Informe 0584/2009

Se consulta si la aplicación informática de que dispone el consultante resulta adecuada a lo previsto en el artículo 103 del 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**.**

Según indica el consultante, realiza el tratamiento de datos que requieren medidas de seguridad de nivel alto y que se encuentran en ficheros office (Word, Excel, etc.) a los que se accede a través de una aplicación que tiene registro de accesos (usuario, fecha, tipo de acceso), de manera que puede saberse si se ha modificado un fichero office en general, por quien y cuando, pero sin que se pueda, a través de dicha aplicación, saber que dato personal en concreto se ha modificado del correspondiente fichero.

El artículo 103 del Reglamento dispone 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.*

2. 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, señala así 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."

Por consiguiente, el responsable del fichero deberá contar con las aplicaciones informáticas necesarias que permitan cumplir con las exigencias establecidas en el Reglamento de desarrollo de la Ley 15/1999 en el que se recogen en la actualidad las medidas de seguridad a aplicar a ficheros y tratamientos, toda vez que el artículo 9.2 de la Ley Orgánica 15/1999 dispone que "*No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas*."

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 según el cual "A los efectos de facilitar el cumplimiento de lo dispuesto en este título, 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, si se dan las condiciones exigidas en dicho artículo, esto es, que se puedan delimitar tanto los datos afectados como los usuarios con acceso a los mismos, podrá efectuarse una segregación de los ficheros limitando las medidas de seguridad de nivel alto a aquellos ficheros que por la naturaleza de los datos que contienen requieren la adopción de este tipo de

medidas, mientras que a los restantes se aplicarían aquéllas que, conforme a lo dispuesto en el artículo 81 del Reglamento, les correspondan.