LA SEGURIDAD EN EL USO DE LA TECNOLOGÍA Y COMUNICACIONES.

Jorge Fondevila Antolín[1]

I. CONSIDERACIONES INICIALES.

Una de las cuestiones que actualmente presentan mayor importancia en el ámbito del desarrollo de la denominada "Administración Digital", es la de la seguridad de la información y su tratamiento, con la finalidad de permitir su protección adecuada, esta materia fue objeto de regulación inicial por el artículo 42 de la hoy derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en adelante (LAE), desarrollado posteriormente por el 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, en adelante (ENS), si bien, en estos momentos el nuevo marco normativo vía Ley ordinaria es mucho más limitado, de manera que parece que formalmente se le otorga mucha menos importancia, así, en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en adelante (LPAC) las referencias a esta materia son de carácter puntual, como posteriormente comprobaremos, y solo el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en adelante (LRJSP) realiza una mención expresa y mínimamente concreta al Esquema Nacional de Seguridad, manteniéndose afortunadamente en vigor las previsiones del ENS. Estas regulaciones constituyen un régimen jurídico de inmediata y directa aplicación al conjunto de las Administraciones Públicas dado el carácter básico de las mismas, conforme determina la Disposición final decimocuarta de la LRJSP, y

[1] Jefe Asesoría Jurídica de la Consejería de Presidencia, Interior, Justicia y Acción Exterior (Gobierno de Cantabria). Doctor en Derecho; Funcionario de habilitación carácter nacional: Escala de secretaria; Funcionario del Gobierno de Cantabria: Cuerpo de Letrados y Cuerpo Técnico Superior. Las líneas de investigación desarrolladas son esencialmente empleo público, e-administración y contratación electrónica, en estas áreas ha publicado siete monografías y participado en diecinueve publicaciones colectivas, además de múltiples artículos en revistas jurídicas.

que como señalaba (Valero 2013: 179) con relación al anterior marco normativo, pero aplicable de igual manera al actual, constituyen "auténticas normas jurídicas cuya infracción no puede quedar simplemente en el ámbito del incumplimiento de buenas prácticas, hasta el punto de que podría afectar incluso a la validez de las actuaciones que se lleven a cabo utilizando medios electrónicos".

Ahora bien, del examen de las previsiones tanto de la derogada LAE como actualmente de la LRJSP y el ENS se aprecia claramente, desde un punto de vista estrictamente jurídico, un claro problema la ausencia de regulación del rango normativo que deberían tener los diferentes instrumentos de desarrollo de sus previsiones, en concreto, nos referimos a las denominadas Guías de seguridad, Instrucciones Técnicas, Normas de seguridad, procedimientos generales y específicos, y ello, por cuánto esta previa determinación de rango normativo condiciona directamente tanto el grado de vinculación "ad intra" como "ad extram" y, lógicamente, las consecuencias jurídicas que puedan derivarse de un supuesto incumplimiento de sus previsiones, especialmente con relación a su vinculación como legislación básica para las Comunidades Autónomas.

Es decir, nos encontramos con un grave problema en la aplicación de las citadas previsiones legales (LPAC, LRJSP y ENS), ya que, del contenido de los citados cuerpos legales y a la vista de las disposiciones adoptadas por diferentes Administraciones Públicas (AGE, CC.AA y EE.LL.), nos encontramos ante la creación de unos instrumentos de dudosa naturaleza jurídica, en algunos casos (normas generales, procedimientos, etc.), con las lógicas consecuencias de inseguridad jurídica en el momento de su aplicación y en especial sobre su obligatoriedad y las consecuencias jurídicas de su incumplimiento, entre la que destaca especialmente la posible exigencia de responsabilidad patrimonial a la administración ante incumplimientos o inactividad en esta materia, ya que las mismas contienen en muchos casos, a título de ejemplo, medidas organizativas que afectan al régimen de desempeño de sus funciones como el disciplinario de los empleados públicos, y también, a cuestiones de gran importancia en el tratamiento de información y que puede afectar a los datos personales de ciudadanos.

Desde luego, de lo que no hay duda es que la totalidad de las Administraciones Públicas deben ajustarse a las citadas previsiones legales, y con independencia de la problemática que hemos señalado y que será objeto de un breve examen en este trabajo, también, es importante destacar otro problema, en concreto, la dificultad presupuestaria y organizativa para cumplimiento de estas obligaciones legales por parte de las Comunidades Autónomas, y lógicamente también por las Entidades Locales (Valero 2013: 180).

II. RÉGIMEN JURÍDICO GENERAL DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

II.1. Examen del Marco Normativo General de la Seguridad de la Información.

El régimen jurídico que regula la problemática de la seguridad de la información en nuestras Administraciones Públicas se encuentra regulado fundamentalmente por el siguiente conjunto normativo, debiendo indicar que para un examen más amplio y detallado de todos los temas expuestos en este apartado nos remitimos a nuestro trabajo (Fondevila 2017: 597- 674).

II.1.1. Examen de la legislación de carácter básico.

Recordemos que la legislación de carácter básico resulta de directa aplicación al conjunto de las Administraciones Públicas. Efectivamente desde el momento en que han desplegado toda su eficacia jurídica tanto la LPAC como la LRJSP, y en especial, dado que esta última es la única norma que realiza una mención expresa a la figura del ENS en su artículo 156.2, como ya hemos indicado, nos encontraremos ante la derogación de las previsiones del artículo 2º de la LAE que delimitaba por reenvío del artículo 3º del ENS el ámbito de aplicación del mismo, por ello, resulta preciso reinterpretar el nuevo alcance subjetivo de esta fórmula de delimitación, tomando como referencia obligada la única norma que hace referencia al ENS de forma diferenciada como institución normativa, es decir, la nueva LRJSP, y por lo tanto, a nuestro juicio, debemos entender que el reenvío debe interpretarse en estos momentos referido al mismo ámbito de aplicación previsto para la LRJSP en su artículo 2º, de forma que, a nuestro juicio, este resulta de aplicación a las Administraciones Públicas territoriales (Administración General del Estado, Comunidades Autónomas y Entidades Locales), no existiendo alteración alguna con relación a la anterior situación y con relación al que denomina la LRJSP como "Sector Público Institucional", el detalle de los organismos y entidades de derecho público, incluida la referencia a las entidades de derecho privado cuándo ejerzan potestades administrativas estimamos que tampoco altera el anterior ámbito de aplicación del ENS.

A) Legislación General.

Pues bien, debemos comenzar refiriéndonos a las previsiones que, con rango normativo de Ley, en primer lugar, nos encontramos ante la desaparición de los principios y requerimientos legales de seguridad de la información, que se encontraban regulados principalmente en la LAE en sus artículos 41 y 42, y por la también derogada Ley Orgánica 15/1999 de 13 de diciembre, de Protección

de Datos de Carácter Personal (LOPD), que se aplicaban de forma concurrente (Valero 2010: 139).

Ahora este régimen legal se encuentra regulado por las nuevas previsiones de la LRJSP, y la LPAC, debiendo reiterar lo ya manifestado sobre la deficiente regulación de esta materia en las nuevas normas básicas a pesar de su importancia destacando en especial las siguientes cuestiones:

1. Llama la atención a este respecto la desaparición de cualquier referencia al principio de seguridad reconocido en el artículo 4º f) de la LAE, que como destaca (Martinez 2009, p. 259), la finalidad del mismo era asegurar el mismo nivel de garantías y seguridad para los ciudadanos en su relación con las Administraciones Públicas independientemente de que su expediente se sustancie en papel o electrónicamente, y ello unido a la necesidad de garantizar igualmente la correcta protección de datos de carácter personal, en el mismo sentido se manifiesta (Gamero 2015: 496), si bien, este lo conecta a las previsiones del artículo 4º d), con relación a la obligación de equivalencia de garantías en la gestión de los expedientes. Esta ausencia supone una manifiesta deficiencia legislativa, que por desgracia se extiende con relación al resto de los principios establecidos en la LAE que regulaban el orden axiológico de la e-Administración y que también han desaparecido del orden normativo. A lo anterior debemos añadir, que a nuestro juicio, el principio de seguridad tiene un alcance mayor aún del recogido legislativamente, en el sentido de que su carácter transversal supone que su incidencia se proyecte en otras áreas tan importantes como, por ejemplo, la interoperabilidad, o los contenidos de pliegos de prescripciones técnicas y administrativas en procesos de licitación tanto en al área informática como en otros ámbitos donde la prestación incida o gestione datos de la administraciones o de los ciudadanos, es decir, la seguridad no es una cuestión a predicar únicamente sobre ciertas actuaciones o sobre la configuración técnica de hardware y software de las administraciones, sino que la misma se constituye en un elemento esencial y determinante en la actual y futura configuración y desarrollo de la Administración Digital en su sentido más amplio.

