Informe 0024/2010

Se consulta si resulta de aplicación lo previsto en el artículo 103.6 del Reglamento de desarrollo de la Ley Orgánica 15/1999, referido a la posibilidad de excepcionar la obligación de establecer un registro de accesos en un fichero al que deben aplicarse medidas de seguridad de nivel alto, en el caso de una sociedad limitada profesional, conformada por un matrimonio, ambos médicos, en que cada uno tiene su propia clientela, a la que atienden en la misma consulta, compartiendo también otros recursos como los de personal administrativo e informáticos. Señala la consulta que existe un ordenador de uso común, si bien cada uno tiene un nombre de usuario y contraseña diferentes y no tiene acceso a los datos de salud de los clientes del otro cónyuge.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar.

En lo que al presente supuesto se refiere resulta de aplicación lo previsto en el artículo 81.3, conforme al cual "*Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:*

a. *Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual."*

Debe tenerse presente, tal y como dispone dicho precepto, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

De esta manera, el artículo 91 del Reglamento impone en los ficheros de nivel básico como una de las medidas de seguridad la del control de acceso, disponiendo en su número primero que "*Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones",* para ello exige en su número tercero que *"El responsable del fichero establecerá*

mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados."

A este respecto, debe recordarse que el artículo 16.1 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, dispone que "*La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia."*

Esta Agencia ha señalado que dicho precepto debe ser interpretado, a sensu contrario, en el sentido de que no será posible que los facultativos no relacionados con la actividad preventiva y diagnóstica de una determinado paciente puedan acceder a sus datos, siendo esta regla igualmente aplicable al personal auxiliar que pudieran haber contratado la entidad consultante, dado que conforme al artículo 16.4 de la misma norma "*El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones."*

Asimismo, el Reglamento de desarrollo de la Ley Orgánica 15/1999 establece una obligación de identificación y autenticación de los usuarios, exigiéndose ya desde el nivel básico una identificación personalizada de los usuarios, a diferencia de la normativa anterior en la que tenían cabida los usuarios genéricos. Dispone el artículo 93.1, a estos efectos, que "*El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios*." Por su parte, el número 2 del mismo artículo prevé que "*El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado."*

En consecuencia, la existencia de un nombre de usuario y contraseña, así como el acceso sólo a recursos propios a que hace referencia la consulta responde a la aplicación de las medidas de nivel básico exigibles a cualquier fichero, debiendo aplicarse, además, las previstas para el nivel medio y alto,

En el nivel medio, la medida de identificación y autenticación se vuelve más rigurosa ya que, a las medidas anteriores previstas para el nivel básico, se añade la contenida en el artículo 98 según el cual "*El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."*

Por último, en el nivel alto, se requiere ya un registro de cada intento de acceso que se produzca, establece el artículo 103.1 que "*De cada intento de*

acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado." Mientras que el número segundo del mismo artículo dispone "*En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido."*

Esta Agencia ha venido señalando el criterio a seguir respecto a la aplicación de este precepto, que recoge las previsiones ya contenidas en el artículo 24.2 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, derogado expresamente por la disposición derogatoria única del Real Decreto 1720/2007.

Así en informe de 16 de enero de 2006, se señala la interpretación que debe darse al precepto al aclarar que del mismo "*se deduce que el registro de accesos se refiere al fichero y, dentro del fichero, a los distintos registros accedidos, es decir, a los concretos datos personales que se consultan."* Indica también cual es la finalidad de la medida de seguridad apuntando que *"El aspecto esencial a tener en consideración en estos casos será el que la información almacenada en el registro de accesos permita identificar inequívocamente qué persona ha tenido acceso y a qué información contenida en el fichero en cada momento, a fin de que, en caso de ser necesario reconstruir cuándo y cómo se produjo una determinada revelación de un dato, sea posible identificar la persona que pudo conocerlo en ese momento concreto."*

Concluye el aludido informe que "*Por tanto, el control de los accesos deberá efectuarse de la forma más detallada posible, a fin de conocer efectivamente quién ha podido en cada momento conocer los datos incorporados al sistema, es decir, a qué datos o recursos se ha accedido, sin que puedan efectuarse meros controles genéricos, por referencia al sistema en su conjunto."*

De la misma manera la Resolución 001/2003 se refiere a la función que cumple dicha medida de seguridad, señalando que "*De ahí, la previsión del artículo 24.2 citado dirigida a poder conocer, cuando los accesos han sido autorizados, los registros a los que se ha accedido, previsión que posibilitará analizar si el acceso a los datos de salud por un usuario autorizado está o no justificado respecto de unos concretos datos personales de salud .*

Por tanto, en el caso de que se produzcan los accesos autorizados a los datos de salud, es preciso, como exige el artículo 24.2 del Reglamento, guardar la información sobre los registros accedidos como requisito necesario para poder comprobar si el acceso responde o no a la finalidad descrita."

La medida de seguridad constituida por el registro de acceso regulado en el artículo 103 del Reglamento solamente conoce una excepción, prevista en el número 6 del mismo artículo que establece lo siguiente:

"*No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:*

a. Que el responsable del fichero o del tratamiento sea una persona física.
b. Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad."

La Ley Orgánica 15/1999, define al responsable del fichero en su artículo 3.d) como la "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". En el presente caso,* debe entenderse que el responsable del fichero es la mercantil consultante y no sus socios individualmente considerados, así se desprende de lo previsto en el artículo 5.2 de la Ley 2/2007, de 15 de marzo, de sociedades profesionales, conforme al cual "*Los derechos y obligaciones de la actividad profesional desarrollada se imputarán a la sociedad, sin perjuicio de la responsabilidad personal de los profesionales contemplada en el artículo 11 de esta Ley."*

Por consiguiente, debe contestarse en sentido negativo a la pregunta formulada en la consulta, dado que en el momento en que no se den las dos circunstancias previstas en el artículo 103.6, será preciso generar el correspondiente registro de accesos en los ficheros calificados como de nivel alto.

No obstante, *a* efectos de no extender las medidas de seguridad de nivel alto a todo el fichero, cabría utilizar la posibilidad prevista el artículo 81.8 del Reglamento de desarrollo de la Ley Orgánica 15/1999 al establecer que "*cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad".*

De esta manera, podrían segregarse del fichero los datos relativos a la salud de los pacientes clientes de cada uno de los profesionales médicos, aplicando a esa parte las normas de seguridad de nivel alto, entre las que se

incluyen la relativa al registro de accesos, aplicando al resto del fichero las medidas de seguridad correspondientes a la naturaleza de los datos tratados.