

ESTADO DE IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS EN 100 EMPRESAS REPRESENTATIVAS DE LOS SECTORES PÚBLICO Y PRIVADO DE CALI

State of implementation of the data protection law in 100 representative companies from public and private sectors in Cali

Cristhian Alcalde Mejía¹
Cristian.alcalde00@usc.edu.co

Ciro Antonio Dussán Clavijo, MGE²
Ciro.dussan00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de Sistemas (1)
Universidad Santiago de Cali, Facultad de Ingeniería, Docente Programa de Ingeniería de Sistemas (2)

Resumen

Actualmente debido a la era tecnológica la información se ha convertido en un activo muy importante para las empresas por los beneficios que se pueden obtener del análisis de la misma, en razón a la gran cantidad de datos personales, privados y sensibles que pueden llegar a afectar los derechos fundamentales de las personas, los gobiernos del mundo han tomado la iniciativa de crear leyes tendientes a la protección de esta información, conocida como ley de protección de datos. En este artículo hablaremos sobre la ley de protección de datos de Colombia (Ley 1581 del 2012) y sobre el estado de implementación de la misma en 100 empresas representativas de la Ciudad de Cali, de lo cual se logró concluir que el 82% de la muestra cumplen con la implementación de esta ley, demostrando una implementación considerable en materia de la ley de protección de datos sobre la muestra representativa tomada de Cali, Colombia.

Palabras Clave: ley de protección de datos; SIC; ley 1581 de 2012; información sensible; Cali; Colombia.

Abstract

Currently, due to the technological era, information has become a very important asset for companies due to the benefits that can be obtained from its analysis, due to the large amount of personal, private and sensitive data that may affect the fundamental rights of people, the governments of the world have taken the initiative to create laws aimed at protecting this information, known as the data protection law. In this article we will talk about the data protection law of Colombia (Law 1581 of 2012) and about the state of its implementation in 100 representative companies of the city of Cali, from which it was concluded that 82% of the sample complies with the implementation of this law, demonstrating a considerable implementation regarding the data protection law on the representative sample taken from Cali, Colombia.

Keywords: Data protection law, SIC; Law 1581 of 2012; sensitive information; Cali; Colombia.

1 INTRODUCCIÓN

La tecnología ha evolucionado a un ritmo acelerado en los últimos años, actualmente nos encontramos en una era tecnológica la cual hace parte de nuestro diario vivir, en la que el manejo e intercambio de datos personales se han tornado en una práctica cotidiana causando que las personas pierdan conciencia sobre los riesgos que implica el análisis masivo de datos sobre sus derechos fundamentales, por lo tanto el gobierno de Colombia ha realizado un gran esfuerzo referente a la protección de datos y privacidad por medio la ley 1581 del 2012 (Silva, Solano, Fernandez, Romero, & Vargas Villa, 2019).

El estado de la implementación de la ley 1581 del 2012 (Protección de Datos Personales) en la ciudad de Cali,

Colombia es el eje central de este artículo, por lo tanto empezaremos hablando sobre la ley de protección de datos de Colombia y su contexto (Sección: 1.1), luego hablaremos sobre las características y generalidades de esta ley (Sección: 2), pasaremos a explicar el control establecido por la Superintendencia de Industria y Comercio para verificar el cumplimiento de esta ley, el cual se realiza por medio del Registro Nacional de Bases de Datos (RNBD) (Sección: 3), basado en lo anterior se realizó la toma de una muestra de empresas las cuales estuviesen inscritas en la Cámara de Comercio de Cali y que su Unidad de Valor Tributario (UVT) fuese mayor a 100.000, sin embargo por el alcance de este proyecto se limitó la muestra a 100 empresas representativas de los sectores público y privado (Sección: 4). La implementación de la ley en la muestra representativa sera analizada en la (Sección: 5). Y mostraremos las conclusiones de este artículo en la (Sección: 6).

El estado ha asignado a la Superintendencia de Industria y Comercio como ente regulador de dicha ley. Los datos personales son utilizados para actividades relacionadas, como las ventas y servicios. Esta información se ha convertido en un bien permanentemente comercializado en el mercado nacional e internacional y en un insumo diario de los sistemas de información privados y del estado, generando nuevos riesgos para las personas (Rojas Bejarano, 2014), por ende, los entes gubernamentales han establecido leyes, normas y procedimientos con la finalidad de buscar un debido tratamiento de la información que se encuentra en las bases de datos. En Colombia se ha procurado establecer leyes que regulen la materia en sentido amplio y general. Cabe resaltar que las entidades públicas y privadas que superan los 100.000 UVT, se encuentran en la obligación de salvar guardar los datos personales que recolectan en sus bases de datos, y respetar los derechos establecidos en la ley a los titulares de los datos (Registro Nacional de Bases de Datos, s.f.).

1.1 Ley de protección de datos

La ley de protección de datos de Colombia proviene de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, referente a la protección de las personas en lo que respecta al tratamiento de los datos personales y a la libre circulación de los mismos (Parlamento Europeo y del Consejo, 1995), sus inicios en Colombia fueron a partir de la ley 1266 Habeas Data de diciembre de 2008, a lo que posteriormente se reconoció la ley 1273 de delitos informáticos en el 2009 y la ley 1581 de 2012 de protección de datos (Silva, Solano, Fernandez, Romero, & Vargas Villa, 2019).

