Información Importante

La Universidad Santo Tomás, informa que el(los) autor(es) ha(n) autorizado a usuarios internos y externos de la institución a consultar el contenido de este documento a través del Catálogo en línea de la Biblioteca y el Repositorio Institucional en la página Web de la Biblioteca, así como en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

Se permite la consulta a los usuarios interesados en el contenido de este documento, para todos los usos que tengan finalidad académica, nunca para usos comerciales, siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de grado y a su autor.

De conformidad con lo establecido en el Artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, la Universidad Santo Tomás informa que “los derechos morales sobre documento son propiedad de los autores, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.”

Bibliotecas Bucaramanga

Universidad Santo Tomás

**Lineamientos para el Aseguramiento de la Protección de bases de datos personales desde
las Empresas**

Maria Teresa González Carvajal

**Trabajo de grado para optar el título de Especialista en Revisoría Fiscal y Auditoría
Externa**

Directora

Doctora Lennix Farley Vega Sepúlveda

**Coordinadora Especialización en Finanzas públicas Docente Facultad de Economía
Universidad Santo Tomás**

Universidad Santo Tomás, Bucaramanga

Posgrados División Ciencias Económicas y Administrativas

Contaduría Pública

2016

Contenido

	Pág.
Introducción	10
1. Objetivos	11
1.1 Objetivo General	11
1.2 Objetivos Específicos.....	11
2. Justificación	12
3. Antecedentes Mundiales	14
4. Normas Importantes en la Protección de Datos Personales en Colombia	17
5. Análisis casos críticos sobre protección de datos	21
5.1 Caso Colmédica Medicina Prepagada S.A. - 2016	21
5.2 Caso María Salomé Sánchez Monsalve - 2015	24
6. Lineamientos que orienten a las organizaciones en el cumplimiento de la norma sobre protección y aseguramiento en el tratamiento de datos personales.	31
6.1 Lineamientos generales para el tratamiento de los datos ingreso, dado de baja, autorización, y solicitudes SIC.....	31
6.1.1 Autorización para el tratamiento de la información.....	31
6.1.2 Realizar auditoria, monitorio o revisión periódica de las bases de datos por lo menos una vez al año para garantizar el cumplimiento de la norma en protección de datos personales.	35
6.1.3 Establecer seguridad de la información.....	36
6.2 Lineamientos para administración y reporte de base de datos ante la Superintendencia de Industria y comercio - SIC.....	37
6.3 Lineamientos para la operación en los diferentes procesos internos de las empresas que pueden ayudar a desarrollar las políticas, procedimientos e instructivos internos.....	38
6.3.1 Procesos con Personal – áreas de Talento Humano o la Administración	44

6.3.2 Procesos de Clientes – áreas Comercial, Cartera, Mercadeo, Administración o Gerencia General	47
6.3.3 Procesos con Proveedores – áreas Compras, Administración o toda la organización cuando desde cualquier área se tiene contacto con proveedores.	53
6.3.4 General para las empresas	55
6.4 Principios claves a tener en cuenta:	56
7. Importancia del manejo de datos y la seguridad de información en la Revisoría Fiscal y Auditoría Externa.....	57
8. Conclusiones	59
Bibliografía	61

Lista de Figuras

	Pág.
<i>Figura 1.</i> Línea tiempo antecedentes mundiales	16
<i>Figura 2.</i> Sanciones de datos personales	27
<i>Figura 3.</i> Principales empresas sancionadas en materia de datos personales.....	28
<i>Figura 4.</i> Motivo de sanción en materia de Datos Personales	30

Lista de Tablas

	Pág.
Tabla 1. <i>Diferencias entre la Ley 1266 de 2008 y la Ley 1581 de 2012</i>	18
Tabla 2. <i>Empresas sancionadas por la Delegatura para la Protección de Datos Personales</i>	29
Tabla 3. <i>Motivo de sanción en materia de Datos Personales</i>	30
Tabla 4. <i>Diferencia entre datos sensibles y dato no sensibles</i>	32
Tabla 5. <i>Matriz de riesgos</i>	39
Tabla 6. <i>Definición para calificar la frecuencia</i>	41
Tabla 7. <i>Definición para calificar el impacto</i>	42
Tabla 8. <i>Calificación y control propuesto para los riesgos en el proceso de selección y reclutamiento</i>	44
Tabla 9. <i>Calificación y control propuesto para los riesgos en el proceso de contratación empleados</i>	45
Tabla 10. <i>Calificación y control propuesto para los riesgos en el proceso de afiliación clientes sistema de información para venta</i>	47
Tabla 11. <i>Calificación y control propuesto para los riesgos en el proceso de tele mercadeo o envío de correo con publicidad o información general de su cuenta</i>	48
Tabla 12. <i>Calificación y control propuesto para los riesgos en el proceso de crédito y manejo de cartera</i>	51
Tabla 13. <i>Calificación y control propuesto para los riesgos en el proceso de creación de proveedores sistema de información para compra de productos o prestación de servicios</i>	53
Tabla 14. <i>Calificación y control propuesto para los riesgos estratégicos</i>	55

Glosario

RNBD: Registro nacional de base de datos – Superintendencia de Industria y comercio; es el Directorio público de las bases de datos con información personal sujetas a Tratamiento que operan en el país.

SIC: Autoridad de Protección de Datos designada por la ley 1581 de 2012, para garantizar que en el tratamiento de esos datos se respeten los principios, derechos, garantías y procedimientos dispuestos en la ley y le atribuyó la administración del RNBD.

TERCEROS: Clientes, proveedores, prestadores de servicios y empleados

INTIMAD: Derecho a que la persona pueda reservar para sí, y decide con quién los comparte.

HABEAS DATA: Derecho al buen nombre, implica la capacidad para correr el riesgo de jugar con el buen nombre de las personas; no se puede realizar cierto tipo de conductas que afecte el buen nombre de las personas. (Derecho habeas data se reconoció en 95, está desde 1991 en la constitución).

La Corte Constitucional lo definió como el derecho que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales. Asimismo, ha señalado que este

derecho tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información.

VIOLACIÓN DERECHO HABEAS DATA: Cuando la información contenida en el archivo o base de datos es recogida de manera ilegal, sin el consentimiento del titular del dato, es errónea o recae, sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente.

DATO PERSONAL: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que pueden asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de dicha ley. Cuando en la misma ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados.

Según la corte constitucional “Los datos serán públicos cuando la ley o la Constitución así lo establezcan, y cuando no sean de aquellos clasificados como semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas y los relativos al estado civil de las personas.”

DATO PÚBLICO Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la Ley de Hábeas Data. Son públicos, entre otros los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

DATO SEMIPRIVADO Es semiprivado el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de

actividad comercial o de servicios (la Corte Constitucional precisa en la Sentencia C--1011 de 2008 que este tipo de datos requieren de autorización previa del titular para ser reportados a las bases de datos y circular en los términos previstos en la ley en comento).

DATO PRIVADO Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular.

DATO SENSIBLE Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

SUJETO ACTIVOS: Toda persona física o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado.

SUJETO PASIVOS: Es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales.

Introducción

Existe una exposición de las empresas a recibir sanciones por parte de la delegataria encargada de la Protección de Datos Personales de la Superintendencia de Industria y Comercio, por contravenciones a las normas de protección de datos financiero y contravención a la ley general de protección de datos, por desconocimiento de la norma o no saber cómo aplicarla en sus empresas.

Durante el desarrollo de este trabajo se detalla un análisis de las normas aplicables al tratamiento de datos, las sanciones económicas que se han impuesto en los últimos años, algunos casos relacionados y como resultado lineamientos enfocados para los diferentes procesos que interactúan con terceros desde cualquier empresa para su aplicación con el fin de disminuir el riesgo al incumplimiento de las normas relacionadas.

1. Objetivos

1.1 Objetivo General

Generar lineamientos para la aplicación de la norma de protección de datos personales para garantizar la integridad, disponibilidad y confidencialidad de la información recibida de terceros dentro de las organizaciones.

1.2 Objetivos Específicos

- Analizar las normas, los requerimientos y consideraciones generales sobre la protección de datos, así como enfoques y estudios en relación con el tema.
- Analizar casos críticos sobre protección de datos desde la jurisprudencia y la práctica empresarial.
- Establecer Lineamientos que orienten a las organizaciones en el cumplimiento de la norma sobre protección y aseguramiento en el tratamiento de datos personales.

2. Justificación

Antes de la promulgación de la Ley 1266 de 2008 los datos personales de los clientes eran intercambiados por las diferentes entidades financieras o empresas para ofrecer servicios o productos a clientes nuevos con el fin de aumentar los ingresos, las personas se veían afectadas cuando se reportaba en las diferentes centrales de riesgos los clientes morosos tanto en el sector financiero como en el sector real, perjudicando la vida crediticia de las personas, basados en información errónea, o por un error en los datos, en muchas ocasiones las obligaciones se encontraban saldadas, ocasionando incomodidad en los clientes al perder posibilidades de acceder a obligaciones nuevas e incluso para acceder a un empleo.

