación, en el ejercicio de esa función tan inequívocamente pública por su trascendencia para el conjunto de la población[946]. Sus fructíferos estudios suelen centrarse en campos como el medio ambiente o la salud pública, por lo que cabe preguntarse por su aplicabilidad a un sector como el desarrollo del *software*, donde existen cuerpos especializados, como se verá *infra*.

Tolivar Alas describe a los empleados públicos como *"profesionales"* y añade *"que han ejercido el derecho constitucional a la libre elección de una actividad especializada* (…)", a quienes las Administraciones públicas, como personas jurídicas que son, encomiendan el servicio a los ciudadanos, convirtiéndolos en sus interlocutores *"identificados y responsables"*[947]. La progresiva implantación de las nuevas tecnologías llevó a la creación en la AGE de cuerpos de personal funcionario especializados en temas relacionados con las TIC, en previsión de asumir los servicios que venían siendo prestados por personal laboral[948]. La ley 4/1990, de 29 de junio, de presupuestos generales del Estado para el año 1990, en su artículo 33, creó el cuerpo superior de sistemas y tecnologías de la información de la Administración del Estado (correspondiente al antiguo grupo A, hoy grupo A subgrupo A1), el cuerpo de gestión de sistemas e informática de la Administración del Estado (antiguo grupo B, hoy grupo A subgrupo

[946] ESTEVE PARDO, J. (2014), contractualización, 1233.
[947] TOLIVAR ALAS, L. (2008), el personal de la Administración, 11.
[948] Desde 1970 existe una escala de informática en la seguridad social, dividida en seis clases diferentes, parcialmente integrada en 1992 en el cuerpo superior de sistemas y tecnologías de la información de la AGE.

A2) y el cuerpo de técnicos auxiliares de informática de la Administración del Estado (antiguo grupo C, hoy grupo C subgrupo C1), disponiendo las condiciones que permitirían la integración en ellos del personal laboral fijo que desempeñaba puestos informáticos[949].

Se puede rescatar del baúl de los recuerdos las palabras que unos años más tarde, a finales del siglo pasado, escribía el director del INAP. Afirmaba que "*la Administración del siglo XXI requerirá, aparte de la adaptación del Derecho administrativo a las nuevas realidades, la incorporación de funcionarios especializados que permitan mantenerla en la vanguardia tecnológica que una sociedad desarrollada requiere*"[950]. Casi dos décadas después es posible observar la evolución del personal TIC de la AGE consultando los datos publicados en los sucesivos informes anuales REINA. Comenzando en 1998, tras unos años de muy leves oscilaciones, en 2005 se incrementa el personal TIC de la AGE en un 15%, se estabiliza en 2006 y se amplía con una espectacular subida del 27% en 2007, el año de nuestra ley 11/2007, nuestra LAE. Ese incremento se compensa al año siguiente, cuando empieza oficialmente la crisis económica, con un descenso del 17%, un recorte quizás excesivo para un país con una ley de acceso electrónico recién estrenada, lo que pudo motivar la nueva remontada del 12% en 2009. Desde entonces, la tónica general es de un prolongado descenso[951].

[949] GUILLÉN CAMARÉS, J. (2010), mito o realidad, 23-24.
[950] ÁLVAREZ CONDE, E. (1998), formación de los funcionarios.
[951] Los datos de los años 2012 y 2013 no pueden ser considerados muy fiables de cara a comparaciones evolutivas, en el sentido de que se modificó la metodología empleada para el recuento de personal en la elaboración del informe REINA.

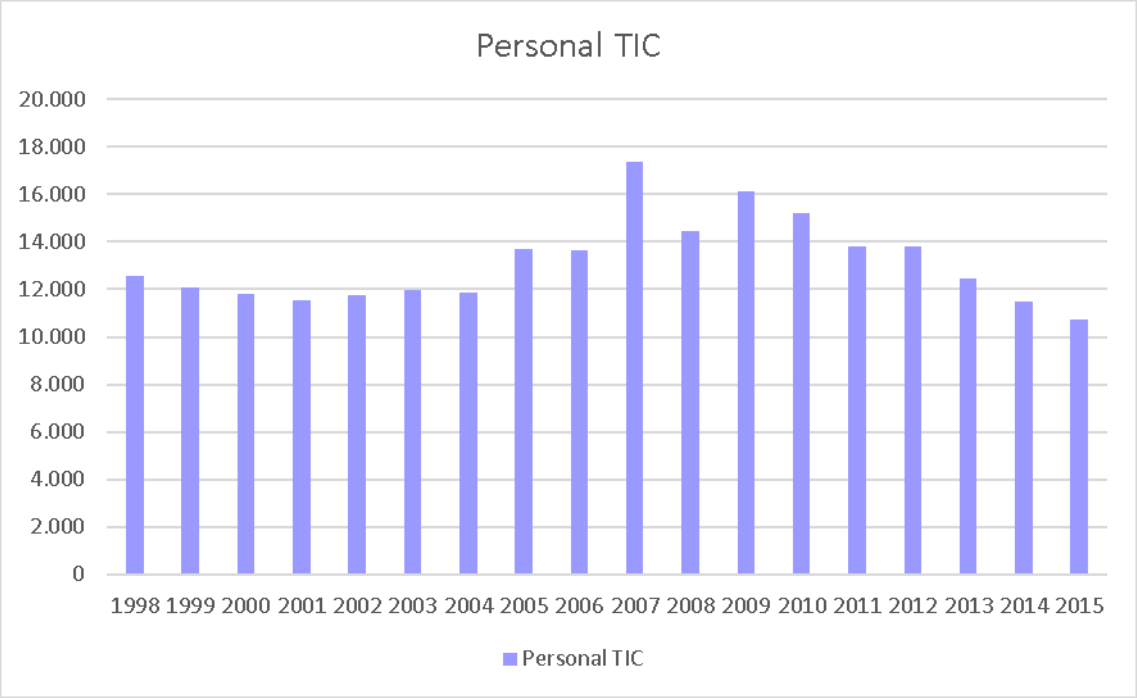

Figura 23: Evolución del personal TIC de la AGE

Fuente: Elaboración propia a partir de los informes REINA

Refiriéndose a la tendencia del gasto público en tecnologías de la información, descontados gastos de personal, hace poco más de tres años el presidente de ASTIC[952] mostraba su preocupación. A juzgar por la evolución de los efectivos antes comentada, los gastos en personal TIC parecen ser merecedores de la misma pesadumbre. Lamentaba que no fuera de esperar en ese año una corrección en la situación de caída libre en los recursos públicos dedicados a la tecnología en la Administración del Estado, advirtiendo que, tras la profundización de la tendencia decreciente del gasto, se corre el riesgo de pérdida de calidad de

[952] GARCÍA GARCÍA, E. (2013), más recursos.

los servicios digitales y, con ello, de las garantías de nuestros derechos y libertades. Transcurridos estos tres últimos años, el personal TIC sigue cayendo.

Su sucesor en el cargo defiende con pasión la labor de estos recursos humanos[953], a los que califica como pieza clave en los procesos profundos de innovación, cambio y optimización. Si bien podemos considerar previsible tal encendida defensa en palabras del presidente de su asociación profesional, podemos extraer unas ideas interesantes que, personalmente, comparto y defiendo:

- Los funcionarios TIC aúnan a su amplia formación en tecnologías de la información[954] el conocimiento interno de la Administración, que solo se logra con la permanencia y la pertenencia a ella, lo que los convierte en quienes mejor pueden encarar los proyectos de reingeniería que incrementen la eficiencia y el ahorro, basándose en una reorganización y rediseño que los haga más adecuados a las necesidades de los ciudadanos. Ahora bien, a esta afirmación debemos añadir algo que los técnicos suelen olvidar, y es que el aumento de eficacia en base a la simplificación y reingeniería de los procedimientos administrativos deberá respetar estrictamente las garantías derivadas de los principios de seguridad y legalidad[955].

- Es habitual oír la frase “pregunta a Informática” como respuesta a dudas de los empleados públicos en referencia al modo de realizar su propio trabajo. Como explica el presidente de ASTIC, esta conducta reiterada tiene una explicación razonable: durante la fase de análisis,

[953] MARTÍN VALLES, D. (2014), gobernanza TIC, 52-54.
[954] El temario incluido en la convocatoria de plazas del subgrupo A1 de 2015 puede consultarse en el BOE de fecha 23 de noviembre del mismo año.
[955] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 345.

imprescindible en todo desarrollo informático, el personal TIC se ve obligado a "*estudiar el funcionamiento a fondo y con todos los detalles de los procesos, ya que "las máquinas" necesitan que se les den instrucciones pormenorizadas de todas la situaciones y de toda la casuística de los procesos sobre los que actuamos*". Este análisis aporta un conocimiento importante a los desarrolladores que lo realizan, saber que debería enriquecer la formación de los propios empleados públicos, en lugar de perderse en el sector privado.

- Este personal TIC se debe potenciar, no disminuir sus efectivos, como instrumento de innovación, reinvirtiendo en ellos los ahorros conseguidos mediante la racionalización y concentración de los servicios.
- Y, por último, resalto y comparto su conclusión: "*estos recursos humanos, no se pueden externalizar ni concentrar fuera de los propios organismos, ya que son precisamente los que preservan conocimientos y habilidades que solo se adquieren en el trabajo diario, desde dentro de las unidades, a lo largo del tiempo*".

Las anteriores referencias a la disminución del personal TIC deben entenderse referidas a los empleados públicos, pues la evolución de los informáticos del sector privado que presta sus servicios en las Administraciones públicas es opuesta.

A modo de ejemplo, se puede analizar la evolución de un organismo destacable en su campo, la Gerencia de informática de la seguridad social, GISS, donde tuve la ocasión de comenzar mi carrera profesional precisamente en 1994, año en el que el apoyo externo se encontraba en un nivel mínimo y la oferta de empleo público para personal TIC funcionario fue masiva.

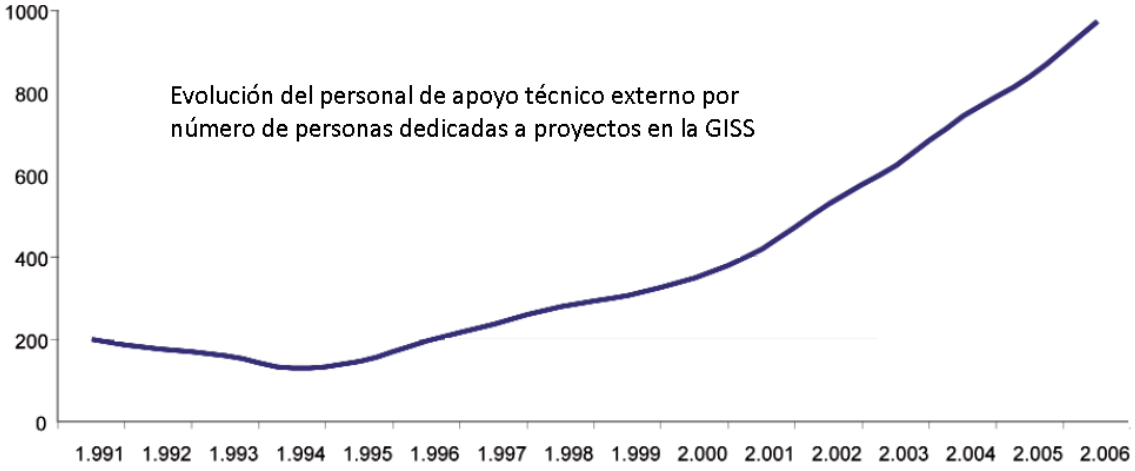

Figura 24: Evolución del apoyo externo en la GISS

Fuente: BoleTIC noviembre – diciembre de 2007

A partir del año 1996 comienza a producirse lo que se describe como una "fuga de cerebros", una pérdida de personal funcionario destinado en la GISS, que obedece a la falta de reposición de un significativo número de bajas por distintas causas[956], en las que parece haber tenido influencia el elevado índice de ocupación de los puestos de la RPT de niveles más altos, lo que dificulta las posibilidades de promoción y, con ello, las expectativas de una carrera profesional atractiva en su seno[957].

[956] La cercanía del año 2000 multiplicó las ofertas de trabajo para el personal TIC en cualquier parte del territorio nacional, incrementando la participación en concursos de traslados o las excedencias voluntarias por interés particular, en busca de nuevas oportunidades en ese sector privado que avanzaba con fuerza.
[957] SANTAMARÍA IBEAS, J.J. (1994), la LORTAD, 26.

Simultáneamente, los servicios informáticos prestados han experimentado un crecimiento totalmente desproporcionado, sobrepasando las disponibilidades de personal cualificado para su gestión. Por ello, "*se ha paliado el déficit de personal funcionario acudiendo como única fórmula posible, a la contratación de asistencia técnica externa* (…)", llegando a una situación no deseable técnicamente, una dependencia de la contratación de servicios que genera, al menos, los siguientes problemas[958]:

- Una progresiva pérdida de control de los proyectos asumidos, con un paulatino desconocimiento de los aplicativos gestionados por la propia organización. Sin control y con desconocimiento, difícilmente podrá la Administración garantizar que sus aplicaciones se ajustan a la legalidad.
- Alta movilidad del personal de las empresas de servicios cuando alcanzan un buen nivel de preparación, constituyendo una falta de continuidad en el equipo de desarrollo. Dada su incidencia, como vimos *supra*, en la estimación de los recursos necesarios para completar el proyecto, provoca incumplimiento de plazos e incremento de costes, con un efecto secundario asociado preocupante: las Administraciones públicas funcionan como una escuela en la que los informáticos noveles/becarios realizan sus prácticas para abandonarla posteriormente cuando empiezan a rendir de forma óptima.
- Dificultades importantes debidas al cambio de personal que se ocasiona al adjudicar los contratos a nuevas empresas. El conocimiento que había recaído en el sector privado que prestaba servicios a la Administración, aspecto ya problemático de por sí, desaparece por

[958] SANTAMARÍA IBEAS, J.J. (1994), la LORTAD, 24-29.

completo de la esfera pública al cambiar el adjudicatario. No existiendo obligación de subrogación, el escenario más favorable para la Administración pasa por el acuerdo individual de los efectivos salientes con la nueva empresa adjudicataria. En previsión de que no se alcancen dichos acuerdos, resulta humanamente comprensible que los usuarios licitadores no sean objetivos y vean su voluntad viciada de parcialidad, habida cuenta de su interés profesional (incluso personal) en mantener el conocimiento acumulado por el equipo desarrollador, en lugar de partir de cero con unos nuevos analistas y programadores.

- En los dos casos anteriores, el nuevo personal tarda un mínimo de tres meses en acomodarse al nuevo proyecto, lo que repercute negativamente en costes, fechas de entrega y dificultades en su dirección.

Años después, las noticias que nos llegan sobre la GISS confirman que la situación no ha mejorado[959]. El 64% de su plantilla en el año 2013 estaba constituida por personal externo. La Junta de personal denunció la privatización en la práctica de un organismo que gestiona bases de cotización, prestaciones por desempleo, datos de mutuas y bajas médicas, nóminas, vidas laborales y pensiones, etc. Precisamente, un grave incidente de seguridad afectó a las vidas laborales, dando lugar a la STSJ de Madrid 1140/2015, sala de lo contencioso, de fecha 30 de enero de 2015, que se comentará *infra*.

A todo ello hay que añadir el dato, confirmado por la propia seguridad social, de que el coste del personal externo es notoriamente más elevado que el de su empleado público

[959] (3 de noviembre de 2014) Recuperado de http://www.20minutos.es/noticia/2271636/0/seguridad-social-informatica/privaticacion-externo/personal-plantilla/ (23 de julio de 2016). Los mismos datos pueden encontrarse en http://www.europapress.es/economia/laboral-00346/noticia-economia-seguridad-social-tiene-casi-doble-informa ticos-contratados-funcionarios-cuestan-14-veces-mas-20141109173336.html (23 de julio de 2016).

equivalente. Las cifras exactas puestas de manifiesto en el Congreso de los Diputados confirman que un técnico medio informático externo cuesta 49.526,40 € anuales, mientras que el gasto por su equivalente funcionario se queda en 33.657,22 €, calculado a fecha de octubre de 2014. En el caso de personal de grupo A1, el externo supone 74.870,40 € anuales, mientras que el empleado público equivalente le cuesta a la Administración únicamente 53.017,40 €[960]. Agrava el problema el hecho de que el personal externo ha recibido formación por parte de la Administración y ha permanecido ubicado en edificios de la propia seguridad social, utilizando medios y recursos de la GISS, incluyendo material de oficina. La propia GISS reconoció tener que cambiar el sistema para minimizar la posibilidad de que se produjera una cesión ilegal de trabajadores, algo que ha salpicado a distintas Administraciones públicas, que aún se sigue planteando ante los tribunales y que trataré más detenidamente *infra*.

El encarecimiento de los gastos en personal externo no se limita al proporcionado a través de contratos de servicios informáticos. También se puede afirmar que el recurso a las ETT nunca es más económico que la contratación laboral directa[961].

Abandonando ya el ámbito de la AGE, en las Comunidades autónomas también se han creado cuerpos de personal TIC. A modo de ejemplo, puede citarse una de pequeñas dimensiones, uniprovincial, como es Cantabria, donde existen tres cuerpos análogos a los descritos en la AGE:

- En el subgrupo A1, cuerpo facultativo superior, especialidad de analistas de informática.

[960] Cifras obtenidas del BOCG, Congreso de los Diputados, serie D, núm. 529, de 6 de octubre de 2014.
[961] NORES TORRES, L.E. (2014), empleo público.

- En el subgrupo A2, cuerpo de diplomados y técnicos medios, especialidad de técnicos informáticos (en 2008 se convocó la oposición con un nombre de especialidad diferente, técnicos de gestión de sistemas, aparentemente por confusión con el nombre de los puestos básicos ofertados).
- En el subgrupo C1, cuerpo de técnicos auxiliares de informática.

A su vez, el Servicio cántabro de salud dispone de sus propios cuerpos informáticos:

- Subgrupo A1: cuerpo superior de sistemas y tecnologías de la información.
- Subgrupo A2: cuerpo de técnicos de gestión de sistemas y tecnologías de la información.
- Subgrupo C1: cuerpo de técnicos especialistas en informática.

A pesar de disponer de cuerpos informáticos y de existir una necesidad permanente de fuerza de trabajo, en lugar de dimensionar adecuadamente la plantilla, se externalizan los nuevos desarrollos de aplicaciones informáticas, cada uno de forma individual[962], mientras que el mantenimiento del *software* ya existente se licita en un único contrato, por dos años prorrogables otros dos más[963]. Pero, tras años de no convocar ninguna oposición para cuerpos informáticos, en 2016 se ofertan cuatro plazas a promoción interna del

[962] A modo de ejemplo, puede consultarse el BOC de 5 de mayo de 2015, 13200 y 13201, en las que figuran un contrato de servicios para el desarrollo de nuevas funcionalidades de los sistemas portafirmas electrónicos y comunicaciones electrónicas internas de la Comunidad autónoma de Cantabria, adjudicado a la empresa andaluza Guadaltel S.A. por 21.767,90 €, y otro contrato de servicios para el desarrollo de un nuevo sistema de información para la solicitud, seguimiento y control de vacaciones, licencias y permisos del personal del Gobierno de Cantabria, adjudicado a la empresa cántabra Viacore I.T. por 14.280,66 €.

[963] Su adjudicación en 2014 por casi 3.750.000 € puede consultarse en el BOC de 31 de julio del mismo año. En el Boletín de 22 de enero de 2016 puede verse una modificación por otros 200.000 € aproximadamente.

subgrupo C1 al A2, junto con una plaza libre del subgrupo C1 como consecuencia de haberse adscrito a ella a un trabajador afectado por una resolución judicial de reconocimiento de una relación laboral de carácter indefinido no fijo[964].

Las previsiones orientadas hacia la sostenibilidad económica recogidas en las sucesivas leyes de presupuestos generales del Estado han impedido la incorporación de nuevo personal fijo en las distintas Administraciones desde la ley 2/2012, aspecto que no ha cambiado hasta 2016. El personal informático destinado a implantar la eAdministración no ha sido contemplado entre los sectores favorecidos por las excepciones a la limitación.

La problemática descrita es consecuente con la filosofía que se deduce de la memoria del análisis de impacto del anteproyecto de ley del procedimiento administrativo común de las Administraciones públicas[965]. En ella se reconoce un posible impacto presupuestario de la nueva ley en la AGE, Comunidades autónomas y Entidades locales, motivado por la extensión del uso de la Administración electrónica y la necesidad, entre otras, de acometer nuevos desarrollos informáticos. Sin embargo, no relaciona este trabajo adicional con un incremento del Capítulo 1 (gastos de personal), sino únicamente con el Capítulo 2 (gastos corrientes en bienes y servicios) y Capítulo 6 (inversiones reales).

La reducción, o incluso desaparición, de las convocatorias de nuevas plazas para cuerpos TIC en las ofertas de empleo de las diferentes Administraciones, conlleva el envejecimiento de las plantillas de empleados públicos y el incremento del gasto al dispararse la externalización de los trabajos.

[964] BOC extraordinario de 31 de marzo de 2016.
[965] Páginas 49-50.

Si se está paliando el déficit de empleados públicos expertos en nuevas tecnologías confiando a empresas privadas el poder de indicar a las máquinas lo que deben hacer, sin que el órgano competente tenga los conocimientos adecuados para poder controlar lo que realmente se les ordena ejecutar[966], no podemos dejar de preguntarnos sobre la licitud de delegar en un sector privado afectado por la crisis del *software* el desarrollo de los programas que sustentarán nuestra nueva Administración electrónica, cuyo principal reto es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización[967]. Pero, además, causa una pérdida de capital intelectual en plena era del conocimiento, como se expone a continuación.

7.2.4. La dimensión humana del capital intelectual

La era del conocimiento ha venido acompañada de una transformación del modelo económico, en la que el "crepúsculo de los tangibles" de las últimas décadas del siglo pasado ha abierto camino al conocimiento como recurso productivo. La creación de capital intelectual es la nueva riqueza de las organizaciones[968].

---

[966] Aprovechando el momento actual en el que la Comisión para la reforma de las Administraciones públicas (CORA) afronta la racionalización y simplificación de los servicios públicos, el presidente de la Asociación profesional de cuerpos superiores de sistemas y tecnologías de la información de las Administraciones públicas, ASTIC, David Martín, nos recuerda la importancia de los recursos humanos para alcanzar los objetivos de la reforma, señalándolos como "*pieza clave en cualquier organización y, especialmente, cuando se abordan procesos profundos de innovación, cambio y optimización*", recalcando que esos recursos humanos no se pueden externalizar fuera de los propios organismos, dado que "*las máquinas necesitan que se les den instrucciones pormenorizadas de todas las situaciones y de toda la casuística de los procesos*", añadiendo que este "*conocimiento profundo de la organización solo se logra con la permanencia y pertenencia a la misma organización*". (2014). *Revista BoleTIC* (71), 52-54.

[967] Así se recoge el legislador en la exposición de motivos de la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

[968] BUENO CAMPOS, E. (2013), capital intelectual, 16-17.

La importancia del conocimiento y del capital intelectual se conoce desde la antigüedad pero, hasta mediada la década de los noventa, no se busca una definición estandarizada de ese concepto. Hoy son múltiples las formuladas y diversos los vocablos con los que se conoce. La literatura contable utiliza preferentemente la expresión "recursos intangibles" mientras que en los entornos económicos se habla más de "activos de conocimiento", dejando para el ambiente empresarial la locución "capital intelectual", que Edvinsson y Sullivan describen como aquel conocimiento que puede ser convertido en beneficio en el futuro, especificando que incluye ideas, inventos, tecnologías, programas informáticos, diseños y procesos. Para Stewart, es la suma de todos los conocimientos que poseen los empleados y que otorgan a la empresa ventaja competitiva. Para Robinson y Kleiner lo conforman conocimientos, habilidades, experiencia, sistemas de información, propiedad intelectual, estructuras organizativas, etc.[969]

Parece existir cierto consenso en dividir el capital intelectual en tres componentes[970]:

- ESTRUCTURAL, que comprende aquellos conocimientos que la empresa ha podido internalizar y que permanecen en la organización incluso cuando los empleados la abandonan lo que incluye el valor del conocimiento que se materializa en sus sistemas y desarrollos tecnológicos.

[969] SÁNCHEZ MEDINA, A.J./ MELIÁN GONZÁLEZ, A./ HORMIGA PÉREZ, E. (2007), concepto de capital intelectual, 97-99.
[970] CIDEC (2004), capital intelectual, 51.

- RELACIONAL, que se extiende al valor que generan las relaciones de la empresa con clientes, proveedores, accionistas y cualquier otro grupo de interés, interno o externo.
- HUMANO, equivalente al valor creado por las personas, que consiste en el conocimiento útil para la misión de la organización, explícito o tácito, individual o social, que poseen las personas y grupos, junto con su capacidad para generarlo[971], y que puede dividirse en tres factores integrantes:
  - ✓ Competencias: conocimientos, capacidades, talento y saber hacer (*know-how*).
  - ✓ Actitud: conducta, motivación, actuación y ética de las personas.
  - ✓ Agilidad intelectual: se aplican conocimientos nuevos o descubrimientos que permiten transformar las ideas en productos y servicios[972].

La disposición de unos recursos humanos competentes, capacitados, con un nivel de formación adecuado al puesto de trabajo, activos, con capacidad para innovar, constituye un activo intangible fundamental para conseguir los objetivos propuestos por la organización. El *know-how*, competencia que hemos denominado como "saber hacer", está relacionado con el conocimiento acumulado por el conjunto del personal de la organización, por una forma de trabajar y por la existencia de unos procedimientos propios característicos de esa entidad, que es uno de los componentes del fondo de comercio bien conocido en la contabilidad empresarial tradicional[973].

[971] BUENO CAMPOS, E./ MERINO MORENO, C. (2007), creación de empresas, 3.
[972] SÁNCHEZ MEDINA, A.J./ MELIÁN GONZÁLEZ, A./ HORMIGA PÉREZ, E. (2007), concepto de capital intelectual, 102-107.
[973] BOSSI QUEIROZ, A., FUERTES CALLÉN, Y. Y SERRANO CINCA, C. (2001), capital intelectual, 10-13.

También se consideran intangibles las condiciones laborales. Conceptos como el ambiente, las posibilidades de promoción, los incentivos o la seguridad en el empleo inciden en el rendimiento de los trabajadores[974].

El sector público ha venido mostrándose más lento a la hora de incorporar la medición y registro de sus activos intangibles, a pesar de que la intangibilidad está presente en él de forma mayor que en las empresas privadas. En estas predominan los objetivos cuantificables ligados a la obtención de beneficios económicos, a la par que las Administraciones públicas buscan la prestación de servicios, claramente intangibles. Los recursos empleados en el sector público son mayoritariamente el capital humano y el conocimiento, ambos intangibles y, aunque también están presentes en el sector privado, difieren en su objetivo, pues aquí tienen que servir para ganar dinero[975]. Obviamente, ese capital humano manifiesta importantes diferencias entre los sectores público y privado; además de que unos se deban al servicio público y otros busquen generar beneficios económicos, no se asemejan ni en su captación, ni en los incentivos que los motivan, ni tampoco en la propia gestión de personal[976].

Entre los retos pendientes está el reconocimiento del papel protagonista de personas y organizaciones, como propietarios o poseedores del conocimiento[977]. Con estas ideas brevemente expuestas en mente, es el momento de revisar el trabajo de los desarrolladores, con una mirada crítica que se plantee la transcendencia de cada paso dado, a la luz de la seguridad

[974] BOSSI QUEIROZ, A., FUERTES CALLÉN, Y. Y SERRANO CINCA, C. (2001), capital intelectual, 14.
[975] BOSSI QUEIROZ, A., FUERTES CALLÉN, Y. Y SERRANO CINCA, C. (2001), capital intelectual, 3-5.
[976] BOSSI QUEIROZ, A., FUERTES CALLÉN, Y. Y SERRANO CINCA, C. (2005), reflexiones, 225.
[977] BOSSI QUEIROZ, A., FUERTES CALLÉN, Y. Y SERRANO CINCA, C. (2005), reflexiones, 17.

del sistema de información y valorando la incidencia de las distintas tareas sobre el capital intelectual humano.

7.3. EL DESARROLLO DEL *SOFTWARE* DE LAS ADMINISTRACIONES PÚBLICAS

"*Una vez más estamos en las manos de los programadores, de los informáticos.* (…) *el mensaje es claro: prestemos atención a la formación de la voluntad de la Administración en un mundo dominado por las nuevas tecnologías*"[978]. Estas acertadas palabras resumen a la perfección el objetivo de este capítulo, algo extenso y relativamente técnico, pero necesario para ser conscientes del modo en que los informáticos marcan la voluntad administrativa.

En el caso concreto de la actuación administrativa automatizada, la voluntad humana desaparece con habilitación legal, aunque de un modo meramente aparente, pues se manifiesta mediante la previa aprobación de la programación, la cual responderá a los criterios técnicos establecidos sobre la base de criterios jurídicos[979].

Las instrucciones que dicten las decisiones del "empleado público electrónico" han de ser las adecuadas y han de cerrar todo resquicio que pueda ser aprovechado por un ciberatacante. Sin embargo, no resulta viable posar la mirada sobre miles, o incluso millones, de líneas de código de una aplicación informática y asegurar su corrección. Es materialmente imposible desde el momento en que los programas superan cierto tamaño. Intentarlo podría significar un reto para su autor pero, sin duda, supondrá una pesadilla condenada al fracaso para

[978] PIÑAR MAÑAS, J.L. (2011), revolución tecnológica, 39.
[979] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 16.

los ojos ajenos, cuya aspereza será proporcional a la carencia o desactualización de la documentación adjunta.

Que el *software* sea un producto muy difícil de validar refuerza la necesidad de incrementar su control durante la etapa de desarrollo, con la pretensión de vigilar y mejorar su calidad y, en consecuencia, disminuir el coste del posterior e imprescindible proceso de mantenimiento. El alto índice de fracasos en la industria del *software* lleva a preguntarse si dichos controles funcionan adecuadamente o, incluso, si se está prescindiendo de su utilización. Es difícil conseguir que las empresas hagan públicas las cifras de sus carísimos desastres pero, aunque sea solo a título ilustrativo, podemos ver valores ofrecidos por el informe *The Chaos Manifesto* de 2013 de *Standish Group*, donde se indica que[980]:

- ✓ Un 18% de los proyectos fracasa, ya sea por su cancelación antes de ser terminado o bien porque nunca se usó tras ser entregado.
- ✓ Otro 43% sufre dificultades durante su desarrollo y se finaliza tarde, sobrepasando el plazo de entrega y/o el presupuesto comprometido y, con frecuencia, sin proporcionar todas las características o funciones solicitadas.
- ✓ El 39% restante culmina con éxito, siendo entregado en el tiempo y presupuesto acordados y con las funciones y características solicitadas.

En mi opinión personal, este porcentaje de proyectos exitosos resulta excesivamente optimista. En mayor o menor grado, sobrepasar el plazo de entrega y/o carecer de

[980] FERNÁNDEZ SÁNCHEZ, C.M./ RODRÍGUEZ MONJE, M./ PIATTINI VELTHUIS, M.G. (2013), calidad del producto *software*, 31.

alguna de las características o funciones solicitada en los pliegos de prescripciones técnicas resulta mucho más habitual que los que finalizan de forma satisfactoria.

El desarrollo de aplicaciones informáticas no es una empresa fácil, y así lo confirman las múltiples metodologías que han intentado abordar de forma homogénea y abierta cada una de las actividades de su ciclo de vida[981]. Un uso excesivamente estricto de dichas metodologías puede ralentizar el desarrollo y, habida cuenta de que las aplicaciones informáticas, por lo general, se construyen con un grado de urgencia cada vez mayor[982], muchas voces se manifiestan en contra de su utilización. Esas opiniones parecen olvidar que esas metodologías de desarrollo, características de una disciplina como la ingeniería del *software,* no son rígidas, sino adaptativas, ajustables a todas las actividades y dominios de aplicación, en función del producto concreto a obtener, de la gente que lo construye y del modelo de negocio[983].

De las múltiples metodologías existentes podríamos haber seleccionado cualquiera para revisar el proceso de desarrollo pero, centrándose en el *software* de las Administraciones públicas, parece suficientemente justificada la elección de la metodología para la planificación, desarrollo y mantenimiento de sistemas de información, Métrica V3[984], elaborada por el Ministerio de Administraciones públicas teniendo en cuenta métodos como MAGERIT, Eurométodo, SSADM V4 o *Information Engineering* y normativas internacionales como ISO 12207, ISO/IEC TR 15504/SPICE, UNE-EN ISO 9001:2000 o IEEE 610.12-1990.[985]

---

[981] LABORATORIO NACIONAL DE CALIDAD DEL *SOFTWARE* (INTECO) (2009), ingeniería del *software*, 39.
[982] No es nada extraño que el usuario indique al informático que "lo necesita para anteayer".
[983] LABORATORIO NACIONAL DE CALIDAD DEL *SOFTWARE* (INTECO) (2009), ingeniería del *software*, 8.
[984] Disponible en el portal de Administración electrónica, recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html#.V3oKZaPp-VM (26 de julio de 2016)
[985] INTECO. *Estudio sobre… Op. cit.* (p. 66).

Métrica V3[986], a pesar de que existen otras metodologías mucho más actualizadas[987], es un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del *software*, contemplando también los aspectos de gestión que aseguran que un proyecto cumple sus objetivos en términos de calidad, coste y plazos, con referencias específicas a la seguridad. Abarca el desarrollo del *software* completo, con independencia de su complejidad y magnitud. Dada su adaptabilidad y flexibilidad, aunque parte de una estructura que responde a desarrollos máximos, en cada proyecto se deberá adaptar y dimensionar conforme a las características del caso concreto.

La metodología Métrica V3 estructura el proyecto en tres grandes partes, de las cuales destaca la segunda por su amplitud y complejidad, por lo que se divide, a su vez, en cinco procesos menores:

- ✓ Planificación de sistemas de información (PSI).
- ✓ Desarrollo de sistemas de información.
  - Estudio de viabilidad del sistema (EVS).
  - Análisis del sistema de información (ASI).
  - Diseño del sistema de información (DSI).
  - Construcción del sistema de información (CSI).

[986] Las versiones 3 de Métrica y de MAGERIT son las incluidas en el catálogo actualizado de servicios de la Administración digital de abril de 2016, descargado de http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/Racionaliza_y_comparte/catalogo/CATALOGO-SERVICIOS-ADMINISTRACION-DIGITAL-V1-0.pdf (11 de septiembre de 2016).
[987] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 196.

- Implantación y aceptación del sistema (IAS).

✓ Mantenimiento de sistemas de información (MSI).

Cada uno de estos siete procesos se descompone en actividades, que pueden realizarse en paralelo o en orden diferente al propuesto. Sin embargo, nunca puede darse por acabado cada uno de los procesos hasta no haber finalizado todas las actividades que, desde el inicio, se hubiesen seleccionado de entre las previstas por Métrica V3[988]. A su vez, cada actividad se divide en tareas. Métrica V3 describe el contenido de cada tarea y hace referencia a las principales acciones a realizar, productos a generar, técnicas a emplear, prácticas a llevar a cabo y participantes de cada una de ellas.

Considerando la posible necesidad de reforzar algunos aspectos concretos, esta metodología proporciona lo que denomina "interfaces", dedicadas específicamente a la gestión de proyectos (permitiendo conocer y resolver o, al menos, paliar los problemas que se producen, para evitar desviaciones temporales y económicas), al aseguramiento de la calidad, a la gestión de la configuración (garantizando que no se realizan cambios incontrolados) y a la seguridad (contemplando únicamente los riesgos lógicos, es decir, fallos propios, ataques externos, virus, etc., obviando los riesgo naturales, como inundaciones, incendios…)[989].

La interfaz de seguridad hace hincapié en la formación en la materia. Su objetivo es incorporar en los sistemas mecanismos de seguridad adicionales a los propuestos en la propia

[988] MAP. Métrica V3. Introducción, 3-4.
[989] MAP. Métrica V3. Inroducción, 14.

metodología, utilizando MAGERIT para el análisis y gestión de riesgos en el caso de que la organización no disponga de su propia metodología.

Resulta obligado destacar el acertado enfoque de la versión 3 de Métrica en relación con la seguridad. Si bien la tradición en la industria del *software* ha venido siendo la consideración de la seguridad como un requisito no funcional, Métrica V3 la tiene en cuenta como un requisito funcional, lo que conlleva su tratamiento desde etapas tempranas[990]. Lo contrario, como ya he señalado *supra*, dispararía los costes a la vez que debilitaría la resistencia de la solución implementada.

Dicha interfaz cubre tanto las actividades relacionadas con la seguridad intrínseca del sistema de información como las que velan por la del propio proceso de desarrollo. Presupone que la organización dispone de un plan de seguridad. En su defecto, deberá ser desarrollado (aunque no de forma imperativa, sugiere para ello la utilización de MAGERIT).

La interfaz se muestra realista, reconociendo la limitación de los recursos disponibles, por lo que parte de la imposibilidad de asegurar todos los aspectos del desarrollo, viéndose obligada a aceptar un determinado nivel de riesgo y a concentrar los esfuerzos en aquellos aspectos que resulten más comprometidos o amenazados en cada caso particular, según la valoración resultante de la reflexión sobre complejidad, tamaño, incertidumbre, participantes, etc. Los responsables de la seguridad del sistema serán quienes fijen el nivel de riesgo aceptable. Determinar quiénes tienen la competencia para desempeñar ese papel y comprometer la seguridad de los aplicativos de las Administraciones son aspectos abiertos a la controversia,

[990] MAP. Métrica V3. Interfaz de seguridad, 4.

donde resulta vital conocer las implicaciones de sus decisiones en cada momento del ciclo de vida del *software*.

7.3.1. Planificación de sistemas de información

La planificación se realiza con anterioridad a lo que generalmente se conoce como desarrollo del *software*, con vistas a alinear las actuaciones posteriores con los objetivos de la estrategia corporativa[991]. No es un cometido que le corresponda realizar, ni siquiera empujar, a la "dirección de informática", a pesar de que será ella la permanente impulsora que velará por una planificación adecuada y a tiempo a lo largo del proyecto[992]. Requiere la participación de los responsables de los procesos de la organización, que son quienes cuentan con una visión estratégica, acompañados de los profesionales de sistemas de información, quienes prestarán su ayuda aportando ventajas competitivas por medio de las TIC[993]. Todos ellos orientarán sus decisiones a la mejora de la seguridad y al aseguramiento de calidad.

La implicación de esa alta dirección, empleados públicos como señala Métrica V3, incrementa las posibilidades de lograr desarrollar el proyecto con los recursos necesarios y en el calendario establecido, atendiendo a intereses globales, no a los particulares, siempre con una visión general que apoye los objetivos estratégicos y establezca prioridades conforme a ellos. Con esas premisas, en este proceso de planificación se propondrá una arquitectura de información con una visión más estratégica que tecnológica[994].

---

[991] Advierte la introducción a Métrica V3 que no se debe confundir esto con una mejora o reingeniería de procesos.
[992] RAMOS ESCOBOSA, J.M. (2001), auditoría de la Dirección, 212.
[993] MAP. Métrica V3. Introducción, 4.
[994] MAP. Métrica V3. Introducción, 4.

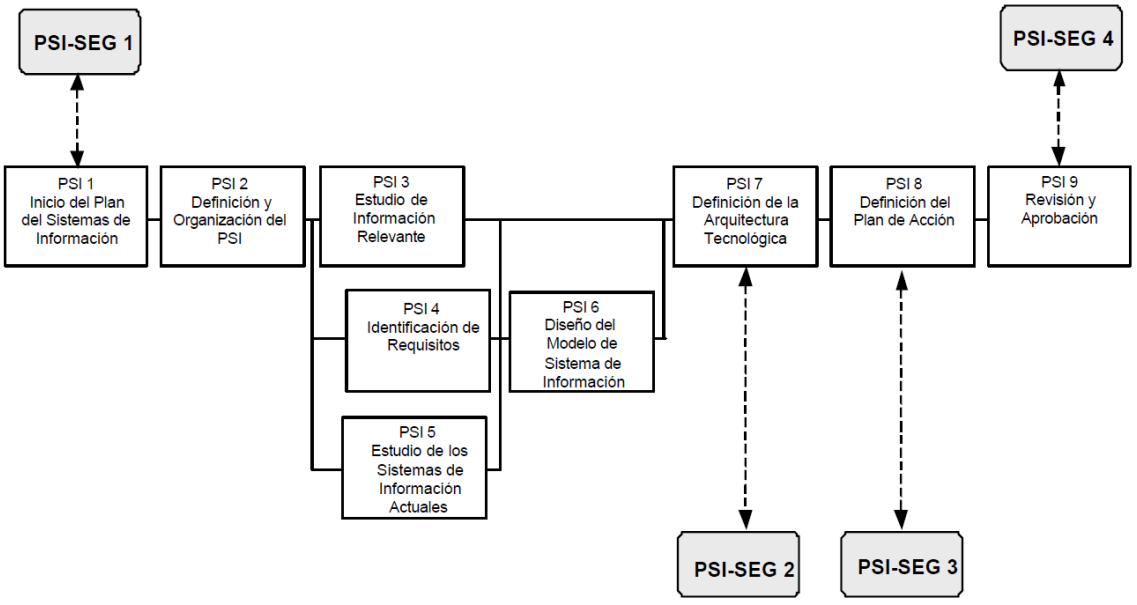

Figura 25: Actividades de PSI

Fuente: Metodología Métrica versión 3. Interfaz de seguridad, 5.

Comentando muy someramente los trabajos a realizar en los diferentes momentos, con la finalidad de argumentar razones a favor o en contra de la intervención del personal del sector privado en los trabajos conducentes a la obtención del *software* que sustentará nuestra Administración electrónica, esta revisión comienza con el análisis de las expectativas de las áreas que han solicitado la realización del proyecto. Si se considera adecuada su continuación, se determinan los objetivos estratégicos, los factores críticos de éxito y los responsables de las áreas implicadas[995]. El responsable de seguridad determina la organización y planificación de la

[995] MAP. Métrica V3. Interfaz de seguridad, 4-5.

misma, necesaria en el PSI desde los puntos de vista de la autenticación, confidencialidad, integridad y disponibilidad[996]. El comité de dirección, los directores de usuarios y el jefe de proyecto indica el ámbito y objetivos más específicos. Los dos últimos precisan detalles logísticos, de organización y de comunicación[997]. Los consultores se reúnen con los usuarios expertos para elaborar la especificación de los requisitos de información de la organización, clasificados y catalogados por su prioridad, obteniendo un modelo de información que refleje las principales entidades y sus relaciones, analizando cómo debería ser cada proceso por contraposición a cómo es en la actualidad[998], acción totalmente coherente con lo establecido por el artículo 34 de nuestra antigua LAE y por el principio de simplificación administrativa.

Los sistemas de información existentes se analizan y valoran, obteniendo un diagnóstico de la situación actual e indicando los sistemas a conservar y los requisitos no cubiertos, con su criticidad y prioridad, así como las mejoras a realizar[999]. Los consultores informáticos y el equipo de soporte técnico analizan las necesidades de infraestructura tecnológica, proponiendo alternativas viables para satisfacerlas con una visión de futuro, considerando la posible evolución de las distintas tecnologías candidatas y de las actuales[1000]. La evaluación de las vulnerabilidades, riesgos y costes de los mecanismos de seguridad a implantar en cada una de las soluciones propuestas le corresponde al responsable de seguridad, con la

[996] MAP. Métrica V3. Interfaz de seguridad, 6-7.
[997] *Vid*. MAP. Métrica V3. Planificación de sistemas de información, 5-7.
[998] MAP. Métrica V3. Planificación de sistemas de información, 8-10.
[999] MAP. Métrica V3. Planificación de sistemas de información, 10-14.
[1000] MAP. Métrica V3. Planificación de sistemas de información, 14.

colaboración de su propio equipo, pudiendo tomar como referencia la metodología de gestión de riesgos MAGERIT[1001].

Tras analizar el impacto en la organización y los medios, tiempo y recursos económicos necesarios para la implantación de cada opción, los consultores informáticos y el equipo de soporte técnico, en colaboración con los usuarios expertos, seleccionan la arquitectura tecnológica más adecuada[1002]. El comité de seguimiento y el responsable de seguridad examinan la alternativa escogida y el estudio de seguridad de las distintas opciones barajadas, manifestando su aceptación o rechazo[1003].

Ya se determinó que el comité de seguimiento está constituido por miembros de la Administración, pero cabe preguntarse si el responsable de seguridad ha de ser un empleado público. En la Administración local, en los casos de muy reducido tamaño, podrían plantearse dificultades para cumplir, únicamente con empleados públicos, el principio básico de "función diferenciada en materia de seguridad", que obliga a que la responsabilidad de la información, el servicio y la seguridad recaigan sobre personas distintas[1004]. En cualquier caso, a los efectos de decidir si la manifestación de aceptación o rechazo de la alternativa seleccionada y del estudio de seguridad obtenido puede ser imputada a la Administración, incluso en los casos en que se contraten servicios externos para la realización del PSI, la respuesta ha de ser afirmativa, habida cuenta de que el comité de seguimiento es un órgano administrativo cuya intervención y aceptación es preceptiva.

[1001] MAP. Métrica V3. Interfaz de seguridad, 8.
[1002] MAP. Métrica V3. Planificación de sistemas de información, 15.
[1003] MAP. Métrica V3. Interfaz de seguridad, 9.
[1004] Artículos 4 y 10 del ENS.

En el plan de acción se definirán los proyectos y acciones con los que llevar a cabo la implantación de la arquitectura de información propuesta, priorizados según los criterios que se consideren oportunos, junto con un calendario en el que se especifiquen recursos y fechas prevista de inicio y fin de cada uno. El orden definitivo de esos proyectos y acciones debe pactarse con los usuarios, para llegar a una solución de compromiso que resulte la mejor posible para la organización, sin olvidar que la sobrecarga es una de las causas de la crisis del *software*. Se propone también un plan de mantenimiento para el control y seguimiento de la ejecución de los proyectos[1005]. El comité de seguimiento y el responsable de seguridad determinan la política de seguridad a llevar a cabo en el plan de acción, en función de los riesgos aceptados, detallando la forma en que efectuar la puesta en marcha de los servicios y mecanismos de salvaguarda y la infraestructura y los recursos necesarios para ello[1006]. Próximo a finalizar el PSI, el responsable de seguridad estudia los productos generados durante el proceso y determina en común el nivel de seguridad de cada uno con respecto a la autenticación, confidencialidad, integridad y disponibilidad[1007].

Tras elaborar, revisar y mejorar un estudio que recoja los resultados de los trabajos realizados hasta ese momento, se somete la propuesta final a la aprobación formal del comité de dirección del PSI[1008]. La colaboración de empresas de consultoría, experimentadas en la elaboración de planes estratégicos de sistemas para el sector público, puede aportar las ventajas de una visión externa que enfoque hacia el objetivo final desde nuevos ángulos

[1005] MAP. Métrica V3. Planificación de sistemas de información, 15-17.
[1006] MAP. Métrica V3. Interfaz de seguridad, 10.
[1007] *Vid.* MAP. Métrica V3. Interfaz de seguridad, 11.
[1008] *Vid*. MAP. Métrica V3. Planificación de sistemas de información, 17-19.

inexplorados. Nada parece obstar a ese aporte de savia fresca procedente del exterior salvo, quizá, la referencia del artículo 41.2 de la ley 40/2015 en cuanto a la competencia para la definición de especificaciones tratada *supra*. Por ello, resulta conveniente reflexionar sobre el alcance del concepto "especificaciones".

Es habitual en el ámbito informático diferenciar los "requisitos o requerimientos", interpretados como la descripción de "qué hay que hacer", de las "especificaciones", entendidas en el sentido de "cómo hay que hacerlo". Examinando el contexto en el que el legislador utiliza el vocablo "especificaciones", es difícil presuponer tal sutileza en su elección de palabras, habida cuenta de que van inmediatamente seguidas por las voces "programación" y "mantenimiento", dos términos de uso cotidiano carentes de cualquier matiz tenue restringido a los especialistas. Sin embargo, este razonamiento se desmonta al leer la expresión "código fuente" cerrando el artículo, dos palabras que rara vez habrá pronunciado juntas el ciudadano medio. Por lo tanto, el contexto no nos ayuda a determinar su intención.

Para la edición 23 del diccionario de la RAE, una especificación, conforme a su acepción 2ª, es la "*información proporcionada por el fabricante de un producto, la cual describe sus componentes, características y funcionamiento*". Realizando una interpretación literal de la expresión "definición de especificaciones", podríamos entender afectada por el tenor del artículo 41.2 a **toda definición de componentes, características y funcionamiento del producto a desarrollar**, rechazando una interpretación restrictiva que limitara su alcance a la noción de "especificaciones" excluyente de los "requisitos o requerimientos".