Se reconoce una aplicabilidad en las organizaciones, en el cual identifica diferentes autorizaciones recibidas de la empresa por parte del titular, en el cual debe caracterizarse por ser previa, expresa e informada por parte del titular, determinando una base de datos, en el que identifique la información que se genera al interior de la empresa; los datos personales, que reconoce todos aquellos datos que se asocia a personas naturales; responsable, que se caracteriza por ser aquella persona natural o jurídica que decide que se puede realizar con esos datos; el encargado, reconocido como aquella persona natural o jurídica que hace el tratamiento de esos datos como en el caso del manejo por parte de Recursos humanos, mercadeo o sectores tecnológicos; tratamiento, reconocido como toda aquella operación realizada sobre los datos.

Es fundamental reconocer los deberes y derechos por parte del titular, en el cual, conoce, actualiza y rectifica los datos, solicitando prueba de autorización otorgada, identificando el derecho de ser informado por el responsable y el encargado; obteniendo el derecho de revocar la autorización o solicitar la suspensión; presentar quejas ante Superintendencia de industria y comercio (SIC).

Se tiene en cuenta el artículo 15 de la Constitución Política de Colombia, en el que hace referencia a que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, además tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en entidades públicas y privadas (Constitución Política de Colombia, 1991, art. 15, s.f.).

Al momento de identificar las responsabilidades por parte de las empresas, se debe reconocer las garantías de los derechos de Habeas Data, solicitud de copia de autorización, información acerca de la finalidad del manejo de datos, conservación bajo seguridad, considerado un tema importante que obliga a la empresa obtener seguridad sobre esos datos y sobre la forma como los está administrando; las empresas deben garantizar la veracidad e integridad, siendo parte de los principios fundamentales de la información que es la integridad, confidencialidad, disponibilidad, identificando la veracidad en los datos; rectificar, reconocido al momento en el que se presente algún cambio frente a esos datos (Cabric,

2015); suministrar responsabilidad al encargado; exigir al encargado seguridad; tramitar consultas y reclamos; adoptar políticas y controles, que deben ser claras y oportunas para garantizar la seguridad; informar al titular y la SIC frente a casos presentados en el interior; y por último reconocer el cumplimiento ante requerimientos SIC en un determinado momento (Dinero, 2017).

Se debe registrar o realizar gestión a los reclamos y tramites presentados por parte del titular; encargado de informar o señalar los datos que han sido objeto de un incidente o algún reclamo para darle una información indicada sobre el proceso que se presente en un momento dado ya sea en términos judiciales o en términos administrativos, teniendo claridad sobre los datos e incidentes generados; abstenerse de circular información; cuidar de accesos no autorizados; informar a la SIC de problemas de seguridad y cumplir con los requerimientos que exige la SIC.

El riesgo es alto frente al incumplimiento de esta ley por parte de las compañías, es relevante tener en cuenta el artículo 23 de la ley 1581 del 2012 la cual indica que la SIC podrá imponer las siguientes sanciones (Ley 1581 de 2012, s.f.):

- Multas de carácter personal e institucional 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.
- Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.
- Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.
- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

Cabe resaltar que las sanciones indicadas en la ley 1581 del 2012 sólo aplican para las personas de naturaleza privada. En el evento en el cual la SIC advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la Norma, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Ante lo anterior, se determina la protección de datos personales como un derecho constitucional, la raíz de protección de datos de Colombia es la constitución (Departamento Nacional de Planeación, s.f.), donde se reconocen 2 normas fundamentales:

- Ley 1266 de 2008: Protección Habeas Data Financiero, supervisión crediticia
- Ley 1581 de 2012: Se establece régimen general de protección de datos personales.

A partir de la ley 1581, se generan facultades a la SIC para sancionar conductas con respecto al régimen de protección de datos personales general, imposición de multas, generación de facultades, principios de seguridad demostrada, creando una cultura de protección de datos en el país.

Se reconocen dos tipos de agentes según la ley que manejan estos datos personales, que son:

- Los responsables: Tiene la disponibilidad sobre los datos personales, quien recolecta y utiliza esa información para un fin determinado.
- El encargado: Es a quien se le ofrece la base de datos para que siga las instrucciones del responsable.

El caso con mayor relevancia por incumplimiento de la ley 1581 en Colombia es hacia la compañía LINIO COLOMBIA S.A. la cual sufrió una sanción monetaria por valor de \$ 351.558.900 de pesos equivalente a cuatrocientos cincuenta (450) salarios mínimos legales mensuales vigentes, cabe resaltar que dicha sanción fue emitida bajo la resolución 83882 de 2018 la cual representa su cuarta sanción económica hacia la compañía, la sumatoria de las sanciones nos lleva a un valor aproximado de \$ 1.000.000.000 de pesos, de acuerdo la resolución 83882 de 2018 dicha sanción se produjo por la solicitud de un ciudadano que en reiteradas veces se dirigió a la compañía LINIO COLOMBIA S.A. para que no se le

enviara información publicitaria y eliminarlo de sus base de datos, a lo que la compañía hizo caso omiso tomando el ciudadano la decisión de reportarlo contra el ente regulador de la ley 1581 en Colombia la SIC (Ministerio de Comercio, Industria y Turismo, Resolución 83882, 2018).

