

**RECOMENDACIONES PARA EL ADECUADO CUMPLIMIENTO DEL RÉGIMEN GENERAL
DE TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LAS INSTITUCIONES DE
EDUCACIÓN PREESCOLAR, BÁSICA Y MEDIA.**

ANDRES MAURICIO GRAJALES CUELLAR

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE ABOGADO

DIRECTOR: SANTIAGO DUSSAN LAVERDE

FACULTAD DE HUMANIDADES Y CIENCIAS SOCIALES

CARRERA DE DERECHO

SANTIAGO DE CALI

2021

Resumen

La protección de datos personales es un tema que en Colombia se ha desarrollado progresivamente. Así, con la expedición de la Ley 1581 de 2012 se dispusieron los aspectos generales en materia de tratamiento de datos personales, sin embargo, los Responsables del tratamiento de datos personales deben dar cumplimiento al régimen general de protección de datos personales atendiendo la naturaleza propia de cada organización. El presente artículo busca proponer lineamientos para las Instituciones de Educación Preescolar, Básica y Media que implementen un programa de cumplimiento en materia de protección de datos personales, teniendo como principal referente la doctrina existente de la Superintendencia de Industria y Comercio frente al cumplimiento de dicho régimen por parte de dichas instituciones. Para ello, se realiza en primer lugar un análisis del marco jurídico sobre tratamiento de datos personales; luego se analizan las particularidades regulatorias propias de la ley general de educación en virtud del principio de responsabilidad demostrada que exige adaptar el cumplimiento a la naturaleza jurídica de las organizaciones Responsables; también, se analizarán las resoluciones sancionatorias que la Superintendencia de Industria y Comercio ha expedido en contra de Instituciones Educativas por incumplimiento al régimen general de datos personales, para identificar las principales acciones y omisiones que acarrearán incumplimiento de este régimen; y así, finalmente, se concluye el presente trabajo con la proposición de recomendaciones que son referencia para las Instituciones de Educación Preescolar, Básica y Media al momento de implementar un programa de cumplimiento del régimen general de protección de datos personales.

Palabras clave: Instituciones Educativas, Datos Personales, Datos Sensibles, Datos privados, Ley de Protección de Datos, Principio de Responsabilidad Demostrada, Tratamiento de Datos, Responsable y Encargados.

Abstract

The protection of personal data is an issue that has developed progressively in Colombia. Thus, with the issuance of Law 1581 of 2012, the general aspects regarding the processing of personal data were established, however, those Responsible for the processing of personal data must comply with the personal data protection regime, taking into account the nature of each organization. This article seeks to propose guidelines for Preschool, Basic and Secondary Education Institutions that implement a compliance program regarding the protection of personal data, having as the main reference the existing doctrine of the Superintendency of Industry and Commerce regarding compliance with said institutions. . To do this, first an analysis of the legal framework on the processing of personal data is carried out; then the regulatory peculiarities of the Institutions of Preschool, Basic and Secondary Education are analyzed by virtue of the principle of demonstrated responsibility that requires adapting compliance to the legal nature of the responsible organizations; Also, the sanctioning resolutions that the Superintendency of Industry and Commerce has issued against Educational Institutions for non-compliance with the general personal data regime will be analyzed, to identify the main actions and omissions that lead to non-compliance with this regime; and thus, finally, the present work is concluded with the proposal of recommendations that are a reference for the Institutions of Preschool, Basic and Secondary Education at the moment of implementing a program of compliance with the general regime of protection of personal data.

Keywords: Educational Institutions, Personal Data, Sensitive Data, Private Data, Data Protection Law, Principle of Accountability, Data Processing, Responsible and Managers.

INTRODUCCIÓN	6
OBJETIVOS	12
OBJETIVO GENERAL	12
OBJETIVOS ESPECÍFICOS	12
1. CAPÍTULO I. MARCO JURÍDICO DE TRATAMIENTO DE DATOS PERSONALES EN COLOMBIA	13
1.1. Antecedentes Constitucionales relativos a la protección de datos personales	13
1.2. Ley 1266 de 2008	15
1.3. Ley Estatutaria 1581 de 2012	17
1.4. Decreto 1377 de 2013	22
1.5. Decreto Único Reglamentario 1074 de 2015	23
2. CAPÍTULO II. ASPECTOS REGULATORIOS DE LA LEY GENERAL DE EDUCACIÓN QUE TIENEN INCIDENCIA EN EL CUMPLIMIENTO DEL RÉGIMEN GENERAL DE TRATAMIENTO DE DATOS PERSONALES POR LAS IEPBM	24
2.1. Conceptualización del principio de responsabilidad demostrada	24
2.2. Aspectos regulatorios del sector educativo para las Instituciones de Educación Preescolar, Básica y Media relevantes para el tratamiento de datos personales.	27
2.2.1. Etapas de formación: Educación Preescolar, Básica y Media	28
2.2.2. Aspectos relacionados a la prestación del servicio educativo	29
2.2.3. Organizaciones al interior de las IEPBM	31
3. CAPÍTULO III: PRONUNCIAMIENTOS DE LA SIC PARA DETERMINAR EL INCUMPLIMIENTO DEL RÉGIMEN GENERAL DE TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LAS INSTITUCIONES EDUCATIVAS	33
3.1. Pronunciamientos de la SIC relativos al tratamiento de datos personales en el sector educativo	33
3.2. Aspectos relevantes comunes tenidos en cuenta por la SIC para determinar el incumplimiento del régimen de tratamiento de datos personales	36

3.2.1. Derechos de los niños, niñas y adolescentes y los datos de carácter sensible	36
3.2.2. Deber de solicitar y conservar autorización previa, expresa e informada por parte del Titular y de informar debidamente la finalidad del tratamiento	38
3.2.3. Deber de conservar la información bajo las condiciones de seguridad y de garantizar la reserva de la información	40
3.2.4. Deber de contar con las políticas de tratamiento de datos y de informar a los Titulares sobre su existencia	42
3.2.5. Deber de adoptar un manual interno de políticas y procedimientos para el tratamiento de datos personales (deber de tramitar consultas y reclamos formulados por los Titulares)	43
4. CONCLUSIONES: RECOMENDACIONES PARA EL EFECTIVO CUMPLIMIENTO DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LAS INSTITUCIONES DE EDUCACIÓN PREESCOLAR, BÁSICA Y MEDIA	46
4.1. Recomendaciones respecto al cumplimiento del deber de solicitar información previa, expresa e informada a los Titulares y la información de las finalidades del tratamiento	46
4.2. Recomendaciones respecto del deber de informar al Titular cuando se le soliciten datos sensibles:	49
4.3. Respecto del deber de conservar la información bajo condiciones de seguridad y de garantizar la reserva de la información	51
4.4. Respecto del deber de contar con un manual interno de políticas y procedimientos para garantizar, en especial, la atención de consultas y reclamos y con ello garantizar el pleno y efectivo ejercicio del derecho de habeas data	53
4.5. Otras recomendaciones y aspectos relevantes a tener en cuenta en los Manuales Internos de Políticas y Procedimientos	54
4.5.1. Designación de un oficial de protección de datos personales	54
4.5.2. Sistema Integrado de Matrícula -SIMAT-	55
4.5.3. Gobierno Escolar	56
4.5.4. Enfermería	57
REFERENCIAS	58

INTRODUCCIÓN

En la actualidad se ha tornado un asunto de especial relevancia la manera en que las organizaciones gestionan los datos personales de sus usuarios. Dicho interés aumenta en la medida que aumenta el uso de tecnologías de la comunicación ya que aumenta el número de usuarios dentro de las bases de información y el intercambio de datos, a raíz de la prestación de algún servicio y en consecuencia, aumenta el riesgo de uso indebido de datos personales en los distintos ámbitos.

Lo anterior ocasiona que los Estados, en aras de proteger la intimidad de las personas opten por regular el derecho que tienen las personas de decidir sobre sus datos personales, la cual se ha llevado a cabo por medio del reconocimiento del derecho de *habeas data*.

Al respecto Perez Luño expone que el actual desarrollo tecnológico ha generado nuevos fenómenos que pueden representar en sí mismos, agresiones a los derechos y libertades, lo cual ha ocasionado que la doctrina jurídica y la jurisprudencia de las naciones hayan tendido al reconocimiento de la libertad y a la facultad de autodeterminación informática, siendo así su garantía principal el *habeas data*, que implica la facultad de las personas de conocer y controlar la información que de ellas ha sido procesada en bancos de datos. Esto correlativamente impone la obligación a las entidades de que hagan tratamiento de dichos

datos personales e incurrir en ciertas prestaciones adicionales para dar cumplimiento a las imposiciones estatales (Perez, 1992, p.153).

Por otra parte, en relación a la importancia de los datos personales, Rojas Bejarano (2014, p. 110) afirma que “ la relevancia legal que tienen los datos personales en los ordenamientos jurídicos se ha desarrollado con el devenir de los años en virtud de la evolución de la sociedad, la tecnología y la relación entre estas”.

Por ello, la legislación colombiana ha consagrado dentro de la categoría de derecho fundamental el derecho al *habeas data*, el cual se encuentra en el artículo 15 de la Constitución Política de Colombia:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

El derecho de *habeas data*, o de protección de datos personales es un derecho fundamental que reviste de importancia en la sociedad de la información que propende por el respeto a la dignidad humana y está relacionado con el uso, administración, almacenamiento de la información propia de las personas. En principio y como se verá, este derecho fue desarrollado por vía jurisprudencial y su desenlace reposa en la Ley Estatutaria 1581 de 2012, como ley principal y el Decreto 1377 de 2013, siendo este el régimen general de tratamiento de datos personales y eje central de posteriores regulaciones y reglamentaciones. El marco jurídico originado en torno a estas normas establecen los deberes y obligaciones correspondientes a las organizaciones que dan tratamiento a los datos personales de los individuos, entre los cuales se encuentran las Instituciones de Educación Preescolar, Básica y Media (IEPBM).

Por ello, es importante conocer en qué medida los mandatos contenidos en la Ley 1581 de 2012, mediante los cuales se representan las disposiciones generales sobre protección de datos personales en Colombia, deben ser cumplidos por las IEPBM como sus destinatarios.

La Constitución Política de Colombia consagró la educación como un derecho de la persona y como un servicio público con función social¹, con la cual se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. Esto en armonía con lo preceptuado en el preámbulo de la Constitución y su artículo primero, en el cual se establece como fin del estado garantizar a sus integrantes el conocimiento, la protección de la dignidad humana y el interés general.

Por esto mismo, la Corte Constitucional sostiene que “(...) *el Constituyente de 1991 otorgó a la educación una doble connotación jurídica, en reconocimiento expreso a su importancia como herramienta en la promoción individual del ser humano y el desarrollo colectivo de la sociedad, responsabilidades estas que constituyen fines esenciales de nuestro Estado Social de Derecho (...)*” (Sentencia T-1101, 2000).

La connotación de la educación como herramienta de promoción individual del ser humano y del desarrollo colectivo de la sociedad, ha sido un argumento fundamental para el desarrollo de posiciones tanto doctrinarias como jurisprudenciales que justifican la importancia del servicio educativo como un servicio único, integral y de interés general, consustancial con la finalidad social del Estado, reconocido por la jurisprudencia colombiana como derecho fundamental.

Según la Corte Constitucional, *"en la medida en que la persona tenga igualdad de posibilidades educativas, tendrá igualdad de oportunidades en la vida para efectos de su realización como persona."* (Sentencia T-002, 1992). Esto hace que sea notoria la inclinación de la protección de la igualdad educativa, estableciendo así la percepción de que las personas deben tener igualdad de condiciones educativas, considerando también que *"tanto por la naturaleza y función del proceso educativo como porque reúne a plenitud los requisitos y criterios de esa categoría constitucional abierta que es hoy el derecho fundamental, esta Corte ha reconocido que la educación es uno de tales derechos que realiza el valor y principio material de la igualdad, consignado en el preámbulo y en los artículos 5o. y 13 de la Carta..."* (Sentencia T-429, 1992).