Métrica V3 dedica su tarea PSI 2.1 a la especificación del ámbito de los procesos de la organización que desea considerar, definiendo su alcance, es decir, los objetivos específicos del plan, algo que no parece abarcado entre la relación de materias enumeradas en el 41.2, a pesar de su apelativo de "especificación". Sin embargo, no puede afirmarse lo mismo sobre la actividad PSI 4, donde Métrica V3 declara que "*el objetivo final de esta actividad va a ser la especificación de los requisitos de información de la organización* (…)"[1009]. En esta ocasión los consultores, ya sean propios o externos, descienden en el nivel de abstracción, llegando a estudiar con los usuarios expertos cómo debería ser cada proceso concreto (lo que puede abarcar actuaciones administrativas automatizadas), identificando y catalogando los requisitos de la información, lo que va a repercutir en la definición de componentes, características y funcionamiento del producto a desarrollar.

Recopilando las reflexiones anteriores y exceptuando los minoritarios casos en que se vean afectadas materias que afecten a la seguridad nacional o defensa nacional, nada parece impedir la intervención de una empresa de consultoría externa en la elaboración del PSI, incluso para colaborar con los usuarios expertos en la obtención de un catálogo de requisitos que recoja las especificaciones acordadas. Para llegar a esta conclusión, resulta primordial tener en cuenta que el catálogo de requisitos es un documento de fácil lectura, apto para su comprensión por el comité de dirección, que ha de aprobar formalmente la propuesta final, aceptación producida con pleno conocimiento y entendimiento de lo que se está avalando, haya intervenido o no una empresa externa en su elaboración. Por tanto, en el hipotético caso de que las especificaciones afectasen a una actuación administrativa automatizada, las exigencias del

[1009] Métrica V3 – Planificación de sistemas de información (p. 8).

artículo 41.2 de la ley 40/2015 se verían válidamente cumplidas si el órgano administrativo que hubiera sido previamente designado como competente para la definición de esas especificaciones, coincidiera con el órgano que Métrica V3 denomina "comité de dirección", dado que aprueba formalmente la propuesta, con el suficiente conocimiento y comprensión de sus implicaciones.

7.3.2. Estudio de viabilidad del sistema

En este proceso se examina un conjunto concreto de necesidades a las cuales dar solución a corto plazo, sustituyendo los criterios estratégicos del PSI por otros tácticos, estudiando las restricciones de tipo económico, técnico, legal y operativo, en aras a decidir si abandonar el proyecto o continuarlo[1010]. En el ámbito legal, se adoptarán decisiones concretas en aras de garantizar que la automatización no solo se ajusta a la normativa, sino que no produce perjuicios o reducción de garantías en los administrados, con la cautela requerida, en la medida en que la capacidad de decisión humana cede paso a la toma decisiones por la máquina.[1011]

En principio es un proceso breve y de bajo coste, orientado a ver si las necesidades pueden ser satisfechas con el sistema actual, si el propuesto será rentable, si se puede desarrollar con las limitaciones presupuestarias existentes y dentro de las fechas propuestas…[1012]. Sin embargo, no es extraña la falta de rigor en la realización del estudio[1013], lo que puede conducir a desagradables sorpresas en momentos más avanzados del desarrollo, al

[1010] MAP. Métrica V3. Introducción, 6.
[1011] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 12.
[1012] GONZÁLEZ GARCÍA, P. (2008), estudios de viabilidad.
[1013] PIATTINI VELTHIUS, M.G. (2001), auditoría de bases de datos, 315.

descubrir la falta de rentabilidad (no necesariamente económica) tras haber consumido recursos apreciables. Es preciso recordar que también se considera *software* fallido aquel que finaliza dentro del plazo y presupuesto establecidos pero nunca llega a usarse.

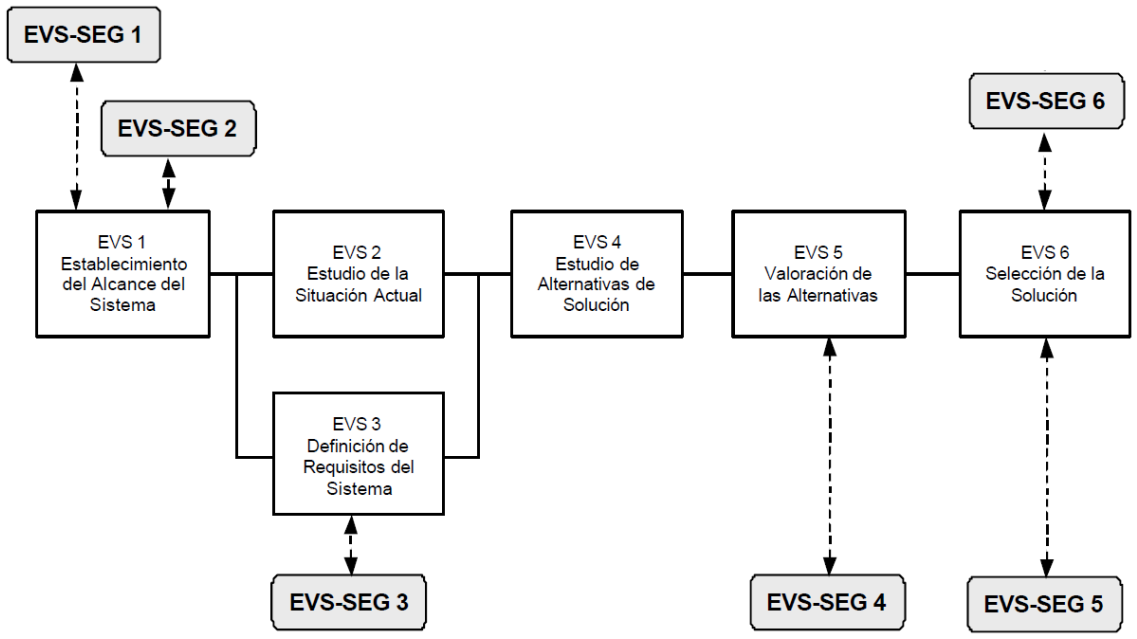

Figura 26: Actividades de EVS

Fuente: Metodología Métrica versión 3. Interfaz de seguridad, 12.

Al inicio del proceso, el responsable de seguridad, acompañado por el jefe de proyecto, analizará las necesidades de seguridad de las actividades y de los productos a elaborar en el EVS, desde los aspectos de autenticación, confidencialidad, integridad y disponibilidad. Según la naturaleza de las funciones a desempeñar y dependiendo de la criticidad y

confidencialidad de la información y de los productos a los que tendrán acceso, será necesaria una selección cuidadosa de los miembros del equipo de seguridad que va a intervenir en el proceso de desarrollo completo, selección que recae en las manos del responsable de seguridad y del comité de seguimiento[1014]. Ya se comentó en el proceso anterior, PSI, que probablemente ambos, pero con certeza el segundo, está constituido por personal propio de la Administración, por lo que sus decisiones son imputables a ella.

No basta con que la aplicación obtenida al finalizar el proyecto sea funcionalmente completa y acorde a su propósito, sino que ha de satisfacer los denominados "requisitos no funcionales"[1015], que incluyen aspectos relativos al rendimiento, accesibilidad, facilidad de mantenimiento,… los cuales no siempre se encuentran especificados formalmente, pero que constituyen propiedades inherentes al producto final, que serán percibidas y apreciadas por los usuarios[1016]. Por ello, el catálogo de requisitos abarcará ambos tipos, e incluirá las restricciones relativas a la sincronización con otros proyectos.

Se realiza el diagnóstico de la situación actual, identificando problemas, deficiencias y mejoras, teniendo en cuenta estas últimas en la definición de los requisitos funcionales y no funcionales, que se catalogan y priorizan, señalando la referencia a aquellas directrices técnicas y de gestión que resulten aplicables (normas, estándares, política de seguridad…). No debe interpretarse esto como que el EVS se ocupa de la definición de la

[1014] *Vid*. MAP. Métrica V3. Interfaz de seguridad, 13-14.
[1015] Como ya indiqué *supra*, Métrica V3 considera la seguridad como un requisito funcional, al contrario de como se venía considerando anteriormente.
[1016] BLANCO GALÁN, M. (2011), aseguramiento de calidad, 49.

política de seguridad, sino que en él se recopila y cataloga aquel conjunto de directrices que habrá que tener en cuenta al proponer una solución[1017].

El equipo de seguridad seleccionado estudiará las amenazas y vulnerabilidades que prevean posibles en función del catálogo de requisitos del sistema, recién elaborado por los analistas y el jefe de proyecto en sus sesiones de trabajo con los usuarios expertos, y anticipará el impacto previsible de su materialización. Estudiando la legislación, normas y procedimientos referentes a la seguridad que son aplicables al sistema, se completa la política de seguridad de la organización y se establecen recomendaciones en función del umbral del riesgo que se consideró aceptado o asumible[1018].

En las actividades EVS 4 (estudio de alternativas de solución) y EVS 5 (valoración de las alternativas) se describen las diferentes opciones disponibles, sopesando la adquisición de productos *software* estándar del mercado, los desarrollos a medida o la reutilización. Todas ellas se valorarán considerando el impacto tecnológico, organizativo y de operación, examinando los posibles beneficios y los costes asociados. A su vez, deben cuantificarse los recursos y plazos precisos para planificar cada alternativa. En el caso de soluciones basadas en productos, se analiza su evolución prevista, su adaptabilidad y portabilidad, los costes ocasionados por licencias, los estándares del producto y su entorno tecnológico. En el análisis coste/beneficio realizado para el estudio de la viabilidad económica,

[1017] MAP. Métrica V3. Estudio de viabilidad del sistema, 4-9.
[1018] MAP. Métrica V3. Interfaz de seguridad, 15.

se han de determinar los costes del sistema y ponderarlos no solo con los beneficios tangibles, sino también con los intangibles, buscando el modo de cuantificarlos[1019].

El equipo de seguridad estudia las alternativas de solución analizando, para cada una de ellas, el nivel de seguridad, las vulnerabilidades, los riesgos y su gestión, determinando los principales recursos del sistema (entorno, aplicaciones, información, funcionalidades de la organización, personal, etc.) y las amenazas relevantes para cada uno, así como el riesgo efectivo e intrínseco y las salvaguardas que lo minimicen[1020].

Una vez realizada la elección, el equipo de seguridad y su responsable profundizan en el estudio de la opción concreta seleccionada, continuando el trabajo ya realizado en la tarea anterior e incorporando nuevos mecanismos, si fuera preciso. Se investigan las vulnerabilidades y los riesgos, con las posibilidades para su gestión y se realiza una nueva evaluación de la seguridad de la solución propuesta[1021].

Finalmente, el responsable de seguridad, el jefe de proyecto y el comité de seguimiento estudian los productos generados durante el EVS, determinando el nivel de seguridad de cada uno con respecto a la autenticación, confidencialidad, integridad y disponibilidad, catalogando y archivándolos según ese nivel[1022].

La tarea que cierra este proceso es la EVS 6.3, denominada “aprobación de la solución”, en la que el comité de dirección da su beneplácito formal. También puede rechazarla, manifestando su inviabilidad, ya sea por motivos económicos o de funcionalidad, por incumplir

[1019] MAP. Métrica V3. Estudio de viabilidad del sistema, 10- 12.
[1020] MAP. Métrica V3. Interfaz de seguridad, 16.
[1021] MAP. Métrica V3. Interfaz de seguridad, 17-18.
[1022] *Vid* MAP. Métrica V3. Interfaz de seguridad, 18-19.

los requisitos identificados en cuanto a plazos o cobertura, etc. El mismo razonamiento empleado para el PSI me lleva a aceptar sin reparos la colaboración de empresas externas en el EVS.

Entendiendo por calidad el grado en que un conjunto de características inherentes cumple con unos requisitos[1023], durante el proceso EVS se constituye un equipo de trabajo para valorar la conveniencia de establecer un plan para su aseguramiento, determinando, para cada alternativa de solución propuesta, los sistemas de información afectados por ese plan y las propiedades que permitan evaluarla (por ejemplo, la facilidad de uso, eficiencia, seguridad, portabilidad, integridad, fiabilidad…). Ese equipo ha de ser totalmente independiente del encargado del desarrollo, para poder asumir la identificación de las posibles desviaciones de los estándares, requisitos y procedimientos, y comprobar la aplicación de las medidas preventivas o correctoras necesarias. Tras definir el alcance del plan de aseguramiento de la calidad, se establece el coste adicional que supondría materializarlo, para sumarlo al coste total del sistema y determinar su viabilidad económica. Finalmente, se registra la aprobación del plan de aseguramiento de calidad asociado a cada sistema de información que conforme la solución seleccionada, o bien el motivo de su rechazo[1024].

Precisamente es el coste adicional de materializar ese plan de calidad uno de los motivos que despierta la desconfianza ante la externalización del desarrollo del *software* de las Administraciones públicas. No puede ignorarse que las empresas de servicios se mueven por motivos económicos, por la búsqueda de la máxima rentabilidad dineraria. Pecaría de inocencia quien pensara que la empresa va a preferir incumplir plazos y arriesgarse a sufrir penalizaciones,

[1023] Definición de ISO 9000:2000.
[1024] MAP. Métrica V3. Aseguramiento de la calidad, 1-8.

a cambio de dedicar más tiempo del previsto a desarrollar una aplicación optimizando su calidad. También muestra cierta ingenuidad quien ignora el ahorro que supone para la empresa la contratación de becarios con poca o ninguna experiencia, o el escatimar recursos humanos a costa de alargar los horarios de cada trabajador implicado, en vez de dimensionar adecuadamente la plantilla asignada al proyecto. Todo ello afectará a la calidad del *software* indefectiblemente.

Antes de estudiar el proceso de análisis del sistema de información, es imprescindible detenerse a comentar las diferentes alternativas que se barajan en el EVS.

7.3.2.1. ADQUISICIÓN DE PROGRAMAS COMERCIALES

Animados por la inmediatez y el ahorro económico, son muchas las organizaciones que se deciden por adquirir productos *software* del mercado. Su adaptación a los propios requerimientos supone un esfuerzo bastante inferior al de un desarrollo a medida[1025], aunque no siempre su encaje es perfecto, pudiendo obligar a que sea el usuario el que se adapte a él, no viceversa. Su gran ventaja recae en su precio reducido, dado que el desarrollador vende el mismo *software* a muchos destinatarios, repartiendo los costes y el margen de beneficios entre todos ellos, logrando comercializar un producto muy competitivo.

El Ministerio de defensa apoya esta opción por razones de calidad, basándose en que los productos del mercado evolucionan a un ritmo que ninguna Administración pública podría mantener con desarrollos propios[1026]. Pero esta decisión ha de tomarse con las debidas

[1025] MAP. Métrica V3. Introducción, 4.
[1026] DELGADO DE LUQUE, J.G. (2008), proceso de selección.

precauciones[1027]. Dicho Ministerio elabora una lista de productos candidatos, realizando un exhaustivo estudio de mercado, teniendo en cuenta las necesidades presentes y futuras, el estado actual de las TIC y la opinión de analistas expertos como Gartner, Forrester o Meta Group. Se establecen criterios predefinidos basados en razones de índole técnica, económica y de mercado, junto con las singularidades del propio Ministerio, como la compatibilidad con sus otros sistemas. Este y otros aspectos empujan a la realización de pruebas que certifiquen su aptitud técnica y la satisfacción de los requisitos, salvo que se trate de productos que ya se encuentren ampliamente implantados, como puede ser Lotus Notes o Microsoft Office. En cuanto a las exigencias en materia de seguridad, en función de lo que indique la propia normativa, es posible exigir que estén certificados por el CCN o que alcancen un determinado nivel de certificación según los estándares de evaluación de seguridad *Common Criteria* e ITSEC.[1028]

Sin embargo, los productos *software* de mercado no están exentos de problemas ni garantizan que las vulnerabilidades que se vayan descubriendo se resuelvan a lo largo del tiempo. En ese sentido, el 12 de enero del pasado año 2016, Microsoft anunció que únicamente proporcionaría apoyo técnico y actualizaciones de seguridad para la versión más reciente de Internet Explorer disponible para cada sistema operativo compatible, por lo que IE 11 continuará recibiendo actualizaciones de seguridad, soluciones de compatibilidad y soporte técnico en Windows 7, Windows 8.1 y Windows 10. Microsoft recomienda a los clientes mantenerse al día sobre la última versión del navegador, dado que la instalación de parches de seguridad de forma regular evita que las vulnerabilidades pueden ser explotadas por el *malware*, lo que ayuda a

[1027] MAP. Métrica V3. Introducción, 4.
[1028] DELGADO DE LUQUE, J.G. (2008), proceso de selección, 51-52.

mantener la seguridad[1029]. En situaciones como las descritas, la Administración puede verse obliga a escoger entre migrar a versiones más avanzadas o mantener las existentes sin disponer ya de soporte técnico.

Los productos *software* existentes en el mercado, incluso los de mayor difusión, tampoco están exentos de riesgos. El CCN ha elaborado distintas series de documentos para apoyar al personal de la Administración en la tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad. La serie 500 incluye 49 guías, en las que establece las configuraciones mínimas de seguridad de los diferentes elementos basados en la tecnología Windows[1030]. A modo de ejemplo, la guía "CCN-STIC-529 Seguridad en Microsoft Office 2013" consta de 327 páginas dedicadas a proporcionar información sobre los procedimientos para su implantación y garantizar la seguridad del sistema mediante el tratamiento de archivos ofimáticos utilizados por Office 2013.[1031]

El aspecto probablemente más problemático a la hora de sujetarse a un producto *software* existente en el mercado es la dificultad o, incluso, imposibilidad de diferenciación y adaptación a las propias necesidades y de interconexión con otros sistemas. Normalmente son productos cerrados, o con pocas posibilidades de parametrización (aunque estas posibilidades y, con ello, su flexibilidad, aumentan si el paquete utiliza SOA[1032]). A modo de ejemplo, podemos referir aplicaciones comerciales funcionalmente muy útiles para la gestión de datos

[1029] Descargado de https://www.microsoft.com/en-us/WindowsForBusiness/End-of-IE-support (25 de agosto de 2016).
[1030] Descargado de https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/500-guias-de-entornos-windows.html (26 de agosto de 2016).
[1031] Descargado de https://www.ccn-cert.cni.es/series-ccn-stic/500-guias-de-entornos-windows/821-ccn-stic-529-seguridad-en-microsoft-office-2013/file.html (26 de agosto de 2016).
[1032] ACCENTURE – CENTRO DE ALTO RENDIMIENTO (2008), arquitectura orientada a servicios, 13.

especialmente protegidos, como los referidos a la salud, que adolecen de las medidas básicas de seguridad, al permitir la existencia de credenciales del tipo usuario igual a ”1234” con contraseña “1234”, como se analizó *supra*, que no se bloquean tras un número determinado de accesos fallidos y que ni siquiera incorporan un CAPTCHA para evitar el descubrimiento de las credenciales correctas utilizando un programa automatizado que prueba todas las posibles combinaciones. La solución a estas deficiencias sería sencillísima en un *software* realizado a medida, pero puede ser imposible si se adquiere una aplicación comercial que, como ocurre con cierta asiduidad, no admite modificaciones.

7.3.2.2. DESARROLLO POR LOS USUARIOS FINALES

La elaboración de pequeños sistemas de información desarrollados por los propios usuarios finales ha proliferado alarmantemente en los últimos tiempos, como respuesta ante la carencia de aplicaciones asequibles que respondieran a sus necesidades. Su obtención ha sido fruto de la motivación, audacia y esfuerzo de los propios empleados públicos no especializados en las TIC. Sin duda, presentan la ventaja de proporcionar un mayor control por parte de los usuarios, acompañado de su inmediatez y un elevado ahorro en costes. Su número puede medirse, como mínimo, en centenas, en prácticamente cualquier Administración de tamaño medio o grande. Han sido desarrolladas con gestores de bases de datos como Access u hojas de cálculo como Excel, y se han vuelto imprescindibles en el quehacer diario. Entre los aspectos negativos de esta solución cabe destacar la baja calidad que puede caracterizarlos y el efecto “isla” que se produce al disponer de múltiples sistemas de información aislados, sin ninguna

conexión entre ellos[1033]. Sin embargo, a pesar del incumplimiento de los mínimos requisitos de seguridad exigidos por el ENS, su sustitución masiva, al menos en un tiempo medianamente próximo, choca frontalmente con las limitaciones presupuestarias públicas, lo que deja a la Administración en la difícil tesitura de escoger si proporciona el servicio público al que está constitucionalmente obligada y que constituye su razón de ser, o si incumple abiertamente las más mínimas exigencias impuestas por el ENS. Parece razonable que se decante por la segunda opción, habida cuenta de que las obligaciones implantadas por el legislador en materia de seguridad informática y de Administración electrónica, han olvidado acompañarse de la adecuada previsión presupuestaria que puede hacerlas realidad.

7.3.2.3. DESARROLLO DE *SOFTWARE* A MEDIDA

Detectada la imposibilidad de satisfacer la totalidad de los requerimientos del usuario con un producto *software* comercial, previamente existente en el mercado, debe plantearse la necesidad de recurrir a la construcción del aplicativo a medida. Resulta sencillo deducir las ventajas e inconvenientes de esta modalidad de desarrollo, por oposición a las debilidades y a los puntos fuertes de las opciones anteriores. Al igual que un traje confeccionado a medida, se prevé su ajuste perfecto a las necesidades de la organización, entre las que se incluye la cobertura total de los requerimientos, la compatibilidad e interconexión con otros sistemas, una flexibilidad y facilidad de uso adaptadas a nuestros gustos, la solución para problemas detectados en el pasado, etc. Mientras esta lista de necesidades a cubrir va creciendo, paralelamente podemos imaginar cómo va subiendo el coste del proyecto. La satisfacción, la

[1033] HERNÁNDEZ TRASOBARES, A. (2003), evolución y desarrollo, 159-160.

calidad y el coste económico se mueven en la misma dirección, al menos teóricamente, porque, en la vida real, no es infrecuente encontrar proyectos caros bastante pobres en calidad que dejan a los usuarios manifiestamente insatisfechos.

Los desarrollos a medida pueden ser realizados por personal propio, por un equipo mixto formado por empleados públicos y por personal externo, o exclusivamente por empresas de servicios.

7.3.2.3.1. POR PERSONAL PROPIO

Por distintas razones que se tratarán *infra*, es esta la opción que defiendo como más recomendable para el desarrollo del *software* de las Administraciones públicas, refiriéndome no a los programas ofimáticos del tipo hoja de cálculo o procesador de textos, sino a aquellos que dotan de vida al "empleado público electrónico". Esta posibilidad requiere contar con una infraestructura informática adecuada y con unos medios humanos propios, especialistas en este campo[1034]. Por ello, las dificultades técnicas y personales por las que pasan las numerosas Entidades locales más pequeñas[1035] les impedirían la extensión de la Administración electrónica si no dispusiesen de otras alternativas[1036].

A la hora de dotarse del personal propio necesario, es difícil negar la costumbre de las Administraciones públicas de proceder a la cobertura temporal de vacantes de sus RPTs

[1034] HERNÁNDEZ TRASOBARES, A. (2003), evolución y desarrollo, 159-160.
[1035] SAN MARTÍN VILLAS, C./ TRICAS LAMANA, F./ MARTÍN FERNÁNDEZ, J./ GARCÍA FRANCÉS, V., creación de comunidades de usuarios, 5.
[1036] En previsión de que ciertos municipios puedan no estar en condiciones de asumir tal obligación, el artículo 36.1.g de la ley 7/1985, de 2 de abril, reguladora delas bases del Régimen Local, confiere a la Diputación o entidad equivalente la competencia sobre la prestación de los servicios de Administración electrónica en los municipios con población inferior a 20.000 habitantes. Esta redacción, introducida por el artículo 1.13 de la ley 27/2013, ha sido considerada constitucional por la STC 111/2016.

mediante la contratación de personal interino, unos 300.000, lo que supone un 11% del personal[1037]. Tampoco se puede rebatir la tendencia a mantener esa situación durante años, ignorando el principio de causalidad, entendido este como la debida concurrencia de una necesidad de tipo productivo u organizativo que justifique la celebración de un contrato de duración determinada. La ausencia de dicho presupuesto legitimador pone de manifiesto el encubrimiento de una relación que debería ser indefinida[1038]. La concreción del plazo máximo que limita esa relación de temporalidad nos viene indicado por el Estatuto básico del empleado público, actual TREBEP, donde su artículo 70.1 obliga a convocar el correspondiente proceso selectivo o instrumento similar dentro del plazo improrrogable de tres años, lo que determina, *ope legis*, el plazo máximo para la cobertura de las vacantes de las Administraciones públicas. Por tanto, de conformidad con el artículo 8.2 del real decreto 2720/1998, de 18 de diciembre, por el que se desarrolla el artículo 15 del estatuto de los trabajadores en materia de contratos de duración determinada, expirada dicha duración máxima sin denuncia expresa, si el trabajador continuara prestando sus servicios, el contrato se considerará prorrogado tácitamente por tiempo indefinido, transformándose en uno de naturaleza diferente, en un contrato indefinido no fijo[1039], como consecuencia del incumplimiento del plazo para cubrir reglamentariamente la plaza en cuestión. Esta operación jurídica provoca una novación del negocio ilícito en un contrato lícito

[1037] http://www.lasexta.com/noticias/economia/los-300000-interinos-de-espana-esperanzados-con-la-senten cia-de-la-ue-ahora-te-despiden-y-te-quedas-en-las-mismas_2016092057e132600cf2b0b9c5a8e00b.html (26 de septiembre de 2016).

[1038] RODRÍGUEZ ESCANCIANO, S. (2010), indefinido no fijo, 34.

[1039] El artículo 11.1 del TREBEP clasifica los contratos del personal laboral en fijos, indefinidos y temporales, siendo la primera vez que se contempla esa triple clasificación en una norma con rango de ley, como señala RODRÍGUEZ ESCANCIANO.

sujeto a condición resolutoria[1040]. Antes de alcanzar esos tres años, el contrato seguirá siendo de interinidad por vacante y podrá extinguirse según las normas aplicables, salvo que se acredite la atribución fraudulenta de vacantes diferentes al trabajador de manera artificiosa, con la intención de superar ese tiempo máximo; después el contrato se convertirá en indefinido y habrá de seguir su regulación específica (STS, sala de lo social, 3425/2014, de 20 de mayo). En el mismo sentido podemos citar la STSJ de Galicia, sala de lo social, 1572/2016, de 11 de marzo.

Ahora bien, a pesar de que la doctrina del Tribunal Supremo mantiene que "*la consecución arbitraria y desmedida de vínculos temporales implica un juicio permanente y favorable a la existencia de mérito y capacidad capaz de suplir la falta de pruebas selectivas*", ese nuevo personal de la Administración, declarado indefinido no fijo por sentencia judicial, no puede adquirir fijeza por vulnerar las reglas imperativas llamadas a garantizar a los principios de igualdad y publicidad en el acceso a la función pública[1041], debiendo el organismo afectado adoptar las medidas necesarias para proceder a la provisión regular de dicho puesto de trabajo y, con ello, a la extinción del vínculo laboral anterior[1042]. Sin embargo, a pesar de que el contrato de interinidad por vacante estaba ligado a una plaza determinada, el trabajador judicialmente convertido en indefinido no fijo ya no está adscrito a un destino específico, por lo que no basta la cobertura reglamentaria de una vacante similar para extinguir el vínculo laboral. Para esa extinción será preciso acreditar la correspondencia entre la vacante ofertada y la que ocupa el

[1040] RODRÍGUEZ ESCANCIANO, S. (2012), políticas de ajuste, 19.
[1041] RODRÍGUEZ ESCANCIANO, S. (2012), políticas de ajuste, 17.
[1042] El rechazo de la posibilidad de que la Administración declare, en virtud de sus poderes de autotutela, la condición de indefinido no fijo de su personal laboral, es objeto del trabajo de CASTILLO BLANCO, F. (4 de mayo de 2016) en http://www.acalsl.com/blog/2016/05/pueden-los-ayuntamientos-declarar-al-personal-laboral-en-la-condicion-de-indefinido-no-fijo (descargado el 21 de marzo de 2017).

trabajador o, dada la posibilidad de movilidad funcional, que no existe ninguna otra vacante ocupada con trabajador de mejor derecho (habría que tener en cuenta las mismas consideraciones en caso de amortización de la plaza).[1043]

Recientemente se ha pronunciado el TJUE en el mismo sentido, concretando que la utilización de nombramientos de duración determinada sucesivos para atender necesidades permanentes es contraria al Derecho de la Unión[1044].

Sin embargo, a pesar de la necesidad de personal, las plantillas funcionariales han reflejado también los efectos de la crisis prolongada que venimos sufriendo, lo que ha afectado a la disponibilidad del personal técnico necesario para acometer con éxito los múltiples proyectos desencadenados con la implantación de la Administración electrónica, situación acentuada por la entrada en vigor de las nuevas leyes 39/2015 y 40/2015.

7.3.2.3.2. POR UN EQUIPO MIXTO

La escasez de personal técnico llevó durante largos años a la opción mixta, que llevó a colaborar a profesionales externos con el propio personal del departamento de informática de la organización. Se ha descrito *supra* la situación de la GISS a modo de ejemplo, extrapolable a las diversas Administraciones públicas y habitual en el trabajo informático durante décadas. En general, el personal externo ha venido prestando sus servicios en las mismas dependencias administrativas que los empleados públicos, de forma tal que las diferencias entre ambos se difuminaban a los ojos de un observador, compartiendo con cierta frecuencia

[1043] RODRÍGUEZ ESCANCIANO, S. (2010), indefinido no fijo, 36-41.
[1044] *Vid.* Sentencia en el asunto C-16/15, http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62015CJ0016&from=ES

instalaciones, material, horario, formación, instrucciones… Tampoco resulta extraña la utilización de sistemas dinámicos de contratación de servicios, conformes al tenor del artículo 199 del TRLCSP, por los que se homologa a una o varias empresas, durante un máximo de cuatro años, para proporcionar determinados "tipos" de trabajadores. A modo de ejemplo[1045], podría contratarse así el trabajo de programadores J2EE con una experiencia mínima de tres años a determinado precio máximo por hora, analistas Natural/ADABAS con una experiencia mínima de cinco años al precio máximo por jornada establecido en la "homologación de tipos", etc.

Si bien es cierto que el artículo 301.4 del TRLCSP excluye cualquier posibilidad de que el empleado de una empresa de servicios, al término del contrato de esta con la Administración, se consolide como empleado público por el simple hecho de haber prestado esos servicios, no resulta aplicable a contratos administrativos que encubran relaciones laborales[1046].

Esta colaboración entre el personal TIC de la Administración y los trabajadores de empresas del sector privado, que durante años se ha desarrollado con asiduidad, puede incurrir en una cesión ilegal de trabajadores contemplada por el artículo 43 del ET, que podría obligar a los tribunales a declarar la condición del trabajador como laboral indefinido no fijo al servicio de la Administración infractora, como concluye la STSJ de Cataluña 4679/2013, sala de lo social, de 30 de abril de 2013, para el caso concreto de un analista programador que prestó servicios para la

[1045] El entonces Director general de desarrollo e innovación tecnológica de la Consejería de industria, trabajo y desarrollo tecnológico de la Comunidad autónoma de Cantabria, Pablo de Castro, destacaba en 2005 entre los concursos públicos más importantes a adjudicar el correspondiente a la homologación de tipos para las tareas de mantenimiento y el desarrollo informático de los sistemas de información del Gobierno de Cantabria, como se publica en el reportaje de C. Sánchez titulado "Auge de concursos públicos en el área de las TIC (1)", publicado en *SOCINFO, Sociedad de la información* (19), 36-37. Ejemplos concretos de ejecución de contratos basados en dicha homologación de tipos pueden consultarse en las páginas 2040 y 2041 de las cuentas anuales de 2006 de la Comunidad autónoma de Cantabria, descargadas de http://cantabria.es/documents/16876/1676728/TOMO+VI.pdf (31 de agosto de 2016).

[1046] RECUERDA GIRELA, M.Á. Y FERNÁNDEZ DEPUECH, L. (2013), contratos administrativos.

empresa pública *Televisió de Catalunya, S.A.* dependiente de la entidad pública *Corporació Catalana de Mitjans Audiovisuals*. La sentencia recoge la evolución jurisprudencial por la que el Tribunal Supremo ha pasado a exigir, para que no se incurra en cesión ilegal, no solo la existencia real y efectiva de la empresa cedente, sino también que esta comprometa sus medios personales, materiales y organizativos, evitando así fenómenos de mera interposición, aclarando en referencia al contratista que "*existe cesión ilegal de trabajadores cuando la aportación de este en un supuesto contractual determinado se limita a suministrar la mano de obra sin poner a contribución los elementos personales y materiales que conforman su estructura empresarial*" (STS 7630/1997), añadiendo algunos indicios que refuerzan la sospecha de ilegalidad, como que el empresario carezca de facultades y poderes sobre sus propios medios patrimoniales, la no asunción de los riesgos propios del negocio, o el tener fuertemente limitada la capacidad de dirección y selección del personal. En cualquier caso, es preciso examinar las circunstancias concretas de cada supuesto, razón que justifica el manifiesto casuismo de los pronunciamientos judiciales en la materia.

En previsión de posibles demandas, el legislador, en la disposición adicional primera del real decreto 20/2012, de 13 de julio, de medidas para garantizar la estabilidad presupuestaria y de fomento de la competitividad, en su primer párrafo, obligó al sector público a dictar instrucciones para evitar esta problemática entes de finalizar ese mismo año. Esta previsión, probablemente pensada para las contratas de obras o servicios, resulta extrapolable también a aquellos casos en que se recurra a servicios de las ETT[1047].

[1047] NORES TORRES, L.E. (2014), empleo público.

En las instrucciones elaboradas por la Junta de Andalucía podemos leer que "(…) *no deben concebirse como contrataciones destinadas a integrar personal en los equipos de trabajo de personal propio* (…)", algo que claramente impide la contratación a través de la homologación de tipos descrita *supra*.

El Tribunal de Cuentas ya había tomado conciencia de la problemática unos años antes, elevando en 2010 una interesantísima moción a las Cortes generales sobre la necesidad de evitar el riesgo de que los trabajadores de empresas de servicios contratadas por la Administración se conviertan en personal laboral por sentencia judicial[1048], lo que llevó a la adopción de la resolución de 27 de octubre de 2010, por la que se insta a las Administraciones públicas a limitar la contratación de servicios externos únicamente cuando esté plenamente justificado, que se determine previamente las funciones y servicios externalizables a fin de evitar su uso para suplir la falta de personal, que se valoren todas las circunstancias concurrentes en cada solicitud de modificación de las RPT, que se detalle con mayor precisión el objeto del contrato en los pliegos de prescripciones y se vigile el ajuste a los mismos, que se eviten los actos que pudieran considerarse determinantes para el reconocimiento de una relación laboral y, finalmente, que las adscripciones a puestos de trabajo debidas a sentencias judiciales no se consideren una adscripción definitiva al puesto, sino que desemboquen en su amortización o en su provisión con respeto a los principios constitucionales de publicidad, igualdad, mérito y capacidad[1049].

[1048] MINHAP (2012), buenas prácticas.
[1049] *Vid.* BOE de 18 de enero de 2011, 5982 y ss, donde puede encontrarse no solo la resolución, sino también la moción presentada.

Dado el interés del contenido de la moción del Tribunal de Cuentas, que denuncia con claridad una situación conocida y, a la vez, ignorada por todos, es imprescindible hacer mención a alguno de sus puntos más destacados, vistos desde la óptica informática del problema. La primera que llama la atención es una matización obvia pero que puede pasar desapercibida, que señala que el peligro ha existido, aunque no se haya llegado a plantear la oportuna reclamación judicial. A juzgar por lo observado en diferentes Administraciones públicas, tanto del lado del sector público como del privado, se trata de una situación generalizada que en contadas ocasiones llega a los tribunales, a veces por la juventud de los afectados, por su inestabilidad laboral, por el miedo a iniciar un pleito difícil de ganar, por la posible adopción de medidas de represalia,… En esencia, por tener poco que ganar y mucho que perder.

También señala el Tribunal de Cuentas en la moción presentada que "*la falta de personal se suplió con la contratación externa de empresas de servicios, en lugar de recurrirse a una ampliación de la Relación de Puestos de Trabajo y a la subsiguiente selección de personal, mediante convocatoria pública y a través del sistema de concurso, oposición o concurso-oposición previsto legalmente*". Este es un problema que, más allá de los aspectos legales que conlleva, desencadenó una fuerte desmotivación en el personal TIC al servicio de las Administraciones públicas, quienes, tras superar una o incluso varias oposiciones informáticas no exentas de dificultad, miran al presente y al futuro desesperanzados, observando cómo las RPTs informáticas se abandonan, cómo las funciones que en ellas se especifican progresivamente van pasando a manos privadas, cómo la que habían escogido como opción profesional cada vez se parece menos a su realidad laboral diaria, viéndose ellos mismos

relegados a la figura de intermediario, de mero "reenviador" de correos electrónicos, de "florero" o, incluso, a los ojos desinformados de la opinión pública, de "vago funcionario que debería ser despedido". Algunos logramos emigrar a otros campos de la Administración; otros se resignan en los servicios informáticos, desilusionados. Con relación a estos últimos, la mayoría, habría que recordar aquí la íntima relación entre motivación y resultados, expuesta *supra*.

Se ha comentado con anterioridad la situación de los informáticos en la seguridad social. A ese respecto, la moción del Tribunal de Cuentas indica que "*la Comisión Mixta para las Relaciones con el Tribunal de Cuentas, a la vista del Informe, recomendó a los Ministerios de Trabajo y Asuntos Sociales y de Sanidad y Consumo incrementar sus plantillas de personal con cualificación informática y limitar la contratación externa*". Esta es la auténtica solución al problema y, curiosamente, es la que no se está adoptado.

Finalmente, cabe destacar en esta moción su comentario sobre la patente discordancia apreciada entre el ordenamiento laboral y el administrativo en referencia a la cesión ilegal de trabajadores. Si bien el ET prevé la adquisición de la condición de fijo por el trabajador cedido, su materialización en el seno de la Administración pública, en calidad de empleador, choca frontalmente con los principios constitucionales que disciplinan el acceso al empleo público. El ordenamiento laboral responde al carácter tuitivo de los derechos del trabajador, mientras que el administrativo "*se orienta primordialmente a satisfacer los intereses generales y garantizar la posición jurídica del ciudadano, en cuanto tal*". Esa contradicción, aparentemente inconciliable, debe resolverse mediante una interpretación integradora de mano de los tribunales de Justicia, sentando la jurisprudencia consolidada relatada *supra*.

A raíz de esta moción y de la resolución consiguiente, la Administración fijó tres principios de actuación[1050]:

a) Evitar la contratación externa para suplir las necesidades permanentes de personal y, en el supuesto de contratar, aportar certificación de la falta de medios personales propios para la realización de las mismas tareas.

b) Establecer con precisión en los pliegos las prestaciones a realizar, perfectamente deslindadas de la actividad desarrollada por el propio personal de la entidad contratante, y vigilar el estricto cumplimiento de lo especificado en el contrato, con especial interés en los plazos.

c) Evitación de cualquier acto que pueda interpretarse judicialmente como indicio de cesión ilegal, en especial la impartición de órdenes o instrucciones directas al personal de la empresa contratada por parte de los responsables de la gestión de los servicios para los cuales se recurre a esa contratación externa.

En el mismo documento se recoge un conjunto de buenas prácticas en la fase de formalización de los contratos, de las que una en concreto repercute profundamente en el ámbito informático. Se trata de la necesidad de indicar en los pliegos la obligación del adjudicatario de consignar al menos un coordinador técnico o responsable, perteneciente a la plantilla del contratista, que actuará como interlocutor y única persona con la que se relacionará la entidad contratante. Este interlocutor ejercerá la dirección del proyecto e impartirá directamente las órdenes e instrucciones de trabajo al resto del equipo del contratista. En la fase de ejecución, cualquier comunicación del personal de la empresa con los responsables de las entidades

[1050] MINHAP (2012), buenas prácticas, 3-4.

públicas se realizará a su través. El coordinador también será el encargado de comunicar a la Administración cualquier baja en el equipo, a los efectos oportunos, como la inhabilitación de sus credenciales de acceso y resto de medidas que correspondan[1051].

Además de contemplar la existencia de dicho coordinador, la Junta consultiva de contratación administrativa de la Comunidad autónoma de Aragón recomienda establecer, con carácter obligatorio, la designación de la figura del responsable del contrato, facultativa a tenor del TRLCSP, en aquellos que supongan un especial riesgo de que los trabajadores del contratante puedan invadir la esfera de dirección que corresponde al contratista respecto de su personal. El responsable del contrato sería el instrumento a través del cual transmitir todas las comunicaciones e instrucciones que la entidad contratante deba hacer llegar a la contratista[1052].

Tras la situación descrita, parece claro concluir que la opción de desarrollo del *software* para las Administraciones públicas de forma colaborativa entre personal TIC funcionario y personal de empresas de servicios externas, parece estar llegando a su punto final, no por obtención de malos resultados técnicos, sino por el riesgo que supone de cara a posibilitar situaciones susceptibles de encubrir una cesión ilegal de trabajadores. Como resultado, esta forma de trabajar podría evolucionar en dos direcciones, la del desarrollo propio por los empleados públicos, descrita *supra*, y la del desarrollo mediante contratos de servicios, que comento a continuación.

7.3.2.3.3. POR EMPRESAS DE SERVICIOS

[1051] MINHAP (2012), buenas prácticas, 4-5.
[1052] JUNTA CONSULTIVA DE CONTRATACIÓN ADMINISTRATIVA DE LA COMUNIDAD AUTÓNOMA DE ARAGÓN (2013), recomendación 1/2013, 7.

Esta opción ha sido tradicionalmente la escogida en el caso de que la organización no disponga de recursos internos adecuados para afrontar ese esfuerzo de desarrollo, viéndose abocada a contratar la realización de los trabajos a personal externo[1053]. Las restricciones a la incorporación de nuevos empleados públicos en las leyes de presupuestos de los últimos años ha dificultado la disponibilidad de esos recursos necesarios. Si bien para 2016 ya se ha eliminado esa prohibición, son muchas las diferentes áreas con necesidades acuciantes de personal, por lo que no puede presuponerse que ese personal de nuevo acceso vaya a resolver las necesidades informáticas, más bien es de esperar una tendencia a la continuidad en la situación anterior, la de la externalización de los servicios de nuevos desarrollos y de mantenimiento del *software*.

Si bien podemos considerar que la incorporación de trabajadores externos dentro de los equipos de empleados públicos puede darse, en general, por finalizada, el desarrollo del nuevo *software* y su mantenimiento por empresas externas no está exento de los mismos problemas. Es preciso ser extremadamente cuidadoso y seguir con esmero las instrucciones dadas por las diferentes Administraciones públicas para evitar futuras demandas judiciales por cesión ilegal de trabajadores. Sin embargo, la aplicación de dichas instrucciones, a mi entender, incrementa notablemente el riesgo de que las aplicaciones desarrolladas incumplan los plazos comprometidos, no satisfagan las necesidades de los usuarios y presenten carencias de seguridad, en sus distintas dimensiones de autenticación, confidencialidad, integridad, disponibilidad y trazabilidad.

[1053] SAN MARTÍN VILLAS, C./ TRICAS LAMANA, F./ MARTÍN FERNÁNDEZ, J./ GARCÍA FRANCÉS, V., creación de comunidades de usuarios, 5.

El primer motivo que me lleva a realizar estas afirmaciones parte de una obviedad: los desarrolladores de la empresa externa no están integrados en la estructura administrativa, lo que disminuye drásticamente la comprensión de las necesidades mutuas. Desarrolladores y usuarios permanecen separados. Dos grupos de personas que tradicionalmente "hablan distintos idiomas" ya no comparten siquiera la Torre de Babel; han levantado un muro que mantiene aislados a los unos de los otros. Posteriormente, al tratar cada una de las tareas a realizar por informáticos y usuarios conforme dispone Métrica V3, incidiré en esta cuestión.

Sin embargo, las dificultades no se limitan a la separación espacial. Si la lejanía fuera un problema insuperable, las factorías de programación localizadas en India no hubieran alcanzado el nivel de competitividad y el volumen de negocio logrado. El segundo motivo de preocupación es la obligación del adjudicatario de consignar a un interlocutor para relacionarse con la entidad contratante, dirigir el proyecto e impartir directamente las órdenes e instrucciones de trabajo al resto del equipo de la empresa externa. Es decir, el equipo de desarrollo no solo está separado de los usuarios, sino que también está incomunicado. Un analista o un programador no puede plantear sus dudas a los usuarios; un usuario no puede explicar nada a los analistas ni a los programadores. Toda comunicación ha de realizarse a través de una única persona de la empresa.

El éxito del proyecto se dificulta aún más cuando la Administración contratante toma la misma determinación, designando a un responsable del contrato y limitando el contacto con la empresa a su través. Con frecuencia la elección recae en un informático de la Administración para que actúe como único interlocutor con la empresa externa, de modo que, al cabo de poco tiempo, las tareas del funcionario TIC se han convertido en el reenvío de correos de

los usuarios al interlocutor de la empresa, así como el redireccionamiento hacia los usuarios de los *e-mails* recibidos de dicho interlocutor, a quien le han llegado de los analistas y programadores. En la transmisión y retransmisión de la información, esta sufre distorsiones y retrasos. Nunca habían sido tan ciertas como ahora las palabras de Pressman, "(…) *es frecuente que el camino que lleva de la comunicación a la comprensión esté lleno de agujeros*"[1054]. A modo de ejemplo, propongo la lectura de un diálogo típico de esta situación:

PROGRAMADOR al RESPONSABLE EXTERNO:

Acabé. Ya lo puede probar.

RESPONSABLE EXTERNO al RESPONSABLE FUNCIONARIO:

Acabó. Ya lo puede probar.

RESPONSABLE FUNCIONARIO al USUARIO:

Dicen que ya lo puedes probar.

USUARIO a RESPONSABLE FUNCIONARIO:

Sale mal. Hay un descuadre de 15,83 €.

RESPONSABLE FUNCIONARIO a RESPONSABLE EXTERNO:

Dice que sale mal, que hay un descuadre de 15,83 €.

RESPONSABLE EXTERNO a PROGRAMADOR:

Que dice que sale mal, que hay un descuadre de 15,38 €.

PROGRAMADOR al RESPONSABLE EXTERNO:

¿Un descuadre? ¿En dónde?

RESPONSABLE EXTERNO al RESPONSABLE FUNCIONARIO:

El programador pregunta que en dónde.

RESPONSABLE FUNCIONARIO al USUARIO:

Que en dónde…

USUARIO a RESPONSABLE FUNCIONARIO:

En la columna del importe líquido.

[1054] PRESSMAN, R.S. (2010), ingeniería del *software*. Un enfoque práctico, 86.

RESPONSABLE FUNCIONARIO a RESPONSABLE EXTERNO:

Que en la columna del importe líquido.

RESPONSABLE EXTERNO a PROGRAMADOR:

En la columna del importe líquido.

PROGRAMADOR al RESPONSABLE EXTERNO:

¿Qué datos está metiendo?

RESPONSABLE EXTERNO al RESPONSABLE FUNCIONARIO:

Que qué datos está metiendo…

RESPONSABLE FUNCIONARIO al USUARIO:

Que qué datos estás metiendo…

USUARIO a RESPONSABLE FUNCIONARIO:

Año 2016, mes 06, consejería 05.

RESPONSABLE FUNCIONARIO a RESPONSABLE EXTERNO:

Año 2006, mes 16, consejería 05.

RESPONSABLE EXTERNO a PROGRAMADOR:

Año 2006, mes 16, consejería 05.

PROGRAMADOR al RESPONSABLE EXTERNO:

¿Mes 16?

RESPONSABLE EXTERNO al RESPONSABLE FUNCIONARIO:

¿Cómo que mes 16?

RESPONSABLE FUNCIONARIO a RESPONSABLE EXTERNO:

No, mes 06.

RESPONSABLE EXTERNO a PROGRAMADOR:

Que no, que mes 06…

Podrán intercambiarse muchos correos electrónicos más y derrochar grandes dosis de tiempo, de paciencia y de cordura, antes de que alguien se dé cuenta de que también se han equivocado de año. Y pasarán bastantes horas antes de que se logre averiguar dónde falla el

programa, suponiendo que realmente falle, pues podría ocurrir que el usuario hubiera calculado mal el importe que esperaba encontrar y que el programa funcionase bien, en cuyo caso la empresa se negará a asumir las consecuencias del retraso en el plazo de entrega, ante lo cual la Administración sacará a relucir otros ejemplos en los que el error lo cometió la empresa. Como resultado, el plazo simplemente se incumplirá, sin que nadie se responsabilice de ello, no pudiendo aplicar las previsiones del artículo 212 del TRLCSP si no se prueba que las causas de la demora son imputables al contratista.

No será extraño que ese intercambio de correos entre los intermediarios de la empresa externa y de la Administración degenere y acabe limitándose a un simple reenvío de los correos del usuario y del programador, algo que, al menos, evitaría los errores involuntarios en la transmisión. Tampoco sería sorprendente que, tras cierto tiempo, los dos intermediarios acabaran desapareciendo de la conversación, contactando directamente programador y usuario, incumpliendo las instrucciones dictadas con la intención de evitar el riesgo de demandas por cesión ilegal de trabajadores. A tal efecto, es preciso recordar que la inobservancia de dichas instrucciones podría dar lugar a la exigencia de las oportunas responsabilidades disciplinarias de los empleados públicos infractores[1055].