En la ciudad de Santiago de Cali también se han presentado algunas sanciones por parte de la SIC, a compañías tales como Conexión Corporativa Cali S.A.S. a la cual se le impuso sanción económica por valor de \$ 48.689.322 pesos equivalente a 66 salarios mínimos legales mensuales vigentes que se encuentra descrita en la resolución 21360 de 2017 (Ministerio de Comercio, Industria y Turismo, Resolución 21360, 2017), por vulnerar los principios y deberes descritos en la ley 1581 del 2012 contra los ciudadanos y Cosmocentro Ciudadela Comercial PH que también recibió una sanción económica por parte de la SIC en este caso por un monto de \$ 30.800.000 pesos, equivalentes a 50 salarios mínimos legales vigentes bajo la resolución 36901 de 2014 por el tratamiento indebido de datos de menores de edad violando sus derechos. Las sanciones más comunes impuestas por la SIC son monetarias afectando los ingresos y reputación de las compañías que incumplen de alguna forma la ley 1581 (Ministerio de Comercio, Industria y Turismo, Resolución 36901, 2014).

Es por esto, que se deben tomar acciones de supervisión efectiva frente a la protección de datos, a través de las diferentes entidades privadas en el caso de Cali, donde permita destacar las disposiciones normativas, dando cumplimiento a lo dispuesto en la Ley 1581 de 2012, en especial en su artículo 17, así como al artículo 13 del Decreto Reglamentario 1377 de 2013 referentes a las obligaciones de los responsables de tratamiento de datos personales y a la generación de las Políticas de Tratamiento de la información, garantizando a los titulares de la información las herramientas y procedimientos para establecer un control sobre su información personal, favoreciendo los derechos de consulta, acceso, rectificación, actualización y supresión de los datos correspondientes a información personal que haya sido recolectada en cualquier base de datos o archivo.

Las entidades privadas de la ciudad de Cali cuyo objetivo fundamental es la formación centrada en el desarrollo regional y Nacional, deben reconocer el compromiso en salvaguardar la seguridad y confidencialidad de los Datos Personales recolectados de sus integrantes, proveedores y en general de la comunidad empresarial (Mendoza Morales, 2015), respetando siempre los derechos otorgados a los mismos en términos de la Corte Constitucional en la cual señala, de manera general, que:

“La función de administrar una base de datos debe fundamentarse en los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad”. Concretamente, ha precisado que los administradores deben:

- Obtener previamente la autorización de la persona cuyos datos se pretende incluir en la base
- Notificar a la persona sobre la inclusión de sus datos en el banco e informarle que va a reportar su información en una base de datos con miras a que el titular pueda desde un comienzo ejercer sus derechos de rectificación y actualización
- Actualizar permanente y oficiosamente la información para que ésta sea veraz, completa y no se omitan factores que pueden cambiar el buen nombre de la persona
- Eliminar de oficio la información negativa que ha caducado con el paso del tiempo
- Indemnizar los perjuicios causados por la falta de diligencia o por posibles fallas en el manejo, tratamiento o administración de datos personales
- Garantizar el derecho de acceso, actualización y corrección.

Estos derechos implican que el ciudadano tenga “la posibilidad de saber en forma inmediata y completa, cómo, por qué y dónde aparece cualquier dato relacionado con él”; si la información es errónea o inexacta, el individuo puede solicitar, con derecho a respuesta también inmediata, que la entidad responsable del sistema introduzca en él las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar sus derechos fundamentales vulnerados”.

Finalmente, la Corte ha precisado que, por regla general, “no puede recolectarse información sobre datos “sensibles” como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación”.

2 GENERALIDADES

2.1 Legislación aplicable y ámbito de aplicación

Se reconoce la aplicación del tratamiento de los datos personales recolectados en las entidades privadas de Cali y se ha redactado teniendo en cuenta:

- Constitución Política de Colombia, artículo 15 y 20.
- La Ley 1266 de 2008 contentiva de las disposiciones generales del HABEAS DATA.
- La Ley 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales” y el Decreto 1377 de 2013 “por el cual se reglamenta parcialmente la ley 1581 de 2012”.
- El Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

2.2 Definiciones

Las siguientes definiciones son tomadas del marco normativo y posibilitan una correcta y apropiada interpretación de la presente política:

- Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- Aviso de privacidad: comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- Base de datos: conjunto organizado de datos personales que sea objeto de tratamiento.
- Causahabiente: persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).
- Dato personal: cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse a una persona natural o jurídica.
- Dato público: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- Datos sensibles: 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.
- Datos indispensables: se entienden como aquellos datos personales de los titulares imprescindibles para llevar a cabo la actividad de la entidad. Los datos de naturaleza indispensable deberán ser proporcionados por los titulares de los mismos o los legitimados para el ejercicio de estos derechos.
- Datos opcionales: son aquellos datos que la entidad requiere para ofrecer servicios de promoción, formación o información, etc.

