ECOS Y COMENTARIOS

Ricardo de Lorenzo

La auditoría bienal de la LOPD

Una de las principales obligaciones que vienen marcadas por la normativa de protección de datos, en concreto en los artículos 96 y 110 del 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, es la realización de una auditoría de carácter bienal, sobre el nivel de cumplimiento de las medidas de seguridad adaptada por las organizaciones, cuando los datos tratados o bien sean de nivel medio y/o alto, o cuando se produzcan modificaciones sustanciales en los sistemas de información.

Es bastante fácil entender cuál fue la voluntad del legislador a la hora de incluir esta obligación. Con la imposición de dicha auditoría se instaura un método que avala el continuo y correcto cumplimiento de las medidas técnicas, organizativas y jurídicas que contribuya a la seguridad de los datos manejados por las empresas, asegurando con ello que no basta una simple adaptación de los procedimientos y sistemas de tratamiento a la Ley Orgánica de Protección de Datos y su normativa de desarrollo, si no también la actualización a los procesos evolutivos que sufra el tratamiento de datos.

Esta obligación cobra especial importancia en los Centros Sanitarios tanto públicos como privados, dado que por un lado, al menos uno de sus ficheros declarados contendrá los datos de salud de sus pacientes y por ende les es de aplicación las medidas de seguridad de nivel alto. La realidad es, como destacó la Agencia Española de Protección de Datos en su última memoria anual, que la realización de la auditoría bienal de seguridad del fichero de Historias Clínicas es uno de los aspectos en los que se observa un menor nivel de cumplimiento de la normativa de protección de datos, ya que en un 32,5% de centros esta actuación no se lleva a cabo. En un 85,6% de los centros que realizan la auditoría, se han detectado en ella deficiencias de seguridad. Un 22,5% de los hospitales han realizado la última auditoría en 2010, un 30,8% en 2009, un 10% en 2008 y un 7,4% en 2006 o años anteriores. Un 29,3% de los centros no aporta información sobre la fecha de la última auditoría de seguridad realizada.

Pero no debemos olvidar, que la obligación de esta Auditoría no se da como hemos dicho, únicamente por tratar datos de nivel medio y/o alto, sino también por cambios sustanciales en los sistemas de tratamiento de datos, que cada vez son más frecuentes, a causa de la integración de las tecnologías de la información y la comunicación aplicadas al mundo sanitario, con conceptos tales como la Historia Clínica Electrónica y la E-Receta, así como la evolución de los software de salud, conllevando la necesidad de una continua actualización y realización de las aquí mencionadas Auditorías con una periodicidad menor a esos dos años marcados.

El incumplimiento por parte de los responsables del tratamiento de datos de la realización de esta revisión de medidas de seguridad lleva aparejada el inicio de un procedimiento sancionador de la Agencia Española de Protección de Datos, que califica el hecho como una infracción grave, con una posible sanción que oscila entre los 40.001€ hasta los 300.000€, acumulándose a la posible sanción por fracción grave por la incumplimiento de requerimiento por parte de las autoridades, ya que este informe final deberá de estar a disposición de la Agencia Española de Protección de Datos, previa solicitud de este organismo.

Por todo lo expuesto, queda claro que el cumplimiento de la normativa de protección de datos va más allá de una simple y primera adaptación, dado que como legislación flexible a los procesos evolutivos de las entidades que la aplican, es necesaria su constante actualización a través de Auditorías, que plasmen en primer lugar, la situación real del cumplimiento de las medidas de seguridad, junto con las recomendaciones necesarias para su correcta aplicación de las deficiencias que puedan ser encontradas.