Informe 0318/2009

La consulta plantea, varias cuestiones relacionadas con el acceso al Sistema de Registros Administrativos de Apoyo a la Actividad Judicial por parte de los funcionarios de los Juzgados de penal e instrucción, para actuar de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y el Reglamento de Desarrollo de la misma aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

El artículo 14 del Real Decreto 95/2009 adopta el criterio de implementar las medidas de seguridad previstas en el Real Decreto 1720/2007, de 21 de diciembre, y en especial las medidas previstas en el artículo 103.1 y las del 104.

Una vez efectuada esta introducción es preciso señalar que atendiendo a las definiciones contenidas en el Reglamento de desarrollo de la Ley Orgánica 15/1999, Artículo 2.2 contiene una serie de definiciones aplicables al supuesto de hecho planteado en la consulta;

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Por tanto, usuario es el sujeto y en los términos de la consulta es la persona física que accede al fichero, por otro lado, el perfil de usuario define el tipo de información a la que éste puede acceder y el tipo de acciones que puede realizar un ejemplo simple, sería permitir el acceso al Registro Centras de Penados y poder modificar los datos contenidos en éste y por último todo usuario con independencia de su perfil debe de tener un acceso controlado

Es control de acceso, se regula en el artículo 91 del Real Decreto 1720/2007 señalando que “1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio”.

El propio artículo 91.1 alude al acceso sólo para el desarrollo concreto de sus funciones, esta medida extrapolada al supuesto de hecho planteado en la consulta, exige analizar el Real Decreto 95/2009, de 6 de febrero, donde se regula en el artículo 5. Acceso general a la información contenida en el Sistema de Registros

1. El Ministerio de Justicia autorizará, estableciendo las medidas de seguridad oportunas, el acceso directo a la información contenida en los Registros Centrales integrados en el Sistema a;

a) Los órganos judiciales, a través del personal de cada oficina judicial autorizado por el Secretario Judicial, a los efectos de su utilización en los procedimientos y actuaciones de los que están conociendo en el ámbito de sus respectivas competencias, conforme a las disposiciones legales vigentes.

Por su parte el artículo 6 del mismo texto legal añade que el acceso a la información contenida en el Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes "Además de los indicados en el artículo anterior, el Ministerio de Justicia autorizará, estableciendo las medidas de seguridad oportunas, el acceso directo a la información contenida en el Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencia no Firmes, siempre que en uno y otro caso se refiera a inscripciones no canceladas, a:

La policía judicial, a través de los funcionarios autorizados que desempeñen estas funciones, en tanto sea necesario para el ejercicio de las competencias previstas en el artículo 549.1 de la Ley Orgánica del Poder Judicial"

Y en los mimos términos se pronuncia el artículo 7 donde se regula el acceso a la información contenida en el Registro Central de Protección a las Víctimas de Violencia Doméstica.

Quiere esto decir que sólo los funcionarios que desarrollen las funciones previstas en los artículo 5, 6 y 7 pueden acceder al sistema y sólo respecto de aquellos recursos, vinculados a las funciones que les compete.

A su vez, el artículo 91.3.señala que "El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados." Esto es, no se permite la existencia de usuarios y contraseñas compartidas, para lo cual es necesario que cada usuario tenga una identificación de carácter exclusivo y la par que sea secreta, por ello, debe implantarse un procedimiento que garantice la seguridad y confidencialidad en el otorgamiento de identificación y autenticación de los usuarios (esto es, que la contraseña sólo sea conocida por el usuario).

Estos dos requisitos se detallan en el artículo 93 del citado Reglamento señalando que " 1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. 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.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."

Además lo señalado sólo es aplicable respecto de las medidas de seguridad de nivel básico, pero el tratamiento o acceso a los datos contenidos en el Registro Central para la protección de las victimas de violencia doméstica, deberá cumplirse con las de nivel alto, así lo exige el artículo 81.3 "3. 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: (..)
c) Aquéllos que contengan datos derivados de actos de violencia de género.

En este último caso se debe crear un Registro de accesos, así lo determina el artículo 103 del Real Decreto 1720/2007 donde se determina que "1. 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.(..)".

El cumplimiento de todas estas medidas deberá de recogerse en el llamado documento de seguridad y que se encuentra regulado detalladamente en el artículo 88 del citado reglamento "1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su

organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:
a) La identificación del responsable o responsables de seguridad.
b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.”