- Encargado del tratamiento: persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
- Ley de protección de datos: es la Ley 1581 de 2012 y sus Decretos reglamentarios o las normas que los modifiquen, complementen o sustituyan.
- Habeas data: derecho de cualquier persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en el banco de datos y en archivos de entidades públicas y privadas.
- Responsable del tratamiento: persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, decida sobre la base de datos y/o Tratamiento de los datos.
- Titular: persona natural cuyos datos personales sean objeto de Tratamiento.
- Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- Transferencia: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
- Transmisión: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable (Superintendencia de Industria y Comercio, Sobre la protección de datos personales, s.f.).

2.3 Principios

En el desarrollo, interpretación y aplicación de la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y las normas que la complementan, modifican o adicionan, se aplicarán de manera armónica e integral los siguientes principios rectores:

- Principio de la legalidad: el Tratamiento de datos es una actividad reglada que debe sujetarse a lo establecido en la ley y las demás disposiciones que la desarrollen.
- Principio de finalidad: el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular. En lo correspondiente a la recolección de datos personales, nombre institución se limitará a aquellos datos que sean pertinentes y adecuados para la finalidad con la cual fueron recolectados.
- Principio de libertad: el tratamiento solo puede ejercerse con el consentimiento previo, expreso, e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- Principio de veracidad o calidad: la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- Principio de transparencia: en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- Principio de acceso y circulación restringida: el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.
- Principio de seguridad: la información sujeta a tratamiento por las entidades privadas se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Principio de confidencialidad: Las entidades privadas están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley (Ley 1581 de 2012, s.f.).

2.4 Legitimación para el ejercicio del derecho del titular

Los derechos de los titulares establecidos en la Ley podrán ejercerse por las siguientes personas:

- Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición las entidades privadas de la Ciudad de Cali.
- Por los causahabientes del titular, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.

3 REGISTRO NACIONAL DE BASE DE DATOS

El Registro Nacional de Base de datos (RNBD), es el sistema de control utilizado por la Superintendencia de Industria y Comercio (SIC) que cuenta con un directorio público de las bases de datos personales, sujetas a tratamientos que operan en el país, acorde con lo establecido con la ley 1581 de 2012 (Cámara de Comercio de Cali, Protección de Datos Personales en Colombia, 2017), régimen general de protección de datos personales de Colombia. Se identifica la inscripción al RNBD de las personas jurídicas de naturaleza privada y las sociedades de economía mixta; a su vez se habilita la inscripción para las personas naturales y las entidades públicas diferentes a las sociedades de economía mixta (Registro Nacional de Bases de Datos, s.f.).

A través de la Ley 1581 de 2012, Régimen General de Protección de Datos Personales de Colombia, se creó RNBD, el cual, el Gobierno Nacional a través del capítulo 26 del Decreto Único 1074 de 2015 (Decreto 1074 del 2015), reglamentó la información mínima que debe contener en dicho registro. Lo anterior, constituye un avance importante para Colombia en materia de Protección de Datos Personales por cuanto a través de dicha figura, se pretende dar protección al derecho a la intimidad y a la información de las personas (Galvis Cano, 2012), lo cual se encuentra igualmente protegido desde la Constitución Política de Colombia como derecho fundamental.

Dentro de los antecedentes del habeas data se encuentra la intervención de la Corte Constitucional en el que determina que es el derecho a obtener información personal en alguna base de datos, el cual implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismos y tener la facultad de corregirlos y/o suprimirlos; buscando así la protección de la intimidad de las personas debido a la creciente utilización de información personal de personas naturales en bases de datos (Chaparro Ronderos, 2014), por parte de la administración pública, entidades financieras, educativas, profesionales y por parte de las personas en el ejercicio del comercio o cualquier otra actividad. Este derecho permite que las personas no pierdan el control sobre su propia información, como también sobre su uso; por lo tanto, la normativa vigente basándose de su facultad, incorpora obligaciones exigibles a todas las personas y entidades de cualquier naturaleza que recopilan y tratan información buscando no solo la protección de este derecho, sino al derecho de la intimidad, el buen nombre, derecho a la privacidad entre otros, rigiéndose por principios de lealtad y de legitimidad con relación a la finalidad para lo que se recolecta los datos.

4 MUESTRA PARA EL ANÁLISIS DE LA IMPLEMENTACIÓN DE LA LEY 1581 EN CALI

Para el análisis de la implementación de la ley 1581 del 2012 en Cali, cabe mencionar que esta ley solo aplica para las empresas públicas y aquellas privadas que cumplan con las siguientes características:

- Empresas inscritas en la Cámara de Comercio de Cali.

- Empresas cuyo valor en activos superen las 100.000 Unidades de Valor Tributario (UVT).

