

PROTECCIÓN DE DATOS PERSONALES - REVISORES FISCALES

Para analizar el deber legal que corresponde a las empresas o personas naturales que prestan servicios de revisoría fiscal de incluir dentro del informe de las auditorías que ejecutan en las empresas (clientes) el cumplimiento del marco legal en Protección de Datos Personales, es necesario señalar tres aspectos importantes: en primer lugar, la definición de contador público y sus facultades dentro de una organización, en segundo lugar, el deber de reportar en el informe de auditoría el cumplimiento de las políticas y normas internas de la compañía que auditan y en tercer lugar, el ámbito de aplicación de la Ley 1581 de 2012 y decretos reglamentarios.

En primer lugar, es importante precisar que la actividad de revisoría fiscal sólo puede ser ejercida por personas que se encuentren inscritas como contadores públicos ante la Junta Central de Contadores, unidad administrativa especial adscrita al Ministerio de Comercio, Industria y Turismo. Las normas que regulan la materia se encuentran especialmente señaladas en el Código de Comercio, dentro del libro dedicado a las sociedades comerciales, y en la Ley 43 de 1990, mediante la cual se reglamenta la profesión de Contador. Ley que fue reglamentada mediante los decretos 1235 de 1991 y 1510 de 1998, la Orientación Profesional No. 5 de 2003 Consejo Técnico de la Contaduría, Resolución 160 de 2004 Junta Central de Contadores, entre otras normas.

De la Ley 43 de 1990, es necesario citar el artículo 1 donde define al contador público como la persona natural, que mediante la inscripción que acredite su competencia profesional, está facultada para dar fe pública de hechos propios del ámbito de su profesión, dictaminar sobre estados financieros, realizar las demás actividades relacionadas con la ciencia contable en general. En concordancia con lo anterior, el artículo 2 de la misma norma señala las actividades relacionadas con la ciencia contable, las cuales, en general, son todas aquellas que implican organización, revisión y control de contabilidades, certificaciones y dictámenes sobre estados financieros, certificaciones que se expidan con fundamento en libros de contabilidad, revisoría fiscal, prestación de servicios de auditoría, así como todas aquellas actividades conexas con la naturaleza de la función profesional de Contador Público, tales como : la asesoría tributaria, la asesoría gerencial, en aspectos contables y similares.

En segundo lugar, la revisoría fiscal implica un servicio integral cuyo énfasis se centra en validar las cifras de los Estados Financieros, verificar los controles de la compañía, administrar riesgos y sistemas de información, **y hacer un barrido del cumplimiento de las normas legales de la empresa auditada**. Si bien es cierto, la labor se concentra en los ciclos de negocios de la compañía como los ingresos, inventarios y tesorería, entre otros; es necesario señalar que la revisoría fiscal incluye además auditoría sobre el cumplimiento de las políticas y normas internas de la compañía como parte del fortalecimiento del sistema de control interno, como se había mencionado. De modo que, el marco legal en protección de datos hace parte de esas políticas y normas internas que deben ser auditadas y, por lo tanto, es un deber del revisor fiscal señalar en su informe de auditoría su cumplimiento.

En este sentido, la auditoría de cumplimiento que realiza el revisor fiscal incluye la comprobación o evaluación de las operaciones no solo en materia financiera, también administrativas, económicas, entre otras, como es el caso de dar fe del cumplimiento del marco legal en protección de datos. Ello

con la finalidad de establecer que estas operaciones se han realizado conforme a las normas legales, estatutarias y si los procedimientos utilizados y las medidas de control interno están de acuerdo con las normas que le son aplicables.

En concordancia con lo anterior, la Superintendencia de Industria y Comercio – SIC- a través de la Guía de Responsabilidad Demostrada estableció la responsabilidad de presentar informes respecto del seguimiento y ejecución del marco legal en protección de datos mediante mecanismos internos. Igualmente, el deber de implementar planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de datos y señalar el procedimiento a seguir en caso de que se presenten violaciones a sus códigos de seguridad o detecten riesgos en la administración de la información de los Titulares.