2. Con relación a la cuestión de los principios de la e-Administración, entendemos que resulta necesario realizar una breve consideración, así, no podemos evitar la crítica a la ausencia de una regulación de los principios de actuación de la Administración (Martínez 2009: 256), con especial interés en su actuación electrónica. Y ello es así especialmente porque se derogan los principios del art. 4 LAE, muchos de los cuales tenían un importante contenido jurídico. Así, llama la atención la desaparición de cualquier mención a los principios de igualdad, accesibilidad, legalidad o inalterabilidad, proporcionalidad, responsabilidad y calidad y neutralidad tecnológica; además, de que debería haberse incluido otros

principios como los de innovación y adaptabilidad tecnológica, entre otros, resultando especialmente destacado también la ausencia de principios como la responsabilidad general por los contenidos, la inalterabilidad de la relación jurídica y el derecho –o principio– de gratuidad.

Por último, con relación a la cuestión del acceso efectivo a los servicios electrónicos y la no discriminación, parece que se deroga el importante principio de no discriminación del artículo 4 de la LAE, sobre la evitación de discriminaciones entre conectados y desconectados. Esta ausencia resulta muy preocupante dado que con ello desaparece uno de los instrumentos esenciales para todo ordenamiento jurídico, así (Rebollo, 2010: 1521) y también la jurisprudencia han establecido básicamente como criterio pacífico considerar que los principios generales ordenadores de cualquier norma se constituyen como fundamento de ese ordenamiento jurídico, también como orientadores en la interpretación de la norma por los operadores jurídicos y finalmente, como fuente en caso de insuficiencia regulatoria de la Ley. Por lo tanto, nos encontramos ante un ámbito material de la Ley que queda absolutamente huérfano de cualquier apoyo técnico jurídico para solventar las lógicas incidencias que su aplicación pueda originar, realmente estamos en presencia de otra manifestación de la mala calidad normativa de la norma y la dejadez del legislador, no sabemos si interesada o no.

3. En cuanto a las concretas previsiones de la nueva legislación (LPAC y LRJSP), a este respecto lo más importante es destacar que salvo las previsiones contenidas en el artículo 156.2 de la LRJSP, donde se procede a una remisión expresa al obligado cumplimiento por las Administraciones Públicas de las previsiones previstas en el ENS, el resto de las previsiones referidas a la "seguridad" de ambas normas son muy poco precisas e incompletas, en este sentido, a título de ejemplo, destaca la ausencia de referencia alguna a este principio en el artículo 70 de la LPAC que regula una institución tan importante como el expediente administrativo electrónico, y en el mismo sentido podemos referirnos al régimen legal de las notificaciones administrativas electrónicas.

Así, podemos resumir las referencias a la "seguridad", en términos generales en el articulado de la LPAC a lo establecido en el artículo 13 h) derecho de los ciudadanos a la seguridad de sus datos; artículos 16 y 31 con relación a los Registros electrónicos; artículo 27.3 en cuánto al régimen de las copias auténticas de documentos administrativos, y finalmente la Disposición adicional segunda que exige a las Comunidades Autónomas y Entidades locales si no quieren adherirse a las plataformas del Estado central garantizar el cumplimiento de las exigencias técnicas del ENS.

Por otro lado, con relación a las previsiones de la LRJSP, nos encontramos ante una situación similar a la anteriormente relatada, con la excepción de las

previsiones contenidas en el artículo 156.2 de la LRJSP, donde se procede a una remisión expresa al obligado cumplimiento por las Administraciones Públicas de las previsiones previstas en el ENS, pero el resto del articulado responde al mismo esquema de la LPAC, en este sentido, artículo 3º en cuánto a las relaciones de interoperabilidad y la necesidad de garantizar la seguridad con relación a los otros sistemas; artículo 38.3 en cuánto a las sedes electrónicas; artículo 44.4 y los entornos cerrados de comunicaciones; artículo 46.3 sobre la seguridad de los archivos electrónicos; y finalmente los artículos 155.1 transmisiones de datos de interesados entre Administraciones Públicas, 157.3 y 158.2 sobre la reutilización de aplicaciones y transferencia de tecnología entre las Administraciones Públicas.

Como se puede apreciar estamos ante referencias puntuales y asistemáticas que entendemos demuestra una falta de interés del legislador por una cuestión tan importante tanto para los ciudadanos como para la propia organización de las Administraciones Públicas como la seguridad de su información y datos, y más en los tiempos que corren.

B) Normativa reglamentaria: Comentario General.

Por otro lado, nos encontramos con el correspondiente desarrollo reglamentario de estas previsiones, también con el carácter de normas "básicas", incluidos sus anexos, que, a pesar de las citadas modificaciones legislativas, mantienen su vigencia. En las mismas se concretan las medidas y controles de seguridad que deben obligatoriamente ser aplicados por todas las Administraciones Públicas, en función de los principios básicos y los ejes fundamentales de la seguridad de la información establecidos en los artículos 4 al 10 del ENS.

A todo esto debemos añadir, otro conjunto de regulaciones, a las que resulta muy discutible atribuir o no, naturaleza normativa a pesar de la denominación utilizada por el ENS, recordemos de carácter básico, y que constituirán una de las cuestiones esenciales de este trabajo, nos referimos tanto a la denominada "Política de seguridad" prevista en el artículo 11, como a las "Guías de Seguridad e Instrucciones Técnicas", reguladas en el artículo 29 del ENS, y en una auténtica "ceremonia de la confusión normativa" dentro del denominado "marco organizativo", previsto en el apartado 3º del Anexo II del citado Real Decreto, en concreto, nos encontramos en el apartado 3.2 lo que denomina "Normativa de Seguridad", con una referencia a "una serie de documentos", a los cuáles se les engloba dentro de un concepto que jurídicamente está acotado, pero en cambio no se específica ni el instrumento jurídico de aprobación ni su naturaleza jurídica, lo que pone en cuestión su grado de vinculación jurídica y las consecuencias legales de su incumplimiento, y por último, en el apartado 3.3 los llamados "procedimientos de seguridad", con el mismo problema. Esta falta de corrección técnico normativa está originando

regulaciones cuándo menos "peculiares" en nuestras Administraciones Públicas, como examinaremos posteriormente, que sin duda van a ser una fuente de conflictos a medio y largo plazo.

C) Examen de la naturaleza jurídica y función de los instrumentos (normativos/ técnicos) de desarrollo del ENS.

En este apartado procedemos al examen de los diferentes instrumentos que reconoce expresamente el articulado del ENS como necesarios o adecuados para su desarrollo y aplicación, si bien, tanto su naturaleza normativa y grado de vinculación para el resto de las Administraciones Públicas, como la delimitación de su contenido material resulta en ocasiones inescrutable y conflictivo como apreciaremos a continuación.

Comenzamos nuestras consideraciones por el examen tanto de las previsiones del artículo 29 del ENS, que fue sido objeto de modificación, por cierto, nada afortunada, mediante el Real Decreto 951/2015, de 23 de octubre, y que se mantiene en el artículo 4 del Proyecto de Real Decreto del nuevo Esquema Nacional de Seguridad. A este respecto, debemos destacar que la redacción de este precepto se limita a regular de forma muy somera el instrumento de las "guías de seguridad", encomendando al CCN la elaboración y aprobación de las mismas, de conformidad con lo previsto en el artículo 2.2. a) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, este precepto nada dice sobre el grado de vinculación para otras administraciones de las previsiones contenidas en estas guías y tampoco establece si las mismas tienen carácter normativo o no, es decir, autismo absoluto, pero curiosamente la actividad de elaboración de las mismas ha sido motorizada en estos años.

a) Las Guías de seguridad.

Pues bien, tras la reciente reforma nos encontramos que la redacción del precepto con respecto a este instrumento no ha sufrido modificación alguna, es decir, seguimos con los mismos silencios e incógnitas que presentaba anteriormente, y que continúan en el proyecto, así, es importante destacar que el anexo IV (Glosario) del ENS no incorpora mención alguna al respecto, si bien, si hay un cambio, y que consiste en la posibilidad de resolver algunas de las lagunas del mismo por interpretación sistemática, tomando en consideración las previsiones del apartado 2º que regula el instrumento de las "instrucciones técnicas de seguridad".

Así, la primera de las cuestiones que vamos a examinar es su naturaleza jurídica, y a este respecto, la primera referencia nos la aporta el apartado 2º, que parece reservar el "obligado cumplimiento" por parte de todas las Administraciones

Públicas comprendidas en el ámbito de aplicación del ENS, a las instrucciones técnicas, luego a *sensu contrario*, debemos considerar que estas guías deben ser reconducidas a la categoría de las "Instrucciones u órdenes de servicio" en su sentido más estricto, y dada la ausencia de vinculación jurídica alguna (inexistencia de obligaciones) para las Administraciones Públicas consideramos que no nos encontramos ante normas jurídicas de carácter reglamentario, sino ante actos administrativos de naturaleza meramente informativa u orientativa de prácticas en la ejecución de la seguridad de la información, es decir, estamos ante unos simples textos de consulta sin vinculación legal alguna. Lo anterior supone que las Administraciones Públicas el elaborar y ejecutar sus políticas de seguridad no están obligadas a seguir ninguno de sus contenidos, de manera que cuentan con absoluta autonomía e independencia para orientar sus actuaciones bajo sus propios criterios, y ante una actuación que entre en contradicción con las indicaciones de las guías no se podrá exigir responsabilidad alguna ni efectuar tampoco ningún requerimiento por parte de la Administración General del Estado, por lo tanto, estamos ante unos instrumentos vacíos de contenido desde un punto de vista jurídico.