Incluso antes de que se tomasen todas estas prevenciones para evitar la cesión ilegal de trabajadores, antes de apreciar todos los efectos negativos que repercutían en el propio *software*, la metodología Métrica V3 ya alertaba de los peligros de la contratación con empresas de servicios, señalando que es una práctica cada vez más habitual que requiere una buena gestión

[1055] MINHAP (2012), buenas prácticas, 7.

y un adecuado control de dichos servicios externos, así como "*del riesgo implícito en todo ello*", para que sus resultados supongan un beneficio.[1056]

La contratación de empresas externas para desarrollar el *software* de las Administraciones públicas protagonizará el siguiente capítulo de este trabajo, por lo que me limitaré a señalar aquí el beneficio potencial que se podría obtener por el aprovechamiento de economías de escala por parte del proveedor, el final de la incertidumbre en los costes y una adaptación a las necesidades de las empresas más adecuada que en la adquisición de productos *software* disponibles en el mercado. A su vez, entre los aspectos negativos de esta elección, cabe destacar la pérdida de control y el riesgo a que surja una dependencia del proveedor[1057].

7.3.2.3.4. POR CONTRATACIÓN DOMÉSTICA

Son habituales los casos en que organismos administrativos o entidades de Derecho público encargan a otros órganos o entidades de la misma o distinta Administración la realización de actividades de carácter material o técnico de su competencia, por razones de eficacia o por no poseer los medios técnicos idóneos para su desempeño, transfiriendo así el ejercicio material de una potestad sin ceder la titularidad de la competencia[1058] aunque, como señala Cantero Martínez, la conocida como contratación doméstica, encomienda de gestión o utilización de medios propios, no puede considerarse como un supuesto de externalización,

[1056] MAP. Métrica V3. Introducción, 4.
[1057] HERNÁNDEZ TRASOBARES, A. (2003), evolución y desarrollo, 159.
[1058] A título de ejemplo, puede verse en el BOC de 30 de diciembre de 2009 la resolución por la que se dispone la publicación del convenio por el que se formaliza la encomienda de gestión del Gobierno de Cantabria a la ahora ya extinta Empresa cántabra para el desarrollo de las nuevas tecnologías en la Administración, S.L. (EMCANTA, S.L.), para ejecución de la actuación denominada "Implantación de la plataforma de Administración electrónica del Gobierno de Cantabria".

habida cuenta de que no se transfiere el ejercicio de funciones administrativas a ningún sujeto privado[1059]. El Tribunal de Cuentas lo describe como una forma de colaboración inter e intra administrativa, de perfiles difusos, situada a caballo entre la actuación directa por parte de la Administración y la contratación externa[1060].

El crecimiento del Derecho de la competencia, de las reglas que buscan su garantía en el mercado libre, ha llevado a cuestionar si las Administraciones públicas pueden recurrir libremente a sus entes instrumentales o deben ajustarse a las normas defensoras de la competencia como cualquier particular. La generalizada imposición del sometimiento de los contratos públicos a pública concurrencia competitiva llevó múltiples conflictos ante el Tribunal de Justicia, el cual, no sin incidir en ciertas contradicciones e incoherencias, se esfuerza por precisar el concepto de contrato *in house* o contrato doméstico con sucesivas precisiones.[1061]

Regulada ahora en el artículo 11 de la ley 40/2015, para el sector público estatal, su artículo 86 recoge algunas prescripciones aplicables[1062]. Esta figura jurídica, conocida también como *in house providing*, que descansa sobre los artículos 4 y 24 del TRLCSP, constituye una excepción a la necesidad de licitación pública, lo que supone un riesgo de abuso con la intención de huir del Derecho administrativo, pues la ejecución del encargo ha de llevarse a cabo conforme a la naturaleza del encomendatario, no del encomendante, facilitando así la elusión de los principios de publicidad, concurrencia, transparencia y no discriminación,

[1059] CANTERO MARTÍNEZ, J. (2011), la sustitución, 4.
[1060] TRIBUNAL DE CUENTAS (2016). Nº 1197. Informe de fiscalización sobre la utilización de la encomienda de gestión, 13.
[1061] *Vid*. SOSA WAGNER, F./ FUERTES LÓPEZ, M. (2007), ¿pueden los contratos quedar en casa?, 1669-1680.
[1062] LOZANO CUTANDA, B./ FERNÁNDEZ PUYOL, I. (2016), contratación *in-house*.

pudiendo incluso encarecer los productos servicios entregados[1063]. Sin perjuicio de que no siempre se produzca un uso indebido, no resulta extraño que se aduzca la falta de medios humanos y materiales para cubrir un mero trámite formal, sin que se justifique la preferencia por esta opción en lugar del recurso a la externalización. En estos casos, el Tribunal de Cuentas alerta del riesgo de infrautilizar los propios medios materiales y humanos, de perder el control directo de la actividad encargada y de descapitalizar los recursos técnicos propios, con las consecuencias que ello conlleva, a lo que se suma el peligro genérico de incurrir en cesión ilegal de trabajadores, especialmente en los casos en los que se pretende suplir un déficit estructural de plantilla[1064]. En mi opinión, estos efectos no son diferentes de los que se presentan cuando se recurre a la externalización.

El PLCSP regula la cooperación horizontal y vertical, optando por emplear los conceptos comunitarios, por lo que no habla de encomiendas, sino de encargos, que han de ser objeto de publicidad. Los entes que tengan la consideración de medios propios han de ser 100% de capital público y contar con los medios idóneos y suficientes para desarrollar la prestación, a la vez que contar con la autorización del poder adjudicador del que dependan y no tener participación de una empresa privada. Además, no podrán realizar libremente en el mercado más del 20% de su actividad[1065].

A efectos de determinar si la entidad adjudicataria ejerce la parte esencial de su actividad para el poder adjudicador, procede no incluir aquella impuesta por una autoridad

[1063] COSSÍO CAPDEVILLA, A. (2013), encomienda de gestión, 26-33.
[1064] TRIBUNAL DE CUENTAS (2016). Nº 1197. Informe de fiscalización sobre la utilización de la encomienda de gestión, 46, 49 y 61-62.
[1065] GIMENO FELIÚ, J.M. (2016), novedades del anteproyecto, 19-20.

pública no asociada de esa entidad, en favor de otras tampoco asociadas de dicha entidad y que no ejercen control alguno sobre sobre ella, debiendo considerarse ejercida para terceros[1066].

La cooperación vertical, *in house providing*, requiere que el poder adjudicador ejerza sobre ese ente un control análogo al de sus propios servicios, que al menos el 80 % de sus actividades sean para el poder adjudicador que la controla o para otras personas jurídicas controladas por el mismo poder adjudicador; y que no exista participación privada en dicho ente. El control análogo no se refiere al porcentaje de participación en el capital social, sino a que el ente instrumental carezca efectivamente de autonomía desde el punto de vista decisorio[1067]. Incorporando la jurisprudencia europea, el proyecto añade, para entender que existe ese control análogo, que los encargos sean de ejecución obligatoria para el destinatario del mismo a tenor de sus estatutos o del acto de creación. Al objeto de acotar la utilización de esta figura, añade como nuevos requisitos la conformidad o autorización expresa del poder adjudicador al que esté adscrito el medio propio y la verificación por la entidad pública de la que dependa de que cuenta con los medios adecuados para la realización del encargo. También se limita, en general, la posibilidad de subcontratación al 60% de la cuantía del encargo salvo que este establezca otro diferente de forma justificada, evitando así el uso del medio propio como una mera entidad intermediaria utilizada solo para flexibilizar el régimen de contratación[1068]. Se trata de un porcentaje claramente excesivo que puede no llegar a corregir el uso indebido de esta técnica[1069]

[1066] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Cuarta) de 8 de diciembre de 2016.
[1067] GIMENO FELIÚ, J.M. (2016), novedades del anteproyecto, 35.
[1068] LOZANO CUTANDA, B./ FERNÁNDEZ PUYOL, I. (2016), contratación *in-house*, 2-7.
[1069] GIMENO FELIÚ, J.M./ MORENO MOLINA, J.A. (dir.). GUERRERO MANSO, C./ FERNÁNDEZ ACEVEDO, R./ GALLEGO CÓRCOLES, I./ LAZO VITORIA, X./ MOREO MARROIG, T./ MEDINA ARNÁIZ, T./ VALCÁRCEL FERNÁNDEZ, P. (30 de enero de 2017), mejora al proyecto, 10.

y que, además, prevé una vía de escape al admitir que pueda establecerse un límite diferente en la propia orden de encargo[1070].

Sin perjuicio de que existan ocasiones en las que un mal uso de las encomiendas de gestión venga motivado por la pretensión de eludir el régimen jurídico del Derecho administrativo o de suplir las carencias estructurales de las plantillas de los organismos públicos, debemos defender la concepción de una Administración fuerte, capaz de dotarse de instrumentos con los que satisfacer necesidades colectivas en ámbitos diversos y trascendentes, sin sacrificar los "recursos propios" de que dispone[1071]. En cualquier caso, la contratación *in house* del desarrollo del *software* a medida recaerá en una de las tres opciones anteriores, por lo que no procede mayor detenimiento.

7.3.2.4. REUTILIZACIÓN DEL *SOFTWARE* DE LA ADMINISTRACIÓN

La racionalización del uso de los recursos informáticos para conseguir una mayor eficiencia y un ahorro sustancial de costes, a través de una mayor homogeneidad y simplicidad, mediante el uso de herramientas comunes y servicios compartidos, es un objetivo de especial interés en un contexto de limitación presupuestaria. En esa dirección, el artículo 10 del real decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las TIC en la AGE y sus organismos públicos, viene a regular la declaración de esos medios y servicios compartidos necesarios para ejecutar y desarrollar la estrategia TIC aprobada por el

[1070] Artículo 32.6.b) del PLCSP.
[1071] *Vid*. SOSA WAGNER, F./ FUERTES LÓPEZ, M. (2007), ¿pueden los contratos quedar en casa?, 1679-1680.

Gobierno[1072]. Se persigue que el organismo adherido reciba un servicio igual o mejor que el que venía disfrutando, a un coste inferior, liberando recursos económicos, técnicos y humanos, entrando así en un proceso de convergencia que irá poco a poco superando la gran heterogeneidad reinante en el punto de partida. El modelo de prestación de servicios compartidos no será único, sino adaptable, y no estará reñido con la contratación externa, si fuera precisa. Esta forma múltiple de prestación requerirá la utilización de instrumentos diversos en función de la naturaleza de los participantes, como la encomienda de gestión, convenio de colaboración o acuerdo de colaboración. Por lo general, también será necesario que el organismo que se adhiere ponga a disposición del proveedor una pequeña parte de sus recursos humanos especializados, con la asignación de sus plazas y dotaciones económicas, salvedad hecha de los casos en que se trate de personal contratado externo, materializándose entonces en una compensación económica por adhesión y/o uso, esta última con carácter periódico[1073].

La reutilización, sin embargo, no tiene que limitarse a esos servicios compartidos. La unificación de esfuerzos de desarrollo entre distintos centros, fruto del fortalecimiento de la cooperación y colaboración, sin duda es beneficiosa, redundando en ventajas como la estandarización de criterios, un óptimo aprovechamiento de los recursos públicos (humanos, técnicos y económicos), una mayor agilidad en la elaboración de nuevos servicios y un incremento en la especialización de los distintos organismos que, gracias a la utilización de servicios comunes, pasan a disponer de recursos para ocuparse de aquellos que les son propios. De este modo, la reutilización de esos elementos comunes facilita el desarrollo de la

[1072] MINHAP (2015), declaración de servicios compartidos.
[1073] MINHAP (2015), marco regulador para la declaración, 4-11.

eAdministración[1074]. Es una expresión de apertura, transparencia, participación y colaboración, que lleva a la "*ruptura de los silos administrativos*", transformando la forma de trabajar de la Administración de forma efectiva[1075]. Su íntima relación con la interoperabilidad se pone claramente de manifiesto en el capítulo VIII del ENI, rubricado como "reutilización y transferencia de tecnología". Su artículo 16 recoge las condiciones de licenciamiento de las aplicaciones y de su documentación asociada, donde exime a la Administración cedente de la obligación de prestar asistencia técnica o mantenimiento, así como de compensación alguna en caso de errores en el *software*. Sin embargo, aunque coincide con la derogada LAE en hacer posible la puesta a disposición de las otras Administraciones públicas y de los ciudadanos de las aplicaciones, sin contraprestación y sin necesidad de convenio, esa previsión cambia con la nueva ley 40/2015, la cual mantiene el requisito de que la cedente sea titular de los derechos de propiedad intelectual, pero le permite acordar con la cesionaria la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

Manteniendo e impulsando esa nueva forma de afrontar el servicio público, nuestra nueva ley no solo reitera las previsiones de reutilización de sistemas y aplicaciones y de transferencia tecnológica entre Administraciones contempladas en los artículos 45 y 46 de la LAE, sino que las potencia con un empuje mucho mayor en sus artículos 157 y 158. Ya no se limita a posibilitar la reutilización, sino que obliga a ello, siempre que los requisitos tecnológicos de interoperabilidad y seguridad lo permitan y la normativa aplicable no lo impida, salvo que la conveniencia de la realización de un nuevo desarrollo se justifique en términos de eficiencia

[1074] TORRES CARBONELL, J.J. (2009), los servicios comunes como soporte, 217-220.
[1075] MINHAP. (2012), reutilización de activos y aplicaciones, 1.

conforme al artículo 7 de la ley orgánica 2/2012, de 27 de abril, de estabilidad presupuestaria y sostenibilidad financiera.

El desconocimiento de los proyectos llevados a cabo en el resto de las Administraciones públicas dificulta la colaboración y la reutilización de las aplicaciones, convirtiendo, por ello, en un factor crítico de éxito la disposición por parte de los responsables informáticos de cada departamento de unas extensas redes de contactos[1076]. Conscientes de ello y decididos a solucionar este problema, la LAE, el ENI y después la ley 40/2015, disponen el mantenimiento por la AGE de un directorio de aplicaciones de libre reutilización, accesible a través del CTT (Centro de transferencia de tecnología), en el que se publicará el código de los programas desarrollados. También prevé el enlace de los de las distintas Administraciones públicas entre sí y con los instrumentos equivalentes del ámbito de la Unión Europea. Por ello, se ha incluido en el portal PAe un directorio de soluciones, donde se habilita un buscador[1077] y se proporciona una adecuada información divulgativa y de uso, materializando así un repositorio común de *software*, una base de conocimiento común, así como un espacio en el que compartir experiencias y cooperar.[1078]

Como ya contemplaba la LAE y hereda literalmente la ley 40/2015, esas aplicaciones reutilizables pueden ser declaradas como de fuentes abiertas, lo que supone, a tenor del artículo 16 del ENI, la posibilidad de ejecutarse para cualquier propósito, de conocer su código fuente, de modificarse y de redistribuirse, con o sin cambios, siempre que la obra

[1076] MUÑOZ SALINERO, E. (2011), reutilización, 49.
[1077] http://administracionelectronica.gob.es/pae_Home/pae_SolucionesCTT/pae_BuscadorSol.html
[1078] MUÑOZ SALINERO, E. (2011), reutilización, 50.

derivada mantenga estas mismas cuatro garantías. El mismo artículo, en su punto 1, exime al cedente de la obligación de asistencia técnica o mantenimiento, de compensación en caso de errores en la aplicación y de responsabilidad por el posible mal uso por parte del cesionario.

La publicación del código fuente, a pesar de las reservas que algunos desarrolladores aún mantenemos, se considera primordial en la reutilización de las soluciones implantadas y un elemento de transparencia tanto en la gestión de las inversiones públicas como en la propia actividad de los servicios y aplicaciones. Facilita la coordinación tanto con el resto de Administraciones como con el sector privado, al compartir estrategias, avances, experiencias y los propios servicios que dan solución a situaciones comunes en materia de Administración electrónica. Adicionalmente, incrementa la concurrencia en los procesos de licitación asociados al mantenimiento de dichas aplicaciones y en el desarrollo de otras que deban integrarse con ellos, algo que contribuye a evitar la posible cautividad de la Administración o, al menos, la preponderancia de un proveedor derivada de la indisponibilidad de la información necesaria que posibilite la participación de otras empresas en términos de igualdad y competencia[1079].

Sin embargo, contra lo que habitualmente se piensa, no resulta sencillo hacer funcionar una aplicación desarrollada para un organismo público en otro diferente. Con cierta frecuencia, la inversión para adaptar *software* cedido para que funcione en otra instalación supone un gasto similar, en orden de magnitud, al de realizar un desarrollo propio, pues no todas las instalaciones son iguales, ni tampoco los estándares establecidos. A modo de ejemplo, el

[1079] Extraído de la noticia de fecha 25 de mayo de 2015, publicada en referencia a la actualización de la información y del código fuente de 25 servicios y aplicaciones de Administración electrónica por parte del Gobierno de Aragón, descargado de http://administracionelectronica.gob.es/ctt/paea#.V9RGN602tc0 (10 de septiembre de 2016).

Gobierno del Principado de Asturias utiliza el *framework* openFWPA[1080], el Gobierno de Cantabria usa el *framework* AMAP 2.0[1081], el Gobierno vasco dispone de UDA[1082], la Comunidad de Madrid emplea ATLAS[1083], la Junta de Andalucía dispone de MADEJA[1084], otros en el Gobierno de Extremadura[1085]…

La reutilización de sistemas y aplicaciones prevista en el artículo 157 de la ley 40/2015 también se satisface a través de un modelo diferente, mediante el ofrecimiento de aplicaciones, plataformas, infraestructuras o procesos en modo servicio, donde se manifiesta de forma común cierta preocupación por la seguridad y confidencialidad de los datos de carácter personal. Supone la compartición de recursos proporcionados por un proveedor, que pueden ser utilizados por diferentes subscriptores en forma de servicios, ahorrando costes y esfuerzos. A modo de ejemplo, se puede citar el servicio de validación de certificados de @firma, donde el proveedor, el MINHAP, presta el servicio a las Administraciones subscriptoras gracias a la colaboración de autoridades de validación como la DGP, Camerfima o la FNMT. El proveedor debe asegurar el cumplimiento del ENS, informando de las medidas de protección articuladas y de los incidentes de seguridad acaecidos a los diferentes subscriptores, quienes deberán aplicar aquellas medidas que sean de su responsabilidad, como la comunicación de las bajas de usuarios, las acciones de concienciación o la formación en materia de seguridad. En el documento de

[1080] Puede consultarse su descripción técnica en http://administracionelectronica.gob.es/ctt/openfwpa/infoadicional#descripcion-tecnica (descargado el 14 de septiembre de 2016).
[1081] *Vid.* http://amap.cantabria.es (consultado el 14 de septiembre de 2016).
[1082] *Vid.* http://administracionelectronica.gob.es/ctt/uda (consultado el 14 de septiembre de 2016).
[1083] *Vid.* http://www.madrid.org/arquitecturasw/desarrollos-atlas (consultado el 14 de septiembre de 2016).
[1084] *Vid*. http://www.juntadeandalucia.es/servicios/madeja/contenido/libro-pautas/321 (consultado el 14 de septiembre de 2016).
[1085] *Vid*. http://www.gobex.es/filescms/con01/uploaded_files/dgaeti/GT_JAVA.PDF (consultado el 14 de septiembre de 2016).

prestación del servicio se definirá el modelo de responsabilidades en relación con los datos a alojar en el servicio prestado y su manejo y/o tratamiento, a los efectos de seguridad de la información, especialmente en cuanto a los aspectos de confidencialidad y disponibilidad.[1086]

7.3.3. Análisis del sistema de información

El entendimiento entre el jurista y el técnico es siempre importante, pero adquiere una trascendencia mayor cuando afecta a la actuación administrativa automatizada[1087], a pesar de que Métrica V3 no contempla un perfil de jurista en ninguno de sus procesos. En su lugar, el contacto con los técnicos se asume por los usuarios expertos.

Al inicio del proceso de análisis, el responsable de seguridad y su equipo, junto al jefe de proyecto, determinan, desde el punto de vista de la autenticación, confidencialidad, integridad y disponibilidad, la seguridad necesaria para los productos y actividades del ASI[1088].

En este proceso, se recogerá con alto grado de detalle el plan de aseguramiento de calidad y las revisiones a llevar a cabo, así como los procedimientos y mecanismos de resolución de problemas, definiendo las acciones preventivas o correctoras y sus responsables. Se incluirá la actualización del catálogo de normas, estándares y recomendaciones, incorporando toda la información que, desde el punto de vista de la instalación, se considere necesaria[1089]. El grupo de aseguramiento de calidad, independiente del equipo encargado del desarrollo, se implicará directamente en la revisión del catálogo de requisitos, en la comprobación de los modelos

[1086] MINHAP (2016), uso de las herramientas tecnológicas, 6-39.
[1087] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 16-17.
[1088] MAP. Métrica V3. Interfaz de seguridad, 21.
[1089] MAP. Métrica V3. Análisis del sistema de información, 8.

resultantes del análisis y en el estudio del plan de pruebas[1090]. Pero cabe cuestionar no solo la independencia de dicho grupo de calidad, sino su propia existencia. Disponer de tal grupo independiente implica indefectiblemente más recursos humanos, escasos cuando el desarrollo lo afronta el propio personal de la Administración, y en añadidura muy costosos cuando el desarrollo se ha externalizado. Asoma en este ámbito la posibilidad de combinar los esfuerzos de los técnicos públicos y privados. El equipo de desarrollo puede pertenecer a la empresa externa y el grupo de aseguramiento de la calidad puede estar integrado por empleados públicos. Esta posibilidad, que sobre el papel no parece desacertada, se encuentra con dos inconvenientes. Por un lado aparecen las restricciones de comunicación establecidas en previsión de posibles demandas por cesión ilegal de trabajadores, que canalizan el contacto a través de portavoces. Por otro, surge el coste económico del aseguramiento de la calidad, que enfrentará a la empresa externa con la Administración en una batalla donde la ley del contrato serán los pliegos de prescripciones técnicas[1091] y, en ellos, previsiblemente no figurará al mínimo detalle qué se considera "calidad", algo completamente razonable pues, hasta que no se ve, no se puede imaginar lo que una aplicación puede contener. A modo de reflexión, planteo aquí una cuestión sencilla: ¿en cuántos pliegos de prescripciones técnicas se ha incluido alguna cláusula que indique que en las pantallas o documentos generados debe usarse adecuadamente el lenguaje, empleando expresiones gramaticales correctas y sin faltas de ortografía? Me atrevería a decir que en ninguno, al tratarse de uno de esos aspectos que no llegan a detallarse al darse por supuestos, cuando, precisamente, es en lo que se da por supuesto donde surgen los enfrentamientos.

[1090] MAP. Métrica V3. Aseguramiento de la calidad, 9.
[1091] Sobre la elaboración de los pliegos de prescripciones técnicas, *vid*. BALLESTEROS MOFFA, L.Á. (2010), adjudicación de contratos en el sector público, 68-75.

Métrica V3 destaca la importancia de la participación de los usuarios en el proceso de análisis, sugiriendo el uso de técnicas interactivas como el diseño de diálogos y prototipos, que les permiten familiarizarse con el nuevo sistema y colaborar en su construcción y perfeccionamiento[1092]. Analistas y usuarios expertos deberán trabajar juntos en las actividades ASI 2, 6, 8, 9 y 10[1093]. Toda restricción que opere sobre la capacidad de relacionarse de los analistas (en muchas ocasiones externos) con los usuarios expertos (empleados públicos) actuará en detrimento de la calidad y potenciará el incumplimiento de plazos y la insatisfacción de las necesidades de los ciudadanos y de los propios usuarios internos de la Administración. Por ello, las instrucciones dictadas por las Administraciones públicas en evitación de los riesgos de incurrir en cesión ilegal de trabajadores deberían ser matizadas para el caso del personal informático. No puede pretenderse mantener aislados a los analistas de los usuarios sin que establezcan más contacto que a través de la intervención de un intermediario, papel desempeñado habitualmente por el jefe de proyecto de la empresa externa.

Señala Métrica V3 que el propósito del proceso de análisis consiste en la obtención de una especificación detallada del sistema mediante un catálogo de requisitos (válidos, consistentes y completos[1094]) que debe cumplir el *software* y una serie de modelos que cubran las necesidades de información de los usuarios[1095], entre los que se incluirá un modelo conceptual de datos con identificación de las entidades y relaciones que forman parte del

[1092] HERNÁNDEZ TRASOBARES, A. (2003), evolución y desarrollo, 9.
[1093] MAP. Métrica V3. Análisis del sistema de información, 45.
[1094] MAP. Métrica V3. Análisis del sistema de información, 13.
[1095] MAP. Métrica V3. Introducción, 7.

sistema[1096] y un modelo lógico normalizado al menos a la tercera forma normal (3FN)[1097]. Además del catálogo, priorizado y detallado, de los requisitos funcionales, que se utilizará para su seguimiento a través de todo el proceso de desarrollo, se identifican los requisitos no funcionales del sistema, como facilidades que ha de proporcionar o restricciones a que estará sometido en cuanto a rendimiento, frecuencia de tratamiento, seguridad[1098], etc.[1099], restricciones que pueden tener su origen tanto en el *hardware* como en el *software*. Métrica V3 señala que se especificarán requisitos del tipo funcional y de seguridad, de rendimiento, de implantación, de disponibilidad del sistema, dejando abierta la lista para contemplar otros tipos que pudieran surgir, y haciendo referencia a la posibilidad de incluir los casos de uso, una técnica de especificación de requisitos válida tanto para orientación a objetos como para desarrollos estructurados[1100].

[1096] MAP. Métrica V3. Análisis del sistema de información, 6.
[1097] MAP. Métrica V3. Análisis del sistema de información, 23. La normalización de bases de datos es una técnica que permite eliminar redundancias e inconsistencias.
[1098] Como se comentó anteriormente, Métrica V3 considera la seguridad como un requisito funcional, aunque no faltan referencias, probablemente desactualizadas, en las que parece no ser así.
[1099] MAP. Métrica V3. Introducción, 8.
[1100] MAP. Métrica V3. Análisis del sistema de información, 10-11.

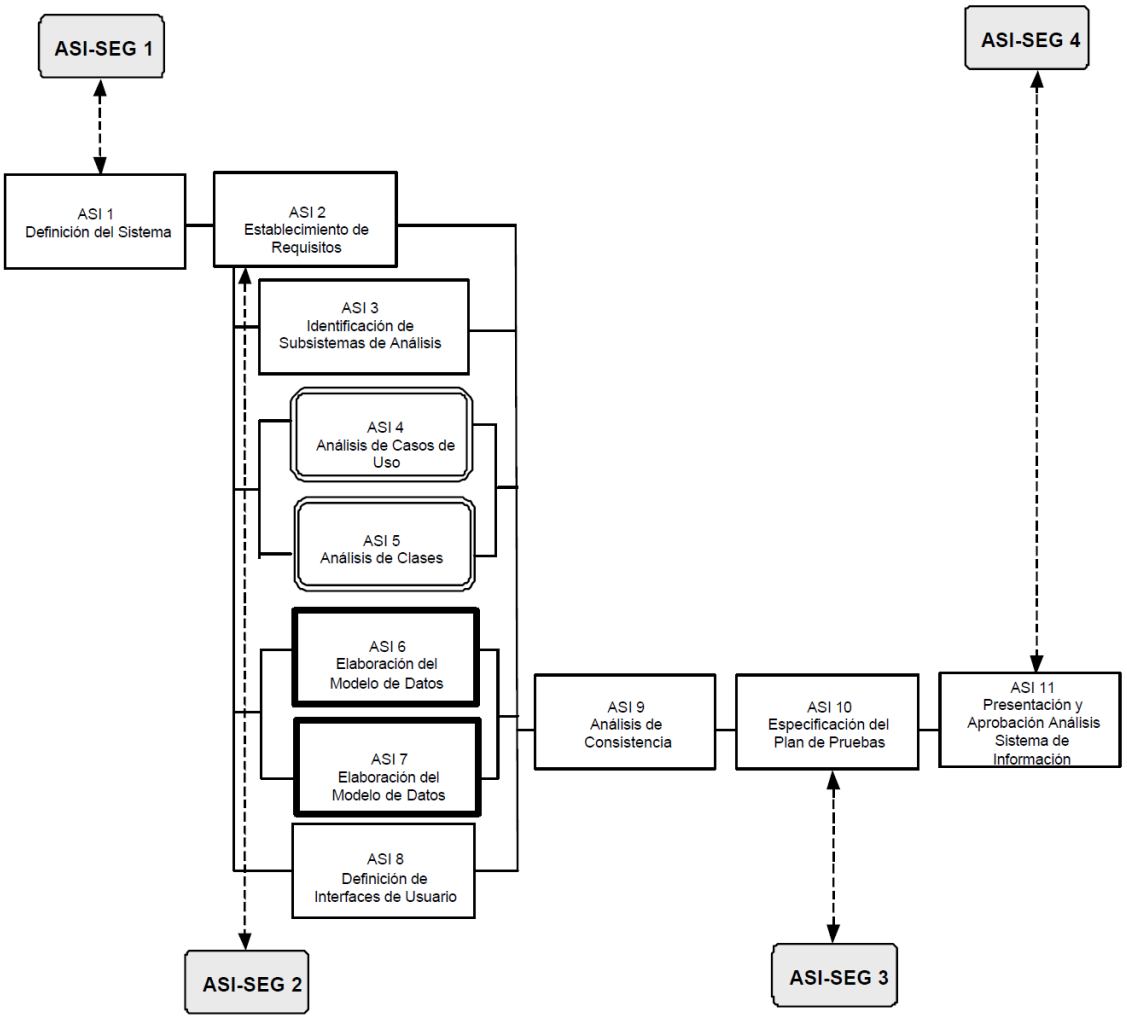

Figura 27: Actividades de ASI

Fuente: Metodología Métrica versión 3. Interfaz de seguridad, 20.

En paralelo con la generación de modelos, se incluye una actividad, ASI 3, al objeto de descomponer el sistema en subsistemas menores, según el criterio que se estime más adecuado. Se necesitará una realimentación, coordinación y ajuste continuo con respecto a la

definición de los subsistemas, sus dependencias y sus interfaces[1101], por lo que se elaborarán y depurarán reiteradamente los modelos de casos de uso y de clases para desarrollos orientados a objetos y los modelos de datos y de procesos para desarrollos estructurados. La definición de las interfaces de usuario se realiza en una actividad específica, la ASI 8, donde se especificarán los formatos de pantallas, diálogos, formatos de informes y formularios de entrada[1102].

En función de la gestión de riesgos escogida (minimizar, eliminar o controlar), el equipo de seguridad determinará el tipo de funciones y mecanismos a implantar (de prevención, detección o corrección) y su naturaleza (técnica, física, organizativa…). Además de recordar la posibilidad de usar MAGERIT, Métrica V3 señala que "*se presta especial atención a los aspectos de seguridad organizativa, ya que son tanto o más importantes que los relativos a la seguridad física y técnica*"[1103].

Habiendo obtenido una primera especificación del plan de migración de datos y carga inicial del sistema, y tras finalizar los distintos modelos, se realiza un análisis de consistencia mediante una verificación y validación, tras la cual se elabora el documento con la especificación de requisitos *software* que servirá de punto de referencia para el desarrollo y para las peticiones de cambio sobre los requisitos inicialmente especificados. Se realiza posteriormente una primera especificación del plan de pruebas unitarias, de integración, del sistema, de implantación y de aceptación[1104]. A su vez, el equipo de seguridad determinará los criterios de aceptación de la misma, incluyendo en las pruebas las funciones y mecanismos

[1101] MAP. Métrica V3. Análisis del sistema de información, 14-16.
[1102] MAP. Métrica V3. Introducción, 8.
[1103] MAP. Métrica V3. Interfaz de seguridad, 22.
[1104] MAP. Métrica V3. Análisis del sistema de información, 24-44.

adicionales de seguridad, de forma que permita comprobar la eficiencia del sistema de información para la eliminación, control o reducción de las amenazas[1105].

Próximo a concluir el proceso ASI, se reúnen el responsable de seguridad, el jefe de proyecto y el comité de seguimiento, para estudiar los productos generados durante el mismo y determinar el nivel de seguridad de cada uno de ellos en cuanto a autenticación, confidencialidad, integridad y disponibilidad[1106].

Los productos resultantes del proceso ASI son[1107] una descripción general del entorno tecnológico, un glosario de términos, el catálogo de normas, el de requisitos y la especificación de interfaz de usuario. En el análisis estructurado, se añade el plan de migración y carga inicial de datos, el contexto del sistema, la matriz de procesos/localización geográfica, la descripción de interfaz con otros sistemas, el modelo de procesos y el modelo lógico de datos normalizado. En el análisis orientado a objetos se aportan también la descripción de subsistemas de análisis, la descripción de interfaces entre subsistemas, el modelo de clases de análisis, el comportamiento de clases de análisis y el análisis de la realización de los casos de uso.

Este conjunto de documentos generados en el ASI encaja perfectamente, en mi opinión, en la noción de "definición de especificaciones" a la que alude el legislador en el artículo 41.2 de la ley 40/2015 refiriéndose a las actuaciones administrativas automatizadas, dado que define componentes, características y/o funcionamiento del producto a desarrollar. La última tarea prevista en la metodología Métrica V3 para el ASI es la 11.1, denominada "presentación y

[1105] MAP. Métrica V3. Interfaz de seguridad, 23.
[1106] *Vid*. MAP. Métrica V3. Interfaz de seguridad, 24-25.
[1107] MAP. Métrica V3. Introducción, 8-9.

aprobación del análisis del sistema de información", en la que el jefe de proyecto entrega el análisis al comité de dirección para someterlo a su aprobación[1108]. Este comité de dirección, de nuevo, en los casos de actuación administrativa automatizada, deberá ser el que se haya establecido previamente como competente para la definición de las especificaciones. Debería poseer los conocimientos de la lógica de negocio suficientes para poder emitir su dictamen con el debido conocimiento. En cuanto a la complejidad técnica, el conjunto de documentos que se someten a su aprobación no resulta excesivamente complejo, aunque podría requerir la intervención de un asesor técnico que explicase el contenido de los mismos, para que el comité de dirección tomase su decisión debidamente informado.

7.3.4. Diseño del sistema de información

El DSI pretende obtener la definición de la arquitectura del sistema y del entorno tecnológico que le va a dar soporte, junto con la especificación detallada de los componentes del sistema de información. Por su dependencia de las características concretas de la instalación, se requiere la colaboración de los responsables de sistemas y explotación de la misma. Tras la obtención de estos productos, se generan todas las especificaciones de construcción, la especificación técnica del plan de pruebas, la definición de los requisitos de implantación y el diseño de los procedimientos de migración y carga inicial si procede[1109].

Durante este proceso, el grupo de aseguramiento de la calidad revisará el diseño para confirmar que los requisitos especificados en el ASI se han traducido en una arquitectura

[1108] MAP. Métrica V3. Análisis del sistema de información, 44.
[1109] MAP. Métrica V3. Introducción, 9.

conforme al entorno tecnológico seleccionado. También comprobará los requisitos que deben cumplir los distintos niveles de pruebas de acuerdo a los criterios de revisión establecidos en el plan de aseguramiento de calidad y revisará la identificación de los requisitos no funcionales relacionados con la documentación de usuario e implantación[1110].

En cuanto a la seguridad del sistema, durante el DSI se diseñan las funciones que gestionarán los riesgos intrínsecos, para lo que resulta especialmente importante la determinación del entorno tecnológico sobre el que se deberán incorporar las funciones y los mecanismos de seguridad[1111].

[1110] MAP. Métrica V3. Aseguramiento de la calidad, 23.
[1111] MAP. Métrica V3. Interfaz de seguridad, 26.

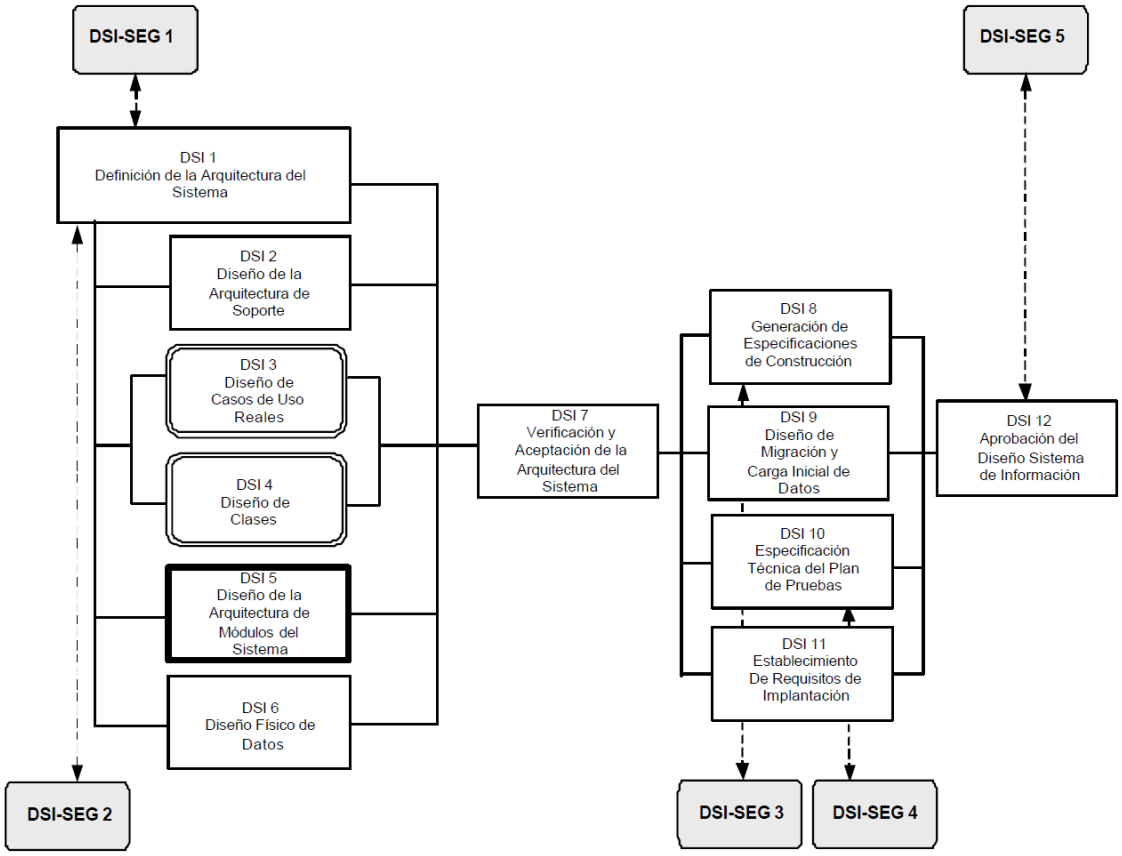

Figura 28: Actividades de DSI

Fuente: Metodología Métrica versión 3. Interfaz de seguridad, 26.

Al inicio del proceso, el responsable de seguridad y su equipo estudian las particularidades del sistema y la necesidad de supervisar los niveles de autenticación, confidencialidad, integridad y disponibilidad de los productos intermedios del DSI, estableciendo el control de la seguridad en las actividades tanto a nivel de ejecución como de los productos

obtenidos y estudiando los riesgos que plantea el entorno tecnológico concreto previsto sobre el sistema de información[1112].

Existe un primer bloque de actividades a desarrollar en paralelo y en continua realimentación, con el objetivo de obtener el diseño de detalle[1113]. Se define la arquitectura general del sistema y se realiza una división en subsistemas, en partes lógicas coherentes con interfaces claramente definidas. Para independizar las funcionalidades a cubrir por el sistema de la infraestructura que le da soporte, se establece una distinción entre los denominados "subsistemas específicos" y los "subsistemas de soporte". También se determina la ubicación óptima de los distintos subsistemas, habida cuenta de la criticidad que podría suponer en el rendimiento. Se catalogan las excepciones, es decir, los comportamientos no habituales que reflejan situaciones anómalas. Se recoge la información de estándares y normas de diseño y construcción que vienen originados por la elección de la propia arquitectura o infraestructura concreta, y se definen los procedimientos de seguridad y operación necesarios para no comprometer el correcto funcionamiento del sistema y garantizar el cumplimiento de los niveles de servicio que pudieran acordarse. Los equipos de seguridad, de arquitectura y de soporte técnico llevan a cabo la definición de los requisitos de seguridad y control de acceso necesarios para garantizar la protección del sistema y minimizar el riesgo de pérdida, alteración o consulta indebida de la información, para lo cual se diseñan los procedimientos relacionados con el acceso al sistema y a sus recursos, el mantenimiento de la integridad y confidencialidad de los datos, el control y registro de accesos al sistema, las copias de seguridad y recuperación de datos

[1112] MAP. Métrica V3. Interfaz de seguridad, 27-28.
[1113] MAP. Métrica V3. Introducción, 9.

y su periodicidad o la recuperación ante catástrofes. Asimismo, se definen los requisitos de operación para los distintos elementos del sistema[1114].

En paralelo con la actividad DSI 1 se llevan a cabo las tareas de las actividades 2 a 6, que incluyen el diseño de la arquitectura de soporte, el diseño de casos de uso reales, el diseño de clases, el diseño de la arquitectura de módulos del sistema y el diseño físico de datos, así como la definición de un plan de migración y carga inicial de datos[1115].

En el primer bloque de actividades se completan los catálogos de requisitos, de excepciones y de normas para el diseño y construcción, el diseño de la arquitectura del sistema, el entorno tecnológico del sistema, los procedimientos de operación y administración del sistema y de seguridad y control de acceso, el diseño detallado de los subsistemas de soporte, el modelo físico de datos optimizado, la asignación de esquemas físicos de datos a nodos y el diseño de interfaz de usuario. Si se trata de diseño estructurado, se adjunta el diseño de la arquitectura modular, pero si es orientado a objetos, se añade el diseño de la realización de casos de uso, el modelo de clases de diseño y el comportamiento de clases de diseño[1116].

Terminado dicho primer bloque, tiene lugar una actividad compleja para la que se recomienda el uso de herramientas de apoyo. Se trata de la verificación y aceptación de la arquitectura del sistema, orientada a garantizar la calidad y viabilidad de las especificaciones del DSI. Para ello se verifica la calidad técnica formal de cada modelo o especificación, se asegura la coherencia entre los distintos modelos, comprobando la falta de ambigüedades o duplicación de

[1114] MAP. Métrica V3. Diseño del sistema de información, 7-16.
[1115] MAP. Métrica V3. Diseño del sistema de información, 3.
[1116] MAP. Métrica V3. Introducción, 9-10.

información, y se lleva a cabo la aceptación del diseño de la arquitectura por parte de las áreas de explotación y de sistemas[1117].

El segundo bloque complementa el diseño generando todas las especificaciones necesarias para el proceso siguiente:

- Las especificaciones de construcción de los componentes del sistema, ya sean módulos o clases, y de las estructuras de datos para los gestores de bases de datos o sistemas de ficheros.
- La especificación del entorno de construcción, como *hardware*, *software*, comunicaciones, herramientas de construcción, generadores de código, compiladores, restricciones técnicas del entorno, planificación de capacidades previstas, requisitos de operación y seguridad del entorno de construcción…
- La especificación del entorno y de los procedimientos de migración y sus componentes asociados (de seguridad y de carga de datos), así como del plan de migración y carga inicial de datos.
- La especificación técnica del plan de pruebas unitarias, de integración, del sistema, de implantación y de aceptación, actualizando el plan de pruebas con información de la especificación del entorno de pruebas, especificación técnica de los niveles de prueba y su planificación.
- El catálogo de excepciones.

[1117] MAP. Métrica V3. Diseño del sistema de información, 38-43.

- La especificación de los requisitos de implantación. Se completa el catálogo de requisitos con los relacionados con la documentación sobre la operación con el nuevo sistema y los relativos a la propia implantación, lo que permite ir adelantando la preparación de los medios y recursos necesarios en los sucesivos procesos de CSI e IAS[1118].

En este segundo bloque interviene de nuevo el equipo de seguridad, que deberá estudiar las condiciones que debe cumplir el futuro entorno de construcción en esa materia, determinando los riesgos intrínsecos y los mecanismos de salvaguarda. Además, realizará el diseño específico de las pruebas de seguridad del sistema. Finalmente, como en procesos anteriores, el responsable de seguridad, el jefe de proyecto y el comité de seguimiento estudian los productos generados y determinan el nivel de seguridad de cada uno de ellos con respecto a la autenticación, confidencialidad, integridad y disponibilidad[1119].

La actividad DSI 12 cierra el proceso con la presentación del diseño por el jefe de proyecto a la aprobación del comité de dirección[1120]. Este conjunto de documentos generados durante el proceso de DSI, como ocurrió en el ASI, encaja perfectamente, en mi opinión, en la noción de "definición de especificaciones" a la que alude el legislador en el artículo 41.2 de la ley 40/2015 refiriéndose a las actuaciones administrativas automatizadas. Este comité de dirección, de nuevo, en los casos de actuación administrativa automatizada, deberá ser el que se haya establecido previamente como competente para la definición de las especificaciones. Sin embargo, a diferencia de lo que ocurría en la aceptación del ASI, el conjunto de documentos que

[1118] MAP. Métrica V3. Diseño del sistema de información, 44-58.
[1119] *Vid*. MAP. Métrica V3. Interfaz de seguridad, 29-31.
[1120] MAP. Métrica V3. Diseño del sistema de información, 59-60.

se someten a su aprobación presenta mayor complejidad técnica y menores exigencias en cuanto al conocimiento de la lógica de negocio. La aceptación emitida por un comité de seguimiento carente de la adecuada formación técnica o, en su defecto, del debido asesoramiento por empleados públicos especializados en las TIC, equivaldría a dejar en manos del personal que ha intervenido en el proceso de diseño la aprobación del mismo, algo especialmente inadecuado cuando el proceso de DSI se haya depositado en manos de personal externo. En estos supuestos de participación de empresas privadas, se deben reforzar las precauciones desde la óptica del respeto al ejercicio de la competencia por quien la tiene atribuida, el órgano administrativo[1121].

7.3.5. Construcción del sistema de Información

En la construcción de servicios públicos electrónicos, debe ser un objetivo la mejora continua y notoria de la calidad. Para lograrlo, los centros de desarrollo pueden hacer uso de un conjunto de plataformas, metodologías y estándares, al objeto de asegurar la fiabilidad de las aplicaciones implantadas y controlar sus cambios, garantizando la calidad técnica y funcional de las nuevas versiones de *software* y evitando los riesgos e incidencias ante el cambio. De ello fueron conscientes en la GISS hace una década, convencidos de que, "*a pesar del tiempo y esfuerzo invertido en una serie de herramientas y metodologías que no ven su repercusión inmediata sino a largo plazo, merece la pena los recursos invertidos* (…)"[1122]. Esta relación entre calidad e inversión en recursos, sin que se vea una repercusión inmediata, deja en el aire la pregunta de si una empresa privada, movida por la legítima búsqueda del beneficio económico, también apostará por dicho gasto. Esa duda toma aún más fuerza cuando el contrato de servicios

[1121] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 70.
[1122] MARTÍNEZ DE DUEÑAS, C./ FERNÁNDEZ FÍRVIDA, M. (Octubre, 2007), tecnologías de desarrollo.

subscrito con esa empresa no abarca la fase de mantenimiento, sino que finaliza con la implantación y aceptación.

Como principio director de todas sus labores los desarrolladores, ya sean empleados públicos o personal externo, han de considerar que toda entrada es potencialmente maliciosa y pensar como lo haría un atacante, planteándose si el proceso que envuelve la funcionalidad es seguro, de qué manera se podría abusar de dicha funcionalidad, si ha de estar activa por defecto y qué opciones minimizan el riesgo de su uso[1123]. La codificación del *software* se realizará asumiendo los principios de "mínimo privilegio" y de "necesidad de conocer", aplicando, por tanto, la conocida como *privacy by default*, limitando el tratamiento a aquellos datos que resulten imprescindibles para los fines específicos a alcanzar[1124].

El grupo de aseguramiento de calidad revisará los estándares de nomenclatura y normativa aplicada en la generación del código, en los manuales de usuario, en el esquema de formación y en la evaluación de los resultados de las pruebas, comprobando también la realización de pruebas unitarias, de integración y del sistema según los criterios de selección de verificaciones y casos de prueba asociados que se hayan fijado previamente en el plan de aseguramiento de calidad[1125].

[1123] MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO, buenas prácticas, 3.
[1124] CARPIO CÁMARA, M. (2016), seguridad del tratamiento, 345.
[1125] MAP. Métrica V3. Aseguramiento de la calidad, 23.

