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 Sanidad, Servicios Sociales e Igualdad, 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.

Conforme indican su rúbrica y su artículo 1.1 el objeto de la norma sometida a informe consiste en la aprobación de la Política de Seguridad de la información y la estructura organizativa de gestión de la seguridad del Ministerio de Sanidad, Servicios Sociales e Igualdad, en desarrollo del Esquema Nacional de Seguridad, aprobado por Real Decreto 3/2010, de 8 de enero, cuyo artículo 11 establece que "todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente", incorporando los principios de su artículo 4 y los contenidos del propio artículo 11.1 y las medidas de seguridad establecidas en su Anexo II.

Como punto de partida debe ponerse de relieve lo ya indicado por esta Agencia en cuanto a la interrelación de las previsiones del Esquema Nacional de Seguridad y la normativa de protección de datos. Así, en su informe al Proyecto de Esquema Nacional de Seguridad, de fecha 2 de diciembre de 2009, esta Agencia indicaba lo siguiente:

> *"(…) la interrelación entre la norma sometida ahora a informe y la normativa vigente en materia de protección de datos de carácter personal resulta incuestionable, dado que el artículo 9 de la Ley Orgánica 15/1999 establece en su apartado 1 que "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural". Además, el artículo 9.3 de la Ley Orgánica añade que*

"reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

El mencionado desarrollo se encuentra actualmente contenido en el Reglamento de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en cuyo Título VIII se establecen las medidas de seguridad que necesariamente deberán contener los sistemas de información en los que se contengan datos de carácter personal.

Ciertamente, el objetivo de la norma ahora sometida a informe no coincide con el descrito en las normas de protección de datos, por cuanto aquél se refiere no sólo a los ficheros que contengan datos de carácter personal, sino a los que incorporen cualquier tipo de información administrativa, con independencia de su contenido real y de la existencia en la misma de tales datos. No obstante, resulta necesario tener en cuenta que la práctica totalidad de las informaciones contenidas en los sistemas de información de las Administraciones Públicas contendrán datos de esa naturaleza.

A tal efecto, debe recordarse que la Ley Orgánica 15/1999 define los datos de carácter personal como "cualquier información relativa a personas físicas identificadas o identificables", añadiendo el artículo 5.1 f) del Reglamento que dicha información podrá ser "numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo".

Además, no es preciso que la información aparezca directamente vinculada a la persona a la que aquélla se refiere, sino que será suficiente que aquélla se refiera a personas identificables, definiendo como tales el artículo 5.1 o) del Reglamento "toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".

En consecuencia, no cabe duda que en la mayor parte de los supuestos, la información administrativa sometida al Esquema Nacional de Seguridad contendrá datos de carácter personal. En ese caso las previsiones del Esquema Nacional de Seguridad deberán resultar concurrentes y no excluyentes de las medidas previstas en el Reglamento de desarrollo de la Ley Orgánica 15/1999."

Quiere ello decir, a juicio de esta Agencia, que el establecimiento de una política de seguridad de la información, como la regulada por el Proyecto sometido a informe, y la adopción de las medidas exigidas por la Ley Orgánica

15/1999 en relación con los tratamientos de datos de carácter personal no pueden ser concebidas como compartimentos estancos y diferenciados, habida cuenta que la interacción entre ambas previsiones determina que la seguridad de la información se encuentre influida por las medidas que garanticen la seguridad de los datos personales y viceversa. Por ello, no parece suficiente a nuestro juicio la mera consideración de las exigencias de protección de datos como separada o complementaria de las directrices de seguridad de la información, sino que dichas exigencias han de ser valoradas en todo momento a la hora de establecer las directrices de seguridad de los sistemas de información, contengan o no contengan datos; del mismo modo, estas últimas garantías de seguridad habrán necesariamente de incluir en la seguridad establecida sobre la información que contenga a su vez datos de carácter personal.

