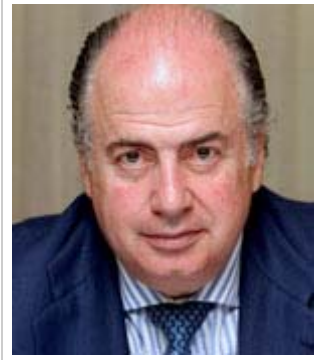
ECOS Y COMENTARIOS

Ricardo de Lorenzo

La identificación y autentificación como medida de seguridad en el ámbito sanitario

Cada vez es más habitual que en los Centros Sanitarios se produzca la informatización de las historias clínicas de los pacientes que son tratados en ellos, comenzando a utilizarse programas informáticos de gestión hospitalaria que recogen los datos de carácter personal de éstos.



Estos programas deben de recoger las diferentes medidas de seguridad que se indican en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 12 diciembre, de Protección de Datos de Carácter Personal, una de ellas es la que se recoge en los Arts. 93 y 98 del citado Reglamento y que hacen referencia a la identificación y autenticación de los usuarios que tienen acceso al sistema informático.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación, siendo la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

El responsable del tratamiento de los datos de carácter personal, en nuestro caso el responsable del Centro Sanitario en cuestión, debe en primer lugar adoptar las medidas para garantizar la correcta identificación y autenticación de todos los usuarios, que para la realización de su trabajo tengan acceso al programa informático que recoge los datos de carácter personal como pueden ser los auxiliares, enfermeros o los doctores, estableciendo un mecanismo que permita su identificación de forma inequívoca y personalizada de todo aquel trabajador que intente acceder al sistema y se verifique que éste se encuentra autorizado para ello.

En la mayoría de los casos este mecanismo de autenticación se basa en la existencia de contraseñas, las cuales se asignarán, distribuirán y almacenarán de tal forma, que se garantice su confidencialidad e integridad, no teniendo que conocerse por parte de los trabajadores la contraseña de sus compañeros.
En el Documento de Seguridad del Centro Sanitario se indicará la periodicidad con la que tienen que ser cambiadas las contraseñas, que en ningún caso será superior a un año, y mientras éstas estén vigentes se almacenará de forma ininteligible.

Para cumplir correctamente con esta medida de seguridad, también se debe establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
El incumplimiento de esta medida de seguridad será considerada como una infracción grave de acuerdo con el Art. 44.3.h. de la Ley Orgánica 15/1999, de 12 diciembre, de Protección de Datos de Carácter Personal “3. Son infracciones graves: (…) h. Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.”, llevando aparejado este tipo de infracciones, una sanción que de acuerdo con el Art. 45 de la Ley Orgánica 15/1999, de 12 diciembre, de Protección de Datos de Carácter Personal, puede oscilar entre los 40.001 a 300.000 euros.

Por todo lo indicado anteriormente, queda claro que se deben cumplir todas las medidas de seguridad que se recogen en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 12 diciembre, de Protección de Datos de Carácter Personal, ya que su incumplimiento conlleva la imposición de una cuantiosa multa.