En cuanto al objeto material de estas guías nos encontramos ante un silencio normativo absoluto solo roto por el examen del contenido de las publicadas hasta este momento, de manera que al examinar las mismas se observa que estas desarrollan cuestiones de lo más variopintas, pero resulta importante destacar que algunos de sus contenidos (auditorias, incidentes de seguridad, adquisición de productos de seguridad, etc.). Pero lo más importante a estos efectos es que la referencia de ámbitos materiales de regulación que establece la disposición adicional cuarta del RD 3/2010 que puede colaborar a la delimitación, interpretando a sensu contrario los ámbitos reservados a las Instrucciones Técnicas.

Como conclusión de lo expuesto, debemos entender que el ámbito material de las guías debe delimitarse de forma concurrente mediante la utilización de dos criterios, a saber, en primer lugar, podríamos considerar que existe un objeto material general de contenidos que alcanza toda clase de cuestiones, y en segundo lugar, este criterio general podría quedar limitado por exclusión en la reserva material conforme la regulación establecida por la Disposición Adicional 4ª del ENS que determina una serie de materias para su regulación por medio de instrucciones.

Ahora bien, la siguiente pregunta sería si es posible la aprobación de guías informativas sobre estas materias reservadas, y en principio, nada se opondría a ello, siempre que estemos ante meras informaciones o reseña de buenas prácticas pero resultaría discutible la incorporación de criterios interpretativos cuándo estas guías carecen de eficacia jurídica en cuanto a su vinculación u obligación de

cumplimiento de sus previsiones para cualquier administración pública, es decir, no existe destinatario legal.

b) Las Instrucciones Técnicas de Seguridad.

Estamos aparentemente en presencia de otro instrumento de desarrollo de las previsiones del ENS, si bien, el anexo IV (Glosario) del ENS no incorpora mención alguna al respecto, lo que va a dificultar su distinción material con las otras clases de "instrucciones" que puede emitir el CCN, conforme establece el artículo 2.2. a) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional y el propio artículo 37.1 b) ENS, y su copia en el artículo 34.1. b) del proyecto.

1. Naturaleza Jurídica.

Dicho lo anterior, la primera cuestión que vamos a analizar es el de la naturaleza jurídica de estos instrumentos (normativa o simples actos administrativos), y a este respecto, la cuestión va a resultar muy complicada dada la alambicada y pésima técnica legislativa del precepto, en concreto, nos referimos al artículo 29.2 del ENS, así, el primer dato que nos puede ofrecer una respuesta, lo encontramos en la declaración de que estas instrucciones serán " de obligado cumplimiento", por lo tanto, en una primera aproximación a la cuestión debemos deducir necesariamente su carácter normativo, nos remitimos en este punto a lo ya expuesto en apartados anteriores sobre la naturaleza de estas figuras, ya que, eso supone establecer un marco de obligaciones para terceros, pero para quién, la respuesta parece obvia a la vista de lo previsto en la Disposición final primera del ENS que declara el carácter de legislación básica de éste, es decir, en principio y como mínimo, para todas las Administraciones Públicas incluidas en su ámbito de aplicación.

Ahora bien, fijadas las cuestiones previas comienza el calvario para cualquier jurista, ya que resulta inescrutable el contenido del precepto con relación a cuestiones tan esenciales como qué tipo de norma reglamentaria, procedimiento y órgano competente se debe utilizar para aprobar estas instrucciones, sin olvidar otra cuestión clave, en concreto, el condicionamiento que esto supone para poder declarar su contenido como básico, conforme la doctrina del Tribunal Constitucional al respecto.

En cuánto, a la cuestión del tipo de norma reglamentaria que debe amparar la aprobación de estas instrucciones, nos encontramos ante un nuevo episodio de autismo, nada se dice, pero lo peor es lo que si se dice, ya que nos conduce a un laberinto de difícil salida. Efectivamente, el precepto (artículo 4 del proyecto de Real Decreto) declara que la aprobación se realizara por el Ministerio de

Asuntos Económicos y Transformación Digital, pero no precisa que órgano del mismo será el competente, podríamos en buena lógica deducir que el único posible sería el Ministro, y ello, al amparo de las previsiones del artículo 61.a) de la LRJSP, en concordancia con lo establecido en el artículo 24.1. f) de la Ley 50/1997, de 27 de noviembre, del Gobierno (LG), a lo que debemos añadir las previsiones de la disposición final segunda del proyecto ya citado, copia idéntica de la vigente actualmente, que establece: *"Se autoriza al titular del Ministerio de Asuntos Económicos y Transformación, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado."*

Por lo tanto, y como consecuencia de todo ello deberíamos concluir que el instrumento normativo de obligada utilización necesariamente sería la "Orden Ministerial". Pero esta lógica conclusión se complica al encontrarnos con una nueva previsión, en concreto, la determinación de que por Resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial se procederá a la publicación de la instrucción. Pues bien, si estamos en presencia de una Orden Ministerial de aprobación, esta previsión resultaría incomprensible legalmente, pues no existe regulación normativa (LRJSP) al respecto, que determine que esta deba ser publicada por resolución de la Secretaria de Estado, entonces qué sentido tienen incorporar esta previsión, la única explicación posible es que la voluntad del gobierno es que la aprobación no se realice por el Ministro, sino por otro órgano inferior, en este caso sería la Secretaria de Estado, pero entonces nos encontramos con un doble problema, pues, en primer lugar, la potestad reglamentaria se encuentra reservada en exclusiva al Gobierno, recordemos que la misma no puede ser objeto de delegación, conforme determina el artículo 9.2. b) de la LRJSP, de manera que estos órganos superiores, conforme establece el artículo 7 de la LG, en concordancia con el artículo 62 de la LRJSP, carecen de competencia normativa alguna, a lo sumo podrán dictar "instrucciones y ordenes de servicio", que solo pueden afectar a su área material de competencias y con eficacia exclusiva *ad intra,* y que conforme hemos examinado anteriormente estas figuras carecen de eficacia normativa por principio, y en segundo lugar, no existe habilitación legal reglamentaria a este respecto, conforme determina la disposición final segunda del ENS.

Así, ante ese panorama debíamos preguntarnos a qué tipo de nueva norma se podía referir el precepto, la respuesta lógica y legal es que, a ninguna, pues resultaba imposible determinar a priori a que se estaba refiriendo el mismo hasta el momento en que se aprobará la primera instrucción. Así, buscando una interpretación sistemática del precepto la única explicación coherente era que estuviéramos en presencia de una difusa atribución competencial a la Secretaria de Estado para

aprobar y publicar una "Instrucción" (previa conformidad *ad intra* ministerial), reconducible a la competencia general atribuible a este órgano al amparo de las previsiones del artículo 6 de la LRJSP. Lógicamente esa posibilidad resulta absolutamente contradictoria con la pretensión legal de que estas instrucciones sean de obligado cumplimiento por todas las Administraciones Públicas, al carecer las instrucciones por exigencia legal del art. 6 LRJSP y doctrina jurisprudencial, de eficacia normativa, y recordemos que en los casos en que se reconoce esta clase de naturaleza normativa a las mismas, ello deviene por su contenido material pero al no haberse respetado el marco legal competencial y de procedimiento de elaboración en la mayor parte de los casos se ha declarado su nulidad. Parece que estamos ante un problema cada vez más generalizado en nuestras administraciones, donde por ciertos sectores se confronta la eficacia y eficiencia técnica con el marco legal de obligado cumplimiento, es decir, el Derecho se constituye en un obstáculo o problema para las exigencias de rapidez y eficacia que requiere los tiempos actuales en ciertos ámbitos como el informático, olvidando que una de las notas características del Derecho es la regulación de soluciones para toda clase de situaciones y conflictos, como se ha demostrado a lo largo de los siglos sin menoscabo alguno de la seguridad jurídica.