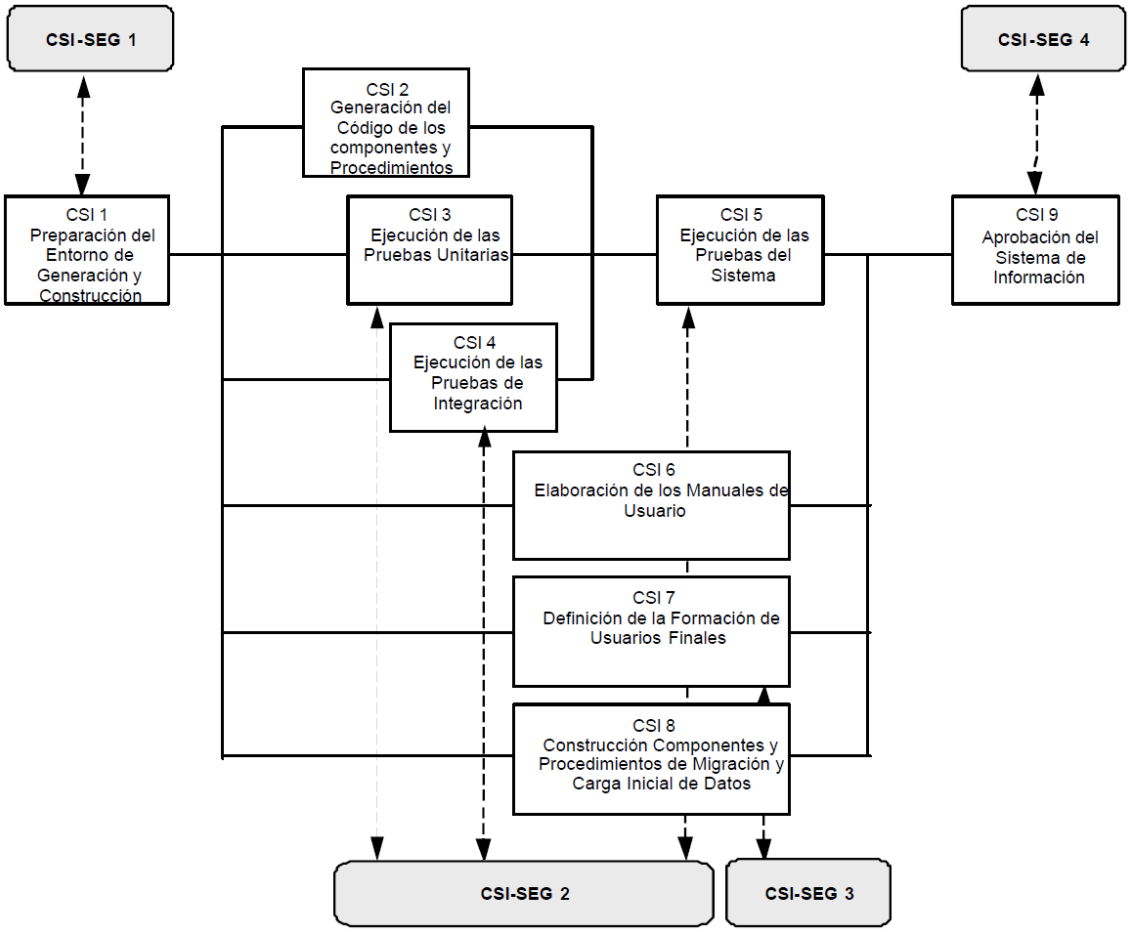

Figura 29: Actividades de CSI

Fuente: Metodología Métrica versión 3. Interfaz de seguridad, 33.

El proceso de construcción se inicia con la intervención del equipo de seguridad para analizar si es necesario supervisar los niveles de autenticación, confidencialidad, integridad y disponibilidad de los productos intermedios de las actividades a realizar en la construcción, elaborando el correspondiente informe al respecto. Para Métrica V3, "*según las características del proyecto, el entorno de construcción debe ser sometido a controles de seguridad que eviten*

filtraciones indeseables de datos relativos al sistema de información"[1126]. Será preciso adecuar ese entorno para las tareas de programación y pruebas, preparando la base de datos física o el sistema de ficheros, las bibliotecas o librerías, otras herramientas varias y los puestos de trabajo, además de implementar los procedimientos de operación y de seguridad prefijados en los requisitos[1127]. En la medida de lo posible, para la realización de las pruebas se utilizarán bases de datos de carácter personal pseudonimizadas o anonimizadas[1128].

Se construirán los componentes del sistema de información, a partir del conjunto de especificaciones lógicas y físicas del mismo. Para generar el código fuente se tienen en cuenta los estándares de nomenclatura, codificación y calidad utilizados por la organización y recogidos en el catálogo de normas. Se verificará que el código fuente especifique de forma correcta el componente, realizando su ensamblaje o compilación, corrigiendo los errores sintácticos y enlazando el código objeto obtenido con las correspondientes bibliotecas. Igualmente, se generará el código de los procedimientos de operación y de administración del sistema, así como los de seguridad y control de acceso, teniendo también en cuenta los estándares y las normas de la instalación recogidos en el catálogo[1129].

Cada componente debe superar las pruebas unitarias tras su codificación, al objeto de comprobar la corrección de su estructura y su ajuste a la funcionalidad establecida. En el plan de pruebas a seguir consta la preparación del entorno necesaria, las verificaciones asociadas, la

[1126] MAP. Métrica V3. Interfaz de seguridad, 33-34.
[1127] MAP. Métrica V3. Construcción del sistema de información, 5-6.
[1128] CARPIO CÁMARA, M. (2016), seguridad del tratamiento, 346.
[1129] MAP. Métrica V3. Construcción del sistema de información, 6-8.

coordinación y secuencia a seguir en su ejecución y los criterios de registro y aceptación de los resultados. Si estos no son los esperados, se han de realizar las correcciones pertinentes[1130].

En paralelo, se realizan las pruebas de integración, orientadas a verificar la correcta interactuación entre los componentes o subsistemas a través de sus interfaces, así como la adecuada cobertura de la funcionalidad establecida y el cumplimiento de los requisitos especificados. Cuando los resultados no son los esperados, es preciso identificar el origen del problema y remitirlo a quien proceda, determinando la envergadura de las modificaciones y las acciones a llevar a cabo su resolución satisfactoria. Igualmente, es preciso indicar si las pruebas han de repetirse total o parcialmente, y si será necesario contemplar nuevos casos de prueba no considerados previamente[1131].

El objetivo de las pruebas del sistema es comprobar la integración globalmente, verificando el funcionamiento correcto de las interfaces entre los distintos subsistemas que lo componen y con el resto de sistemas de información con los que se comunica, comprobando la cobertura de los requisitos. Todas las pruebas se analizan, informan y registran conforme a los criterios establecidos en el plan de pruebas. Al igual que se procedió con las pruebas de integración, localizado un resultado inesperado, se identifica el origen y se le remite para su resolución satisfactoria, indicando si se han de repetir las pruebas total o parcialmente, o si se han de incluir otras no previstas previamente[1132].

[1130] MAP. Métrica V3. Construcción del sistema de información, 8-10.
[1131] MAP. Métrica V3. Construcción del sistema de información, 10-12.
[1132] MAP. Métrica V3. Construcción del sistema de información, 12-14.

La realidad evidencia que no todas las organizaciones pueden asumir los costes de disponer un departamento dedicado a validar las aplicaciones desarrolladas. Por lo general, es el propio equipo de desarrollo quien realiza íntegramente las pruebas, algo que condiciona y limita la visión con que se realizan y, en consecuencia, puede sacrificar la calidad del *software*, incluso de forma inconsciente, a cambio de reducir tiempos de entrega, recursos y costes, obteniendo productos que no siempre satisfacen los requisitos y las expectativas.[1133]

El equipo de seguridad estudia los resultados obtenidos en las pruebas de seguridad unitarias, de integración y del sistema para comprobar si ha habido problemas debidos a las funciones y mecanismos adicionales de seguridad incorporados[1134].

Superadas las tareas más estresantes del proceso de construcción, llega el momento de elaborar la documentación de usuario, tanto usuario final como de explotación, conforme a los requisitos establecidos en el proceso de diseño. Se determinan las necesidades, contenido, duración y recursos referentes a la formación del usuario final, con la pretensión de conseguir la explotación eficaz del nuevo sistema. También es preciso definir las características que debe reunir el entorno para realizar la formación, en cuanto a cargas iniciales o migración de datos, activar los procedimientos de seguridad y control de acceso específicos, etc.[1135]

El equipo de seguridad y su responsable, en aras de garantizar que los usuarios sean conscientes de las amenazas y riesgos, desarrollan un plan de formación para intentar reducir el peligro que provoca el factor humano, por acción o negligencia, conscientes de que las

[1133] BLANCO GALÁN, M. (2011), aseguramiento de calidad, 49.
[1134] MAP. Métrica V3. Interfaz de seguridad, 35.
[1135] MAP. Métrica V3. Construcción del sistema de información, 15-17.

medidas son inútiles si las personas no las aplican. Dicho equipo de seguridad define planes de formación en seguridad específicos, contemplando distintos niveles y perfiles, siendo el responsable de seguridad quien establece la manera en que debe acometerse la formación de los grupos de usuarios[1136].

En el supuesto de que se requiera la realización de una migración o de una carga inicial de datos, entrará en escena la actividad CSI 8, lo que implica disponer del entorno y de los datos necesarios para realizar las pruebas de los componentes y procedimientos precisos para llevar a cabo la migración. Para generar el código fuente se tienen en cuenta de nuevo los estándares de nomenclatura y codificación utilizados por la organización y recogidos en el catálogo de normas para este tipo de componentes. Tras efectuar las pruebas y evaluar su resultado, si no es el esperado, se identifica el origen de cada problema detectado para poder remitirlo a quien proceda, determinando la envergadura de las modificaciones y las acciones para resolverlo de forma satisfactoria. Debe indicarse si el plan de pruebas debe volver a realizarse total o parcialmente y si será necesario contemplar nuevos casos no considerados anteriormente[1137].

Como resultado del proceso de construcción se obtiene el resultado y evaluación de las pruebas unitarias, de integración y del sistema, junto con el producto *software*, constituido por el código fuente de los componentes, los procedimientos de operación y administración del sistema, los procedimientos de seguridad y control de acceso, los manuales de usuario, la especificación de la formación a usuarios finales, el código fuente de los componentes de

[1136] MAP. Métrica V3. Interfaz de seguridad, 35-36.
[1137] MAP. Métrica V3. Construcción del sistema de información, 17-20.

migración y carga inicial de datos, los procedimientos de migración y carga inicial de datos y, por último, la evaluación del resultado de las pruebas de migración y carga inicial de datos. [1138]

Como viene reiterándose en los procesos anteriores, próximos a finalizar las actividades y tareas del mismo, el responsable de seguridad, el jefe de proyecto y el comité de seguimiento estudian los productos generados y determinan los niveles de autenticación, confidencialidad, integridad y disponibilidad[1139].

Valero Torrijos parece ser consciente de la problemática realidad que supone poner en manos ajenas las tareas de construcción del *software* público cuando, en referencia al órgano que tiene atribuida la competencia, afirma que "*a lo sumo, podría haber emitido un informe en relación con el funcionamiento de una aplicación informática que, debido a la complejidad que conlleva, con relativa frecuencia ni siquiera podría comprender y mucho menos controlar*"[1140]. Es en la última tarea, CSI 9.1, cuando el jefe de proyecto recopila los productos generados en el proceso de CSI y los presenta al comité de seguimiento para su aprobación[1141]. En el caso de actuación administrativa automatizada, conforme al artículo 41.2 de la ley 40/2015, ha de establecerse previamente el órgano u órganos competentes para la programación. En los procesos anteriores el artículo 41.2 se refería a la competencia "*para la definición de las especificaciones*", algo sustancialmente diferente de la competencia "*para (…) la programación*". La definición de especificaciones se recoge por completo en un conjunto de documentos, y el órgano competente, aunque no haya participado en su definición, es

[1138] MAP. Métrica V3. Introducción, 11.
[1139] *Vid*. MAP. Métrica V3. Interfaz de seguridad, 37-38.
[1140] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 193-194.
[1141] MAP. Métrica V3. Construcción del sistema de información, 20.

perfectamente capaz, aunque sea con el asesoramiento de un empleado público con perfil técnico, de comprobar cada una de las especificaciones, comprenderlas y aprobarlas o rechazarlas con pleno conocimiento. Sin embargo, la programación puede constar de miles o incluso millones de líneas de código. Como comenté *supra*, a modo de ejemplo, en 2009 las aplicaciones de la AEAT estaban formadas por más de 160 millones de líneas de código. Ningún órgano declarado competente será capaz de comprobarlas ni comprenderlas, con o sin asesoramiento especializado.

Por lo tanto, en el caso de actuaciones administrativas automatizadas, la designación previa del órgano u órganos competentes para la programación, necesariamente ha de significar su competencia para escribir directamente el código. En mi opinión, en ningún modo puede delegar esa competencia en las manos de informáticos de empresas externas, puesto que estos escribirían unos programas que el órgano no podrá comprobar materialmente y, por ello, no podrá asumirlos como propios.

En el caso de tareas de programación no destinadas a realizar actuaciones administrativas automatizadas, carecemos de un precepto legal equivalente que disponga la asignación a algún órgano administrativo de la competencia para programar, por lo que, en principio, nada impediría externalizar la programación. El comité de seguimiento, volviendo a utilizar la terminología de Métrica V3, designado por ese órgano administrativo, será el encargado de expresar su aceptación o rechazo de los productos generados en el proceso CSI, entre los que se incluyen los programas *software*. Sin embargo, el comité de seguimiento no

tendrá capacidad para manifestar la aprobación de algo que no ha programado y que, por sus dimensiones, se da la imposibilidad material de que realice su comprobación.

A pesar de la trascendencia de la supervisión, no solo formal, por parte de la Administración, en demasiados casos no se lleva a cabo, ya sea por falta de conocimientos o, lo que resulta más grave, por inercia o confianza[1142], a lo que hay que añadir la imposibilidad práctica de poder garantizar que el código ajeno cumple las directrices marcadas por nuestro ordenamiento jurídico desde el momento en que los programas alcanzan un volumen de líneas de código que convierte las desviaciones en indetectables.

No se puede ignorar que el programador tiene la responsabilidad de la seguridad en el proceso de creación de firma externo en el dispositivo seguro, de la relación con el firmante de una manera fiable y de intermediar entre el firmante y su dispositivo de firma[1143]. También la manipulación, corrupción o sustitución del documento o de los datos a firmar conducen a la creación de firmas falsas[1144]. Los programas entregados por las empresas externas pueden carecer de la calidad adecuada, puede ofrecer vulnerabilidades que abran puertas a los ciberataques, puede esconder fragmentos de código maliciosos, pueden apropiarse de las contraseñas de los usuarios para proceder a su suplantación, pueden firmar electrónicamente documentos diferentes de los que el usuario creía estar firmando con su certificado digital, etc. El comité de seguimiento se limitaría a pronunciar su aceptación basándose únicamente en la buena

[1142] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 70.
[1143] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 287.
[1144] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 301.

fe, porque las probabilidades de encontrar algo escondido dentro de millones de líneas de código es muy pequeña. Y, si es malicioso, estará muy bien escondido.

El ejercicio por la Administración de las facultades de dirección y control del contrato administrativo presenta especiales dificultades en los contratos de servicios de carácter intelectual, como es el de desarrollo de aplicaciones a medida, en los que se requiere una cualificación importante del personal del contratista. A ello es preciso añadir la falta de adecuación de los medios propios de la Administración, que impide el control de la ejecución del contrato, o la saturación de trabajo de los mismos, que produce efectos similares.[1145] A su vez, es difícil negar la práctica imposibilidad de que un informático que no ha realizado materialmente las tareas de programación, pueda validar su corrección, habida cuenta de que probablemente tardaría menos tiempo en escribirlo por sí mismo que en averiguar qué hace lo que está programado y verificar su correcto funcionamiento.

Como consecuencia de ello, se aprecia un preocupante comportamiento que Menéndez Sebastián describe para los contratos de servicios de carácter intelectual en general:"(…) *la Administración tiende a todo tipo de artimañas que le permitan celebrar el contrato con alguien que conoce y le inspire confianza* (…)".[1146]

Ante una aplicación informática compleja que no puede comprender ni controlar, solo acudiendo a una ficción legal cabría considerar que la actuación administrativa ha sido llevada a cabo por el órgano administrativo que tiene atribuida la competencia[1147]. Por ello,

[1145] *Vid*. MENÉNDEZ SEBASTIÁN, E.M. (2009), contratos de servicios del sector público, 600-614.
[1146] MENÉNDEZ SEBASTIÁN, E.M. (2009), contratos de servicios del sector público, 617-618.
[1147] VALERO TORRIJOS, J. (2013), Derecho, innovación y Administración electrónica, 193-194.

reafirmo mi creencia de que el *software* desarrollado a medida para las Administraciones públicas ha de ser programado por los propios empleados públicos en cualquier caso, pero especialmente si se trata de actuaciones administrativas automatizadas. El abandono de las RPTs del personal TIC en nuestras Administraciones, denunciado *supra*, lo convierte en inviable y nos condena a confiar en la buena fe de unas empresas de servicios movidas por la búsqueda de su propio beneficio económico.

7.3.6. Implantación y aceptación del sistema

El grupo de aseguramiento de calidad revisará la existencia de un plan de implantación y su conformidad con la estrategia determinada en el EVS y con los requisitos establecidos en el DSI. Comprobará también la realización de las pruebas de implantación y de aceptación según el plan de pruebas y la normativa acordada en el plan de aseguramiento de calidad, revisando la totalidad de las verificaciones y casos de prueba especificados y las incidencias producidas, determinando si puede afectar a alguna propiedad de calidad. Se asegurará de que se entrega el producto *software* al responsable de mantenimiento de forma que le permita asumir dicho servicio de mantenimiento tras su puesta en producción[1148]. En este punto puede surgir un importante problema cuando el *software* no ha sido desarrollado por un equipo propio, sino externo, y no se ha contratado el mantenimiento con la misma empresa, en cuyo caso el código no podrá ser alterado hasta que finalice el plazo de garantía del aplicativo, salvo que se decida renunciar a la misma.

[1148] MAP. Métrica V3. Aseguramiento de la calidad, 30.

El proceso IAS tiene por objetivos la entrega y aceptación del sistema en su totalidad, sin perjuicio de que pueda comprender varios sistemas de información desarrollados de manera independiente, y la preparación del paso a producción[1149]. A estas finalidades hay que añadir la definición detallada de la seguridad para la implantación del sistema una vez construido[1150].

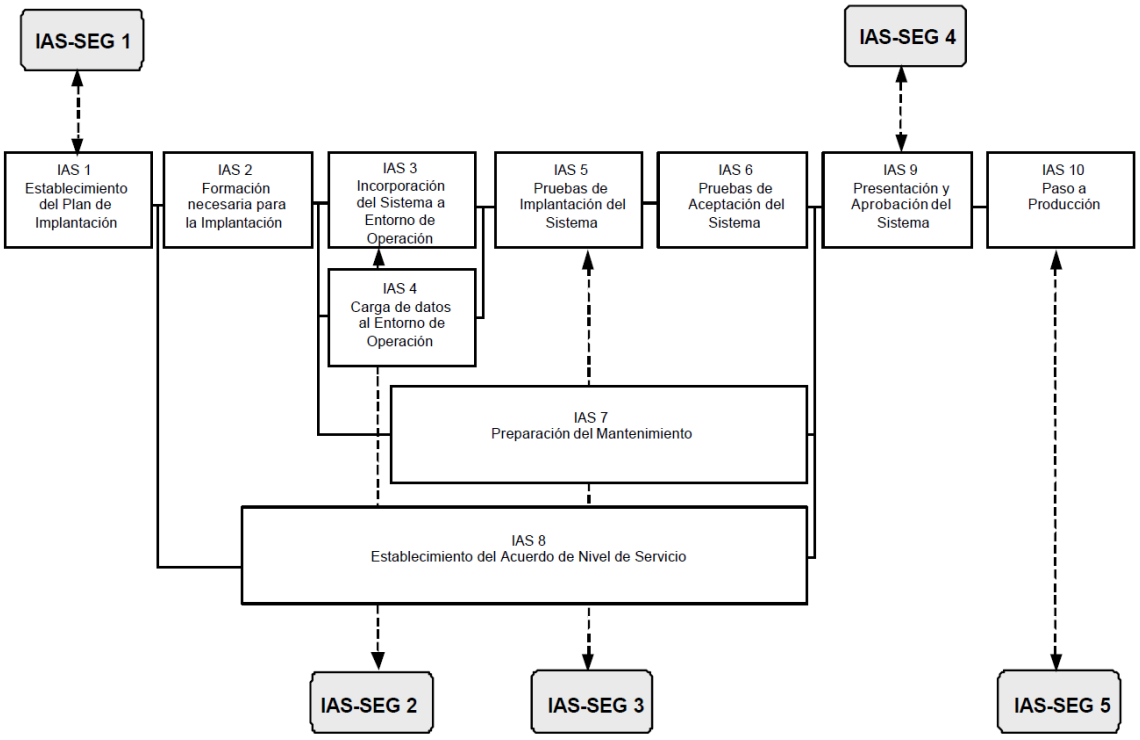

Figura 30: Actividades de IAS

Fuente: Metodología Métrica versión 3. Interfaz de seguridad, 39.

[1149] MAP. Métrica V3. Introducción, 11-12.
[1150] MAP. Métrica V3. Interfaz de seguridad, 39.

Una vez más, como al inicio de cada proceso, el equipo de seguridad analiza la necesidad de supervisar los niveles de autenticación, confidencialidad, integridad y disponibilidad de los productos intermedios y establece el control de la seguridad en las actividades tanto a nivel de ejecución como de los productos obtenidos[1151].

Se revisa la estrategia de implantación establecida inicialmente en el EVS y se analizan las posibles dependencias con otros proyectos que la puedan condicionar. Se establece una estrategia concreta plasmada en un plan de implantación, que permite calcular adecuadamente el esfuerzo y los recursos necesarios para llevarla a cabo con éxito, y que contempla aspectos como formación, preparación de la infraestructura, instalación de todos los componentes y procedimientos manuales o automáticos, ejecución de la carga inicial y migración, realización de pruebas de implantación y aceptación, así como la formalización del plan de mantenimiento. Se constituye el equipo de implantación determinando los recursos humanos necesarios e identificando los respectivos perfiles y niveles de responsabilidad, así como las fechas previstas de participación[1152].

La formación necesaria para el personal de implantación contempla diferencias en función de los distintos perfiles y niveles de responsabilidad. Aunque también se realiza la preparación y el seguimiento de la formación de los usuarios finales, establecida en CSI 7, su impartición queda fuera del ámbito de Métrica V3[1153].

[1151] MAP. Métrica V3. Interfaz de seguridad, 40.
[1152] MAP. Métrica V3. Implantación y aceptación del sistema, 5-6.
[1153] MAP. Métrica V3. Implantación y aceptación del sistema, 7-9.

En la preparación de la instalación, el equipo de seguridad refuerza las acciones relativas a procedimientos de seguridad y control de accesos, verificando el cumplimiento de las medidas de seguridad necesarias que hacen referencia al entorno de operación sobre el que se implantará el sistema y a la carga inicial de datos.[1154]

Se prepara la instalación y se incorpora el sistema al entorno de operación. Aunque las pruebas unitarias, de integración y del sistema se pueden ejecutar en un entorno distinto de aquel en el que finalmente se implantará, las pruebas de implantación y aceptación del sistema deben ejecutarse en el entorno real de operación[1155], para comprobar que satisface todos los requisitos especificados por el usuario en las mismas condiciones que cuando se inicie la producción[1156].

Se introducen los datos al entorno de operación, mediante una carga inicial y/o una migración que transforme la estructura existente a la nueva y depure las inconsistencias detectadas[1157]. Las migraciones entrañan un riesgo importante para los datos, especialmente por pérdidas en la transmisión al sistema nuevo, siendo importante realizar pruebas en paralelo comparando ambos[1158].

Se realizan las pruebas de implantación, con la doble finalidad de comprobar el funcionamiento correcto del sistema en el entorno de operación y de permitir al usuario verificar el cumplimiento de los requisitos especificados y dar su aceptación.

[1154] MAP. Métrica V3. Interfaz de seguridad, 41.
[1155] También denominado producción, explotación y entorno real.
[1156] MAP. Métrica V3. Implantación y aceptación del sistema, 10-12.
[1157] MAP. Métrica V3. Implantación y aceptación del sistema, 12-13.
[1158] PIATTINI VELTHIUS, M.G. (2001), auditoría de bases de datos, 319.

Las pruebas que realizan técnicos de sistemas y de operación, adecuadamente formados, cubren el comportamiento del sistema bajo las condiciones más extremas, y versan sobre aspectos como la recuperación ante fallos forzados, el funcionamiento de los mecanismos de protección de la seguridad, el rendimiento en cuanto al tiempo de respuesta de ejecución y tiempo de utilización de recursos, comunicaciones, etc. Si los resultados obtenidos difieren de los esperados, se identifica el origen del problema y se remite a quien proceda, determinando la envergadura de las modificaciones y las acciones necesarias para resolverlo de forma satisfactoria, e indicando si el plan de pruebas debe repetirse total o parcialmente y si se deben contemplar nuevos casos de prueba no considerados. Tomadas las medidas correctoras, se comprueba el cumplimiento de los requisitos de implantación y se registra el resultado de la evaluación de las pruebas de implantación, incluyendo la aprobación o rechazo.[1159]

El equipo de seguridad estudia los resultados obtenidos en las pruebas de seguridad del sistema y verifica que las funciones y mecanismos adicionales incorporados no han originado problemas[1160].

El usuario final ha de realizar las pruebas de aceptación del sistema, con el objetivo de validar el cumplimiento de los requisitos básicos de funcionamiento, pudiendo así pronunciar su aceptación. Se registran las pruebas realizadas junto con un informe que indique las desviaciones detectadas y los problemas que quedan sin resolver. Tras evaluarlas y analizar las incidencias recibidas, cuando los resultados difieran de los esperados, se identificará el origen del problema para poder remitirlo a quién proceda y determinar las acciones o medidas

[1159] MAP. Métrica V3. Implantación y aceptación del sistema, 13-15.
[1160] MAP. Métrica V3. Interfaz de seguridad, 42.

correctoras precisas, indicando qué pruebas volver a realizar, o si será necesario contemplar nuevos casos. Tras comprobar la efectividad de las correcciones, se documenta el resultado global de la evaluación, incluyendo la aprobación del sistema por parte del usuario final.[1161]

La actividad IAS 7 pretende familiarizar con el nuevo sistema al equipo que asumirá su mantenimiento antes de que llegue a producción, incluyendo al responsable de mantenimiento como parte del equipo de implantación, para que vaya obteniendo, de una forma gradual, un conocimiento profundo del funcionamiento y facilidades que incorpora el sistema, lo que le permitirá acometer los cambios solicitados por los usuarios con mayor facilidad y eficiencia, reduciendo el esfuerzo invertido en el mantenimiento[1162]. Una vez en el entorno de producción, se establece formalmente el plan de mantenimiento y se estiman los recursos humanos necesarios para el servicio establecido, definiendo sus perfiles, asignando responsabilidades y determinando las funciones que van a llevar a cabo, con el fin de garantizar la coordinación en la gestión del mantenimiento[1163]. Sin embargo, hay que recordar aquí el problema de la pérdida de la garantía si se altera el *software* antes de su finalización, lo que provoca, con relativa frecuencia, que la Administración tenga que incluir en el contrato de desarrollo, al menos, un año de mantenimiento, lo que lo encarece. Finalizado el plazo de garantía o el contrato de mantenimiento, los servicios informáticos de la propia Administración ya pueden libremente hacerse cargo del mantenimiento del mismo, no exento de dificultades añadidas por no haber participado en el desarrollo inicial.

[1161] MAP. Métrica V3. Implantación y aceptación del sistema, 15-17.
[1162] MAP. Métrica V3. Implantación y aceptación del sistema, 17-18.
[1163] MAP. Métrica V3. Implantación y aceptación del sistema, 19.

La actividad IAS 8 contempla el establecimiento de los acuerdos de nivel de servicio para cada uno de los subsistemas. Con ellos se determinan los servicios requeridos, los niveles con los que se va a valorar la calidad de esa prestación y los compromisos adquiridos. La negociación se realiza entre los máximos responsables del usuario y de operación, quienes establecen formalmente el acuerdo de nivel de servicio, considerando los recursos necesarios, plazos de restablecimiento del servicio, coste y mecanismos de regulación. Esos acuerdos abarcan aspectos como el tiempo de respuesta, rendimiento, disponibilidad, planificación y reanudación de trabajos, prerrequisitos y condiciones de ejecución, condiciones de rearranque, gestión y control de red, estaciones de trabajo locales, vigilancia del uso no autorizado de sistemas, redes y *software*, garantía y restauración de la disponibilidad de sistemas y funciones, gestión de la capacidad, etc. Para cada tipo de servicio se detallan sus propiedades funcionales y se especifican las propiedades de calidad que constituyen el nivel de servicio y que permiten su valoración, que estarán relacionadas con la eficiencia, fiabilidad y facilidad de uso, entre otros. La estimación de los recursos humanos necesarios para prestar el servicio con el nivel de calidad deseado debería especificar la cantidad y perfil de las personas requeridas y su responsabilidad, determinando los niveles de cualificación necesarios.[1164]

De nuevo, como es habitual al aproximarse a la finalización de un proceso, el responsable de seguridad, el jefe de proyecto y el comité de seguimiento estudian los productos

[1164] MAP. Métrica V3. Implantación y aceptación del sistema, 19-21.

generados durante el proceso IAS y determinan el nivel de seguridad de cada uno de ellos con respecto a la autenticación, confidencialidad, integridad y disponibilidad.[1165]

Si las pruebas de implantación no se han realizado en el entorno de producción, el equipo de seguridad deberá asegurar de nuevo que se cubren las medidas de seguridad esenciales sobre ese entorno definitivo, teniendo en cuenta el control y registro de incidentes y la respuesta dada a los mismos, lo que podría suponer volver a etapas previas para resolver los problemas detectados.[1166]

Para formalizar la aprobación del sistema, IAS 9 prevé una presentación general del sistema al comité de dirección, a quienes se hace entrega de la información recopilada del sistema (evaluación de las pruebas, acuerdo de nivel de servicio y plan de mantenimiento), esperando su aprobación formal[1167]. Cabe señalar la diferencia con los procesos anteriores, en los que la aceptación o rechazo se encomendaba al comité de seguimiento, no al de dirección.

Tras la aprobación del comité de dirección, IAS 10 marca el punto en que el sistema pasa a producción, se traspasa la responsabilidad al equipo de mantenimiento[1168] y se empieza a dar los servicios establecidos en el ANS. Si las pruebas de implantación y aceptación del sistema no se han realizado en el entorno de producción, habrá que determinar la fecha para la activación del sistema y eliminación del antiguo, si existiera, estableciendo cómo se va a llevar a cabo la transición de uno a otro. Se tendrá que instalar los componentes del sistema total o parcialmente, migrar todos los datos o una parte de ellos (valorando la necesidad de realizar una

[1165] *Vid*. MAP. Métrica V3. Interfaz de seguridad, 43.
[1166] MAP. Métrica V3. Interfaz de seguridad, 44.
[1167] MAP. Métrica V3. Implantación y aceptación del sistema, 22-23.
[1168] Con la salvedad comentada sobre la pérdida de la garantía.

nueva carga, una inicialización o una restauración) y comprobar que la instalación del sistema es correcta. Con el arranque en producción se activará tanto el proceso de mantenimiento como los servicios que se van a prestar.[1169]

El aumento de la externalización se refleja en la mayor importancia que están cobrando las actividades relacionadas con la calidad del *software*, al volverse necesarios la evaluación y control de los productos entregados por las empresas desarrolladoras. No es suficiente que estas empresas cuenten con certificaciones basadas en los procesos seguidos para la obtención del *software*, sino que han de basarse en evidencias directas del propio producto pues, tras su implantación en la instalación, pueden ponerse de manifiesto graves problemas de calidad[1170] y complicaciones a la hora de corregirlo, adaptarlo o evolucionarlo. Por tanto, el aumento de los riesgos en las operaciones de *outsourcing* y la falta de control sobre el *software* recibido, dispara la necesidad de su evaluación y del aseguramiento de su calidad, abriendo un campo de gran actividad investigadora donde las propuestas de normas y estándares están en ebullición, sin que se haya alcanzado todavía un consenso definitivo. Analizado el estado del arte en la materia, la mayoría de los estudios señalan la necesidad de que la certificación de los procesos de desarrollo del *software* se extienda a las características del propio producto, para lo que ya existen varias propuestas, pero con un número muy reducido de aplicaciones reales, las cuales coinciden en la importancia de disponer de herramientas que automaticen las actividades[1171].

[1169] MAP. Métrica V3. Implantación y aceptación del sistema, 23-24.
[1170] FERNÁNDEZ SÁNCHEZ, C.M./ RODRÍGUEZ MONJE, M./ PIATTINI VELTHUIS, M.G. (2013), calidad del producto *software*, 31-32.
[1171] RODRÍGUEZ, M./ PEDREIRA, Ó./ FERNÁNDEZ, C.M. (2015), certificación de la mantenibilidad, 127-128.

El artículo 41.2 de la ley 40/2015 desconoce el proceso de implantación y aceptación, pero sí se preocupa de indicar que "*en caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes (…) para (…), en su caso, la auditoría del sistema de información y de su código fuente*". Sin embargo, no especifica ningún criterio que indique cuándo es conveniente, mucho menos necesario, realizar una auditoría[1172]. En cualquier caso, el órgano auditor del sistema de información deberá ser independiente del que tenga asignadas las funciones TIC y contar con autoridad y acceso no restringido a la información requerida para el ejercicio de sus funciones[1173]. Entre los procedimientos y técnicas empleados por el auditor se incluye la revisión de los programas, incluido su código fuente, persiguiendo el objetivo de obtener un conocimiento detallado de su operatividad, comprender los tratamientos realizados, detectar errores en la interpretación e implantación de las especificaciones funcionales y garantizar la existencia y funcionamiento de los controles oportunos. Esta técnica se convierte en inabordable si los programas no están bien modulados y suficientemente documentados, carencias que ya ponen de manifiesto su debilidad y que apuntan a dificultades e introducción de errores en el mantenimiento de los mismos. Habida cuenta del gran consumo de recursos que implica la revisión de los programas, por lo que se ha de seleccionar muy cuidadosamente los programas a inspeccionar, centrándose exclusivamente en los que sean críticos.[1174]

[1172] En materia de auditoría de sistemas informáticos, resulta imprescindible la consulta de la *web* dela asociación de auditoría y control de sistemas de información, ISACA, www.isaca.org
[1173] RODRÍGUEZ RIVADULLA, F. (Mayo-junio, 2006), reto para los profesionales TIC, 4.
[1174] AMADOR CONTRA, P. (2001), auditoría informática, 519-520.

7.3.7. Mantenimiento del sistema de información

Mientras los programas están en la fase de explotación, es preciso implementar una función de vigilancia de las normas jurídicas, para detectar las derogaciones con tiempo suficiente para actualizar el sistema o, en su defecto, para detenerlo[1175].

Métrica V3 señala la importancia de contemplar las cuestiones de seguridad también en el proceso de mantenimiento, en la toma de decisiones ante las peticiones de desarrollo de nuevas funcionalidades o de modificación de otra ya existente. La seguridad debe ser un parámetro más a contemplar en el análisis y evaluación de soluciones. Como en los procesos anteriores, también al inicio del MSI, el responsable de seguridad, junto con su equipo, estudia la necesidad de supervisar los niveles de niveles de autenticación, confidencialidad, integridad y disponibilidad de los productos generados en las actividades del proceso, estableciendo el control de la seguridad en las actividades tanto a nivel de ejecución como de los productos obtenidos.[1176]

El grupo de aseguramiento de calidad debe efectuar revisiones para constatar la realización correcta de las operaciones de mantenimiento. Ello puede requerir la revisión puntual del contenido y la ejecución del plan de pruebas de regresión y de las verificaciones y casos de prueba incluidos en el plan de pruebas previsto para los cambios desencadenados por la petición.

[1175] ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011), actuación administrativa automatizada, 32.
[1176] MAP. Métrica V3. Interfaz de seguridad, 45-46.

También podrá requerir el examen de las incidencias detectadas por si alguna pudiera tener repercusión en la calidad.[1177]

De los tipos de mantenimiento ya descritos s*upra*, Métrica V3 solo considera los tipos correctivo y evolutivo, excluyendo, en consecuencia, al adaptativo y al perfectivo, que abarcan actividades como la migración y la retirada de *software*, que precisarían el desarrollo de un tipo de metodología específica para resolver su cometido[1178].

Las tareas a realizar dependen de los componentes del sistema afectados por la modificación, pudiendo pertenecer a actividades de los procesos de análisis, diseño, construcción e implantación; en cualquier caso, antes de la aceptación del usuario, es preciso establecer un plan de pruebas de regresión que asegure la integridad del sistema de información afectado.[1179]

[1177] MAP. Métrica V3. Aseguramiento de la calidad, 37.
[1178] MAP. Métrica V3. Introducción, 12.
[1179] MAP. Métrica V3. Mantenimiento del sistema de información, 1.

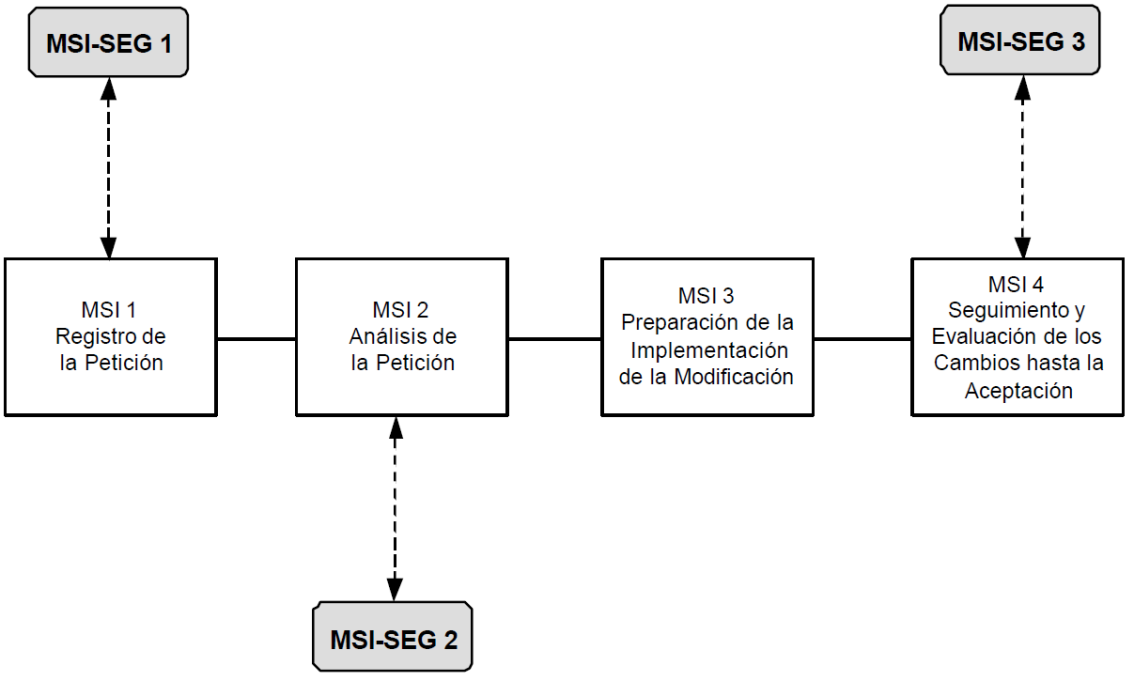

Figura 31: Actividades de MSI

Fuente: Metodología Métrica versión 3. Interfaz de seguridad, 45.

Debe existir un sistema estandarizado de registro y gestión de peticiones de mantenimiento que permita controlar y canalizar los cambios propuestos por el usuario, que evite aquellos que beneficien a uno produciendo un impacto negativo sobre otros muchos.

Se creará un catálogo de peticiones que sirva de base para abordar su análisis y la realización del cambio solicitado, junto con la obtención de información estadística. Para el mantenimiento correctivo, se incluirá toda la información disponible que pueda ayudar a su resolución. Para peticiones de mejora se remitirá una especificación de los requisitos a contemplar. En ambos casos se le asigna una prioridad inicial y se le incorpora una descripción

lo más precisa posible, que facilite su posterior análisis. Una vez determinado el tipo de mantenimiento requerido, hay que identificar los sistemas inicialmente afectados por petición y comprobar que el servicio necesario está previsto en el plan de mantenimiento, según lo cual se acepta o rechaza la petición, se notifica a quien corresponda y, en su caso, se determina quién ha de atenderla.[1180]

El equipo de seguridad y su responsable estudian la petición, viendo sus posibles efectos, en cuyo caso se especifican las funciones y mecanismos de seguridad a incorporar en el mantenimiento. Si el motivo de la petición es un fallo interno en materia de seguridad o un ataque externo, adoptarán las medidas oportunas para paliarlo. Señala Métrica V3 la importancia de tener en cuenta en el fututo cualquier petición de cambio originada por problemas de seguridad, con el objetivo de que toda la organización se beneficie de esa experiencia. Habrá que revisar la selección de las funciones de seguridad realizada en el proceso ASI y comprobar si se requiere la implantación de alguna adicional o la modificación de las ya existentes.[1181]

Las peticiones aceptadas son analizadas para determinar la necesidad de desviar la petición hacia el proceso EVS o hacia el ASI. Si se trata de un mantenimiento correctivo por un error crítico, debe abordarse el cambio de inmediato, postergando la profundización en el origen del mismo hasta que se haya reanudado el servicio. Si el mantenimiento es evolutivo, se analiza si se trata de una modificación o una incorporación de nuevas funcionalidades[1182].

[1180] MAP. Métrica V3. Mantenimiento del sistema de información, 4-5.
[1181] *Vid*. MAP. Métrica V3. Interfaz de seguridad, 47-48.
[1182] MAP. Métrica V3. Mantenimiento del sistema de información, 5.

También se estudian las diferentes peticiones para determinar cuáles se pueden resolver juntas, cómo interaccionan y en qué orden tratarlas, junto con el impacto que la modificación puede provocar en el entorno tecnológico y en los niveles de servicio inicialmente acordados[1183].

En los mantenimientos evolutivos ha de tenerse en cuenta la política de versiones vigente y ver si se ha de llevar a cabo algunas actividades del proceso ASI o del EVS, atendiendo a los requisitos a cubrir, al alcance de la modificación, a las implicaciones en el entorno tecnológico, al ciclo de vida estimado para los sistemas de información afectados, así como a la existencia de opciones de mercado más idóneas.[1184]

Si el mantenimiento es correctivo de emergencia, no se cerrará la incidencia hasta comprobar que ningún sistema se ha visto comprometido, o bien que, después de haber aplicado y probado una solución a corto/medio plazo, el sistema conserva su integridad y operatividad, lo que exige que, tras reanudar el servicio, haya que detectar el origen del problema y asegurar que los cambios introducidos no generan otros de mayor envergadura o comprometen el correcto funcionamiento de otros sistemas de información relacionados[1185].

Si se considera necesario, hay que proponer alternativas de solución para dar respuesta de forma satisfactoria a los requisitos planteados o problemas detectados, determinando una fecha límite de implantación y un coste aproximado, eligiendo, junto con el

[1183] MAP. Métrica V3. Mantenimiento del sistema de información, 6-7.
[1184] MAP. Métrica V3. Mantenimiento del sistema de información, 7.
[1185] MAP. Métrica V3. Mantenimiento del sistema de información, 7.

usuario, la solución más adecuada, y obteniendo la aprobación o rechazo de la petición. En caso de rechazo, la petición se da por cerrada en el catálogo[1186].

En MSI 3 se prepara la implementación de la modificación, comenzando por realizar un análisis de impacto para determinar qué parte del sistema se ve afectado y en qué medida. Ello permitirá identificar las actividades y tareas de los procesos de desarrollo EVS, ASI, DSI, CSI e IAS a realizar en función de las características, complejidad y alcance de la petición, así como fijar un plan de acción y asociar los elementos afectados a cada petición, lo que permitirá el control de la gestión del cambio sobre un mismo elemento. En el plan de trabajo se determina el coste asociado, los plazos estimados para su implementación con las fechas de comienzo y fin, la composición del equipo de trabajo inicial necesario y el nivel de esfuerzo requerido. Se activan los procesos de desarrollo y se especifican las pruebas de regresión con el fin de evitar el efecto onda, de forma que los cambios provocados por una petición no introduzcan un comportamiento no deseado o errores adicionales en otros componentes. Por ello, se deben especificar los casos de prueba en función de las relaciones existentes entre los distintos componentes, que aseguren que la nueva versión satisface las necesidades sin afectar a otros sistemas.[1187]

En la actividad MSI 4 se comprueba que solo se han modificado los elementos adecuados y que se han realizado las pruebas unitarias, de integración y del sistema. Es importante llevar el control de los distintos desarrollos existentes en paralelo sobre un mismo componente y asegurar que en el paso a producción se implantan correctamente. También se

[1186] MAP. Métrica V3. Mantenimiento del sistema de información, 7.
[1187] MAP. Métrica V3. Mantenimiento del sistema de información, 8-10.

realizan las pruebas de regresión, comprobando que ningún sistema no modificado y con posibilidades de verse afectado haya variado su comportamiento. Los problemas detectados se recogen en un informe de incidencias que se remite a quien corresponda para que tome las medidas correctivas oportunas. De no haber problemas, se aprueba formalmente la finalización y se actualiza el catálogo de peticiones anotando el cierre, registrando datos cuantitativos relativos a los recursos empleados, de cara a disponer de una base cuantitativa sobre la que tomar decisiones relativas a la eficacia de las técnicas y procedimientos de mantenimiento.[1188]

Finalmente, el responsable de seguridad y el jefe de proyecto estudian los productos generados durante el proceso MSI y determinan el nivel de seguridad de cada uno de ellos con respecto a la autenticación, confidencialidad, integridad y disponibilidad.[1189]

El mantenimiento del *software* consume la mayor parte de los recursos empleados en un proyecto, más del 60%, razón por la cual es prioritario construir aplicaciones que sean fácilmente mantenibles, lo que debe plasmarse en los productos generados desde las primeras etapas del ciclo de vida. Con frecuencia las empresas de *software* intentan minimizar sus gastos, buscando la máxima productividad en la etapa de desarrollo, relegando a un segundo término la facilidad de mantenimiento futura, operación que, con mucha frecuencia, ya no les afecta, pues la realizan otros. Cuando la productividad del proceso de mantenimiento es baja, puede consumir la totalidad de la jornada de trabajo de los integrantes del equipo que lo desarrolló, impidiéndoles asumir otros proyectos, obligando a la empresa a ampliar su plantilla con un nuevo equipo,

[1188] MAP. Métrica V3. Mantenimiento del sistema de información, 10-12.
[1189] *Vid*. MAP. Métrica V3. Interfaz de seguridad, 49-50.

probablemente carente de la experiencia del anterior[1190]. Resulta sencillo imaginar cómo empeora la situación cuando el equipo encargado de mantener la aplicación no intervino en su desarrollo.

Con fundamento en el modelo COCOMO de Boehm, se han desarrollado propuestas para medir la facilidad de mantenimiento del *software*, considerando dividido ese esfuerzo en tres componentes[1191]: el necesario para comprender el problema, el que va unido a la elaboración de la propia modificación y el que suponen sus pruebas. Por tanto, el índice que nos indica la facilidad de mantenimiento se define como la suma de otros tres, relacionados con la comprensión, modificación y prueba. La primera siempre es más alta cuando el mantenimiento lo realiza el mismo equipo que desarrolló el programa.

7.4. LA OPCIÓN DE EXTERNALIZACIÓN DEL DESARROLLO DEL *SOFTWARE* DE LAS ADMINISTRACIONES PÚBLICAS

Desde finales del siglo pasado estamos siendo testigos de un traslado masivo de labores del Estado, realizadas directa o indirectamente por sus Administraciones, hacia la sociedad[1192]. Ante el avance de los diferentes procesos de privatización, con la transferencia al ámbito privado de funciones que antes correspondían al sector público, a este le corresponde ahora la utilización de sus poderes de regulación y vigilancia para garantizar la realización de los intereses generales allí donde estos pudiesen verse afectados[1193]. Estamos ante un Estado garante que, mediante las oportunas medidas normativas y organizativas, debe garantizar los servicios de

[1190] GRANJA ÁLVAREZ, J.C. (2001), auditoría del mantenimiento, 295-296.
[1191] GRANJA ÁLVAREZ, J.C. (2001), auditoría del mantenimiento, 297-309.
[1192] ESTEVE PARDO, J. (2014), contractualización, 1231.
[1193] CARRO FERNÁNDEZ-VALMAYOR, J.L. (2014), reflexiones, 31.

carácter esencial ahora gestionados por sujetos privados[1194]. Pero, entre esos sujetos privados, pueden establecerse diferencias. Las entidades privadas colaboradoras de la Administración en el ejercicio de funciones públicas se caracterizan por su imparcialidad y objetividad, cualidades esenciales que se predican de la actividad administrativa y que son trasladadas a la actuación de estos sujetos privados[1195]. Sin embargo, esas mismas exigencias no son predicables de las empresas del sector privado que trabajan para la Administración en virtud de contratos de servicios para el desarrollo de *software*.

