

LA AUDITORIA DE LA PROTECCIÓN DE DATOS

Jordi Verdaguer López
Abogado. Master en Derecho & TIC

La auditoría de seguridad a la que se debe someter los sistemas de información e instalaciones de tratamiento de datos, es una obligación legal que plantea no pocas cuestiones a los agentes involucrados en el tratamiento de datos de carácter personal.

Auditoría de seguridad

La auditoría de la protección de datos de carácter personal, que regula el artículo 17 del RMS, establece una obligación que no viene vinculada a la titularidad del fichero o tratamiento. La responsabilidad de efectuar la auditoría de seguridad recae tanto en la figura del responsable del fichero como en la del encargado del fichero. Un encargado de tratamiento muy habitual, las gestorías y asesorías laborales o fiscales, pueden ser sancionadas en caso de incumplimiento de esta obligación, con independencia de que efectúe el tratamiento por cuenta del responsable del fichero.

Referencias legales

La LOPD señala en su artículo 9.1 la obligación de cumplir una serie de medidas de seguridad:

“El responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.”

En el apartado tercero del mismo artículo se anuncia su desarrollo reglamentario:

“Reglamentariamente se establecerán los requisitos y condiciones que deben reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.”

El desarrollo reglamentario no se ha producido todavía con posterioridad a la entrada en vigor de la LOPD, por lo que en virtud de la Disposición Transitoria Tercera de la LOPD, continúa plenamente vigente el Reglamento de Medidas de Seguridad (RMS) aprobado por el RD 994/1999, que estaba pensado para la derogada LORTAD y cuyo ámbito de aplicación era exclusivamente los ficheros automatizados.

“Hasta tanto se lleven a efecto las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.”

Así el RMS dispone en su artículo 17.1 que:

“1.- Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años.”

Tendremos que tener en cuenta no sólo la verificación del Reglamento sino, además, **procedimientos e instrucciones** vigentes en materia de protección de datos. No hay que

olvidar que la AGEPD tiene competencias para dictar instrucciones y recomendaciones, como dispone el artículo 37 de la LOPD, en su apartado c):

“Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente ley.”

Por último, conviene hacer una referencia a lo dispuesto en la LOPD sobre la tipificación de las infracciones y, concretamente, a lo contenido en el artículo 44.3.h), que tipifica como infracción grave:

“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.”

Auditoría externa o interna

La auditoría puede ser interna o externa, el artículo 17 del RMS deja la elección a exclusivo criterio del obligado al cumplimiento de esta medida de seguridad, esto es, el responsable del fichero y el encargado del tratamiento.

La auditoría externa puede parecer, en principio, que aporta más garantías de independencia y objetividad que la interna. No obstante, si bien la visión del auditor interno puede pecar de una perspectiva poco objetiva, en cambio su conocimiento de la organización y su entorno es mayor.

Lo que tiene que primar en cualquier caso, con independencia de la opción escogida (auditoría interna o externa), es que el auditor verifique que se cumple con el Reglamento de Medidas de Seguridad, comprobando que las medidas propuestas en el Documento de Seguridad cumplen con el RMS y que a su vez éstas responden a la realidad.

Los plazos

La fecha límite para la implantación de las medidas de seguridad a los ficheros y tratamientos preexistentes era el 26 de junio de 2000, un año después de la entrada en vigor del RMS, por lo que todas aquellas entidades o personas obligadas a realizar la auditoría de seguridad tendrían que haber realizado su primera auditoría antes del 26 de junio de 2002, en la interpretación más favorable.

Ficheros de nueva creación

Para los ficheros de nueva creación, tendremos dos años desde su creación, teniendo en consideración que la notificación de la existencia del fichero o tratamiento es siempre previa a su creación. Una referencia clara para no inducir a error es realizar la auditoría a los dos años de la notificación del fichero o tratamiento.

Ficheros preexistentes

¿Qué sucede con los ficheros preexistentes y no notificados a la AGEPD? En este caso, y aunque nos consta que la AGEPD no viene imponiendo sanciones por la notificación tardía del fichero o tratamiento y admite la notificación sin más, lo más conveniente será realizar la auditoría lo antes posible sin contar el plazo de dos años desde la notificación del fichero o tratamiento.

Los sistemas de información

El alcance de la auditoría de protección de datos no viene dado en la propia redacción del artículo 7.1 del RMS:

“Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa...” Por tanto deberemos conocer qué entiende la normativa por “sistemas de información”.

Estos **sistemas de información** vienen definidos en el artículo 2.1 como el “conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal”.

Respecto al término **instalaciones**, se refiere a aquellas que contienen y complementan los sistemas de información, por ejemplo los locales e instalaciones donde están ubicados los sistemas de información que tratan los datos personales.

Los ficheros y tratamientos

La obligación de realizar la auditoría bianual viene señalada para aquellos ficheros o tratamientos cuyo nivel de seguridad viene indicado por lo dispuesto en los apartados 2, 3 y 4 del artículo 4 del RMS.

Nivel de seguridad	Datos objeto de tratamiento	Auditoría bianual
Básico	Cualquier dato de carácter personal.	NO
Básico superior	Conjunto de datos que permitan obtener una evaluación de la personalidad del individuo.	SÍ
Medio	Relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y servicios sobre solvencia patrimonial o de crédito.	SÍ
Alto	De ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin el consentimiento de las personas afectadas.	SÍ

El informe de auditoría

El informe de auditoría debe dictaminar sobre la adecuación de las medidas y controles al RMS, identificar las deficiencias y proponer las medidas correctoras o complementarias necesarias. También deberá incluir los datos, hechos y observaciones en que se basen los dictámenes y recomendaciones propuestas.

El análisis del informe de auditoría le corresponde al Responsable de seguridad, quien deberá elevar las conclusiones al Responsable del fichero para que adopte las medidas adecuadas.

El informe de auditoría deberá estar siempre a disposición de la AGEPD. Esto no quiere decir que se tenga que notificar su puesta a disposición a la Agencia, sencillamente habrá de "existir" y estar a disposición de la AGEPD cuando así lo requiera o se persone en los locales del Responsable del Fichero y solicite su exhibición y consulta.

Normativa aplicada

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 994/1999 de Medidas de Seguridad (RMS).