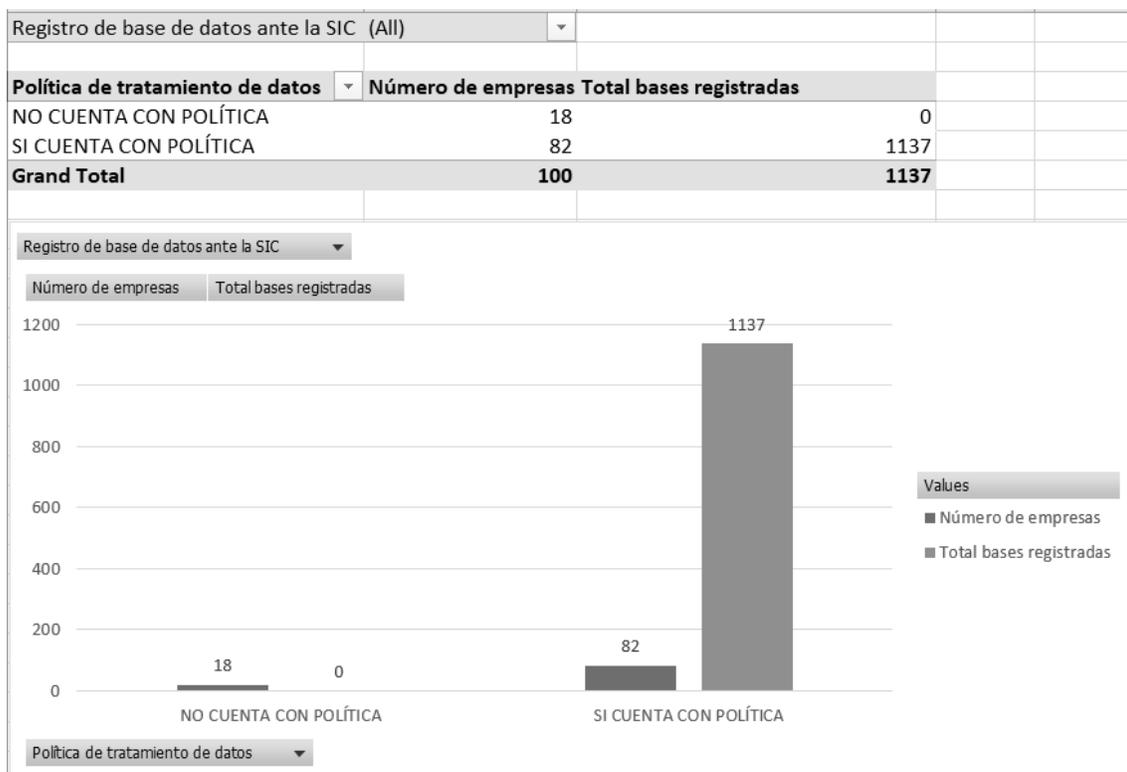
Debido al alcance de este proyecto se limitó la muestra a 100 empresas representativas de los sectores público y privado de la ciudad, de las cuales se realizó la debida verificación de cada una con respecto a las características antes mencionadas, esta verificación se llevó a cabo por medio de la información brindada por la entidad eInforma, la cual es una marca de Informa Colombia S.A. Líder en el mercado de suministro de información comercial, Financiera y de Marketing de empresas colombianas, perteneciente al Grupo Informa D&B (Informa Colombia S.A., s.f.).

5 ANÁLISIS DE LA MUESTRA

Las compañías cada día adquieren más activos algunos de mayor valor e importancia que otros, esto requiere de la implementación de controles robustos para evitar el robo o fuga de información de las empresas. En el 2018 el valor agregado de los activos reportados por las empresas que renovaron su registro mercantil ante la Cámara de Comercio de Cali ascendió a COP 154,2 Billones, con un aumento del 5.1% con respecto al año 2017, esto nos indica que las compañías adquieren una mayor responsabilidad frente al cuidado de sus activos de información (Cámara de Comercio de Cali, Ritmo Empresarial Informe #19, 2019).

De acuerdo a la investigación realizada sobre el estado de implementación de la ley 1581 del 2012 - protección de datos personales, en 100 empresas representativas de los sectores público y privado de Cali se procedió a realizar la verificación que dichas compañías contaran con registros de sus bases de datos frente a la Superintendencia de industria y comercio (SIC) y que tuviesen una política de tratamiento de datos personales. Según los datos recolectados se logró evidenciar que de las 100 empresas escogidas, 18 empresas equivalente a 18% no cuentan con una política de tratamiento de datos personales de las cuales 16 no se han registrado ante la SIC y 2 si cuentan con el registro pero no tiene bases de datos a su nombre, por otro lado 82 de las 100 empresas equivalentes al 82% de la muestra si cuentan con una política de tratamiento de datos y han registrado por lo menos una (1) base de datos RNBD ante la SIC, la suma de las bases registradas del 82% de las empresas es de 1137 bases (ver: Figura 1).