Esta situación se daba cuando algunas empresas hacían un uso indebido de la información de sus titulares, negociando el contenido de sus bases de datos a otras empresas para poder promocionar sus productos o servicios sin la autorización de sus titulares. Con la aparición de la ley 1266 se regula el manejo de la información contenida en bases de datos personales especialmente la financiera, crediticia, comercial y de servicios; beneficiando de esta manera a empresarios, accionistas y los terceros que principalmente eran afectados por el mal uso de sus datos personales, esta ley permite además la exclusión o borrón de la información negativa en las centrales de riesgo, es decir de la información relativa a la mora en el pago de las cuotas u obligaciones, y excluyendo de su historial apenas trascurra un año de permanencia en las centrales, contado desde la fecha de pago o rectificando los errores reportados.

En el año 2012 con la promulgación de la Ley 1581 se estableció el régimen general de protección de datos personales que busca que los titulares de información ejerzan su derecho constitucional a conocer, actualizar, rectificar y suprimir los datos personales almacenados en bases de datos y archivos, mediante las consultas, reclamos y quejas ante la Superintendencia, reglamentada por el decreto 1377 en el año 2013 que establece los procedimientos para la protección de datos personales; faculta al Estado para controlar las entidades en la administración de las bases de datos.

El incumplimiento y no implementación de estas normas puede acarrear en sanciones hasta \$1.179 millones; con el fin de no incurrir en estas sanciones, este trabajo busca ayudar a las empresas a dar un buen manejo de la información de terceros con un análisis de riesgos y la creación de unos lineamientos que ayuden a dar cumplimiento a las regulaciones existentes en materia de manejo de datos.

3. Antecedentes Mundiales

Dos jóvenes abogados de Boston Samuel D. Warren y Louis D. Brandeis, en la revista Harvard Law Review (vol. IV, núm. 5, 15 de diciembre de 1890, págs. 194-220) publicaron el ensayo “The Right To Privacy”, alarmados ante el inicio de la prensa sensacionalista (que incluye titulares con fotografías, información detallada acerca de accidentes, crímenes, adulterios y enredos políticos), insistieron el reconocimiento del derecho de la persona a oponerse a toda intromisión a su vida privada; convirtiéndose en la génesis de la protección de la privacidad en el sistema constitucional norteamericano, buscando un sistema jurídico que reconociera este derecho; publicación referida como defensa en varias demandas contra el derecho a la privacidad en algunos casos fallando a favor y en otros desechando el mismo por no considerarse como ley.

El 10 de Diciembre de 1948 en París la Asamblea General presidida por varios países impulsada por Eleanor Roosevelt, aprobó la Declaración Universal de los derechos humanos, que en su Artículo 12 “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

El primer trabajo desarrollado por el consejo de Europa en la resolución 509 de 1968 de la Asamblea del Consejo de Europa relativa a “Los derechos humanos y los nuevos logros científicos y técnicos”, buscando la necesidad de buscar medidas de protección a los derechos humanos que se pueden afectar por el uso de la TIC.

En Alemania fue aprobada la primera ley de protección de datos (Datenschutz) en el estado de Hesse en Alemania, posteriormente en 1977, el Parlamento Federal Alemán aprueba una Ley Federal que impide la transmisión de cualquier dato personal sin la autorización de la persona interesada.

En 1981 se firma el primer convenio internacional de protección de datos (convenio 108) por Alemania, Francia, Dinamarca, Austria y Luxemburgo, que establece Principios, derechos y obligaciones de los responsables para el tratamiento de información con respecto al tratamiento automatizado de datos de carácter personal.

El tribunal constitucional federal alemán, denominó por primera vez en su sentencia del 15 de diciembre de 1983 como respuesta a la posibilidad del tratamiento masivo de datos, el derecho a la protección de datos personales, en la defensa de los derechos de la persona a preservar y proteger su vida privada.

En 1995 se aprueba la Directiva 95/46/CE del parlamento Europeo y del consejo, garantizando los derechos y libertades de las personas físicas creando un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea

El 23 de septiembre de 1980

La Comisión Europea pone en marcha el Privacy Shield - Escudo de la privacidad entre Estados Unidos y la unión Europea el 12 de Julio de 2016; protege los derechos fundamentales de cualquier persona en la Unión Europea cuyos datos personales se transfieran a los Estados Unidos y aporta claridad jurídica para las empresas que dependen de transferencias transatlánticas de datos.

Figura 1. Línea tiempo antecedentes mundiales

4. Normas Importantes en la Protección de Datos Personales en Colombia

Siguiendo como referente de la Declaración Universal de Derechos Humanos (1948) en su artículo 12, se redactó el Artículo 15 de la Constitución Política de Colombia 1991, es el inicio del derecho a la intimidad utilizado en diferentes acciones de tutela, desprendiéndose de este dos derechos adicionales el derecho al buen nombre y el derecho habeas data lo cual influyó en las diferentes normas en materia de protección de datos personales en Colombia; en 2008 reglamentó la Ley Estatutaria 1266 como un medio idóneo para lograr la efectividad del derecho constitucional consagrado en el artículo 15 de la Constitución Política de Colombia, como marco claro sobre la protección de datos personales buscando el desarrollo de la personalidad, autodeterminación, al tratamiento de datos, a la actualización y rectificación de los datos, entre otros a la libertad personal requiriendo las disposiciones generales de esta ley que regula estándares básicos sobre el manejo de información contenida en bases de datos personales en el sector financiero y comercial, beneficiando en parte a las personas en su derecho a conocer sus reportes, incluso para quienes durante la crisis de los 90 presentaron mora en sus obligaciones financieras, que luego de varios años de realizar el pago definitivo de estas aún se encontraban reportadas en las centrales de riesgo o entidades crediticias, permitiendo un tiempo máximo de 4 años de permanencia desde su pago en mora, según el artículo 13, con el fin de acceder a nuevas obligaciones con el sector financiero o real; en esta misma ley en su artículo 12 establece que sólo procederá el reporte negativo ante las centrales de riesgo si se cuenta con los soportes de la comunicación ante el tercero (persona) a reportar 20 días antes del reporte, para que este pueda

demostrar o realizar su pago, el incumplimiento a la presente ley permitirá a la superintendencia de industria y comercio y la superintendencia financiera imponer multas hasta de 1.500 SMMLV, hasta la suspensión de las actividades del banco de datos; posteriormente se evidencia que esta ley se orientó a un tipo de datos específico y no a la protección general de todos los datos y es por esto que se reglamentó la Ley 1581 de 2012, que establece disposiciones generales, determina un obligatorio seguimiento y cumplimiento de los principios que la ley describe para todo tipo de datos; destacando a continuación la diferencia con respecto a la ley 1266 de 2008:

Tabla 1. *Diferencias entre la Ley 1266 de 2008 y la Ley 1581 de 2012*

ley 1266 de 2008	Ley 1581 de 2012
Protege datos de personas naturales y jurídicas	Protege solo personas naturales
Protege información financiera	Protege un marco general
hacía énfasis exclusivamente en la protección de datos de carácter financiero y comercial, reportados en las llamadas centrales de riesgo	Aplicable a todas las bases de datos de entidades públicas y privadas que almacenen y utilicen datos personales.
Sigue vigente para los datos personales financieros, crediticios, comerciales y de servicios registrados en un banco de datos.	

La Ley 1581 de 2012 establece el marco general para todas las bases de datos de entidades públicas y privadas que almacenen o utilicen datos personales, quienes deberán establecer políticas internas de manejo de datos personales, procedimientos para la atención de consultas y reclamos, así como ajustar procesos y procedimientos en la aplicación de esta norma; reconociendo cómo se produce el flujo de información en sus procesos y actividades, identificando los procesos de obtención, por creación o captura, transformar, usar, almacenar,

transferir, circular, compartir, eliminar o archivar hasta la disposición final de los datos, esto conocido como el ciclo de vida del dato. Respetando el derecho de las personas a conocer la información que sobre ellas está recogida en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información y el derecho a incluir nuevos datos con el fin de que se provea una imagen completa al titular; el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos, de tal manera que concuerde con la realidad; el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular.

La ley en mención establece principios para en el tratamiento por parte de las empresas de los datos cualquiera que sea su finalidad, protegiendo los datos de menores de edad y dando importancia en establecer las medidas de seguridad de las bases de datos automatizadas y no automatizadas que contengan datos de carácter personal, distinguiendo los niveles de seguridad, partiendo de la naturaleza de la información; cualquier asociación empresa o entidad que trate datos de carácter personal tiene la obligación cumplir lo establecido, el incumplimiento de estas obligaciones puede ser sancionado por la superintendencia de industria y comercio con importes hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción, Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó, puede llegar hasta el cierre temporal o definitivo de la operación que involucre tratamiento de datos sensibles.

En conjunto con el decreto 1377 de 2012, que reglamentó parcialmente la ley de protección de base de datos, empieza a desarrollarse el sistema completo en Colombia, que empieza a con la orientación del estado actual de los datos personales y su tratamiento automatizado o no, buscando un repositorio nacional central de las bases de datos sujetas a

tratamiento que operan el país y será administrado por la Superintendencia de Industria y Comercio, su principal uso como herramienta de supervisión, monitoreo de los sujetos pasivos obligados y que le permitirá el acceso a la información de los titulares.