También señala la creación del material que sustente la implementación de un Programa Integral de Gestión de Datos Personales, el cual, debe incluirse dentro de la información que es enviada a los accionistas o socios, con el fin de mantenerlos plenamente informados, teniendo en cuenta los siguientes criterios:

1. Definir de manera clara la estructura de la generación de reportes. Esto implica saber qué empleado genera qué tipo de reporte, para asignar responsabilidades claras en el evento de una queja o de una violación a los códigos de seguridad.
2. Documentar el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.
3. Generar reportes para los accionistas o socios de manera periódica, e informar en estos el estado del programa de protección de datos personales.

En tercer lugar, respecto de la obligación de implementar el marco legal en materia de protección de datos personales el artículo 2 de la Ley 1581 de 2012, señala éste deber a las personas naturales o jurídicas, tanto públicas como privadas que registren datos personales en cualquier base de datos que los haga susceptibles de tratamiento, indicando las siguientes excepciones:

Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley [1266](#) de 2008;

f) A las bases de datos y archivos regulados por la Ley [79](#) de 1993. (Resaltos fuera de texto)

Así las cosas, todo registro de datos personales en una base de datos implica recolección, almacenamiento y tratamiento, aspectos que gozan de especial protección constitucional, esto es, se deben garantizar derechos fundamentales de los titulares de los datos que contengan las bases de datos. Por lo tanto, el ordenamiento jurídico establece como un deber legal del Responsable del tratamiento (persona natural o Jurídica) aplicar políticas y prácticas que garanticen los principios fundamentales de la protección de datos personales en desarrollo de las funciones que le sean asignadas en la ley o en los reglamentos.

Al respecto, el numeral 1.1 de la Guía de Responsabilidad Demostrada señala que, para lograr estos objetivos, la alta dirección debe (i) designar a la persona o al área que asumirá la función de protección de datos dentro de la organización, (ii) aprobar y monitorear el Programa Integral de Gestión de Datos Personales, y (iii) informar de manera periódica a los órganos directivos sobre su ejecución. Adicional a ello, señala la importancia de destinar recursos suficientes que le permitan al área o persona encargada diseñar e implementar un programa que se ajuste a la realidad de la organización, como también que, a través de esa persona o área, se establezcan responsabilidades específicas para otras áreas de la organización respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan.

Es importante tener en cuenta que, por tratarse de derechos fundamentales que deben ser garantizados por el Responsable, es necesario y de obligatorio cumplimiento la solicitud de autorización de que trata el artículo 9° de la Ley 1581 de 2012, siendo entonces un deber de los Responsables del Tratamiento de datos personales el establecer unos mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 de del Decreto 1377 de 2013. Para ello, el artículo 7 del Decreto 1377 de 2013, faculta a los responsables para que a través de medios técnicos que faciliten al Titular su manifestación automatizada se obtenga dicha autorización, que podrá efectuarse: (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

Dichas autorizaciones deben contar con el lleno de los requisitos establecidos en la ley, que, para el efecto, el artículo 5 del Decreto Reglamentario 1377 de 2013, señala la obligación de quien recoge los datos personales de informar al titular las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento. Adicionalmente, como se había mencionado el artículo 7 de la misma norma señala que la autorización debe obtenerse mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

Finalmente, es necesario reiterar la obligatoriedad de los revisores fiscales de reportar en sus informes de auditoría el cumplimiento del marco legal en protección de datos, esto es, Ley 1581 de 2015, decretos reglamentarios y la Circular No. 002 de 2015 emitida por la Superintendencia de Industria y comercio. Se trata de una responsabilidad propia del profesional en contaduría pública e inherente a su función no omitir la verificación del cumplimiento de la implementación de la Ley 1581 de 2012 en los dictámenes o informes de las empresas que audita.