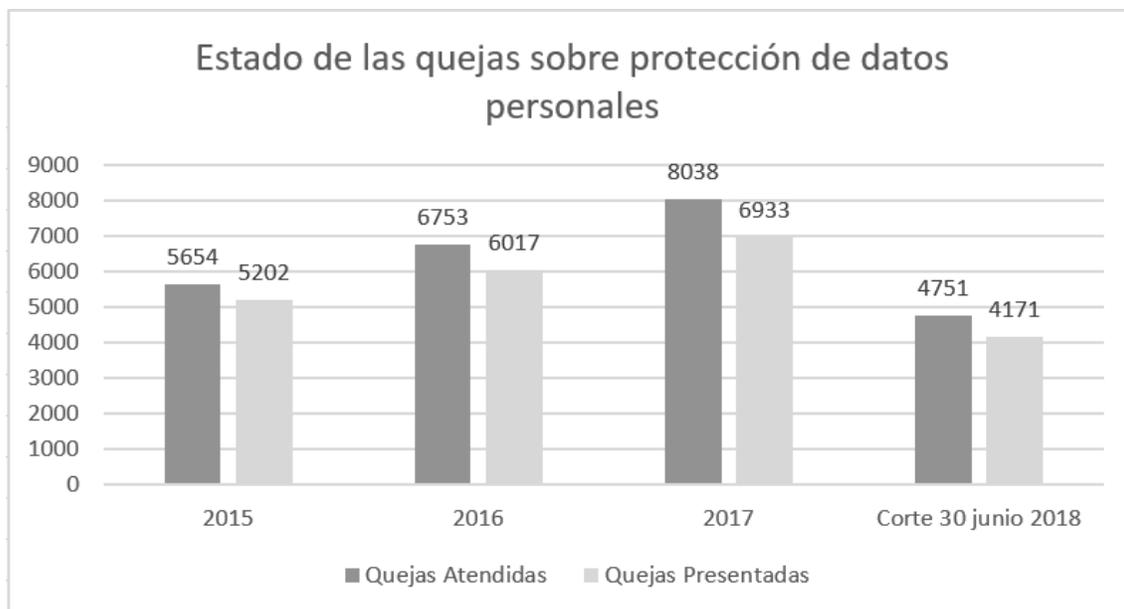
Figure 1. Registro nacional de base de Registro nacional de base de datos ante la SIC por empresas de la ciudad de Cali



Fuente: Elaboración Propia.

Actualmente la Delegatura para la Protección de Datos Personales, recibe un promedio de quinientas (500) quejas a nivel nacional al mes y, desde la creación de la Delegatura en el 2012, la cantidad de denuncias recibidas anualmente ha incrementado gradualmente (ver: Figura 2), esto debido a que la protección de los datos y el cumplimiento de la ley toman una mayor relevancia en el país por ende la entidad encargada la SIC realiza monitoreos y aplica controles que le ayuden a la mejora continua, como se evidencia en este grupo de Datos (Superintendencia de Industria y Comercio, Quejas presentadas v/sus atendidas 2015 a 2017 y parte 2018 Delegatura para la Protección de Datos Personales, s.f.).

Figure 2. Quejas presentadas versus atendidas a nivel nacional 2015 a 2017 y parte 2018 Delegatura para la Protección de Datos Personales



Fuente: Elaboración Propia.

De acuerdo a datos obtenidos de la SIC y publicados por el gobierno, se puede evidenciar el Registro Nacional de Bases de Datos – RNBD - es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos (Superintendencia de Industria y Comercio, Registro Nacional de Bases de Datos 2016 y 2017, 2019).

En el marco del RNBD, en este grupo de Datos se evidencia el cumplimiento de las personas jurídicas por zonas, siendo Bogotá, seguido de Antioquia y Valle del Cauca, las que más han realizado el Registro de sus Bases de Datos en el año 2017, Valle del Cauca con un crecimiento del 3.4% con respecto al año 2016 (ver: Figura 3).

Figure 3. Registro Nacional de Bases de Datos 2017.



Fuente: Elaboración Propia.

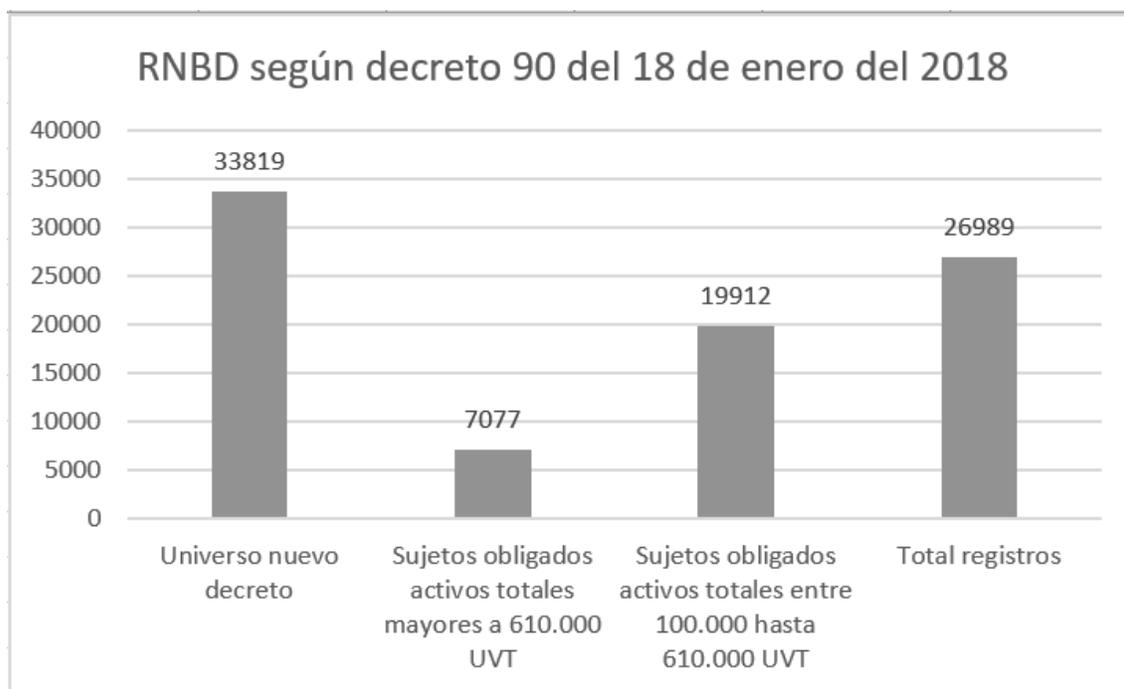
Mediante Decreto 90 del 18 de enero de 2018, el Gobierno Nacional modificó el ámbito de aplicación del Registro Nacional de Bases de Datos y creo unos nuevos plazos para que los sujetos que resulten obligados realicen la inscripción de sus bases de datos, los sujetos que continúan con el deber de registrar sus bases de datos son las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100 mil Unidades de Valor Tributario (UVT) y las entidades de naturaleza pública (ver: Figura 4).