El Decreto 886 de 2014 reglamentó el artículo 25 de la Ley 1581 de 2012 y estableció la información mínima que debe contener el Registro, donde el Objetivo principal del RNBD (Registro Nacional de Base de Datos) es contar con un directorio público de las bases de datos personales sujetas a tratamiento que operan en el país, cuya administración está a cargo de la Superintendencia de Industria y Comercio; con el fin de garantizar y proteger el tratamiento de los datos personales de los terceros que tiene algún vínculo con la organización, así como cumplir con los derechos fundamentales de las personas y especialmente de su honor e intimidad personal y familiar, y será de libre consulta para los ciudadanos.

5. Análisis casos críticos sobre protección de datos

Antes de abordar y enumerar los casos críticos se hace énfasis en la importancia del cumplimiento de la norma para no incurrir en sanciones por desconocimiento de los posibles riesgos que se puedan presentar en el transcurso de las operaciones de las empresas, es por eso que al intentar llevar un registro caso por caso se puede notar en orden de relevancia en que son descritos su incumplimiento a la norma; destacando el primero en incurrir con la multa más alta hasta el momento en Colombia. En la mayoría de los casos y muy a pesar que las multas pueden ser considerables, lo que se quiere es demostrar la responsabilidad que se tiene con el tratamiento de los datos personales.

5.1 Caso Colmédica Medicina Prepagada S.A. - 2016

El pasado mes de Junio de 2016, la Delegatura para la Protección de Datos Personales la Superintendencia de Industria y Comercio, impuso multa de más de Mil millones de Pesos, en materia de protección de datos personales a la empresa COLMÉDICA MEDICINA PREPAGADA S.A., que ascienden a 1.500 SMMLV, siendo la multa más alta hasta la fecha por no proteger la información de sus pacientes, castigando la falta de diligencia y la inobservancia del deber de informar al ente supervisor sobre la ocurrencia de una brecha de seguridad que expuso información sensible por internet. (Marrugo Jimenez Ivan Dario, 2016, Párr.# 20).

COLMÉDICA no había tomado las medidas de seguridad adecuadas para su aplicación de consultas médicas por medio de la página WEB de COLMÉDICA (atención en línea), al no deshabilitar el ingreso anónimo de sharepoint best doctors; incidente de seguridad que comprometió los datos personales de 30 titulares poniendo en riesgo los mismos, situación que debió ser informada en su momento por Colmedica a la Superintendencia, se limitó a resolver un caso dejando de lado los 29 titulares, dando solución inmediata a la señora que demandó, asignándole usuario y clave sin revisar detalladamente los demás usuarios (29) que incluían tres menores de Edad exponiendo sus datos personales sin control a partir del cache Google, así mismo no informó a la SIC cometiendo con esto infracción del literal n) art 17 de la ley 1581; Colmedica no conservó las medidas que se requieren hacer parte de las categorías especiales de los datos, no existe justificación válida para no haber conservado la información personal de los 30 casos y más de los 3 casos de menores de edad, bajo las medidas de seguridad que demandaban, No hay lugar a dudas para la entidad de la dimensión del daño que efectivamente se materializó en el caso en cuestión al divulgarse información sensible en un medio de comunicación masiva, por cuanto es evidente que los intereses tutelados por ley estatutaria de protección de datos, fueron vulnerados incumpliendo lo dispuesto en el literal d) art 17 y literales f y g del art 4 de la ley 1581 del 2012 (Marrugo Jimenez Ivan Dario, 2016, Párr.# 14-19).

La forma en que se dio cuenta Colmedica de este error fue que uno de los pacientes digitó su nombre en un motor de búsqueda www.colmedica.com – consulta best doctors, cuando le arrojó como resultado, la información que había suministrado en dicho portal para su consulta médica, además, aparecía divulgados los datos como nombre y apellido, cédula, dirección de residencia, correo electrónico, género, fecha de nacimiento, una descripción de la consulta formulada por el usuario del servicio en la que hace relación a su estado de salud actual

indicando las patologías que padece; diagnósticos y reportes de exámenes médicos en general y estado de la solicitud. La Superintendencia pudo comprobar que este hecho no había sucedido solo con un paciente, sino con unas treinta personas más, los cuales tenían expuesto todo tipo de información personal, encontrando tres casos de forma aleatoria, que hacía relación a información personal de salud de menores, sin restricciones. (Marrugo Jimenez Ivan Dario, 2016, Párr.# 5)

Colmedia apenas tuvo conocimiento de la queja, implementó una medida de seguridad para el ingreso a su portal utilizando usuario y contraseña, en desarrollo de la etapa preliminar, la superintendencia por medio de su laboratorio de informática forense realizo una prueba ingresando a internet (motor de búsqueda) y digitando en google el nombre de la persona que interpuso la queja, en su primer intento, efectivamente se encontró que para acceder a la información era necesario digitar usuario y contraseña, pero en su segundo intento, utilizando la opción EN CACHE del motor de búsqueda de google, encontró que tal y como había manifestado el usuario, antes no existía una medida de control de acceso y el ingreso era directo y sin ningún tipo de restricción (Marrugo Jimenez Ivan Dario, 2016, Párr.# 4).

Colmedica no garantizó a los titulares de los datos el pleno y efectivo ejercicio al derecho de hábeas data, al no conservar la información en condiciones de seguridad, permitiendo el acceso no autorizado de cualquier persona, infringiendo los principios consagrados en el artículo 4 de la Ley 1581 de 2012.

Colmedica ya implementó las medidas de seguridad correspondiente para todos los usuarios mencionados en esta sanción, no obstante este hecho afectó reputacionalmente a la EPS, lo cual se puede ver afectado por la confianza de los afiliados, provocando deserción de los mismos a esta EPS o Servicio que representa agilidad y oportunidad para las persona. En este

caso se puede observar que por implementar un nuevo servicio que ante el auge de la tecnología prometía estar acorde a ella, no se realizó la medición de los riesgos que podían ser implícitos de la nueva operación o que son inherentes a la misma, verificando temas de seguridad, confiabilidad para proteger los datos personales, bajo un adecuado uso de la información, este fue el primer error de Colmedica.

El segundo Error fue no informar a la Superintendencia de Industria y Comercio (SIC) del caso presentado por falta de controles en la seguridad de información y que a su vez no fue el único caso, en total fueron 30 casos incluyen 3 menores de edad.

Por lo anterior se impuso la multa más alta en materia de protección de datos personales en Colombia.

5.2 Caso María Salomé Sánchez Monsalve - 2015

En Octubre de 2015 La Delegatura para la Protección de Datos Personales la Superintendencia de Industria y Comercio (SIC), ordenó a la sociedad GEOSTIGMA MEDIA S.A.S. que bloquee la información personal de la señora MARÍA SALOMÉ SÁNCHEZ MONSALVE, contenida en el sitio web www.plagiosos.org para proteger su derecho de hábeas data, teniendo en cuenta que no se le garantizó a la titular el derecho de acceso, corrección, actualización o supresión de los datos personales divulgados en ese portal Web e indexados por el motor de búsqueda Google, los cuales se refieren al presunto plagio realizado en su trabajo de tesis de grado, contra la decisión no proceden recursos. (Superintendencia de Industria y Comercio, 2015)

El episodio, que comenzó como un incidente pequeño, terminó dominando su vida. “Durante mucho tiempo estuve escondida y negando la cosa, porque no lo podía entender. Estaba asustada, intimidada y como perseguida”, le contó la afecta a ENTER.CO. (ENTER.CO)

Todo inicio con el envío de un correo anónimo a la Universidad acusando a MARÍA SALOMÉ SÁNCHEZ MONSALVE de plagio en su tesis de pregrado ante la facultad de Filosofía de la Universidad Javeriana; quienes no hicieron caso de esto, razón por la cual un troll al no recibir respuesta envió el caso a Plagiosos escalando sus acusaciones al aparecer comentarios en sitios de noticias y blogs, en los que la mencionaban con nombre y apellido y enlazaban al sitio. Incluso, su firma y su número de cédula de ciudadanía aparecen en las imágenes de Google cuando se busca su nombre (ENTER.CO).

María Salomé duró más de un año intentando evitar el tema que la asustaba, además, que quien hacía los comentarios sabía mucho sobre su vida.

Este hecho adicional al daño psicológico que recibió MARIA le impidió acceder a un empleo “...no te podemos contratar, no porque dudemos de ti, sino porque eres un riesgo para la comunidad académica y para los estudiantes, porque si quieren atacarte físicamente, si quieren lanzarte un ácido o algo, no podemos poner en riesgo a la comunidad educativa por ti”, asegura que le dijeron; razón por la cual decidió perder el miedo, reunir fuerza y dignidad para enfrentar la situación como lo que era: como un acoso, solicitando a Google desindexara el sitio en el que aparecía la acusación, sin recibir respuesta a las solicitudes que hizo a través del formulario estándar del buscador para esa clase de casos, luego entabló una queja ante la Superintendencia de Industria y Comercio (SIC) contra Plagiosos, pues consideraba que el sitio violaba el derecho a la protección de sus datos personales por lo cual la SIC consideró que Plagiosos “no ha

dispuesto un canal o medio para que [María Salomé] ejerza sus derechos de acceso, corrección, actualización o supresión de los datos personales divulgados” en el sitio, y ordenó su bloqueo.

