ADMINISTRACIÓN ELECTRÓNICA Y SEGURIDAD. DOS CARAS DE LA MISMA MONEDA

José Luis COLOM PLANAS

Director de Auditoría y Cumplimiento Normativo
Entidad de Certificación del Esquema Nacional de Seguridad AUDERTIS

Trabajo de Evaluación presentado en el Curso: Cómo diseñar e implantar una Administración Local sin papeles (II edición)

SUMARIO:

1. EL DINAMISMO DE LA SOCIEDAD ACTUAL (ENTENDIENDO EL CONTEXTO)

La tecnología ha arraigado con fuerza en todas nuestras vidas siendo cada vez más difícil, si no imposible, mantenernos apartados de ella. Esta relación se justifica, siempre desde mi personal parecer, ya que la tecnología, más que poseer un valor intrínseco en sí misma, actúa como un catalizador de la evolución social y como tal debe ser entendida, aceptada, controlada y desmitificada.

Para refrendarlo, solo tenemos que ver cómo las nuevas tecnologías han cambiado la manera de trabajar, el modo de comunicarse, la forma de aprender e incluso de relacionarse. Y el Derecho está para regular y proteger estos avances de modo que sean sostenibles en el tiempo y aporten valor efectivo a la sociedad que, en el caso que nos ocupa, son los ciudadanos.

Derecho y Sociedad es un binomio intrínsecamente indivisible, ya que el primero es necesario para preservar la convivencia de las personas en la sociedad. Ésta debemos entenderla como el espacio donde el individuo se desarrolla física e intelectualmente, como un ser completo que es, interactuando con los demás directamente o sirviéndose de la tecnología. Y las Administraciones públicas son un actor más.

Así las cosas, es necesario que el Derecho esté permanentemente emparejado con la realidad social, lo que significa que debe acompañarla en su evolución para preservarla, pero nunca para ser un obstáculo a su evolución misma.

En otras palabras, las leyes deben ser coherentes con la realidad social a la cual regulan. Deben encauzar el uso de la tecnología preservando los derechos de las personas, sin que sea esta regulación un freno para la innovación. En esta línea se expresó ya en 2013 NEELIE KROES, comisaria de la Agenda Digital y Vicepresidenta de la Comisión Europea, en su intervención en el IAPP Europe Data Protection Congress en Bruselas.

2. LA ADMINISTRACIÓN ELECTRÓNICA O E-ADMINISTRACIÓN

2.1 Los objetivos últimos de la Administración electrónica

Los objetivos últimos de la e-Administración son lograr una Administración más cercana al ciudadano en tiempo y lugar, llevar a cabo la tan reclamada Transformación Digital para aumentar la eficacia y la eficiencia de los procedimientos administrativos, e incluso generar nuevas oportunidades de negocio digital para las empresas del territorio, a partir de los datos abiertos (open-data) como matrería prima.

La modernización de las Administraciones públicas debe ser el resultado de un proceso estudiado y razonado, de manera que seamos capaces de innovar transformando los servicios proporcionados, o creando nuevos, manteniendo lo que funciona bien y adaptando todo lo que pueda mejorarse, así como siendo conscientes de los recursos con los que contamos y las limitaciones a las que nos enfrentamos. Se puede y podemos innovar mucho y bien. Los ciudadanos y la mejora en los servicios prestados se presentan como el propósito último de la Transformación Digital que, como afirma ANTONIO IBAÑEZ de la Junta de Castilla y León, es el medio, no el fin.

2.2 Una nueva realidad social para la Administración electrónica

Como afirma VICTOR ALMONACID, quién forma parte del Comité de Imparcialidad de la entidad en la que ejerzo mi desempeño profesional: "*con las nuevas leyes de procedimiento administrativo y de régimen jurídico - Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPA) y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJ), respectivamente - el procedimiento electrónico es el único, ya que los actos administrativos se producirán por escrito a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia (art. 36 LPA).*

Además, el procedimiento, sometido al principio de celeridad, se impulsará de oficio en todos sus trámites y a través de medios electrónicos, respetando los principios de transparencia y publicidad (art. 71 LPA, "Impulso"). Como vemos, la LPA no deja lugar a dudas: los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice numerado de todos los documentos que contenga cuando se remita. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada. Además, el Registro es electrónico (art. 16), al igual que el Archivo (art.17), todo ello sin perjuicio de los "derechos electrónicos" de las personas (art. 13)".