¹ Constitución Política de 1991. Artículo 67: La educación es un derecho de la persona y un servicio público que tiene una función social; con ella se busca el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura.

Sin embargo, es importante distinguir que la educación posee una doble connotación: por un lado, a educación como derecho fundamental² y, por otro, la educación como servicio público³, entendiendo que la educación como derecho fundamental se entiende como tal y, por consiguiente, un deber del estado de garantizar su oferta y su acceso para todos los menores de 18 años y garantizar por lo menos el acceso a la educación preescolar y básica hasta el noveno grado.

La educación es, sin duda, un aspecto social de especial importancia constitucional que se le ha dado. Pues Como bien lo estableció Goyes Moreno, citando la sentencia C-376 de 2010, a la educación se le reconoce el carácter de derecho fundamental, atendiendo al relevante papel que cumple en la promoción del desarrollo humano (Goyes Moreno, 2014). El sector educativo Colombiano comprende

² La Corte Constitucional en distintos pronunciamientos expone la educación como derecho fundamental, bajo el entendido que ésta (i) es una herramienta necesaria para hacer efectivo el mandato de igualdad del artículo 13 superior, en tanto potencia la igualdad de oportunidades; (ii) es un instrumento que permite la proyección social del ser humano y la realización de sus demás derechos fundamentales; (iii) es un elemento dignificador de las personas; (iv) es un factor esencial para el desarrollo humano, social y económico; (v) es un instrumento para la construcción de equidad social, y (vi) es una herramienta para el desarrollo de la comunidad, entre otras características.

Ahora bien, el inciso tercero del artículo 67 superior dispone que la educación será obligatoria “(...) entre los cinco y los quince años de edad y que comprenderá como mínimo, un año de preescolar y nueve de educación básica”. La redacción de este aparte genera varias inquietudes como, por ejemplo, dentro de qué edades la educación es obligatoria y cuáles son los grados de instrucción que el Estado está en la obligación de garantizar. Sin embargo, la Corte ha sostenido que una interpretación armónica del artículo 67 de la Carta, con el artículo 44 ibídem y con los tratados internacionales de derechos humanos suscritos por el Estado Colombiano en la materia, lleva a concluir que **la educación es un derecho fundamental de todos los menores de 18 años**.

Adicionalmente, ha determinado que **los grados de instrucción que el Estado está en la obligación de garantizar**, la Corte ha afirmado lo siguiente **(i) que los grados previstos en inciso 3° del artículo 67 de la Carta un grado de educación preescolar y nueve años de educación básica constituyen el contenido mínimo del derecho que el Estado debe garantizar**, y (ii) que como se trata de un contenido mínimo, el Estado debe ampliarlo progresivamente, es decir, debe extender la cobertura del sistema educativo a nuevos grados de preescolar, secundaria y educación superior. La Corte Constitucional se ha pronunciado sobre este aspecto en sentencias T-1030 de 2006; C-284 de 2017; T-323 de 1994; C-376 de 2010, entre otras.

³ Por otro lado, al referirse a la educación como servicio público con función social, la Corte Constitucional ha expuesto que se estableció un sistema mixto al otorgarle a los particulares la libertad de fundar establecimientos educativos, dentro de las condiciones de creación y gestión que la ley estableciera y bajo el control, la supervisión y la vigilancia estatal, conforme a lo dispuesto en los artículos 67 y 69 de la Carta. La educación como servicio público está constitucionalmente garantizada y es complementaria de la actividad a cargo del Estado al involucrar la iniciativa privada para brindar una mayor cobertura y calidad en los procesos de enseñanza, dándole la posibilidad a los asociados de ejercer el tipo de educación que desean recibir (artículo 68 superior).

Este Tribunal colige que la educación como servicio público se ha concebido como un instrumento a través del cual el Estado cumple con las finalidades sociales, al satisfacer necesidades básicas y recortar la brecha social que existe entre sus habitantes al otorgarles posibilidades de progresar a través del conocimiento, la técnica y la cultura, lo que se traduce en la materialización de la dignidad humana.

Así, la jurisprudencia constitucional ha determinado que la educación como **servicio público** es una actividad organizada para satisfacer necesidades de interés general, en forma regular y continua, conforme a un régimen jurídico especial, bien sea que se realice por el Estado, directa o indirectamente, o por personas privadas. De la naturaleza de servicio público se deducen los fines generales que persigue la educación: (i) el servicio a la comunidad, (ii) la búsqueda del bienestar general, (iii) la distribución equitativa de las oportunidades y los beneficios del desarrollo, y (iv) la elevación de la calidad de vida de la población. La Corte Constitucional se ha pronunciado sobre este aspecto en sentencias C-520 de 2016; Sentencias T-129 de 2016 y T-592 de 2015, entre otras.

tanto el servicio de educación superior, el cual se encuentra regulado en la ley 30 de 1992; y por otro lado se encuentra la ley 115 de 1994 o Ley General de Educación, en la cual se regula lo atinente a la prestación del servicio de educación en la educación Preescolar, Básica y Media. Este último aspecto es sobre el que se desarrolla el presente trabajo, excluyendo por consiguiente a las Instituciones de Educación Superior, y dirigiendo las recomendaciones que se formulan a las IEPB y al análisis de su norma regulatoria.

La relevancia que tienen las IEPBM en el desarrollo de las personas conlleva a que en el transcurso de las etapas educativas que atraviesan las personas en las instituciones sea necesario un tratamiento de los datos personales, por ello las IEPBM también son sujetos obligados por la normativa vigente en protección de datos mencionada⁴, de manera que, por su misma actividad, “implica adentrarnos a aquellos factores humanos que interfieren en el proceso educativo, tales como maestros, alumnos y administradores del proceso” (Alonso, 2004, p.3).

Las IEPBM, recolectan, administran, almacenan y en general realizan tratamiento de una gran cantidad de información de los aspirantes, los estudiantes, sus acudientes, sus egresados, proveedores, empleados, contratistas, y en general a toda la comunidad educativa que hace parte de las mismas. Así, esta investigación representará utilidad al realizar un análisis del cumplimiento de las normas de protección de datos para las IEPBM, exponiendo las conductas que tiene en cuenta la SIC para determinar el incumplimiento del régimen general de tratamiento de datos personales por parte de las mismas.

Las IEPBM son sujetos obligados al cumplimiento de los deberes y obligaciones establecidos en el régimen de tratamiento de datos personales, la Superintendencia de Industria y Comercio⁵ (SIC) ha establecido diversas (aunque pocas) y cuantiosas sanciones⁶ en contra de estas por violaciones al régimen

⁴ El literal e) del artículo 3 de la ley 1581 de 2012 define **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 el Tratamiento de los datos.

⁵ Según el artículo 19 de la Ley 1581 de 2012, La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

⁶ Ver Resoluciones de la Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio No. 85323 de 2016; 46693 de 2016; 63316 de 2017; 48813 de 2018; 51290 de 2018; 5848 de 2019 y 44029 de 2019. Las mismas se analizan en el presente artículo.

general de tratamiento de datos personales. De manera que la relevancia de la investigación se justifica en el análisis de la doctrina expedida por la SIC en términos de sanciones por violación al régimen general de tratamiento de datos personales en el ámbito educativo. Identificando para el efecto las conductas repetitivas que son analizadas por la SIC a la hora de imponer sanciones por violación a este régimen, y proponiendo recomendaciones para que las IEPBM implementen un programa de cumplimiento del régimen general de tratamiento de datos personales, teniendo en cuenta tanto las investigaciones de la SIC, así como pronunciamientos concretos respecto de obligaciones propias del sector educativo que implican el tratamiento de datos personales.

Teniendo en cuenta que las pocas sanciones administrativas analizadas en el presente trabajo son investigaciones adelantadas en contra de Instituciones de Educación Preescolar, Básica y Media, como en contra de Instituciones de Educación Superior; así como el hecho de que la SIC ha expedido guías en materia de protección de datos personales únicamente enfocado en IEPBM, el presente trabajo aborda únicamente los deberes y obligaciones que en materia de protección de datos personales le corresponden a estas últimas, teniendo en cuenta su marco jurídico aplicable propio del sector educativo básico, excluyendo por lo tanto a las Instituciones de Educación Superior.

A partir de lo mencionado, se propone como pregunta de investigación: ¿Cuáles podrían ser los lineamientos que debe seguir una IEPBM, para conseguir un adecuado cumplimiento del régimen de tratamiento de datos personales? Teniendo como objetivo general proponer recomendaciones que sirvan como referencia y puedan ser tenidas en cuenta por las IEPBM al momento de implementar un sistema de cumplimiento del régimen de protección y tratamiento de datos personales.

Así, en primer lugar se se expondrá el marco jurídico vigente en Colombia para la protección y el tratamiento de datos personales en general; posteriormente se analizarán los aspectos regulatorios propios del sector educativo para las IEPBM más relevantes que inciden en el tratamiento de datos personales, a la luz del principio de responsabilidad demostrada, el cual exige que para un adecuado cumplimiento se deben tener en cuenta las particularidades propias de cada Responsable tales como su naturaleza jurídica y el tratamiento que realiza; luego se identificarán aquellas conductas u omisiones de las Instituciones

Educativas que constituyen violaciones al régimen general de protección de datos personales, en virtud del análisis las resoluciones sancionatorias expedidas por la SIC en contra de Instituciones Educativas por violación a dicho régimen; por último, como conclusión se proponen recomendaciones que sirven de referencia para las IEPBM que implementen un programa de cumplimiento del régimen general de tratamiento de datos personales, recomendaciones que tienen en consideración tanto las conductas investigadas por la SIC para imponer sanciones, como los aspectos regulatorios propios del sector que inciden en el tratamiento de datos personales.

OBJETIVOS

OBJETIVO GENERAL

Proponer recomendaciones a seguir por parte de las Instituciones de Educación Preescolar, Básica y Media para un adecuado cumplimiento del régimen general de tratamiento de datos personales.

OBJETIVOS ESPECÍFICOS

1. Exponer el marco jurídico colombiano vigente en materia de tratamiento de datos personales así como los principios, obligaciones y conceptos clave aplicables a la materia.
2. Identificar, a la luz del principio de responsabilidad demostrada, los aspectos regulatorios de la ley general de educación que tienen incidencia en el tratamiento de datos personales realizado por las IEPBM y en el cumplimiento del régimen general de tratamiento de datos personales.
3. Analizar los aspectos relevantes que han sido tenidos en cuenta por la SIC para determinar el incumplimiento de los deberes del régimen general de tratamiento de datos personales en sus resoluciones proferidas en contra de Instituciones Educativas.

1. CAPÍTULO I. MARCO JURÍDICO DE TRATAMIENTO DE DATOS PERSONALES EN COLOMBIA

El marco jurídico que regula el régimen de tratamiento de datos personales gira en torno a los artículos 15 y 20 de la Constitución Nacional, en los cuales se consagran derechos y libertades que le otorgan a cada persona la oportunidad de conocer, actualizar o rectificar información que se encuentre en bases de datos. Estos derechos consagrados en los artículos mencionados son regulados, en principio por medio de pronunciamientos que realizó la Corte Constitucional ante la carencia de regulación legislativa expresa. Posteriormente fue regulado por la Ley Estatutaria 1266 del 2008; la Ley Estatutaria 1581 de 2012 y el Decreto 1377 del 2013, el cual se encuentra compilado en el Decreto Único reglamentario 1074 de 2015.

1.1. Antecedentes Constitucionales relativos a la protección de datos personales

El régimen de tratamiento de datos en Colombia se cimienta en el derecho constitucional de *habeas data*, de conformidad con lo dispuesto en el artículo 15 de la Constitución Política de Colombia, el cual dispone lo siguiente:

“Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (...)” (Const.,1991, art.15)

Dicha norma evidencia dos dimensiones, por un lado, la obligación del Estado de garantizar el respeto a la intimidad y al buen nombre, y de otra parte el derecho que tienen las personas de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos de entidades públicas y privadas. Esto evidencia la relación directa que existe entre la intimidad personal, el buen

nombre y la protección de los datos personales. Durante varios años la regulación frente al uso y tratamiento de datos en Colombia se desarrolló por medio de jurisprudencia, por esto es importante dar a conocer el marco de reglamentación que se generó.