2. El Dudoso carácter Básico de las Instrucciones Técnicas de Seguridad.

Efectivamente, los problemas de este precepto no acaban con lo señalado anteriormente, ya que es preciso tomar en consideración que de sus previsiones resulta que este impone que su contenido debe considerarse como de carácter básico, pues las instrucciones técnicas de seguridad serán de "obligado cumplimiento", lógicamente para todas las Administraciones Públicas incluidas en el ámbito de aplicación del ENS, y es esta declaración la que origina que debamos enfrentarnos con otro conflicto, pues el instrumento utilizado para la aprobación (Resolución) resulta claramente inadecuado para la aprobación de cualquier instrumento de naturaleza normativa, pues recordemos que la utilización tanto de "Órdenes ministeriales" y más aún en el caso de simples "Resoluciones" o "Instrucciones" resultan inconstitucionales conforme la doctrina del Tribunal Constitucional con respecto a los tipos de instrumentos normativos adecuados para el establecimiento de legislación cuyo contenido debe ser calificado como "básico" (SsTC 76/83 FJ 241, 33/84 FJ 2, 80/88, 248/88, 86/89, 132/89 y en especial resulta destacable al respecto la reciente Sentencia 7/2016 de 21 Ene. 2016, Rec. 5107/2013. pues bien, de la citada doctrina podemos extraer varias conclusiones:

a) Que resulta respetuoso con el orden constitucional la regulación reglamentaria de materias básicas por parte del Gobierno, siempre y cuando se cumplan los siguientes requisitos:

1. Existencia de una habilitación legal expresa.

2. Que su rango reglamentario viniera justificado por tratarse de materias cuya naturaleza exigiera un tratamiento para el que las normas legales resultaran inadecuadas por sus mismas características.

3. Que la utilización de esta posibilidad de regulación reglamentaria tiene carácter excepcional, y por ello, deberán concurrir razones coyunturales que lo aconsejen por el carácter marcadamente técnico o provisional de las materias susceptibles de regulación normativa.

b) Que solo excepcionalmente es posible utilizar otros instrumentos normativos, en concreto, las Órdenes ministeriales, pero siempre que estas cumplan los concretos requisitos reseñados anteriormente, si bien, por pura lógica la excepcionalidad de la utilización del instrumento de las órdenes ministeriales resulta más acentuada.

A la vista de lo expuesto, las previsiones del vigente artículo 29.2 y el artículo 4 del proyecto de Real Decreto del nuevo ENS, al regular las instrucciones técnicas de seguridad y su carácter de obligado cumplimiento por parte de todas las Administraciones Públicas, resultan siendo benevolentes de dudosa legalidad y constitucionalidad, por cuánto:

1. Como ya hemos visto el precepto no determina qué tipo de instrumento debe utilizarse para su aprobación, y desde luego parece que la finalidad del Gobierno se orienta más en el sentido de la figura de las "instrucciones" (artículo 6 LRJSP), que de la utilización de las órdenes ministeriales. Desde luego está claro que la figura administrativa de las instrucciones no cumple las exigencias jurídico formales establecidas por el Tribunal Constitucional.

2. En el caso de que al final el instrumento elegido resulte ser la correspondiente orden ministerial, conforme la habilitación legal establecida en la disposición final segunda del ENS, no encontramos las razones que puedan justificar ante la doctrina constitucional para la utilización generalizada de la aprobación de "instrucciones técnicas" por este medio, cuándo ese alto tribunal ha reiterado, ya como hemos visto, el carácter coyuntural y excepcional del uso del rango reglamentario para legislar con carácter básico, aunque el único punto a favor de su admisión podría sería su carácter técnico, si bien lo estimamos insuficiente por lo que expondremos a continuación.

3. Efectivamente, no hay que olvidar cuál es el sentido y alcance del concepto de legislación básica, así, dos son los criterios fundamentales que de forma pacífica son actualmente reconocidos tanto por la doctrina científica como por el propio Tribunal Constitucional (SsTC 32/1981, 1/1982, 80/1988,147/1991, 172/1996,197/1996, 37/1997 y destacando en especial la siguiente declaración

de la STC 103/1997, para la delimitación y precisión del concepto "básico", en concreto: " *….una norma merece tal calificativo (de básica) cuando garantiza en todo el Estado un común denominador normativo dirigido a asegurar, de manera unitaria y en condiciones de igualdad, los intereses generales; regulación normativa uniforme que, no obstante, debe permitir que cada Comunidad Autónoma introduzca, en persecución de sus propios intereses, las peculiaridades que estime pertinentes dentro del marco competencial que en la materia dibuje el bloque de constitucionalidad...".*

Así pues, como resumen de toda esta doctrina:

a) Criterio Positivo: que considera que las bases no son sino la traducción normativa de los principios de unidad y de interés general nacional, es decir, las bases se identifican con una regulación mínima en todo el territorio nacional de una materia o sector de la realidad.

b) Criterio Negativo: según el cual la regulación básica no puede llegar a tener una densidad tal que anule cualquier opción de regulación peculiar de desarrollo, es decir, una política legislativa propia por parte de la Comunidad Autónoma, de forma que las bases no pueden suponer en ningún caso una ordenación agotadora de la materia, siendo por ello, susceptible de diferentes regulaciones en tanto no se opongan o contradigan las previsiones de las bases.

Así pues, a nuestro juicio, esta normativa no implementa de forma adecuada los límites materiales de la legislación básica, de forma que esta regulación puede incidir e invadir ámbitos competenciales autonómicos, y por lo tanto, carecer de competencia al respecto, pues la declaración de los títulos competenciales citados en la disposición final primera no pueden constituir una carta blanca para toda clase de actuaciones o desarrollos estatales que pueden invadir claramente competencias de autoorganización de la Comunidad Autónoma.

II.1.2. La Autorregulación: mejores prácticas de seguridad.

Finalmente, como denomina (Alamillo 2013: 411) tenemos el "Nivel de autorregulación" en materia de seguridad, que supone la búsqueda de las mejores prácticas de seguridad, en este sentido podemos destacar las normas recogidas en la serie ISO/IEC 27000, sobre sistemas de gestión de la seguridad de la información, o la norma ISO 22301, sobre sistemas de gestión de la continuidad del negocio[2].

[2] La propia Norma ISO conecta el concepto de continuidad del «negocio» con la seguridad de la Sociedad, al efecto de aclarar que no se trata de una norma sólo aplicable a actividades mercantiles o lucrativas, sino a cualquier tipo de actividad y a juicio de Alamillo (2013, aplicable a la Administración Digital.

Dichas normas resultan aplicables a voluntad de la Administración como reconocía de forma indirecta el propio artículo 42.4 de la LAE, previsión que desaparece en la nueva regulación del artículo 156.2 de la LPAC, pero tampoco se puede negar que pueden completar algunas de las llamadas que el propio ENS realiza, en una particular colaboración del sector privado en lo regulatorio, si bien, volvemos a enfrentarnos con el problema del grado de vinculación jurídica de las mismas. Así, el artículo 13 del ENS determina que cada administración deberá establecer una propia gestión de riesgos por medio de un análisis y tratamiento concreto de los riesgos a los que se encuentre expuesto el sistema de tratamiento de la información y las comunicaciones.

En sentido similar, el artículo 26 del mismo cuerpo legal impone la obligación de actualizar y mejorar de forma continua la seguridad, admitiendo la utilización para ello de los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Finalmente, el artículo 34.4 del ENS, cuando regula la auditoría de la seguridad, admite que para su realización deberán utilizarse criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

En todos estos casos, puede verse con claridad como el legislador permite la existencia de un nivel de autorregulación para la aplicación de las mejores prácticas para el cumplimiento de los objetivos y mandatos reglamentarios. Dicho lo anterior, debemos disentir de (Alamillo 2013: 422), cuándo este autor considera correcta y adecuada esta práctica por suponer: *"…una orientación que resulta más flexible y pragmática que la incorporación constante de un cuerpo de práctica de seguridad a una disposición de carácter general que devendría de excesiva magnitud y fácil obsolescencia."*

Y ello, por cuánto, si bien no resulta discutible sino incluso recomendable la incorporación de "buenas prácticas" en cualquier ámbito de gestión, no podemos olvidar que nos encontramos en el ámbito de una Administración pública, la cual por imperativo constitucional (artículo 103.1 C.E.) se encuentra sometida a la ley y al Derecho, lo que supone que todas sus decisiones y actuaciones necesitan de un instrumento normativo para que estas actuaciones administrativas cuenten con amparo legal, el resto es una simple "vía de hecho", figura rechazada por nuestro ordenamiento jurídico, quizás la cuestión se deba centrar en la búsqueda de aquellos instrumentos normativos que permitan una gestión más ágil, pues adjudicar por principio a toda regulación normativa rigidez no responde a la realidad, sino más bien, en la mayoría de los casos a la ineficiencia de los procedimientos de toma

de toma de decisiones de los órganos directivos encargados de su elaboración y aprobación, o es que acaso una Norma ISO no lleva también un largo proceso de elaboración y aprobación, en este sentido destacamos el trabajo de (Moles 2013).