Lo que sigue para María Salomé es explorar la posibilidad de entablar una demanda penal por injuria y calumnia contra Plagiosos. Ella espera que, “a partir de que se haga público esto, se paren todos los comentarios que han dañado la imagen, que han sido demasiados” (ENTER.CO).

Este caso no se impuso una sanción por que no es posible identificar el responsable que actuó con mala fe para dañar la reputación de la señora MARÍA SALOMÉ SÁNCHEZ MONSALVE; donde un anónimo denunció plagio en la tesis de grado de la señora Maria, afectando considerablemente su vida personal hasta el punto que MARÍA no le daban trabajo por esta denuncia, sin embargo lo único que pudo hacer la Superintendencia de Industria y Comercio fue ordenar a la página dónde llegó la denuncia anónima fue eliminarla y no dejar rastro.

Después de revisar estos casos puntuales en materia de protección de datos personales, se relaciona a continuación informe de sanciones de la Superintendencia de Industria y comercio para ilustrar aún más, los efectos al no realizar un adecuado uso de los datos personales de los diferentes terceros, con el fin de buscar cumplimiento de la protección de datos personales.

Para el primer semestre del 2014, la Delegatura encargada de la Protección de Datos Personales de la Superintendencia de Industria y Comercio, impuso en primera instancia 19 sanciones en esta materia por la suma de \$ 686.224.000 millones de pesos (SIC).

A la fecha es posible que alguna de estas sanciones no se encuentre en firme toda vez que existen recursos de reposición sin resolver (SIC).

Figura 2. Sanciones de datos personales

Fuente Superintendencia de Industria y comercio

En materia de protección de datos personales el sector de las telecomunicaciones obtuvo un 35% del total de las multas impuestas por la Delegatura, lo cual equivale a la suma de \$271.040.000 millones de pesos, seguido por un 21% en las empresas colectoras de cartera por un valor de \$141.680.000 millones de pesos. En la gráfica se puede evidenciar las principales empresas sancionadas en esta materia y el respectivo valor de las sanciones para el primer semestre del 2014 (SIC).

Principales empresas sancionadas en materia de Datos Personales

Figura 3. Principales empresas sancionadas en materia de datos personales

Fuente Superintendencia de Industria y comercio

En la siguiente tabla se mencionan las empresas sancionadas por la Delegatura para la Protección de Datos Personales, y el valor de cada sanción recibida en el primer semestre del 2014. Como se evidencia la sanción más alta la obtuvo la empresa Comunicación Celular Comcel S.A. por un valor de \$160.160.000 millones de pesos, seguida de Colombia Comunicaciones S.A. con sanciones por valor de \$110.880.000 millones de pesos (SIC).

Tabla 2. *Empresas sancionadas por la Delegatura para la Protección de Datos Personales*

Nombre Empresa	Valor Sanción
Lisbeth Bejarano Castillo	\$ 616.000
Asociación Bancaria	\$ 6.160.000
Groupon Colombia S.A.	\$ 6.160.000
MetroFlex	\$ 12.320.000
Abogados Especializados en Cobranzas S.A.	\$ 14.784.000
Protección S.A.	\$ 21.560.000
Cobranzas Especiales Gerc S.A.	\$ 30.800.000
Cosmocentro Ciudadela Comercial	\$ 30.800.000
Refinancia S.A.	\$ 32.648.000
Almacenes Éxito S.A.	\$ 36.960.000
Crear País S.A.	\$ 63.448.000
Metrokia S.A.	\$ 66.528.000
Caja Colombiana de Subsidio Familiar - Colsubsidio	\$ 92.400.000
Colombia Telecomunicaciones S.A. E.S.P.	\$ 110.880.000
Comunicación Celular S.A. Comcel S.A.	\$ 160.160.000
Total	\$ 686.224.000

Fuente Superintendencia de Industria y comercio

Los principales motivos de sanción a las empresas en materia de protección de datos personales se concentró en un 75% por contravenciones a las normas de protección de datos financiero con sanciones que ascendieron a la suma de \$511.896.000 millones de pesos y en un 25% por contravención a la ley general del protección de datos con sanciones por la suma de \$174.328.000 millones de pesos (SIC).

Motivo de sanción en materia de Datos Personales

Figura 4. Motivo de sanción en materia de Datos Personales

Fuente Superintendencia de Industria y comercio

Tabla 3. Motivo de sanción en materia de Datos Personales

No. Sanciones	Tema	Valor
13	protección de datos financiero	\$511.896.000
6	ley general del protección de datos	\$174.328.000
19	Total	\$686.224.000

Fuente Superintendencia de Industria y comercio

6. Lineamientos que orienten a las organizaciones en el cumplimiento de la norma sobre protección y aseguramiento en el tratamiento de datos personales.

6.1 Lineamientos generales para el tratamiento de los datos ingreso, dado de baja, autorización, y solicitudes SIC

6.1.1 Autorización para el tratamiento de la información

Es necesario reconocer cómo se produce el flujo de información en sus procesos y actividades, identificar los procesos de obtención, por creación o captura, transformar, usar, almacenar, transferir, circular, compartir, eliminar o archivar hasta la disposición final de los datos.

Se debe adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento. (Decreto 1377, 2013, Artículo 5)

Si por parte de la empresa se requiere información sensible es importante informar a la persona lo correspondiente al tratamiento de datos sensibles de acuerdo al artículo 6 del Decreto 1377 de 2013:

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles que se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o

étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377, 2013 Artículo 3)

Tabla 4. *Diferencia entre datos sensibles y dato no sensibles*

Datos Sensibles	Datos no Sensibles
Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.	Son aquellos de datos de origen público que se pueden incluir en bases de datos cumpliendo con la autorización del titular para esto.
Origen racial o étnico	Nombres y Apellidos
Estado de salud	Cédula
Información genética,	Dirección y Teléfono
Creencias religiosas, filosóficas y morales, Afiliación sindical
Opiniones políticas
Preferencias sexuales.	

La autorización debe conservarse como prueba para su tratamiento puede ser en medio físico o electrónico, en ningún caso el silencio a esta autorización puede asimilarse aceptado, es decir debe existir la firma de recibido y aceptado en el físico o si es por medio electrónico debe existir expresamente la respuesta del cliente validando la información y aceptando el tratamiento de sus datos personales. (Decreto 1377, 2013, Artículo 7 y 8 -).

Ejemplo:

De acuerdo a la ley 1266 de 2008 autorizo de manera expresa e irrevocable a **La Empresa** o a quien represente sus derechos u ostente en el futuro cualquier título en calidad de acreedor, a consultar, solicitar, suministrar, reportar, procesar, transmitir, transferir, usar, poner en circulación y divulgar toda la información que se refiere a mi comportamiento crediticio, financiero y comercial, cuantas veces se requiera, por mis transacciones comerciales a las Centrales de Riesgo: CIFIN (ASOCIACION BANCARIA) y DATA CREDITO

(COMPUDEC) y a Entidades Financieras de Colombia, que presten el mismo servicio o a quien represente sus derechos.

Lo anterior implica que mi comportamiento presente y pasado frente a mis obligaciones, permanecerá reflejado de manera completa en las mencionadas bases de datos con el objeto de suministrar información suficiente y adecuada al mercado, sobre el estado de mis obligaciones financieras, comerciales y crediticias, por lo tanto, conocerán mi información quienes se encuentren afiliados a dichas centrales y/o que tengan acceso a estas, de conformidad con la legislación aplicable.

La permanencia de mi información en las bases de datos será determinada por el ordenamiento jurídico aplicable, en especial por las normas legales y la jurisprudencia, las cuales contienen mis derechos y obligaciones, que por ser públicos, conozco plenamente. Así mismo, manifiesto que conozco el reglamento de CIFIN y DATA CREDITO.

En caso de que en el futuro, el autorizado en este documento efectúe una venta de cartera o cesión a cualquier título de las obligaciones a mi cargo a favor de un tercero, los efectos de la presente autorización se extenderán a éste, en los mismos términos y condiciones.

Autorizó a que me sea remitida la información relacionada con reportes, proceso y/o divulgación sobre mi comportamiento crediticio, financiero y comercial, mediante correo físico, mensajes al teléfono celular y/o teléfono fijo y correo electrónico.

Deudor

Nombre Firma

C.C / NIT

Huella

Codeudor / Fiador

Nombre Firma

C.C / NIT

Huella

Es importante establecer medidas, recursos, herramientas para el adecuado y oportuno manejo de las solicitudes que realizan las personas teniendo en cuenta en cualquier momento pueden retractarse solicitando la eliminación o revocar la autorización, salvo cuando existan deudas o un estado legal que lo vincule actualmente con la empresa; vencido el término legal respectivo, el responsable y/o el encargado, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

Debe ser demostrable a petición de la Superintendencia de Industria y Comercio y que sea proporcional a lo siguiente:

- La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
- La naturaleza de los datos personales objeto del tratamiento.
- El tipo de Tratamiento.
- Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares. (Artículo 13-19 y 26-28 Decreto 1377 de 2013)

6.1.2 Realizar auditoria, monitorio o revisión periódica de las bases de datos por lo menos una vez al año para garantizar el cumplimiento de la norma en protección de datos personales.