En el ámbito informático, el *outsourcing* se presenta como una actividad en alza que ha calado incluso en las empresas más grandes. En nuestro país, en el año 2010, generó 4.418 millones de euros, calculándose un crecimiento anual de entre 5 y 8% hasta 2016[1196]. Los estudios sobre las razones que lo hacen brillar con fuerza y los riesgos que se esconden en su faz oscura han proliferado en la literatura dedicada a esta materia, exhaustivamente recopilada y valorada por González, Gascó y Llopis en 2010 y revisada en 2015[1197]. Pero se ha de tener en cuenta que la externalización de las TIC muestra matices particulares que la hacen única en comparación con el resto de objetivos, con implicaciones en la forma de gestionarla y llevarla a cabo[1198]. Incluso dentro de ese mismo sector tecnológico, el *outsourcing* del desarrollo del *software* presenta especialidades que obligan a analizar los pros y los contras centrados específicamente en esta materia. Igualmente, aparecen diferencias en el modo de enfrentarse a la

[1194] CARRO FERNÁNDEZ-VALMAYOR, J.L. (2014), reflexiones, 35.
[1195] GALÁN GALÁN, A./ PRIETO ROMERO, C. (2008), funciones públicas, 75.
[1196] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 176.
[1197] *Vid*. también GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2010), situación y evolución, 55-76.
[1198] COX, M./ ROBERTS, M./ WALTON, J. (2011), *IT Outsourcing*, 194.

externalización en el sector privado y en el público, ambos muy diferentes ideológica y operativamente[1199]. En el ámbito público implica una decisión voluntaria y reflexiva de la Administración y una transferencia de funciones a un tercero privado, lo que deja fuera del concepto aquellas que vienen impuestas por el Derecho comunitario o por el propio legislador estatal[1200], como es el caso de la colaboración privada en el ejercicio de funciones de autoridad[1201].

Dado que la motivación del sector público no consiste en la búsqueda del rendimiento financiero, sus directivos pueden plantearse objetivos y considerar valores distintos al ahorro en costes, algo que podría dar lugar a un enfoque más cauteloso, que se oriente a la minimización de riesgos[1202], acorde con la imagen tradicional del funcionario, caracterizado por el aprecio de la seguridad como modo de vida. Por ello, no todos los argumentos en defensa o en crítica de la externalización mantendrán aquí su aplicabilidad de la misma forma para los sectores público y privado, por lo que procede revisarlos individualmente, centrándose en organismos con capacidad de elección entre externalizar el desarrollo o no hacerlo, opción que sería impensable en entidades de tamaño muy pequeño que no cuenten con unos recursos TIC humanos y materiales mínimos.

[1199] COX, M./ ROBERTS, M./ WALTON, J. (2011), *IT Outsourcing*, 194.
[1200] CANTERO MARTÍNEZ, J. (2011), la sustitución, 6.
[1201] *Vid*. RIDAURA MARTÍNEZ, M.J. (2014), seguridad ciudadana, donde se analiza detenidamente el entramado constitucional que reserva las funciones esenciales de garantía de la seguridad ciudadana a las fuerzas y cuerpos de seguridad, permitiendo la colaboración y auxilio de agentes externos, como se desprende de la legislación de desarrollo, sin entrañar la asunción de funciones que afecten a los derechos fundamentales.
[1202] COX, M./ ROBERTS, M./ WALTON, J. (2011), *IT Outsourcing*, 194.

7.4.1. Análisis de los argumentos a favor y en contra de la externalización

Mediante la externalización de funciones, la Administración confía a sujetos privados ajenos a su organización la realización de determinadas funciones administrativas, suponiendo la sustitución del empleado público por el trabajador privado, bajo la creencia generalizada de que el coste de esta alternativa es menor y constituye un factor de eficacia y eficiencia[1203]. La **reducción de los costes de personal** se encuentra entre las justificaciones más repetidas[1204], argumento que apunta en la misma dirección que la prohibición de incorporar nuevo personal fijo en nuestras Administraciones, sufrida durante los últimos años y ya comentada, que ha empobrecido nuestras plantillas y puesto en dificultades a muchos servicios públicos. Pero no se debe olvidar que el ahorro en capítulo I a costa de incrementar otros capítulos de los presupuestos no redunda en un beneficio a las arcas públicas, y que los gastos supuestos por los trabajadores externos son superiores a los del personal propio. De hecho, llevado al campo concreto del desarrollo del *software* de nuestras Administraciones, ya se expuso *supra* que el coste de un técnico medio informático externo es casi 16.000 € anuales superior al de su equivalente funcionario, diferencia que asciende a casi 22.000 € anuales para el caso del técnico superior. A mayor abundamiento, resulta obligado reiterar la moción del Tribunal de Cuentas donde se recomienda el incremento de las plantillas de personal con cualificación informática y la limitación consecuente de la contratación externa[1205]. Con respecto

[1203] CANTERO MARTÍNEZ, J. (2011), la sustitución, 1.
[1204] Podría incluirse en el ahorro los gastos asociados al espacio físico que ocupan y al consumo de electricidad, teléfono, calefacción…
[1205] Con fecha 27 de febrero de 2017, el Tribunal de Cuentas continúa pronunciándose en sentido similar, alertando de la cautividad tecnológica que genera dependencia de un proveedor concreto y de la insuficiencia del personal

al reciclaje constante que requiere el trabajador informático, sin perjuicio de reivindicar el uso de la técnica del *mentoring* en toda ocasión posible, es preciso recordar que la Administración ya cuenta con organismos dedicados a la formación de empleados públicos y una oferta de calidad envidiable por las empresas del sector privado[1206], que cubren las áreas de organización y gestión de los sistemas de información, de redes, comunicaciones e Internet, de programación y lenguajes, de seguridad de sistemas y de herramientas informáticas, a las que se suma la formación en seguridad en TIC realizada en colaboración con el CCN. La sustitución del trabajador TIC público por personal externo podría reducir el número de asistentes a dichos cursos y, con ello, una disminución clara del capital intelectual, pero no producirá un ahorro apreciable en gastos de formación. En cualquier caso, la economía que pudiera generar en cuanto a la preparación y actualización del personal técnico se perderá en los "costes ocultos"[1207]. Además del importe del contrato, IVA incluido, han de tenerse en cuenta otros gastos presentes en la externalización, como los asociados al procedimiento de licitación, los costes de transacción entre cliente y proveedor, los asociados a la coordinación y control e, incluso, los de un posible *insourcing*. Además del tiempo y el esfuerzo requerido por la coordinación y comunicación con el proveedor, será preciso gestionar las interdependencias entre los servicios externalizados y los internos, o entre diferentes servicios externalizados.[1208]

---

propio de la GISS. http://www.europapress.es/economia/noticia-tribunal-cuentas-insta-administracion-utilizar-sistemas-informaticos-abiertos-ser-mas-baratos-20170227121334.html (accedido el 21 de marzo de 2017).

[1206] *Vid*. http://www.inap.es/formacion-en-tic (accedido el 21 de enero de 2017).

[1207] Concepto definido por Barthélemy en 2001. *Vid* GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 182.

[1208] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 180-182.

Otro argumento tradicional a favor del *outsourcing* orbita alrededor del **ahorro en costes de tecnología** debido a las economías de escala que pueden conseguir los proveedores de servicios. Aplicado al desarrollo del *software* a utilizar en las Administraciones públicas, alcanza toda su potencialidad en las clásicas herramientas ofimáticas. El desarrollo por empleados públicos de un procesador de textos carece totalmente de fundamento, habida cuenta de que siempre será muchísimo más caro que la adquisición de paquetes ofimáticos como Microsoft Office o similares que, como se afirmó *supra*, ganarán en aptitud técnica y la satisfacción de requisitos, al tratarse de productos que ya se encuentren ampliamente implantados en la sociedad, y no solo en el sector público, sino también entre los particulares y en empresas privadas. Por el contrario, al enfrentarse al desarrollo de aplicaciones realizadas a medida para dar servicio a necesidades específicas de nuestras Administraciones públicas, como podría ser la obtención de una aplicación de gestión de la selección y provisión del personal funcionario y laboral a su servicio, el aprovechamiento de las economías de escala no juega a favor de la externalización, pues si tal *software* puede ser reutilizado por otros organismos públicos, los beneficios no recaerán fuera de las arcas públicas, sino directamente dentro de ellas.

Se afirma que la externalización conlleva la **mejora de la calidad**, al complementar los recursos técnicos y humanos del cliente con las tecnologías avanzadas a las que puede tener acceso el proveedor y con un personal motivado y especializado que centra su carrera profesional en servicios de alto nivel[1209]. Sin embargo, la Administración que duda entre la externalización del desarrollo de su *software* o su producción con medios propios también

[1209] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 176.

puede acceder a las mejores tecnologías y contar con cuerpos de funcionarios especializados cuya proceso de selección, descrito anteriormente, se somete a unos principios de publicidad, igualdad, mérito y capacidad poco o nada comparables a los que permiten el acceso a puestos de trabajo del sector privado. A ello hay que añadir, como se señaló *supra*, que la materialización del plan de calidad tiene un coste adicional notable, lo que justifica cuestionarse si las empresas privadas, movidas por su propio beneficio económico, son valedoras de esa supuesta calidad superior a la proporcionada por los servicios informáticos de la Administración, orientados al servicio público. El incremento de calidad y la reducción de costes se mueven en sentidos opuestos, y una de las formas de disminuir gastos con la externalización se fundamenta en que el proveedor externo tiene "*mejor acceso a mano de obra a bajo costo*"[1210], afirmación que apunta más hacia la contratación de becarios que a la de personal especializado en servicios de alto nivel que reiteradamente se esgrime a favor del *outsourcing*[1211] y que da pie a plantearse el problema de la **cualificación del personal**, cuya importancia ya se comentó *supra*. Sin embargo, incluso si el personal externo está altamente cualificado, las consecuencias para la Administración pueden ser negativas, si el personal clave pertenece al sector privado. En la creación de aplicaciones de cierta complejidad e importancia, el saber adquirido por el equipo desarrollador externo va inherentemente unido a la privación de esa misma experiencia por parte de los empleados públicos, generando una **dependencia de la empresa externa y pérdida del control y del**

[1210] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 179. *Vid*. razones esgrimidas por Smith et al. (1998) en tabla 1.

[1211] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 177-179. *Vid*. tabla 1, donde se recoge la misma idea bajo diferentes descripciones: el acceso a personal de alto nivel, defendida por Alner (2001), el acceso a expertos y la evitación de problemas de reclutamiento, formulada por Cox et al. (2011), el beneficio de la competencia de los proveedores, esgrimida por Grover y Teng (1993), la habilidad para acceder a los mejores conocimientos y capacidades y ls transferencia del *know how* del proveedor al cliente, alegadas por Harland et al. (2005) o el acceso a expertos TIC, señalada por Jurison.(1995).

conocimiento, que conlleva un descuido de las mejoras internas y de la formación del personal propio. Por ello, conviene no externalizar servicios esenciales que puedan escapar así del control público.

Al margen de las tensiones y dificultades que puede suscitar la convivencia de personal involucrado en el proyecto, procedente de distinto origen, con régimen jurídico diverso y diferencias económicas y laborales[1212], hay que analizar **otros problemas de personal**. El sector privado tiende a pagar salarios más altos, por lo que los organismos públicos podrían encontrarse con dificultades para atraer a la gente con las mejores habilidades[1213]. Pero en épocas de crisis prolongadas, e incluso en ausencia de ellas, la seguridad del empleo público muestra un poderoso atractivo. Combinado con la dureza de las pruebas selectivas, especialmente si están bien diseñadas, proporciona unos recursos humanos altamente competentes que, ante la externalización de las funciones que han sido tradicionalmente suyas, pueden optar a mantenerse en el cuerpo de funcionarios en el cual prestan servicio únicamente por la consideración de su seguridad laboral, pero sumidos en el desánimo y la preocupación por las posibles modificaciones en sus tareas y las consecuencias negativas sobre su esfera personal y profesional[1214]. La situación de incertidumbre que genera la externalización puede desencadenar disminuciones de productividad, pérdida de motivación, baja moral, ansiedad, inseguridad… Cuando el personal del departamento de informática se siente amenazado por el *outsourcing*, es

[1212] ALLÍ ARANGUREN, J.C. (2006), nuevas formas, 133.
[1213] COX, M./ ROBERTS, M./ WALTON, J. (2011), IT Outsourcing, 196.
[1214] La STC 112/2004 reconoce la afección de la esfera económica y profesional de los empleados públicos como consecuencia de la externalización de labores informáticas, en particular, la carrera administrativa, los ámbitos de trabajo, las perspectivas de formación o las posibilidades de promoción o traslado. En su FJ5 concluye la existencia de un "*interés de los empleados públicos en que los servicios de apoyo informático que se pretenden contratar al exterior sean realizados por empleados públicos* ".

esperable cierta oposición[1215]. Es posible que algunos de ellos se trasladen a la empresa de servicios voluntariamente. Los que permanezcan, pueden cambiar sus responsabilidades, realizando trabajos distintos a los que estaban habituados[1216].

El **aumento de la flexibilidad** ante la variabilidad del volumen de trabajo que recaiga sobre el departamento de informática sí favorece claramente al *outsourcing* con respecto al desarrollo por medios propios. Solo es preciso licitar un contrato de servicios cuando surge la necesidad de desarrollar o mantener una aplicación, pudiendo así afrontar las fluctuaciones en los niveles de trabajo. La plantilla de funcionarios presenta una menor elasticidad y las sobrecargas únicamente pueden afrontarse con la cobertura de las vacantes dotadas a través de la contratación de personal interino o, de forma alternativa, mediante el recurso puntual a la externalización. Por otra parte, la licitación de un contrato de mantenimiento de la totalidad de las aplicaciones implantadas en un organismo público permite transferir el riesgo asociado a la demanda creciente de servicios hacia el sector privado.

Tradicionalmente se ha defendido el **desprendimiento de las tareas rutinarias para centrarse en temas estratégicos**, es decir, la externalización de lo más superfluo, de las tareas rutinarias, carentes de valor añadido, especialmente las que son una molestia o una función problemática a minimizar o eliminar, para poder trasladar recursos a las funciones básicas. Entre las aplicaciones a desarrollar habrá algunas de poca envergadura, cuyos efectos carezcan de trascendencia, sin que puedan generar repercusiones de importancia, las cuales podrían ser las

[1215] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 182.
[1216] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2010), situación y evolución, 61.

primeras candidatas a ser externalizadas, pero habría que meditar detenidamente la conveniencia o no de externalizar aquellas aplicaciones llamadas a implementar actuaciones administrativas automatizadas, a tratar datos especialmente sensibles o que puedan generar sobre la ciudadanía repercusiones difícilmente reparables.

La afirmación de que los proveedores pueden realizar el **trabajo más rápido** por ser expertos en el desarrollo[1217] no parece adaptarse al presupuesto de una Administración pública dotada de un departamento informático que asume la creación de sus propios programas. La externalización implica el ajuste a un procedimiento de licitación que incrementará el tiempo necesario para alcanzar la implantación y aceptación del nuevo sistema.

Aplicando **consideraciones técnicas**, el *outsourcing* puede verse motivado por una carencia de experiencia entre los empleados públicos en una determinada tecnología. La organización administrativa puede carecer de la experiencia técnica necesaria para introducir una nueva tecnología concreta por primera vez, prefiriendo contratar los servicios de una empresa que posea ya ese conocimiento, aprendiendo así sobre el terreno para poder asumir los desarrollos futuros.

No se puede ignorar la influencia de **factores del entorno** en la decisión. Existe una cierta propensión a seguir la moda e imitar la tendencia a la externalización de otras organizaciones, con el apoyo de la prensa económica y la presión de las propias empresas de servicios. Esos factores, en ocasiones tienen una base política. Así, la evaluación de las ofertas recibidas en una licitación para externalizar un proyecto puede utilizarse como herramienta para

[1217] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 178. *Vid*. razones esgrimidas por Jurison (1995).

probar la eficiencia del departamento de informática, demostrando con ello que el desarrollo por medios propios resulta más económico, justificando así ampliaciones de recursos humanos y materiales.[1218]

Como ponen de manifiesto los distintos medios de información, nuestro país, al igual que otras naciones de nuestro entorno, no es ajeno a los **fenómenos de corrupción**[1219] en la adjudicación y ejecución de los contratos públicos, un ámbito proclive a tales prácticas a consecuencia de los elevados recursos que mueve, especialmente si comporta una cierta complejidad tecnológica que pueda facilitar la ocultación de las prácticas corruptas. La ausencia de una competencia real en el proceso contractual ocasiona el aumento del coste en la prestación de servicios y la desviación, por tanto, de los recursos públicos, efectos que resultan más evidentes en épocas de crisis[1220]. Se estima que la ausencia de concurrencia puede elevar en un 25% el presupuesto de contratación pública, lo que podría suponer unos 47.500 millones de euros anuales[1221]. Se han diagnosticado riesgos de corrupción por clientelismo en las adjudicaciones, debido a la influencia y capacidad de presión de grupos de intereses no necesariamente económicos, así como debilidad de los instrumentos públicos de seguimiento y

[1218] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 179.
[1219] *Vid*. MARTÍNEZ FERNÁNDEZ, J.M. (2016), contratación pública y transparencia, obra donde su autor analiza el fenómeno de la corrupción en la contratación pública y propone una serie de medidas, orientadas hacia la transparencia, que encaran el problema en busca de la eficiencia e integridad.
[1220] GIMENO FELIÚ, J.M. (2010), mecanismos de control, 523-526.
[1221] GIMENO FELIÚ, J.M./ MORENO MOLINA, J.A. (dir.). GUERRERO MANSO, C./ FERNÁNDEZ ACEVEDO, R./ GALLEGO CÓRCOLES, I./ LAZO VITORIA, X./ MOREO MARROIG, T./ MEDINA ARNÁIZ, T./ VALCÁRCEL FERNÁNDEZ, P. (30 de enero de 2017), mejora al proyecto, 3.

control, agravado por cláusulas de salvaguarda insuficientes sobre la garantía de la prestación y sus condiciones. También se aprecia dejación por los funcionarios en sus labores.[1222]

Entre las prácticas corruptas patológicas que apunta Gimeno Feliú como habituales, fácilmente aplicables también a los proyectos de desarrollos *software*, hay algunas que nos pueden resultar tristemente familiares:

- Inadecuada planificación de los sistemas de información, en la que se demanden de forma artificiosa servicios que realmente no se necesiten.
- Elaboración de unas especificaciones técnicas especialmente ideadas para favorecer a un determinado licitador.
- Aporte de información a algún licitador a los efectos de proporcionarle ventaja frente a los demás participantes.
- Fraccionamiento del contrato para eludir las reglas establecidas para el proceso de contratación.
- Utilización del contrato menor o del procedimiento negociado indebidamente, como si se tratara de una adjudicación directa.
- Ponderación inadecua de los criterios de adjudicación.
- Ausencia de controles sobre la prestación efectivos, que acaban reflejándose en problemas de calidad.

[1222] ALLÍ ARANGUREN, J.C. (2006), nuevas formas, 133.

- Modificaciones de contratos desproporcionadas y en fraude legal que quiebran los principios de concurrencia, igualdad de trato y selección objetiva del contratista, dañando a su vez, por los sobrecostes que implican, al erario público, pudiendo llegar a pagar finalmente una cantidad que sobrepasa notablemente la más onerosa de las ofertas presentadas[1223].

El recurso a empresas externas con frecuencia va acompañado de **problemas con la especificación de los requerimientos a satisfacer**[1224]. Esas especificaciones técnicas que los describen, a la hora de adquirir impresoras mediante un contrato de suministro, presumiblemente no serán muy complejos y, una vez establecidos, no variarán durante la vigencia del mismo. Sin embargo, la estabilidad no es característica de los requerimientos del *software* que se aportan al licitar un contrato de servicios. Como se indicó *supra* al analizar la tasa de fallos de los programas informáticos, no resulta extraño que estos cambien incluso antes de que hayan sido puestos en producción. A su vez, tampoco resulta sencillo recoger en un pliego de prescripciones técnicas, de forma exhaustiva, todos los requisitos a cumplir por el *software* a desarrollar. A modo de ejemplo, puede citarse una situación que se viene repitiendo con relativa frecuencia tras la entrada en vigor del ENS, concretamente la necesidad de sustituir complejas aplicaciones creadas con Access por otras programadas en lenguajes como Java. Los propios usuarios no saben realmente lo que hace su aplicación ni lo que debe realizar la nueva, solo saben, y pretenden licitar así el contrato de servicios, que necesitan “un programa Java que haga lo mismo que su Access”.

[1223] GIMENO FELIÚ, J.M. (2010), mecanismos de control, 529.
[1224] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 180-182. Los autores recopilan, en su tabla 2, diversos problemas con los requerimientos que se engloban y explican a continuación.

Tales especificaciones técnicas cambiantes, incompletas o carentes de exhaustividad, conducirá con toda probabilidad a modificaciones contractuales que, en caso de controversia, pueden generar además costes judiciales. Esos modificados no deben afectar a ninguna condición que pueda considerarse esencial ni responder a necesidades nuevas o complementarias, que, en principio, deberían ser objeto de licitación independiente, algo no siempre factible debido a la interrelación de los distintos programas entre sí. En cualquier caso, la posibilidad de modificación, indispensable, imprevisible y motivada suficientemente en un interés público, debería haberse advertido expresamente en los pliegos o en el anuncio de licitación, detallando de forma clara, precisa e inequívoca, las condiciones en que podrá realizarse, así como su alcance y límites[1225]. A su vez, el artículo 107 del TRLCSP, rubricado como "modificaciones no previstas en la documentación que rige la licitación", abre la puerta a los cambios originados por la inadecuación de la prestación contratada para satisfacer las necesidades a causa de errores u omisiones padecidos en las especificaciones técnicas, sin que puedan alterarse las condiciones esenciales del contrato, concepto jurídico controvertido que el legislador trata de determinar en su apartado tercero.

Detectados problemas con los requerimientos, el poder de la Administración se pone de manifiesto en prerrogativas como las de interpretar el contrato, aclarar las dudas que puedan surgir, modificarlo o, incluso, resolverlo. En el envés de ese poder aparecen los derechos del contratista[1226], surgiendo la necesidad de mantener un equilibrio entre ambos. Sin embargo, como refiere Melián Gil, el Consejo de Estado ha podido comprobar el uso de dichas

[1225] GIMENO FELIÚ, J.M. (2010), mecanismos de control, 529-531.
[1226] MELIÁN GIL, J.L. (2013), prerrogativas de la Administración, 24.

prerrogativas a iniciativa e interés del contratista[1227], algo que no siempre se ajusta a prácticas manifiestamente corruptas. Con frecuencia, Administración y contratista desarrollan cierta cercanía, familiaridad y confianza, fruto del trabajo diario en colaboración que, si bien facilita el entendimiento para lograr el progreso del proyecto en un entorno de requisitos cambiantes, bordea peligrosamente los límites de la legalidad y relaja las actividades de vigilancia y comprobación por parte del personal de la Administración.

Resulta conveniente en todo contrato público llevar a cabo una gestión pausada del proyecto que conduzca a una ejecución rápida y sin incidentes, así como una regulación adecuada de la responsabilidad de los autores de proyectos y de los responsables de su ejecución[1228].

Aunque las organizaciones se han preocupado siempre por sus propias debilidades para enfrentarse a la externalización, se viene observando un cambio en sus inquietudes, una mayor reticencia ante los riesgos procedentes de la empresa externa, en lo referente a su posible **falta de cumplimiento**. Quizá esa evolución surge como consecuencia de la experiencia acumulada, que lleva a conocer mejor las posibles debilidades de dichas empresas[1229]. Un incumplimiento del proveedor podría llegar a paralizar la actividad empresarial[1230], o la administrativa, en nuestro caso. Esa forzada inactividad no se soluciona por retener o rechazar el pago, ni por aplicar las posibles penalidades acordadas en el contrato. Es más, incluso la determinación de si se ha producido un incumplimiento o no es difícil, tratándose de un contrato

[1227] MELIÁN GIL, J.L. (2013), prerrogativas de la Administración, 17-19.
[1228] GIMENO FELIÚ, J.M. (2013), la modificación, 52.
[1229] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2010), situación y evolución, 72.
[1230] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 43.

de *outsourcing* para el desarrollo de aplicaciones de cierta complejidad[1231]. El incumplimiento puede producirse por motivos diversos, pero no hay que descartar la presentación de una oferta excesivamente baja por parte del proveedor para asegurarse la adjudicación del contrato. Se aprecia cierta tendencia en el sector público a considerar el precio como criterio único de adjudicación, costumbre que puede poner en peligro la calidad[1232].

A su vez, la externalización incrementa los **problemas específicos de seguridad**, en concreto los riesgos de acceso indebido a los sistemas de información y comunicaciones, que pueden afectar a la confidencialidad, al permitir el acceso a las bases de datos o documentos[1233]. También se ha comentado anteriormente el problema del conocimiento de contraseñas que no se cambian cuando el personal abandona la empresa.

Por último, cabe señalar la **difícil reversibilidad** del proceso, especialmente cuando la externalización ha sido total y la vuelta atrás implica reconstruir el departamento de informática.[1234]

[1231] En la STS 4314/2012, de 11de Junio de 2012, se discute el pago de más de 149 millones de pesetas, a una empresa informática contratada para la preparación e instalación de un programa de Gestión Informática de Personal del Gobierno de Canarias. Tras la entrega del producto, se produjeron una serie de vicisitudes motivadas por la complejidad del sistema y la necesidad de dar plena satisfacción a las demandas solicitadas por la Administración. Esta puso de relieve determinadas deficiencias técnicas, algunas calificadas como graves. Un dictamen pericial califica esas quejas de insustanciales. La Sentencia de instancia se funda exclusivamente en el informe pericial para condenar a la Administración al pago de parte de la cantidad reclamada. La STS aprecia indefensión de la Administración por haberse visto privada de la oportunidad de solicitar aclaraciones al informe del perito, quien no consta que inspeccionara directamente el programa y la documentación pertinente.
[1232] COX, M./ ROBERTS, M./ WALTON, J. (2011), IT *Outsourcing*, 194.
[1233] ALLÍ ARANGUREN, J.C. (2006), nuevas formas, 133.
[1234] GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L./ LLOPIS TAVERNER, J. (2015), grandes empresas españolas, 182.

7.4.2. Buena técnica contractual

En el desarrollo de aplicaciones basadas en el tratamiento de datos personales, o durante su selección, ha de alentarse el respecto del derecho a su protección con la debida atención al estado de la técnica, asegurándose también de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en la materia. Los principios de la protección de datos desde el diseño y por defecto también han de tenerse en cuenta en los contratos públicos.[1235]

Los servicios prestados a las Administraciones públicas por terceros afectan a las garantías sobre la seguridad, por las condiciones de contratación y por el seguimiento que se haga de la ejecución de esos contratos, adquiriendo especial importancia el contenido recogido en los pliegos de cláusulas administrativas particulares y en los de prescripciones técnicas, que deben contemplar la atribución de obligaciones y responsabilidades que recaen entre las partes[1236]. Sin embargo, como ya intuye Menéndez Sebastián, "*en los contratos de servicios de prestaciones intelectuales la necesidad de precisar adecuadamente el objeto contractual adquiere matices que lo dificultan* (…)"[1237]. El esmero en la preparación de los pliegos de prescripciones técnicas sin duda repercutirá favorablemente sobre las posibilidades de éxito de la externalización del desarrollo del *software* de nuestras Administraciones. Conscientes de ello, sus redactores se afanan en mejorar la descripción del servicio requerido. En cualquier caso, no

[1235] Considerando 78 del RGPD.
[1236] Introducción a la orden PRE/57/2016, de 14 de septiembre, por la que se regulan las condiciones sobre seguridad de la información y de los sistemas de información a incorporar en los pliegos de cláusulas administrativas particulares y de prescripciones técnicas en la contratación pública de la Administración de la Comunidad autónoma de Cantabria, publicada en el BOC de 30 de septiembre de 2016.
[1237] MENÉNDEZ SEBASTIÁN, E.M. (2009), contratos de servicios del sector público, 519.

es una tarea sencilla, pues la descripción de las necesidades de los usuarios en el pliego requeriría haber realizado ya el proceso de análisis del sistema de información que, precisamente, es una de las tareas que ha de ejecutar la propia empresa adjudicataria. Por tanto, en sistemas complejos, si no existe cierta flexibilidad por ambas partes, existe una elevada probabilidad de que los desacuerdos acaben en los tribunales[1238].

El Derecho irrumpe con fuerza en el modo en que los técnicos informáticos detallan sus necesidades. Hasta hace poco tiempo, un departamento de informática de una Administración que contase con herramientas escritas en un determinado lenguaje de programación como .Net, Java o Natural, que necesitase integrar una nueva aplicación con las preexistentes, que dispusiese de personal formado en ese lenguaje concreto capaz de mantener las aplicaciones existentes y las nuevas adquisiciones, pero sin los suficientes recursos humanos como para desarrollar un nuevo aplicativo desde sus inicios, podía licitar un contrato para el análisis, diseño, construcción e implantación de una nueva aplicación en .Net, o en Java, o en Natural o en el lenguaje concreto que necesitase, conociese, dominase y del que contara con especialistas que lo pudieran mantener. Ahora, nuestro Tribunal Supremo, no llegando a comprender las extensas explicaciones técnicas dadas por la Generalidad de Cataluña, impide licitar un programa en .Net por infracción del artículo 101.2 y 8 de la ley 30/2007, de 30 de octubre, de contratos del sector público[1239]. Por ello, es preciso ser muy escrupuloso en la

[1238] En la STS 4314/2012, de 11 de junio de 2012, se plantea el conflicto entre la Comunidad autónoma de Canarias con la empresa adjudicataria del contrato de desarrollo de una aplicación de gestión de personal, por el derecho a percibir casi 150 millones de las antiguas pesetas. Este caso plantea una situación real que fácilmente puede producirse en la externalización del desarrollo de aplicaciones informáticas de las Administraciones públicas, habida cuenta de la imposibilidad de incluir en el pliego los detalles que posteriormente se dirimirán en el proceso de análisis. Esta problemática no se presentaría si el desarrollo fuese asumido por los propios empleados públicos.

[1239] El artículo 101.2 y 8 de la LCSP pasa a ser el artículo 117.2 y 8del TRLCSP con el mismo tenor.

redacción de las prescripciones técnicas, evitando toda referencia a productos comerciales concretos, directa o indirecta, detallando al máximo nivel las necesidades a cubrir, separando las imprescindibles de las recomendables, y valorando su grado de satisfacción en los criterios de adjudicación. Anticipándose a posibles recursos, convendría exteriorizar los aspectos técnicos que permitan hacer desaparecer los obstáculos a la competencia[1240]. Con respecto a la posible infracción del artículo 101.8 del mismo texto legal, siempre deberá incluirse la mención "o equivalente" y, habida cuenta de que los recursos pueden ser resueltos sin la intervención de peritos informáticos, habrá de motivarse y justificarse hasta el más mínimo detalle, por obvio que pueda parecerle al personal técnico, cualquier falta de equivalencia que pueda existir entre las diferentes soluciones propuestas y la necesitada, con referencia explícita a las consecuencias producidas por las carencias que puedan presentar esas propuestas alternativas. En cualquier caso, sentencias como la citada, muy loables en su intención pero discutibles en su fundamento tecnológico, empujan a las Administraciones públicas a abstenerse de licitar el desarrollo de determinados programas informáticos, depositando dichos encargos en las manos de su propio personal técnico.

En cualquier caso, considero de gran acierto la medida propuesta por Martínez Fernández para fomentar que las prescripciones técnicas garanticen la competencia efectiva: "*exigir al redactor del PPT un informe específico en el que asevere que los requerimientos*

[1240] A modo de ejemplo, relacionado con la STS citada, el hecho de que la plataforma .NET sea utilizada en la Administración y se licite el desarrollo de una aplicación para ella, no supone ningún obstáculo a la competencia en el momento de que al adjudicatario se le permite conectarse a ella a través de una conexión VPN, es decir, es la Administración la que dispone de esa plataforma y cualquier posible adjudicatario podrá conectarse a ella, disponga o no de la misma en sus propias instalaciones. No existe, de ese modo, ninguna restricción a la competencia y no se ve conculcado el artículo 101.2 dela LCSP.

técnicos no restringen la competencia". Si bien no está previsto en la normativa de contratación, cualquier poder adjudicador puede imponerlo en ejercicio de su potestad de normarse.[1241]

Al objeto de alcanzar las máximas ventajas eludiendo los inconvenientes, ha de afrontarse con prudencia la fase precontractual y plasmar los acuerdos en el contrato de una manera clara y exacta, en aras de establecer una relación de confianza en la cual se hayan determinado suficientes criterios de protección de los intereses del cliente y se haya abierto unos canales de comunicación permanente entre las partes, antes, durante y después de la ejecución del servicio acordado.[1242]

La fijación de un único criterio de selección del proveedor, el precio, con frecuencia augura problemas inminentes pues, por lo general, esa competitividad se alcanza contratando personal con menos expectativas salariales y escatimando gastos, como el coste asociado a la calidad, comentado *supra*. Rara vez lo mejor es lo más barato. Por ello, es importante escoger adecuadamente los criterios a definir y, sobre todo, asegurar que el adjudicatario seleccionado es quien realmente ejecute la prestación de servicios. Si bien se recomienda la inclusión de una cláusula que impida la subcontratación salvo consentimiento expreso del cliente, para evitar posteriores conflictos, puede entenderse que su ausencia no obsta al carácter *intuitu personae* del contrato de *outsourcing*, haciendo que la intervención de terceros en el "núcleo duro" del servicio pueda considerarse un incumplimiento *per se* del contrato que faculte para su resolución, mientras que la falsedad o incorrección relevante en relación a las

[1241] MARTÍNEZ FERNÁNDEZ, J.M. (2017), medidas de transparencia, 20.
[1242] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 43.

cualidades y aptitudes del proveedor para prestar el servicio puede resultar invalidante de la voluntad emitida por el cliente y viciar de nulidad el contrato concluido[1243].

A falta de limitaciones contractuales concretas, el adjudicatario podrá planificar los recursos humanos necesarios para prestar el servicio conforme a su *lex artis*, dentro de las facultades empresariales para ordenar su actividad que le son propias, empleando personas suficientemente capacitadas. Sin embargo, nada obsta que, una vez conseguido el contrato, el empresario mueva a los mejores profesionales para atraer a otro cliente, prestando el servicio otros profesionales menos competentes, planteándose una posible violación de la buena fe contractual.[1244]

Habida cuenta de la importancia que reviste el equipo de desarrollo en la elusión de la "crisis del *software*", la valoración de la experiencia de los medios humanos de los licitadores se convierte en una cuestión crucial[1245]. La STJUE C-601/13, de 26 de marzo de 2015, entiende admisible la inclusión de un criterio de valoración de ofertas que evalúe la constitución, competencia, formación, experiencia y el currículo de los miembros del equipo concretamente propuesto para la ejecución del contrato, en los contratos de servicio de carácter intelectual, considerando que la calidad de la ejecución puede depender de manera determinante de la valía profesional de las personas encargadas de ejecutarlo. Esta "experiencia concreta" a evaluar en la fase de valoración de ofertas difiere de la "experiencia general" de la empresa, utilizada tradicionalmente para verificar la capacidad y aptitud del licitador. Esta postura,

[1243] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 58-59.
[1244] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 97-98.
[1245] *Vid*. MENÉNDEZ SEBASTIÁN, E.M. (2009), contratos de servicios del sector público, 539-554. La autora estudia con detalle los problemas que se plantean por la influencia de la capacidad intelectual del contratista y su titulación en el resultado de los contratos de servicios intelectuales.

coherente con el artículo 67 de la directiva 2014/24/UE y con su considerando 94, pasa a reflejarse en el PLCSP y, casi con seguridad, necesitará ser concretada vía jurisprudencia[1246].

El contrato de desarrollo de programas a medida no presupone la transmisión de la propiedad de los mismos ni implica unos derechos irrenunciables de explotación. Sujetos a la autonomía de las partes, habrá que detallarlos específicamente en el clausulado para evitar sorpresas al término de la relación, contemplando también su subsistencia una vez finalizado el contrato de *outsourcing*[1247].

El deber de colaboración es una obligación inherente al contrato y un requisitos *sine qua non* para alcanzar el éxito del proyecto. Su incumplimiento puede imposibilitar la adecuada prestación del servicio, permitiendo la resolución anticipada del contrato. Las nuevas políticas orientadas a evitar incurrir en cesión ilegal de trabajadores, comentada *supra*, dificultan la materialización de esa colaboración. Esa carga, típica de todos los contratos de servicios, pesa sobre el cliente[1248]. Resulta conveniente que se especifique y detalle en el contrato las obligaciones de colaboración por su parte.[1249]

El PPT debería detallar la categoría a la que corresponde la aplicación a desarrollar conforme a las especificaciones del ENS, recogiendo las medidas a aplicar por el adjudicatario a consecuencia de dicha clasificación, examinado previamente el resultado del

[1246] TABERA PÉREZ, O. (2016), los medios humanos y la experiencia.
[1247] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 116.
[1248] *Vid*. CRESPO MORA, M.C. (2013), obligaciones de medios y de resultado, 30-31.
[1249] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 123-125.

análisis de riesgos[1250]. Igualmente, para aquellas aplicaciones que gestionen datos de carácter personal, constará el nivel de los ficheros y las medidas de seguridad a aplicar de conformidad con la legislación de protección de datos analizada *supra*.

Otras cláusulas referentes al deber de secreto[1251] y confidencialidad[1252], a la protección de datos personales[1253], a la exigencia de diligencia o a la buena fe contractual, aunque, *a priori*, podrían parecer innecesarias o redundantes, representan la inclusión expresa en el contrato de todas las obligaciones no referidas en el mismo pero que constituyen el lógico y necesario cumplimiento del contrato de *outsourcing*[1254].

El conocimiento de las obligaciones asumidas por la empresa en cuanto a seguridad de la información y de los sistemas, incluyendo las ya citadas confidencialidad y la protección de los datos de carácter personal, debe alcanzar fehacientemente no solo al todo el personal del adjudicatario involucrado en el proyecto, sino que ha de trasladarse también a las subcontratas, suponiendo que estas fuesen admisibles.

[1250] Esta conveniencia puede tornarse en obligación, como se plasma en la precitada orden PRE/57/2016, que viene a desarrollar la Política de seguridad de la información de la Administración de la Comunidad autónoma de Cantabria, aprobada por el Decreto 31/2015, de 14 de mayo.
[1251] Extensible a los datos de la Administración que se hayan podido conocerse de manera fortuita.
[1252] Un modelo de acuerdo de confidencialidad para terceros es el que ofrece el CCN en el apéndice VI de su documento CCN-STIC-821, anexo que lleva por título "*Normas de Seguridad en el ENS. Acuerdo de confidencialidad para terceros. NP50*".
[1253] Entre los datos personales a proteger también han de incluirse los del propio personal asignado a la ejecución del contrato.
[1254] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 138.

Suele incluirse una cláusula representativa del *favor negotii* por la que se acuerdan que la nulidad o invalidez de alguna de las cláusulas del contrato no afectará al contrato mismo, que seguirá surtiendo efectos entre las partes.[1255]

A pesar de que se haya hecho uso de la mejor técnica contractual, los desacuerdos entre la empresa desarrolladora y el contratante con frecuencia acaban dilucidándose en los tribunales. El desarrollo del *software* no es una tarea fácil, la comunicación entre los informáticos y los usuarios que han de especificar sus necesidades muchas veces parece reflejar que cada uno se expresa en un idioma diferente, y el producto obtenido no llega a satisfacer plenamente las esperanzas depositadas en el contrato. La Jurisprudencia[1256] describe el desarrollo del *software* como una obligación de resultado[1257] aunque no cualquier incumplimiento permite la resolución del contrato[1258].

7.4.3. La colaboración público-privada

Las empresas llevan a cabo una parte sustancial de una función pública en numerosas ocasiones, en actividades como la seguridad privada, la construcción de infraestructuras públicas, la seguridad industrial, la concentración parcelaria, las actividades

[1255] APARICIO VAQUERO, J.P. (2002), nueva contratación informática, 143.
[1256] Entre otras muchas, Sentencia del Juzgado de lo mercantil de Zaragoza 2382/2015 de 15 de mayo de 2015, Sentencia de la Audiencia provincial de Madrid 14355/2008 de 23de septiembre de 2008, Sentencia de la Audiencia provincial de Madrid 5647/2006de 19 de mayo de 2006, etc.
[1257] Sobre la dicotomía entre obligaciones de medios y obligaciones de resultado, *vid*. JORDANO FRAGA, F. (1991). Obligaciones de medios y de resultados: (a propósito de alguna jurisprudencia reciente). Anuario de derecho civil, 44 (1), 5-96.
[1258] El FJ6 de la Sentencia del Tribunal Supremo 5031/2013, de 22 de Octubre de 2013, analiza el incumplimiento con entidad resolutoria, si bien no aplicado directamente a los contratos de desarrollo del *software*.

asistenciales…[1259]. Incluso el control de la calidad del propio aire que respiramos descansa sobre manos privadas[1260].

La sociedad viene a aceptar con relativa normalidad la externalización de las actividades más técnicas de nuestras Administraciones públicas, sin pretender que la ejecución de obras o el mantenimiento de los servicios sean siempre realizados con recursos materiales propios y por los empleados públicos. Esta nueva realidad, que se ha vuelto cotidiana, viene acompañada de un modo de financiación diferente para la ejecución de dichas obras y servicios[1261]. Entre esas formas diferentes a las tradicionales, cabe pararse a observar la colaboración público-privada.

En el plano europeo, no existe un instrumento con fuerza normativa que regule la colaboración público privada, pero, en su lugar, contamos con instrumentos de gran valor interpretativo, *soft law*[1262]. La carencia de definición y marco jurídico específico en el Derecho comunitario no debe considerarse como despreocupación por el desarrollo de esta técnica. La posible superación de los niveles de endeudamiento y déficit público alcanzables con su utilización y el incumplimiento de las normas y principios comunitarios de contratación son, de hecho, inquietudes manifiestas en la Unión. El interés europeo por dichos aspectos nos ha dejado diversos documentos de la Comisión que ofrecen la luz necesaria para comprender e interpretar

[1259] GONZÁLEZ-VARAS IBÁÑEZ, S.J. (2006), nuevos desarrollos, 32.
[1260] A modo de ejemplo, el decreto 50/2009, de 18 de junio, por el que se regula el control de la contaminación atmosférica industrial en la Comunidad autónoma de Cantabria, en su artículo 26, prevé la intervención de entidades privadas colaboradoras de la Administración en materia de medio ambiente atmosférico. Puede consultarse el listado de empresas autorizadas actualmente en la página *web* http://www.medioambientecantabria.es/emisiones-atmosfera/ampliar.php?Id_contenido=24066&Id_tipo=0 (consultado el 19 de diciembre de 2016).
[1261] RAMALLO MASSANET, J. (2007), control externo, 20.
[1262] BERNAL BLAY, M.A. (2010), colaboración público-privada institucional, 96.

la legislación en la materia, incluyendo a la normativa española[1263], ciertamente ambigua[1264]. Destacado entre ellos, el "Libro verde sobre la colaboración público-privada y el Derecho comunitario en materia de contratación pública y concesiones" lo describe genéricamente como "*las diferentes formas de cooperación entre las autoridades públicas y el mundo empresarial, cuyo objetivo es garantizar la financiación, construcción, renovación, gestión o el mantenimiento de una infraestructura o la prestación de un servicio*"[1265].

Hernando Rydings[1266] resume las causas que, a juicio de la Comisión, han motivado el auge la colaboración público privada, comenzando por el cambio de rol de las Administraciones públicas, que abandonan su papel de prestadoras de servicios para convertirse en coordinadoras. A ello añade el pacto de estabilidad presupuestaria y la necesidad de aprovechar el *know-how* del sector privado.

Albergada de forma dispersa en nuestra LCSP[1267], su regulación resulta más novedosa que su utilización, ya encontrada con anterioridad en la práctica jurídica española. Esta ley recoge por primera vez un tipo contractual con esa denominación, acompañado por un mecanismo de adjudicación ideado en el ámbito comunitario para los contratos especialmente complejos, denominado "diálogo competitivo". El vigente TRLCSP, en sus artículos 11[1268] y 134-136, se adentra en este tipo contractual, señalando algunos elementos clave que posibilitad

[1263] SÁNCHEZ LAMELAS, A. (2010), el nuevo contrato, 116-118.
[1264] GIMENO FELIÚ, J.M. (2012), delimitación conceptual, 40.
[1265] COMISIÓN DE LAS COMUNIDADES EUROPEAS (2004), libro verde sobre la colaboración, parágrafo 1.
[1266] *Vid*. HERNANDO RYDINGS, M. (2012), colaboración público privada, 163-181.
[1267] CHINCHILLA MARÍN, M.C. (2009), contrato de colaboración, 453-488.
[1268] El apartado c) del artículo 11 contempla la prestación de servicios que incorporen tecnología específicamente desarrollada con el propósito de aportar soluciones más avanzadas y económicamente más ventajosas que las existentes en el mercado

el recurso a la colaboración público-privada, como son la complejidad de la operación, la subsidiariedad en el uso de esta modalidad y la obtención de ventajas con su empleo[1269], en un texto impreciso, quizá de forma intencionada, incluso inevitable, que define un marco mínimo de actuación, unos elementos caracterizadores, dejando a las partes concretar el resto[1270].

El marco jurídico del contrato, conforme al artículo 313, será el que rige la prestación principal, con la salvedad de permitir la separación del mismo en lo que se oponga a su naturaleza, funcionalidad y contenido peculiar, posibilitando así la apertura de regímenes con especialidades relevantes[1271]. La posibilidad de separarse del régimen sustantivo que resulte de la prestación principal, es decir, si es Derecho necesario o simplemente supletorio, no se deduce inmediatamente de la ley. En opinión de Chinchilla Marín, la interpretación más lógica apunta a que el legislador ha querido diseñar un contrato flexible cuya configuración y diseño se dejan a la definición que convenga al tipo de prestaciones de que se trate y a los objetivos perseguidos por el contratante[1272].

Entre sus elementos característicos, su carácter absolutamente residual y subsidiario pretende evitar que se utilice el pretexto de la complejidad para eludir el régimen general de selección de contratistas, con la intención de garantizar así al máximo la concurrencia. Sin embargo, esta subsidiariedad pone en riesgo su utilización. Para Ridao i Martín, este tipo de contrato no debería ser apelable exclusivamente por una Administración turbada por la

[1269] SÁNCHEZ LAMELAS, A. (2010), el nuevo contrato, 119-121.
[1270] CHINCHILLA MARÍN, M.C. (2009), contrato de colaboración, 454-456.
[1271] SÁNCHEZ LAMELAS, A. (2010), el nuevo contrato, 122.
[1272] CHINCHILLA MARÍN, M.C. (2009), contrato de colaboración, 474.

incapacidad objetiva, sino que habría de ser suficiente la mera complejidad económico-financiera de la prestación[1273].

La complejidad intrínseca que se exige para hacer uso de la colaboración público privada y la consecuente falta de concreción del contenido prestacional, incluso en cuanto a los aspectos financieros, ha llevado al legislador a sustituir el tradicional pliego de cláusulas administrativas por un documento descriptivo del contrato, en el que ni siquiera se fija el precio, y que no está sometido a control previo de legalidad, aunque sí es posible realizar esa fiscalización con posterioridad, tras la adjudicación.[1274]

Las modificaciones e innovaciones tecnológicas que permitan hacer realidad la Administración electrónica apuntada por las nuevas y muy ambiciosas leyes administrativas, tendrán un coste económico difícilmente asumible por la Administración en un momento como el actual, afectado por fuertes restricciones presupuestarias. La necesidad de financiación privada puede despertar el interés de recurrir a la colaboración público privada[1275], cuyo éxito frecuentemente va ligado a los intentos de minimizar el déficit presupuestario y de deuda para cumplir con el pacto de estabilidad y crecimiento, habida cuenta de que esas cantidades, desembolsadas durante un periodo de tiempo largo, hacen frente a pagos constitutivos de un gasto corriente, que no consolida en el déficit si el socio privado soporta el riesgo de construcción y, además, el de disponibilidad o el de demanda[1276]. Por ello, considerados como riegos de construcción la entrega tardía del *software*, la falta de cumplimiento de los estándares

[1273] RIDAO I MARTÍN, J. (2013), el contrato de colaboración, 243-244.
[1274] RIDAO I MARTÍN, J. (2013), el contrato de colaboración, 247-248.
[1275] Comisión de las Comunidades europeas. (2004). *Libro verde…*, parágrafo 3.
[1276] Sobre los riesgos de construcción, disponibilidad y demanda, *vid.* HERNANDO RYDINGS, M. (2012), colaboración público privada, 84-86.

preestablecidos, las deficiencias técnicas, los efectos externos negativos que impliquen el pago de compensaciones a terceros y el sobrecoste que haya podido producirse en su desarrollo siempre serán asumidos por la empresa externa. Lo usual es que también asuma el riesgo de disponibilidad, que incluye la imposibilidad de entregar el volumen convenido en el contrato, el incumplimiento de las normas de seguridad o de certificación públicas vinculadas al servicio dirigido a los usuarios finales o la insatisfacción de los estándares de calidad fijados contractualmente[1277]. Cuando no se proporcionen los servicios acordados en las condiciones pactadas, descenderán los pagos conforme se haya especificado. Esta asunción de riesgos admite como causa de exoneración los cambios en el marco legal[1278], relativamente frecuentes y potencialmente muy perjudiciales, como ya se analizó *supra*, al tratar las repercusiones sobre el *software* cuando aparecen o cambian los requerimientos en fases avanzadas del proyecto.