Está claro que este "nuevo" escenario es consecuencia lógica de las cada vez mayores presiones sociales de la ciudadanía frente a la Administración pública, la cual ha de ser ágil, accesible desde cualquier lugar y dispositivo, y en cualquier momento. En un reciente debate que mantuve en un foro de CEMCI hacía notar que los llamados "milenials", los nativos digitales nacidos a partir del año 2000, adquirieron la mayoría de edad en 2018. No se trata de una simple anécdota o curiosidad cronológica, sino la consolidación de una forma de entender la sociedad actual de la que el Sector Público no puede sentirse desarraigado.

No obstante, la entrada en vigor de algunos preceptos de las leyes de procedimiento administrativo y de régimen jurídico se ha prorrogado hasta 2020, en cumplimiento de lo dispuesto en el al Real Decreto-ley 11/2018, de 31 de agosto, por el que se modifica la disposición final séptima de la Ley 39/2015 para ampliar en dos años el plazo inicial de entrada en vigor de las previsiones relativas a la puesta en marcha de la Administración electrónica. Como dice GERARDO BUSTOS, Subdirector general del Ministerio de Hacienda y Administraciones Públicas: "*Para unos este aplazamiento es una desgracia. Para otros el reconocimiento de una realidad. Apostemos por valorar la conveniencia de convertir el retraso en una oportunidad para hacer las cosas bien y llegar a 2020 en las mejores condiciones para un arranque íntegro de la Administración electrónica*".

2.3 Principios generales respecto a la Administración electrónica

Como constan en el preámbulo de la Ley 40/2015, son conocidos los principios de funcionamiento y actuación de las Administraciones Públicas de responsabilidad, calidad, seguridad, accesibilidad, proporcionalidad, neutralidad y servicio a los ciudadanos. En ese mismo preámbulo se contempla también como principio de actuación la interoperabilidad de los medios electrónicos y sistemas y la prestación conjunta de servicios a los ciudadanos. Ese principio tiene su desarrollo, pese a ser una norma jurídica anterior, en 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.

Como señala en su art. 2, sobre principios generales, el Proyecto de Real Decreto por el que se desarrollan la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en materia de actuación y funcionamiento del sector público por medios electrónicos, sometido a trámite de información pública el 23 de mayo de 2018,el Sector Público deberá respetar los siguientes principios en sus actuaciones y relaciones electrónicas:

a) Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas, para garantizar la independencia en la elección de las alternativas tecnológicas por las personas y por el sector público, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos, el sector público utilizará estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado. Las herramientas y dispositivos que deban utilizarse para la comunicación por medios electrónicos, así como sus características técnicas, serán no discriminatorios, estarán disponibles de forma general y serán compatibles con los productos informáticos de uso general, y no restringirán el acceso de las personas a los servicios electrónicos.

b) Principio de usabilidad, por el que se promueve que el diseño de los servicios electrónicos esté centrado en el usuario, de forma que se minimice el grado de conocimiento tecnológico necesario para el uso del servicio.

c) Principio de proporcionalidad en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos.

A pesar de que el legislador no ha incluido un principio con identidad propia, básico a mi entender cuando hablamos de servicios prestados a la ciudadanía apoyados en medios electrónicos, como es el principio de seguridad, al menos lo ha incardinado dentro del principio de proporcionalidad para destacar que la seguridad total no existe, igual que no existe el riesgo cero, y debe dotarse la seguridad necesaria a los trámites electrónicos tras analizar y evaluar los referidos riesgos. Es un hecho corroborado a lo largo del tiempo que nadie usa aquello en lo que no confía.

Todo ello sin menoscabo de los principios generales de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a las leyes y al Derecho en sentido amplio.

2.4 La Agenda Digital

Uno de los seis objetivos básicos de la Agenda Digital, concretamente el tercero, es mejorar la e-Administración y adoptar soluciones digitales para una prestación eficiente de los servicios públicos. Tiene como fin incrementar la eficacia y eficiencia de nuestras Administraciones y optimizar el gasto público, manteniendo al mismo tiempo unos servicios públicos universales y de calidad. La participación ciudadana y la utilización de canales electrónicos para la comunicación entre ciudadanos, empresas y Administraciones son factores clave por los que la Unión Europea ha apostado decididamente.