Es importante establecer las medidas de seguridad de las bases de datos automatizadas y no automatizadas que contengan datos de carácter personal, distinguiendo los niveles de seguridad, partiendo de la naturaleza de la información, así como la necesidad de realizar una auditoría de las bases de datos, al menos cada dos años, cualquier asociación empresa o entidad que trate datos de carácter personal tiene la obligación cumplir lo establecido, el incumplimiento de estas obligaciones puede ser sancionado por la superintendencia de industria y comercio con importes hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción, Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó, puede llegar hasta el cierre temporal o definitivo de la operación que involucre tratamiento de datos sensibles.

6.1.3 Establecer seguridad de la información

Seguridad de información: se debe definir una política de seguridad que esté dirigida a la salvaguarda y disponibilidad de todos los activos de información, incluyendo el cumplimiento de la legislación vigente en protección de datos personales, la seguridad de la información debe garantizar los siguientes aspectos:

- Confidencialidad de la información: se debe asegurar que solamente los usuarios autorizados tengan acceso a la información
- Integridad de la información almacenada, asegurando que la información es correcta.
- Disponibilidad de la información en los sistemas de información y otros sistemas de almacenamiento de información.
- Se debe asegurar que los usuarios autorizados puedan acceder a los sistemas cuando estos sean requeridos.
- Revisión y en su caso generación de las clausulas legales y carteles informativos tanto para cumplir con el deber de informar, obtener el consentimiento al tratamiento de datos.
- Certificar cumplimiento de la legislación en materia de protección de datos personales, es importante poder certificar a los clientes, proveedores y empleados que su información de carácter personal se está gestionando correctamente de forma totalmente segura y que dicha información no se utiliza para otros temas diferentes para los que se suministraron.

6.2 Lineamientos para administración y reporte de base de datos ante la Superintendencia de Industria y comercio - SIC

Como lo establece la ley 1581 de 2012 el manejo establecido debe generar una política de tratamiento de la información, que debe ser reportada ante la Superintendencia de Industria y comercio – SIC quien es la autoridad delegada para la protección de datos personales y cuyas funciones entre otras Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento (Artículo 19 y 21, h de la ley 1581 de 2012). Estas Políticas deberán constar en medio físicas o electrónicas en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:

- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
- Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando no se haya informado mediante el aviso de privacidad.
- Derechos que le asisten como Titular.
- Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
- Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.

- Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos. (Artículo 2.2.2.25.3.1. Políticas de Tratamiento de la información – Decreto 1074/2015)

En el Decreto 1074 del 26 de Mayo de 2015, Capítulo 25 estableció la información mínima que debe contener las bases de datos, términos y condiciones para dicha inscripción que posteriormente según la circular externa 002 del 3 de Noviembre de 2015 se estableció información adicional para el registro y el procedimiento de inscripción el cual es muy sencillo de entender y aplicar ver [link](http://www.sic.gov.co/drupal/recursos_user/documentos/normatividad/circular/2015/Circular_02.pdf) http://www.sic.gov.co/drupal/recursos_user/documentos/normatividad/circular/2015/Circular_02.pdf

6.3 Lineamientos para la operación en los diferentes procesos internos de las empresas que pueden ayudar a desarrollar las políticas, procedimientos e instructivos internos.

Se debe realizar un Inventario de bases de datos automatizadas y no automatizadas, teniendo en cuenta:

- Información detallada de los canales PQR de los titulares
- Tipos de datos contenidos en la base de datos
- Ubicación de contacto y ubicación de los encargados del tratamiento
- Medidas de seguridad implementadas
- Forma de obtención de los datos
- Análisis de la información de datos personales de terceros que maneja la organización

Se debe analizar los procesos que originan la información de datos sensibles - datos personales de terceros

Se debe revisar autorización del titular

Revisión para el registro nacional de bases de datos

Registro de base de datos RNDB en la Superintendencia de Industria y Comercio.

A continuación relacionamos los riesgos más comunes que enfrentan las empresas calificando para clasificarlo así:

Tabla 5. *Matriz de riesgos*

		IMPACTO				
		1	2	3	4	5
P r o b a b i l i d a d	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Calificación Riesgo	
15 - 25	Riesgo Extremo
10 - 12	Riesgo Alto
5 - 9	Riesgo Moderado
1 - 4	Riesgo Bajo

Impacto	Probabilidad	Resultado	Calificación
5	5	25	Extremo
4	5	20	Extremo
5	4	20	Extremo
4	4	16	Extremo
3	5	15	Extremo
5	3	15	Extremo
3	4	12	Alto
4	3	12	Alto
2	5	10	Alto
5	2	10	Alto
3	3	9	Moderado
2	4	8	Moderado
4	2	8	Moderado
2	3	6	Moderado
3	2	6	Moderado
1	5	5	Moderado
5	1	5	Moderado
1	4	4	Bajo
2	2	4	Bajo
4	1	4	Bajo
1	3	3	Bajo
3	1	3	Bajo
1	2	2	Bajo
2	1	2	Bajo
1	1	1	Bajo

Tabla 6. *Definición para calificar la frecuencia*

Calificación	Descriptor	Definición
5	Casi Seguro	Alta probabilidad de que se presente, ha ocurrido o podría ocurrir varias veces al año.
4	Frecuente	El evento ha ocurrido o podría ocurrir alguna vez en un período de un año.
3	Ocasional	El evento ha ocurrido o podría ocurrir alguna vez en un período de cinco años.
2	Improbable	Baja probabilidad de que se presente, ha ocurrido o podría ocurrir alguna vez en un período de diez años
1	Raro	Muy baja probabilidad de que se presente, ha ocurrido o podría ocurrir alguna vez en un período de quince años o más.

Tomando como base la probabilidad de que ocurra al no implementar los controles que se van a proponer:

Multiplicando esta probabilidad por el impacto, que aunque se utilice la siguiente tabla, en todas se tendrá como impacto alto al contemplar todos estos hallazgos con un impacto económico y reputacional independiente de la cantidad de ocurrencia:

Tabla 7. Definición para calificar el impacto

Calificación	Descriptor	ECONÓMICO:	REPUTACIÓN:
		Este factor es considerado cuando la materialización del riesgo afecta negativamente la solidez financiera de la compañía.	Se considera este factor cuando la materialización del riesgo afecta la percepción/opinión que tienen los diferentes grupos respecto a la organización.
5	Alto	Pérdida económica superior a COP 500MM	El evento genera un concepto público desfavorable que afecta la credibilidad y confianza de la Compañía, ésta es acusada por los públicos clave y el evento es desplegado continuamente por los medios de comunicación local, regional, nacional y/o redes sociales; o Pérdida grave del apoyo o credibilidad de la mayoría de grupos de interés
4	Mayor	Pérdida económica entre COP 101MM y COP 500MM	El evento genera un concepto público desfavorable que afecta la credibilidad y confianza de la Compañía, ésta es cuestionada por los públicos clave y el evento es desplegado continuamente por los medios locales y regionales y de manera aislada por los medios de comunicación nacionales y redes sociales. Disminución del apoyo o credibilidad de algunos grupos de interés
3	Moderado	Pérdida económica entre COP 50 MM y COP 100MM	El evento genera un concepto público desfavorable que afecta la credibilidad de la Compañía, es conocido por los públicos clave y es desplegado por los

Calificación Descriptor		ECONÓMICO: Este factor es considerado cuando la materialización del riesgo afecta negativamente la solidez financiera de la compañía.	REPUTACIÓN: Se considera este factor cuando la materialización del riesgo afecta la percepción/opinión que tienen los diferentes grupos respecto a la organización.
			medios de comunicación local y redes sociales y a nivel regional de manera aislada. Disminución del apoyo o credibilidad de máximo dos <i>grupos</i> de interés
2	Menor	Pérdida económica entre COP 10MM y COP 49MM	El evento genera un concepto público desfavorable que afecta la credibilidad de la Compañía, es conocido por los públicos clave y es desplegado de manera aislada por los medios de comunicación local y redes sociales. Inquietudes de algunos grupos de interés.
1	Bajo	Pérdida económica menor a COP 10MM	El evento no afecta la credibilidad y confianza en la compañía. Puede generar inquietudes al interior de la compañía y no trasciende a los medios de comunicación. De manera puntual se comenta en redes sociales.