Al objeto de garantizar y controlar el riesgo de disponibilidad, hay que fijar un número elevado de estándares de calidad en el contrato, así como asegurar que su incumplimiento represente una disminución apreciable del pago final, suficiente para que el socio privado realmente se resienta. De lo contrario, la empresa externa tendrá nulos o escasos incentivos para el cumplimiento esos estándares de calidad.[1279]

Teniendo en cuenta que al poder público se le exige la eficaz realización de sus funciones sin endeudarse presupuestariamente[1280], la colaboración público privada ha estado ganando aceptación al objeto de cubrir la distancia entre necesidades existentes y recursos

[1277] MACHO PÉREZ, A.B./ MARCO PEÑAS, E. (2014), déficit y deuda, 448-450.
[1278] RAMALLO MASSANET, J. (2007), control externo, 24-29.
[1279] MACHO PÉREZ, A.B./ MARCO PEÑAS, E. (2014), déficit y deuda, 450.
[1280] GONZÁLEZ-VARAS IBÁÑEZ, S.J. (2006), nuevos desarrollos, 33.

disponibles, posibilitando una relación de duración mayor de la habitual, en la que los socios público y privado comparten riesgos, pudiendo acordar en el contrato la vinculación de la totalidad o de parte de los honorarios de la empresa privada a la consecución de objetivos cualitativos y cuantitativos[1281], lo que permitiría ir haciendo frente a los pagos conforme fuesen poniéndose en producción nuevos servicios electrónicos, un esquema denominado "pago por disponibilidad". Los criterios de disponibilidad y estándares de calidad, así como las posibles penalizaciones, deben definirse detalladamente en el contrato. Con ello, resulta un sistema de pagos predecible y estable que agradecerán los socios privados, quienes normalmente aportan la mayor parte de los fondos, aunque pueda existir alguna subvención o financiación por parte de los organismos públicos.[1282]

Destaca en este tipo contractual, además de la estructuración de la financiación, la novedosa posibilidad de un nuevo reparto de riesgos, transfiriendo algunos que tradicionalmente soportaba la Administración hacia el socio privado[1283]. La transferencia de los riesgos de construcción, disponibilidad y demanda al contratista marcada en el contrato se acompaña de la ventaja de la no consolidación en el déficit público[1284], pero cabe cuestionar ese carácter ventajoso de la denominada "huida de la consolidación", que permite transferir considerables fondos públicos con cargo a partidas contables diferentes e incrementar el gasto público, en la

[1281] CANO RODRÍGUEZ, M./ PRADO GARCÍA, S./ ROMÁN BOCANEGRA, J. (2013). Colaboración Público-Privada, 4-6. Los autores describen en este trabajo la experiencia de la contratación de las TIC de la Generalitat de Catalunya mediante la colaboración público-privada, estructurando el nuevo modelo en cuatro bloques, de los cuales el primero corresponde al servicio del mantenimiento de sus 1800 aplicaciones informáticas.
[1282] DÍAZ PÉREZ, J. (2011), infraestructuras públicas, 21-29.
[1283] GIMENO FELIÚ, J.M. (2012), delimitación conceptual, 49.
[1284] YSA, T. (2009), gestión de partenariados público-privados, 29.

medida en que soportar los beneficios del sector empresarial, mayores que con las formas tradicionales de contratación[1285].

No debe recurrirse a la colaboración público-privada únicamente buscando dar respuesta a las dificultades financieras, sino con la pretensión fundada de obtener un mayor valor por precio. No siempre será la opción más eficiente y menos costosa. De hecho, es posible encontrar casos de fracasos estrepitosos, con las inherentes e indeseadas consecuencias para la Administración y para el servicio público. La prevención de estos problemas pasa por una buena selección del socio privado y un seguimiento adecuado del contrato por empleados públicos debidamente capacitados para los perfiles que surgen de las nuevas necesidades derivadas del contrato[1286]. El éxito del proyecto va directamente relacionado con el acierto del clausulado, el concreto reparto de riesgos y de los mecanismos de evaluación periódica de la actividad del socio privado[1287].

Los reproches que podríamos plantear a la técnica de colaboración público privada, al margen de su posible motivación por huida de la consolidación, se centran en su deficiente marco regulatorio, tanto europeo como estatal[1288]. Es patente la necesidad empírica de modificar el sistema de concepción y adjudicación de estos contratos, complejos y dilatados en cuanto a tiempo de ejecución, especialmente en ciertos sectores carentes de suficiente

[1285] RAMALLO MASSANET, J. (2007), control externo, 22-23.
[1286] YSA, T. (2009), gestión de partenariados público-privados, 35-36.
[1287] CHINCHILLA MARÍN, M.C. (2009), contrato de colaboración, 474.
[1288] RIDAO I MARTÍN, J. (2012), la colaboración público-privada, 191.

experiencia previa, habida cuenta de la frecuencia con que se producen modificados, paralizaciones y sobrecostes, con un alto grado de litigiosidad y de inseguridad jurídica.[1289]

Uno de los aspectos problemáticos reside en la retención del *know how* y la protección de la información declarada como confidencial en las ofertas, en cuanto a secretos técnicos y comerciales que puedan verse difundidos, establecida por ley en cinco años, salvo que los pliegos o el contrato establezcan un plazo mayor. Ello dificulta el aprovechamiento de las ideas propuestas por los diferentes concursantes por parte de la Administración, e inhibe la presentación de proposiciones innovadoras por parte de las distintas empresas, temerosas de que puedan ser aprovechadas por los competidores.[1290]

Si puede suponerse que la novedosa incorporación del CPP a la LCSP obedeció, en parte, a la necesidad de acoger normativamente una realidad jurídica y social o económica existente[1291], hoy el legislador parece retroceder sobre sus pasos por análogo motivo. En el nuevo PLCSP desaparece el CPP, a la vista de la experiencia que aconseja evitar confusiones o su uso incorrecto[1292]. Según indican la memoria del análisis de impacto normativo y el dictamen del Consejo de Estado sobre el mismo, dicha figura contractual se suprime a consecuencia de su escasa utilidad en la práctica.

El nuevo paquete de directivas continúa sin regular los contratos de colaboración público privada, aunque sí afronta la contratación mixta y el régimen jurídico de los contratos S.A.R.A. En referencia a la aplicación a este tipo de contratos de dichas directivas, en nuestro

[1289] RIDAO I MARTÍN, J. (2012), la colaboración público-privada, 198.
[1290] RIDAO I MARTÍN, J. (2012), la colaboración público-privada, 202-203.
[1291] GONZÁLEZ-VARAS IBÁÑEZ, S.J. (2006), nuevos desarrollos, 35.
[1292] GIMENO FELIÚ, J.M. (2016), novedades del anteproyecto, 20.

país, a partir del 18 de abril y en ausencia de la preceptiva transposición, la recomendación de la junta consultiva de contratación administrativa del Estado señala su consideración como contrato de tipo mixto, cuyo régimen jurídico se determinará de conformidad con los artículos 3 de la directiva de contratos y 20 de la de concesiones, respecto a materias que son reguladas por normas de estas directivas con efecto directo. En caso contrario, se continuará aplicando el criterio de la prestación principal conforme a los artículos 136.a) y 313 del TRLCSP.

Por último, cabe apuntar que, durante la tramitación del PLCSP, podría resucitar este tipo contractual, a tenor de las enmiendas presentadas.

8. LA MATERIALIZACIÓN DE LOS RIESGOS

Los ciudadanos nos sometemos a las más diversas prácticas médicas en la sanidad pública. Previamente se nos entrega un documento informativo con referencias incluso a los más improbables riesgos que podrían llegar a materializarse, muchos de los cuales no logramos comprender. Se nos da a escoger entre aceptarlos y someternos al procedimiento médico, con un consentimiento informado, o rechazar la práctica. Sin embargo, nadie nos advierte de los riesgos que se asumen al utilizar un procedimiento informatizado por las Administraciones públicas y, a los colectivos obligados a relacionarse con ellas a través de medios electrónicos, ni siquiera se les deja escoger si continuar o no. Tal vez el futuro diluya esas diferencias y la información sea igual de explícita en ambos ámbitos.

Los riesgos de cualquier tecnología siempre vienen precedidos de las decisiones humanas, públicas y privadas, adoptadas en su investigación, desarrollo y aplicación. De esas

decisiones y de los daños que por ellas se produzcan, inmediatos o futuros, hemos de ser responsables. Ello convierte a los riesgos tecnológicos en objeto de atención por el Derecho, el cual debe pronunciarse sobre quién adopta esas decisiones, con qué legitimación y, también, con qué responsabilidades[1293].

Sabemos que el *software* falla y que, por encima de cierto tamaño, es materialmente imposible probar todas las opciones que puede ejecutar el programa, lo que implica incerteza sobre su funcionamiento, razonablemente superior cuando los programas no han sido realizados por la propia Administración, sino por una empresa externa, movida por unos objetivos que no coinciden con el interés público[1294], sino con un legítimo afán de lucro económico propio, que va directamente relacionado con la rapidez en la entrega y la liberación de recursos humanos para poder asignarlos a otro proyecto. Pone de manifiesto Esteve Pardo la complejidad de la incerteza que se cierne en torno a las intervenciones de la técnica en un mundo saturado de ella, reiterando la gran relevancia para el Derecho que se plantea especialmente en el momento de adoptar decisiones y en el de afrontar la responsabilidad por los daños causados en esos entornos de incerteza, con origen en una o varias decisiones humanas[1295]. Esas decisiones que se adoptan durante el proceso de desarrollo se han tratado *supra*. La responsabilidad por los daños causados se analiza a continuación.

[1293] ESTEVE PARDO, J. (2003), ciencia y Derecho, 140-148.

[1294] *Vid*. HERNANDO RYDINGS, M. (2012), colaboración público privada, 88-90. La autora describe los objetivos del sector privado señalando que "*en la mayoría de los casos van a ser opuestos a los perseguidos por la autoridad pública*", afirmación señalada para la colaboración público privada que considero extensible a los contratos de servicios.

[1295] ESTEVE PARDO, J. (2003), riesgos desconocidos, 55.

8.1. RESPONSABILIDAD DE LOS USUARIOS

No son extrañas las alegaciones de los ciudadanos o de las empresas del sector privado referentes al mal funcionamiento de las aplicaciones, algo que, en muchas ocasiones, parecen ser excusas fáciles que pretenden evitar sanciones. En cualquier caso, la actitud diligente resulta ser para la jurisprudencia un criterio básico para inclinar la balanza de la justicia o, al menos, para modular su contribución en una hipotética concurrencia de culpas. Así, un ejemplo en el ámbito de la salud lo protagonizó la nueva aplicación informática SIGMA de la Oficina del Plan del cáncer, que sustituyó en la Comunidad valenciana al preexistente sistema de información. Un error administrativo-informático produjo una demora de más de dos años en la realización de mamografías de mujeres valencianas de entre 45 y 69 años, lo que dificultó el diagnóstico inicial del cáncer de mama de una de ellas. Se afirma, en cambio, que no se puede atribuir la exclusiva responsabilidad de la salud de los pacientes al sistema sanitario. En el caso concreto, la paciente era la única que conocía la existencia de antecedentes familiares de cáncer de mama, a lo que se añade que el nódulo que presentaba era evidente a la palpación, por lo que se le atribuye una parte de la responsabilidad, se estima parcialmente su recurso y se le reconoce una indemnización de 5.000 €.[1296]

Una supuesta desidia inclinó la balanza de la justicia en contra de una entidad mercantil dedicada a la adquisición y explotación de centros médicos hospitalarios, siendo sancionada por una infracción tributaria grave. A pesar de argumentar la existencia de un error informático para justificar unas deducciones de casi 3.600.000 €, su alegación no fue admitida

[1296] STSJ de la Comunidad Valenciana 2672/2016 de 25 de mayo de 2016, sala de lo contencioso.

como causa exculpatoria. El Tribunal Supremo entendió que no había actuado con el debido cuidado, aun cuando hubiera incurrido en un supuesto error informático, considerando que fácilmente habría constado la irregularidad con una simple revisión de la declaración-liquidación practicada. Afirma la sentencia que "*la responsabilidad del obligado tributario en comprobar los datos declarados no desaparece o minora por el mero hecho de optar por utilizar un determinado programa informático específico*"[1297].

Pero, por seguridad jurídica, el ciudadano no puede ser condenado sino hasta el límite a que pudiera alcanzar su voluntad o el resultado previsible y evitable de su comportamiento negligente, principal manifestación del principio de culpabilidad, siendo este el elemento esencial para calificar su conducta como sancionable. Por ello, es preciso analizar las razones expuestas por el ciudadano como justificadoras del incumplimiento de sus obligaciones, para descartar las que sean meros pretextos o se basen en criterios de interpretación absolutamente insostenibles. Aspectos como el error de hecho invencible han de excluir la responsabilidad. Igualmente, a tenor de artículo 179.2.d) de la LGT, las acciones u omisiones tipificadas en las leyes no darán lugar a responsabilidad por infracción tributaria cuando se haya puesto la diligencia necesaria en el cumplimiento de las obligaciones. El mismo artículo, en su apartado e), prevé la ausencia de responsabilidad cuando su comisión sea imputable a una deficiencia técnica de los programas informáticos de asistencia facilitados por la propia Administración para el cumplimiento de las obligaciones tributarias, precepto del que no puede deducirse que, cuando el fallo se produzca en un *software* no facilitado por la Administración tributaria, haya de ser sancionada sin posibilidad de exoneración. La diligencia necesaria es un

[1297] STS 2658/2015 de 4 de junio de 2015, sala de lo contencioso.

concepto jurídico indeterminado a concretar casuísticamente en función de aspectos como la obligación tributaria específica, la naturaleza de la norma de cuidado, el grado de atención o dificultad que requiere su cumplimiento, el resultado lesivo y otras circunstancias concurrentes[1298].

En enero de 2013, se sancionó al titular de una estación de servicio por el incumplimiento de la obligación de enviar información al Ministerio de industria, energía y turismo de los precios de venta al público de los carburantes comercializados en su gasolinera. En su defensa planteó la cuestión del manido error informático. Parece deducirse de la lectura de la sentencia[1299] que se comprobó la carencia de la información requerida en la base de datos del Ministerio, pero nada consta de que se haya revisado el funcionamiento de la oficina virtual ni del registro telemático. De hecho, parece que en ningún momento se estudió la posibilidad de que el *software* mostrase un comportamiento inesperado, dado que la propia sentencia da por bueno que "*si hay un error informático como pretende el demandante no se podrá validar el envío; y si por el contrario la aplicación funciona correctamente la remisión a la sede electrónica genera un apunte en el Registro telemático del Ministerio de Industria y un justificante de presentación*". Lo correcto hubiera sido comenzar esa frase diciendo "si hay un error informático, puede desencadenarse cualquier comportamiento difícilmente imaginable". Sin embargo, coincido con el resultado final de desestimación del recurso, no porque se haya probado el correcto funcionamiento de los sistemas informáticos fuera de toda duda razonable, sino por lo que parece ser una falta de diligencia del titular de la estación de servicio, quien dice

[1298] STSJ de Cataluña 2073/2012 de 23 de febrero de 2012, sala de lo contencioso.
[1299] SAN 4886/2013 de 20 de noviembre de 2013, sala de lo contencioso.

haber enviado la información requerida puntualmente, sin haber realizado ninguna acción dirigida a manifestar la no emisión de resguardo justificante de la operación nada menos que durante 29 semanas no consecutivas, algo que, de haber sido puesto en conocimiento de los servicios informáticos del Ministerio, sin duda hubiera sido puntualmente investigado. Aunque, si ese *software* hubiera sido desarrollado por una empresa de servicios externa, si ya no estuviera en garantía, si no existiera un contrato de mantenimiento en vigor, cabe plantearse quién podría investigarlo, quién tendría el suficiente conocimiento de esa aplicación. Y otra duda surge de inmediato... ¿Cuántas comunicaciones sobre un posible mal funcionamiento tienen que reportarse antes de que se encargue a los sobrecargados servicios de informática la revisión de los programas? ¿Con la primera queja, muchas veces inventada como excusa de un incumplimiento, ya se debe iniciar una revisión?

Con respecto a esta última sentencia citada, cabe apuntar que la obtención de un justificante de presentación telemática no garantiza inequívocamente que dicha acción haya tenido lugar, puesto que no descarta un fallo del programa informático o su inadecuado diseño. Sin embargo, la consecución de ese resguardo sí permite rechazar la idea de que el ciudadano o la empresa en cuestión hayan actuado negligentemente, como indica otra sentencia: "(…) *constaba el número de justificante que el sistema informático otorgó a su presentación telemática generándose un número de referencia de presentación con fecha y hora por lo que no cabe mayor diligencia* (…)".[1300]

[1300] STSJ de Madrid 6271/2016 de 7de julio de 2016, sala de lo contencioso.

Precisamente la diligencia de la persona encargada de recibir las notificaciones es lo que se cuestiona en la sentencia de la sala de lo contencioso-administrativo del Tribunal Supremo, de 16 de noviembre de 2016. La persona que accedió a la dirección electrónica habilitada, DEH, abrió el documento y, al encontrar las primeras páginas de la notificación en blanco, interpretó que era un error informático y no identificó dicho documento, a pesar de que realmente contenía todos los requisitos previstos para considerarla una notificación válida. Entiende el abogado del Estado que no existió fallo técnico informático sino falta de diligencia por no pasar de la segunda página. Aunque realmente no se cuestiona la validez de las notificaciones por comparecencia electrónica, su FJ3 destaca la transformación tan radical que supone este cambio de paradigma, que afecta directamente al principio básico de no indefensión y es medio necesario para alcanzar la tutela judicial efectiva, afirmando que lo relevante no es que se cumplan las previsiones legales sobre cómo se llevan a efecto las notificaciones, sino que los administrados lleguen a tener conocimiento de ellas o haya podido tener conocimiento del acto notificado. En este caso, el Tribunal aprecia falta de diligencia en la empleada, pero también deficiencias en la notificación efectuada, a lo que añade que la Administración se apartó de la forma habitual de notificar que venía utilizando. En su sentencia, el Supremo considera que si en las notificaciones de sanciones ha de extremarse el celo en la notificación plena, exacta y formal, también ha de hacerse al tratarse de un recargo de apremio, aunque no tenga carácter sancionador, por lo que la Administración tiene la carga del rigor en su práctica. Introduce, también, una suerte de proporcionalidad entre rigor de la notificación y consecuencias de sus

deficiencias, de manera que a mayores gravámenes en liza, mayor celo ha de otorgar a la forma de notificar[1301].

Además de la diligencia debida, se exige al ciudadano y al sector empresarial la carga de la prueba, algo que no siempre resulta sencillo. En un recurso contra una resolución sancionadora del TEAR de Madrid, se alega la improcedencia de la infracción por concurrencia de supuesto de fuerza mayor y ausencia del elemento subjetivo de la infracción, al no poder elaborar el modelo 190 en plazo para su presentación en plazo, por errores informáticos. La entidad recurrente manifiesta la dificultad o incluso imposibilidad de prueba de dicho extremo, pero recuerda la sentencia que, de conformidad con lo dispuesto en el artículo 105.1 de la LGT, le correspondía a la recurrente la carga de la prueba de los pretendidos errores informáticos[1302].

La jurisprudencia ha invertido la carga de la prueba en el Derecho de daños en múltiples ocasiones relacionadas con la complejidad técnica de las actividades, una inversión que debe tener relación con el hecho de que, para el demandante, resulte complejo, inasequible o muy difícilmente accesible la demostración[1303]. Sin embargo, no parece tarea sencilla la búsqueda de un criterio general para determinar cuándo podría proceder una inversión de la carga de la prueba en los casos de uso de las aplicaciones informáticas. En una cara de la moneda aparece la falta de conocimientos especializados del ciudadano medio enfrentada a la abrumadora capacidad técnica de las Administraciones públicas, que le permite la elaboración de programas *ad hoc* según sus necesidades y el uso de los ficheros de *logs* para poder analizar

[1301] *Vid*. https://delajusticia.com/2016/11/28/el-supremo-advierte-las-notificaciones-electronicas-no-admiten-rebaja-en-las-garantias/
[1302] STSJ de Madrid 16319/2013 de 5 de diciembre de 2013, sala de lo contencioso.
[1303] DÍEZ-PICAZO PONCE DE LEÓN, L. (2000), culpa y riesgo, 164.

detenidamente las trazas de lo sucedido. Pero las monedas tienen dos lados y, por el otro, nos encontramos con unas Administraciones públicas incapaces de dar servicio igualmente óptimo a las innumerables combinaciones de sistemas operativos, navegadores, versiones de java, etc., que no pueden controlar lo que los usuarios tienen instalado y parametrizado en sus ordenadores particulares.

En mi opinión, la imposición del uso de la Administración electrónica debe ir acompañada, indefectiblemente, de unas instrucciones *for dummies*, permanentemente actualizadas, que expliquen de forma sencilla su uso y despejen cualquier sombra de duda que pueda existir en el usuario sobre la instalación de los certificados, los sistemas operativos aceptados, los navegadores compatibles, las versiones de java utilizables, la parametrización a establecer en las distintas opciones (no solo del panel de control de java, sino de cualquier recóndito lugar escondido, incluso, para los que nos hemos dedicado durante años a estos menesteres) y un largo etcétera que probablemente no puedo ni imaginar. Para quien se esté preguntando si esto es la neutralidad tecnológica que proclaman nuestros legisladores, responderé que no. Esto no es neutralidad tecnológica, esto es, simplemente, la realidad, y probablemente va a seguir siéndolo durante tiempo.

Incluso siguiendo esos manuales *for dummies* al pie de la letra, habrá ciudadanos y empresas para quienes su acercamiento a las nuevas tecnologías seguirá siendo un calvario. Para esos casos, que ya no serán tan numerosos si se les han proporcionado las instrucciones correctas, debería existir un CAU especializado en cada Administración, con un alto nivel técnico, preparado para registrar las incidencias descritas por los usuarios, solventar los

problemas en la medida de lo posible y dejar constancia de aquellos que no han sido resueltos, para su estudio posterior y, sobre todo, para su aportación como prueba ante los tribunales tanto de la diligencia del usuario como de la incapacidad técnica acaecida.

Solo así, en mi opinión, estaríamos en condiciones de empezar a pensar en imponer el uso de la Administración electrónica a determinados colectivos.

8.2. ERRORES INFORMÁTICOS IMPUTABLES A LA ADMINISTRACIÓN

Alegar el mal funcionamiento de sus propios programas informáticos, incluso cuando a los errores cometidos no puede aplicarse en modo alguno tal calificación, también resulta habitual en el seno de las Administraciones públicas. La representación procesal del Servicio andaluz de salud, debido a lo que describe como un error informático, confundió un recurso de casación ordinario con uno para la unificación de doctrina, sin suponer mayores consecuencias, al ser considerado por el Tribunal Supremo como un error meramente material[1304]. Si el supuesto error se debió a utilizar una plantilla incorrecta o a realizar un *copy-paste* sin recordar cambiar después determinados datos, no se trataría de un fallo informático, sino de un error humano ajeno al funcionamiento técnico del sistema. Resulta habitual calificar de error informático a las equivocaciones humanas ocurridas al utilizar una herramienta informática, como la que describe el siguiente fragmento de otra sentencia: "*un error informático al pinchar con el ratón en un calendario desplegable. Se puede comprobar fácilmente que el 8 y*

[1304] ATS 11317/2000 de 2de octubre de 2000, sala de lo contencioso.

el 15 de octubre de 2012 fueron lunes, por lo que en el calendario están uno encima de otro"[1305]. Obviamente, no se trata de un error informático, sino de un error humano.

Pero no siempre esos llamados fallos informáticos, sean humanos o técnicos, reales o fruto de la creatividad, pueden tratarse como simples errores materiales. La Jefatura provincial de tráfico de Valladolid sancionó con multa de 600 € a un centro de reconocimiento de conductores por emitir informes de aptitud psicofísica sin haber sometido al interesado a la correspondiente exploración. Esta resolución y su notificación fueron fruto de un error de carácter informático. Cuando esa primera resolución ya había adquirido firmeza, se dictó la resolución correcta, con la misma fecha que la anterior y en su sustitución, siendo notificada al interesado seis meses más tarde, incluyendo, además de la multa, la suspensión de la eficacia de la inscripción del citado centro de reconocimiento de aptitudes de conductores por un plazo de seis meses. Parece extraño que un ordenador decidiera de forma autónoma y equivocada cuál era la sanción a imponer. Se podría pensar que realmente fue un error humano que, posteriormente, se intentó enmendar, aplicando la rectificación de los errores materiales, de hecho o aritméticos del artículo 105.2 de la LRJPAC (ahora 109.2 de la ley 39/2015) para sustituir la resolución inicial por otra de contenido diferente y más gravoso, olvidando el criterio jurisprudencial que limita su aplicación a las situaciones en las que concurran las siguientes circunstancias:

"*1) Que se trate de simples equivocaciones elementales de nombres, fechas, operaciones aritméticas o transcripciones de documentos;*

[1305] SAP de A Coruña 1317/2016 de 11de julio de 2016.

2) Que el error se aprecie teniendo que cuenta exclusivamente los datos del expediente administrativo en el que se advierte;

3) Que el error sea patente y claro, sin necesidad de acudir a interpretaciones de normas jurídicas aplicables;

4) Que no se proceda de oficio a la revisión de actos administrativos firmes y consentidos;

5) Que no se produzca una alteración fundamental en el sentido del acto (pues no existe error material cuando su apreciación implique un juicio valorativo o exija una operación de calificación jurídica);

6) Que no padezca la subsistencia del acto administrativo es decir, que no genere la anulación o revocación del mismo, en cuanto creador de derechos subjetivos, produciéndose uno nuevo sobres bases diferentes y sin las debidas garantías para el afectado, pues el acto administrativo rectificador ha de mostrar idéntico contenido dispositivo, sustantivo y resolutorio que el acto rectificado, sin que pueda la Administración, so pretexto de su potestad rectificatoria de oficio, encubrir una auténtica revisión; y

7) Que se aplique con un hondo criterio restrictivo"[1306].

La sala de lo contencioso del TSJ de Castilla y León con sede en Valladolid anuló la segunda de las resoluciones y reconoció el derecho de la recurrente al resarcimiento de daños y perjuicios por parte de la AGE[1307].

[1306] STS 2618/2012de 19 de abril de 2012.

Tampoco procedía la revocación ni la corrección de un mero error material en el caso de Servicio vasco de salud, que reconoció a un trabajador, por un error informático, un trienio del grupo C cuando realmente correspondía al D. Frente a su pretensión de "*modificar un error informático, sin que ello afecte al reconocimiento de derechos, sino únicamente a la cuantía del trienio*", la sentencia sí considera que se ha producido un reconocimiento de derechos con respecto al que no cabe acudir a la vía de la revocación, por tratarse de un acto favorable al interesado, ni a la rectificación de errores del artículo 105.2 de la LRJPAC, al alterar de forma sustancial un acto previo firme. La vía para rectificar ese acto firme solo puede ser la revisión de oficio[1308], como en otro error informático producido en relación a la expedición de un visado de residencia familiar ciudadano de la Unión Europea, válido desde el 26 de enero hasta el 23 de julio de 2012, al no constar la prohibición de entrada en territorio Schengen a pesar de que tenía numerosos antecedentes penales en vigor, con diversas condenas por sentencias judiciales firmes, y de que había sido expulsado de nuestro país con prohibición de retorno hasta el 30 de septiembre de 2020. Como indica la sentencia[1309], se otorgó al recurrente un derecho que posteriormente no le puede denegar por la existencia de un presunto error informático; detectado dicho error, lo procedente era que se hubiera declarado la lesividad del acto que concedió el citado visado, y se hubiera llevado a cabo una revisión de oficio del mismo.

No son infrecuentes los errores informáticos en la transcripción de las sentencias, aunque más bien podrían tratarse de errores humanos al usar un ordenador, algo conceptualmente bastante diferente. Si bien los tribunales no pueden variar las resoluciones después de firmadas,

[1307] STSJ de Castilla y León 3842/2013de 10de septiembre de 2013.
[1308] STSJ del País Vasco 3923/2013 de 22 de noviembre de 2013, sala de lo contencioso.
[1309] STSJ de Madrid 7972/2016 de 14 de julio de 2016, sala de lo contencioso.

sí pueden aclarar algún concepto oscuro y rectificar cualquier error material manifiesto, así como los aritméticos, en cualquier momento, pudiendo proceder así a su subsanación[1310].

Otros fallos informáticos impidieron la grabación de un juicio rápido, no constando siquiera sucinta acta extendida por fedatario judicial en la que se recoja el resultado de la prueba practicada, por lo que se acuerda retrotraer las actuaciones al momento procesal inmediatamente anterior a la convocatoria a juicio oral, dejando sin efecto este y la resolución recaída, para que por un nuevo juzgador se lleve a cabo nueva convocatoria de plenario, se celebre juicio oral y se dicte nueva sentencia.[1311]

8.3. LA RESPONSABILIDAD PATRIMONIAL ANTE LA ADMINISTRACIÓN ELECTRÓNICA

Nos recuerda Tolivar Alas que "(…) *tramitación telemática no equivale a procedimiento anónimo e irresponsable*"[1312]. La responsabilidad es una garantía del ciudadano, un principio de orden y un instrumento más de control del poder, que juega, además, una función pedagógica a través de la cual la Administración aprende cómo actuar en el futuro para no ser condenada. El instituto de la responsabilidad no debe ser considerado como un freno a la actividad pública, sino una pieza esencial de las relaciones entre los ciudadanos y la Administración[1313].

[1310] Auto Aclaratorio TSJ de Madrid 247/2016 de 24 de mayo de 2016, sala de lo contencioso.
[1311] Sentencia de la Audiencia Provincial de Cádiz 589/2013 de 12 de abril de 2013.
[1312] TOLIVAR ALAS, L. (2008), el personal de la Administración, 10.
[1313] MARTÍN REBOLLO, L. (2000), reflexiones, 307-308.

Si el error de una máquina, el fallo informático, causa un daño un daño indemnizable, podrá ser objeto de responsabilidad patrimonial, afirma Tolivar Alas[1314]. Nuestras Administraciones públicas tienen el deber de garantizar unos servicios eficientes y de calidad, manteniendo el control en el caso de externalización, de forma que pueda garantizar los derechos de los ciudadanos, algo que difícilmente podrán lograr si no mantienen un dominio y control reales, dándose ocasiones en las que la opción más correcta será intentar mejorar las organizaciones públicas sin tener que recurrir a la externalización[1315]. También tiene el deber de mantener la neutralidad tecnológica, por lo que las decisiones que tome al respecto, que pueden condicionar el acceso a la información y los servicios de forma que se requiera un desembolso económico adicional por parte del ciudadano que, en caso de estimarse antijurídico, serían susceptibles de indemnización[1316]. El artículo 32.9 de la ley 40/2015 contempla la posible responsabilidad de las Administraciones públicas por los daños y perjuicios causados a terceros durante la ejecución del contrato cuando sean consecuencia de una orden inmediata y directa de la Administración o de los vicios del proyecto elaborado por ella misma, pero no parece fácilmente aplicable al desarrollo del *software* más allá del incumplimiento de la normativa de protección de datos de carácter personal. En este supuesto, el artículo 19 de la LOPD reconoce un derecho a la indemnización por el daño o lesión en los bienes o derechos que se aplica tanto para los ficheros públicos como para los privados, y es ejercitable ante la jurisdicción

[1314] TOLIVAR ALAS, L. (2008), el personal de la Administración, 11. El autor señala también la repetición contra el empleado público o autoridad cuando media dolo, culpa o negligencia grave por su parte, advirtiendo también la posibilidad de que incurra en la responsabilidad derivada del delito.
[1315] RAMIÓ MATAS, C. (2009), fenómeno de la externalización, 66.
[1316] VALERO TORRIJOS, J. (2008), acceso a los servicios, 246.

contencioso-administrativa por el procedimiento de responsabilidad patrimonial o ante la jurisdicción civil[1317]

Los principios del sistema de responsabilidad de nuestras Administraciones se establecen y regulan hoy en la nueva ley 40/2015, artículos 32 y siguientes, donde se mantienen los principios contemplados en la normativa anterior, por los que se reconoce el derecho de los particulares a ser indemnizados de toda lesión que sufran en sus bienes y derechos, a consecuencia del funcionamiento normal o anormal de los servicios públicos, a excepción de los casos de fuerza mayor o de daños que tengan el deber jurídico de soportar, recordando que el daño deberá ser efectivo (en su doble modalidad de daño emergente y de lucro cesante[1318]), evaluable económicamente e individualizado con relación a una persona o grupo de personas. La lesión sufrida ha de ser real y efectiva, nunca potencial o futura, pues el perjuicio tiene naturaleza exclusiva con posibilidad de ser cifrado en dinero[1319]. Se trata de un sistema objetivo cuyas claves son el criterio de la causalidad y el concepto de lesión como daño antijurídico[1320], donde puede haber responsabilidad sin culpa, pero no responsabilidad sin perjuicio[1321]. Por tanto, son cuatro los requisitos que han de coexistir para poder exigir responsabilidad patrimonial derivada del funcionamiento de los servicios públicos electrónicos: un hecho imputable a la Administración, un daño antijurídico, un nexo causal y la ausencia de fuerza mayor. Martínez Gutiérrez incluye como hechos imputables a la Administración los contenidos y servicios

[1317] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 286.
[1318] Los elementos constitutivos de la responsabilidad patrimonial de las Administraciones públicas han sido concretados en numerosas sentencias del Tribunal Supremo, por todas, la sentencia de 28 de enero de 1999.
[1319] TRONCOSO REIGADA, A. (2010), en busca del equilibrio, 286.
[1320] MARTÍN REBOLLO, L. (2000), reflexiones, 309.
[1321] MARTÍN REBOLLO, L. (2000), reflexiones, 312.

publicados en los portales y sedes de su titularidad, aunque no sean gestionados directamente por ella, pues lo publicado allí es fruto del ejercicio de la competencia administrativa. En mi opinión, ha de considerarse de la misma forma cualquier programa desarrollado específicamente por o para la actividad administrativa siguiendo las instrucciones dictadas por la Administración. Las cláusulas de exención de responsabilidad que pueden encontrarse en algunas sedes electrónicas no podrán eliminarla en la práctica, habida cuenta del tenor de los artículos 38.2 y 38.3 de la ley 40/2015. Su inclusión resulta tan abusiva como si se estableciera para la información proporcionada por los empleados públicos a los administrados de forma presencial en la sede física.

La fuerza mayor se caracteriza por la imprevisión, inevitabilidad y origen externo, diferenciándose del caso fortuito, supuesto, este último, en el que sí puede existir responsabilidad patrimonial. En el ámbito de la Administración electrónica, la caída de la red debida a un terremoto o un rayo sería considerada fuerza mayor, mientras que, ajeno a motivos similares, el caso fortuito podría incluir la saturación o caída de servidores, sedes y portales electrónicos, registros telemáticos o sistemas de notificaciones, entre otros, si bien el uso de la palabra "fortuito" puede ser poco acertado en los casos en que las caídas se deban a una programación inadecuada que no resista ataques malintencionados que busquen, precisamente, la denegación de servicio. De hecho, la situación más habitual se corresponderá con una actuación objetivamente inadecuada o técnicamente incorrecta, con infracción de los estándares medios admisibles de rendimiento y calidad de los servicios.[1322]

[1322] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 460-469.

El artículo 34 de la precitada ley 40/2015 establece que solo serán indemnizables las lesiones producidas al particular provenientes de daños que este no tenga el deber jurídico de soportar de acuerdo con la ley, pero excluye de indemnización los que se deriven de hechos o circunstancias que no se hubiesen podido prever o evitar según el estado de los conocimientos de la ciencia o de la técnica existentes en el momento de producción de aquellos, algo que no parece fácilmente aplicable a los errores de programación o a la materialización de los riesgos a los que se someten los sistemas informáticos. Cuando se afirma que "*el desconocimiento de los riesgos, de los posibles efectos dañosos de una actividad, exime de responsabilidad en el caso de que se produzcan daños*"[1323] se hace referencia a la falta, en ese momento, del adecuado saber que se alcanzará en un momento futuro como fruto de un proceso de investigación científica. Los riesgos informáticos no pueden considerarse como tales, puesto que son conocidos, analizados, evaluados y, con frecuencia, indebidamente infravalorados. Esa "*ignorancia como eximente*" no es aplicable, en mi opinión, a un órgano administrativo que ostenta la competencia de aprobar la programación de un sistema informático y se escuda en la falta de conocimientos técnicos suficientes para conocer el acierto o el desatino, accidental o intencionado, del *software* que ha aprobado y puesto en servicio. Más que ante un caso de ignorancia como eximente, podría tratarse de una imputación por *culpa in vigilando, in omitendo, in eligendo*, reconducible al funcionamiento anormal de los servicios públicos[1324]. En cualquier caso, esa cláusula de exclusión de la responsabilidad por riesgo tecnológico, conlleva que los daños o lesiones deban ser soportados por quienes aceptan voluntariamente los riesgos inherentes a la intervención de la

[1323] ESTEVE PARDO, J. (2003), riesgos desconocidos, 61.
[1324] *Vid*. GALLEGO CÓRCOLES, I. (2008), *in vigilando*, 267-270.

que resultan[1325], voluntariedad que difícilmente puede suponerse a los obligados a relacionarse electrónicamente con la Administración, y sí a esta, quien se beneficia de los múltiples aspectos positivos proporcionados por la eAdministración. Afirma Esteve Pardo que "*Las decisiones con márgenes de incerteza o de desconocimiento de los riesgos que generan serán, desde luego, más precavidas y prudentes si quien las adopta responde de las mismas, aunque no se conozcan con seguridad los riesgos y efectos negativos derivados de esas decisiones*"[1326].

La posibilidad de imputar a la Administración los daños ocasionados por sus contratistas es técnicamente viable cuando ha incumplido sus deberes de inspección sobre la ejecución del contrato administrativo, ya sea por su pasividad absoluta o por el carácter deficiente o insuficiente del obrar administrativo. Pero, suponiendo que a la Administración, en su cualidad de garante, le corresponde evitar la producción del resultado lesivo, ¿cuál es la acción que debe realizar la Administración? Si bien la revisión y prueba minuciosa del código programado puede llegar a ser casi imposible, en mi opinión, ello no libera a la Administración de su responsabilidad, pues ha asumido el riesgo de perder el control de sus aplicaciones optando por la externalización, en lugar de afrontar el desarrollo con sus propios recursos humanos. Con ello, la Administración está perdiendo el control de las máquinas que ejecutan actos administrativos, otorgándoselo a los trabajadores del sector privado. Debe ser consciente de que la responsabilidad administrativa incluye también la responsabilidad tecnológica del correcto funcionamiento de las máquinas utilizadas por los organismos públicos[1327]. De hecho, el artículo 38.2 de la ley 40/2015 asocia el establecimiento de una sede electrónica con la responsabilidad

[1325] MARTÍNEZ GUTIÉRREZ, R. (2009), Administración pública electrónica, 463.
[1326] ESTEVE PARDO, J. (2003), riesgos desconocidos, 56.
[1327] EDOARDO FROSINI, T. (1984), informática y Administración pública, 454.

de su titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma, sin perjuicio de la exoneración de responsabilidad contemplada por el artículo 17 de la ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico[1328].

Sabemos que el *software* falla con elevada frecuencia, que están catalogadas numerosas amenazas potenciales y que el ENS establece cuantiosas medidas de seguridad que habría que cumplir. Por todo ello, es interesante examinar estos aspectos en una sentencia donde ninguno de ellos se ha revisado, donde parecen detectarse datos erróneos en los ficheros de la Administración y el reclamante no obtiene una resolución favorable. Se trata de la reciente STSJ de Madrid 1140/2015, sala de lo contencioso, de fecha 30 de enero de 2015, cuya lectura abre las puertas a la reflexión. Refiere el caso de un trabajador que está en posesión de seis informes de vida laboral emitidos entre 2009 y 2012, en los cuales figura un determinado período de cotización de ocho años. En marzo de 2013, ese periodo aparece sustituido por otro de tan solo seis meses, con el considerable perjuicio que puede ocasionar, al repercutir en el cálculo de la pensión de jubilación. Solicitada la rectificación de la vida laboral, su petición es desestimada, viéndose condenado en costas por el TSJ.

En la sentencia se omiten toralmente los aspectos informáticos del caso, basándose únicamente en la resolución de 29 de agosto de 2013 de la jefa de la Unidad de impugnaciones de la Dirección provincial de Madrid de la TGSS, donde se trae a colación la doctrina del Supremo referida a los informes de vida laboral, según la cual "*estos documentos,*

[1328] *Vid*. VALERO TORRIJOS, J. (2008), acceso a los servicios, 253.

reflejan exclusivamente la información contenida en los Ficheros de Datos de esta Tesorería General, fundamentalmente el General de Afiliación, sin que lleguen a constituir estado ni a declarar situaciones jurídicas invocables por el interesado ni siquiera hacia el futuro, por ejemplo, ante la solicitud o reconocimiento de futuras prestaciones".

El recurrente puede probar fehacientemente que en las fechas 3/3/09, 9/6/09, 27/9/10, 17/6/11, 9/3/12 y 31/7/12, en el fichero de afiliación aparecía el dato correspondiente a los ocho años cotizados. En cambio, en 2013, ese período aparece limitado a seis meses. No consta en la sentencia que se haya comprobado la calidad de los datos existentes, cuando hay pruebas irrefutables de que un año antes eran diferentes.

Desde el punto de vista informático, se plantean muchos interrogantes y algunas certezas preocupantes. Para comenzar, cabe cuestionar el respeto del principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones públicas a través de medios electrónicos, reconocido por la LAE en su artículo 4.h), que ahora la ley 40/2015 invoca en su preámbulo y exige para la sede electrónica. Se ha incumplido en las seis ocasiones anteriores o en la actualidad, pero en alguno de los momentos la información registrada no era auténtica. Aparentemente, tampoco se ha garantizado la integridad de la información, puesto que la misma ha sido alterada, se diría que de manera no autorizada, y parece haberse impedido también la trazabilidad, que permitiría saber quién modificaron esos datos.

Ante un problema similar, la primera comprobación que deberían realizar los informáticos que presten servicio a la Administración sería averiguar si la modificación de la

información fue realizada por algún usuario o proceso determinado. A tal efecto, hemos de recordar aquí la medida de seguridad op.exp.8 (registro de la actividad de los usuarios) descrita *supra*, en combinación con la op.exp.10 (protección de los registros de actividad).

En caso de que no haya quedado registrada tal modificación, lo adecuado sería determinar, con la mayor aproximación posible, el momento en que ocurrió, para lo cual habría que recurrir a la medida de seguridad contemplada por el ENS como mp.info.9 (copias de seguridad o *backup*). Se trataría de recuperar la copia de seguridad existente más cercana al día 31/7/12 (fecha del último informe de vida laboral en el que se sabe con certeza que el dato original estaba grabado en el fichero de afiliación), tanto anterior (para verificar la existencia de la información perdida) como posterior (para comprobar si permanece inalterada o ya ha sido modificada). La localización de las copias de seguridad más cercanas a la alteración permitirá acotar el periodo en que ese cambio pudo ocurrir. La periodicidad en la realización de las copias y el tiempo de retención de las mismas serán factores críticos. Si se dispusiese de una copia de respaldo diaria, podría determinarse la fecha exacta de la modificación, permitiendo así investigar en profundidad lo ocurrido durante esas horas, incluyendo los *logs*, para tratar de determinar quién y por qué motivo se realizó el cambio. Si únicamente se dispone de una copia mensual, la dificultad sería notablemente mayor.

Si con ello no se determina en qué forma se produjo la alteración, resultaría imprescindible la revisión del *software*, aunque las esperanzas de encontrar el hipotético fallo podrían ser escasas. Un problema fácil de detectar probablemente habría originado una pluralidad de errores similares. Si solo ha ocurrido en una ocasión, o en pocas, su origen podría

hallarse relativamente alejado y deberse a una combinación de acontecimientos en principio inimaginable. Los problemas para llegar a determinar lo sucedido serán mayores en el caso de que su origen haya sido intencionado, materializando la amenaza [A.15] (modificación deliberada de la información) o mayor incluso si el autor fue personal informático con accesos privilegiados, pudiendo convertir en realidad simultáneamente la amenaza [A.3] (manipulación de los registros de actividad – *logs*).

Habida cuenta de que la doctrina del Tribunal Supremo acepta la validez de la información que figura actualmente en el fichero, ello abre la puerta a reflexionar sobre los riesgos que sufren nuestros datos. Recordando las afirmaciones que Esteve Pardo dedica a los riesgos sobre la salud, y salvando las diferencias, ¿podríamos aplicar los mismos principios a los riesgos producidos por las tecnologías informáticas? La cuestión planteada versa sobre el modo en que el Derecho resuelve las situaciones de incerteza, en particular mediante presunciones, el traslado de la carga de la prueba o la aplicación del principio de precaución[1329]. En el caso referido, el riesgo existente se ha materializado y la integridad, autenticidad y trazabilidad de la información parecen haberse visto afectadas. Se presume válida la información existente en la actualidad en los ficheros de la GISS, pero también parecen ser auténticos (y contradictorios con los datos actuales) los informes aportados por el recurrente, quien sobradamente ha probado cuál era la situación de su vida laboral recogida en el fichero en las fechas señaladas. Llegados a este punto, el recurrente no tiene capacidad para probar la forma en que se ha producido esa modificación de los datos, mientras que la Administración tiene a su disposición todos los recursos que, conforme al ENS, tiene obligación de mantener y que hemos descrito

[1329] ESTEVE PARDO, J. (2003), ciencia y Derecho, 143-144.

sobradamente *supra*. Por ello, es la Administración quien debería asumir la carga de la prueba de que la información actual es correcta y la antigua no. A su vez, el recurrente no tiene ni ocasión ni capacidad técnica para manipular la información almacenada en los ficheros de la GISS, mientras que cientos de informáticos que han (hemos) prestado servicio en la GISS hubieran (hubiéramos) podido manipular voluntaria o accidentalmente esa información dejando poco o, quizá, ningún rastro. Intuitivamente, podríamos considerar atentatorio contra el principio de precaución el hecho, ampliamente argumentado *supra*, de que la GISS ha depositado el poder de manipular los ficheros que contienen nuestra vida laboral en manos de empresas externas, en el sector privado. Pero, abandonando la intuición, ciñéndonos a lo que parece ser la realidad y tratando de llevar al terreno informático el principio de precaución que Esteve Pardo[1330] invoca en otros campos de la ciencia, nos encontramos ante una situación de incerteza en cuanto a cómo se ha materializado la pérdida de información, en la que los tribunales han aplicado la presunción de exactitud de los datos obrantes en la actualidad, algo opuesto al principio *in dubio pro* administrado.

La prohibición de *venire contra factum proprium* supone no lícita la adopción unilateralmente de decisiones incompatibles con la conducta mantenida con anterioridad en sus relaciones con otro, con la que se le haya generado una situación jurídica de algún modo favorable. Se trata de una exigencia de coherencia en el comportamiento que enlaza directamente con el principio de buena fe y el de confianza legítima[1331]. Sin embargo, aunque podría plantearse la cuestión de si la Administración queda vinculada por hechos reconocidos en

[1330] ESTEVE PARDO, J. (2003), ciencia y Derecho, 145.
[1331] SÁNCHEZ MORÓN, M. (2003), v*enire contra factum propiam*, 228.

certificaciones propias como las que obran en poder del recurrente, no siempre se entiende -más bien al contrario- que las certificaciones surten los efectos de los actos propios[1332], por lo que no sería aplicable en la sentencia concreta que se comenta. En ella, parece deducirse que se ha producido una violación de la seguridad de los datos personales, definida por el RGPD como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Cabe plantearse si el recurrente tendría derecho a ser indemnizado en virtud de la lesión que haya podido sufrir en sus bienes y derechos a consecuencia del funcionamiento de los servicios públicos, reconocido en el artículo 106.2 de nuestro Texto constitucional, que vino a consagrar el principio, acuñado con anterioridad, de la responsabilidad patrimonial de la Administración Pública[1333]. Nos encontramos ante un hecho imputable a la Administración (alteración de los datos referentes a los períodos de cotización a la seguridad social), un daño antijurídico (reducción del importe de la pensión de jubilación), un nexo causal (el incumplimiento de las medidas de seguridad por la GISS ha impedido la demostración de que la información que obraba en los certificados era la auténtica y no la que figura actualmente) y la ausencia de fuerza mayor. Por todo podría el recurrente ejercer la acción de responsabilidad patrimonial. Su pretensión muestra la dificultad de la concreción del daño, imposible de calcular con certeza al desconocer el número de pagas que puede recibir el recurrente desde el momento de su jubilación hasta su fallecimiento. Sin embargo, si resulta factible el cálculo de la cifra correspondiente a la cotización a la seguridad social que ha

[1332] SÁNCHEZ MORÓN, M. (2003), *venire contra factum propiam*, 226.
[1333] CUESTA DE LOÑO, P./ GÓMEZ-ACEBO & POMBO ABOGADOS, S.L.P. (2010), repetir contra el contratista, 145.

desaparecido del fichero, pudiendo reclamar la cotización de esas cantidades en los momentos en que hubieran debido tener lugar, sin perjuicio de la reclamación por daños morales que pudiera considerarse procedente.

