VIOLACIONES EN LA GESTIÓN DE DATOS PERSONALES POR ENTIDADES PRIVADAS EN COLOMBIA

Violations in the management of personal data by private entities in Colombia

José Mario Chaverra Ramírez
jmchaverra@poligran.edu.co

Yornis Murillo Palomeque
yornis22outlook.com

José Nilson Sanchez

Jonis898@hotmail.com

Institución Universitaria Politécnico Grancolombiano
Derecho
Colombia

Resumen

El articulo busca establecer si existe eficacia en las medidas que ha implementado la Superintendencia de Industria y Comercio - SIC[1] con el ánimo de salvaguardar a las personas frente a las vulneraciones que se presentan en el manejo le dan a sus datos personales por entidades privadas en Colombia. Como metodología de investigación acudiremos a la cualitativa y deductiva, donde se aplica la recolección de información que ha emitido la SIC relacionada con información estadística de procesos que se han adelantado y los que hay en curso por esa entidad contra entidades privadas por el uso indebido de datos personales incluidas las entidades financieras, asimismo se acudirá a una revisión detallada investigaciones realizadas por universidades colombianas y publicaciones de artículos relacionados con el tema abordado, destacando de esta investigación las vulnerabilidades en seguridad que presentan los encargados de la gestión de datos de carácter personal y la poca operatividad de la SIC para sancionarlos, los datos para el desarrollo dela investigación abarcan un periodo comprendido entre 2014 y 2020 a fin de tener información actualizada al respecto.

Palabras clave:
Datos personales, datos privados, consentimiento, base de datos, titular.

Recepción:
Aceptación:
Cite este artículo como: Chaverra, J. Murillo, Y. y Sánchez, J. (2020). Violaciones en la gestión de datos personales por entidades privadas en Colombia. *Revista Politécnico Grancolombiano*. Medellín, Colombia.

[1] SIC, Superintendencia de Industria y Comercio

José Mario Chaverra Ramírez
Yornis Murillo Palomeque
José Nilson Sánchez

INTRODUCCIÓN

Con este artículo se pretende divulgar los resultados que arrojaron de las investigaciones realizadas por estudiantes de la carrera de Derecho del Politécnico Grancolombiano, orientada a establecer de manera clara, objetiva, precisa y detallada, las violaciones que se presentan en la gestión de datos personales por entidades privadas del territorio colombiano, así como determinar las medidas que adelanta la entidad encargada de su vigilancia y control para evitar que se continúe realizando esta mala práctica y llegar a establecer si son eficaces los controles que se realizan para proteger a las personas de este acto que vulnera de manera directa lo consagrado en la carta magna en su artículo 15 y 20.

La institución jurídica constitucional para el debido trato, protección y gestión de datos personales no es en sí una creación propia del ordenamiento jurídico colombiano, sino una adaptación a nuestro ordenamiento jurídico de la medida implementada en el año 1988 en Brasil denominada remedio o acción procedimental de habeas data[2], el cual es un mecanismo jurídico-constitucional preventivo para el acceso y conocimiento de los datos e informaciones de carácter personal, así como instrumento sancionatorio, de actualización, corrección y supresión de datos cuando estos son incorrectos (Libardo Riascos. Derecho y Realidad. 2016. p.2)

Dicha institución jurídica fue acogida en Colombia en el Art. 15.2 de la CP de 1991, reglamentado posteriormente desde el punto de vista de la información relacionada con datos financieros (ley 1266 de 2008, por medio de la ley 1273 de 2009) con las implementaciones que a la ley penal añadieron en el año 2000 un nuevo bien jurídico orientado a salvaguardar los datos personales y la información, donde en el año 2012 se reglamentada parcialmente y se dictan disposiciones cuya finalidad es proteger los datos personales (ley estatutaria 1581 y decreto Nacional 1377).

Con la creación e implementación de la ley 1266 de 2008 se crean una serie de derechos, deberes y obligaciones entre los titulares de la información y quienes están encargados de la protección de esta y se delega a la SIC para que sea la encargada de la vigilancia y control de todo lo relacionado con el tratamiento de datos personales, posteriormente con la ley 1581 de 2012 y para garantizar que lo expresado en esta ley se cumpla, se crea dentro de la SIC la DPDP[3] y con ella el RNBD[4], a fin de darle una mayor seguridad a la protección de los datos personales.

El trámite, sanciones y medidas que se deben tomar para tasar o graduar las sanciones impuestas por la SIC se encuentran estipuladas en la ley 1581 / 2012 - capítulo II, art. 22 a 24, además el Código Penal Colombiano en sus artículos 269F y 269H hace referencia a la tipificación punitiva de esta conducta y las circunstancias de agravación de la misma.

El ámbito de aplicación del RNBD fue modificado (decreto 090 de 2018 del Gobierno Nacional) haciendo referencia a quienes están obligados a hacer el registro de las bases de datos ante la SIC, los cuales deben cumplir con una serie de requisitos siendo fundamental el de contar con activos

[2] El Derecho de Habeas Data está orientado a permitir a los ciudadanos conocer toda la información que entidades públicas y privadas posean sobre ellos en bases de datos, pudiendo solicitar que se actualice y rectifique y así como proteger derechos fundamentales como el 15 y 20 de la CP.
[3] DPDP, Delegatura encargada de la protección de los datos de las personas que se hayan registrado en las SIC.
[4] RNBD. Directorio público de bases de datos sujetas a tratamiento en Colombia, administrada por las SIC.

iguales o superiores a 100.000 UVT y las entidades de naturaleza pública (ley 905 de 2004).

Limitar el registro de una base de datos ante la SIC bajo la existencia de una cantidad de activos por parte del ente de comercio que tratará dicha información, crea una brecha muy grande que excluye de la obligación de hacer este registro a entidades que no cuenten con los activos señalados, situación que además dificultaría la labor de la SIC para hacer un control de esa información, toda vez que muchas empresas no registrarían esos datos.

La información y datos personales son activos importantes para las empresas, situación que derivó en la necesidad de crear mecanismos para su protección (ley 1266 / 2008 y ley 1581 / 2012) y que no se convirtiera en un modelo de negocio que pusiera en riesgo bienes jurídicos y afectara a las persona que cedieron su información y que es tratada por diversas entidades del orden privado.

