



La consulta plantea el plazo durante el cual deberá conservarse a disposición de la Agencia Española de Protección de Datos el informe de auditoría de seguridad al que se refiere el artículo 96 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.

Como señala la consulta, el mencionado precepto dispone en su primer apartado que “a partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente Título”, añadiendo que “con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior”.

A su vez, el apartado 3 del precepto establece que “los informes de auditoría (...) quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas”, si bien no se establece el plazo de conservación a disposición de la Agencia de tales informes.

El artículo 44.2 h) de la Ley Orgánica 15/1999 dispone que constituirá infracción grave de la Ley “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”. Dicha infracción prescribirá a los dos años de su comisión, tal y como dispone el artículo 47.1 de la Ley.

Como puede comprobarse, el responsable del fichero y el encargado se encuentran obligados a la realización, siempre que sean de aplicación las medidas de seguridad de nivel medio, como mínimo, de una auditoría cada dos años, siendo precisamente de dos años el plazo de prescripción de la sanción consistente en no haber cumplido con dicha obligación.

De este modo, en caso de que por esta Agencia se requiriese el último informe de auditoría presentado conforme a lo dispuesto en el artículo 96 del reglamento de desarrollo de la Ley Orgánica 15/1999, la entidad requerida debería siempre tener a disposición de la Agencia un informe emitido durante los dos años anteriores al momento en el que se solicita el requerimiento,



siendo éste precisamente el último informe de auditoría al que debería haberse sometido la entidad.

A la vista de lo anterior, teniendo en cuenta los plazos de prescripción y de obligación de sometimiento a la auditoría, el término durante el cual el informe debería estar a disposición de la Agencia Española de Protección de Datos o autoridad autonómica de control competente debería ser el de dos años, de modo que si no se dispusiera de un informe de esa antigüedad la entidad responsable o encargada estaría vulnerando lo dispuesto en la Ley Orgánica 15/1999 y su Reglamento de desarrollo, al no haber sometido los sistemas a una nueva auditoría en el plazo señalado.

En todo caso, y a fin de evitar la posible comisión de una infracción en caso de haberse llevado a cabo una nueva auditoría y no haberse ultimado las conclusiones de la misma, se considera que sería conveniente que en todo caso se encontrase a disposición de la Agencia el último informe de auditoría que se hubiese emitido, no siendo preciso mantener a su disposición los anteriores a aquél.