Para el año 1992, se evidenciaba un vacío regulatorio para los derechos establecidos en el artículo en mención. Reconociendo que el derecho a la intimidad no lograba abarcar todos los aspectos referentes al tratamiento de datos personales, la Corte Constitucional en Sentencia T - 414 de 1992 introduce la definición de “dato personal” como aquel que debe estar referido a aspectos exclusivos y propios de una persona natural, permitir identificar una persona en mayor o menor medida de acuerdo a la visión de un conjunto de datos, contener información que pertenece a la propiedad de un Titular, proteger el interés del Titular en la medida que el tratamiento es sometido a reglas especiales de captación, administración y divulgación, ilustrar la información como constitución de una persona virtual con derechos que puede estar en peligro al no existir regulación. (Corte Constitucional, Sentencia T- 414, 1992).

Seguido de esto, un posterior pronunciamiento de esta corporación en la Sentencia SU- 082 de 1995, la cual busca unificar las directrices jurisprudenciales respecto del uso y tratamiento de datos personales, ampliando el alcance del derecho que tienen los individuos de conocer, actualizar y rectificar la información que sobre ellos reposa en bases de datos, incorporando las facultades de autorizar el tratamiento de datos, incluir nuevos datos, excluirlos y suprimirlos, reconociendo a los individuos la facultad de generar, actualizar y rectificar su información personal. Bajo el entendido que, existe un derecho informativo el cual es inherente al interés público y su vez un derecho a la intimidad que limita el suministro de información, concediéndole un término de caducidad, para que esta no sea eterna y pueda ser modificada en cualquier momento. (Corte Constitucional, Sentencia SU – 082, 1995).

Para el año 2002 se expide Sentencia T- 729, la cual introduce definiciones y clasificaciones propias de cualquier pieza de información vinculada a una o varias personas. Adicionalmente, le otorga una protección judicial hacia este derecho por medio de tutela, y a su vez delimita los ámbitos de protección, y régimen jurídico aplicable.

En igual sentido, debe resaltarse que el segundo párrafo del artículo 15 de la Constitución Política dispone que “en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la constitución”, lo cual evidencia que si bien del derecho de *habeas data* es un

derecho fundamental y autónomo, está relacionado con el derecho a la libertad consagrado en el artículo 28 *ibidem*, e igualmente con el derecho a la libertad de expresión.

1.2. Ley 1266 de 2008

La Ley Estatutaria 1266 fue la primera disposición legislativa en desarrollar el contenido y el alcance del *habeas data* y su régimen de protección, pues hasta el momento se había desarrollado mediante la jurisprudencia de la Corte Constitucional.

Dicha ley fue declarada exequible por la Corte Constitucional mediante Sentencia C-1011 del 16 de octubre de 2008 (Corte Constitucional, Sentencia C-1011, 2008). Esta ley tiene por objeto la regulación de los derechos fundamentales consagrados en los artículos 15 y 20 de la Constitución, relativo al tratamiento de información personal en bases de datos personales, financieras y comerciales. Que si bien se trata de una norma cuyas disposiciones y principios son de aplicación sectorizada, por referirse al tratamiento de datos realizado en el ámbito comercial y financiero -y que no se abordarán en el presente artículo por ser ajeno al mismo-, La Corte Constitucional realizó un estudio detenido de las disposiciones de la Ley 1266, desde la restricción alcance de la norma hasta su régimen de sanciones, lo cual supone un gran aporte bajo las precisiones jurisprudenciales adoptadas en el estudio de constitucionalidad de la misma.

Así, la Sentencia C-1011 de 2008, la cual abre una brecha que busca enmarcar todos los aspectos y ámbitos referentes al tratamiento de datos personales, reconociendo el derecho de los individuos de salvaguardar su dignidad e intimidad, por medio del derecho a conocer la información que tengan almacenada sobre sí mismo, derecho a incluir nuevos datos, derecho actualizar su información, derecho a que la información sea rectificada y corregida, y derecho a excluir información su propia voluntad. (Corte Constitucional, Sentencia C – 1011, 2008).

Es así como con esta sentencia se les otorgan nuevas cargas a las organizaciones, fomentando el desarrollo de reglamentación y políticas internas que logren darle cumplimiento a la normatividad del *habeas data*, y garantizar el derecho a sus Titulares. Para el año 2008, nace la Ley 1266, la cual es denominada ley *habeas data*, pues se encarga de la regulación de información relacionada con el

cumplimiento o incumplimiento de obligaciones dinerarias, financieras, crediticias, comerciales, y de servicios.

Sin embargo, a pesar de que el legislador se esforzó en formular una norma que abordara los aspectos relativos al tratamiento de los datos personales, la misma ley 1266 de 2008 no cubre todos los aspectos involucrados en el tratamiento general de datos personales. Pues como se expresó, dicha ley reguló de manera particular la recolección y circulación de datos comerciales y financieros para la identificación de riesgos crediticios, haciendo de esta norma una norma de carácter sectorial, pues, de acuerdo con Remolina (2010), reguló en forma exhaustiva sobre el cumplimiento e incumplimiento de obligaciones dinerarias.

Con todo, el cambio constante y la adaptación a las nuevas tecnologías derivó en una nueva necesidad de emitir una norma que englobe y regule de manera general todo el tratamiento y protección de los datos personales de los Titulares.

En ese mismo sentido lo expresó Pérez Fernández, en su artículo *El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales* (2016):

Si bien es cierto la expedición de la ley 1266 representó un avance en materia regulatoria del *habeas data*, su implementación no fue la adecuada frente a todo lo que se refiere al manejo y protección de datos personales, habida cuenta que aun existían grandes vacíos que permitían que los problemas por la falta de reglamentación aumentarían; dicha problemática del manejo de las bases de datos en las diferentes entidades (públicas y/o privadas), generó la necesidad de la promulgación de una nueva ley que regulara de una manera general e integral el *habeas data* los datos personales en un ámbito diferente o lo comercial y financiero (Pérez, 2016 p.8-9).

Así las cosas, ante la necesidad de regular todo el tema relacionado con los datos personales y la protección de los mismos, se da entrada a la Ley 1581 de 2012, a través de la cual se dictan todas las disposiciones generales en materia de protección de datos personales.

Recuérdese que el sistema de protección de datos personales surge de la necesidad de controlar el uso que se le da a la información de cada persona. “En este contexto, el derecho fundamental a la protección de datos constituye el punto de equilibrio necesario que garantizará nuestros derechos y las autoridades de protección de datos están llamadas a jugar un papel esencial” (Martínez, 2007, p.60).

1.3. Ley Estatutaria 1581 de 2012

La Ley Estatutaria 1581 de 2012 es el resultado de la incorporación legislativa de las recomendaciones propuestas por la Corte Constitucional en la Sentencia C-1011, en la cual señaló la importancia de expedir una regulación general de tratamiento de datos, es decir, el ámbito no regulado por la ley 1266.

La ley 1581 fue declarada exequible mediante Sentencia C-748 de 2011, su objeto principal es desarrollar los derechos consagrados en los artículos 15 y 20 de la Constitución Política y en especial la facultad de los individuos de conocer, actualizar y rectificar cualquier información suministradas a las bases de datos de entidades públicas o privadas, y también la capacidad de “autorizar el tratamiento, incluir nuevos datos, o excluirllos o suprimirlos de una base de datos o archivo” (Corte Constitucional, Sentencia C-1011, 2008).

La promulgación de esta norma ha traído importantes avances en el tratamiento de datos personales, debido a que en el pasado existía un notorio vacío regulatorio sobre este tema, lo que generaba incertidumbre e incluso desprotección de este importante derecho.

Tal y como lo mencionó Galvis (2012) “la Ley Estatutaria 1581 de 2012 ha significado un adelanto importante en torno a la protección de cualquier dato personal que sea administrado por entidades públicas y privadas, de acuerdo con los principios generales establecidos en la Constitución.” (p. 212).

Dicha ley estableció una estructura definida en materia de protección de datos, pues tal y como lo advierte Aguilar (2018, p.18), en esta se desarrollaron los siguientes aspectos: (i) definió de manera concreta a que personas iba dirigida la aplicación de dicha Ley; (ii) identificó y clasificó los datos objetos de protección; (iii) estableció los deberes y los derechos que poseen los Titulares de la información, pues a través de estos, cada persona podía conocer de manera concreta que garantías tenía sobre sus datos y la responsabilidades que conllevaba la recolección y circulación de los mismos; (iv) estructuró en detalle una herramienta indispensable para efectos de la circulación de la información, la autorización. Así mismo como complemento reglamentario a través del Decreto reglamentario 1377 de 2013 se definió los

componentes y alcances exactos de la autorización; (v) definió el procedimiento de consultas y reclamos por parte de los Titulares, luego entonces, se evidenció el alcance de la norma respecto al derecho de acceso a la información, así como su rectificación, actualización o modificación. Pilares indispensables que componen el derecho de *habeas data*; (vi) Estructuró una política de tratamiento de datos personales, en la cuales definió roles y funciones sobre los Responsables de la información y los Encargados del tratamiento de la misma; y finalmente (vii) designó la autoridad de vigilancia y control en materia de datos, la cual quedo en cabeza de la SIC a través de la delegatura de protección de datos.

Entonces se puede ver que la norma mencionada reguló todos los aspectos generales relacionados con el tratamiento de los datos personales. Tal y como lo señaló Bautista (2015):

Esta ley pretende desarrollar, de acuerdo a su objeto, un aspecto esencial del derecho al *habeas data*, en particular, el derecho a conocer, actualizar y rectificar información personal. Conforme a lo expresado previamente en el análisis sobre el artículo 15 constitucional, esta norma aporta su aplicación en conjunto con la garantía del artículo 20, conjugando la libertad de expresión y el derecho a la intimidad personal y familiar. (Bautista, 2015, p.7)

1.3.1.Principios del tratamiento de datos personales en la ley 1581 de 2012

La ley 1581 estableció principios rectores para el tratamiento de datos personales, los cuales establecen las pautas generales para el correcto tratamiento de los datos personales. Son por lo tanto el eje central y guía para el adecuado cumplimiento del régimen de tratamiento de datos personales, ya que estos principios sientan las bases para el cumplimiento del mismo. Remolina (2013) los definió como “(...) aquellos postulados generales que, incluidos o no formalmente en el ordenamiento jurídico, sirven de base o de razón de ser de enunciados normativos particulares del derecho del debido tratamiento de datos personales” (p.177). Estos principios se encuentran consagrados en el artículo 4 de la ley 1581 de 2012 y se describen a continuación:

- **Principio de legalidad:** Principalmente significa que el procesamiento de datos personales es una actividad regulada y, por lo tanto, es de interpretación restrictiva.

- **Principio de finalidad:** Se refiere a que el tratamiento de datos es necesario para el desarrollo de actividades legítimas, debiendo informarse claramente al Titular con antelación, claridad y suficiencia.
- **Principio de libertad:** Enmarca la autonomía y potestad exclusiva de cada Titular para autorizar o no el tratamiento de sus datos personales.
- **Principio de veracidad o calidad:** Hace referencia a que la información personal a tratar debe ser verdadera, exacta, actualizada, verificable y actualizada.
- **Principio de transparencia:** Consiste en el deber que tienen el Responsable o el Encargado de informar al Titular cómo están manejando sus datos.
- **Principio de acceso y circulación restringida:** Implica que el uso o tratamiento de los datos debe limitarse al alcance indicado por la finalidad, y el acceso a los mismos debe ser controlado.
- **Principio de seguridad:** Los datos personales deben almacenarse utilizando medidas de seguridad técnicas, de personal y administrativas para reducir el riesgo de fuga de información o adulteración, que puede causar daños o perjuicios al propietario de los datos o ponerlos en riesgo.
- **Principio de confidencialidad:** Toda persona que intervenga en el tratamiento de datos está obligada a mantener en absoluta confidencialidad los datos personales que conoció en el desempeño de sus funciones, incluso después de la resolución del contrato con el Responsable, esta obligación sigue existiendo.