Frente a lo expuesto anteriormente las entidades privadas y en especial las financieras juegan un papel fundamental, quienes, con el fin de ofrecer servicios crediticios a clientes y potenciales clientes, adquieren por diferentes medios información de carácter privado de las personas para luego darles a conocer sobre productos y servicios a través de mensajes de texto, por correo electrónico, telefónico, en medios físicos mediante cartas, entre otros. Superintendencia de Industria y Comercio (2019).

Es preciso señalar que el sujeto activo (titular de la información) debe dar un consentimiento previo, expreso e informado para que sus datos sean tratados, tratamiento que debe ser única y exclusivamente para lo que esta persona ha indicado y no para fines distintos a lo expuesto en el documento donde da su autorización, documento además al cual el titular puede tener acceso en cualquier momento, ante esto se evidencia que debido al uso extensivo de las TIC[5] se ha ocasionado que frecuentemente los datos no sean tratados para lo cual fueron recolectados inicialmente afectando la intimidad, así como otros derechos y libertados, esto a través del tráfico de datos personales entre entidades sin las debidas medidas de seguridad que protejan a los titulares de la información. Superintendencia de Industria y Comercio. DPDP (2019).

Las entidades de carácter privado adquieren información de clientes y potenciales clientes por diferentes medios como lo son es en encuestas físicas y digitales, formularios físicos y digitales, cookies, redes sociales, vía telefónica entre otros, ante esta situación es preciso señalar que los encargados del tratamiento de esta información deben estar disponible en todo momento para que el titular pueda acceder a la información que se posee de él en sus bases de datos y no se pueden crear o fijar tiempos de permanencia de sus datos en dichas bases, además de ello si los encargados del tratamiento de la información desean realizar modificaciones o actualizaciones de la información debe solicitar un nuevo consentimiento del titular.

La transferencia de información almacenada en las bases de datos entre entidades privadas obtenidas mediante consentimientos de los titulares constituye violación a los expuesto en la ley 1266 de 2008 y 1581 de 2012 si no se solicita el consentimiento previo del titular de la información. Es además una violación grave a estas leyes el no contar o implementar las medidas necesarias de seguridad para salvaguardar la información que se les ha confiado por lo que su perdida,

[5] TIC. Tecnologías de la Información y la Comunicación.

adulteración, modificación implicaría poner el riesgo el bien jurídico tutelado en el artículo 269F y 269H del Código Penal, así como los derechos constitucionales fundamentales consignados en los Arts. 15 y 20 de la CP.

A corte 31 de diciembre de 2019, la DPDP, registró 6515 denuncias relacionadas con el uso de datos personales, donde se expidieron 379 órdenes de multas quedando 13 multas en firme. Superintendencia de Industria y Comercio. DPDT (2019).

Lo anterior nos permite realizarnos la siguiente pregunta orientadora ¿son eficaces las medidas tomadas por la SIC para proteger a las personas frente a las violaciones que se ven expuestos ante el uso indebido de sus datos por entidades privadas?

Ante lo expuesto anteriormente y con el ánimo de dar solución la pregunta planteada, desarrollaremos una investigación de tipo cualitativo – deductivo, acudiendo a consulta en bases de datos, doctrina, estadística, fuentes nacionales e internacionales enmarcadas en la gestión de datos personales.

Su desarrollo constará de 3 fases o momentos determinados donde la fase 1 consiste en dar a conocer en que consiste el tratamiento o gestión de datos personales en Colombia, dando a conocer cuál es la ley y su ámbito de aplicación y alcance, para pasar a la fase 2 haciendo un análisis de la ley, desde el punto de vista normativo, cuáles son las limitaciones y extralimitaciones en las entidades privadas frente al uso que estas hacen de los datos personales que poseen de sus clientes, para finalizar con la fase 3 donde se determinará si existen vacíos normativos que dan pie a que se genere la vulneración de los datos personales de los ciudadanos que han confiado sus datos personales a las entidades privadas para determinar seguidamente cuales con las acciones que toma la SIC para proteger a los ciudadanos cuando sus derechos son vulnerados así como paras sancionar a las entidades que violan la ley de protección de datos personales.