Finalmente, nos encontramos con otros instrumentos como las especificaciones técnicas metodológicas, operativas, mejores prácticas sectoriales y otras herramientas adecuadas para conseguir una práctica adecuada al objetivo de proteger la información, a partir de los principios y requerimientos legales, y de los controles obligatorios previstos en la reglamentación, en estos casos entendemos que el problema de la normatividad de la misma no existe, dada su naturaleza de meras ordenes de servicio, en términos jurídico administrativos.

III. BREVE APROXIMACIÓN A LA LEGISLACIÓN AUTONÓMICA GENERAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN.

Con independencia de la normativa básica estatal a la que nos hemos referido anteriormente, existe otro mundo jurídico, aunque en estos tiempos parece que existe un especial interés en olvidarlo, nos referimos al ámbito competencial legislativo de las comunidades autónomas, ya que, nos encontramos en un Estado constitucionalmente descentralizado.

Efectivamente, debemos recordar que como ya hemos señalado anteriormente la normativa estatal solo tiene un alcance básico, la cual proviene de las previsiones establecidas en la Constitución Española. Esa atribución competencial tiene una configuración legal que alcanza tanto la delimitación de la potestad jurídica de actuación como el ámbito material sobre el que recae la misma, pues estamos en presencia de un Estado descentralizado donde la proyección de la competencia sobre la materia, constituye el eje clave del reparto competencial entre el Estado y las Comunidades Autónomas de conformidad con las previsiones de los artículos 148 y 149 de la Constitución Española (CE). Y es en este punto, donde debemos recordar que la definición de lo que es básico o no, es un ámbito cerrado sobre las materias consideradas básicas y aunque exista un margen discrecional de decisión política, este nunca podrá superar o alterar ese límite, pues lo que no podría admitirse es que el legislador básico modificase sin límite alguno sus criterios sobre lo básico, ampliando o reduciendo el ámbito del mismo, es decir, existe un mínimo común uniforme o núcleo de lo básico sobre el que no es posible disponer (irrenunciabilidad de la competencia), lo que no supone cercenar en ningún caso los ámbitos de decisión de los legisladores, dado que ellos mismos se encuentran sometidos a los límites que la propia Constitución impone, salvo que estos procedan a acordar la modificación de la norma fundamental.

Asimismo, no existe duda con respecto a que el pronunciamiento expreso del Tribunal Constitucional al examinar el alcance y contenido de unas bases supone una delimitación definitiva (García 1996: 133), al menos, en la fijación del *"mínimo común uniforme"* en que se constituye esa legislación básica. De lo expuesto, solo podemos concluir que las Comunidades Autónomas tienen competencia plena para el desarrollo normativo de las previsiones legales estatales básicas, pues su regulación no puede agotar el contenido material competencial, y en base a la concurrencia de los títulos competenciales del artículo 148.1.1º y 149.1.18 que no resultan en ningún caso excluyentes, cuestión diferente es que la actuación de la mayoría de las administraciones ha sido la del puro seguidismo sin discrepancia normativa alguna, de forma que se han limitado a trasladar a sus ordenamientos una copia casi mimética de la normativa estatal con mínimas adaptaciones organizativas a las necesidades y especialidades de cada administración.

Dicho lo anterior, en el marco normativo autonómico debemos destacar la existencia de normativas generales regulatorias de la "e-Administración" por parte de muchas Comunidades Autónomas que han procedido a realizar desarrollos normativos propios, y hay que destacar que los instrumentos normativos utilizados al efecto han variado desde el uso de las normas reglamentarias (Ordenes o Decretos) a la aprobación de la correspondiente Ley por parte de las Comunidades Autónomas, ahora bien, en esta concreta cuestión prácticamente se limitan a realizar un reenvío general a las previsiones del Esquema Nacional de Seguridad, renunciando a realizar un desarrollo normativo propio, al cual competencialmente están habilitadas como hemos visto.

Pero la cuestión se complica más cuándo examinamos el desarrollo de las previsiones del apartado 3º del Anexo II del citado Real Decreto, apartado 3.2 "Normativa de Seguridad", al que ya nos hemos referido, siguiendo de forma casi mimética los instrumentos aprobados por la AGE, para la configuración de esa peculiar "normativa", aunque en estrictos términos jurídicos no merezcan esta calificación, lo que supone también una renuncia a su adecuación e integración en el régimen normativo en sus propios ordenamientos jurídicos, a estos efectos destaca la Comunidad Autónoma de Cantabria[3], que a diferencia de las previsiones de otras Comunidades Autónomas, establece la obligación de que la aprobación de los diferentes instrumentos técnicos en esta materia se realice por medio de Decreto u Orden, es decir, se reconoce el carácter normativo de aquellos contenidos que por su naturaleza y efectos deben ser así considerados.

[3] Decreto 31/2015, de 14 de mayo, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.

IV. EL RÉGIMEN JURÍDICO GENERAL SOBRE SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES DE LA JUNTA DE ANDALUCÍA.

En este apartado vamos a realizar un examen del marco regulatorio general autonómico sobre la seguridad de la información y comunicaciones, así, analizaremos su adecuación al marco normativo estatal básico, así como su régimen organizativo, y finalmente expondremos algunas propuestas.

IV.1. El marco jurídico general autonómico sobre seguridad de la información y comunicaciones.

En este apartado nuestra exposición se limitará para un adecuado conocimiento y posible consulta por los lectores a una exposición general del marco normativo, organizativo y también de algunos documentos administrativos informativos u orientativos, pero que carecen de eficacia jurídica, si bien, se estima que estos desempeñan una función importante en la implementación de la seguridad de la información.

1. Régimen Jurídico General para la Administración Digital.

– Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía (BOJA 31-12-2019).
– Decreto 114/2020, de 8 de septiembre, por el que se establece la estructura orgánica de la Consejería de la Presidencia, Administración Pública e Interior.
– Creación de la Agencia Digital de Andalucía por la disposición adicional vigesimosegunda de la Ley 3/2020, de 28 de diciembre, del Presupuesto de la Comunidad Autónoma de Andalucía para el año 2021.
– Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía (BOJA 8-4-2021).

2. Régimen Jurídico específico de la Seguridad de la Información y Comunicaciones.

– Decreto 99/1997, de 19 de marzo, que autorizó a la Empresa Pública de la Radio y Televisión de Andalucía y al Instituto de Fomento de Andalucía para la constitución de la sociedad mercantil «Sociedad Andaluza para el Desarrollo de las Telecomunicaciones, S.A. (SANDETEL), como empresa de la Junta de Andalucía (BOJA 6-05-1997).
– Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración

de la Junta de Andalucía (BOJA 18-01-2011), modificado parcialmente por el Decreto 70/2017, de 6 de junio (BOJA 12 junio 2017).

- Orden de 26 de noviembre de 2014, por la que se crea y regula la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad de las Tecnologías de la Información y de las Telecomunicaciones (TIC).
- Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

3. Otros instrumentos no normativos.

- Acuerdo de 16 de noviembre de 2010, del Consejo de Gobierno, por el que se aprueba el Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía (2010-2013). (BOJA 30-11-2010).
- Plan de Seguridad y Confianza Digital Andalucía 2020 (Periodo 2014-2016).
  https://www.juntadeandalucia.es/export/drupaljda/Plan%20de%20Seguridad%20y%20Confianza%20Digital%20Andalucia%202020%20para%20el%20periodo%202014-2016.pdf
- Plan de Seguridad y Confianza Digital Andalucía 2020 (Periodo 2017-2020).
  https://www.juntadeandalucia.es/export/drupaljda/Plan%20Seguridad%20y%20Confianza%20Digital%202017-2020.pdf
- Programa de Seguridad Digital en Andalucía (Sedian). Alineado con el Plan de Seguridad y Confianza Digital Andalucía 2020. (Adjudicado en el año 2019).
- Resolución de 26 de enero de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre integración en el Centro de Seguridad TIC AndalucíaCERT (BOJA 6-02-2018)
- Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía (BOJA 27-10-2020).

IV.2. Examen del régimen autonómico en materia de seguridad de la información y comunicaciones.

En este punto del trabajo nos centraremos en la realización de un examen descriptivo jurídico material del vigente marco organizativo y normativo de la Junta de Andalucía sobre la seguridad de la información y comunicaciones.

IV.2.1. Los Ámbitos de Planificación y Organizativo.

Es preciso comenzar nuestra exposición destacando que la Junta de Andalucía se ha destacado por sus decisiones organizativas e implementación en materia de seguridad de la información desde fechas incluso anteriores a la entrada en vigor del Real Decreto 3/2010 (ENS), en concreto, nos referimos a la aprobación del Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones de la Administración de la Junta de Andalucía (2010-2013), ello, ha supuesto que tanto normativamente como organizativamente esta administración ha tenido una implicación e interés destacado en esta materia, incorporando incluso instrumentos esenciales en la gestión de la seguridad como el grupo de resolución e incidentes de seguridad "AndalucíaCERT", en directa coordinación con el CNN-CERT. Por otro lado, como veremos en fechas recientes se ha producido un cambio organizativo de gran importancia en la implementación y gestión de la seguridad de la información, al crearse la "Agencia Digital de Andalucía", centralizando en esta toda la gestión de la administración digital, con excepción del Servicio Andaluz de Salud.