Para desarrollar este objetivo la Agenda Digital establece el desarrollo de un Plan de Acción de Administración Electrónica de la Administración General del Estado que permita acercar la Administración a ciudadanos y empresas, incrementar los niveles de uso de la administración electrónica, racionalizar y optimizar el empleo de las TIC en las Administraciones Públicas, aumentar la colaboración entre las distintas Administraciones Públicas y romper la brecha digital que separa geográficamente el centro de la periferia.

Se definen una serie de sub-objetivos y líneas de actuación, entre las que citaré:

- Avanzar hacia una Administración integrada en la sociedad con servicios públicos de calidad centrados en ciudadanos y empresas. Para ello, una de las líneas de actuación concordante con el objeto de este estudio consiste en "*Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados de conformidad con las actuaciones previstas en la Estrategia Española de Ciberseguridad*".
- Incrementar el uso de los servicios públicos electrónicos por parte de ciudadanos y empresas. Una de cuyas líneas de actuación para lograr este objetivo es "*Facilitar los mecanismos de identificación y autenticación frente a la Administración*", como una de las cinco dimensiones de la seguridad contempladas en el ENS (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).

3. PRINCIPIO DE SEGURIDAD. IMPRESCINDIBLE EN LA E-ADMINISTRACIÓN

3.1. Seguridad según las leyes 39/2015 y 40/2015

Ya en el art. 13 LPA sobre los derechos de las personas en sus relaciones con las Administraciones Públicas, de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas se señala que "*Quienes de*

conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos: (…) h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Del mismo modo el art. 16 LPA habla tanto del Registro Electrónico General de cada Administración, como los registros electrónicos de cada Organismo, en el sentido de que deben cumplir las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal que, como ha dejado claro la AEPD y comentaré más adelante, coincidirán con las dispuestas por el Esquema Nacional de Seguridad (ENS).

A su vez, el art. 17 LPA, sobre el archivo de documentos, señala que "*Los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión*", y también que "*Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados*". Es más que evidente la convicción del legislador de que el Esquema nacional de Seguridad es el garante de las medidas de seguridad que se requieren para proteger a la Administración Electrónica.

Únicamente matizar, respecto a los atributos de la seguridad en general, entendidos como bien jurídico a proteger, que existen tres dimensiones universalmente reconocidas y dos más que adiciona el ENS. Las tres primeras son confidencialidad, integridad y disponibilidad. Las dos adicionales autenticidad y trazabilidad. En consecuencia, cuando el art. 17 LPAC habla de calidad, ésta corresponde al autor del documento original; cuando lo hace de protección se está refiriendo al conjunto de las 5 dimensiones –seguridad en sentido amplio-; y cuando habla de conservación, podríamos entenderlo como un caso extremo de disponibilidad en el tiempo manteniendo la integridad.

El art. 27 LPA, sobre validez y eficacia de las copias realizadas por las Administraciones Públicas, señala que "*Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, así como a las siguientes reglas: a) Las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento. (…)".*

El art. 3.2 LRJ, sobre principios generales, señala: "*Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados*".

El art. 38 LRJ, sobre la sede electrónica, señala que "*Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad*". Vemos que se introducen al menos dos principios nuevos respecto a los analizados anteriormente: El principio de transparencia, entendiendo el legislador que la sede electrónica es el marco ideal para poder ejercerla de forma plena, y el principio de publicidad, única forma de poner en conocimiento de la ciudadanía aquello que ofrece la Administración y a lo que tiene derecho.

Ese mismo artículo 38 LRJSP señala que "*Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias*", denotando que seguridad y funcionalidad son complementarias y necesarias para ofrecer cualquier servicio público de calidad.

El art. 46 LRJ, sobre archivo electrónico de documentos, considera la seguridad de forma análoga a como hemos visto lo hace el art. 17 LPAC.

El art. 151 LRJ, sobre transmisiones de datos entre Administraciones Públicas, señala: "*Cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad*". Continúa el legislador insertando el contenedor en el contenido, ya que las dimensiones básicas de la seguridad hemos visto que son confidencialidad, integridad y disponibilidad". Por otro lado, relaciona acertadamente interoperabilidad con seguridad como disposición inexcusable.

Y llegamos al art. 156 LRJ, sobre Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad, dónde se da una definición de cada uno, desarrollados respectivamente en los Reales Decretos 4/2010 y 3/2010, respectivamente, transcrita del art. 42.2 de la derogada ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).