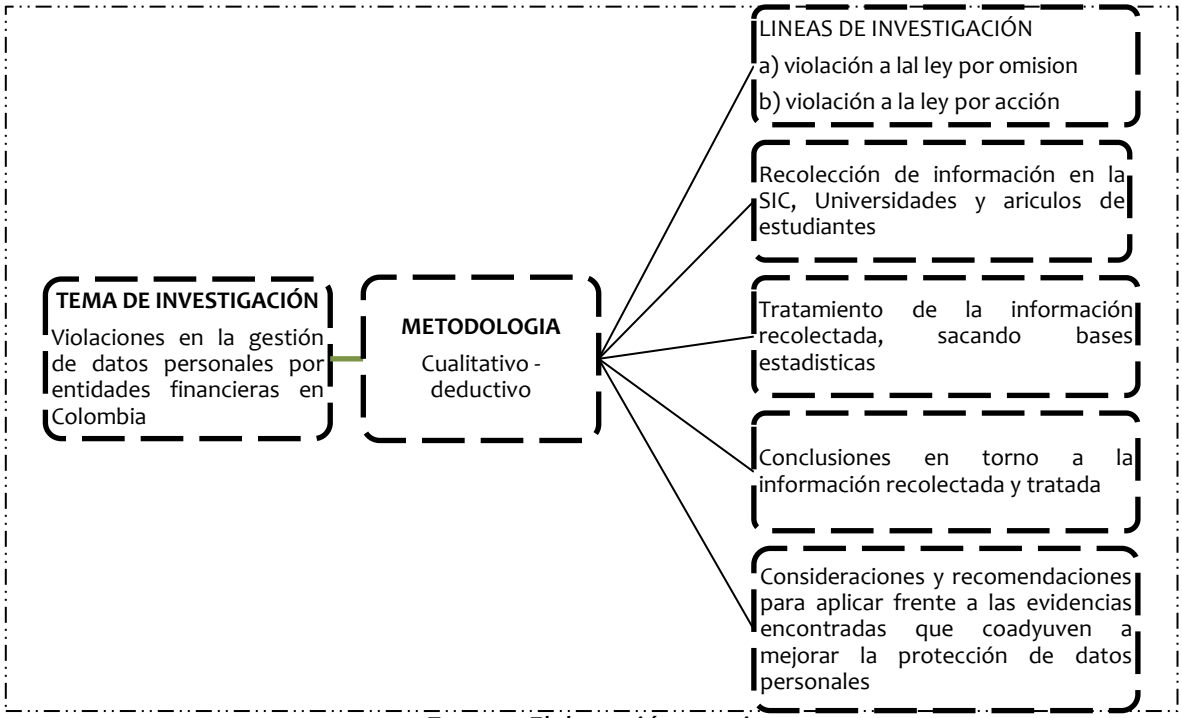
Marco normativo

El marco normativo que abarca este artículo se basa en la Constitución Política de Colombia de 1.991 en el Art. 15.2, y 20, así como por la ley 1266 de 2008, por medio de la ley 1273 de 2009, la cual trata de la información relacionada con datos financieros, aunado al bien jurídico añadido al Código Penal ley 599 del 2000 orientado a la protección los datos personales y la información, y la ley 1581 de 2012 cuya finalidad es proteger los datos personales apoyada del decreto Nacional 1377, decreto 090 del 2018 del Gobierno Nacional, ley 906 de 2004.

Método

La metodología a aplicar es desde un enfoque cualitativo – deductivo, esto en el entendido que se pretende recolectar información de medios digitales presente en las bases de datos de la SIC, universidades y artículos de publicaciones de estudiantes de pregrado hasta doctorado, con el propósito de conocer los estudios que se han adelantado en torno a la ley de protección de datos personales, contrastarla entre ellas y hacer un análisis que permita objetivamente establecer conclusiones sobre la eficacia de esta ley desde su implementación hasta la época actual orientado a la aplicación que las entidades privadas en Colombia dan a la misma.

Grafica 1. *Mapa conceptual del desarrollo de la investigación*



Fuente: *Elaboración propia*

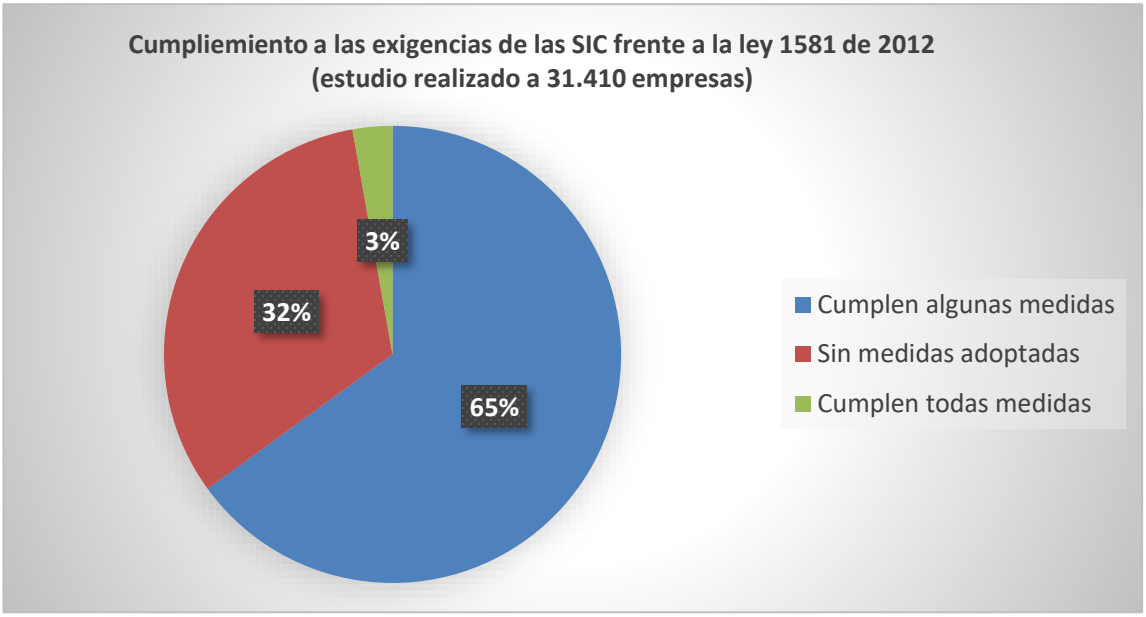
Resultados

1. Violación a la ley 1581 de 2012 por omisión en la gestión de datos personales

Para determinar si son eficaces las acciones tomadas por la SIC para proteger a las personas de las violaciones en el tratamiento de sus datos por parte de entidades privadas incluidas en estas las entidades financieras, se tomaron varias vías de acción siendo las más importantes la omisión por parte de estas al momento de proteger la información personal, donde se denotan vulnerabilidades en las medidas adoptadas para la protección de la información conferida, así como el uso abusivo o indebido por parte de las entidades al compartirla entre pares y divulgarla por diferentes medios, llegando al punto de contactar personas con fines distintos para los cuales le fueron entregados dichos datos personales.

Es por el ello, que con el propósito de salvaguardar la información personal de los ciudadanos residentes en Colombia, la SIC ha realizado diversas acciones tendientes mitigar y prevenir que se comentan violaciones por parte de entidades públicas y privadas, entre las medidas adoptadas está la verificación de las acciones tomadas a fin de evitar vulnerabilidades en las políticas de protección de datos y que pongan en riesgo los datos personales de sus usuarios, clientes y empleados, riesgos que van desde la adulteración, consulta, perdida hasta el uso fraudulento o acceso no acreditado a sus bases de datos. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDP (2019).

Grafica 2. *Cumplimiento a las exigencias de las SIC por entidades privadas en Colombia.*



Fuente: *Creación propia datos de la SIC 2019*

Mediante estudio presentado por la SIC en 2.019 donde se recolecto información de 32.763 empresas públicas y privadas, siendo 31.410 (95.8%) empresas privadas y se puedo establecer que existen grandes deficiencias en las acciones que adelantan las entidades para proteger los datos personales de quienes les han confiado esta información, estableciendo que el 65.5% (20.416) han cumplido con algunos de los requerimientos exigidos por la SIC en torno a la protección de la información, 884 han cumplido con todas las medidas necesarias y 10.110 de las empresas no han adoptado medidas para la protección de esta información. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

Entre las medidas que deben tomar las entidades se encuentra la (1) la creación de políticas especifica encaminada a regular el acceso a información sensible, (2) política para la protección frente al acceso remoto y consulta de información personal, (3) implementar sistemas de gestión de tratamiento y seguridad de la información personal (4) controles de seguridad al momento de tercerizar información personal.