El Proyecto sometido a informe, sin embargo, parece mantener estos dos tipos de garantías y procedimientos de prevención de los riesgos de seguridad como compartimentos diferenciados. En este sentido, las únicas referencias contenidas en el texto ahora informado a las normas de seguridad en el tratamiento de datos de carácter personal son las incorporadas a su artículo 3.1, al citar en las letras f) y g) a la Ley Orgánica 15/1999 y su reglamento de desarrollo como parte del marco normativo aplicable al Departamento, y en el artículo 14, que se limita a señalar que “en los casos en que un sistema trate datos de carácter personal, el Responsable de la información será el responsable del fichero”.

De este modo, al hacerse referencia a la estructura de seguridad no se valora a quién deberían corresponder las responsabilidades que la normativa de protección de datos, y en particular el artículo 95 del Reglamento de desarrollo de la Ley Orgánica 15/1999 atribuyen al responsable de seguridad. A nuestro juicio, **sería conveniente que se clarificase que dicha función corresponderá al responsable de seguridad, incluyendo así en las funciones establecidas para el mismo las relacionadas con la garantía de la seguridad establecidas en la normativa de protección de datos de carácter personal**.

Del mismo modo, la descripción de la política de seguridad prevista en el Anexo se lleva a cabo prescindiendo de la aplicabilidad de las medidas específicas de seguridad que correspondan cuando la información contenga datos de carácter personal, siendo así que en tales casos el Reglamento de desarrollo de la Ley Orgánica 15/1999 fija unos criterios mínimos de seguridad que deberán ser necesariamente respetados.

De este modo, los distintos aspectos de la seguridad de la información a garantizar llevan siempre aparejada la implantación, en caso de existir datos de carácter personal, de una serie de medidas mínimas que habrán de ser respetadas por la organización y que podrían resultar igualmente aplicables al resto de la información incluida en los sistemas. En este sentido, cabe hacer

referencia a las disposiciones del Reglamento en relación con la elaboración del documento de seguridad, sobre la que se hará posteriormente una específica referencia, la gestión de los soportes y equipos que contengan datos de carácter personal, el control de los usuarios y los procedimientos para su identificación y autenticación, el cifrado de la información más sensible cuando la misma vaya a salir de la organización, bien mediante un soporte físico bien a través de redes públicas de comunicaciones electrónicas, la realización de copias de seguridad, el control de acceso físico a las zonas donde residan los equipos y sistemas, el control o registro de accesos a la información y la gestión de incidencias y las medidas de recuperación de la información.

Estas medidas igualmente se complementan con las relacionadas con la necesaria auditoría de los sistemas, que en el caso de contener datos personales y ser exigibles las medidas de seguridad de nivel medio o alto establecidas en la normativa de protección de datos de carácter personal no serán disponibles en cuanto a su periodicidad o alcance por la estructura organizativa de la seguridad de la información.

Como se ha dicho, la interrelación entre las normas de seguridad de la información y las de seguridad en el tratamiento de los datos ha de reputarse continua y no separada. Por ello, se considera que **en la Política de seguridad debería hacerse expresa referencia a las normas de protección de datos dentro de cada política de seguridad de las que el documento establece y, particularmente, a lo largo de cada epígrafe de los que componen el Anexo**.

En este sentido, en cuanto a las cuestiones organizativas, debe reiterarse que esta Agencia considera que sería deseable la especificación de las mismas dentro de las funciones propias de los distintos órganos que componen la estructura del Departamento en relación con la seguridad de la información. Este mismo criterio es el que en nuestra opinión debería regir la determinación sustantiva de las medidas, no considerándose suficiente esa mera referencia genérica al documento de seguridad.

En consecuencia, esta Agencia considera que **sería preciso modificar el Proyecto sometido a informe estableciendo los criterios mínimos de seguridad exigidos por la legislación de protección de datos como parte de la política de seguridad y en cada uno de los aspectos de la misma y adaptando la estructura de seguridad a las exigencias de la normativa de protección de datos, particularmente en la determinación de las funciones de cada uno de los órganos que la integran en relación con la función de responsable de seguridad establecida en el reglamento de desarrollo de la Ley Orgánica 15/1999**.