Los plazos establecidos para realizar el registro de las bases de datos son tres:

- El primero de ellos es para las sociedades y entidades sin ánimo de lucro que tengan activos por más de 610.000 UVT, que deberán registrar sus bases de datos a más tardar el 30 de septiembre de 2018.
- El segundo plazo es para las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100.000 y hasta 610.000 UVT, quienes tendrán plazo de realizar el registro hasta el 30 de noviembre de 2018.
- Por último, el tercer plazo corresponde a las entidades públicas, quienes tendrán plazo para registrar sus bases de datos hasta el 31 de enero de 2019.

Las bases de datos que se creen con posterioridad al vencimiento de los plazos ya mencionados, deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación (Superintendencia de Industria y Comercio, Registro Nacional de Bases de Datos según decreto 90 del 18 de enero de 2018, s.f.).

Figure 4. Registro Nacional de Bases de Datos según decreto 90 del 18 de enero de 2018



Fuente: Elaboración Propia.

Posterior a la aplicación del nuevo decreto se evaluaron los resultados con cifras recolectadas en junio del 2018, se puede establecer que el nivel de cumplimiento por parte de los sujetos obligados a cumplir el decreto se extiende a un 80% del universo con un total de registros de 26.989.

6 CONCLUSIONES

En conclusión, este artículo nos muestra la importancia de implementación de la ley 1581 del 2012 de protección de datos en Colombia, debido a la importancia que tiene la información y al gran valor que representan para las personas y la información sensible que puede llegar a ser comprometida, por lo tanto, esta información debe permanecer custodiada, protegida y que se garantice la seguridad de la información (Buitrago Botero, 2016).

El Registro Nacional de Bases de Datos (RNBD) es el control por el cual se puede verificar el cumplimiento de la implementación de la ley de protección de datos ya que este registro está sujeto a la inscripción de las bases de datos y políticas de cada entidad las cuales son evaluadas y confirmadas por la SIC.

El gran valor que tiene la información está generando que las compañías creen políticas empresariales para salvaguardar la integridad, la confidencialidad y la disponibilidad de la misma (Cabarique Álzate, Salazar Romana, & Quintero Barco, 2015), lo cual se vio evidenciado en la (Figura 1) donde el 82% de las empresas tomadas en la muestra cuentan con la política de tratamiento de la información.

Según la firma global de abogados DLA Piper el estado de implementación de esta ley en Colombia es moderado (Piper, s.f.), por lo que se puede evidenciar el trabajo realizado por el Gobierno de Colombia hasta el momento en materia de ley de protección de datos y su cumplimiento en las compañías, sin embargo, debido al aumento gradual de las denuncias recibidas por temas relacionados a la protección de datos personales (Figura 2), se puede concluir que se requiere un mayor compromiso por parte de los entes designados y las compañías obligadas a cumplir con la ley 1581 del 2012, con el fin de mejorar en este aspecto.