6.3.1 Procesos con Personal – áreas de Talento Humano o la Administración

Tabla 8. *Calificación y control propuesto para los riesgos en el proceso de selección y reclutamiento*

Proceso Clave	Procesos de Selección – Reclutamiento		
Riesgos	Probabilidad	Impacto	Calificación
Reclamo de personas que entregan su hoja de vida al participar en los procesos de selección y no se les devuelve.	4	5	20
Reclamo de personas que participan en los procesos de selección y no reciben repuesta a su solicitud de información proceso de selección.	4	5	20
Control Propuesto	Implementar formato para firma una vez entreguen la hoja de vida física o correo automático una vez envíen por correo que contenga: Físico: Nombre completo con número de cédula y firma aceptando estar informado que si dentro de 20 días la empresa no le llama se da por rechazada su hoja de vida al proceso de selección al cual participa y debe acercarse por la hoja de vida, de lo contrario en 60 se procede a destruir su hoja de vida del archivo físico. Correo: Si dentro de 20 días la empresa no le llama se da por rechazada su hoja de vida al proceso de selección al cual participa.		
	Implementar un correo institucional para el reclutamiento		

Proceso Clave	Procesos de Selección – Reclutamiento		
Riesgos	Probabilidad	Impacto	Calificación
	de las hojas de vida para evitar envíos a correos de personal que en algún momento se desvincule de la empresa.		
	Incluir en el procedimiento e instructivos del proceso de selección detalladamente la implementación de la respuesta automática o formato físico según corresponda, para que en las auditoría interna se valide el control.		
	Incluir en la política de tratamiento de datos personales estas medidas de control que ayudaran a mitigar la materialización del riesgo.		

Tabla 9. *Calificación y control propuesto para los riesgos en el proceso de contratación empleados*

Proceso Clave	Contratación empleados		
Riesgos	Probabilidad	Impacto	Calificación
Reclamo de empleados por no autorizar su inclusión en Base de datos.	3	5	15
Control Propuesto	<p>Implementar formato para firma del empleado antes de ser ingresado en la base de datos para mitigar el riesgo, como lo vemos en esta propuesta de formato que los datos serán almacenados en nuestras bases de datos, se reporta ante la SIC, aclarando en este mismo que el manejo de estos datos se realiza de acuerdo a las políticas internas en tratamiento de datos personales y en cumplimiento a las normas que lo regulan, garantizando transparencia, confiabilidad y que en cualquier momento puede rectificar estos datos o retractarse, así como presentar quejas ante la SIC:</p> <p>En cumplimiento de la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, le informamos que los datos personales que usted nos entregue serán</p>		

Proceso Clave	Contratación empleados
	<p>almacenados, usados, circulados, actualizados y en general tratados con la siguiente finalidad: (i) envío de información relacionada con el objeto social de La Empresa (ii) Contacto por medio telefónico o por correo electrónico para mantenerlo informado de la empresa, sus pagos de nómina y seguridad social o solicitar repuesta por incumplimiento al reglamento interno de trabajo y sus debidas sanciones (iii) Transmitir los datos personales a la SIC o entidades públicas. El responsable de los datos recolectados es La Empresa domiciliado en la Dirección, identificado con Nit:, Teléfono:, Página web:, con correo electrónico. El manejo de dichos datos se hará de acuerdo a lo establecido en las Políticas de Tratamiento de la Información de La Empresa que contiene las políticas establecidas por La Empresa para el tratamiento de los datos, los mecanismos y procedimientos para la efectividad de los derechos del Titular de la información a: (i) Conocer, actualizar y rectificar los Datos Personales. (ii) Solicitar prueba de la autorización para la recolección y el tratamiento de los datos personales. (iii) Ser informado por los responsables del uso que se le han dado a sus datos personales. (iv) Presentar quejas ante la Superintendencia de Industria y Comercio en el caso en que haya una violación por parte de los responsables de las disposiciones de la Ley 1581 de 2012, el Decreto 1377 de 2013 y otras normas que los modifiquen. (v) Revocar la autorización otorgada para el tratamiento de los datos personales. (vi) Solicitar ser eliminado de la base de datos siempre y cuando no exista un deber legal o contractual de permanecer en las mismas y (vii) Tener acceso a los Datos Personales que los responsables hayan recolectado y tratado.</p> <hr/> <p>Incluir en el procedimiento e instructivos del proceso de contratación que el formato mencionado sea requisito de los documentos para la elaboración del contrato de trabajo; de esta forma en las auditoría interna se valide el control.</p> <hr/> <p>Incluir en la política de tratamiento de datos personales estas medidas de control que ayudaran a mitigar la materialización del riesgo.</p>

6.3.2 Procesos de Clientes – áreas Comercial, Cartera, Mercadeo, Administración o Gerencia General

Tabla 10. *Calificación y control propuesto para los riesgos en el proceso de afiliación clientes sistema de información para venta*

Proceso Clave		Afiliación Clientes Sistema de Información para Venta		
Riesgos		Probabilidad	Impacto	Calificación
Reclamo de Clientes por no autorizar su inclusión en Base de datos.		4	5	15
Control Propuesto	<p>Implementar formato para firma del cliente antes de ser ingresado en la base de datos; para mitigar el riesgo, como lo vemos en esta propuesta de formato que los datos serán almacenados en nuestras bases de datos, se reporta ante la SIC, aclarando en este mismo que el manejo de estos datos se realiza de acuerdo a las políticas internas en tratamiento de datos personales y en cumplimiento a las normas que lo regulan, garantizando transparencia, confiabilidad y que en cualquier momento puede rectificar estos datos o retractarse, así como presentar quejas ante la SIC:</p> <p>En cumplimiento de la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, le informamos que los datos personales que usted nos entregue serán almacenados, usados, circulados, actualizados y en general tratados con la siguiente finalidad: (i) envío de información relacionada con el objeto social de La Empresa (ii) Contacto por medio telefónico o por correo electrónico para ofrecer los productos o servicios, (iii) Transmitir los datos personales a la SIC o entidades públicas. El responsable de los datos recolectados es La Empresa domiciliado en la Dirección, identificado con Nit:, Teléfono:, Página web:, con correo electrónico. El manejo de dichos datos se hará de acuerdo a lo establecido en las Políticas de Tratamiento de la Información de La Empresa que contiene las políticas establecidas por La Empresa para el</p>			

Proceso Clave	Afiliación Clientes Sistema de Información para Venta
	<p>tratamiento de los datos, los mecanismos y procedimientos para la efectividad de los derechos del Titular de la información a: (i) Conocer, actualizar y rectificar los Datos Personales. (ii) Solicitar prueba de la autorización para la recolección y el tratamiento de los datos personales. (iii) Ser informado por los responsables del uso que se le han dado a sus datos personales. (iv) Presentar quejas ante la Superintendencia de Industria y Comercio en el caso en que haya una violación por parte de los responsables de las disposiciones de la Ley 1581 de 2012, el Decreto 1377 de 2013 y otras normas que los modifiquen. (v) Revocar la autorización otorgada para el tratamiento de los datos personales. (vi) Solicitar ser eliminado de la base de datos siempre y cuando no exista un deber legal o contractual de permanecer en las mismas y (vii) Tener acceso a los Datos Personales que los responsables hayan recolectado y tratado.</p> <p>Incluir en el procedimiento e instructivos del proceso de creación de clientes que el formato mencionado sea requisito de los documentos para el ingreso en base de datos como cliente; de esta forma en las auditoría interna se valide el control.</p> <p>Incluir en la política de tratamiento de datos personales estas medidas de control que ayudaran a mitigar la materialización del riesgo.</p>

Tabla 11. *Calificación y control propuesto para los riesgos en el proceso de tele mercadeo o envío de correo con publicidad o información general de su cuenta*

Proceso Clave	Tele Mercadeo o envío de correo con publicidad o información general de su cuenta		
Riesgos	Probabilidad	Impacto	Calificación
Reclamo de Clientes por no autorizar le sean llamados o el envío de correo electrónico.	4	5	20
Control Propuesto	Implementar formato para firma del cliente antes de ser ingresado en la base de datos; para mitigar el riesgo, como lo vemos en esta propuesta de formato		

Proceso Clave	Tele Mercadeo o envío de correo con publicidad o información general de su cuenta
	<p>que los datos serán almacenados en nuestras bases de datos, se reporta ante la SIC, aclarando en este mismo que el manejo de estos datos se realiza de acuerdo a las políticas internas en tratamiento de datos personales y en cumplimiento a las normas que lo regulan, garantizando transparencia, confiabilidad y que en cualquier momento puede rectificar estos datos o retractarse, así como presentar quejas ante la SIC:</p> <p>En cumplimiento de la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, le informamos que los datos personales que usted nos entregue serán almacenados, usados, circulados, actualizados y en general tratados con la siguiente finalidad: (i) envío de información relacionada con el objeto social de La Empresa (ii) Contacto por medio telefónico o por correo electrónico para ofrecer los productos o servicios, (iii) Transmitir los datos personales a la SIC o entidades públicas. El responsable de los datos recolectados es La Empresa domiciliado en la Dirección, identificado con Nit:, Teléfono:, Página web:, con correo electrónico. El manejo de dichos datos se hará de acuerdo a lo establecido en las Políticas de Tratamiento de la Información de La Empresa que contiene las políticas establecidas por La Empresa para el tratamiento de los datos, los mecanismos y procedimientos para la efectividad de los derechos del Titular de la información a: (i) Conocer, actualizar y rectificar los Datos Personales. (ii) Solicitar prueba de la autorización para la recolección y el tratamiento de los datos personales. (iii) Ser informado por los responsables del uso que se le han dado a sus datos personales. (iv) Presentar quejas ante la Superintendencia de Industria y Comercio en el caso en que haya una violación por parte de los responsables de las disposiciones de la Ley 1581 de 2012, el Decreto 1377 de 2013 y otras normas que los modifiquen. (v) Revocar la autorización otorgada para el tratamiento de los datos personales. (vi) Solicitar ser eliminado de la base de datos siempre y cuando no exista un deber legal o contractual de permanecer en las mismas y (vii) Tener acceso a</p>