A) Planificación.

Dicho lo anterior, es preciso reseñar la existencia de un proceso de elaboración y planificación de la implementación de la seguridad de la información por medio de diferentes Planes estratégicos, que a nuestro juicio, resulta una decisión muy acertada y necesaria, y que muy pocas administraciones han desarrollado, en este sentido como ya hemos indicado anteriormente ya en el año 2010, se aprobó un Plan Director a este respecto, el cual ha tenido continuidad mediante dos Planes de Seguridad y Confianza Digital Andalucía, el último referido al periodo (2017-2020), que como se expone en el mismo, este persigue los siguientes objetivos:

- *Potenciar la adopción de buenas prácticas en materia de seguridad digital en la administración autonómica y local de Andalucía*
- *Extender la cultura de confianza y seguridad digital, mediante programas de sensibilización, asistencia y formación, con especial atención a los menores*
- *Impulsar el mercado de la seguridad digital y la creación de empleo, mediante el estímulo de la oferta y la demanda de productos, servicios y profesionales de la seguridad digital*
- *Reforzar las capacidades de prevención, detección y respuesta a incidentes de seguridad en Andalucía (AndalucíaCERT)*

Asimismo, las líneas de trabajo del Plan son:

1. *Coordinación de la seguridad TIC en la Administración autonómica, potenciando la adopción de buenas prácticas y ofreciendo servicios de asesoramiento, apoyo y coordinación*

2. *Formación y concienciación de los trabajadores del sector público, la ciudadanía y las empresas, y extensión de la cultura de confianza y seguridad digital*
3. *Impulso de la industria de la seguridad digital, mediante el estímulo de la oferta y la demanda de productos, servicios y profesionales de la seguridad digital, y promoción de la adopción de buenas prácticas y de la cultura de seguridad en el tejido empresarial andaluz*
4. *Coordinación con otras Administraciones y Organismos Públicos en materia de seguridad TIC*
5. *Protección frente a ciberamenazas, mediante la mejora de las capacidades de prevención, detección y respuesta a incidentes de seguridad en Andalucía (a través del centro AndalucíaCERT)*

Finalmente, debemos destacar la implementación del Programa de Seguridad Digital en Andalucía (Sedian), adjudicado definitivamente en el año 2020, el cual se desarrolla sobre tres líneas de actuación:

1. La promoción de buenas prácticas de seguridad digital en la administración autonómica y local de la mano de la Oficina de Apoyo a la Seguridad TIC.
2. La extensión de la cultura de confianza y seguridad digital al conjunto de la sociedad.
3. El refuerzo de las capacidades de prevención, detección y respuesta a incidentes de ciberseguridad, a través de "AndalucíaCERT"

B) Organización administrativa.

Debemos comenzar este apartado señalando que hasta este año 2021 donde se ha procedido a la creación de la Agencia Digital de Andalucía, las competencias sobre digitalización y la seguridad de la información han estado adscritas a diferentes Consejerías y entidades o sociedades públicas, de forma, que a pesar de existir como ya hemos visto, una estrategia de planificación global al respecto, su gestión no se encontraba centralizada, la utilización de este modelo de gestión ha sido objeto de consideración favorable por nuestra parte en otro trabajo (Fondevila 2020: 118-131). Efectivamente esta opción organizativa centralizada responde también a la consecución de los objetivos de lo que se entiende por "economías de escala", es decir, el poder que tiene una organización cuando alcanza un nivel óptimo de producción para ir produciendo más a menor coste, es decir, a medida que la producción en una organización crece, sus costes por unidad producida, en este caso, el servicio prestado, se reducen y cuantos más servicios se prestan, menos cuesta prestar los mismos.

Así, podemos señalar las posibles actuaciones que se benefician de esta clase de modelo, en concreto:

1. Una mejora en la delimitación de los ámbitos de actuación competencial a desarrollar por un órgano directivo para una adecuada gestión de los sistemas de información transversales.
2. Recursos Humanos. Indudablemente, una de las áreas más importantes en la implementación de la innovación en la gestión electrónica de nuestras administraciones, es la intervención de los recursos humanos adecuados, tanto para su establecimiento como posteriormente su control y mantenimiento.

   Así, la centralización en un único Departamento de todo el personal técnico responsable sobre sistemas de la información (Analistas, programadores, operadores, etc.), permite establecer una política común de gestión de la seguridad de la información sobre unos instrumentos tecnológicos que se caracterizan por su transversalidad, a este respecto, podemos citar: (gestor común de expedientes electrónicos, sistema de archivo electrónico único, sistemas de firma electrónica común, sistemas de seguridad de la información comunes, etc.).

   Además, la adscripción funcional directa de esta clase de personal a unidades específicas de cada Departamento, generan de forma habitual la creación de espacios de gestión "autónoma" y "disfuncional" con el resto de los sistemas informáticos transversales, lo que provoca de forma generalizada conflictos y daños en los sistemas por problemas de seguridad informática, además de suponer normalmente la creación de un debate y colisión con el modelo general de sistemas de la información, al pretender instaurar aplicaciones individualizadas solo para el servicio de determinados operadores o gestores que no suelen responder a necesidades estratégicas sino a meros criterios tácticos de carácter temporal muy limitado, lo que supone un despilfarro de gasto público y recursos, salvo que en una gestión integradora se habilite su incorporación al sistema general, o bien, si esto no es posible se pueda garantizar que esos sistemas no interfieran en los sistemas generales.
3. Medios materiales: Contratación a gran escala de hardware y software: Eficiencia en el gasto público.
4. Implementación integral y coordinada de sistemas informáticos, de forma que se desarrolle una interoperabilidad interna de los mismos. En este caso, nos queremos referir a la cuestión de la interoperabilidad interna y la creación de sinergias entre sistemas, a este respecto, nos referimos, en concreto, a la implementación organizativa y técnica de la administración digital y la transparencia activa y, otra cuestión esencial, las comunicaciones electrónicas no procedimentales y sus efectos jurídicos, así como la intervención en los portales o páginas web, no integrados en la sede electrónica de la administración.

Pues bien, en estos momentos nos encontramos con una adscripción competencial integral a la Consejería de la Presidencia, Administración Pública e Interior a la cual se adscribe la Agencia Digital de Andalucía, y asimismo, como ente instrumental la Sociedad Andaluza para el Desarrollo de las Telecomunicaciones, S.A. (SANDETEL), de manera que nos encontramos ante una reorganización competencial y funcional que estimamos puede mejorar de forma sustancial la gestión en materia de seguridad de la información y comunicaciones, por las razones ya expuestas.

A lo anterior, debemos añadir el programa gestionado por SANDETEL de gran importancia, y con una larga trayectoria, nos referimos a "AndalucíaCERT", cuyos principales objetivos son:

a) Proporcionar la capacidad de detección y respuesta eficaz y coordinada ante incidentes de ciberseguridad a la Administración general, Organismos y Entidades de la Administración de la Junta de Andalucía.

b) Entre los servicios que se prestan destacamos:

   - Alerta temprana de ciberamenazas. Difusión a las entidades atendidas de amenazas publicadas en la comunidad y que puedan afectar gravemente a los sistemas informáticos.
   - Detección y respuesta a incidentes. Detección automatizada y recepción de notificaciones, análisis experto y asesoramiento en la respuesta a incidentes de seguridad en redes y sistemas informáticos, incluso se realiza el análisis forense tras la contención y resolución del ciberataque.
   - Información, formación y concienciación. Elaboración y distribución de boletines de ciberseguridad, de carácter divulgativo, sobre nuevas amenazas, tecnologías de seguridad, buenas prácticas y temas de actualidad del sector.

Ahora bien, en el momento que se elabora este trabajo se ha anunciado en prensa por la Junta de Andalucía la creación de un "Centro de Ciberseguridad de Andalucía", que lógicamente puede alterar la situación descrita, no pudiendo especificar mayor detalle dado que estamos en presencia de una propuesta política pendiente de desarrollo e implementación administrativa.

IV.2.2. El Ámbito Jurídico material.

En cuanto al régimen jurídico material regulador de la seguridad de la información y comunicaciones, es preciso comenzar destacando que de forma temprana ya se aprobó un marco normativo autonómico que regulaba la Política de Seguridad de la Junta de Andalucía, en concreto, nos referimos al Decreto 1/2011, de 11 de enero,

por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, objeto de alguna modificación puntual (Decreto 70/2017, de 6 de junio), pero que no afecta a su regulación esencial. Pues bien, nos encontramos ante un instrumento que resulta plenamente conforme con las exigencias del ENS, y que ha sido objeto de un desarrollo normativo que procedemos a examinar.