3.2. El Esquema Nacional de Seguridad (ENS)

Como se define en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJ), "*El Esquema Nacional de Seguridad tiene por objeto 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 garanticen adecuadamente la seguridad de la información tratada".

No es mala definición, pero obvia algunos aspectos fundamentales del ENS que no pueden ningunearse, surgiendo del propio concepto de Servicio Público. El Sector público no se limita a tratar información de los ciudadanos sin ninguna razón, sino que lo hace en el ámbito de un servicio o, si se prefiere, de determinados procedimientos y trámites administrativos, dentro de sus competencias.

En consecuencia, el ENS protege esos servicios prestados a la ciudadanía, apoyados directa o indirectamente en medios electrónicos, y a la información que tratan, apoyados en sistemas de información.

El propio preámbulo del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), señala "*El Esquema Nacional de Seguridad 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*".

Al final, también en el preámbulo, se habla de la finalidad perseguida, que no deja lugar a dudas: "*La finalidad del Esquema Nacional de Seguridad es la creación de 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*". Es la calidad de los servicios ofrecidos, junto a la confianza respecto a ellos que perciba la ciudadanía, que hará popular a la Administración electrónica y la generalizará sin posibilidad de involución.

La seguridad debe contemplarse con visión global. Del mismo modo que se contempla la interoperabilidad de los sistemas de información de la Administración Pública en beneficio de que el ciudadano no tenga que aportar en cada trámite aquella información que la propia Administración en sentido amplio ya dispone, la seguridad debe afectar a todos los que constituyen el Sector Público y a sus proveedores relevantes en base a la cadena de subcontratación.

Fue a partir de la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, que hubo un punto de inflexión en relación al ENS. Se introduce la obligación de certificar por una entidad acreditada a todos los sistemas de categoría MEDIA y ALTA y se recomienda hacerlo a los de categoría BÁSICA a los que bastaría una declaración de conformidad.

Pero para mí, lo más significativo ha sido incluir de forma obligatoria en el proceso de certificación a toda la cadena de suministro de la Administración, perteneciente al Sector Privado. Concretamente el capítulo VII, sobre soluciones y servicios prestados por el sector privado, señala: "*VII.1 Cuando los operadores del*

sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.

VIII.2 Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la presente Instrucción Técnica de Seguridad".

De este modo se consigue que la cada vez mayor innovación en el Sector Público, habitualmente de la mano de la Administración electrónica, sea sostenible, con independencia que se apoye en el Sector Privado, o no. Esta sostenibilidad la marcará el equilibrio obtenido al conjuntar la calidad con la seguridad de los servicios ofrecidos a la ciudadanía y la información que estos tratan. Puede consultarse en la página Web del Centro Criptológico Nacional la relación de organizaciones pertenecientes al sector privado que están certificadas en la actualidad: https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/empresas-certificadas pudiéndose apreciar su crecimiento exponencial. Podemos afirmar en la actualidad que un proveedor del sector público o está certificado de los servicios que proporciona, o dejará de serlo.

3.3. El ENS como palanca para cumplir también con el RGPD

En el apartado 2.4.2. *Implementación de medidas de seguridad* de la Guía sectorial de la AEPD sobre "Protección de Datos y Administración Local" se señala por una parte que "*El RGPD no establece medidas de seguridad estáticas, por lo que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales*", y por otra "*lo previsto en el Esquema Nacional de Seguridad es aplicable a cualquier información de las Administraciones Públicas sin distinción del soporte en el que se encuentre, por lo que en cuanto a las medidas de seguridad se refiere, este esquema es acorde al enfoque de riesgo del RGPD y se constituye en una herramienta válida para la gestión del riesgo y la adopción de las medidas de seguridad en las citadas Administraciones*". Del mismo modo, en un documento publicado el 12 de diciembre de 2017 por la AEPD titulado "El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas" se señala que "*En el caso de las AAPP, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad*".

Análogamente, y en este caso con efectos jurídicos plenos, en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, respecto a medidas de seguridad en el ámbito del sector público, dispone: "*1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679. 2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad*".

En consecuencia, contemplar el ENS en la Administración electrónica, no únicamente aporta seguridad, sino que contribuye al cumplimiento de la legislación vigente por partida doble: Esquema Nacional de Seguridad, por un lado, y Protección de Datos, por otro. Esta dualidad pone en valor a los servicios públicos.