Frente a lo anterior y teniendo en cuenta las 31.410 empresas privadas sometidas a consulta se detalla el grado de cumplimiento adoptado por las entidades a fin de propender por la seguridad de la información que le ha sido confiada.

a) En cuanto a las medidas de seguridad relacionadas con los datos de carácter personal que poseen (cumplimiento de un 48%). Se logró establecer que el 41% han documentado los procesos que llevan en su interior para proteger datos personales, el 49% cuenta con procesos y procedimientos para asignar responsabilidades a las personas que emitirán autorizaciones orientadas al tratamiento de datos personales, el 58% han generado pactos de confidencialidad quienes pueden acceder a los datos personales de clientes, usuarios y empleados, el 29% ha generado controles orientados a la seguridad al momento de tercerizar información personal, el 62% cuenta con documento aprobado que trate de la seguridad de la información. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

b) En cuanto a controles de acceso a información personal (cumplimiento 35.4%). Solo el 37% cuenta como procedimiento establecido para gestionar usuarios que puedan acceder a información personal, el 21% ha creado política concreta para determinar los parámetros de acceso a las bases de datos con información personal sensible, un 50% cuenta con copias de respaldo para garantizar plenamente la seguridad de las bases de datos, el 12% cuenta con políticas para ejecutar el acceso remoto a datos personales y el 57% a diseñado políticas de acceso y control a información personal en instalaciones físicas y por medios técnicos o tecnológicos. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

c) En lo atinente a la seguridad en los sistemas de información personal (cumplimiento21.5%). Aquí el 38% ha implementado controles de seguridad a fin de evitar la perdidas o fugaz de información al momento de realizar cambios o modificaciones en sus plataformas digitales, solo un 17% cuenta con procedimientos implementados para la auditoria de los sistemas donde poseen información personal que han recolectado, el 16% hace un monitoreo permanente de la información que poseen en bases de datos y un 15% implemento procedimientos donde fijen las especificaciones y requisitos de seguridad que deben tener en cuenta con los sistemas de información personal. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

d) Para el procesamiento de información personal (cumplimiento 33.6%). En lo atinente a este acápite el 31% tiene procedimientos para validar datos de ingreso y gestión de información personal, para que los datos recolectados y sujetos a tratamiento sean verídicos y pertinentes, el 26% posee controles para validar datos que salen de sus entidades, 24% ha diseñado políticas para el intercambio de información por medios físicos y digitales, el 39% ha creado procedimientos específicos para la supresión o eliminación de información personal y un 485 ejecuta políticas para la debida recolección, tratamiento, circulación y supresión de información. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

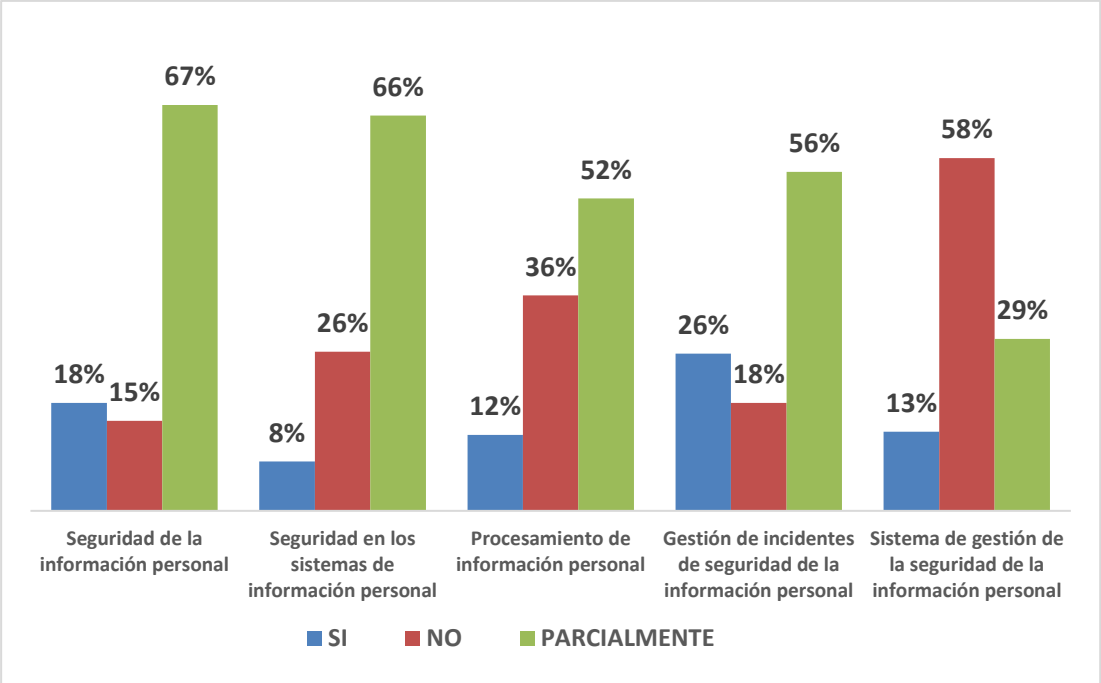
e) Frente a la seguridad de la información frente a incidentes (cumplimiento 32%). El 26% ha generado políticas para la seguridad de la información cuando se detectan vulnerabilidades o vulneraciones en sus sistemas de información y el 38 % creó políticas para gestión de incidentes de seguridad y proteger las bases de datos donde existe información personal sensible. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

Tabla 1. *Medidas de seguridad adoptadas por entidades privadas para la protección de datos personales*

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES			
PREGUNTA	SI	NO	PACIALMENTE
Seguridad de la información personal	5615(18%)	4679(15%)	21116(67%)
Seguridad en los sistemas de información personal	2575(8%)	8277(26%)	20558(66%)
Procesamiento de información personal	3957(12%)	11203(36%)	16250(52%)
Gestión de incidentes de seguridad de la información personal	8170(26%)	5610(18%)	17630(56%)
Sistema de gestión de la seguridad de la información personal	4116(13%)	18353(58%)	8941(29%)

Fuente: *Elaboración propia con base en datos de la SIC 2019*

Grafica 3. *Medidas de seguridad adoptadas por entidades privadas para la protección de datos personales en Colombia*



Fuente: *Creación propia datos de la SIC 2019*

Los datos mostrados en la gráfica, permite evidenciar el bajo índice de medidas de seguridad que poseen las entidades para proteger la información que posee de los ciudadanos quienes de buena fe han brindado sus datos a fin de que sean tenidos en cuenta para que les brinden información de productos y servicios y que por la falta de control de estas entidades podrían terminar siendo objeto de acciones delictivas (extorsión, adquisición fraudulenta de servicios o productos crediticios, etc.) por parte de personas que puedan sustraer sus datos.