Efectivamente, la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, incorpora una serie de previsiones tanto organizativas como de implementación material de la seguridad que resulta destacables, en concreto:

a) Se reitera la obligación legal, ya prevista en el Decreto 1/2011, de 11 de enero de que, por parte de cada Consejería como las entidades instrumentales, de aprobar su concreta "política de seguridad" que desarrolle en su ámbito la "Política de seguridad general".

b) Debe destacarse el establecimiento de una organización de la gestión de la seguridad, acorde y conforme con las previsiones del ENS, incluso conforme lo anticipado en el Proyecto de Real Decreto que debería sustituir el actual Real Decreto 3/2010 (ENS), en especial, la cuestión de la delimitación de funciones entre el responsable de seguridad y el responsable de sistema, cuestión sobre la que la Memoria del Proyecto de Real decreto del nuevo ENS hace especial hincapié, y que la regulación autonómica actual se encontraría perfectamente adecuada, a título de ejemplo nos remitimos al examen de la Orden de 30 de agosto de 2018, por la que se establece la política de la seguridad de las tecnologías de la información y telecomunicaciones, así como el marco organizativo y tecnológico en el ámbito de la Consejería Presidencia, Administración Local y Memoria Democrática.

c) También es muy importante, a nuestro juicio, la previsión establecida en el artículo 2.4 que determina: "*Los procedimientos y guías técnicas tendrán carácter de recomendaciones y serán desarrollados, por cada organismo o entidad, con arreglo a los ámbitos en materia de seguridad de la información que se establezcan*", que a diferencia de la normativa estatal (ENS), delimita la naturaleza jurídica de esta clase de instrumentos de la seguridad, de manera que nos encontramos ante "recomendaciones", pero no ante disposiciones de carácter general obligatorias, lo que resulta concordante con la fórmula de aprobación. Esta regulación es de destacar pues aporta una seguridad jurídica de la que carece la legislación estatal, como ya hemos indicado en un apartado anterior.

d) Asimismo, esta Orden en su Capítulo II delimita de forma precisa los ámbitos materiales que serán objeto de desarrollo por medio de los "Procedimientos y Guías Técnicas", lo cual supone también una mejora normativa con relación a la legislación estatal (ENS), la cual, en este punto, como ya hemos indicado, supone una regulación disfuncional y de manifiesta inseguridad jurídica.

Por otro lado, es preciso añadir que el mandato legal de aprobación por parte de cada Consejería como por las entidades instrumentales, de aprobar su concreta "política de seguridad", se encuentra en estos momentos cumplimentada en su integridad por las Consejerías[4], y gran parte de los entes instrumentales, lo que ha supuesto que se hayan obtenido las certificaciones de adecuación al ENS en la mayoría de los casos.

También resulta de interés y por ello, es destacable la regulación establecida por la "*Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía*", regulación esencial a los efectos de la gestión de la seguridad de la información y comunicaciones, que sustituye a otra Resolución de 27 de septiembre de 2004, esta clase de previsiones todavía son muy poco usuales en las administraciones, a pesar de resulta de gran necesidad y utilidad. Destaca de la Resolución su amplio y detallado ámbito material de aplicación sobre toda clase de medios electrónicos de uso por los empleados públicos, o como los denomina la misma "profesionales", aunque a nuestro juicio, la misma resulta incompleta y con algunas dudas con relación a su implementación obligatoria, cuestiones estas que analizaremos posteriormente.

IV.3 Una Valoración general y algunas propuestas sobre la implementación de la seguridad de la información y comunicaciones.

Alcanzado este punto, y tras el examen del marco normativo y organizativo en la Junta de Andalucía sobre la seguridad de la información y las comunicaciones, es preciso destacar que nos encontramos ante una implementación muy desarrollada y completa, destacando tanto el desarrollo estratégico mediante la aprobación de los correspondientes planes de actuación, como, asimismo, un amplio desarrollo normativo y finalmente, la creación de una estructura organizativa con amplia experiencia, y que en estos momentos parece haber optado por un modelo centralizado y transversal de la gestión digital y en especial de la seguridad de

[4] A mero título de ejemplo, Orden de 30 de agosto de 2018, por la que se establece la política de la seguridad de las tecnologías de la información y telecomunicaciones, así como el marco organizativo y tecnológico en el ámbito de la Consejería Presidencia, Administración Local y Memoria Democrática (BOJA 4-9-2018).

la información, lo que a nuestro juicio, como ya hemos indicado es el modelo adecuado para este ámbito.

Dicho lo anterior, vamos a formular algunas propuestas sobre el actual marco de la seguridad de la información y comunicaciones que estimamos quizás puedan ayudar a mejorar la actual situación:

Primera. Con relación a la Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía, se estima realizar las siguientes recomendaciones, siguiendo la experiencia utilizada por la Comunidad Autónoma de Cantabria[5], en concreto:

a) Para establecer una mayor vinculación de carácter obligacional a los sujetos objeto de aplicación, se recomendaría utilizar un instrumento de carácter normativo, es decir, una Orden o Decreto.
b) Efectivamente, en concordancia con lo anteriormente señalado, eso permitiría establecer de forma directa una regulación de régimen de responsabilidades disciplinarias y de medidas complementarias, como, por ejemplo, la suspensión de los servicios[6].
c) Por último, se recomendaría la extensión del ámbito subjetivo de aplicación también a los órganos directivos de la administración, y no solo a los empleados públicos, y más aun teniendo en cuenta que los riesgos de la seguridad de la información, son más complejos y extremos en las actuaciones administrativas desarrolladas por esa clase de personal.

Segunda. Se observa también, la ausencia de una regulación específica sobre la categorización del tipo de firma electrónica a utilizar por las autoridades y empleados públicos, esta cuestión afecta de forma directa y esencial a la seguridad de la información, de forma que existe una directa conexión entre el tipo de firma electrónica a utilizar y el régimen de seguridad exigible a la actuación administrativa, es decir, no es lo mismo la emisión de un informe preceptivo o la firma de una resolución, que la simple implementación interna de actuaciones de trámite en un gestor electrónico de expedientes, de forma que un proceso de categorización de la seguridad de la actuación administrativa permite una determinación del tipo de firma electrónica asignable a la autoridad o empleado público, a este respecto

[5] Orden PRE/48/2016, de 22 de julio, por la que se regulan las normas de seguridad sobre utilización de los recursos y sistemas tecnológicos y de información en la Administración de la Comunidad Autónoma de Cantabria.

[6] A estos efectos nos remitimos a la consulta de los artículos 25 y 27 de la Orden PRE/48/2016, de 22 de julio.

nos remitimos al ejemplo del Decreto aprobado al respecto por la Comunidad Autónoma de Cantabria[7].

Tercera. Finalmente, tras el examen de los pliegos tipo aprobados por la Dirección general de Patrimonio de la Junta de Andalucía, se comprueba, que si bien, resulta correcta la regulación sobre Protección de Datos Personales, se aprecia una ausencia regulatoria de la cuestión de la seguridad de la información, cuestión esta de gran importancia a nuestro juicio, y en este sentido es destacable que la disposición adicional tercera del Proyecto de Real Decreto del nuevo Esquema Nacional de Seguridad establece la obligación de incorporan las exigencias de cumplimiento de las previsiones del ENS en los Pliegos de cláusulas administrativas.

Pues bien, a este respecto, recomendamos la consulta de la experiencia de la Comunidad Autónoma de Cantabria, en concreto, la "*Orden PRE/59/2018, de 2 de noviembre, por la que se regulan las condiciones sobre seguridad de la información y protección de datos personales 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" (BOC 12-11-2018)*, que entendemos resulta muy ilustrativa, así que procederemos a realizar un breve examen de las que estimamos necesarias incorporaciones a los Pliegos reguladores de los procesos de licitación, de forma que la seguridad de la información tenga el adecuado reconocimiento y además, las administraciones públicas puedan garantizar la protección de la información y datos de los ciudadanos y de sus organizaciones, en los casos de intervención de terceros ajenos a estas como consecuencia de la ejecución de contratos públicos.

1. Delimitación de la información objeto de protección y tipos de tratamiento de la misma.

a) Sobre la información objeto de protección.

La información a proteger estará referida a cualquier dato, conocimiento o técnica recogida en soportes tanto tecnológicos como no tecnológicos, que sea propiedad de la Administración o que esté tratando, incluida la simple recogida y almacenamiento, para el cumplimiento de sus competencias y obligaciones legales. Esto incluye los datos sobre personas físicas, que se denominarán datos personales o datos de carácter personal.

