Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Proyecto de Orden por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Justicia, solicitado de esta Agencia Española de Protección de Datos de conformidad con lo dispuesto en los artículos 37 h) de la Ley Orgánica, de 13 de diciembre, de Protección de datos de Carácter Personal, y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, cúmpleme informarle lo siguiente:

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

Tal y como dispone el artículo 1.1 del texto sometido a informe constituye su objeto "la aprobación de la Política de Seguridad de la Información (en adelante PSI) en el ámbito de la Administración Electrónica del Ministerio de Justicia, así como del marco organizativo y tecnológico de la misma".

En este sentido, recuerda la Exposición de Motivos que el artículo 11 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 "exige que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11.1".

De este modo, el Proyecto desarrolla los principios de la seguridad de la información así como los objetivos que garantizan su cumplimiento. Igualmente se desarrolla la estructura organizativa del Departamento en relación con la seguridad de la información, bajo la dirección del Comité de Dirección de la Sociedad de la Información, presidido por la persona que sea titular de la Subsecretaría del Ministerio, las directrices en materia de gestión de riesgos y los instrumentos normativos de la política de seguridad, conformados por tres niveles normativos estructurados jerárquicamente.

En lo que atañe a la protección de datos de carácter personal, el artículo 2.1 d) establece, dentro de los principios rectores de la seguridad de la información, y siguiendo lo establecido en el artículo 6 del Esquema nacional

de Seguridad, el de gestión de riesgos, indicando que “El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad”.

Asimismo se configura como primero de los objetivos instrumentales enumerados en el artículo 2.2 el de protección de datos de carácter personal, indicando que “Se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal”.

Dentro de la regulación de la estructura organizativa del departamento se determina que cada órgano superior o directivo del Ministerio así como cada Organismo dependiente del mismo a los que sea de aplicación la presente política de seguridad de la información designará un responsable de seguridad, así como los perfiles de responsables de la información, responsables del servicio y responsables del sistema, asumiendo el responsable de la información “las funciones del responsable del fichero”, conforme al artículo 14.2 del Proyecto.

De este modo, y respecto de las funciones de dichos responsables de la información, el artículo 7.1 dispone que “Los Responsables de la Información tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de la información que manejan. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos”.

El artículo 14, a cuyo apartado 2 ya se ha hecho referencia, lleva por rúbrica protección de datos de carácter personal, estableciendo en su apartado 1, en los términos establecido por el Esquema Nacional de Seguridad, que “Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Justicia las medidas de seguridad determinadas en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y resto de normativa sobre la materia vigente”. Finalmente, el artículo 14.3, también de conformidad con lo previsto en el citado Esquema nacional de Seguridad, establece que “En caso de conflicto entre los diferentes responsables, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal”.

Debe recordarse que la Exposición de Motivos del Real Decreto 3/2010 recuerda que “La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de

Datos de Carácter Personal y sus normas de desarrollo, determinan las medidas para la protección de los datos de carácter personal. Además, aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger".

El texto sometido a informe debe ser objeto de análisis desde una doble perspectiva: la del régimen actualmente vigente, conformado por la Ley Orgánica 15/1999 y su Reglamento de desarrollo, y la del régimen que será de aplicación al tratamiento de datos de carácter personal y consiguientemente a la seguridad de la información que contenga dichos datos a partir de la entrada en vigor del Reglamento (UE) 2016/679, comúnmente denominado Reglamento General de Protección de Datos, en que habrá de estarse a lo que disponga la mencionada norma de la Unión Europea así como las disposiciones que se adopten para la adaptación al mismo del derecho español. En este sentido, cabe hacer referencia al Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, que en el presente momento ya ha sido objeto de dictamen del Consejo de Estado en su sesión de 26 de octubre de 2017.

En efecto, como indica la Exposición de motivos del Anteproyecto al que se ha hecho referencia "la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan". De este modo, el cambio de aproximación de la normativa de protección de datos implica necesariamente una modificación en el enfoque que habrá de darse a las políticas de seguridad de la información, en que se evoluciona de un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos que deberá incardinarse en el texto ahora sometido a informe.