8.4. LA RESPONSABILIDAD DEL CONTRATISTA

El artículo 214 del TRLCSP establece la obligación del contratista de indemnizar todos los daños y perjuicios que se causen a terceros como consecuencia de las operaciones que requiera la ejecución del contrato, con la salvedad de que hayan sido ocasionados como consecuencia inmediata y directa de una orden de la Administración, en cuyo caso será esta la responsable. Durante un año desde la producción del hecho, los terceros podrán requerir al órgano de contratación para que se pronuncie sobre a cuál de las partes contratantes corresponde la responsabilidad de los daños. Sin embargo, no parece probable su aplicación al proceso de desarrollo del *software* de las Administraciones públicas, habida cuenta del nulo contacto existente entre el contratista y el tercero durante la ejecución del contrato, salvedad hecha del posible incumplimiento de la normativa de protección de datos de carácter personal.

Sufridos daños y perjuicios por el incorrecto funcionamiento del *software* de las Administraciones públicas desarrollado por empresas externas, el posible resarcimiento del tercero parece apuntar al ejercicio de la acción de responsabilidad patrimonial contra el organismo público competente. En caso de que se reconozca la procedencia de la indemnización, sería abonada por la propia Administración titular de la prestación del servicio público, que es quien debe responder primero ante el usuario, en virtud del principio de economía procesal, reservándose el ejercicio de la acción de regreso contra el contratista.

La resolución que acuerde la procedencia de la indemnización debe señalar si procede o no esa acción de repetición contra el contratista, habiendo sido oído este previamente en el trámite de audiencia. Dicha repetición debe ejercitarse en un procedimiento autónomo posterior, con un nuevo trámite de audiencia, y su cuantía vendrá limitado por el *quantum* indemnizatorio efectivamente abonado por la Administración.

El régimen jurídico de la responsabilidad patrimonial de la Administración, objetiva no puede extenderse al contratista, cuya responsabilidad es subjetiva y ha de estar prevista en las cláusulas del expediente de contratación, por lo que, para poder ejercitar la acción de regreso, ha de acreditase su culpabilidad[1334].

8.5. LA RESPONSABILIDAD DEL TRABAJADOR

La indemnización por los daños y perjuicios causados por las autoridades y personal al servicio de la Administración, conforme al artículo36 de la ley 40/2015, en su artículo 36, la exigirán los particulares de forma directa a la Administración, si bien esta, cuando hubiere indemnizado a los lesionados, repercutirá de oficio al personal a su servicio que hubiera incurrido por dolo, o culpa o negligencia graves, previa instrucción del correspondiente procedimiento. La obligatoriedad de la acción de regreso queda matizada, en el mismo artículo, al contemplar cierto espacio de maniobra en cuanto a la ponderación del resultado dañoso producido, el grado de culpabilidad, la responsabilidad profesional y su relación con la producción del resultado dañoso. Sin embargo, las Administraciones públicas se resisten a

[1334] CUESTA DE LOÑO, P./ GÓMEZ-ACEBO & POMBO ABOGADOS, S.L.P. (2010), repetir contra el contratista, 145-147.

ejercitar esta acción de regreso, que se podría calificar de ignota[1335], lo que ha merecido críticas por cargar las consecuencias patrimoniales negativas de las conductas gravemente irregulares de los empleados públicos a los contribuyentes, en lo que se considera una práctica insana que deja inmune al funcionario, perpetuando las condiciones que dieron lugar a la lesión, desincentivando el comportamiento atento y diligente[1336]. En ausencia de repetición al autor material del daño, son los contribuyentes quienes deben sufragar la indemnización[1337].

La mejora de la regulación de la responsabilidad del personal a cargo de la ejecución del proyecto mejoraría aspectos como la utilización de la técnica del modificado como fraude[1338], que no es extraña en nuestras Administraciones.

En lo que se refiere específicamente al desarrollador, para poder emitir juicios sobre la responsabilidad ética del ingeniero del *software*, es necesario previamente conocer las particularidades de la profesión, las condiciones en que se ejerce el trabajo y su experiencia. En cualquier caso, se requiere una sólida formación ética que permita la obtención de un *software* que respete y valore a las personas, e impida que el desarrollador se convierta en un mero instrumento técnico en manos de otros. Las consecuencias perjudiciales que pueden derivar del funcionamiento un sistema informático defectuoso son difíciles de predecir, un inconveniente que crece según se incrementa la complejidad del sistema y que, paralelamente, se convierte en

[1335] SAURA FRUCTUOSO, C. (2015), ignota acción de regreso.
[1336] DOMÉNECH PASCUAL, G. (2008), acción de regreso, 6 y 8.
[1337] Saura Fructuoso, C. (2015). La ignota acción de regreso de la Administración en la era de la transparencia, la eficiencia y la responsabilidad. *Documentación Administrativa: Nueva Época* (2), 4.
[1338] GIMENO FELIÚ, J.M. (2010), mecanismos de control, 531.

un escollo a la hora de determinar a quién corresponde la responsabilidad por los defectos que puedan albergarse, por incumplir los plazos…[1339]

En una primera aproximación al problema, es posible examinar los defectos y las consecuencias asociadas a ellos desde la óptica de su predecibilidad, complementándola con un enfoque basado en su inmediatez. Así, las consecuencias inmediatas o directas son las que se derivan de la propia naturaleza de la acción, sean o no predecibles, es decir, se espere que ocurran o no. Al ingeniero del *software* se le considera responsable de las consecuencias predecibles y directas de sus propios desarrollos, las cuales se podrían asimilar a intencionadas, mientras que no se le recriminan las consecuencias indirectas. En cuanto a las directas impredecibles, por lo general, se derivan de un desconocimiento de la acción y sus consecuencias, algo que el ingeniero *software* tiene obligación de conocer por recaer directamente de la propia naturaleza de sus actividades profesionales. La responsabilidad es graduable en función de cuánto se haya satisfecho la obligación de prever las consecuencias directas.[1340]

A los ingenieros del *software* que, a su vez, disfrutan del *status* de empleado público, hemos de añadir la exigencia de algo que los ciudadanos esperan de los funcionarios, su entrega al trabajo bien hecho, como señala Sáinz Moreno, autor que, si bien no se refiere específicamente al personal informático, se muestra coherente con la necesidad, analizada *supra*, de observar la actitud mental del trabajador y corregir, en la medida de lo posible, las causas que generan malas consecuencias, habida cuenta de que "*no es posible realizar reformas en la*

[1339] GÉNOVA, G., GONZÁLEZ, M.R. Y FRAGA, A. (2007), *Ethical Education in Software Engineering*, 2.
[1340] GÉNOVA, G., GONZÁLEZ, M.R. Y FRAGA, A. (2007), *Ethical Education in Software Engineering*, 12-13.

Administración que tiendan a fortalecer el comportamiento éticamente positivo de los empleados públicos si no se tiene en cuenta la unidad de la vida humana que impide que se produzca la ruptura total entre la realización de la vida personal y la realización de las tareas que se asumen en la Administración pública"[1341]. La desmotivación se respira en el seno de nuestras Administraciones públicas, sin que la razón más aducida sea injusticia retributiva. Para un buen funcionario resulta tanto o más frustrante ser tratado como un objeto remplazable, sin que para el alto cargo haya diferencia entre un funcionario dedicado a su trabajo con excelencia y otro abiertamente incumplidor.[1342]

Cuando la Administración carece de medios o conocimientos y se enfrenta al reto de mantener los fines sin disponer de los medios, su papel pasa a ser el de garantizar la adecuada realización de sus cometidos, con los niveles de objetividad, accesibilidad y calidad exigibles, por las empresas del sector privado. Esa privatización constituye un presupuesto del llamado "Estado garante" que no sería concebido como tal si dispusiera de todos los medios para hacer efectivos sus fines. El Estado garante asume una responsabilidad de garantía de esas prestaciones.[1343]

9. CONCLUSIONES

I. Debemos asumir la certeza de que la Administración electrónica no siempre funcionará adecuadamente. Todo *software* contiene errores y la tasa de fallos se dispara temporalmente tras los imprescindibles cambios a los que es sometido. La modificación indebida

[1341] SÁINZ MORENO, F. (2004), ética pública positiva, 517-532.
[1342] IRURZUN MONTORO, F. (2010), ética y responsabilidad, 95-97.
[1343] ESTEVE PARDO, J. (2015), Administración garante, 21.

de una sola letra puede desencadenar un comportamiento totalmente imprevisto y muy difícil de detectar. Miles o millones de líneas de código forman los programas informáticos que dan vida a los ordenadores, los cuales ejecutan con obediencia ciega el *software* que su programador ha escrito, incluso cuando no es correcto, sin cuestionarlo. Por ello, los desarrolladores han de evitar prácticas inadecuadas que dificulten o impidan garantizar la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad, dimensiones que integran el concepto de seguridad, prioritaria para el desarrollo económico y social e imprescindible para la tutela de los derechos y el normal funcionamiento de la actividad administrativa.

II. La identidad personal digital resulta de especial importancia en el ámbito de la eAdministración, constituyendo un elemento valioso, merecedor de la protección del Derecho. Pero la gran heterogeneidad de sistemas, conceptos legales, requisitos y procedimientos habilitados en los distintos Estados miembros de la Unión, junto con la dificultad de movilizar al unísono a tantos países, se alzan como obstáculos ante los intentos de alcanzar una identidad digital única y una Administración electrónica interoperativa a nivel comunitario, una tarea ardua que se entorpece por la atribución de las competencias en materia de organización y funcionamiento de las Administraciones públicas a los propios Estados miembros.

En nuestro país, la existencia de un marco jurídico y tecnológico adecuado sustenta la utilización de la firma electrónica con validez equivalente a la de la firma manuscrita, siempre y cuando cumpla determinados requisitos. Aunque la tecnología involucrada es vulnerable, sus debilidades se mantienen poco divulgadas, pues pueden minorar notablemente el grado de confianza de la ciudadanía en la firma electrónica, aumentando las reticencias que aún

persisten sobre su uso. Algunos de esos aspectos problemáticos guardan relación con las vulnerabilidades del *software*, pero pueden mitigarse con un diseño seguro de las aplicaciones, recayendo sobre los desarrolladores, de nuevo, el peso de la seguridad.

III. Desde que nuestro ordenamiento jurídico inició su progresivo camino hacia la Administración sin papeles, adolece de obligaciones concretas para las Administraciones públicas que vayan acompañadas de consecuencias expresas a su incumplimiento, con el riesgo de que su ausencia relaje el riguroso cumplimiento de la normativa, alguna de enorme transcendencia, como es el ENS, que recoge los principios básicos y los requisitos mínimos que permitan una protección adecuada de la información en cada una de las dimensiones de la seguridad. El establecimiento de sanciones para los órganos administrativos incumplidores, sin duda, despertaría el interés de los altos responsables públicos, que hoy duerme profundamente mientras espera la llegada de tiempos mejores, presupuestariamente hablando.

IV. Es preciso gestionar los riesgos de las TIC asegurando la proporcionalidad en las medidas de protección adoptadas, de forma que incremente la confianza, aunque no existen sistemas informáticos totalmente seguros. Cualquier *software* basado en el comportamiento del usuario puede ser manipulado para hacer cosas que sus creadores no tenían previstas y que cualquier dispositivo conectado a una red puede verse comprometido por un tercero. Se precisa una actitud proactiva de cara a mantener el análisis de riesgos permanentemente actualizado, de forma que permita el mantenimiento de un entorno controlado, donde se minimicen hasta niveles aceptables mediante el despliegue de medidas de seguridad. La

justificación de costos/beneficios de las contramedidas son fundamentales para la construcción de una buena estrategia de mitigación que busque el equilibrio entre seguridad y productividad.

Buscando incrementar la productividad de la eAdministración y justificado por la necesidad de posibilitar el derecho, que no la obligación, de los ciudadanos a no aportar datos y documentos que obren en poder de las Administraciones públicas, crece día a día la potencialidad de la plataforma de intermediación del MINHAP, una interconexión de bases de datos que amenaza la confidencialidad de los datos de carácter personal, poniendo a disposición de miles de empleados públicos los datos personales de más de 38.000.000 de ciudadanos, ignorando el hecho de que este es el dueño de los datos y solo a él le corresponde ejercer el control de los mismos. Frente a ello, planteo una modificación sencilla, factible y necesaria, que permite al ciudadano habilitar o deshabilitar el acceso a sus datos a través de la plataforma a voluntad. Habida cuenta de que la Administración debe buscar la máxima eficacia del derecho fundamental de protección de datos de carácter personal, aplicando el principio *in dubio por libertate*, debe adoptarse siempre el sentido más favorable para la existencia y garantía del derecho fundamental puesto en riesgo. La modificación técnica que sugiero, otorga, sin duda, esa máxima eficacia e implica la programación de un *software* sumamente sencillo y económico.

V. La nueva legislación administrativa estatal posibilita la ampliación, mediante reglamento, del conjunto de obligados a relacionarse con la Administración por medios electrónicos. Simultáneamente, les niega el derecho a recibir asistencia en la utilización de los mismos. Pero, con frecuencia, los intentos por establecer esa interrelación resultan infructuosos debido a que la vertiginosa evolución de las TIC impide, en la práctica, el respeto estricto del

principio de neutralidad tecnológica, viéndose incapacitadas las Administraciones públicas para acompasar las versiones probadas de sus productos con el ritmo de actualización de los entornos informáticos de los ciudadanos y de las empresas. Quienes, por tal motivo, se ven impedidos para cumplir con su obligación, han de soportar, además, la carga de la prueba, una *probatio diabolica*. Considero necesario un radical giro jurisprudencial que, lejos de condenar al obligado, pase a estimar que el incumplimiento de la neutralidad tecnológica por la Administración condiciona el acceso a la información y los servicios electrónicos e impone restricciones indebidas, que no solo eliminan la culpabilidad del ciudadano, sino que podrían resultar susceptibles de indemnización. Los tribunales deberían apreciar este hecho y no repercutir al ciudadano las consecuencias de las carencias públicas. Ante los potenciales problemas en el funcionamiento de las aplicaciones, deberían reconocerse unas garantías específicas, configurando una presunción favorable para el ciudadano que interactúa electrónicamente, un principio *in dubio por actionem* electrónico.

VI. La seguridad ha de estar contemplada desde los inicios del desarrollo del *software*, que es, en sí mismo, una empresa difícil. Los riesgos se incrementan con su complejidad y tamaño, la ambigüedad y variabilidad de las especificaciones, inadecuada gestión de la demanda, los errores de estimación y fecha de entrega… La estimación del esfuerzo requerido en personal, coste y tiempo depende de factores inciertos, entre los que aparecen la capacidad de los analistas y los programadores y su continuidad, así como su experiencia en la aplicación, plataforma, lenguaje y herramientas… Que el *software* sea un producto muy difícil

de validar refuerza la necesidad de incrementar su control durante la etapa de desarrollo, con la pretensión de vigilar y mejorar su calidad y legalidad.

Aunque la complejidad alcanzada por la tecnología imposibilita, en la mayor parte de los sectores, que los empleados públicos tengan el conocimiento y control de sus posibles riesgos, en el ámbito de las TIC existen cuerpos especializados, suplidos frecuentemente por servicios externos notoriamente más costosos, lo que supone una progresiva pérdida de control de los proyectos asumidos y un paulatino desconocimiento de los aplicativos que dan vida al "empleado público electrónico".

VII. El perfil directivo contemplado en la metodología Métrica V3 está integrado por empleados públicos con autoridad para validar y aprobar cada uno de los procesos realizados durante el desarrollo del *software*. El resto de figuras, prominentemente técnicas, no se reconocen obligatoriamente como empleados públicos, pero el examen detallado de los distintos procesos proporciona la luz necesaria para valorar dónde resulta factible recurrir a la colaboración de personal externo y en qué casos está justificado manifestarse en contra de su intervención, especialmente en los supuestos de actuación administrativa automatizada, para la que el artículo 41.2 de la nueva ley 40/2015 reitera la obligación de establecer previamente el órgano u órganos competentes para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente, competencia que es irrenunciable y no puede cederse a empresas del sector privado.

VIII. Durante la planificación del sistema de información, para alinear las actuaciones posteriores con los objetivos de la estrategia corporativa, participan los responsables de los procesos de la organización, que cuentan con una visión estratégica, acompañados de los profesionales TIC. Los resultados de los trabajos realizados no revisten una complejidad técnica que impida su comprensión por el comité de dirección, órgano administrativo con capacidad de decisión llamado a realizar su aprobación, la cual debe entenderse emitida por la Administración incluso aunque en la planificación hayan intervenido empresas del sector privado y ello pudiera afectar a las especificaciones a las que hace mención el artículo 41.2 de la ley 40/2015.

IX. En el estudio de viabilidad se examina un conjunto concreto de necesidades, a las cuales dar solución a corto plazo, ahora desde criterios tácticos, contemplando las restricciones de tipo económico, técnico, legal y operativo, en aras a decidir si abandonar el proyecto o continuarlo. Entre sus actividades se incluye la valoración de las diferentes opciones de desarrollo (adquisición de productos *software* estándar del mercado, desarrollos por los usuarios finales, desarrollos a medida o reutilización), considerando el impacto tecnológico, organizativo y de operación y cuantificando recursos y plazos. Al igual que en el proceso anterior, la aprobación de la solución por el comité de dirección, órgano público con poder de decisión, es suficiente para considerar la evaluación del sistema realizada por la propia Administración a pesar de que hayan podido participar técnicos de empresas privadas.

X. El proceso de análisis del sistema de información requiere un buen entendimiento entre los usuarios expertos y el personal técnico, frecuentemente perteneciente a empresas privadas, algo que puede cuestionar la propia existencia de los equipos de calidad y

desencadenar demandas por cesión ilegal de trabajadores. El propósito del proceso de análisis incluye la obtención de una especificación detallada del sistema mediante un catálogo de requisitos válidos, consistentes y completos a cumplir por el *software* y una serie de modelos que cubran las necesidades de información, que encaja en la noción de "definición de especificaciones" aludida en el precitado artículo 41.2. Su aprobación por el comité de dirección podría requerir la intervención de un asesor técnico que explicase el contenido de los mismos, para que el comité de dirección tomase su decisión debidamente informado. Esta última afirmación puede hacerse extensible al proceso de diseño del sistema.

XI. Durante la construcción del sistema de información, en cuanto el *software* alcanza un determinado tamaño, el comité de seguimiento que debe aprobarlo no tiene capacidad para controlar ni comprender lo que hace el código, ni siquiera con asesoramiento técnico. La programación en general, y especialmente en la actuación administrativa automatizada, no se podrá externalizar, salvo en los casos en que se trate de programas manifiestamente simples, en los que el comité de seguimiento pueda aprobarla con el debido asesoramiento técnico.

XII. El comité de dirección será el encargado de aprobar la implantación y aceptación del sistema, momento en que la responsabilidad pasará al equipo de mantenimiento, pudiendo plantearse graves problemas en el caso de externalización durante el periodo de garantía.

XIII. Analizados los distintos procesos que completan el desarrollo de aplicaciones y los argumentos que tradicionalmente se plantean sobre las bondades o carencias de la externalización, aplicados a la obtención del *software* de las Administraciones públicas, la

balanza se inclina hacia el desarrollo por parte del personal público, pero, si finalmente se decide licitar un contrato, los pliegos de cláusulas administrativas particulares y los de prescripciones técnicas han de establecer cuidadosamente la atribución de obligaciones y responsabilidades que recaen entre las partes, algo que puede ser complejo en contratos de desarrollo y que puede verse dificultado por una interpretación excesivamente rigorista de lo que puede constituir un obstáculo para la competencia.

XIV. El contrato de colaboración público-privada, que comenzaba a utilizarse en casos de operaciones complejas, con necesidades especiales de financiación y un novedoso reparto de riesgos, parece perder fuerza con la nueva normativa que está llamada a regir en la materia, por lo que su utilización actual debe rechazarse.

XV. La alegación de fallos informáticos como impedimento para la realización de las más diversas actividades es frecuente por parte de los ciudadanos, las empresas e, incluso, los propios organismos públicos, sin que resulte inusual que el conflicto surgido llegue a los tribunales.

A la hora de juzgar las pretensiones de los ciudadanos, suelen invocarse el criterio de la diligencia debida, o su cara opuesta, la negligencia, para inclinar la balanza de la justicia. Sin embargo, no parece mantenerse la misma regla cuando se trata de obligados a relacionarse con la Administración por medios electrónicos, en cuyo caso prima esta imposición, sin apreciar el grado de diligencia empleado ni si la imposibilidad de utilizar esos medios se debe al incumplimiento del principio de neutralidad tecnológica por parte de los organismos públicos.

La falta de neutralidad tecnológica del *software* de nuestras Administraciones públicas posibilitaría la acción de responsabilidad patrimonial, reclamación que no se ejercita, en mi opinión, por la falta de conocimientos técnicos de los obligados a relacionarse por medios electrónicos, inermes por ello para lograr superar la *probatio diabolica* a la que se verían obligados.

10.BIBLIOGRAFÍA

ACCENTURE – CENTRO DE ALTO RENDIMIENTO (2008). ***Arquitectura orientada a servicios*** *(SOA). Cómo reformular la Arquitectura Corporativa para alcanzar el alto rendimiento*. https://www.accenture.com/es-es/insight-arquitectura-orientada-servicios.aspx (25 de agosto de 2016).

ADSUARA VARELA, B. (2016). **El consentimiento**. En J.L. Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

AEPD (2014). ***Guía para una evaluación de impacto*** *en la protección de datos personales*. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf (13 de julio de 2016).

AGUILAR ALONSO, I./ CARRILLO VERDÚN, J./ TOVAR CARO, E. (2008). Importancia de la gestión del proceso de la **demanda de TI**. *RPM-AEMES, 5*(2), 25-34.

AGUILAR ROS, R./ PALOMAR OLMEDA, A. (2011). **Procedimiento electrónico** (gestión electrónica de los procedimientos). En J.L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos*, 633-666. Navarra, España: Ed. Aranzadi.

ALABAU MUÑOZ, A (2004). ***La Unión Europea*** *y su política para el desarrollo de la Administración electrónica. Tras los objetivos de la Estrategia de Lisboa*. http://www.upv.es/~lguijar/socinfo/docs/Alabau2004Libro.pdf (2 abril 2016).

ALAMILLO DOMINGO, I./ URIOS APARISI, X. (2011). *La* ***actuación administrativa automatizada*** *en el ámbito de las Administraciones públicas. Análisis jurídico y metodológico para la construcción y la explotación de trámites automáticos*. Generalitat de Catalunya. Escola d'Aministració Pública de Catalunya.

ALLÍ ARANGUREN, J.C. (2006). Las **nuevas formas** de la actividad administrativa: participación, ejercicio privado de funciones públicas y gestión privada de servicios públicos. *Revista de estudios de la administración local y autonómica*, (302), 91-136.

ALMEIDA CERREDA, M. (2009). La **evaluación del desempeño** de los empleados públicos.: En particular, el establecimiento de sistemas de evaluación del desempeño en las Administraciones locales. *Anuario de Derecho Municipal* (3), 115-158.

ÁLVAREZ, D.A. (2014). **Identificación biométrica en gemelos**. *Skopein: La justicia en manos de la Ciencia*, (3), 50-59.

ÁLVAREZ CONDE, E. (Octubre, 1998). La **formación de los funcionarios** y las tecnologías de la información. En *V Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, Tecnimap'1998*, convocado por la Comisión Nacional para la Cooperación entre las Administraciones públicas en el campo de los sistemas y tecnologías de la información, COAXI, Salamanca, España.

ÁLVAREZ GARCÍA, V. (1999). ***La normalización industrial***. Valencia, España: Tirant lo Blanch.

ÁLVAREZ HERNANDO, J. (2004). **Firma electrónica**: seguridad a través de la Red. *LEX NOVA La revista,* (37), 5-10.

ÁLVAREZ RODRÍGUEZ, M. (2007). **Consorcio de AA.PP. europeas STORK**: Hacia un marco europeo de gestión de identidades electrónicas. En *X Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, X Tecnimap,* convocado por el Consejo superior de Administración electrónica, Gijón, España.

– (2011). ***El DNIe español*** *como puerta de entrada a servicios de Administración electrónica en Europa: Proyecto STORK*. http://administracionelectronica.gob.es/ctt/resources/Soluciones/213/Area%20descargas/Guia-del-proyecto-STORK.pdf?idIniciativa=213&id_Elemento=320 (31 de marzo de 2016).

AMADOR CONTRA, P. (2001). **Auditoría informática** en el sector bancario. En M. Piattini Velthius y E. del Peso Navarro (Coord.), *Auditoría informática - Un enfoque práctico* (509-532). Madrid, España: RA-MA editorial.

AMICH ELÍAS, C./ VELÁQUEZ ORTIZ, A.P. (2014). **La ciberdefensa y sus dimensiones** global y específica en la estrategia de seguridad nacional española. *ICADE. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales,* (92), 49-76.

AMUTIO GÓMEZ, M.A. (2006). Los **servicios paneuropeos** de administración electrónica. *IDP: revista de Internet, derecho y política*, (2), 4-22.

– (2012). Las **normas técnicas** de interoperabilidad relativas al documento electrónico. *MÉI: Métodos de Información*, *3*(4), 127-149.

APARICIO VAQUERO, J.P. (2002). *La **nueva contratación informática**. Introducción al outsourcing de los sistemas de información*. Granada, España. Editorial Comares.

AREITIO BERTOLÍN, J. (2010). Protección del ***Cloud Computing*** en seguridad y privacidad. *Revista española de electrónica*, (666), 42-48.

AREITIO BERTOLÍN, J./ AREITIO BERTOLÍN, T. (2007). Análisis en torno a la **tecnología biométrica** para los sistemas electrónicos de identificación y autenticación. *Revista española de electrónica*, (630), 52-67.

ARENILLA SÁEZ, M. (2011). ***Crisis y reforma** de la Administración pública*. La Coruña, España: Netbiblo.

ARIAS MARTÍNEZ, M.A. (2011). El **principio de objetividad** en el empleo público II: la objetividad como deber de los empleados públicos. *DA. Revista Documentación Administrativa*, (289), 183-209.

ARROYO YANES, L.M. (2012). La **carrera profesional** y la evaluación del desempeño de los funcionarios públicos. *Revista catalana de dret públic*, (45), 94-128.

AUDISEC. (2008). ***Retorno de inversión*** *(ROI) en proyectos ISO 27001:2005. Alineamiento con el estándar*. www.iso27000.es/download/Audisec_ROSI_ISO27000.pdf (15 de julio de 2016).

ÁVILA RODRÍGUEZ, C.M. (2012). Respeto de la **vida privada** y familiar. En C. Monereo Atienza y J.L. Monereo Pérez (dir.), *La Europa de los derechos – Estudio sistemático de la Carta de los derechos fundamentales de la Unión Europea* (157-180): Ed. Comares.

BALLESTEROS MOFFA, L.Á. (2010). *La* ***adjudicación de contratos en el sector público***. Navarra: Thomson Reuters - Civitas.

BAÑO LEÓN, J.M. (2015). La **reforma del procedimiento**. Viejos problemas no resueltos y nuevos problemas no tratados. *Documentación Administrativa: Nueva Época* (2).

BARROSO BARRERO, J. (2004). La administración electrónica en España: un análisis de sus **sectores clave**. *Información Comercial Española, ICE: Revista de economía,* (813), 55-72.

BERNADÍ GIL, X. (2005). **Derecho público** y administración electrónica: una visión panorámica. *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas,* (1), 211-241.

BERNAL BLAY, M.A. (2010). La **colaboración público-privada institucional**. *Revista Aragonesa de Administración Pública* (37), 93-138.

– (2014). La contratación de las **Entidades Locales** en el nuevo paquete legislativo europeo sobre contratación pública. *Revista de Estudios de la Administración Local y Autonómica: Nueva Época,* (2), 1-17.

BERROCAL LANZAROT, A.I. (2006). **La firma electrónica** y su regulación en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. *Foro, Nueva época*, (3), 397-465.

BISTARELLI, S./ FIORAVANTI, F./ PERETTI, P. (2006). ***Defense trees** for economic evaluation of security investments*. http://doi.ieeecomputersociety.org/10.1109/ARES.2006.46

BLANCO GALÁN, M. (2011). **Aseguramiento de calidad** del *software* en las Administraciones públicas. *Revista española de innovación, calidad e ingeniería del software (REICIS), 7*(2), 48-51.

BLANCO LÓPEZ, F. Observatorio de Contratación Pública. (7 de diciembre de 2015). "*La **contratación pública electrónica***". http://www.obcp.es/index.php/mod.opiniones/mem.detalle/id.212/relcategoria.121/relmenu.3/chk.8ab625f8e13461f009c5d60faccc27b5 (3 de marzo de 2017).

BOCANEGRA REQUENA, J.M./ BOCANEGRA GIL, B. (2011). *La Administración electrónica en España. **Implantación y régimen jurídico***. Barcelona, España. Atelier.

BOEHM, B.W./ PAPACCIO, P.N. (1998). *Understanding and Controlling **Software Costs***. *The IEEE Computer Society, 14* (10), 1462-1477.

BOIX PALOP, A. (2007). **La neutralidad tecnológica** como exigencia regulatoria en el acceso electrónico a los servicios administrativos. Revista general de Derecho administrativo (16).

– (2010). **Previsiones en materia de neutralidad** tecnológica y acceso a los servicios de la Administración. En L. Cotino Hueso y J. Valero Torrijos (dir.), *Administración electrónica - La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España* (305-322). Valencia, España: Tirant Lo Blanch.

BOSSI QUEIROZ, A./ FUERTES CALLÉN, Y./ SERRANO CINCA, C. (2001). El **capital intelectual** en el sector público. En línea, *5campus.org*, Descargado de http://www.5campus.org/leccion/cipub (6 de agosto de 2016).

– (2005). **Reflexiones** en torno a la aplicación del capital intelectual en el sector público. *Revista española de financiación y contabilidad, XXXIV* (124), 211-245.

BRU CUADRADA, E. (2007). La protección de datos en España y en la Unión Europea. Especial referencia a los **mecanismos jurídicos** de reacción frente a la vulneración del derecho a la intimidad. *IDP: revista de Internet, derecho y política* (5):78-92.

BUENO CAMPOS, E. (2013). El **capital intelectual** como sistema generador de emprendimiento e innovación. *Economía industrial*, (388), 15-22.

BUENO CAMPOS, E./ MERINO MORENO, C. (2007). El capital intelectual y la **creación de empresas** en la sociedad del conocimiento. *Encuentros multidisciplinares*, *9*(26), 1-10.

CABALLERO GIL, P. (2000). **Algunos hitos** de la criptografía del siglo XX. *Números*, (43-44), 405-408.

CAICEDO ORTIZ, H.E. (2010). **Algoritmo de factorización** para un computador cuántico. *Latin-American Journal of Physics Education 3*(2), 352-353.

CALVIÑO SANTAMARÍA, N. (2006). **Regulación y competencia en telecomunicaciones**: los retos derivados del nuevo marco normativo. *Información comercial española, ICE: revista de economía*, (832), 59-74.

CANO RODRÍGUEZ, M./ PRADO GARCÍA, S./ ROMÁN BOCANEGRA, J. (2013). **Colaboración Público-Privada**. Una nueva forma de relación. *White Papers - Associació Catalana d'Empreses Consultores*. http://www.consultoras.org/frontend/aec/descargar.php?idf= 23178 (24 de noviembre de 2016).

CANTERO MARTÍNEZ, J. (2011). El **principio de transparencia** en la ley de acceso electrónico de los ciudadanos a los servicios públicos. En J.L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos* (289-324). Navarra, España: Ed. Aranzadi.

– (2011). *La **sustitución del empleado público** por el trabajador privado: ¿es realmente posible y ventajosa la opción de externalizar funciones administrativas?* Conferencia impartida

dentro del curso de verano de la UNED titulado “Crisis económica y Función pública”, en Palma de Mallorca, el 4 de julio de 2011.

– (2013). **Criterios para la clasificación** del empleado público ¿funcionario o laboral? *Revista vasca de gestión de personas y organizaciones públicas* (5), 82-99.

CANTÓN, D. (2014). ***Computación cuántica*** *y el cambio de paradigma en seguridad*. https://www.certsi.es/blog/computacion-cuantica-y-el-cambio-de-paradigma-en-seguridad (3 de marzo de 2017).

CARO BEJARANO, M.J. (2013). **Peligros tecnológicos**. *Cuadernos de estrategia,* (159), 183-227.

CARPIO CÁMARA, M. (2016). **Seguridad del tratamiento** de los datos personales y notificaciones de violaciones de seguridad. En J.L. Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. 335-348. Madrid: Ed. Reus.

CARRASCO NÚÑEZ, Á. (2013). **Conceptos de seguridad informática** y su reflejo en la Cámara de Cuentas de Andalucía. *Auditoría pública: revista de los Órganos autónomos de control externo,* (61), 111-117.

CARRO FERNÁNDEZ-VALMAYOR, J.L. (2010). **Ética pública** y normativa administrativa. *Revista de Administración pública* (181), 9-37.

– (2014). **Reflexiones** sobre las transformaciones actuales del Derecho público, en especial del Derecho administrativo. *Revista de Administración Pública* (193), 11-44.

CASARES MARCOS, A. (2016). **Novedades** en materia de administración electrónica en la nueva legislación administrativa básica. *Revista jurídica de Castilla y León* (40), 61-100.

CASTILLO BLANCO, F.A. (2003). El **principio de seguridad jurídica**: especial referencia a la certeza en la creación del Derecho. *Documentación administrativa* (263-264), 21-72.

– (2016). ¿**Pueden los ayuntamientos** declarar al personal laboral en la condición de indefinido no fijo? http://www.acalsl.com/blog/2016/05/pueden-los-ayuntamientos-declarar-al-personal-laboral-en-la-condicion-de-indefinido-no-fijo (21 de marzo de 2017)

CASTILLO HOLGADO, A. **Innovación tecnológica** y regulación en el sector de las telecomunicaciones y los sistemas de información. En T. de la Quadra-Salcedo Fernández del Castillo, *Derecho de la regulación económica, IV. Telecomunicaciones* (25-81). Madrid, España: Ed. IUSTEL.

CASTILLO RUBÍ, M.A./ SANTANA DE LA CRUZ, N./ DÍAZ LOBATON, A.M./ ALMANZA RODRÍGUEZ, G./ CASTILLO RUBÍ, F. (2011-2012). **Teoría de números** en criptografía y su debilidad ante la posible era de las computadoras cuánticas. *CIENCIA ergo sum*, *18*(3), 264-273.

CCN. (2011). *Guía de seguridad (**CCN-STIC-803**) – Esquema nacional de seguridad – Valoración de sistemas*. https://www.ccn-cert.cni.es/guias /guias-series-ccn-stic.html

– (2011). *Guía de seguridad de las TIC (**CCN-STIC-808**). Verificación del cumplimiento de las medidas en el ENS*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

– (2013). *Guía de seguridad de las TIC (**CCN-STIC-400** v1.1). MANUAL STIC.* Disponible en https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

– (2013). *Guía de seguridad (**CCN-STIC 804**) - Esquema nacional de seguridad - Guía de implantación*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

– (2013). *Guía/norma de seguridad de las TIC (**CCN-STIC-807**) - Criptología de empleo en el esquema nacional de seguridad*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

– (2013). *Guía de seguridad de las TIC (**CCN-STIC- 820**). Guía de protección contra la denegación de servicio*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

– (2013). *Guía de seguridad (**CCN-STIC-821**) - Esquema nacional de seguridad - Normas de seguridad*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

– (2014). *Guía de seguridad de las TIC (**CCN-STIC-660**) – Seguridad en proxies*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html.

– (2014). *Guía de seguridad de las TIC (**CCN-STIC-823**) – Utilización de servicios en la nube*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html.

– (2014). *Guía de seguridad de las TIC (**CCN-STIC-850A**) - Implementación del esquema nacional de seguridad en WINDOWS 7 (cliente miembro de dominio)*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

– (2015). *Guía de seguridad de las TIC (**CCN-STIC-809**). Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento*. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

CENATIC. (2009). *Software de **fuentes abiertas** en la Administración electrónica. Análisis del impacto de la LAESCP en la Administración pública*. https://web.aoc.cat/wp-content/uploads/2014/09/LAECSP_analisis-administracion-publica.pdf (6 de agosto de 2016).

CEREZO MIR, J. (2002). Los delitos de **peligro abstracto** en el ámbito del Derecho penal del riesgo. *Revista de Derecho penal y criminología, 2ª época*, (10), 47-72.

CHAVES GARCÍA, J.R. (2015). *El BOE alumbra **siamesas administrativas**: Ley 39/2015 de Procedimiento y Ley 40/2015 de Régimen Jurídico*. https://delajusticia.com/2015/10/02/el-boe-alumbra-siamesas-administrativas-ley-392015-de-procedimiento-y-ley-402015-de-regimen-juridico/ (8 de enero de 2016).

– (2016). El procedimiento administrativo común de la Ley 39/2015: **nuevos forjados** sobre viejos cimientos. *Actualidad administrativa* (2).

CHINCHILLA MARÍN, M.C. (2009). El **contrato de colaboración** entre el sector público y el sector privado (CPP). En Jesús Colás Tenas y Manuel Medina Guerrero (Coord.) *Estudios sobre la Ley de contratos del sector público* (453-488).

CIDEC (2000). *Gestión del conocimiento y **capital intelectual***. www.cidec.net/cidec/pub/archivos/31.pdf (26 de julio de 2016).

COLOMO PALACIOS, R./ TOVAR CARO, E./ CARRILLO VERDÚN, J. (2004). El **factor humano**: instrumentos de medida competencial y estimación. *RPM-AEMES, 1*(2), 26-38.

COLOMO PALACIOS, R./ TOVAR CARO, E./ GÓMEZ BERBIS, J.M./ GARCÍA CRESPO, A. (2007). **Recomendaciones** para el desarrollo del capital humano desde la perspectiva de la mejora del proceso *software*. *RPM-AEMES, 4*(1), 1-8.

COMISIÓN DE LAS COMUNIDADES EUROPEAS (2001). *Seguridad de las redes y de la información: Propuesta para un **enfoque político** europeo*. COM(2001)298 final.

– (2003). *El **papel de la administración electrónica** en el futuro de Europa*. COM(2003) 567 final.

– (2004). ***Libro verde sobre la colaboración** público-privada y el Derecho comunitario en materia de contratación pública y concesión.* COM(2004)327 final.

– (2004). *Plan de acción para la **aplicación del marco jurídico** de la contratación pública electrónica.* COM(2004) 841 final.

– (2006). *Plan de acción sobre administración electrónica i2010: **Acelerar la administración electrónica** en Europa en beneficio de todos.* COM(2006) 173 final.

COMISIÓN EUROPEA. (2010). *Una estrategia para un **crecimiento inteligente**, sostenible e integrador*. COM(2010) 2020 final.

– (2010). *Plan de acción sobre administración electrónica 2011-2015. **Aprovechamiento de las TIC** para promover una administración pública inteligente, sostenible e innovadora.* COM(2010) 743 final.

– (2011). *Una **visión estratégica** de las normas europeas: Avanzar para mejorar y acelerar el crecimiento sostenible de la economía europea de aquí a 2020*. COM(2011) 311 final.

– (2012). *Liberar el potencial de la **computación en nube** en Europa*. COM(2012) 529 final.

– (2015). *Una estrategia para el **mercado único digital** de Europa*. COM(2015) 192 final.

– (2016). *Plan de Acción sobre Administración Electrónica de la UE 2016-2020. Acelerar la **transformación digital** de la administración*. COM(2016) 179 final.

CONSEJO DE ESTADO (2010). *Informe del Consejo de Estado sobre las garantías del **cumplimiento** del Derecho comunitario*. http://www.consejo-estado.es/pdf/derecho%20comunitario.pdf (28 de mayo de 2016).

COSSÍO CAPDEVILLA, A. (2013). La fiscalización de la **encomienda de gestión** como forma de autoorganización administrativa: poniendo límites a la huida del derecho

administrativo en materia de contratación pública *Auditoría pública: revista de los Órganos autónomos de control externo*, (61), 25-33.

COTINO HUESO, L. (2008). **Derechos del ciudadano**. En E. Gamero Casado y J. Valero Torrijos (Coord.). *La ley de Administración electrónica - Comentario sistemático a la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* (117-234). Navarra, España. Ed. Aranzadi.

– (2015). *Los derechos de los ciudadanos ante la* ***Administración electrónica***. http://documentostics.com/component/option,com_docman/task,doc_view/gid,1518/ (5 de mayo de 2016).

COX, M./ ROBERTS, M./ WALTON, J. (2011). ***IT Outsourcing*** *in the Public Sector: Experiences Form Local Government*. *Electronic Journal Information Systems Evaluation 14 (*2), 193-203.

CRESPO MORA, M.C. (2013). Las **obligaciones de medios y de resultado** de los prestadores de servicios en el DCFR. *Indret: Revista para el Análisis del Derecho* (2), 1-45.

CRIADO GRANDE, J.I. (2004). Midiendo los **usos y recursos** tecnológicos de las administraciones locales. *Revista de estudios de la administración local y autonómica* (294-295), 281-314.

CUESTA DE LOÑO, P. Y GÓMEZ-ACEBO & POMBO ABOGADOS, S.L.P. (2010). Cuidado con el derecho de la Administración a **repetir contra el contratista**. *Revista de estudios locales* (135), 145-147.

DAVARA FERNÁNDEZ DE MARCOS, L./ DAVARA RODRÍGUEZ, M.A. (2016). Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas: **novedades** en materia de Administración electrónica. *Actualidad administrativa* (1).

DAVARA RODRÍGUEZ, M.A. (2016). **Comentario de urgencia** del reglamento europeo de protección de datos. *LA LEY* 3702/2016.

DELGADO DE LUQUE, J.G. (2008). **Proceso de selección** de productos *software* en el Ministerio de defensa. *Revista española de innovación, calidad e ingeniería del software (REICIS), 4*(1), 50-52.

DELGADO GARCÍA, A.M./ OLIVER CUELLO, R. (Mayo-junio, 2006). **Regulación de la informática decisional** en la administración electrónica tributaria. En *IX Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, Tecnimap 2006*, convocado por el Consejo superior de Administración electrónica, Sevilla, España.

DÍAZ PÉREZ, J. (2011). Retos de la colaboración público-privada para el desarrollo de **infraestructuras públicas** (PPP). *Boletín económico de ICE, Información Comercial Española*, (3012), 15-32.

DÍEZ-PICAZO PONCE DE LEÓN, L. (2000). **Culpa y riesgo** en la responsabilidad civil extracontractual. *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid* (4), 153-166.

DIFFIE, W./ HELLMAN, M.E. (1976). ***New Directions*** *in Cryptography*. *IEEE Transactions on Information Theory*, *IT-22*(6).

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (2015). *Plan de* ***transformación digital*** *de la Administración general del Estado y sus Organismos públicos. Estrategia TIC 2015-2020.* http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/Estrategia_TIC/20151002-Plan-transformacion-digital-age-oopp.pdf (7 de agosto de 2016).

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA. Manual del integrador del ***MiniApplet*** v1.2 del Cliente @firma. https://sede.gobcan.es/repositorio_comun/galerias/galerias_descargas/MCFv1.2_manual-integrador_ES.pdf (27 de enero de 2017).

DOMÉNECH PASCUAL, G. (2008). Por qué la Administración nunca ejerce la **acción de regreso** contra el personal a su servicio. *Indret: Revista para el Análisis del Derecho* (2).

ECHEVARRÍA EZPONDA, J. (2007). **Gobernanza** de la sociedad europea de la información. *CTS: Revista iberoamericana de ciencia, tecnología y sociedad, 3*(8), 67-80.

EDOARDO FROSINI, T. (1984). **Informática y Administración pública**. *Revista de Administración pública* (105), 447-460.

ENISA (2011). *Seguridad y fiabilidad en las nubes de la Administración Pública - Informe para la **toma de decisiones***. https://www.incibe.es/file/NeYqRDXyqg6aO5H_qdVh60g (10 de julio de 2016).

– (2012). *Introduction to Return on **Security Investment**. Helping CERTs assessing the cost of (lack of) security*. https://www.enisa.europa.eu/_publications/introduction-to-return-on-security-investment/at_download/fullReport (7 de Agosto de 2016).

ESTEVE PARDO, J. (2003). **Ciencia y Derecho** ante los riesgos para la salud: evaluación, decisión y gestión. *DA. Revista Documentación Administrativa*, (265-266), 137-150.

– (2003). La protección de la ignorancia: exclusión de responsabilidad por los **riesgos desconocidos**. *Revista de Administración pública* (161), 53-82.

– (2006). Derecho y medio ambiente: problemas generales. El Derecho del medio ambiente como **Derecho de decisión** y gestión de riesgos. *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR*, (4), 7-16.

– (2014). La deconstrucción de las fórmulas de intervención administrativa: de la aplicación de la Ley a la **contractualización**. *Revista Vasca de Administración Pública*, (99-100), 1231-1239.

– (2015). La **Administración garante**. Una aproximación. *Revista de Administración Pública*, (197), 11-39.

FERNÁNDEZ FERNÁNDEZ, S. (2004). La **criptografía clásica**. *Sigma: revista de matemáticas, matematika aldizkaria*, (24), 119-142.

FERNÁNDEZ RODRÍGUEZ, J.J. Y SANJURJO RIVO, V.A. (2010). **Acceder o no** acceder: esa es la cuestión. En L. Cotino Hueso y J. Valero Torrijos (dir.), *Administración electrónica - La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España* (263-289). Valencia, España: Tirant Lo Blanch.

FERNÁNDEZ RODRÍGUEZ, T. R. (2015). Una llamada de atención sobre la regulación de las **notificaciones electrónicas** en la novísima Ley de Procedimiento Administrativo Común de las Administraciones Públicas. *Revista de Administración pública* (198), 361-367.

FERNÁNDEZ SÁNCHEZ, C.M./ RODRÍGUEZ MONJE, M./ PIATTINI VELTHUIS, M.G. (2013). **Calidad del producto *software***. *AENOR: Revista de la normalización y la certificación* (288), 30-35.

FUENTETAJA PASTOR, J.Á. (2009). La **carrera horizontal** en el empleo público: una oportunidad para las Administraciones parlamentarias. *Corts: Anuario de derecho parlamentario* (22), 61-75.

FUERTES LÓPEZ, M. (2014). ***Neutralidad en la red:*** *¿realidad o utopía?* Madrid, España. Editorial Marcial Pons.

FUNDACIÓN TELEFÓNICA (2008). Las TIC en la **Administración local** del futuro. http://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/24/ (7 de agosto de 2016).

– (2016). ***Ciberseguridad****, la protección de la información en el mundo digital*. http://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/531/ (20 de septiembre de 2016).

– (2016). *La* ***sociedad de la información*** *en España 2015*. http://www.fundaciontele fonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/483/ (7 de agosto de 2016).

FUSTER SABATER, A. Instituto de física aplicada CSIC y CCN. (2009). *Procedimientos de* ***cifrado en flujo***. http://digital.csic.es/bitstream/10261/24545/2/Flujo_2.pdf (15 de marzo de 2016).

GALÁN GALÁN, A./ PRIETO ROMERO, C. (2008). El ejercicio de **funciones públicas** por entidades privadas colaboradoras de la Administración. *Anuario de Derecho Municipal*, (2), 63-104.

GALÁN PASCUAL, C./ MAROTO ILLERA, R. (2013). *El **gobierno electrónico** en Europa: reflexiones y propuestas*. https://dialnet.unirioja.es/descarga/libro/572417.pdf (7 de agosto de 2016).

GALENDE DÍAZ, J.C. (2006). Principios básicos de la criptología: el **manuscrito** 18657 de la biblioteca nacional. *Documenta & Instrumenta*, (4), 47-59.

GALLEGO CÓRCOLES, I. (2008). Daños derivados de la ejecución de contratos administrativos: la culpa "***in vigilando***" como título de imputación. *Revista de Administración pública* (177), 265-291.

GAMERO CASADO, E. (2008). El Derecho administrativo ante la **Era de la Información**. En E. Gamero Casado y J. Valero Torrijos (Coord.). *La ley de Administración electrónica - Comentario sistemático a la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* (29-56). Navarra, España. Ed. Aranzadi.

– (2009). **Interoperabilidad** y administración electrónica: conéctense, por favor. *Revista de Administración pública*, (179), 291-332.

– (2015). *Desafíos del Derecho administrativo ante un **mundo en disrupción***. Granada, España: Ed. Comares, S.L.

– (2016). **Panorámica** de la administración electrónica en la nueva legislación administrativa básica. *Revista española de derecho administrativo* (175), 15-27.

GARCÍA GARCÍA, E. (17 de abril de 2013). ***Más recursos*** *tecnológicos para la Administración*. http://cincodias.com/cincodias/2013/04/16/economia/1366134471_88026_2.html (22 de julio de 2016).

GARCÍA GARCÍA, M.J. (2008). Los **principios constitucionales** de igualdad, mérito y capacidad: su plasmación en el Estatuto del Empleado Público. *Revista jurídica de Castilla y León*, (15), 129-156.

GARCÍA MEXÍA, P.L. (2001). La **ética pública**: Perspectivas actuales. *Revista de estudios políticos* (114), 131-168.