1.3.2. Conceptos clave del tratamiento de datos personales

Para comprender el contenido y alcance de las disposiciones del tratamiento de datos personales, es importante aclarar algunos conceptos legales relevantes. A continuación se relacionan importantes definiciones de la Ley 1581 de 2012:

Tabla 1. *Definiciones en el marco de tratamiento de datos personales de la ley 1581 de 2012*

Concepto	Definición
Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales
Base de Datos	Conjunto organizado de datos personales que sea objeto de tratamiento
Dato Personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables
Tratamiento	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
Dato Sensible	aqueellos 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.
Menores de edad	Personas físicas menores de 18 años. Los datos de los menores están sujetos a una protección especial, en cuanto a las medidas de seguridad para protegerlos, deben contar con las más altas medidas de protección.
Titular	Persona natural cuyos datos personales sean objeto de tratamiento
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

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 el tratamiento de los datos
------------------------------------	--

Fuente: Elaboración propia

Como se evidencia de las definiciones expuestas, los sujetos que intervienen en la relación del tratamiento de datos personales son i) el Titular; ii) El Responsable del tratamiento y, iii) el Encargado del tratamiento. En cuanto al Titular, es la persona de la cual se predica la protección de su derecho fundamental al *habeas data* y demás derechos relacionados a este.

Por otra parte, el Responsable del tratamiento y el Encargado del tratamiento son dos roles de notoria distinción en la relación de tratamiento de datos personales, sin embargo, ambos roles pueden recaer en la misma persona o ser dos personas diferentes en torno a la relación. Los deberes de uno y otro se encuentran contenidos en los artículos 17 y 18 de la ley 1581 de 2012, respectivamente.

Los sujetos antes mencionados cuentan con una participación activa en todo el proceso de procesamiento de datos personales. Son responsables de la correcta implementación de los tratamientos antes mencionados y de cumplir con los lineamientos legales para cumplir y observar adecuadamente el cumplimiento de sus deberes.

Las IEPBM, recolectan, administran, almacenan y en general realizan tratamiento de una gran cantidad de información de los aspirantes, los estudiantes, sus egresados, proveedores, empleados, contratistas, y en general a toda la comunidad educativa de su entorno. Por ello la SIC ha determinado que las IEPBM son Responsables de tratamiento de datos personales, por medio de resoluciones sancionatorias que son objeto de análisis en el capítulo III del presente artículo.

Por último, la ley también establece las autoridades de supervisión y control que realizarán funciones para la vigilancia del tratamiento de datos personales. Esta es la SIC a través de la delegatura para la protección de datos personales. En cuanto a sanciones, se prevén multas, suspensión de actividades relacionadas con el tratamiento de datos personales, cierre temporal, cierre inmediato o permanente (Ley 1581 de 2012). Finalmente, la Ley 1581 de 2012 crea el Registro Nacional de Bases de

Datos, regulado por el Decreto 886 de 2014, que actúa como el "registro público de bases de datos sujetas a tratamiento que operan en el país" (Ley 1581 de 2012, Art. 25).

1.4. Decreto 1377 de 2013

El Decreto 1377 de 2013 es la norma reglamentaria de la Ley Estatutaria 181 de 2012, desarrolla especialmente: i) aspectos relativos a la autorización del tratamiento de datos personales; ii) el contenido de las políticas de tratamiento de datos y de los manuales internos de tratamiento de datos; iii) el principio de responsabilidad demostrada.

En primer lugar, se debe señalar que la autorización para la recolección y tratamiento de datos personales es la base de legitimación de esta actividad, de conformidad con los principios de finalidad y libertad. El tratamiento de datos personales está prohibido salvo que cuente con autorización expresa y previa, que, según el artículo 5 del decreto correspondiente, deberá ser "a más tardar cuando se recojan sus datos"(Decreto 1377, 2013, art. 5).

Al momento de obtener la autorización se debe informar al Titular de los datos cuáles datos serán tratados y la finalidad del tratamiento de los mismos. A demás, de acuerdo con el numeral 1 del artículo 6, el Titular de los datos debe ser informado de que no está obligado a dar permiso para el procesamiento de sus datos sensibles (Decreto 1377, 2013). En cuanto a las formas de obtención de la autorización, se admite que la misma se obtenga de manera escrita, oral o mediante conductas inequívocas del Titular que permitan concluir su autorización.

En relación a las políticas de tratamiento de datos personales, contar con las mismas es una condición obligatoria para las personas que realizan actividades que impliquen el tratamiento de datos personales. Estas políticas deben informar al Titular de los datos la razón social, domicilio, los derechos que respaldan, el tratamiento de los datos al que serán sometidos, y en el caso de que sea imposible facilitar al Titular de los datos la política de tratamiento, se debe contar con un aviso de privacidad, en el cual se informe sobre la existencia de la política de tratamiento y la forma de acceso a la misma. (Decreto 1377, 2013).

Por último, el Decreto 1377 contempla la responsabilidad demostrada en la actividad del tratamiento de datos personales, según la cual los Responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la SIC, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto (Decreto 1377, 2013, art. 26).

1.5. Decreto Único Reglamentario 1074 de 2015

El Decreto Único Reglamentario del Sector Comercio, Industria y Turismo expedido en el año 2015, compiló entre otras disposiciones, las establecidas en materia de protección de datos tanto del sector financiero como aquellas que regulan el *habeas data* de aplicación general, y las reunió en los siguientes capítulos:

- Capítulo 25 y capítulo 26, reglamentó la ley 1581 de 2012 y sus decretos reglamentarios Decreto 1377 de 2013 y Decreto 886 de 2014.
- Capítulo 27 y Capítulo 28, reglamentó la ley 1266 de 2008 y sus decretos reglamentarios Decreto 1727 de 2009 y Decreto 2952 de 2010.

(Dirección de Investigación de Protección de Datos Personales, 2020)

Debido a que el Decreto en mención compiló en su totalidad las disposiciones en materia de *habeas data* es preciso indicar que según el artículo 3.1.1 del mismo señala la derogatoria integral de las disposiciones compiladas por el decreto, sin embargo, aún se siguen remitiendo a las normativas nacionales, con las notas de vigencia pertinentes.

2. CAPÍTULO II. ASPECTOS REGULATORIOS DE LA LEY GENERAL DE EDUCACIÓN QUE TIENEN INCIDENCIA EN EL CUMPLIMIENTO DEL RÉGIMEN GENERAL DE TRATAMIENTO DE DATOS PERSONALES POR LAS IEPBM

El presente capítulo busca identificar los aspectos regulatorios propios de la ley 115 de 1994, ley general de educación, que tienen incidencia o implicaciones en el tratamiento de datos personales que realizan las IEPBM. Esto teniendo en cuenta el concepto del principio de responsabilidad demostrada regulado en el Decreto 1377 de 2013, el cual exige que para un adecuado cumplimiento se deben tener en consideración aspectos como la naturaleza jurídica del Responsable, y el tratamiento al cual serán sometidos los datos personales.

Para ello se recurre a la conceptualización del principio de responsabilidad demostrada, responder en qué consiste, a la finalidad del mismo; y a la exposición de las normas nacionales que lo consagran. Posteriormente se analizan algunos aspectos regulatorios propios de la ley general de educación, que tienen implicaciones en el tratamiento de datos personales para identificar qué aspectos deben ser considerados por las IEPBM al momento de implementar el cumplimiento del régimen general de tratamiento de datos personales, para así acreditar el efectivo cumplimiento de sus obligaciones.

2.1. Conceptualización del principio de responsabilidad demostrada

El término *accountability* (responsabilidad) proviene del mundo anglosajón y a pesar de las diferentes acepciones que puedan darse de él, se ha entendido que en el área de la protección de datos dicha expresión se refiere al modo como una organización debe cumplir en la práctica las regulaciones sobre la materia y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente. (Remolina y Álvarez, 2018, p.p. 28- 29).

Este principio tiene relación con la forma en que se lleva a cabo el tratamiento y la protección de datos en las organizaciones y también representa el desafío continuo de una organización en términos de cumplimiento, en este sentido:

Garantizar la aplicación efectiva y práctica de lo que ordenan las normas sobre protección de datos es un reto permanente de cualquier organización. El principio de responsabilidad cobra cardinal

importancia para lograr ese propósito. Dicho principio exige que los Responsables y Encargados del tratamiento de datos, implementen medidas apropiadas, efectivas y verificables que les permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales. (Remolina y Álvarez, 2018, p. 29)

El objetivo de este principio es que se desarrollen e incorporen políticas y procedimientos medibles y sobre todo demostrables que evidencien un adecuado nivel de protección en el tratamiento de datos, de manera que a través de los mismos se demuestre a la SIC por parte de los Responsables y Encargados del tratamiento que se ha realizado una correcta gestión en la recolección, administración, uso y circulación de los datos personales registrados en las bases de datos.

De esta manera se encuentra establecido en el Decreto Reglamentario 1377 de 2013 en su artículo 26, el cual dispone que los Responsables del tratamiento de datos personales deben **ser capaces de demostrar, a petición de la SIC, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones** establecidas en la Ley 1581 de 2012 y este decreto (...) (Decreto 1377, 2013, art. 26).

Por ello, los Responsables y Encargados del tratamiento de datos personales, deben desarrollar políticas que garanticen la seguridad de conformidad con las directrices establecidas para el efecto, ya que las mismas garantizan el cumplimiento de los principios y deberes en la materia. Estas políticas deben tener como objetivo implementar y constatar los procedimientos que se lleven a cabo para asegurar un adecuado tratamiento de datos personales.

De igual manera lo ratificó la SIC como organismo responsable de velar por la correcta administración de datos personales, al determinar que:

Estas políticas internas efectivas no pueden limitarse a reproducir los textos legales ni son meras declaraciones de principios. Por el contrario, la adopción de políticas internas efectivas parte del Desarrollo de un Programa Integral de Gestión de Datos Personales, que debe ser el resultado de un proceso de debida diligencia al interior de la organización que permita formularlo. (Superintendencia de Industria y Comercio, 2015, p. 9).

Para desarrollar este principio, es necesario examinar en detalle aspectos como la cantidad de bases de datos gestionadas, la calidad y naturaleza de los datos recogidos en ellas, la finalidad de estos

datos y los estándares de seguridad que se relacionan con la difusión y circulación de los mismos y, en general realizar una revisión del tratamiento de datos realizado para determinar qué aspectos se están desarrollando de acuerdo con la normativa aplicable y, por otro lado, identificar debilidades. Esto se puede utilizar para diagnosticar el nivel de cumplimiento con los deberes y las políticas de seguridad. El principio de responsabilidad demostrada se encuentra regulado en el capítulo VI del decreto 1377 de 2013, el cual Desarrolla expresamente los lineamientos de los programas de responsabilidad demostrada.

Además de las políticas de protección de datos, los Responsables del tratamiento de datos en Colombia deben contar con los procesos, procedimientos y controles necesarios para demostrar a la autoridad de vigilancia la efectividad de las políticas para garantizar el derecho a la protección de datos. Así, el artículo 26. del Decreto 1377 de 2013 acerca de la responsabilidad demostrada frente al tratamiento de datos personales, establece que los Responsables del tratamiento deben ser capaces de demostrar, a petición de la SIC, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente: 1. 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. 2. La naturaleza de los datos personales objeto del tratamiento. 3. El tipo de tratamiento. 4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los Titulares.