4. EL ESQUEMA NACIONAL DE INTEROPERABILIDAD

El Esquema Nacional de interoperabilidad (ENI), regulado por el Real Decreto 4/2010, establece las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad de los sistemas empleados por las administraciones públicas, contribuyendo, además, a una mejor eficiencia, gracias a una mejor racionalidad en los intercambios de información, a ahorros en costes y a la eliminación de duplicidades. Es de aplicación para todas las administraciones públicas, en las relaciones entre ellas y con los ciudadanos.

El Real Decreto 4/2010 es el resultado de un proceso en el que han participado todas las Administraciones Públicas, a través de los órganos colegiados con competencia en materia de administración electrónica y en el que se ha contado también con la opinión de asociaciones de la industria del sector de las TIC.

Según AMUTIO, MIGUEL ÁNGEL, del Ministerio de Hacienda y de la Función Pública, [3] al tratar la interoperabilidad hablamos de sus dimensiones legal, organizativa, semántica, técnica y temporal:

- Legal: Relativa al marco legal que ampara la cooperación y el intercambio de información entre entidades.
- Organizativa: Relativa a la colaboración entre entidades, y a la interacción de los servicios, los procedimientos y los procesos.

- Semántica: Relativa a la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.
- Técnica: Relativa a la interacción de los sistemas tecnológicos, incluyendo estándares y especificaciones abiertas, de forma que las soluciones técnicas respeten la libertad de las partes en cuanto a elección entre alternativas tecnológicas.
- Temporal: Relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas. Se manifiesta especialmente en la conservación de la información en soporte electrónico.

El ENI trata todos aquellos aspectos que conforman de manera global la interoperabilidad. Así, su contenido recoge diferentes cuestiones como son los principios específicos de la interoperabilidad, las pautas relativas a las dimensiones organizativa, semántica y técnica de la misma, la selección y utilización de estándares, las infraestructuras y servicios comunes, la red de comunicaciones de las Administraciones Públicas, la reutilización de aplicaciones, la firma electrónica, la recuperación y conservación del documento electrónico; y finalmente, la creación de las diferentes normas técnicas de interoperabilidad.

5. EPÍLOGO

De todo lo planteado en apartados anteriores, podemos sacar algunas conclusiones finales.

- Todo procedimiento que sea configurado en aras a dar cumplimiento a las leyes 39 y 40, deberá partir de la base del respeto y cumplimiento de los principios que en materia de protección de datos recogen el RGPD y la LOPDGDD.
- La seguridad de los servicios prestados, junto a la información que éstos tratan y su interoperabilidad, son pilares fundamentales de la Administración electrónica. Para ello, el ENS y el ENI son regulaciones que nacieron con visión de ayudar a hacer sostenible la e-Administración, de forma que no solo se potencie, sino que se consolide y sea perdurable en el tiempo.
- En un entorno altamente externalizado, los proveedores de la Administración están igualmente obligados por las disposiciones del Esquema Nacional de Seguridad (ENS) y deben evidenciarlo con el correspondiente certificado.

6. BIBLIOGRAFÍA:

ALMONACID LAMELAS, VICTOR. "IMPLANTACIÓN PRÁCTICA DE LA ADMINISTRACIÓN ELECTRÓNICA: COLABORACIÓN DEL SECTOR PÚBLICO CON EL SECTOR PRIVADO". Revista digital CEMCI. Número 30-31. Abril a septiembre de 2016.

IBAÑEZ, ANTONIO. "DIGITALIZACIÓN EN LAS ADMINISTRACIONES PÚBLICAS. El caso de la Junta de Castilla y León". U.GOB (La revista de novagob). Marzo-abril de 2018.

AMUTIO, MIGUEL ÁNGEL. "Interoperabilidad y Seguridad en las Administraciones Públicas" del libro "Tú, Yo y la Administración Electrónica".

AEPD / FEMP. Guía sectorial sobre "PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL". 2018.

AEPD. "EL IMPACTO DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS SOBRE LA ACTIVIDAD DE LAS ADMINISTRACIONES PÚBLICAS". 12 de diciembre de 2017.

GERARDO BUSTOS. "10 reflexiones sobre el retraso de la administración electrónica". LEGALTODAY. Septiembre 2018.