No será necesario proteger, y por lo tanto no será necesario incluir cláusulas en los pliegos de contratación correspondientes para ese fin, los datos, conocimientos o

[7] Decreto 42/2017, de 22 de junio, por el que se regula el Régimen Jurídico de la Autorización y Uso de la firma electrónica de autoridades y empleados públicos de la Administración de la Comunidad Autónoma de Cantabria y su Sector Público

técnicas que vayan a ser utilizados por el órgano de contratación o el adjudicatario procedentes de fuentes públicas de información: textos normativos, publicaciones científicas, técnicas o profesionales, información de medios de comunicación, información difundida públicamente por otras entidades o información de dominio público.

b) Sobre los tratamientos.

Por tratamiento de la información se entenderá cualquier operación o conjunto de operaciones realizadas sobre la información, incluyendo entre otras la recogida, el almacenamiento, la consulta, la modificación, la transferencia o la difusión.

Se considerará tratamiento automatizado aquel tratamiento que emplee tecnología y en el que las operaciones sobre la información se realizan automáticamente, como sucede al emplear aplicaciones informáticas de gestión.

Se considerará tratamiento no automatizado aquel en que las operaciones se realizan con la intervención directa de una persona, que ejecuta directamente o controla todos los detalles del proceso y toma todas las decisiones, ya sea empleando tecnología tradicional o herramientas informáticas de manera meramente auxiliar.

Se considerará tratamiento mixto a aquel tratamiento de la información que combine operaciones automáticas y operaciones no automáticas.

2. Contratos a los que resultaría necesario incluir en sus pliegos esta clase de obligaciones:

a) Contratos cuyo objeto incluye el tratamiento de información.

b) Contratos cuyo objeto implique el acceso a sistemas de información de la administración por parte del personal del adjudicatario.

c) Contratos cuyo objeto corresponda al suministro de aplicaciones software realizadas a medida y su periodo de mantenimiento correspondiente.

d) Contratos cuyo objeto corresponda a la prestación de un soporte tecnológico avanzado.

e) Contratos cuyo objeto implique el suministro de aplicaciones comerciales o de elementos hardware, así como la subscripción a servicios tecnológicos.

f) Contratos integrales de soporte tecnológico y otros tipos de objeto del contrato relacionados con la tecnología.

3. Especificación de las cláusulas esenciales a incluir en los Pliegos:

a) Pliegos de cláusulas administrativas particulares.

– Cláusula relativa a datos personales de los responsables, representantes o personas de contacto de las partes.

– Cláusula sobre acceso fortuito a información.
– Cláusulas sobre penalidades:
  1. Cláusulas sobre porcentajes de las penalidades a aplicar por incidentes de seguridad de la información.
  2. Cláusulas sobre los niveles de los incidentes de seguridad de la información relacionados con el tratamiento de información.
  3. Cláusulas sobre los niveles de los incidentes de seguridad de la información relacionados con el tratamiento de información para el caso particular del tratamiento de datos personales.
  4. Cláusulas sobre los niveles de los incidentes de seguridad de la información relacionados con el acceso a sistemas de información.
  5. Cláusulas sobre los niveles de los incidentes de seguridad de la información que afecten a la reputación de la Administración.
– Cláusulas sobre información base, propiedad del resultado de los trabajos, requisitos de seguridad de la información del Pliego de Prescripciones Técnicas y Subcontrataciones.
– Cláusulas relativas al acceso a sistemas de información por parte del personal del adjudicatario.
– Cláusulas específicas sobre el tratamiento de datos personales.

b) Pliegos de prescripciones técnicas.

– Cláusulas sobre Acuerdos de Nivel de Servicio.
– Cláusulas sobre interlocución entre las partes.
– Cláusulas para contratos cuyo objeto incluye el tratamiento de información.
– Cláusulas para contratos cuyo objeto del contrato consiste en la prestación de servicios informáticos, incluidos los servicios en la nube.
– Cláusulas para contratos cuyo objeto incluya suministro de aplicaciones software realizadas a medida.

Lógicamente los detalles del contenido de todas estas cláusulas no pueden ser aportadas a este trabajo por limitación de espacio, dicho lo anterior, como se puede comprobar por el lector, este conjunto de previsiones otorga a la administración un plus de seguridad y protección sobre cualquier incidencia que pueda surgir tanto en el desarrollo de la licitación como en especial, y esto es muy importante, durante la ejecución del contrato, lo que significa establecer un marco de protección especial para las administraciones contra posibles sanciones o reclamaciones de responsabilidad patrimonial de la administración por incumplimientos en estas materias.

REFERENCIAS BIBLIOGRÁFICAS

ALAMILLO DOMINGO, I., (2013): "Esquema Nacional de Seguridad en la Administración Electrónica y Responsabilidad Patrimonial por incidentes de seguridad"; en ALMONACID LAMELAS, V. (coord.); *Manual para la Gestión Inteligente del Ayuntamiento*; págs. 411-422; Madrid: El Consultor de los Ayuntamientos – La Ley. 1ª ed.

FONDEVILA ANTOLÍN, J. (2017): "Seguridad en la utilización de medios electrónicos. El Esquema Nacional de Seguridad", en GAMERO CASADO, E. (dir.) y FERNÁNDEZ RAMOS, S. y VALERO TORRIJOS, J. (coord.); *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público*, Vol. I, págs. 674 -597; Valencia: Tirant lo Blanch. 1ª ed.

– (2020): "La organización de la Administración digital" en MARTIN DELGADO, I. (dir); *El Procedimiento administrativo y el Régimen jurídico de la Administración Pública desde la perspectiva de la innovación tecnológica*; págs. 105-142; Madrid: Iustel. 1º ed.

GAMERO CASADO, E. (2015): *Manual Básico de Derecho Administrativo*; pág. 415; Madrid; Tecnos: 16ª ed.

GARCIA MORILLO, J., (1996): "La versatilidad de lo básico", *Revista de Administración Pública (RAP)*; nº 139; págs 125-151; Madrid: Centro de Estudios Constitucionales.

MARTINEZ GUTIERREZ, R. (2009), *Administración Pública Electrónica*; pág. 256; Madrid: Civitas Ediciones – Thomson Reuters. 1ª ed.

MOLES PLAZA, R. J. (2001): *"Derecho y Calidad. El Régimen Jurídico de la normalización técnica"*; Barcelona: Ariel. 1ª ed.

REBOLLO PUIG, M. (2010): "Los Principios Generales del Derecho (Atrevimiento atribulado sobre su concepto, funciones e inducción)", en SANTAMARIA PASTOR, J.A. (dir), *Los Principios Jurídicos del Derecho Administrativo*; pág. 1521; Madrid: La Ley. 1ª ed.

VALERO TORRIJOS, J. (2010): "El alcance de la protección constitucional del ciudadano frente al uso de medios electrónicos por las Administraciones Públicas", en COTINO HUESO, L. y VALERO TORRIJOS, J. (coord.); *Administración Electrónica*; pág. 139; Valencia: Tirant lo Blanch. 1ª ed.

VALERO TORRIJOS, J. (2013): *Derecho, Innovación y Administración Electrónica*; págs. 179-180; Sevilla: Global Law Press- Editorial Derecho Global. 1ª ed.

ANÁLISIS DEL RÉGIMEN JURÍDICO DE LOS DERECHOS DIGITALES DE LOS CIUDADANOS EN SUS RELACIONES CON LA ADMINISTRACIÓN PÚBLICA ANDALUZA

Ariana Expósito Gázquez[1]

I. EL AVANCE DE LA SOCIEDAD DIGITAL Y LOS EFECTOS EN LOS DERECHOS DE LOS CIUDADANOS EN SUS RELACIONES CON LA ADMINISTRACIÓN.

El régimen jurídico y de organización de la Administración Pública lleva años sumergido en una vorágine de reformas para intentar adaptarse a las posibilidades que implican las nuevas tecnologías y dar respuesta a las necesidades que estas generan en la sociedad (Valero y Cerdá, 2020:103). El mejor ejemplo de este proceso de cambio lo encontramos en los instrumentos que se han ido incluyendo dentro de su régimen jurídico: primero, se incorporan *"los medios mecánicos de producción en serie"*[2] para resolver los expedientes administrativos; luego, se incluye *"la aplicación de las técnicas y medios electrónicos, informáticos y telemáticos"*[3]; después, *"la aplicación de medios electrónicos a los proceso de trabajo y la gestión de los procedimientos y de la actuación administrativa"*[4]; y, finalmente, la actuación automatizada íntegra del procedimiento administrativo[5].

---

[1] Doctora en Derecho por la Universidad de Almería. Miembro del Grupo de Investigación "Ciencia y Derecho Público en el S. XXI". La línea de investigación actual está centrada en el análisis jurídico de las nuevas tecnologías y su aplicación e incorporación dentro del Derecho Administrativo.

ORCID: https://orcid.org/0000-0002-6718-5148

aeg581@ual.es

[2] *Vide* Ley de 17 de julio de 1958, de Procedimiento Administrativo, artículo 38.

[3] *Vide* Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, artículo 45.1.

[4] *Vide* Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, artículo 33.1.

[5] *Vide* Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, artículo 41.1.