Informe 0494/2009

La consulta plantea la aplicación de sistemas alternativos al cifrado de documentos, tal y como prevé el artículo104 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Según se desprende del contenido de la consulta, esta cuestión se planteó con anterioridad, dando lugar a un informe de fecha 9 de junio de 2009. Sin embargo la entidad consultante, en este momento, aporta más información a los efectos de analizar la situación desde otro prisma.

La respuesta ha sido efectuada según el criterio técnico de la Subdirección General de Inspección señalando que;

> *"En anteriores informes se ha señalado que la información que se pretende intercambiar a través de la red contiene datos a los que se les ha de aplicar un nivel de seguridad alto.*
>
> *Como indica el artículo 104 de Reglamento aprobado por RD 1720/2007, al pretender realizar el intercambio de información a través de redes públicas es necesario garantizar que los datos que viajan por dicho medio no sea ni inteligibles ni manipulables por terceros.*
>
> *El legislador indica que el medio de obtener ese objetivo es mediante cifrado, aunque deja abierta la posibilidad, cuando habla de "utilizando cualquier otro mecanismo" de utilizar otros métodos que ofrezcan las mismas garantías con el propósito de no cerrarse a tecnologías actuales de aplicación específica o, sobre todo, a tecnologías futuras.*

Existen técnicas que actualmente se pueden emplear como alternativa al cifrado de datos, como son la esteganografía para el caso de ocultación de mensajes a nivel de aplicación o la transmisión mediante espectro ensanchado (spread-spectrum) para el caso inalámbrico a nivel físico. Todas ellas con una implementación y una gestión mucho más compleja y problemática que la que ofrecen los actuales sistemas de cifrado. En este momento no se disponen de tecnologías más ágiles para preservar la confidencialidad de la información que emplear herramientas de cifrado, aunque en un futuro estas puedan aparecer.

Pero no sólo es necesario cifrar, sino cifrar de forma que la información no sea inteligible ni manipulada por terceros. Sin esta última condición, no se cumplirá lo estipulado en el citado artículo 104. Esto implica dos cosas, por un lado que el sistema de cifrado a emplear no esté comprometido, es decir, que no se conozca forma de romperlo. En la propuesta señalada en su último escrito, tanto el cifrado que ofrecen los productos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable. Aunque para el uso particular pudieran considerarse adecuadas, no así para el intercambio de información con las garantías que se precisan en el Reglamento.

Por otro lado, esta garantía necesaria para preservar la confidencialidad de las comunicaciones no sólo descansa en el sistema de cifrado, sino también en el sistema de gestión de claves, en particular, y en el procedimiento de administración de material criptográfico, en general. Sin una correcta definición de ambos, que no se encuentran en su escrito, las comunicaciones a largo plazo estarán comprometidas y no se cumplirá con lo estipulado en el artículo 104 señalado anteriormente.

La seguridad en el intercambio de información de carácter personal en la que hay que adoptar medidas de seguridad de nivel alto, en particular los requisitos de cifrado de datos, no es un tema baladí, ni un mero trámite administrativo, ni una cuestión de comodidad. Es el medio técnico por el cuál se garantiza la protección de un derecho fundamental y al que hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación."

A la vista del criterio técnico emitido por la Subdirección General de Inspección, esta Agencia, no puede sino ratificarse en las conclusiones alcanzadas en el informe de fecha 9 de junio de 2009.