CNS 12/2010

Dictamen en relación con la consulta sobre el plazo durante el cual las entidades quedan obligadas a conservar la documentación relativa a las auditorías

Se presenta ante la Agencia Catalana de Protección de Datos un escrito en el que se solicita que la Agencia emita un dictamen sobre el plazo durante el cual las entidades quedan obligadas a conservar la documentación relativa a las auditorías.

[...]

I

[...]

II

Tal como expone la entidad que plantea la consulta, el artículo 96 del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, regula como obligación de los responsables de ficheros que tengan nivel medio o alto la necesidad de elaborar auditorías internas o externas, cada dos años o siempre que se lleven a cabo modificaciones sustanciales del sistema de información que puedan repercutir en las medidas de seguridad implantadas. El objetivo de dichas auditorías, de acuerdo con el apartado primero del artículo 96, es verificar el cumplimiento del Título VIII del Reglamento, dedicado a las medidas de seguridad:

> «1. 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.
>
> 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.»

En cuanto al contenido de la auditoría, de acuerdo con el apartado segundo de dicho artículo, deberá incluir, además de las conclusiones del auditor, que tienen que pronunciarse claramente sobre la adecuación de las medidas de seguridad efectivamente implantadas a lo establecido en el RLOPD, el detalle de las deficiencias detectadas y la propuesta de las medidas correctoras, así como todos aquellos datos, hechos y observaciones en que se base el auditor para dictaminar y recomendar. En principio, esta será la documentación a la que hay que entender que se refiere la consulta, es decir, toda la documentación que forma parte de la auditoría.

Aparte de esta información, de acuerdo con el apartado 3 del mismo artículo, hay que elaborar, por parte del responsable de seguridad, unas conclusiones que deben ser elevadas al responsable del fichero o tratamiento, a fin de que adopte las medidas adecuadas. Aunque, estrictamente, dichas conclusiones no forman parte de la auditoría, sí que son una consecuencia directa de la misma y están estrechamente vinculadas a ella, por lo que se considera que también hay que conservarlas en las mismas condiciones que los documentos que integran la auditoría.

De acuerdo con este mismo apartado tercero del artículo 96, el informe de auditoría debe quedar a disposición de la autoridad de control competente; en este caso, la Agencia Catalana de Protección de Datos.

III

Centrándonos ya en la cuestión planteada en la consulta, dado que ni el artículo 96 ni ninguna de las demás disposiciones vigentes en materia de protección de datos establecen de forma expresa el plazo durante el que hay que conservar la documentación que integra la auditoría, hay que determinar dicho plazo a partir del análisis de las obligaciones del responsable del fichero, y en especial del régimen de responsabilidades que le puede resultar aplicable.

Un primer criterio obvio, pero válido como punto de partida, puede ser que en la medida en que un informe de auditoría no es un documento aislado, sino que forma parte de un proceso continuado de implantación y evaluación de medidas de seguridad, se deberá conservar, como mínimo, hasta que exista un ulterior informe de auditoría, con independencia de que haya transcurrido el plazo de dos años desde que fue redactado. Ahora bien, como veremos a continuación, la existencia de un informe de auditoría posterior, ya sea por la auditoría bianual o por una modificación sustancial del sistema de información, no implica, sin más, que haya cesado la obligación de conservar el de la auditoría anterior.

Al margen de lo que diremos a continuación, desde un punto de vista estricto de auditoría, resulta coherente conservar toda la documentación de la auditoría mientras se mantenga un determinado sistema de información. Disponer de esta documentación puede aportar información valiosa a procesos de auditoría posteriores, a fin de seguir la evolución de las medidas de seguridad aplicadas. Y aún resulta más recomendable cuando se trata de ámbitos, como el sanitario, en que el ordenamiento vigente obliga a la conservación de determinada información —en concreto, la información que forma parte de la historia clínica— durante períodos de tiempo muy largos.

Pero más allá de esto, para determinar el plazo de conservación habrá que atenerse al régimen de responsabilidades establecido en la LOPD y en el resto del ordenamiento jurídico. En este sentido, el apartado tercero del artículo 96 exige que la documentación que forma parte de la auditoría esté a disposición de la autoridad de control. Y no solamente como un medio que permita aportar información sobre determinados incumplimientos, sino también, desde el punto de vista de la entidad responsable del fichero, como un medio para acreditar el cumplimiento de la normativa vigente.

Desde el punto de vista del régimen sancionador establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), la obligación de llevar a cabo las auditorías es una medida de seguridad, por lo que el hecho de no realizarlas puede ser sancionado como falta grave, a tenor de lo dispuesto en el artículo 44.3.h) de la LOPD. De acuerdo con el artículo 47.1 de la propia LOPD, el plazo de prescripción para las infracciones graves es de dos años; plazo de dos años que habría que contar desde la fecha en que se realiza la auditoría. Por consiguiente, este sería un primer plazo a tener en cuenta desde el punto de vista de las responsabilidades. Ahora bien, no se puede descartar que la auditoría, al igual que lo puede ser, por otros motivos, el registro de incidencias, pueda resultar un valioso elemento probatorio en la investigación de otros tipos de infracciones que tienen atribuido un plazo de prescripción más largo, como es el caso de la infracción

muy grave prevista en el artículo 44.4.f) de la LOPD, que tendría un plazo de prescripción de tres años.

Sin embargo, hay que hacer una aclaración, porque el plazo de conservación, en estos casos, no abarcaría solamente el plazo de prescripción, sino también el plazo necesario para la conclusión de los procedimientos sancionadores que se hayan podido incoar antes de que transcurra dicho plazo.

Pero el régimen de responsabilidades establecido en la LOPD no se agota con el régimen sancionador, sino que el artículo 19 de la LOPD también contempla la responsabilidad por daños o lesiones que las personas afectadas sufran en sus bienes o derechos, ya sea mediante la reclamación de la responsabilidad de la Administración, cuando el daño sea imputable a una Administración pública, o mediante el sistema de responsabilidad extracontractual establecido en el derecho civil. En este sentido, disponer de la documentación relativa a las auditorías puede ser un elemento probatorio importante para la acreditación de la diligencia del responsable en el cumplimiento de las medidas de seguridad exigibles. Al respecto hay que recordar que la letra d) del artículo 121-21 del Libro primero del Código Civil de Cataluña establece que prescriben a los tres años las pretensiones derivadas de responsabilidad extracontractual, y las demás pretensiones al cabo de diez años, salvo la recuperación de la posesión (artículos 121-20 y 121-22).

De acuerdo con las consideraciones efectuadas en estos fundamentos jurídicos en relación con la consulta planteada respecto al plazo durante el cual las entidades están obligadas a conservar la documentación relativa a las auditorías, se formulan las siguientes

Conclusiones

De acuerdo con la normativa de protección de datos, la documentación que forma parte de las auditorías de seguridad requeridas por dicha normativa debe conservarse durante un período mínimo de tres años, o hasta que se realice la auditoría de seguridad siguiente, si esta no se ha efectuado dentro del plazo de dos años exigible.

Al margen de ello, la conservación de dicha documentación puede resultar conveniente durante un plazo más extenso, a efectos de disponer de una información completa que permita evaluar la evolución de las medidas de seguridad aplicadas, así como a efectos de disponer de elementos probatorios del cumplimiento de la normativa vigente en materia de protección de datos, mientras no hayan prescrito las responsabilidades por los daños que se hayan podido ocasionar con el tratamiento de datos.