El principio de responsabilidad probada tiene como objetivo, por tanto, que el tratamiento de los datos cumpla las directrices legales y que de esta forma se garantice una correcta gestión de los datos respetando y adoptando todas las medidas disponibles en esta materia. Así lo expresó Quiroga (2014): De este modo, con la aplicación del principio de la responsabilidad demostrada, se crean mecanismos estables y seguros para los Titulares respecto al tratamiento efectivo de sus datos personales, es decir que estos sean tratados para los fines concretamente autorizados y con los más altos estándares de protección y confidencialidad. (Quiroga, 2014)

En virtud de lo anterior, las IEPBM como Responsables del tratamiento de datos personales deben proporcionar evidencia del efectivo cumplimiento de sus obligaciones, así como de los procedimientos y estrategias que utilizan para manejar los datos personales que recolectan, en caso de ser

requeridos por la SIC para ello. Por ese motivo, la implementación del principio de responsabilidad demostrada es una práctica útil para las IEPBM, pues en caso de verse en una investigación adelantada por la SIC por el posible incumplimiento de sus obligaciones del régimen general de tratamiento de datos personales, pueden contar con los elementos de prueba necesarios para demostrar el efectivo cumplimiento de sus deberes en este ámbito.

Como bien se advierte del principio de responsabilidad demostrada, un aspecto que cobra especial relevancia es que la implementación del cumplimiento del régimen de tratamiento de datos personales debe adaptarse a los aspectos particulares propios de cada organización, teniendo en cuenta “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”. Así, se analizarán los aspectos relevantes de las IEPBM, a la luz de las principales normas jurídicas del sector educativo contempladas en la ley 115 de 1994, ley general de educación.

2.2. Aspectos regulatorios del sector educativo para las Instituciones de Educación Preescolar, Básica y Media relevantes para el tratamiento de datos personales.

Teniendo presente que los elementos a considerar por los Responsables frente al principio de responsabilidad demostrada, según los cuales se debe tener en cuenta, entre otros: la naturaleza jurídica del responsable del tratamiento, la naturaleza de los datos objeto de tratamiento y el tipo de tratamiento, es evidente que la implementación del principio tendiente a evidenciar a la SIC el adecuado cumplimiento del régimen general de tratamiento de datos personales debe adaptarse a las particularidades propias de cada Responsable, bien sea por su naturaleza jurídica, industria, tipos de usuario e inclusive los aspectos regulatorios del sector del Responsable que impliquen de manera directa o indirecta el tratamiento.

Por ello, se tiene como punto de partida la Guía para el tratamiento de datos personales para el Sector Educativo Público y Privado de la SIC, en la cual hace alusión específica a aspectos regulatorios relevantes de la ley 115 del 94, por lo que se reitera, en el presente trabajo se aborda el cumplimiento del régimen de protección de datos personales únicamente para las Instituciones de Educación Preescolar, básica y media, excluyendo a las Instituciones de Educación Superior; adicionalmente, se analizan

elementos adicionales contemplados en la ley general de educación que implican de manera directa o indirecta el tratamiento de datos personales, y los cuales deben ser considerados por las IEPBM al momento de implementar el cumplimiento del régimen general de protección de datos.

A través de la Guía para el Tratamiento de Datos Personales para el Sector Educativo Público y Privado, la SIC instruye a las instituciones y centros de educación formal e informal sobre la forma de manejar los datos personales de los estudiantes en los diferentes momentos de la recolección y tratamiento de estos datos, identificando para el efecto que las Instituciones Educativas, en especial aquellas que prestan servicios de educación preescolar, básica y media, deben tener en consideración, en primer lugar, tres aspectos:

- i. El tratamiento que se da a los datos, teniendo como punto inicial el momento desde que se acude a un centro educativo público o privado para obtener cupo escolar a través de un proceso de inscripción o matrícula.
- ii. Tratamiento de Datos Personales durante todo este tiempo, tanto del estudiante como de familiares, seres cercanos y allegados, como los padres, acudientes, docentes y personal administrativo.
- iii. El momento de finalización del vínculo entre la IEPBM y el estudiante, bien sea porque se culminan los estudios o porque se retira de la IEPBM.

Ahora bien, la Ley 115 de 1994, ley general de educación, regula diversos aspectos que son relevantes y de necesaria evaluación para la adecuada implementación del cumplimiento del régimen general de protección de datos personales, como se expone a continuación:

2.2.1. Etapas de formación: Educación Preescolar, Básica y Media

En primer lugar, la Ley General de Educación regula las etapas de la educación formal, siendo éstas i) Educación Preescolar; ii) educación básica; iii) educación media.

La educación preescolar comprende como mínimo un grado obligatorio, y corresponde a la

educación ofrecida al niño para su desarrollo integral en los aspectos biológico, cognoscitivo, sicomotriz, socio-afectivo y espiritual, a través de experiencias de socialización pedagógicas y recreativas, de acuerdo a lo dispuesto en el artículo 15 de la ley 115 de 1994.

La educación básica tiene una duración de nueve (9) grados, desarrollando la educación básica primaria en cinco (5) grados, y la educación básica secundaria en cuatro (4) grados. De acuerdo al artículo 19 de la ley general de educación, la educación básica obligatoria corresponde a la identificada en el artículo 356 de la Constitución Política como educación primaria y secundaria; comprende nueve (9) grados y se estructurará en torno a un currículo común, conformado por las áreas fundamentales del conocimiento y de la actividad humana.

La educación media comprende una duración de dos (2) grados, constituye la culminación, consolidación y avance en el logro de los niveles anteriores y comprende dos grados, el décimo (10°) y el undécimo (11°). Tiene como fin la comprensión de las ideas y los valores universales y la preparación para el ingreso del educando a la educación superior y al trabajo. Además, tiene el carácter de académica o técnica. A su término se obtiene el título de bachiller que habilita al educando para ingresar a la educación superior en cualquiera de sus niveles y carreras. De conformidad con los artículos 27 y siguientes de la ley 115 de 1994.

La presente distinción empieza a ser relevante, por cuanto desde ya se evidencia que las IEPBM cuentan con una clasificación de la etapa del ciclo formativo en la que se encuentran sus educandos, teniendo implicaciones en tratamiento que se le da a los datos personales, existiendo la posible presencia de varias bases de datos que se encuentren clasificadas con este criterio.

2.2.2. Aspectos relacionados a la prestación del servicio educativo

En segundo lugar, la Ley General de Educación regula y desarrolla conceptos que se encuentran relacionados directamente con el servicio educativo, entre los cuales se identificaron aquellos que guardan relación con el tratamiento de datos personales, siendo estos:

- a. **Comunidad educativa:** Definida en el artículo 6 de la ley 115 de 1994, como aquella conformada por estudiantes o educandos, educadores, padres de familia o acudientes de los estudiantes, egresados, directivos docentes y administradores escolares. Todos ellos, según su competencia, participarán en el diseño, ejecución y evaluación del Proyecto Educativo Institucional y en la buena marcha del respectivo establecimiento educativo.

El mismo artículo advierte como la comunidad educativa también participa en la dirección de los establecimientos educativos, por lo tanto, las IEPBM dan tratamiento a los datos personales de la comunidad educativa, aspecto que es igualmente destacado por la SIC en su guía para el sector de educación, dando así tratamiento de datos personales tanto a sus estudiantes (principales usuarios del servicio educativo), como de sus padres o acudientes; colaboradores como el personal docente, directivo y administrativo; e incluso sus egresados, todos estos en su calidad de Titulares de datos personales en los términos de la ley 1581 de 2012.

- b. **El alumno o educando:** El artículo 91 de la ley general de educación lo define como el centro del proceso educativo y debe participar activamente en su propia formación integral. Es el usuario principal del servicio de educación prestado por las IEPBM y, como se expuso anteriormente, un grupo de personas que son Titulares de datos personales en los términos de la ley 1581 de 2012.
- c. **El educador:** Definido en el artículo 104 de la ley 115 de 1994 como el orientador en los establecimientos educativos, de un proceso de formación, enseñanza y aprendizaje de los educandos, acorde con las expectativas sociales, culturales, éticas y morales de la familia y la sociedad. Es igualmente un grupo de personas Titulares de datos personales respecto de los cuales las IEPBM realizan tratamiento.
- d. **Matrícula:** La matrícula es el acto que formaliza la vinculación del educando al servicio. De acuerdo con el artículo 95, se realizará por una sola vez, al ingresar el alumno a un establecimiento educativo, pudiéndose establecer renovaciones para cada período académico.
- Es evidente pues, que la matrícula es el acto por el cual se formaliza y da inicio a la relación entre la IEPBM y el alumno, así como con su familia, siendo este un acto en el cual se recolectan datos personales, implicando que sea un aspecto a tener en cuenta frente a las obligaciones que en su calidad de Responsable del tratamiento le asisten a las IEPBM.

- e. **Establecimiento educativo:** El artículo 138 de la Ley general de educación lo define así: Se entiende por establecimiento educativo o institución educativa, toda institución de carácter estatal, privada o de economía solidaria organizada con el fin de prestar el servicio público educativo. Entre sus requisitos se encuentra contar con una estructura administrativa, planta física y medios educativos adecuados.
- Este aspecto de la prestación del servicio educativo tiene incidencia en el tratamiento de datos personales, pues al tratarse del espacio físico donde acuden alumnos, colaboradores, directivos, padres y acudientes, las IEPBM pueden dar tratamiento a datos personales en los eventos en que controlen el ingreso a las instalaciones, o en el uso de sistemas de seguridad que impliquen el uso de sistemas de videovigilancia, siendo este otro punto de recolección de datos personales.

2.2.3. Organizaciones al interior de las IEPBM

En tercer lugar, la ley general de educación en su artículo 139 establece que en cada establecimiento educativo se debe promover la presencia de organizaciones internas, tales como asociaciones de padres de familia y de estudiantes vinculados a la respectiva IEPBM, con el fin de dinamitar el proceso educativo. Lo cual implica que frente al tratamiento de datos se generen nuevas bases de datos e incluso, nuevos puntos donde se recolecten datos personales, siendo así un factor relevante a tener en cuenta por parte de las IEPBM frente al cumplimiento de sus obligaciones derivadas del régimen general de tratamiento de datos personales.

Adicionalmente, en relación a las organizaciones en las IEPBM se encuentran aquellos grupos colegiados propios de la conformación del gobierno escolar, según el artículo 142 de la ley general de educación. El cual se encuentra conformado por el rector, el consejo directivo, y el consejo académico, estos dos últimos como cuerpos colegiados para las instituciones educativas estatales. Por otro lado, las instituciones educativas privadas deben establecer en su reglamento un gobierno escolar y su estructura para la participación de la comunidad educativa.

Los anteriores aspectos tienen incidencia en el tratamiento de datos personales en virtud de que las mismas pueden suponer la recolección y creación de bases de datos que serán objeto de tratamiento,

afectando directamente las obligaciones que en calidad de Responsables del tratamiento le asisten a las IEPBM.

En consecuencia se puede identificar existen aspectos regulatorios propios del sector educativo para las IEPB contenidos en la ley general de educación que inciden o guardan relación directa o indirecta con el tratamiento de datos personales. Lo cual ocasiona que estos aspectos deban ser identificados y considerados al momento de implementar un programa de cumplimiento del régimen general de tratamiento de datos personales por parte de las IEPBM ya que de lo contrario, pueden afectar el adecuado cumplimiento de sus obligaciones que en su calidad de Responsables del tratamiento le corresponden.

Por lo tanto, el adecuado análisis de estos aspectos regulatorios propios de las IEPBM son un punto de partida de especial relevancia, ya que hace alusión directa a la consideración de la naturaleza jurídica del Responsable del tratamiento, así como del tipo de datos y tratamiento al que se someterán, de acuerdo a lo dispuesto por el mismo principio de responsabilidad demostrada, ya que se tienen en cuenta su actividad particular, y aquellos aspectos que durante la prestación del servicio educativo tiene implicación directa en el tratamiento de los datos personales.