Se evidencia que el mayor grado de vulnerabilidad se centra en la seguridad de los sistemas que han dispuesto para para contener o guardar la información recolectada, seguido del tratamiento que dan

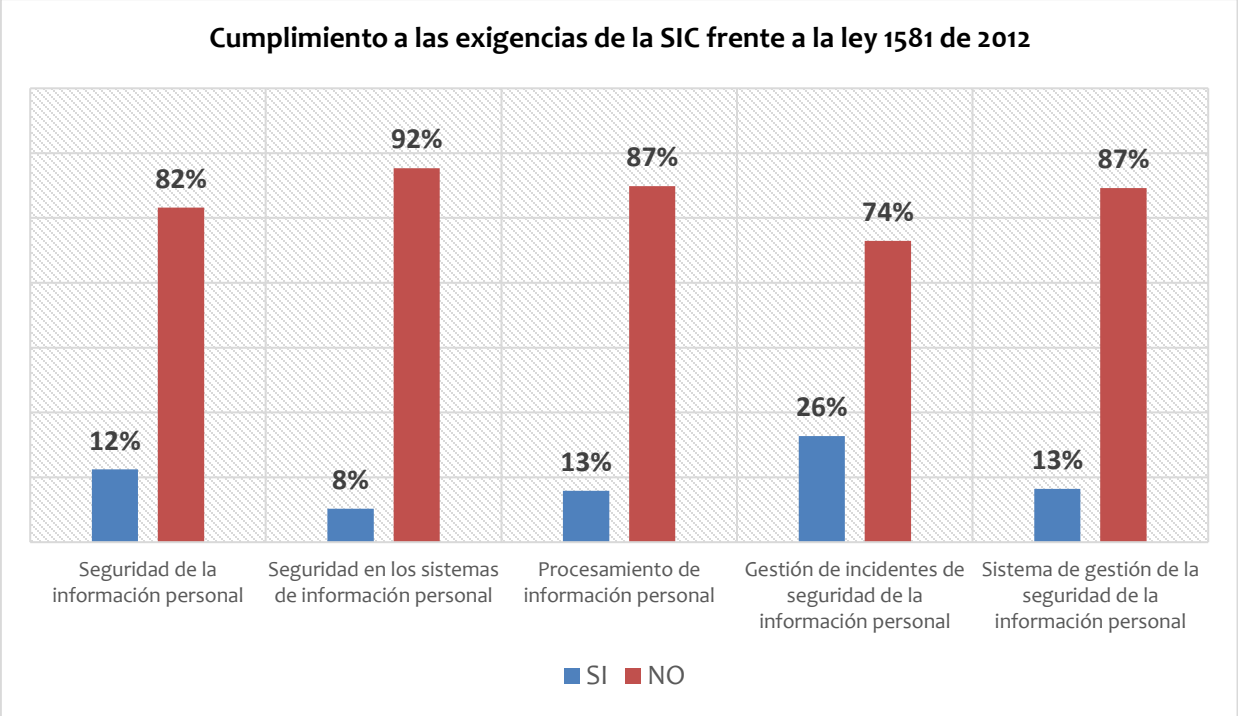
a esta información y un aspecto muy importante a tener en cuenta son las pocas acciones correctivas que toman luego que se ven expuestos a vulneraciones en sus sistemas de información.

Tabla 2. *Cumplimiento a las Exigencias de las SIC frente a la ley 1582 de 2012*

CUMPLIMIENTO A LAS EXIGENCIAS DE LA SIC FRENTE A LA LEY 1581 DE 2012		
PREGUNTA	SI	NO
Seguridad de la información personal	5615(18%)	25795(82%)
Seguridad en los sistemas de información personal	2575(8%)	28835(92%)
Procesamiento de información personal	3957(13%)	27453(87%)
Gestión de incidentes de seguridad de la información personal	8170(26%)	23240(74%)
Sistema de gestión de la seguridad de la información personal (SG-SIP)	4116(13%)	27294(87%)

Fuente: *Elaboración propia con base en datos de la SIC 2019*

Grafica 4. *Cumplimiento a las exigencias de las SIC por entidades privadas en Colombia frente a la ley 1581 de 2012*



Fuente: *Creación propia datos de la SIC 2019*

En lo que concierne a las exigencias que realiza las SIC para que se adopten acciones tendientes a la seguridad de la información personal, se establece que son casi nulas las medidas que toman las empresas para proteger los datos que estas recopilan y que están obligados a proteger frente a los diversos factores de riesgo electrónico y físicos que se pueden presentar, donde los sistemas de información cuentan con pocas medidas de seguridad que permitan proteger los datos, aunado al inadecuado tratamiento que hacen de la información recolectada la cual puede ser duplicada,

eliminada sin cumplir una política específica para ello o sustraída y teniendo en cuenta que no cuentan con un sistema de gestión de seguridad de la información no podrían establecer con claridad quien, como y cuando tuvieron perdidas de información personal de sus bases de datos. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

Teniendo en cuenta que las entidades no cuentan con UN SG-SIP, estas no evidencian las fugas de información o accesos no autorizados a las mismas, razón por la cual no advierten a las autoridades competentes de estos hechos y a los titulares de la información a fin de que se tomen las medidas necesarias que permitan que no sean objeto de hechos fraudulentos que quedan realizar con su información y que afecte su intimidad personal buen nombre y hasta su patrimonio. SIC. Estudio de medidas de seguridad en el tratamiento de datos personales. DPDT (2019).

2. Violación a la ley 1581 de 2012 por acción indebida e inadecuada en el tratamiento de los datos personales

Las bases de datos se han convertido a lo largo de los años en un activo para las empresas, toda vez que permite el contacto directo con clientes y potenciales clientes por medio de la utilización de correos electrónicos, contactos telefónicos, toda esta información que generalmente se encuentra sistematizada se desplaza a una velocidad incalculable a través de diferentes medios de comunicación y tecnológicos, razón por la cual los administradores de estos datos deben de propender cuente con el debido cuidado, custodia, garantía y seguridad.