GELBSTEIN, E. (2011). **La integridad** de los datos: el aspecto más relegado de la seguridad de la información. *ISACA Journal 6*. http://www.isaca.org /Journal/Documents /11v6-Data-Integrity-Information-Securitys-Poor-Relation-spanish. pdf (3 de julio de 2016).

GÉNOVA, G./ GONZÁLEZ, M.R./ FRAGA, A. (2007). ***Ethical Education in Software Engineering****: Responsibility in the Production of Complex Systems. Science and Engineering Ethics 13*, (4), 505–522. En castellano en http://www.ie.inf.uc3m.es/grupo /docencia/reglada/Is1y2/Is1/ResponsabilidadIS.pdf (26 de diciembre de 2016).

GIL DURÁN, M.P. (2016). El **derecho de control** de los datos personales en la plataforma de intermediación de la nueva e-administración. *Revista de privacidad y Derecho digital* (5), 109-146.

GIMENO FELIÚ, J.M. (2010). La Ley de Contratos del Sector Público: ¿una herramienta eficaz para garantizar la integridad? **Mecanismos de control** de la corrupción en la contratación pública. *Revista española de Derecho administrativo*, (147), 517-535.

– (2012). **Delimitación conceptual** entre el contrato de gestión de servicios públicos, contratos de servicios y el CPP. *Revista española de Derecho administrativo* (156), 17-58.

– (2013). ***La modificación*** *de los contratos: límites y derecho aplicable*. Jornada sobre contratación pública. Madrid, 25 de abril de 2013. http://www.madrid.org/ccmadrid/images/adjuntos/segundaponencia_modificacin_contratos_gimeno_feli.pdf (18 de diciembre de 2016).

– (2016). **Novedades del anteproyecto** ley contratos sector público. La trasposición de las directivas de contratación pública en España. En *Congreso internacional sobre contratación pública*. Cuenca, 21 y 22 de enero de 2016.

GIMENO FELIÚ, J.M./ MORENO MOLINA, J.A. (dir.). GUERRERO MANSO, C./ FERNÁNDEZ ACEVEDO, R./ GALLEGO CÓRCOLES, I./ LAZO VITORIA, X./ MOREO MARROIG, T./ MEDINA ARNÁIZ, T./ VALCÁRCEL FERNÁNDEZ, P. (30 de enero de 2017). Propuesta de modificaciones y **mejora al Proyecto** de Ley de Contratos del Sector Público, por el que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo, 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (publicado en el Boletín oficial de las Cortes generales, Congreso de los Diputados 2 de diciembre de 2016). *Observatorio de contratación pública*.

GOBIERNO DE ESPAÑA. PLATAFORMA @FIRMA. (2016). ***Cambios asociados al reglamento eIDAS*.** http://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Area descargas/Cambios asociados al reglamento eiDAS en cuestion de identidad y firma electronica v-9.pdf?idIniciativa =190 &idElemento=6269 (7 de agosto de 2016).

GÓMEZ-BARROSO, J.L./ FEIJÓO GONZÁLEZ, C./ RAMOS VILLAVERDE, S. El reformado **marco europeo** regulador de las telecomunicaciones: ¿un avance para el mercado único? *Revista de Derecho comunitario europeo,* (40), 917-941.

GONZÁLEZ CALDERÓN, C./ FERRÁN RIERA, O. (2009). El ***software* libre** y las Administraciones públicas. Una visión actualizada. *IDP: Revista de Internet, derecho y política* (8), 25-35.

GONZÁLEZ GARCÍA, I. (2009). De oficina virtual a servicios transparentes. La **experiencia de la AEAT** en la aplicación de la ley 11/2007. En *La administración electrónica y el servicio a los ciudadanos - El Ministerio de economía y hacienda ante los retos de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos* (107-116). http://www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf (7 de agosto de 2016).

GONZÁLEZ GARCÍA, P. (2008). **Estudios de viabilidad**. *Revistas científicas de la universidad de Jaén.* revistaselectronicas.ujaen.es/index.php/pruebas/article/download /2/3 (28 de julio de 2016).

GONZÁLEZ RAMÍREZ, M.R./ GASCÓ GASCÓ, J.L/ LLOPIS TAVERNER, J. (2010). Razones y riesgos del *outsourcing* de sistemas de información: un análisis de su **situación y evolución**. *Investigaciones europeas de dirección y economía de la empresa, 6* (1), 55-76.

– (2015). Razones y riesgos del *outsourcing* de sistemas de información en las **grandes empresas españolas**. *Revista europea de dirección y economía de la empresa, 24* (3), 175-189.

GONZÁLEZ-VARAS IBÁÑEZ, S.J. (2006). **Nuevos desarrollos** de la idea de colaboración privada empresarial en el ejercicio de las funciones públicas. *Presupuesto y gasto público* (45), 31-39.

GRANJA ÁLVAREZ, J.C. (2001). **Auditoría del mantenimiento**. En M. Piattini Velthius y E. del Peso Navarro (Coord.), *Auditoría informática - Un enfoque práctico* (295-310). Madrid, España: RA-MA editorial.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. (8 de mayo de 2003). ***Documento de trabajo*** *sobre la administración en línea.* http://ec.europa.eu/ justice /policies/privacy/docs/wpdocs/2003/e-government_es.pdf (21 de abril de 2016).

GUASCH PORTAS, V./ SOLER FUENSANTA, J.R. (2016). Computación en la nube y **puerto seguro**. *RDUNED. Revista de derecho UNED* (18), 331-346.

GUILLÉN CAMARÉS, J. (2010). *La Administración electrónica: ¿**Mito o realidad** para los ciudadanos del siglo XXI?* http://cisp.ie.edu/sites/all/themes /cisp/pdf/adm_elec.pdf (7 de agosto de 2016).

GUILLÉN PINTO, E.P./ NAVARRO GASCA, J.J. (2006). Sistema de **distribución de claves** mediante criptografía cuántica para evadir ataques del tipo '*man in the middle*'. *Ciencia e Ingeniería Neogranadina, 16*(2), 64-73.

HERNÁNDEZ-ARDIETA, J.L./ GONZÁLEZ-TABLAS, A.I./ RAMOS, B. (2012). ***Repudio** de firmas electrónicas en Infraestructuras de Clave Pública*. http://163.117.149.64/papers /2008recsi3.pdf (19 de marzo de 2016).

HERNÁNDEZ ROJAS VALDERRAMA, R./ RIVAS TOVAR, L.A. (2008). La teoría de la **complejidad**: una nueva disciplina multicientífica y sus bases para la aplicación en la administración. *Universidad & Empresa, 10*(14), 129-154.

HERNÁNDEZ TRASOBARES, A. (2003). Los sistemas de información: **evolución y desarrollo**. *Proyecto social: Revista de relaciones laborales* (10-11), 149-165.

HERNÁNDEZ-LÓPEZ, A./ COLOMO PALACIOS, R./ GARCÍA CRESPO, Á. (2011). Medición de la **productividad** de los puestos de trabajo en ingeniería del *software. RPM 8* (1), 44-58.

HERNANDO RYDINGS, M. (2012). *La **colaboración público privada. Fórmulas contractuales***. Navarra: Thomson Reuters - Civitas.

HUERTAS MÉNDEZ, F.A. (2009). El *software* libre como **elemento de desarrollo** de la Administración electrónica. *IDP: revista de Internet, derecho y política*, (8), 36-47.

IDOATE GIL, A./ GARCÍA-MERÁS CAPOTE, T. (Septiembre, 2013). *Dificultades en la aplicación **práctica de la neutralidad** tecnológica en la Administración Electrónica innovadora*. Documento para su presentación en el IV Congreso Internacional en Gobierno, Administración y Políticas Públicas GIGAPP-IUIOG. INAP, Madrid, España.

IHERING, R. VON. ***La lucha por el derecho***. Biblioteca virtual universal. http://www.biblioteca.org.ar/libros/1721.pdf (22 de abril de 2016).

INCIBE (17 de julio de 2015). *Cómo gestionar una **fuga de información**. Una guía de aproximación al empresario*. https://www.incibe.es/empresas/guias/ Guia_fuga_informacion (3 de julio de 2016).

INSTITUTO NACIONAL DE SEGURIDAD E HIGIENE EN EL TRABAJO (2006). *Guía técnica de **evaluación y prevención** de los riesgos relativos a la utilización de equipos con pantallas de visualización*. http://www.insht.es/InshtWeb/Contenidos/Normativa/GuiasTecnicas/Ficheros/pantallas.pdf (1 de junio de 2016).

INTECO (2008). ***Guía avanzada de gestión de riesgos***. https://www.incibe.es/ file/ teW3c 753 nhRRK6a0e7iZKg (13 de julio de 2016).

– (2011). ***Cómo comprobar la integridad de los ficheros***. https://www.incibe.es /file/5ZOhqplBAZMCN-GUWrwDAQ (17 de marzo de 2016).

– (2012). ***Desmontando el malware***. https://www.incibe.es/file/_18H7L9lQPedm-YRQlNJucQ (18 de marzo de 2016).

– (2012). ***Estudio sobre riesgos de seguridad*** *derivados del software de uso no autorizado*. https://www.incibe.es/file/RKOfXVCd7NOC_bcRKSFfbg (13 de julio de 2016).

– (2012). ***Guía sobre riesgos y buenas prácticas*** *en autenticación online*. https://www.incibe.es/CERT/guias_estudios/guias/Guia_Autenticacion (20 de marzo de 2016).

INTECO-CERT (2011). ***Riesgos y amenazas en cloud computing***. https://www.incibe.es/file/uHEodcNkHfbaXKiMJlkT_g (10 de julio de 2016).

– (2012). *Gestión de* ***sesiones web****: ataques y medidas de seguridad*. https://www.incibe.es/file/AJql3gjLviflBliD4wnTxQ (22 de julio de 2016).

INTEL CORPORATION IBERIA (2009). La **ley de Moore** mantiene su vigencia. *Física y sociedad*, (20):33. http://www.cofis.es/pdf/fys/fys20/fys20_33.pdf (7 de agosto de 2016).

IRURZUN MONTORO, F. (2010). **Ética y responsabilidad** en la Administración pública. *Documentación administrativa*, (286-287), 79-111.

JARAUTA SÁNCHEZ, J. (Noviembre, 2007). Protección en la **cadena de confianza** de la documentación electrónica en la Administración pública. En *X Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, X Tecnimap*, convocado por el Consejo superior de Administración electrónica, Gijón, España.

JORDANO FRAGA, F. (1991). Obligaciones de medios y de resultados: (a propósito de alguna jurisprudencia reciente). *Anuario de derecho civil*, *44* (1), 5-96.

JUNTA CONSULTIVA DE CONTRATACIÓN ADMINISTRATIVA DE LA COMUNIDAD AUTÓNOMA DE ARAGÓN (2013). ***Recomendación 1/2013**, de 27 de febrero, relativa a la necesidad de aprobar en el ámbito del sector público unas instrucciones para la correcta ejecución de servicios externos*. http://www.aragon.es/estaticos/GobiernoAragon/OrganosConsultivos/JuntaConsultivaContratacionAdministrativa/Areas/02_Informes_Actuaciones/RECOMENDACION%201_2013.pdf (3 de septiembre de 2016).

JUNTA CONSULTIVA DE CONTRATACIÓN ADMINISTRATIVA DEL ESTADO (2016). ***Resolución de 16 de marzo de 2016**, de la Dirección General del Patrimonio del Estado, por la que se publica la Recomendación de la Junta Consultiva de Contratación Administrativa, sobre el efecto directo de las nuevas Directivas comunitarias en materia de contratación pública*. BOE de 17 de marzo de 2016.

JUNTA DE ANDALUCÍA. CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA (2012). *Firma electrónica **avanzada y reconocida***. https://ws024.juntadeandalucia.es/ae/descargar/4226 (9 de marzo de 2016).

– (2012). *Plataforma @firma. **Buenas prácticas** de seguridad en los procesos de autenticación y firma*. https://ws024.juntadeandalucia.es/ae/descargar/3936 (20 de marzo de 2016).

– (2013). ***Plataforma @firma**. Problemática con la actualización de Java 7 update 45.* https://ws024.juntadeandalucia.es/ae/descargar/4120 (23 de marzo de 2016).

KNUTH, D.E. (1974). *Computer* ***Programming as an Art***. *Communications of the ACM (Association for Computing Machinery), 17*(12), 667-673.

KRUGMAN, P.R./ WELLS, R./ OLNEY, M.L. (2008). ***Fundamentos de economía***. Barcelona, España: Reverté.

LABORATORIO NACIONAL DE CALIDAD DEL *SOFTWARE* - INTECO (2009). ***Ingeniería del software****: metodologías y ciclos de vida*. http://docplayer.es/1898708-Ingenieria-del-software-metodologias-y-ciclos-de-vida.html (21 de julio de 2016).

LAUDON, K.C./ LAUDON, J.P. (2014). ***Management Information Systems***. *Managing the Digital Firm*. Harlow, England:Pearson Education Limited.

LINARES GIL, M.I. (2008). **Identificación y autenticación** de las Administraciones públicas. En E. Gamero Casado y J. Valero Torrijos (Coord.). *La ley de Administración electrónica - Comentario sistemático a la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* (281-316). Navarra, España. Ed. Aranzadi.

LÓPEZ, J./ MAÑA, A./ MONTENEGRO, J.A./ ORTEGA, J.J. (2000). *Aspectos de* ***Implementación*** *de una Infraestructura de Clave Pública Distribuida*. https://www.nics.uma.es/pub/papers/JavierLopez2000.pdf (7 de agosto de 2016).

LÓPEZ MUÑOZ, J./ MARTÍNEZ NADAL, A./ PATEL, A. (2004). La **firma electrónica**, clave para la seguridad en la sociedad de la información. *Novática: Revista de la Asociación de Técnicos de Informática (ATI)*, (169), 3-4.

LÓPEZ PORTAS, M.B. (2015). La configuración jurídica del **derecho al olvido** en el Derecho español a tenor de la doctrina del TJUE. *UNED Revista de Derecho político,* (93), 143-175.

LÓPEZ TALLÓN, A. (2013). *El conflicto entre @firma y el principio de* ***neutralidad tecnológica***. http://www.microlopez.org/afirma-conflicto-neutralidad-tecnologica/ y http: //www.micro lopez.org/propuestas-desarrollo-afirma/ (22 de marzo de 2016).

LOZANO CUTANDA, B./ FERNÁNDEZ PUYOL, I. (2016). Hacia una nueva regulación de la **contratación *in-house*** en la transposición de la nueva Directiva sobre contratación pública y en la Ley de Régimen Jurídico del Sector Público. *Análisis GA&P*.

LUEDERS, H. (Septiembre - octubre, 2004). El marco europeo de **interoperabilidad**. Recomendaciones de la industria de las tecnologías de la información y comunicación. En *VIII Jornadas sobre Tecnologías de la Información para la Modernización de las Administraciones Públicas, TECNIMAP'2004*, convocado por la Comisión Nacional para la Cooperación entre las Administraciones Públicas en el campo de los sistemas y tecnologías de la información (COAXI), Murcia, España.

MACHO PÉREZ, A.B./ MARCO PEÑAS, E. (2014). El impacto de las colaboraciones público-privadas en los niveles de **déficit y deuda** públicos: análisis de los criterios de Eurostat. *Revista de Administración pública* (194), 437-474.

MACKINNON, R. (2012). *No sin nuestro consentimiento: la lucha por la* ***libertad en Internet***. Ed. Deusto. 1ª ed. en libro electrónico.

MADURGA OTEIZA, J.M. (2001). **Auditoría de aplicaciones**. En M. Piattini Velthius y E. del Peso Navarro (Coord.), *Auditoría informática - Un enfoque práctico* (445-465). Madrid, España: RA-MA editorial.

MAÑAS ARGEMÍ, J.A. (2003). La **confianza** y la seguridad aspectos vitales para los servicios electrónicos. *Novática: Revista de la Asociación de Técnicos de Informática (ATI),* (163), 58-62.

MAP. ***Métrica V3***. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html#.VtmxK9Cp3Dc (4 de marzo de 2016).

MARCOS MARTÍN, J.L./ BALSELLS TRAVER, M. (2000). La firma electrónica: **génesis y regulación**. *Boletín económico de ICE, Información Comercial Española,* (2646), 31-36.

MARTÍ DEL MORAL, A./ DE LA TORRE MARTÍNEZ, L. Las obligaciones de **servicio público**. En T. de la Quadra-Salcedo Fernández del Castillo, *Derecho de la regulación económica, IV. Telecomunicaciones*, 355-387. Madrid, España: Ed. IUSTEL.

MARTÍN DELGADO, I. (2008). **Identificación y autenticación** de los ciudadanos. En E. Gamero Casado y J. Valero Torrijos (Coord.). *La ley de Administración electrónica - Comentario sistemático a la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* (317-368). Navarra, España: Ed. Aranzadi.

– (2009). Naturaleza, concepto y régimen jurídico de la **actuación administrativa automatizada**. *Revista de Administración pública,* (180), 353-386.

MARTÍN GONZÁLEZ, Y. (2009). La **Unión Europea** y su política para la promoción de la ciberadministración en la sociedad de la información. *Anales de documentación*, (12), 159-179.

MARTÍN MORENO, F. (2013). El valor de la **experiencia profesional**. *BoleTIC (ASTIC)* (65), 58-59.

MARTÍN REBOLLO, L. (1992). La Administración de garantías: **vigencia y limitaciones**. *Revista del Centro de Estudios Constitucionales* (13), 31-54.

– (2000). Ayer y hoy de la responsabilidad patrimonial de la Administración: un balance y tres **reflexiones**. *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid* (4), 273-316.

– (2015). ***Leyes administrativas***, *volúmenes I y II*. Navarra, España: Thomson Reuters Aranzadi.

MARTÍN ROMERAL, L./ TORRES GALLEGO, A. (2008). Gestión de los **riesgos tecnológicos**. *Revista de procesos y métricas de las tecnologías de la información*, *5*(1) (2008), 15-23.

MARTÍN VALLES, D. (2014). La **gobernanza TIC** en la AGE y los recursos humanos. *BoleTIC (ASTIC)* (71), 52-54.

MARTÍNEZ DE DUEÑAS, C./ FERNÁNDEZ FÍRVIDA, M. (Octubre, 2007). **Tecnologías de desarrollo** para una Administración electrónica de calidad. En *X Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, X*

Tecnimap, convocado por el Consejo superior de Administración electrónica, Gijón, España.

MARTÍNEZ FERNÁNDEZ, J.M. (2016). ***Contratación pública y transparencia***. *Medidas prácticas para atajar la corrupción en el marco de la nueva regulación*. Madrid: Wolters Kluwer.

– (2017). **Medidas de transparencia** como antídoto contra la corrupción en la contratación pública. Revista jurídica de Castilla y León (41), 1-46

MARTÍNEZ GARCÍA, J./ ELEZ GÓMEZ, A.I. (2015). Comentario a las **nuevas directivas** europeas en materia de contratación pública (I). *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha*, (4), 147-167.

MARTÍNEZ GUTIÉRREZ, R. (2009). ***Administración pública electrónica***. Navarra, España: Thomson Reuters Limited. Ed. Aranzadi.

– (2011). **Cooperación y coordinación** entre administraciones públicas para el impulso de la Administración electrónica. La interoperabilidad. En J.L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos* (667-717). Navarra, España: Ed. Aranzadi.

– (2011). **Identificación y autenticación**: DNI electrónico y firma electrónica. En J.L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos* (407-454). Navarra, España: Ed. Aranzadi.

– (2015). *La **contratación pública electrónica**. Análisis y propuesta de transposición de las Directivas Comunitarias de 2014*. Valencia. Tirant Lo Blanch.

MARTÍNEZ ZORRILLA, D. (2009). Presentación monográfico ***Software* libre**. *IDP: revista de Internet, derecho y política,* (8), 2-3.

MATÍAS CLAVERO, G. (2005). La **estrategia de Lisboa** sobre la sociedad del conocimiento: la nueva economía. *Información Comercial Española, ICE: Revista de economía,* (820), 169-194.

MELIÁN GIL, J.L. (2013). Las **prerrogativas de la Administración** en los contratos administrativos: propuesta de revisión. *Revista de Administración Pública,* (191), 11-41.

MENÉNDEZ SEBASTIÁN, E.M. (2009). *Los **contratos de servicios del sector público**. Prestaciones intelectuales, asistencias y consultorías*. Navarra: Thomson Reuter - Civitas.

– (2016). La implementación de la Administración electrónica en **las nuevas Leyes**. *El Cronista del Estado Social y Democrático de Derecho* (63), 28-37. http://laadministracionaldia.inap.es (23 de enero de 2017).

MIGUEL MOLINA, M. DE. (2010). Análisis del derecho a la calidad de los servicios públicos prestados por la Administración electrónica desde el paradigma "renovado" de la **Nueva Gestión Pública** (NGP). En L. Cotino Hueso y J. Valero Torrijos (dir.), *Administración electrónica - La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a*

los Servicios Públicos y los retos jurídicos del e-gobierno en España (119-138). Valencia, España: Tirant Lo Blanch.

MINHAP. (2012). *Instrucciones sobre **buenas prácticas** para la gestión de las contrataciones de servicios y encomiendas de gestión a fin de evitar incurrir en supuestos de cesión ilegal de trabajadores*. http://libros-revistas-derecho.vlex.es/vid/anexo-iii-instrucciones-buenas-558340026 (2 de septiembre de 2016).

– (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. **Libro I – Método***.

– (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. **Libro II - Catálogo de Elementos***.

– (2012). ***Reutilización de activos y aplicaciones** en la Administración. Una oportunidad para la eficiencia a través de la apertura y la innovación*. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/OBSAE/pae_Notas_Tecnicas/2012-08_nota_tecnica_reutilizacion/2012-08_nota_OBSAE_reutilizacion.pdf (7 de septiembre de 2016).

– (2015). ***Declaración de servicios compartidos***. http://administracionelectronica.gob.es/_pae_Home/dms/pae_Home/documentos/Estrategias/Estrategia_TIC/20151002-Declaracion-servicios-compartidos.pdf (10 de octubre de 2016).

– (2015). ***Marco regulador para la declaración*** *de servicios compartidos*. https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/Estrategia_TIC/20151002-Marco-regulador-declaracion-servicios-compartidos.pdf (29 de octubre de 2016).

– (2015). *Reutilización de activos. Guía de publicación y* ***licenciamiento de activos***. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Gobierno_Abierto/pae_Reutilizacion_de_la_informacion_en_el_sector_publico/ENI_Guia_reutilizacion_activos_v1-0.pdf (11 de septiembre de 2016).

– (2016) ¡DIGITALÍZA-T! Guía para facilitar a las Entidades Locales el cumplimiento de las obligaciones digitales de las Leyes 39 y 40/2015. **Uso de las herramientas tecnológicas** de la DTIC. https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/Leyes-39-40/GUIA-PARA-EELL-PARA-EL-CUMPLIMIENTO-DIGITAL-DE-LAS-NUEVAS-LEYES-ADMINISTRATIVAS0/GUIA-PARA-EELL-PARA-EL-CUMPLIMIENTO-DIGITAL-DE-LAS-NUEVAS-LEYES-ADMINISTRATIVAS.pdf (7 de enero de 2017).

– (2016). ***Leyes 39 y 40****, novedades en el procedimiento administrativo. La visión de las Administraciones públicas con respecto a la aplicación de las nuevas leyes*. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/OBSAE/pae_Notas_Tecnicas/2016-06-nota-tecnica-OBSAE-leyes39y40.pdf (11 de septiembre de 2016).

– (2017). ***Catálogo de servicios*** *de verificación y consulta de datos SCSP*. Edición 1.27.0.

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO. ***Buenas prácticas*** *de calidad en el desarrollo de aplicaciones*. http://docplayer.es/8470203-Buenas-practicas-de-calidad-en-el-desarrollo-de-aplicaciones.html#download_tab_content (15 de julio de 2016).

– (2015). *La sociedad en red.* ***Informe anual 2014****. Edición 2015*. http://www.ontsi.red.es/ontsi/es/estudios-informes/informe-anual-la-sociedad-en-red-2014-edición-2015 (23 de marzo de 2016).

– (2016). *Estudio sobre la* ***ciberseguridad y confianza*** *en los hogares españoles*. http://www.ontsi.red.es/ontsi/sites/ontsi/files/ciberseguridad_y_confianza_en_los_hogares_espanoles_junio_2016.pdf (20 de septiembre de 2016).

MINISTERIO DE LA PRESIDENCIA (2010). ***Normalización*** *en seguridad de las tecnologías de la información.* http://administracionelectronica.gob.es/pae_Home_/dms/pae_Home/documentos/Estrategias/pae_Seguridad_Inicio/pae_Seguridad_Normalizacion_en_seguridad_TIC/Normalizacion_seguridad_3ed/Normalizaci%C3%B3n_seguridad_3%C2%AAed.pdf (12 de junio de 2016).

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA (2011). *60 + 1* ***prácticas de referencia*** *en el impulso de la Administración electrónica en España*.

– (2012). *Sustitución de Certificados en Soporte Papel.* ***Especificación Funcional*** *SCSPv3 1.0*.

MIRALLES LÓPEZ, R. (2009). **Modelos de evaluación** del impacto sobre la privacidad (PIA, "*Privacy lmpact Assessments*") y el artículo 34 de la ley 11/2007. En *La administración electrónica y el servicio a los ciudadanos - El Ministerio de economía y hacienda ante los retos de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*, 749-764. http://www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf (7 de agosto de 2016).

MOLES I PLAZA, R.J. (2001). ***Derecho y calidad***. *El régimen jurídico de la normalización técnica*. Barcelona, España: Ed. Ariel S.A.

MOLINA MATEOS, J.M. (2015). ***Aproximación jurídica*** *al ciberespacio*. http://www.ieee.es/publicaciones-new/documentos-de-opinion/2015/DIEEEO57-2015.html (8 de julio de 2016).

MONTALBÁN CARRASCO, R. (2013). Las tecnologías de la información, **impulsoras de la transformación** de la Administración pública española. *Economía industrial (EI),* (390), 117-126.

MONTORO CHINER, M.J. (2001). **Técnica legislativa** y evaluación de las normas. *Anuario jurídico de La Rioja*, (6-7), 155-172.

– (2003). **Seguridad jurídica**, principio de cautela y comités científicos. *DA. Revista Documentación Administrativa,* (265-266), 319-363.

MORENO MOLINA, J.A. (2015). Las **nuevas directivas** de la Unión Europea sobre contratación pública y su necesaria incorporación al Derecho español. *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha*, (extra 2), 227-256.

MUÑOZ SALINERO, E. (2011). El Centro de transferencia de tecnología. **Reutilización** en las AA.PP. *BoleTIC (ASTIC*) (57), 48-54.

MURILLO DE LA CUEVA, P.L. (1998). La construcción del derecho a la **autodeterminación informativa**. En *V Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, Tecnimap'1998,* convocado por la Comisión Nacional para la Cooperación entre las Administraciones públicas en el campo de los sistemas y tecnologías de la información, COAXI, Salamanca, España.

NAVAS NAVARRO, S. (2015). **Computación en la nube**: Big Data y protección de datos personales. *Indret: Revista para el Análisis del Derecho*, (4), 1-48.

NIETO GARRIDO, E. (2014). **Transparencia y acceso** a los documentos versus derecho a la protección de datos de carácter personal en la reciente jurisprudencia del TJUE. En J.L. Piñar Mañas (dir.), *Transparencia, acceso a la información y protección de datos*, 63-96. Madrid, España: Ed. Reus.

NORES TORRES, L.E. (2014). El **empleo público** en tiempos de crisis: la descentralización productiva en las AA.PP. *Revista General de Derecho Administrativo* (35).

NORTON, P. (2006). ***Introducción a la computación***. México D.F., México: McGrawHill Interamericana.

NOVOA BERMEJO, J.A. (2001). **Auditoría de técnica de sistemas**. En M. Piattini Velthius y E. del Peso Navarro (Coord.), *Auditoría informática - Un enfoque práctico*, 336-360. Madrid, España: RA-MA editorial.

ORDÓÑEZ SOLÍS, D. (2013). La administración electrónica en el contexto de la Unión Europea: **programación, legislación y financiación**. *Cuadernos de derecho local* (31), 23-39.

OROZCO PARDO, G. (2012). Respeto de la **vida privada** y familiar. En C. Monereo Atienza y J.L. Monereo Pérez (dir.), *La Europa de los derechos – Estudio sistemático de la Carta de los derechos fundamentales de la Unión Europea*, 133-156: Ed. Comares.

PABÓN CADAVID, J.A. (2010). La **criptografía** y la protección a la información digital. *Revista La propiedad inmaterial*, (14), 59-90.

PALOMAR OLMEDA, A. (2009). Administración electrónica y **actuación jurisdiccional**. En *La administración electrónica y el servicio a los ciudadanos - El Ministerio de economía y hacienda ante los retos de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*, 77-92. http://www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf (7 de agosto de 2016).

PARADA VÁZQUEZ, R. (2015). *Derecho administrativo I. Introducción. Organización administrativa. **Empleo público***. Madrid: OPEN Ediciones Universitarias.

PARADA VÁZQUEZ, R./ FUENTETAJA PASTOR, J. (2016). ***Derecho de la Función Pública***. Madrid: OPEN Ediciones Universitarias.

PAREDES MORENO, A. (2015). ***Big Data***: Estado de la cuestión. *International Journal of Information Systems and Software Engineering for Big Companies: IJISEBC 2*(1), 38-59.

PARRA SÁEZ, S./ CAMPANILLAS CIAURRIZ, J. (2010). El **procedimiento administrativo electrónico** y la normativa de protección de datos de carácter personal. En L. Cotino Hueso y J. Valero Torrijos (dir.), *Administración electrónica - La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España,* 807-818. Valencia, España: Tirant Lo Blanch.

PÉREZ ABELEIRA, M.A. (2006). **La belleza del *software***. *Cuadernos de la Facultad de Ingeniería e Informática UCS*, (1), 55-68.

PÉREZ VELASCO, M.M. (2006). **Intercambio de datos** entre Administraciones públicas. *IDP: revista de Internet, derecho y política*, (2), 45-51.

PIATTINI VELTHIUS, M.G. (2001). **Auditoría de bases de datos**. En M. Piattini Velthius y E. del Peso Navarro (Coord.), *Auditoría informática - Un enfoque práctico*, 311-333. Madrid, España: RA-MA editorial.

PIÑAR MAÑAS, J.L. (2011). **Administración electrónica** y protección de datos personales. *Dereito monográfico: estudios sobre la modernización administrativa*, 145-175.

– (2011). **Revolución tecnológica** y nueva Administración. En J.L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos*, 25-52. Navarra, España: Ed. Aranzadi.

– (2014). **Transparencia** y protección de datos. Una referencia a la ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. En J.L. Piñar Mañas (dir.), *Transparencia, acceso a la información y protección de datos*, 45-62. Madrid, España: Ed. Reus.

– (2016). Introducción. Hacia un **nuevo modelo europeo de protección de datos**. En J.L. Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. 13-20. Madrid: Ed. Reus.

PRADES LÓPEZ, A./ ESPLUGA TRENC, J./ HORLICK-JONES, T. (2015). **Riesgos tecnológicos**, conflictos sociales y políticas ambientales: del estudio de las percepciones a la implicación pública. *Papers: revista de sociología*, *100*(4), 395-423.

PRESIDENCIA DEL GOBIERNO (2013). ***Estrategia de ciberseguridad nacional***. www.dsn.gob.es/es/file/146/download?token=Kl839vHG (10 de julio de 2016).

PRESSMAN, R.S. (2010). ***Ingeniería del software. Un enfoque práctico.*** México D.F., México: McGrawHill.

PUNZÓN MORALEDA, J./ SÁNCHEZ RODRÍGUEZ, F. (2010). El "**sellado de tiempo**" ("*time-stamping*") como garantía del "no repudio temporal" en la ley de acceso electrónico de los ciudadanos a las Administraciones públicas. En L. Cotino Hueso y J. Valero Torrijos (dir.), *Administración electrónica - La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*, 709-728. Valencia, España: Tirant Lo Blanch.

QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T. DE LA. (2015). La primera ley española de Protección de Datos (**LORTAD**) y el proceso de su elaboración. En *20 años de protección de datos en España*, AEPD, 27-39.

QUINTANA DAIMIEL, A. (2015). **Análisis preliminar** de la nueva Ley Reguladora del Sector Público. *Actualidad administrativa* (11).

QUINTO ZUMÁRRAGA, F. DE. (2006). El **Documento Nacional de Identidad electrónico**. Un potente instrumento para superar la 'brecha digital'. *Revista de Derecho vLex*, (42).

RAMALLO MASSANET, J. (2007). El **control externo** en las nuevas formas de colaboración público-privada. *Revista española de control externo*, *9*(26), 13-34.

RAMIÓ MATAS, C. (2009). Teoría y práctica del **fenómeno de la externalización**. En C. Ramió (Coord.), *La colaboración público-privada y la creación de valor público*, 57-80. Colección_Estudios. Serie Gobierno Local, 14. Diputación de Barcelona.

RAMOS ESCOBOSA, J.M. (2001). **Auditoría de la Dirección**. En M. Piattini Velthius y E. del Peso Navarro (Coord.), *Auditoría informática - Un enfoque práctico*, 211-229. Madrid, España: RA-MA editorial.

RECUERDA GIRELA, M.Á./ FERNÁNDEZ DEPUECH, L. (2013). Los **contratos administrativos** que encubren relaciones laborales o tienen por objeto funciones reservadas al personal funcionario (partes I y II). *Revista General de Derecho Administrativo*, 32. Iustel. http://laadministracionaldia.inap.es/noticia.asp?id=1500353 y http://laad ministracionaldia.inap.es/noticia.asp?id=1500397 (1 de septiembre de 2016).

RIBAGORDA GARNACHO, A. (2011). **Aspectos técnicos** de seguridad en la ley 11/2007 y su reglamento de desarrollo parcial. En J.L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos*, 715-742. Navarra, España: Ed. Aranzadi.

RIBAGORDA GARNACHO, A./ AREITIO BERTOLÍN, J. (2004). Una **breve panorámica** de la criptografía. *Novática: Revista de la Asociación de Técnicos de Informática (ATI)*, (172), 8-9.

RIDAO I MARTÍN, J. (2012). **La colaboración público-privada** en la provisión de infraestructuras de servicio público. Revisión crítica y alternativas al actual marco regulador. *Revista catalana de dret públic*, (45), 191-214.

– (2013). **El contrato de colaboración** público privada para la provisión de servicios y obras de interés público en España. La incidencia de las futuras Directivas de la Unión Europea

para la modernización de la contratación pública y las concesiones. *Círculo de Derecho administrativo. Revista de Derecho administrativo*, (13), 241-260.

RIDAURA MARTÍNEZ, M.J. (2014). La **seguridad ciudadana** como función del Estado. *Estudios de Deusto 62*(2), 319-346.

RIVERO ORTEGA, R. (2011). **Simplificación administrativa** y administración electrónica: objetivos pendientes en la transposición de la directiva de servicios. *Revista catalana de dret públic*, (42), 115-138.

RODERO RODERO, J.A. (2001). **Auditoría del desarrollo**. En M. Piattini Velthius y E. del Peso Navarro (Coord.), *Auditoría informática - Un enfoque práctico*, 261-293. Madrid, España: RA-MA editorial.

RODRÍGUEZ, M., PEDREIRA, Ó./ FERNÁNDEZ, C.M. (2015). **Certificación de la mantenibilidad** del producto *software*: un caso práctico. *Revista latinoamericana de ingeniería de software*, *3*(3), 127-134.

RODRÍGUEZ, G.S. (2008). El ***software* libre** y sus implicaciones jurídicas. *Revista de Derecho: División de ciencias jurídicas de la Universidad del Norte* (30), 164-169.

RODRÍGUEZ DAPENA, P. (2009). Asegurar que el ***software* crítico** se construye fiable y seguro. *Revista española de innovación, calidad e ingeniería del software (REICIS)*, *5*(2), 38-48.

RODRÍGUEZ ESCANCIANO, S. (2010). Trabajador **indefinido no fijo** al servicio de la Administración e interino por vacante: similitudes y diferencias. *Aranzadi Social: Revista Doctrinal 3*(12), 33-42.

– (2012). ***Políticas de ajuste*** *del personal laboral al servicio del sector público local en un contexto de control del gasto*. Premio Fernando Albi 2012. Diputación de Alicante.

– (2015). *Poder de* ***control empresarial****, sistemas tecnológicos y derechos fundamentales de los trabajadores*. Valencia, España: Tirant Lo Blanch. 1ª ed. en libro electrónico.

RODRÍGUEZ RIVADULLA, F. (Mayo-junio, 2006). Auditoría informática en la Administración: un **reto para los profesionales TIC**. En *IX Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, Tecnimap 2006*, convocado por el Consejo superior de Administración electrónica, Sevilla, España.

ROIG BATALLA, A. (2009). **Intimidad y Administración electrónica**. En *La administración electrónica y el servicio a los ciudadanos - El Ministerio de economía y hacienda ante los retos de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*, 729-748. http://www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf (7 de agosto de 2016).

ROSADO, D.G./ BLANCO, C./ SÁNCHEZ, L.E./ FERNÁNDEZ-MEDINA, E./ PIATTINI VELTHUIS, M. (2010). **La seguridad** como una asignatura indispensable para un ingeniero del *software*. *XVI jornadas de enseñanza universitaria de la informática*.

Universidade de Santiago de Compostela. *Escola* Técnica Superior *d'Enxeñaría*, 205-212.

RUILOBA CASTILLA, J.C. (2006). La **actuación policial** frente a los déficits de seguridad de Internet. *IDP: revista de Internet, derecho y política,* (2), 52-62.

SÁINZ MORENO, F. (2004). **Ética pública positiva**. En F. Sáinz Moreno (dir.), *Estudios para la reforma de la Administración pública*, 517-532. España. INAP. http://libros-revistas-derecho.vlex.es/vid/etica-positiva-339394258 (26 de diciembre de 2016).

SALVADOR AYESTARÁN, I. (2001). La **firma digital**: una tecnología para la intercomunicación en la sociedad-red. *Revista española de documentación científica, 24*(1), 51-69.

SAN MARTÍN VILLAS, C./ TRICAS LAMANA, F./ MARTÍN FERNÁNDEZ, J./ GARCÍA FRANCÉS, V. **Creación de comunidades de usuarios**. Desarrollo de herramientas de e-Administración en EE.LL. En *IX Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, Tecnimap 2006*, convocado por el Consejo superior de Administración electrónica, Sevilla, España.

SÁNCHEZ, C. (2005). **Auge de concursos** públicos en el área de las TIC (1). *SOCINFO, Sociedad de la información* (19), 32-41. http://www.socinfo.info/contenidos/pdf19/ p32-40concursos.pdf (31 de agosto de 2016).

SÁNCHEZ GARCÍA, S. (2012). **Tendencias pan-europeas** en gestión de identidad digital. Ciudadanía y Administraciones Públicas. *Telos. Cuadernos de comunicación e innovación,* (91).

SÁNCHEZ GARCÍA S./ GÓMEZ OLIVA, A. Gestión de la identidad entre las Administraciones públicas. **Interoperabilidad pan-europea**. http://oa.upm.es/23019/1/INVE_MEM_2009_142759.pdf (23 de abril de 2016).

SÁNCHEZ LAMELAS, A. (2010). **El nuevo contrato** de colaboración público privada en el ámbito sanitario. *DS: Derecho y salud, 19*(Extra 1), 115-123.

SÁNCHEZ MEDINA, A.J./ MELIÁN GONZÁLEZ, A./ HORMIGA PÉREZ, E. (2007). El **concepto de capital intelectual** y sus dimensiones. *Investigaciones europeas de dirección y economía de la empresa, 13*(2), 97-111.

SÁNCHEZ MORÓN, M. (2003). ***Venire contra factum propiam*** *non valet*. *Documentación administrativa* (263-264), 223-246.

– (2011). El **empleo público en España**: problemas actuales y retos de futuro. *Revista Aragonesa de Administración Pública* (extra 13), 19-27.

– (2011). Sobre la **captura del empleo público**. *Revista Vasca de Gestión de Personas y Organizaciones Públicas* (1), 71-79.

SANGRONIZ GÓMEZ, J. (2004). Criptografía de clave pública: **el Sistema RSA**. *Revista Sigma* (25), 149-165.

SANTAMARÍA IBEAS, J.J.. (1994). **La LORTAD**. Breve análisis de sus antecedentes. *Informática y Derecho: Revista iberoamericana de derecho informático,* (4), 261-276.

SANTAMARÍA ZAPATA, F.J. (2007). Los recursos humanos en la **informática de la seguridad social**. *BoleTIC* (ASTIC) (44), 22-29.

SAURA FRUCTUOSO, C. (2015). La **ignota acción de regreso** de la Administración en la era de la transparencia, la eficiencia y la responsabilidad. *Documentación Administrativa: Nueva Época* (2).

SCHAULL, S.F. (2011). El '**desarrollo de *software***' como 'ingeniería de *software*'. *Ing. USBMed*, *2*(2).

SEGURINFO 2013.¿Cómo desarrollar **aplicaciones más seguras**? *XXVI congreso y feria de interamericana de seguridad de la información*. http://www.cybsec.com /upload/Seguinfo2013_Seg_Desarrollo_Software_Ardita_Stock.pdf (7 de agosto de 2016).

SEVILLA ANTÓN, I./ LÓPEZ TEJERA, L. Puesta en marcha del **Plan Avanz@** en convergencia con e-Europa. En *IX Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, Tecnimap 2006*, convocado por el Consejo superior de Administración electrónica, Sevilla, España.

SHANNON, C.E. (1949). ***Communication Theory of Secrecy Systems***. *The Bell System Technical Journal XXVIII*,(4), 656-715.

SOLÁ, R./ PRADES LÓPEZ, A./ ESPLUGA TRENC, J./ REAL, M. (2009). **Confianza, incertidumbre y percepción social** de las tecnologías avanzadas: un estudio de caso. *Revista internacional de sociología*, *67*(1), 161-175.

SORIANO MALDONADO, S. (2001). La firma electrónica en la UE y España: panorama del **marco regulatorio general**. *Economía industrial*, (338), 79-86.

SOSA WAGNER, F./ FUERTES LÓPEZ, M. (2007). ¿**Pueden los contratos quedar en casa**? (la polémica europea sobre la contratación *in house*). *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía* (3), 1669-1680.

STALLINGS, W. (2004). ***Fundamentos de seguridad en redes***. *Aplicaciones y estándares*. Madrid, España:Ed. Pearson Educación S.A.

STALLMAN, R. *El* ***peligro de las patentes de software***. http://www.gnu.org/philosophy/danger-of-*software*-patents.es.html (20 de mayo de 2016).

SUÁREZ VILLEGAS, J.C. (2014). **El derecho al olvido**, base de tutela de la intimidad: Gestión de los datos personales en la Red. *Telos. Revista de pensamiento sobre comunicación, tecnología y sociedad.* (97).

TABERA PÉREZ, O. (2016). De **los medios humanos y la experiencia** como criterio de valoración de ofertas en la contratación pública. *Observatorio de contratación pública*. http://www.obcp.es/index.php/mod.opiniones/mem.detalle/id.218/relcategoria.208/relmenu.3/chk.4c66a0e8143716a101936531b7e68603 (4 de enero de 2017).

TARRÉS VIVES, M. (2003). Las **normas técnicas** en el Derecho administrativo. *DA. Revista Documentación Administrativa*, (265-266), 151-184.

TASCÓN RUIZ, A. M. (2013). **Introducción: *Big Data***. Pasado, presente y futuro. *Telos: Cuadernos de comunicación e innovación*, (95), 47-50.

TOLIVAR ALAS, L. (2008). **El personal de la Administración** Local y el nuevo marco regulador de la función pública. Revista de estudios de la administración local y autonómica (308), 9-46.

TOMÁS MORALES, S. DE. (2014). Hacia una cultura de ciberseguridad: **capacitación especializada** para un "proyecto compartido". Especial referencia al ámbito universitario. *ICADE. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, (92), 13-47.

TOMÉ MUGURUZA, B. (2001). El plan de acción **INFO XXI**. La sociedad de la información para todos. *Economía industrial (EI)*, (338), 19-23.

TORRES CARBONELL, J.J. (2009). **El papel de la seguridad** en la prestación de servicios electrónicos. En *La administración electrónica y el servicio a los ciudadanos - El Ministerio de economía y hacienda ante los retos de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*, 233-242. http://www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf (7 de agosto de 2016).

– (2009). **Los servicios comunes como soporte** de la Administración electrónica. En *La administración electrónica y el servicio a los ciudadanos - El Ministerio de economía y hacienda ante los retos de la ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*, 217-226. http://www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf (7 de agosto de 2016).

TOVAR, E./ CARRILLO, J./ VEGA, V./ GASCA, G. (2006). **Desarrollo de productos** de *software* seguros en sintonía con los modelos SSE-CMM, COBIT e ITIL. *RPM-AEMES*, *3*(2), 62-69.

TRIBUNAL DE CUENTAS (2016). **Nº 1197. Informe de fiscalización sobre la utilización de la encomienda de gestión**, regulada en la legislación de contratación pública aplicable, por las entidades del sector público autonómico español durante el ejercicio 2013.

TRIBUNALES ADMINISTRATIVOS DE CONTRATACIÓN PÚBLICA. (1 de marzo de 2016). *Los **efectos jurídicos de las directivas** de contratación pública ante el vencimiento del plazo de transposición sin nueva ley de contratos del sector público*. http://noticias.juridicas.com/actualidad/noticias/11021-18-de-abril:-vencido-el-plazo-de-transposicion-de-las-directivas-sobre-contratacion-publica-procede-la-aplicacion-directa-de-las-mismas-/ (11 de diciembre de 2016).

TRONCOSO REIGADA, A. (2010). *La protección de datos personales. **En busca del equilibrio***. Valencia, España: Ed. Tirant Lo Blanch.

– (2011). **La Administración electrónica** y la protección de datos personales. En J.L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos*, 172-288. Navarra, España: Ed. Aranzadi.

UNIVERSIDAD DE ALICANTE. DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL. (2012-2013). ***Servicios Web y SOAP***. http://www.jtech.ua.es/j2ee/publico /servc-web-2012-13/wholesite.pdf (20 de abril de 2016).

URIOS APARISI, X./ ALAMILLO DOMINGO, I. (2007). Los **límites a la utilización del sello de órgano** por parte de las Administraciones públicas en la ley 11/2007. En *X Jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas, X Tecnimap*, convocado por el Consejo superior de Administración electrónica, Gijón, España.

VALERO TORRIJOS, J. (1998). **Administración pública, ciudadanos y nuevas tecnologías**. *Revista jurídica de la Región de Murcia*, (25), 13-35.

– (2002). **La Administración electrónica en el ámbito local** cinco años después. *Diario del Derecho municipal Iustel*. http://www.um.es/idertec/la-administracion-electronica-en-el-ambito-local-cinco-anos-despues/ (3 de mayo de 2016).

– (2007). **La nueva regulación legal** del uso de las tecnologías de la información y las comunicaciones en el ámbito administrativo: ¿el viaje hacia un nuevo modelo de Administración, *electrónica*?". *Revista catalana de dret públic*, (35), 207-246.

– (2008). **Acceso a los servicios** y difusión de la información por medios electrónicos. En E. Gamero Casado y J. Valero Torrijos (Coord.). *La ley de Administración electrónica - Comentario sistemático a la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*, 235-280. Navarra, España. Ed. Aranzadi.

– (2009). **Las garantías jurídicas** en la Administración electrónica ¿avance o retroceso? *Cuenta con IGAE,* (22), 19-28.

– (2013). ***Derecho, innovación y Administración electrónica***. Sevilla, España: Global Law Press.

– (2014). **De la digitalización a la innovación tecnológica**: valoración jurídica del proceso de modernización de las Administraciones públicas españolas en la última década (2004-2014). *IDP: revista de Internet, derecho y política,* (19), 117-129.

VERA PARRA, N.E./ LÓPEZ, D.A./ MANTA CARO, H.C. (2014). Modelo test-bed de simulación y evaluación de **criptografía de curva elíptica** en redes IPv6 de próxima generación. *Tecnura: Tecnología y Cultura Afirmando el Conocimiento, 18*(41), 27-37.

VERNAM, G.S. (1926). ***Cipher Printing Telegraph Systems***. *Journal of the American Institute of Electrical Engineers* (ahora IEEE) XLV, 109-115.

VIDA FERNÁNDEZ, J. (2009). El **marco normativo comunitario** europeo de la Administración electrónica. *Cuadernos de derecho local,* (21), 59-83.

VIZCAÍNO BARCELÓ, A./ GARCÍA, F./ PIATTINI, M. (2014). Visión general del **desarrollo global de *software***. *International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC) 1* (1), 8-22.

Wilhoit, K./ Hilt, S. (2015). ***North American Underground****: The Glass Tank.* Trend Micro Incorporated.

YSA, T. (2009). La **gestión de partenariados público-privados**: tipologías y retos de futuro. En C. Ramió (Coord.), *La colaboración público-privada y la creación de valor público*, 23-38. Colección_Estudios. Serie Gobierno Local, 14. Diputación de Barcelona.