3. CAPÍTULO III: PRONUNCIAMIENTOS DE LA SIC PARA DETERMINAR EL INCUMPLIMIENTO DEL RÉGIMEN GENERAL DE TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LAS INSTITUCIONES EDUCATIVAS

Luego de analizar los aspectos regulatorios relevantes del sector educación preescolar, básica y media para la implementación del cumplimiento del régimen de tratamiento de datos personales, en el presente capítulo se analiza toda la doctrina expedida por la SIC en ejercicio de sus funciones administrativas⁷, resoluciones sancionatorias en contra de instituciones educativas tanto básica y media como superior, con el fin de identificar los aspectos que son tenidos en cuenta por dicha entidad para determinar el incumplimiento de las Instituciones Educativas.

3.1. Pronunciamientos de la SIC relativos al tratamiento de datos personales en el sector educativo

La SIC en ejercicio de las funciones que le fueron otorgadas en el Capítulo II de la Ley 1581 de 2012, ha llevado a cabo procedimientos administrativos sancionatorios en contra de diversas instituciones educativas, en los cuales ha realizado sus investigaciones por medio de informática forense, requiriendo a las mismas instituciones y a sus representantes legales para que alleguen documentos o realizando inspecciones presenciales. En concreto se han analizado las resoluciones No. 85323 de 2016; 46693 de 2016; 63316 de 2017; 48813 de 2018; 51290 de 2018; 5848 de 2019 y 44029 de 2019. Es de aclarar que el objeto de todas estas resoluciones es determinar el incumplimiento de las obligaciones en materia de tratamiento de datos personales. En la *tabla 2* se exponen los datos relevantes de las mismas.

Si bien es cierto el presente trabajo de grado se enfatiza el cumplimiento del régimen general de tratamiento de datos personales por parte de las IEPBM, en el presente acápite se analizan resoluciones expedidas en contra de IEPBM como de Instituciones de Educación Superior, lo anterior en virtud del poco precedente que al respecto ha expedido la SIC, y en igual sentido en consideración a que el análisis

⁷ Ley 1581 de 2012. Artículo 22. La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

de las obligaciones incumplidas en cada una de las siete (7) resoluciones analizadas es común en cada caso.

Tabla 2. Resoluciones de la SIC por violación al régimen de tratamiento de datos personales en contra de instituciones educativas.

RESOLUCIÓN	INSTITUCIÓN EDUCATIVA INVESTIGADA	DECISIÓN
Resolución No. 85323 de 2016	COLEGIO BILINGUE CLERMONT LTDA.	Imponer una sanción pecuniaria de DOSCIENTOS CUARENTA Y OCHO MILLONES DOSCIENTOS TRES MIL OCHOCIENTOS PESOS (\$248,203,800), equivalente a trescientos sesenta (360) salarios mínimos legales mensuales vigentes, por la violación a lo dispuesto en los literales a), b), c) y k) del artículo 17 de la ley 1581 de 2012 en concordancia con los artículos 2.2.25.2.2, 2.2.25.2.9 y 2.2.25.3.1. del Decreto 1074 del 2015.
Resolución No. 46693 de 2016	Corporación Universitaria Iberoamericana	Imponer una sanción pecuniaria de VEINTE MILLONES SEISCIENTOS OCHENTA Y TRES MIL SEISCIENTOS VEINTE (\$20,683,629), equivalente a treinta (30) salarios mínimos legales mensuales vigentes, por el incumplimiento del deber establecido en el literal d) del artículo 17 de la Ley 1581 de 2012.
Resolución No. 63316 de 2017	Corporación Universitaria de la Costa	PRIMERO: Imponer una sanción pecuniaria de CIENTO CUARENTA MILLONES SEISCIENTOS VEINTITRÉS MIL QUINIENTOS SESENTA PESOS (\$140.623.560), equivalente a ciento ochenta (180) salarios mínimos legales mensuales vigentes.

Resolución No. 48813 de 2018	Colegio Provincia Nuestra Señora de la Gracia de Colombia - Liceo Cervantes el Retiro	Imponer una sanción pecuniaria de TRESCIENTOS DOCE MILLONES CUATROCIENTOS NOVENTA Y SEIS MIL OCHOCIENTOS PESOS (\$312.496.800.00), equivalentes a CUATROCIENTOS (400) salarios mínimos legales mensuales vigentes, por el incumplimiento del deber establecido en (i) el literal k) del artículo 17 de la Ley 1581 de 2012 en concordancia con el artículo 25 de la misma norma, así como el artículo 2.2.2.25.3.1 del Decreto Unica Reglamentaria 1074 de 2015; (ii) el inciso segundo del artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015, en concordancia con los artículos 2.2.2.25.3.2 y 2.2.2.25.3.5 de la misma disposición; (iii) el literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y las artículos 5,6 y 9 de la misma disposición, así como el incisa primero del artículo 2.2.2.25.2.2 y los artículos 2.2.2.25.2.3 y 2.2.2.25.2.9 del Decreto Unico Reglamentario 1074 de 2015; (iv) el literal a) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal b) del articula 4 y los artículos 6 y 12 de la misma disposicion, así como el incisa primero del artículo 2.2.2.25.2.2 y el articula 2.2.2.25.2.3 del Decreto Único Reglamentario 1074 de 2015 y (v) el literal k) del artículo 17 de la Ley 1581 de 2012.
Resolución No. 51290 de 2018	Universidad de San Buenaventura	Ordenar que ajuste la "política de tratamiento de datos personales" en los términos establecidos en el artículo 2.2.2.25.3.1 del Decreto Unico Reglamentario 1074 de 2015, de manera que contenga (i) Los derechos que le asisten al titular del dato; (ii) La 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; (iii) El procedimiento para que los Titulares de la información puedan ejercer lo derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización y; (iv) el periodo de vigencia de las bases de datos.
Resolución No. 5848 de 2019	Centro Educativo Superior Interamericano S.A.S.	Imponer una sanción pecuniaria de un millón seiscientos cincuenta y seis mil doscientos treinta y dos pesos (\$1,656,232), equivalente a dos (2) salarios mínimos legales mensuales vigentes.

Resolución No. 44029 de 2019	Colegio Congregación de Hermanas Franciscanas de Nuestra Señora de Lourdes	Imponer una sanción pecuniaria de TRESCIENTOS TREINTA Y CINCO MILLONES NOVECIENTOS TREINTA Y CUATRO MIL SESENTA PESOS (\$335,934,060), equivalente a cuatrocientos treinta (430) salarios mínimos legales mensuales vigentes, por la violación a lo dispuesto en los literales b), c), y k) del artículo 17 de la Ley 1581 de 2012 en concordancia con el artículo 7 de la norma en mención y el deber establecido el artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015.
-------------------------------------	--	---

Fuente. Elaboración propia

3.2. Aspectos relevantes comunes tenidos en cuenta por la SIC para determinar el incumplimiento del régimen de tratamiento de datos personales

En virtud de dichas resoluciones, la SIC ha resaltado en los puntos comunes objeto de estudio para la verificación del cumplimiento del régimen de tratamiento de datos por parte de las IEPBM, siendo sus más relevantes: i) derechos de los niños, niñas y adolescentes y los datos personales de carácter sensible; ii) Deber de solicitar autorización previa, expresa e informada por parte del Titular y de informar debidamente la finalidad de la recolección; iii) Deber de conservar la información bajo las condiciones de seguridad y de garantizar la reserva de la información; iv) Deber de contar con las políticas de tratamiento de datos y de informar a los Titulares sobre su existencia; v) Deber de adoptar un manual interno de políticas y procedimientos para el tratamiento de datos personales.

3.2.1. Derechos de los niños, niñas y adolescentes y los datos de carácter sensible

La SIC ha determinado que las IEPBM son organizaciones que se encargan de recoger, decidir y hacer tratamiento sobre datos personales de los menores, razón por la cual se constituyen en Responsables del tratamiento de datos personales en los términos del literal e) del artículo 3 de la Ley 1581 de 2012.

Esta connotación se fundamenta debido a que en el marco legal establece que los datos personales de los menores de edad es son una categoría especial de datos, materializando la prevalencia de sus

derechos e interés superior del menor, quienes tienen especial protección constitucional en virtud del Artículo 44 de la Constitución Política de Colombia e igualmente desarrollado en el artículo 8 del Código de Infancia y Adolescencia.

De manera que en el régimen general de tratamiento de datos se encuentran expresamente establecidos parámetros, condiciones, requisitos y obligaciones que el Responsable, el Encargado, y la comunidad en general deben cumplir respecto de cualquier operación que se realiza de datos personales de menores. Y como consecuencia lógica del principio de seguridad, el tratamiento de datos de esta categoría especial exige una implementación de mayores controles de seguridad por parte del Responsable de su tratamiento; aún cuando el artículo 7 de la ley 1581 de 2012 proscriba el tratamiento de datos personales de los menores salvo los que sean de carácter público, la SIC, apoyándose de la interpretación dada por la Corte Constitucional en Sentencia C-748 de 2011⁸ argumenta que tal prohibición no es absoluta, sino que se trata de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluyendo el derecho al *habeas data*.

Adicionalmente, hace referencia a cómo la legislación nacional impone mayores cargas a los Responsables y Encargados del tratamiento de datos personales de carácter sensible, por ejemplo los relativos a salud toda vez que evidenció que en reiteradas ocasiones las instituciones educativas investigadas requerían en sus formularios datos sensibles como el grupo sanguíneo, estatura, peso, a cuál entidad promotora de salud se encuentra afiliado o si tiene condiciones especiales de aprendizaje, entre otras.

Indica la SIC que en virtud de su regulación en el artículo 5 de la ley 1581 de 2012 y su interpretación por la Corte Constitucional en Sentencia C-748 de 2011 como aquellos datos por los cuales existe riesgo de discriminación del individuo afectando su derecho a la intimidad, determina cómo los Encargados y Responsables del tratamiento deben ser aún más diligentes cuando realicen operaciones de datos sensibles. Indica también que los Responsables del tratamiento deben informar al Titular el carácter facultativo que tienen sus respuestas en virtud de lo establecido por el artículo 6 de la Ley 1581 y su

⁸ “esa interpretación no debe entenderse en el sentido de que existe una prohibición casi absoluta del tratamiento de datos de los menores, pues ello daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, lo cuál una interpretación así sería inconstitucional”.

correspondiente reglamento contemplado en el artículo 2.2.2.25.2.3 del Decreto Único Reglamentario 1074.

Así, las conductas u omisiones que representan un incumplimiento del régimen general por parte de las IEPBM con relación a este punto son las siguientes:

- No tener en cuenta que se realizan tratamiento de datos personales de menores de edad, los cuales tienen una categoría especial y una mayor exigencia de cuidado en su tratamiento en lo que refiere a la autorización previa, expresa e informada.
- Adicionalmente, en muchas ocasiones se realiza tratamiento de datos de carácter sensible de menores de edad, lo cual conlleva a una mayor carga de cuidado tanto al momento de la obtención de la autorización, toda vez que se debe informar el carácter facultativo que tiene el suministro de dicha información, así como la privacidad y seguridad con la que se conserve la misma.

3.2.2. Deber de solicitar y conservar autorización previa, expresa e informada por parte del Titular y de informar debidamente la finalidad del tratamiento

En cuanto al deber de solicitar autorización previa, expresa e informada por parte del Titular y de informar debidamente la finalidad del tratamiento, la SIC analizó en sus resoluciones sancionatorias cómo estas obligaciones -que se encuentran reguladas en los literales b) y c) del artículo 17 de la ley 1581 de 2012- derivan del derecho de autodeterminación informática y principio de libertad consagrados en el artículo 15 de la Constitución Política y que se plasman en los principios de libertad y finalidad del tratamiento de datos consagrados en los literales b) y c) del artículo 4 de la ley 1581.