Con los avances de esta nueva era sé a establecido que existen diferentes métodos para franquear sistemas de seguridad donde se encuentren almacenados bases de datos almacenados por empresas y que el acceso no autorizado a estos poner en riesgo los derechos fundamentales que busca proteger la ley 1581 de 2012, es por ello que las empresas deben implementar políticas claras para la protección de los datos personales y poder proteger dicha información por medio de un SG-SIP evitando de este modo perjuicios futuros a los titulares de la información.

Las empresas privadas incluidas las entidades financieras recurren a la recolección de información por diferentes fuentes a fin de tener un mayor acercamiento con clientes y poderles informar de los diferentes productos y servicios con los que cuentan, así como novedades que se vayan generando, situación que también adoptan con potenciales clientes quienes brindan sus datos con el propósito de estar enterados si hay algún producto o servicio que le atraiga y pueda acceder en el futuro.

La buena fe de las personas que brindaron esta información a las empresas se ve quebrantada cuando de manera arbitraria quienes poseen sus datos personales los contactan para ofrecerles servicios que ellos no han requerido o convenido un contacto previo para atender dicha oferta, convirtiéndose esta práctica en una violación a la ley en comento.

Ante lo expuesto en el párrafo anterior se conoce que las empresas recurren a diferentes practicas indebidas que van en contravía a la ley de protección de datos personales como lo es el intercambio de base de datos de información de clientes entre empresas, obtener información personal sin su previo consentimiento, extraviar, suprimir o alterar los consentimientos para el tratamiento de datos personales, contactar clientes con fines distintos para los cuales fueron recolectados sus datos, no rectificar la información que poseen de sus clientes aun con previa solicitud del titular de la información, etc.

Estas violaciones a la ley han originado que la SIC, adelante investigaciones contra dichas entidades que han permitido que de 2014 a 2019 se hayan emitido 94 sanciones económicas ejemplarizantes contra estas entidades y más de 500 sanciones que tratan de llamados de atención encaminados a la corrección o rectificación malas prácticas en la aplicación de la ley de protección de datos personales.

Tabla 3. *Violaciones a la ley 1581 de 2012 periodo 2014 – 2019*

VIOLACIONES A LA LEY 1581 DE 2012 PERIODO 2014 – 2019						
	2014	2015	2016	2017	2018	2019
No ejecutar el principio de seguridad	1	0	1	0	1	1
No conservar copia de la autorización ni informar de su finalidad	3	4	7	8	17	3
No atender solicitudes de supresión del dato o revocatoria de la autorización	0	0	3	2	7	5
No conservar la información en condiciones de seguridad necesarias	1	2	3	0	3	2
No adoptar política de tratamiento de la información y aviso de privacidad	0	0	0	1	4	2
No acatar los requerimientos efectuados por la SIC	0	0	0	2	1	1
No atender consultas y reclamos presentados por el titular	5	1	0	3	4	0

Fuente: *Elaboración propia con base en datos de la SIC 2019*

Grafica 5. *Violaciones a la ley 1581 de 2012 periodo 2014 - 2019*

Fuente: *Creación propia datos de la SIC 2019*

La violación más frecuente a la ley ha sido la de no informar a los titulares de la información la finalidad para la cual es recolectada y almacenada su información en bases de datos, seguida de la inobservancia al deber de atender las solicitudes que realizan los titulares de la información para que sus datos sean suprimidos o rectificados y la falta de respuesta a las PQRS que se generan.

El no conservar la copia de la autorización que emite el titular de la información, así como el no informarle en debida forma para que serán usados los datos recolectados es la violación mas frecuente desde el año 2014, donde se evidencia un incremento progresivo de este ítem pasando de tres casos anuales a llegar a 17 casos sancionados en el 2018, lo que advierte de la vulneración que cometen las entidades privadas contra los ciudadanos que suministran la información.

3. *Acciones adelantadas contra entidades financieras en el periodo 2016 - 2020*

Mediante solicitud realizada a la SIC se pudo tener acceso a información detallada y concreta de las acciones que esta entidad ha adelantado contra entidades financieras que han vulnerado el tratamiento de datos personales, estableciéndose lo siguiente:

✓ A corte 15 de noviembre de 2020, se han sancionado entidades crediticias en las cuales se han vulnerado los siguientes artículos de la Ley 1581 de 2012, "Régimen General de Protección de Datos Personales".

- Artículo 8, literal e.
- Artículo 9
- Artículo 9, numeral 1
- Artículo 4, literal a
- Articulo 12
- Artículo 12, literal a
- Artículo 17, literales a, b, c, d, g, j, k, n, o.

✓ A corte 15 de noviembre de 2020, se han sancionado las siguientes 31 entidades crediticias por el mal uso de datos personales.

1. Renovar financiera S.A.S
2. Recuperadora y cobranzas S.A.
3. Asegúrate fácil LTDA
4. Bancolombia S.A.
5. Central de inversiones S.A. C.I.S.A.
6. Star seguros VIP LTDA
7. Banco falabella S.A.
8. Fundación de la mujer
9. Entidad promotora de salud servicio occidental de salud S.A. SOS
10. Grupo reddial S.A.S.
11. Cooperativa multiactiva de profesionales -SOMEC
12. Credivalores - Crediservicios S.A
13. Banco popular S A
14. Scotiabank Colpatria S.A

15. Renovar financiera S.A.S
16. Cooperativa de los profesionales Coasmedas
17. Refinancia S.A.S.
18. Refinancia S.A.S.
19. Refinancia S.A.S.
20. Refinancia S.A.S.
21. Crear país S.A.
22. Cobranza nacional de creditos S.A.S.
23. Créditos & avales sociedad anónima simplificada sigla Crediavales S A S
24. Promotora de inversiones y cobranzas S.A.S
25. Serlefin BPO&O Serlefin S.A.
26. Global Center Ilec S.A.S.
27. Negocios estratégicos globales S.A.S.
28. Services & consulting S.A.S.
29. Service & Consulting S.A.S.
30. Servicio integrado de ventas S.A.S. - Servivente S.A.S.
31. Zamora Global Internacional SAS

✓ A corte 15 de noviembre de 2020, se tienen 363 quejas y se han realizado 1570 solicitudes de explicaciones a entidades del sector crediticio, para un total de 1933 procesos que se adelantan contra entidades que posiblemente están vulnerando la Ley 1266 de 2008 y la Ley 1581 de 2012.