7 REFERENCIAS

- Silva, J., Solano, D., Fernandez, C., Romero, L., & Vargas Villa, J. (2019). Privacy Preserving, Protection of Personal Data, and Big Data: a Review of the Colombia Case. *Procedia Computer Science*, 151, 1213-1218. doi:<https://doi.org/10.1016/j.procs.2019.04.174>
- Buitrago Botero, D. M. (2016). El valor de los datos personales en Colombia. *Revista CES Derecho*, 7, 1-2. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2145-77192016000100001&lng=en&tlng=en
- Cabarique Álzate, W. A., Salazar Romaña, C. A., & Quintero Barco, Y. A. (2015). Factores y causas de la fuga de información sensibles en el sector empresarial. *Cuaderno Activa*, 7(7), 67-73. Obtenido de <http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/249>
- Cabric, M. (2015). Chapter 11 - Confidentiality, Integrity, and Availability,. En M. Cabric, *Corporate Security Management* (págs. 185-200). Butterworth-Heinemann. doi:<https://doi.org/10.1016/B978-0-12-802934-3.00011-1>
- Cámara de Comercio de Cali. (Junio de 2017). Protección de Datos Personales en Colombia. *Revista Acción*(193). Obtenido de https://www.ccc.org.co/categoria_articulo/proteccion-datos-personales-colombia/
- Cámara de Comercio de Cali. (2019). *Ritmo Empresarial Informe #19*. Cali: Cámara de Comercio de Cali. Obtenido de <https://www.ccc.org.co/inc/uploads/2019/01/Ritmo-Empresarial-N19.pdf>
- Chaparro Ronderos, M. F. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. *INVENTUM*, 32-37. doi:<https://doi.org/10.26620/uniminuto.inventum.9.17.2014.32-37>
- Constitución Política de Colombia, 1991, art. 15. (s.f.). *Artículo 15*. Recuperado el 1 de Julio de 2019, de Constitución Política de Colombia: <http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15>
- Corte Constitucional de Colombia. (s.f.). *Sentencia C-748/11*. Recuperado el 1 de Junio de 2019, de Corte Constitucional: <http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>
- Decreto 1074 del 2015. (s.f.). *Decreto 1074*. Recuperado el 1 de Julio de 2019, de Presidencia: <http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201074%20DEL%2026%20DE%20MAYO%20DE%202015.pdf>
- Departamento Nacional de Planeación. (s.f.). *Protección de datos personales*. Recuperado el 1 de Junio de 2019, de Departamento Nacional de Planeación: <https://www.dnp.gov.co/programa-nacional-del-servicio-al-ciudadano/Paginas/Proteccion-de-datos-personales.aspx>
- Dinero. (31 de 1 de 2017). *¿Hasta qué punto es legal el uso que le dan las empresas a sus datos personales?* Obtenido de Dinero: <https://www.dinero.com/empresas/articulo/ley-de-proteccion-de-datos-personales-y-el-uso-por-empresas/241498>
- Galvis Cano, L. (2012). Protección de datos en Colombia, avances y retos. *Lebret*, 195-214. doi:<https://doi.org/10.15332/rl.v4i4.336>
- Informa Colombia S.A. (s.f.). *informa*. Recuperado el 1 de Junio de 2019, de <https://directorio-empresas.einforma.co/localidad/cali/>
- Ley 1581 de 2012. (s.f.). *Ley 1581 de 2012*. Recuperado el 1 de Junio de 2019, de Función Pública: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Mendoza Morales, J. (2015). *Protección de datos personales en Colombia*. Obtenido de Unimilitar: <http://hdl.handle.net/10654/7650>
- Ministerio de Comercio, Industria y Turismo. (30 de Mayo de 2014). *Resolución 36901*. Obtenido de Superintendencia de Industria y Comercio: http://www.sic.gov.co/sites/default/files/files/Res%20No_%2036901%20de%202014-%20COSMOCENTRO.pdf

- Ministerio de Comercio, Industria y Turismo. (20 de Abril de 2017). *Resolución 21360*. Obtenido de Superintendencia de Industria y Comercio: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2017021360RE000000001.pdf.
- Ministerio de Comercio, Industria y Turismo. (15 de Noviembre de 2018). *Resolución 83882*. Obtenido de Superintendencia de Industria y Comercio: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/Resolucion83882de2018.pdf
- Parlamento Europeo y del Consejo. (24 de 10 de 1995). *Directiva 95/46/CE del Parlamento Europeo y del Consejo*. Recuperado el 1 de Junio de 2019, de WIPO: <https://wipolex.wipo.int/es/text/313009>
- Piper, D. (s.f.). *Data Protection Laws Of The World*. Recuperado el 1 de Junio de 2019, de DLA PIPER: <https://www.dlapiperdataprotection.com/>
- Registro Nacional de Bases de Datos. (s.f.). *Registro Nacional de Bases de Datos*. Recuperado el 1 de Junio de 2019, de Superintendencia de Industria y Comercio: <http://www.sic.gov.co/registro-nacional-de-bases-de-datos>
- Rojas Bejarano, M. (2014). Evolución Del Derecho De Protección De Datos Personales En Colombia Respecto A Estándares Internacionales. *Novum Jus: Revista Especializada En Sociología Jurídica Y Política*, 8(1), 107-139. doi:<http://dx.doi.org/10.14718/NovumJus.2014.8.1.6>
- Superintendencia de Industria y Comercio. (Mayo de 2019). *Registro Nacional de Bases de Datos 2016 y 2017*. Obtenido de Datos Abiertos Gobierno de Colombia: <https://www.datos.gov.co/Comercio-Industria-y-Turismo/Registro-Nacional-de-Bases-de-Datos-2016-y-2017/x54j-ffxv>
- Superintendencia de Industria y Comercio. (s.f.). *Quejas presentadas v/ sus atendidas 2015 a 2017 y parte 2018 Delegatura para la Protección de Datos Personales*. Recuperado el Mayo de 2019, de Datos Abiertos Gobierno de Colombia: <https://www.datos.gov.co/Comercio-Industria-y-Turismo/Quejas-presentadas-v-sus-atendidas-2015-a-2017-y-p/rsmm-xj97>
- Superintendencia de Industria y Comercio. (s.f.). *Registro Nacional de Bases de Datos según decreto 90 del 18 de enero de 2018*. Recuperado el Mayo de 2019, de Datos Abiertos Gobierno de Colombia: <https://www.datos.gov.co/Comercio-Industria-y-Turismo/Registro-Nacional-de-Bases-de-Datos-seg-n-decreto-/gpcc-k67c>
- Superintendencia de Industria y Comercio. (s.f.). *Sobre la protección de datos personales*. Recuperado el 1 de Junio de 2019, de Superintendencia de Industria y Comercio: <http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>