De estos principios derivan el deber de solicitar y conservar copia de la autorización, previa y expresa; de informar debidamente la finalidad de la recolección y los derechos que le asisten a los Titulares; de tener un especial tratamiento de información personal de menores de edad, es decir informar el carácter facultativo de las respuestas cuando las preguntas versen sobre datos sensibles o de menores.

La SIC luego de analizar varios de los medios por los cuales las instituciones investigadas recolectaban información, tales como formularios físicos o formatos web, encontraron que muchas de

ellas no solicitaban la autorización expresa e informada por parte de los Titulares para el tratamiento de sus datos personales. En virtud de esto la SIC advirtió que dicha situación debe ser cumplida por las instituciones educativas no sólo para el tratamiento de datos personales de los estudiantes, sino también para el tratamiento de datos de los padres o acudientes, personal administrativo y docente en sus formularios y/o contratos laborales.

De manera que indicó a las respectivas instituciones que las personas deben autorizar expresamente la información que pueda ser incluida en una base de datos. Sin autorización previa y expresa del Titular, los datos no pueden ser tratados, recolectados, divulgados o almacenados. Se refirió igualmente al artículo 9 de la Ley 1581, el cual establece los modos por los cuales se puede obtener la autorización del tratamiento.

La SIC hace el análisis de cómo debe solicitar la autorización de menores de edad, cuando éstos son adolescentes, situación que incluye tanto a colegios como a instituciones de educación superior. Apoyándose para ello en el concepto de la misma entidad con Radicado No. 13-232774 frente al tratamiento de datos personales realizado por instituciones educativas, concluyendo que resulta razonable obtener la autorización previa, expresa e informada directamente del adolescente, cuando se recolectan datos de estos para que se puedan inscribir como aspirantes o matricular en alguno de los programas ofrecidos por la institución, mientras que tratándose de niños y niñas, debe obtener la autorización de sus padres o representantes legales.

Por otro lado, en virtud del principio de finalidad se deriva el deber de informar al Titular las finalidades del tratamiento, la SIC ha establecido que los datos deben ser procesados por un propósito específico y explícito, razón por la que se impone el deber de informar clara, suficiente y previamente al Titular acerca de la finalidad de la información suministrada, prohibiendo así la recopilación de datos sin la especificación clara acerca de su finalidad, obligación impuesta por el literal c) del artículo 17 de la ley 1581.

De acuerdo con la SIC este deber cobra especial relevancia, pues sólo conociendo las finalidades del tratamiento el Titular podrá libremente otorgar la autorización previa, expresa e informada para el tratamiento de sus datos personales. Por tal motivo la SIC indica que el Responsable del tratamiento de datos debe informar a su Titular: el tratamiento al cuál serán sometidos sus datos personales y la finalidad

del mismo; el carácter facultativo de las respuestas cuando las preguntas versen sobre datos sensibles; los derechos que le asisten como Titular; la identificación, dirección física o electrónica y teléfono del Responsable del tratamiento.

En virtud de lo anterior, los principales aspectos que constituyen un incumplimiento por parte de las IEPBM son:

- No solicitar y conservar autorización previa, expresa e informada por los Titulares. Para ello es importante que las IEPBM conozcan plenamente aquellos puntos en los cuales se realiza recolección.
- No implementar la solicitud de autorización previa, expresa e informada por parte de todas las personas de quienes recolectan datos. Siendo estos los alumnos, padres o acudientes, personal administrativo, personal docente, entre otros.
- No realizar distinción al momento de recolección de datos de menores de edad, si se realiza recolección de adolescentes o de niños y niñas, ya que la obtención de la autorización varía. De esta manera, cuando se recolectan datos personales de adolescentes es factible obtener la autorización directamente del Titular, mientras que si se recolectan datos personales de niños y niñas, ésta debe obtenerse directamente de los padres o acudientes.

3.2.3. Deber de conservar la información bajo las condiciones de seguridad y de garantizar la reserva de la información

El literal d) del artículo 17 de la ley 1581 de 2012 estableció como deber de los Responsables del tratamiento la conservación de la información con todas las medidas que sean necesarias con el fin de no poner en riesgo los datos de los Titulares. Dicho deber deriva de los principios de seguridad y confidencialidad establecidos en los literales g) y h) del artículo 4 de la Ley 1581.

En virtud de este deber, el Responsable debe manejar los datos recolectados con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a sus registros evitando la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

La SIC estableció en sus resoluciones sancionatorias que las instituciones Responsables del tratamiento, para el cumplimiento de este deber y principios, debe tener en cuenta por un lado el volumen de la base de datos y la naturaleza de los datos que trata. Haciendo que las medidas o controles de seguridad sean directamente proporcionales a los datos alojados.

De la adopción de medidas de conservación de la información y de los controles de seguridad implementados dependen que se minimicen los riesgos de filtración de los datos personales. Es por eso que la SIC indicó a las instituciones educativas su deber de contar con manuales internos de seguridad en el manejo de la información de los Titulares; contar con cláusulas de confidencialidad en sus contratos laborales o suscribir acuerdos de confidencialidad adjuntos a estos, indicando que dichos acuerdos de confidencialidad deben establecer claramente la obligación de garantizar la reserva de la información personal de los Titulares incluso después de finalizada su relación con alguna de las labores que comprende el tratamiento; y contar con manuales y procedimientos claros para garantizar la seguridad de la información.

La necesidad de que el dato se mantenga bajo los controles de seguridad necesarios y suficientes se desprende de fenómenos como la globalización el internet de las cosas o el “big data”, que día a día propician un escenario benéfico para el flujo constante de información a nivel internacional, la cual, a su vez, al encontrarse almacenada en sistemas automatizados, aumenta los riesgos de filtración de datos y hace necesaria la adopción de medidas eficaces para su conservación dentro de los dispositivos idóneos y bajo parámetros adecuados para evitar su circulación desmedida. (Superintendencia de Industria y Comercio, 2017).

También menciona la SIC que el deber de seguridad se encuentra vinculado con el principio de confidencialidad, en la medida en que el tratamiento de datos sólo puede hacerlo la persona autorizada y debe estar sujeto a los límites que se derivan de la naturaleza del mismo y de la ley, igualmente se ven relacionados los principios de acceso, y de circulación restringida. (Superintendencia de Industria y Comercio, 2016).

En consecuencia, los principales incumplimientos que se dan con relación a este deber son los siguientes:

- No tener en cuenta el volumen de bases de datos ni la naturaleza de los datos personales contenidos en dichas bases, a efectos de determinar cuáles son las medidas humanas, técnicas y administrativas necesarias para conservar la información bajo adecuados niveles de seguridad
- No identificar ni minimizar los riesgos de filtración de datos personales.
- No contar con manuales internos de seguridad en el manejo de la información de los Titulares.
- No contar con cláusulas de confidencialidad en sus contratos laborales o suscribir acuerdos de confidencialidad adjuntos a estos.

3.2.4. Deber de contar con las políticas de tratamiento de datos y de informar a los Titulares sobre su existencia

Este aspecto se encuentra regulado en el artículo 25 de la ley 1581 y reglamentado en los artículos 2.2.2.25.3.1. y 2.2.2.25.3.2 del Decreto Único Reglamentario, normas en virtud de las cuales el Responsable del tratamiento no puede dar tratamiento a la información bajo estándares inferiores a los establecidos en las mencionadas normas, las cuales son medidas mínimas establecidas.

Así pues, la SIC ha hecho mención en sus resoluciones sancionatorias contra instituciones educativas y ha reiterado la obligatoriedad que para estas también represente el deber de contar con políticas de tratamiento de datos ajustadas, cuando menos, a los mínimos legales establecidos. También ha hecho mención a la posibilidad contemplada en el artículo 2.2.2.25.3.2 del Decreto Único Reglamentario en virtud de la cual se establece que, de ser imposible poner en conocimiento inmediato las políticas de tratamiento de datos a los Titulares, se les debe informar mediante un aviso de privacidad sobre la existencia de dichas políticas y la forma de acceder a las mismas.

Este último aspecto torna relevancia para las IEPBM, pues la SIC se ha pronunciado respecto del deber de contar con avisos de privacidad para los datos personales recolectados a través de sistemas de videovigilancia. (Superintendencia de Industria y Comercio, 2018)

Así pues, hizo mención a la Resolución 61950 de 2017, respecto de los datos recolectados a través de sistemas de video vigilancia, determinando que estas actividades implican cualquier forma de

tratamiento de imágenes de datos personales a través de cámaras IP, mini-cámaras, Circuito Cerrado de Televisión (CCTV), entre otros.

Indicando que las actividades de tratamiento de imágenes implican, entre otras, la captación, grabación, transmisión, almacenamiento, conservación o su reproducción en tiempo real o posterior, por lo que al igual que el resto de datos personales se encuentran sujetas al régimen general de protección de datos personales. La recolección de imágenes a través de sistemas de video vigilancia requiere previamente de la autorización suministrada por parte de su Titular bien sea por escrito, de forma oral o mediante conductas inequívocas. Por lo tanto, para la aplicación de las garantías del marco legal antes señalado, se hace necesario adoptar los mecanismos necesarios suficientes para informar a los Titulares que sus datos están siendo recolectados por medio de un sistema de videovigilancia.

Concluyendo así pues, que las IEPBM que usen sistemas de videovigilancia deben contar con un aviso de privacidad que cumpla con los requisitos del Art. 2.2.2.25.3.2. del Decreto Único Reglamentario.

i) el Responsable del tratamiento; ii) cuál será el tratamiento que se dará a su información; iii) los derechos que le asisten al Titular; iv) en dónde se encuentra publicada la política.

En consecuencia, los principales incumplimientos a este deber son:

- No contar con políticas de protección de datos personales que se adecuen a, por lo menos, los estándares mínimos establecidos en el régimen general de tratamiento de datos personales.
- No contar con mecanismos que permitan poner de conocimiento inmediatamente la política de tratamiento de datos personales a los Titulares.
- No contar con avisos de privacidad que cumplan con los requisitos legales mínimos, cuando no sea posible poner en conocimiento inmediato la política a los Titulares, como es en el caso de uso de sistemas de videovigilancia en los establecimientos educativos.

3.2.5. Deber de adoptar un manual interno de políticas y procedimientos para el tratamiento de datos personales (deber de tramitar consultas y reclamos formulados por los Titulares)

La SIC hace mención a este deber, el cual se encuentra consagrado en el literal k) del artículo 17 de la ley 1581 y se encuentra reglamentado por el artículo 2.2.2.25.3.1 del Decreto Único Reglamentario, indicando que para dicha entidad, la adecuada gestión y utilización de la información personal depende en gran medida de la consagración de un procedimiento claro, expedito, sin restricciones que sea puesto en conocimiento de los Titulares y, que sobre todo sea implementado por las instituciones, pues no basta con simplemente contar con los referidos manuales, sino que debe implementarse de manera que garantice la protección del *habeas data*. (Superintendencia de Industria y Comercio, 2016).

Así, menciona que dichos manuales propenden en especial por garantizar a los Titulares que se les preste atención a sus consultas y reclamos, lo que se materializa en garantizar el pleno y efectivo ejercicio del derecho de *habeas data*, en virtud del deber que en igual sentido se encuentra en el literal a) del artículo 17 de la ley 1581, implementando así mecanismos que le permitan a los Titulares acceder en cualquier momento a su información.

Haciendo reiterada mención a lo indicado por la Corte Constitucional en Sentencia C-748 de 2011, según la cual los contenidos mínimos del *habeas data* comprende el derecho de acceso a la información que reposa en bases de datos; el derecho a incluir nuevos datos; el derecho a actualizar información; el derecho a que la información se rectifique o corrija y; el derecho a excluir información de una base de datos.