✓ Las ciudades donde existen entidades con mayor índice de vulneración al tratamiento de datos personales son:

Bogotá D.C
Medellín
Barranquilla
Cali.

4. Medidas adoptadas para proteger a las personas ante las violaciones más frecuentes

La SIC por medio de la delegatura para la protección de tratamientos de datos personales cumple con la función de promoción y divulgación de estrategias encaminados proteger a los ciudadanos ante la vulneración a sus datos personales, quienes unidos con la Oficina de Servicios al Consumidor y Apoyo Empresarial (OSCAE) realizan capacitaciones sobre la protección de datos personales a entidades públicas y privadas, universidades y cámaras de comercio realizando hasta el momento la capacitación de 32.879 personas, en 432 eventos en distintas ciudades.

Estas capacitaciones se realizan también virtualmente, adicionalmente se llevó a cabo un congreso internacional donde se contó con la participación de 1,700 personas, es de resaltar que la información sobre el debido tratamiento que se debe dar a los datos personales se encuentra plasmado en diferentes cartillas físicas y digitales elaboradas por la SIC la cual está disponible para personas naturales y jurídicas.

✓ Las siguientes son las principales acciones que ha realizado por la SIC para proteger a las personas frente a las vulneraciones que realizan las entidades privadas incluidas las entidades crediticias y/o

financieras con el tratamiento de sus datos personales:

1. Se han elaborado 76 formulaciones de cargos.
2. Se han requerido 1570 solicitudes de explicaciones.
3. Se han proferido 31 sanciones administrativas.
4. Se han emitido 1548 órdenes por vulneración a la Ley 1266 de 2008 y 204 órdenes por vulneración a la Ley 1581 de 2012.
5. Se han analizado y archivado 1160 quejas.
6. A la fecha se encuentran en trámite 363 procesos administrativos (quejas) que posiblemente podrían estar vulnerando el régimen general de protección de datos personales.
7. Se han realizado visitas administrativas a sociedades que prestan servicios de crédito con el fin de analizar el cumplimiento de la Ley 1581 de 2012 y la Ley 1266 de 2008.

✓ A la fecha la sanción más ejemplarizante, es la proferida contra SCOTIABANK COLPATRIA S.A, mediante Resolución No. 10720 de 11 de marzo de 2020 por un monto de $356.070.000, por la vulneración de las disposiciones contenidas en el literal b) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal c) del artículo 4 de la misma Ley, el artículo 9 ejúsdem, y el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015.

5. Discusión

Frente al problema planteado en este artículo, se logró identificar que diversos grupos investigativos entre ellos los integrados por académicos y estudiantes a nivel local y en el exterior, han tratado de determinar si las entidades encargadas de la salva guarda de la información personal que se les ha confiado realizan las actividades necesarias tendientes a garantizar la protección de dicha información y si estas medidas han sido eficaces para cumplir con esa función.

En Colombia la SIC, teniendo en cuenta los resultados que se ilustraron en la gráfica No 5, permite evidenciar la poca operatividad de la entidad al momento de realizar medidas sancionatorias ejemplarizantes contra las entidades privadas que violan la ley de protección de datos personales, evidenciándose que desde 2014 a 2019 se realizaron 7, 7, 14, 16, 37, y 14 sanciones anual respectivamente, para un total de 98 sanciones en u lapso de 6 años, lo cual es un porcentaje mínimo frente a la cantidad de quejas y demandas que se presentan contra las distintas entidades del sector privado por la vulneración a los derechos fundamentales 15 y 20 de la carta magna.

Las entidades que vulneran los derechos fundamentales ya mencionados, realizan este tipo de acciones sistemáticamente debido a la inocua sanción que reciben la cual generalmente se trata de correcciones en sus sistemas de información frente a la persona vulnerada o violentada, la supresión de datos o una rectificación de la información, situación que para estas entidades es algo trivial frente al daño que ocasionaron o el que pudieron generarle al titular de la información.

Con los avances tecnológicos y la trasmisión de datos incluidos en estos los datos personales, se evidencia la vulnerabilidad que existe en un gran porcentaje de las entidades privadas al momento de proteger los datos que obtienen de sus usuarios, empleados o clientes, donde la fragilidad de sus bases de datos permite que sus sistemas de información sean violentados y la información sustraída, alterada, secuestrada o eliminada, poniendo en riesgo a los titulares de la información frente a terceros, siendo

necesario en este sentido una exigencia a dichas entidades para que procuren tomar medidas que permitan mitigar el acceso de personas no autorizadas a sus bases de datos

Aunque la SIC realice campañas orientadas a la sensibilización de las empresas para que en estas se tomen medidas que protejan a los titulares de la información que ellos poseen, es preciso indicar que estos no acatan o cumplen a cabalidad con las instrucciones impartidas por la entidad encargada de su vigilancia y control, razón por la cual a pesar que se evidencian grandes cantidades de capacitaciones de manera virtual y presencial, así como la entrega de elementos físicos (cartillas) y publicaciones web con información relacionada con la protección de datos personales, el número de quejas y demandas cada vez va en aumento porque no se aplican al interior de la empresas las ordenes emitidas por la SIC frente a esta problemática.

6. Recomendaciones

La SIC debe propender porque las empresas que vayan a registrar sus bases de datos en esta entidad cuenten con una política ya implementada para la correcta protección de dicha información, esto con el fin de garantizar que desde el momento del registro de la información ya se cuente con la protección de la misma.

Incentivar a que los titulares de la información realicen las respectivas quejas, denuncias o demandas cuando se les vulneren sus derechos concernientes a los que busca proteger la ley 1581 de 2012, obteniendo de esta manera información más clara y precisa de las entidades que cometen esta violación, el tipo de violación, su frecuencia y aplicar medidas más severas y que no sea solo una simple corrección del daño causado a sus clientes, usuarios o empleados.

No limitar el registro de bases de datos a un factor patrimonial del ente económico, debido a que esto da pie a que muchas bases de datos no sean registradas ante la SIC y se cometan violaciones contra titulares de la información y que no se posea registro y control de estos hechos para la aplicación de una efectiva sanción.