Proceso Clave	Tele Mercadeo o envío de correo con publicidad o información general de su cuenta
<p>los Datos Personales que los responsables hayan recolectado y tratado.</p> <p>Adicional de incluir en los procedimiento y/o instructivos del proceso de creación de clientes, es necesario en los procesos y/o instructivos para captar clientes o realizar campañas publicitarias voz a voz o puerta a puerta de mercadeo, se incluya el formato mencionado como requisito ineludible para poder realizar este tipo de procesos, solo el cliente que firmo este documento se puede utilizar para este tipo de campañas.</p> <p>Es importante para los clientes creados en años anteriores a la presente reglamentación seguir lo dispuesto en el Decreto 1377 de 2013, arto 10 y el Decreto 1074 de 2015 en su capítulo 25 Artículo 2.2.2.25.2.7. Datos recolectados antes del 27 de junio de 2013, justificando ante la SIC en el caso que le sea imposible contactar o financieramente imposible realizarlo uno a uno pero que realizó de acuerdo a lo dispuesto en la norma lo posible para comunicarles a sus clientes antes creados antes de dicha fecha. No obstante debe hacer caso una vez el cliente en la primera llamada o correo enviado solicita ser eliminado de la base de datos, así mismo deben tener cuidado si es un cliente recurrente de la empresa lo que se considera si le es posible recoger su autorización y por ende no existe excusas para estos casos puntuales del incumplimiento en la norma.</p> <p>Incluir en la política de tratamiento de datos personales estas medidas de control que ayudaran a mitigar la materialización del riesgo.</p>	

Tabla 12. *Calificación y control propuesto para los riesgos en el proceso de crédito y manejo de cartera*

Proceso Clave		Crédito y Manejo de cartera		
Riesgos		Probabilidad	Impacto	Calificación
Reclamo de Clientes, codeudores o fiadores por no autorizar ser consultados en centrales de riesgo		4	5	20
Reclamo de Clientes, codeudores o fiadores por no autorizar ser reportados en centrales de riesgo positivo o negativo e incluso por error en reporte		4	5	20
Reclamo de clientes, codeudores o fiadores por no informar de su obligación antes de ser reportado en una central de riesgo negativamente por mora en las obligaciones.		4	5	20
Control Propuesto	<p>Implementar formato para firma de Clientes, codeudores o fiadores antes de ser ingresado en estudio de crédito; para mitigar el riesgo, como lo vemos en esta propuesta de formato que los datos serán almacenados en nuestras bases de datos, se reporta ante la SIC, aclarando en este mismo que el manejo de estos datos se realiza de acuerdo a las políticas internas en tratamiento de datos personales y en cumplimiento a las normas que lo regulan, garantizando transparencia, confiabilidad y que en cualquier momento puede rectificar estos datos o retractarse, así como presentar quejas ante la SIC:</p> <p>De acuerdo a la ley 1266 de 2008 autorizo de manera expresa e irrevocable a La Empresa o a quien represente sus derechos u ostente en el futuro cualquier título en calidad de acreedor, a consultar, solicitar, suministrar, reportar, procesar, transmitir, transferir, usar, poner en circulación y divulgar toda la información que se refiere a mi comportamiento crediticio, financiero y comercial, cuantas veces se requiera, por mis transacciones comerciales a las</p>			

Proceso Clave	Crédito y Manejo de cartera
	<p>Centrales de Riesgo: CIFIN (ASOCIACION BANCARIA) y DATACREDITO (COMPUTEC) y a Entidades Financieras de Colombia, que presten el mismo servicio o a quien represente sus derechos.</p> <p>Lo anterior implica que mi comportamiento presente y pasado frente a mis obligaciones, permanecerá reflejado de manera completa en las mencionadas bases de datos con el objeto de suministrar información suficiente y adecuada al mercado, sobre el estado de mis obligaciones financieras, comerciales y crediticias, por lo tanto, conocerán mi información quienes se encuentren afiliados a dichas centrales y/o que tengan acceso a estas, de conformidad con la legislación aplicable</p> <p>La permanencia de mi información en las bases de datos será determinada por el ordenamiento jurídico aplicable, en especial por las normas legales y la jurisprudencia, las cuales contienen mis derechos y obligaciones, que por ser públicos, conozco plenamente. Así mismo, manifiesto que conozco el reglamento de CIFIN y DATACREDITO.</p> <p>En caso de que en el futuro, el autorizado en este documento efectúe una venta de cartera o cesión a cualquier título de las obligaciones a mi cargo a favor de un tercero, los efectos de la presente autorización se extenderán a éste, en los mismos términos y condiciones.</p> <p>Autorizó a que me sea remitida la información relacionada con reportes, proceso y/o divulgación sobre mi comportamiento crediticio, financiero y comercial, mediante correo físico, mensajes al teléfono celular y/o teléfono fijo y correo electrónico.</p> <p>Deudor</p> <p>Nombre Firma</p> <p>C.C / NIT</p> <p>Huella</p>

Proceso Clave	Crédito y Manejo de cartera
	Codeudor / Fiador Nombre Firma C.C / NIT Huella
	Realizar envío de carta al cliente moroso, codeudores y/o fiadores informando que si no se pone al día en 20 días será reportado en las centrales de riesgo cumpliendo con los requisitos del artículo 20 de la ley 1266 de 2008.
	Incluir en los procedimientos y/o instructivos del proceso de Crédito a clientes, el formato mencionado como requisito ineludible para poder realizar estudio de crédito.
	Incluir en el instructivo de reporte a centrales de riesgo la confirmación del envío de la carta al cliente, codeudores y/o fiadores informando el estado de la obligación y el posible reporte al no ponerse al día.

6.3.3 Procesos con Proveedores – áreas Compras, Administración o toda la organización cuando desde cualquier área se tiene contacto con proveedores.

Tabla 13. *Calificación y control propuesto para los riesgos en el proceso de creación de proveedores sistema de información para compra de productos o prestación de servicios*

Proceso Clave	Creación de Proveedores Sistema de Información para Compra de productos o prestación de servicios		
Riesgos	Probabilidad	Impacto	Calificación
Reclamo de Proveedores por no autorizar su inclusión en Base de datos.	4	5	15
Control Propuesto	Implementar formato para firma de Proveedores antes de ser ingresado en la base de datos:		

Proceso Clave	Creación de Proveedores Sistema de Información para Compra de productos o prestación de servicios
	<p>En cumplimiento de la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, le informamos que los datos personales que usted nos entregue serán almacenados, usados, circulados, actualizados y en general tratados con la siguiente finalidad: (i) envío de información relacionada con el objeto social de La Empresa (ii) Contacto por medio telefónico o por correo electrónico para ofrecer los productos o servicios, (iii) Transmitir los datos personales a la SIC o entidades públicas. El responsable de los datos recolectados es La Empresa domiciliado en la Dirección, identificado con Nit:, Teléfono:, Página web:, con correo electrónico. El manejo de dichos datos se hará de acuerdo a lo establecido en las Políticas de Tratamiento de la Información de La Empresa que contiene las políticas establecidas por La Empresa para el tratamiento de los datos, los mecanismos y procedimientos para la efectividad de los derechos del Titular de la información a: (i) Conocer, actualizar y rectificar los Datos Personales. (ii) Solicitar prueba de la autorización para la recolección y el tratamiento de los datos personales. (iii) Ser informado por los responsables del uso que se le han dado a sus datos personales. (iv) Presentar quejas ante la Superintendencia de Industria y Comercio en el caso en que haya una violación por parte de los responsables de las disposiciones de la Ley 1581 de 2012, el Decreto 1377 de 2013 y otras normas que los modifiquen. (v) Revocar la autorización otorgada para el tratamiento de los datos personales. (vi) Solicitar ser eliminado de la base de datos siempre y cuando no exista un deber legal o contractual de permanecer en las mismas y (vii) Tener acceso a los Datos Personales que los responsables hayan recolectado y tratado.</p> <p>Incluir en el procedimiento e instructivos del proceso de creación de proveedores que el formato mencionado sea requisito de los documentos para el ingreso en base de datos como cliente; de esta forma en las auditorías internas se valide el control.</p> <p>Es importante para los Proveedores creados en años anteriores a la presente reglamentación seguir lo dispuesto en el Decreto 1377 de 2013, arto 10 y el</p>

Proceso Clave	Creación de Proveedores Sistema de Información para Compra de productos o prestación de servicios
	Decreto 1074 de 2015 en su capítulo 25 Artículo 2.2.2.25.2.7. Datos recolectados antes del 27 de junio de 2013, justificando ante la SIC en el caso que le sea imposible contactar o financieramente imposible realizarlo uno a uno pero que realizó de acuerdo a lo dispuesto en la norma lo posible para comunicarles a sus proveedores antes creados antes de dicha fecha. No obstante debe hacer caso una vez el proveedor solicite ser eliminado de la base de datos, así mismo deben tener cuidado si es un proveedor activo de la empresa se considera que si es posible recoger su autorización y por ende no existe excusas para estos casos puntuales del incumplimiento en la norma.
	Incluir en la política de tratamiento de datos personales estas medidas de control que ayudaran a mitigar la materialización del riesgo.