Así, el artículo 24.1 del Reglamento General de Protección de Datos dispone que "Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".

Esta previsión se completa con lo señalado en el considerando 75 del Reglamento, según el cual "Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento

pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".

A su vez, en relación con la seguridad de la información, el artículo 32.1 establece que "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".

Un papel fundamental, en fin, dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el Delegado de Protección de Datos, que el Reglamento General regula en sus artículos 37 a 39. En particular, el artículo 37.1 a) impone obligatoriamente la designación de un Delegado en los supuestos en que "el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial".

A su vez, el artículo 38.1 establece claramente que "El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales" y el artículo 39.2 dispone que "El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento".

Finalmente, el artículo 39.1 enumera las funciones del delegado de Protección de Datos, entre las que se encuentran ""informar y asesorar al

responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros" (apartado a), "supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes" (apartado b) y "ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 (apartado c).

De lo que acaba de indicarse se desprenden dos conclusiones que afectan sustancialmente al Proyecto objeto de informe: por una parte, la evolución del modelo desde la lista de cumplimiento a la responsabilidad activa impone que el análisis de riesgos en materia de protección de datos y, en su caso la evaluación de impacto en la misma, pase a formar parte integrante de la política de seguridad de la información, de modo que no se produzca una mera remisión a las normas de protección de datos, habida cuenta que éstas ya no establecen un modelo tasado de cumplimiento.

Por otra, el papel del Delegado de Protección de Datos, obligatorio en el supuesto que ahora se está analizando, resulta esencial en todo el diseño y desarrollo de la política de seguridad de la información, debiendo tener pleno conocimiento de la misma y asesorar en su diseño e implantación, en virtud de las funciones que el reglamento general de Protección de Datos le otorga expresamente.

Ello impone la introducción de importantes modificaciones en el Proyecto sometido a informe, siendo la primera de ellas evidentemente la inclusión del delegado de protección de datos dentro de la estructura organizativa de la gestión de la seguridad de la información y atribuyendo al mismo las funciones que establece el propio Reglamento, de modo que sea oído en todo caso en el diseño e implantación de dicha política de seguridad.

Pero también exige un nuevo enfoque del texto basado en la necesidad de realización del análisis de riesgos establecido en el artículo 24 del Reglamento y, en su caso, de la evaluación de impacto en la protección de datos a la que se refiere su artículo 35 para la determinación de las medidas que garanticen adecuadamente la seguridad de la información desde el enfoque de la protección de datos de carácter personal.

Ello supone que el artículo 2.1 d) y el artículo 2.2 a) deberían modificarse a fin de tener en cuenta este nuevo enfoque, recogiendo las exigencias del artículo 24 del Reglamento General de Protección de Datos y eludiendo la

referencia a las medidas establecidas en la normativa vigente, dado que en el nuevo marco normativo no existirá una lista tasada de medidas, sino que aquéllas procederán del resultado del análisis que habrá de llevar a cabo el responsable del tratamiento.

Además, este nuevo enfoque debería ser tenido en cuenta en la descripción de las funciones del responsable de seguridad y del responsable de información, teniendo en cuenta que sería necesario modificar la referencia que el artículo 14.2 del Proyecto efectúa cuando indica que el responsable de la información “asumirá las funciones de responsable del fichero”, dado que dicha función corresponderá, según el artículo 4.7 del Reglamento General de Protección de Datos, a la “autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento”, siendo además su denominación la de responsable del tratamiento, dado que el concepto “responsable del fichero” no aparece recogido en el citado Reglamento.

Finalmente, sería preciso modificar el apartado 1 del artículo 14, teniendo en cuenta que las medidas de seguridad ya no vienen “determinadas” por la normativa de protección de datos, sino que serán las que corresponda implantar atendidos los riesgos generados por el tratamiento una vez llevada a cabo la evaluación exigida por el artículo 24.1 del Reglamento General de Protección de Datos.