7. Conclusiones

En el ordenamiento jurídico colombiano el tratamiento de los datos personales fue incluido como derecho fundamental, que goza de protección constitucional y que permite el disfrute de la vida íntima, al igual que otros derechos fundamentales como lo es el de la dignidad humana. Constitución Política de Colombia (Art. 15 y 20).

Colombia posee un amplio componente normativo orientado a la protección de datos personales aquí encontramos la ley 1266 de 2008 para el habeas data financiero, ley 1581 de 2012 con su decreto reglamentario 1377 de 2013 con todo lo atinente con los datos personales y el tratamiento de que deben dar a estos los responsables de su tratamiento y custodia.

Por medio de la ley 1581 de 2012 y con su decreto 1377 de 2013, se indican los mecanismos cuales son los mecanismos de seguridad más idóneos para la recolección, tiramiento y circulación de los datos personales de los titulares de la información, permitiendo a los titulares de esta tener un control más preciso de donde está su información y para que esta siendo utilizada.

La ley 1266 de 2008 se mostró insuficiente para garantizar y proteger de forma efectiva y adecuada los derechos fundamentales de los numerales 15 y 20 consignados en la carta magna, notándose la trasgresión sistemática a estos derechos a pesar de la promulgación, divulgación y aplicación de esta ley.

Debido a las sanciones que aplica la SIC a las entidades que violan la ley de protección de datos personales, estas deberían ser más severas a fin de evitar que dichas vulneraciones se sigan presentando, toda vez que estas empresas al notar la poca afectación que reciben versus los hechos que cometen, sopesan las cargas y evidencian que se encuentran en ventaja frente a los titulares de la información, ya que el ser sancionados (llamado de atención), se limitaran a cumplir la exigencia de la SIC sin mayor o ninguna afectación (económica o restrictiva de su objeto social).

Las empresas no están cumpliendo con lo que se les ha encomendado por parte de la SIC para la protección de los datos personales, observándose que muy pocas cumplen con las políticas adecuadas de recolección de datos personales y el tratamiento de los mismos, esto en el entendido que no informan a los titulares de la información el fin de dicha recolección de datos, dan información parcial sobre el uso que le darán a estos o en el peor de los casos son usados con fines distintos para los cuales fueron obtenidos y sus sistemas de protección de datos no cuentan con la seguridad necesaria para proteger a los titulares de la información.

Las empresas deben implementar sistemas de seguridad que garanticen la protección de la información personal que se les confía, a fin de evitar perjuicios para los titulares de la información en la violación de sus derechos fundamentales o hasta su patrimonio y para ellas mismas por la omisión en la protección de los datos.

Con la implementación del principio de responsabilidad demostrada inmerso en el decreto 1377 de 2013, se garantiza que las empresas implementen políticas de protección de datos personales a fin de prevenir que se presenten violaciones a la ley y vulneraciones a la intimidad de los titulares de la información.

Se concluye luego de la revisión de la información estadística obtenida que existen sanaciones pero estas en su mayoría se limitan a la corrección o rectificación posterior a la violación de la ley, razón por la cual no son elevadas las sanciones ejemplarizantes contra las entidades que violan la ley de protección de datos personales lo que permite determinar que aun con la existencia de una ley creada para sancionar la vulneración de un Derecho la SIC es ineficaz en sus acciones para que dicha violación no se siga presentando.

Referencias bibliográficas

Dialnet (2020). Protección de datos personales. Recuperado de: https://dialnet.unirioja.es/buscar/documentos?querysDismax.DOCUMENTAL_TODO=proteccion+de+datos+personales+colombia

Superintendencia de Industria y Comercio SIC (2020). Boletín Jurídico. Recuperado de: https://www.sic.gov.co/sites/default/files/boletin-juridico/Resoluci%C3%B3n%20n%C3%BAmero%201292%20de%202020.pdf

Superintendencia de Industria y Comercio SIC (2020). La autorización para el tratamiento de datos personales. Recuperado de: https://www.sic.gov.co/boletin/juridico/habeas-data/la-autorizaci%C3%B3n-para-el-tratamiento-de-datos-personales-debe-ser-previa-expresa-e-informada-los-responsables-y-encargados-del-tratamiento-de-datos-personales

Superintendencia de Industria y Comercio SIC (2020). Boletín Jurídico. Recuperado de: https://www.sic.gov.co/boletin/juridico/habeas-data/una-base-de-datos-puede-contener-diversa-clase-de-informaci%C3%B3n-y-utilizarse-para-m%C3%BAltiples-prop%C3%B3sitos-cuando-ello-sucede-est%C3%A1-dentro-del-%C3%A1mbito-de-aplicaci%C3%B3n-de-las-leyes-1266-de-2008-y-1581-de-2012

Superintendencia de Industria y Comercio SIC (2020). Boletín Jurídico. Recuperado de: https://www.sic.gov.co/boletin/juridico/habeas-data/son-contrarios-la-ley-1581-de-2012-los-acuerdos-de-confidencialidad-que-fijen-un-tiempo-para-mantener-la-reserva-de-la-informaci%C3%B3n-de-los-titulares

Superintendencia de Industria y Comercio SIC (2020). Boletín Jurídico. Recuperado de: https://www.sic.gov.co/sites/default/files/boletin-juridico/Res%2076538%20del%2027XII2019%20Aseg%C3%BArate%20F%C3%A1cil%20Ltda.pdf

Superintendencia de Industria y Comercio SIC (2020). Boletín Jurídico. Recuperado de: https://www.sic.gov.co/boletin/juridico/habeas-data/cambios-sustanciales-en-pol%C3%ADtica-de-tratamientos-de-datos-personales

Código Penal Colombiano. Ley 906 de 2004 (2006).

Universidad Catolica (2018). Protección de Datos Personales. Recuperado de: https://repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Protecci%C3%B3n%20De%20Datos%20En%20Colombia.pdf

Universidad del Rosario (2018). Política de tratamiento de datos personales.

Superintendencia de Industria Y comercio DPDT (2019). Recuperado de https://www.sic.gov.co/content/estudio-de-medidas-de-seguridad-en-el-tratamiento-de-datos-personales-2019.

Superintendencia de Industria Y comercio. Guía para el tratamiento de datos personales (2019). Recuperado de https://issuu.com/quioscosic/docs/guia_sic_tratamiento_datos_personales_comercioelec

Universidad del Rosario (2019) Política de tratamiento de datos personales.

Dialnet (2017) Mecanismos de protección de datos personales.