6.3.4 General para las empresas

Tabla 14. *Calificación y control propuesto para los riesgos estratégicos*

Proceso Clave	Estratégico		
Riesgos	Probabilidad	Impacto	Calificación
Desinformación del personal en el conocimiento de las normas de protección de datos personales	5	5	25
Control	Realizar campañas de capacitación por áreas mínimo dos veces al año, e incluir para todo ingreso de personal nuevo en su malla de inducción requisito socialización normas de protección de datos personales y sus implicaciones.		
Propuesto	Socialización de los diferentes procedimiento e instructivos que tiene que ver con el ingreso en base de datos como empleados, cliente y proveedores.		
	Socialización política de tratamiento de datos personales estas medidas de control que ayudaran a mitigar la materialización del riesgo.		

6.4 Principios claves a tener en cuenta:

- Definición de los responsables dentro de la empresa del tratamiento de datos personales, que de acuerdo al tamaño de la empresa puede ser designado el Ing. de Sistemas por parte del representante legal; si es una empresa grande se puede evaluar si crear un comité de base de datos donde intervengan por lo menos Talento Humano, Tesorería, Cartera, Jurídica y Auditoría con el fin de establecer la política de no existir, el cumplimiento de esta y las evaluaciones de los riesgos mencionados.
- Si la empresa requiere utilizar fotos o datos con fines publicitarios se debe solicitar autorización expresa de las personas para esto.
- Informar a los terceros el manejo que se le da a los datos y la ubicación de los mismos.
- Establecer mecanismos de control apoyados del experto en este tema para detectar si se puede presentar acceso no autorizado a las bases de datos y de ser así informar al tercero y a la SIC.
- Evaluación por medio de auditores interno el cumplimiento de la política, procedimientos o lineamientos establecidos y/o auditores externos para evaluar estos documentos vs el cumplimiento de la norma.

7. Importancia del manejo de datos y la seguridad de información en la Revisoría Fiscal y Auditoría Externa

Al revisar Una de las funciones del Revisor Fiscal es: “...Inspeccionar asiduamente los bienes de la sociedad y procurar que se tomen oportunamente las medidas de conservación o seguridad de los mismos y de los que ella tenga en custodia a cualquier otro título;” (artículo 207, código de comercio), lo que para este trabajo podemos llamar la pérdida de dinero por la materialización del riesgo al recibir una sanción en tema de protección de datos, se puede entender como una falta en la inspección por parte del revisor fiscal a los bienes de la sociedad.

El revisor fiscal para ejercer sus funciones consagradas en el código de comercio debe indagar, consultar, validar según lo mencionado en el código de comercio “..Impartir las instrucciones, practicar las inspecciones y solicitar los informes que sean necesarios para establecer un control permanente sobre los valores sociales, por consiguiente la empresa está en la obligación de permitirle toda información sin restricciones, con la plena seguridad que los datos no serán reportados o utilizados con fines diferentes a las de emitir una opinión sobre la razonabilidad de los estados financieros, el control interno de la empresa y el cumplimiento a las diferentes normas que aplique para las empresas.

Para el cumplimiento a sus funciones consagradas en el código de comercio es obligación de la empresa suministrar la información necesaria para cumplir con sus funciones, recordemos que el Contador Público que ejerce como Revisor Fiscal en Colombia que es el único en Colombia que puede ejercer esta función no requiere explícitamente de un acuerdo de

confidencialidad para acceder a la información contable, financiera, de procesos, bases de datos teniendo en cuenta lo consagrado en la Ley 43 de 1990, en su artículo 63 donde detalla el secreto profesional del Contador Público quien está obligado a guardar la reserva profesional de todo lo que conozca en ejercicio de su profesión. No obstante todo delito evidenciado producto de la función como Revisor Fiscal no debe ser ocultado ante las entidades regulatorias, ya que su atestación o firma se presumen legalmente como un documento público

8. Conclusiones

Las empresas se ven obligadas a incluir dentro de sus procesos e instructivos medidas de control para mitigar los riesgos a exposición o materialización de sanciones por el incumplimiento a las normas en materia de protección de datos personales para garantizar la integridad, disponibilidad y confidencialidad de la información bajo los diferentes formatos que sustentan su tratamiento y lo definido en la política que debe ser reportada a la Superintendencia de Industria y Comercio – SIC junto al registro de base de datos en el RNBD.

En este trabajo de grado se incluyen algunos lineamiento para incluir en los procesos que intervienen información de terceros (Empleados, clientes, Proveedores) los controles que pueden mitigar el riesgo que existe, lo que permite en la función del Revisor Fiscal y Auditor Externo un enfoque de cara al cumplimiento de las funciones como Revisor Fiscal la importancia en la sujeción a las normas legales, la eficiencia en la gestión administrativa, de ejercer controles, y evaluar el cumplimiento a las normas en todos los ámbitos que tiene relación en una empresa.

De igual manera en las Norma Internacional de Auditoría (NIAs) se puede observar claramente el campo de aplicación de la Auditoría con relación a la Responsabilidad que tiene el auditor de considerar las disposiciones legales y reglamentarias en la auditoría de estados financieros (NIA 250), aunque es claro que existe gran cantidad de reglamentación que puede dar un alcance diferente en la planeación, se debe analizar el efecto material en los estados financieros si se materializa una sanción de hasta \$1.179 millones, lo que conlleva la responsabilidad del auditor a la aplicación de procedimientos de auditoría específicos que ayuden

a identificar incumplimientos de aquellas disposiciones legales y reglamentarias que puedan tener este efecto y por ende la evaluación de los controles para el cumplimiento de las normas en protección de datos personales.(norma NIA 250 pag 4, Numeral 6 y 7 b.)

Este trabajo aporta al Revisor Fiscal o al Auditor Interno o Exteno de manera importante para utilizarlo como modelo de identificación del riesgo que tienen las empresas en materia de protección de datos, generando recomendaciones inmediatas a posibles hechos que no son tan fáciles de detectar en la profesión por el primer enfoque existente hacia los riesgos contables buscando validar exactitud, registros, integridad de la información, Homogeneidad de criterios, cierres, existencia, la presentación de los estados financieros, valoración entre otros, un segundo enfoque hacia los riesgos de procesos, buscando conocer cómo son aplicados en la empresa según lo definido por ellos, que mejoras se pueden aportar, tercero o en el orden de cada Revisor o Auditor que de acuerdo a los primeros indicios puede auditar riesgo con relación al personal por riesgo de fraude, falta o rechazo a cultura de control, comunicación o socialización de los procesos entre otros; con estos lineamientos se puede basar para validar que de esto aplica, se está realizando y que no para recomendar la implementación en busca de no incumplir la norma y evitar sanciones que se pueden materializar afectando los estados resultados que firma como Revisor Fiscal.

Bibliografía

Colombia, Congreso de la Republica. (Diciembre 31 de 2008) *Ley 1266. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.* Art. 12 y 13 Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488>

Colombia, Congreso de la Republica. (Octubre 17 de 2012) *Ley 1581. Por la cual se dictan disposiciones generales para la protección de datos personales.* Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>

Colombia, Presidente de la República. (Agosto 6 de 2010). *Decreto 2952. en ejercicio de sus facultades constitucionales y legales, en especial, las conferidas por el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en los artículos 12 y 13 de la Ley 1266 de 2008,* Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=40120>

Colombia, Presidente de la República. (Junio 27 de 2012) *Decreto 1377. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646>

Colombia, Presidente de la República. (Mayo 13 de 2014) *Decreto 886. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.* Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338>

Colombia, Presidente de la República. (Mayo 15 de 2009) *Decreto 1727. Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.* Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36251>

El Pueblo de Colombia. (1991) *Constitución Nacional de Colombia* Artículo 15

Ministerio de Comercio Industria y Turismo (s.f.) *Capítulo 26 registro nacional de bases de datos* Recuperado de: <http://www.mincit.gov.co/publicaciones.php?id=35994>

Superintendencia de Industria y Comercio (noviembre 3 2015) *Circula 002*. Recuperado de: http://www.sic.gov.co/drupal/recursos_user/documentos/normatividad/circular/2015/Circular_02.pdf

Superintendencia de Industria y Comercio (s. f.) *Registro Nacional de base de datos* Recuperado de: <http://www.sic.gov.co/drupal/registro-nacional-de-bases-de-datos>

Superintendencia de Industria y Comercio. (29 de octubre de 2015). *Superindustria ordena bloqueo temporal de información personal contenida en el portal web www.plagiosos.org por presuntas infracciones al régimen de datos personales*. Recuperado de <http://www.sic.gov.co/drupal/noticias/superindustria-ordena-bloqueo-temporal-de-informacion-personal-contenida-en-el-portal-por-presuntas-infracciones-al-regimen-de-datos-personales>).