Lo anterior en concordancia con el artículo 2.2.2.25.4.2 del Decreto Único Reglamentario señala que los Responsables y Encargados deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares, para que estos puedan acceder a los datos personales que estén bajo el control de aquellos y ejercer sus derechos sobre los mismos. Por lo cual se le exige a las instituciones de educación, en materia de protección de datos personales tener un correo electrónico; un funcionario; un acceso directo en el portal web; una línea telefónica; entre otros. Y adicionalmente que dichas medidas se encuentren implementadas y documentadas, a efectos de demostrar a la SIC la implementación del principio de responsabilidad demostrada, de tal suerte que la organización sea capaz de evidenciar que ha adoptado medidas proporcionales con la naturaleza jurídica y dimensión de la organización, la naturaleza de los datos que son objeto de tratamiento el tipo de tratamiento y, sobre todo,

que ha implementado un mecanismo para la medición y control de los riesgos que puedan presentarse frente al derecho de los Titulares. (Superintendencia de Industria y Comercio, 2017).

Por lo tanto, las principales conductas que acarrearán el incumplimiento a este deber son las siguientes:

- No identificar los flujos de información interna por los cuales atraviesen los datos personales.
- No establecer mecanismos y procedimientos para la atención de quejas y reclamos en torno al habeas data.
- No documentar debidamente un manual interno de políticas y procedimientos para el tratamiento interno que se da a los datos personales y el procedimiento para la atención de consultas, quejas y reclamos por parte de los Titulares.

En virtud de las resoluciones expuestas, se evidencia que las IEPBM son sujetos Responsables del tratamiento y protección de datos personales. Por ello, las mismas están obligadas al cumplimiento de lineamientos, y políticas de seguridad que deben cumplir con los parámetros impuestos en el régimen general para el manejo de información de carácter personal.

Para el caso de las IEPBM existen distintas circunstancias que implican tratamiento de datos personales, pues se deben dar tratamiento a información personal tanto de colaboradores, como de estudiantes los cuales en algunas circunstancias pueden ser menores de edad, generando una responsabilidad adicional sobre la IEPBM, lo cual deberá plasmarse en sus manuales de procedimientos internos de la institución, en su calidad de Responsables del tratamiento de datos personales.

De los pronunciamientos de la SIC, se puede resaltar como punto de partida el Principio de Responsabilidad Demostrada en la recolección de información y datos personales que realizan distintas entidades y organizaciones como las IEPBM, toda vez que este principio propende por la implementación de aquellas prácticas que permitan evidenciar el modo como se dispone dicha información y las estrategias o modos de garantizar su protección. Generando deberes como lo son la incorporación y desarrollo de políticas de tratamiento de datos según los lineamientos antes expuestos, que bajo ninguna circunstancia se podrán disminuir o prestar una protección inferior a la ya dispuesta por ley.

4. CONCLUSIONES: RECOMENDACIONES PARA EL EFECTIVO CUMPLIMIENTO DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LAS INSTITUCIONES DE EDUCACIÓN PREESCOLAR, BÁSICA Y MEDIA

Como se evidenció, el ordenamiento jurídico colombiano exige que los sujetos obligados adopten políticas internas efectivas, por disposición expresa del artículo 27 del Decreto 1377 de 2013. Estas políticas internas no pueden limitarse a reproducir textos legales ni son meras declaraciones de principios. Por el contrario, la adopción de políticas internas efectivas parte del resultado de un proceso de debida diligencia al interior de la organización que permita formularlo (Superintendencia de Industria y Comercio, 2015). Un programa efectivo de protección de datos debe incorporar políticas que, i) respondan a los ciclos internos de gestión de datos de la organización y ii) generen resultados medibles que le permitan probar ese grado de diligencia especial. Concretamente el artículo en cita exige que esas políticas garanticen la existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del Responsable para la adopción e implementación de políticas consistentes con la ley.

Dada la necesidad de adaptar las políticas y procedimientos relativos al tratamiento de datos personales a las particularidades administrativas y operativas propias de cada obligado, en este acápite se hará referencia a las principales obligaciones de los Responsables y Encargados del tratamiento de datos personales, y se referirán a aspectos concretos de las IEPBM atendiendo a la experiencia brindada por las sanciones impuestas por la SIC, las disposiciones de la Ley General de Educación y a pronunciamientos del Ministerio de Educación respecto a obligaciones propias del sector educativo que implica que se realice tratamiento de datos personales.

4.1. Recomendaciones respecto al cumplimiento del deber de solicitar información previa, expresa e informada a los Titulares y la información de las finalidades del tratamiento

Las IEPBM cuentan con diversos procesos internos que necesariamente implican la recolección de datos personales (Superintendencia de Industria y Comercio, 2012). La identificación de estos procesos cobra relevancia pues los momentos en los cuales la IEPBM solicite información personal a los Titulares es el inicio de las actividades de tratamiento de datos y donde inician sus deberes como Encargado del tratamiento. Así pues, algunos de los momentos relevantes de la recolección de datos son:

1. Procesos de inscripciones y preinscripciones;
2. Procesos de matrículas
3. Recepción de candidatos de talento humano, docente o administrativo
4. Registro de acudientes
5. Recolección de imágenes personales a través de video vigilancia

En estos procesos internos la IEPBM se ve abocada a recolectar datos personales, en virtud de su propia actividad. Sin embargo, es importante también tener en cuenta que es el inicio del tratamiento de datos personales realizado por estas instituciones, por lo cual es preciso que las IEPBM auditen sus procesos internos e identifiquen aquellos puntos de recolección de información.

Como se evidenció en las resoluciones evaluadas en el capítulo anterior, muchas son las formas que existen hoy día para solicitar datos personales a los Titulares, una de dichas formas utilizadas por las IEPBM es por medio de formularios de inscripción. Dichos formularios pueden ser tanto para aspirantes académicos como para aspirantes a hacer parte del talento humano de la institución y puede verse de manera física (mediante formularios impresos) o electrónica (por medio de páginas web propias o de terceros, formularios de redes sociales, entre otros).

En este y todos los momentos es importante que previamente la IEPBM tenga claro las finalidades para el tratamiento de datos, concretamente, la finalidad que persigue en este punto es simplemente identificar al individuo que pretende vincularse a la IEPBM, por lo que la información debe guardar estrecha relación con dicha finalidad (Superintendencia de Industria y Comercio, 2012).

En virtud de dicha finalidad se evidencia cómo el Titular aún no se ha vinculado con la institución, razón por la cual en este punto no se estima conveniente solicitar datos sensibles tales como

relativos a salud, requerimientos de educación especiales, información financiera, ni ningún otro tipo de dato sensible toda vez que no se evidencia guardar relación alguna con el fin perseguido en esta etapa, cuando se trata de los primeros contactos que el Titular tiene con la institución.

Distinta situación se presenta en el proceso de matrícula, pues en esta etapa se requiere más información por parte de los Titulares que permita prestar adecuadamente el servicio de educación y que variará dependiendo del enfoque de la misma IEPBM, pudiendo incluso presentarse la situación en la cual se solicite información adicional para otras actividades curriculares o extracurriculares. La ley 115 de 1994 define matrícula como el acto que formaliza la vinculación del educando al servicio educativo. Se realizará por una sola vez, al ingresar el alumno a un establecimiento educativo, pudiéndose establecer renovaciones para cada período académico." De manera que existe regulado en la legislación nacional un contrato específico, el cual es el contrato de matrícula". (Ministerio de Educación, 2016, p. 6).

En todo caso se debe incluir en dichos formularios un texto claro en el cual se informe, cuando menos i) qué tipo de información se va a recolectar, (ii) el uso o finalidad específico que el centro educativo considera darle a esa información; (iii) el acceso que personal del centro educativo o terceros autorizados por la ley pueden tener a esa información; (iv) la posibilidad acorde con la ley de transferir esa información – entre otros – a otros centros educativos, autoridades y Encargados del tratamiento ubicados en el territorio nacional o en un lugar en el extranjero; (v) los casos en que la información personal recolectada puede ser cancelada o eliminada definitivamente de los archivos o bases de datos del centro educativo; (vi) los derechos que les asisten; y (vii) la forma como pueden acceder a las políticas de tratamiento de la información adoptadas por este.

Cuando la IEPBM cuente con sistemas de videovigilancia en sus instalaciones, debe instalar un aviso de privacidad con los anteriores elementos en zonas visibles aledañas a los sitios donde se esté realizando la videovigilancia.

Así, en síntesis de las recomendaciones, se debe tener en cuenta lo siguiente:

- Identificar aquellos puntos de contacto con los Titulares de datos personales en los cuales se realice la recolección de sus datos personales.
- Identificar los tipos de datos personales que se recolectan en cada punto de recolección.

- Determinar la necesidad de la recolección de datos personales en cada punto identificado y los fines de la recolección para cada uno.
- Identificar los tipos de Titulares a los cuales se les hará recolección y tratamiento de datos personales.
- Implementar formatos de solicitud de autorización previa, expresa e informada, donde se informe a los Titulares las finalidades y la no obligatoriedad de suministrarlos cuando se traten de datos personales sensibles o de menores, y demás requisitos legales
- Implementar formatos de avisos de privacidad en aquellos puntos de recolección donde no sea posible obtener la autorización de manera escrita, con el lleno de los requisitos legales.

4.2. Recomendaciones respecto del deber de informar al Titular cuando se le soliciten datos sensibles:

La Sentencia C-748 de 2011 señaló que, “la prohibición de tratamiento de datos sensibles es una garantía del *habeas data* y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana. Sin embargo, en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios como la atención médica y la educación para la realización de derechos ligados precisamente a la esfera íntima de las personas”.

Es pertinente aclarar que, en materia de datos personales, más exactamente cuando se habla del sector educación, las IEPBM deben realizar la distinción legal que se encuentra en el artículo 3 del Código de Infancia y adolescencia que clasifica como menores de edad a todas aquellas personas entre 0 y 18 años. Por tal motivo, aunque sea indispensable el tratamiento de datos para la prestación del servicio de educación, el suministro de esta información puede poner en riesgo los derechos fundamentales propios de esta población, convirtiéndose en una obligación indispensable para el Responsable, la solicitud de una autorización expresa.

A manera de ejemplo, la IEPBM pueden tener en consideración lo conceptuado por el Ministerio de Educación, en concepto 37329 de 2019, en el cual concluyó que en virtud de lo dispuesto en el artículo

2.3.3.2.2.1.9 del Decreto 1075 de 2015⁹, que cuando se trata de educación preescolar los únicos datos que se le deben solicitar a los representantes legales de los menores es i) el registro civil de nacimiento y; ii) Certificación de vinculación a un sistema de seguridad social, no obstante el deber de las IEPBM de formalizar la matrícula aún cuando los padres del menor no aporten dicha información (Ministerio de Educación, concepto 37329, 2019). Este aspecto debe ser tenido en cuenta por aquellas IEPBM al prestar servicios de educación para la etapa preescolar, pues es un insumo relevante a efectos de determinar las finalidades del tratamiento de datos para esta etapa en específico y, la consecuente solicitud de autorización de tratamiento de datos personales y datos sensibles.

Por esto el artículo 12 de la ley 1581 de 2012, coloca en cabeza de la entidad Responsable de los datos el cumplimiento del deber de información y la solicitud de una autorización previo suministro de datos al momento de recolectar los mismos, el cual debe contener: a) El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; c) Los derechos que le asisten como Titular; d) La identificación, dirección física o electrónica y teléfono del Responsable del tratamiento.”

En el caso de incorporarse dentro de cualquier expediente o documento académico datos sensibles, los cuales son aquellos que hacen referencia a la “historia o reportes clínicos, diagnósticos y evaluaciones psicológicas, particulares requerimientos o limitaciones por cuestiones físicas o de salud, necesidades educativas especiales o preferencias sexuales o religiosas” (Superintendencia de Industria y Comercio, 2018). Deben tener una autorización previa y expresa por parte del Titular de los mismos y a su vez las IEPBM, deben otorgarle mayor control y protección frente a los sujetos que tengan acceso a estos, limitando su utilización solo a su ámbito material, es decir, a su finalidad.

Así, en síntesis de las recomendaciones, las IEPBM deben tener en cuenta lo siguiente:

⁹ “Requisitos para el ingreso al nivel de preescolar. Para el ingreso a los grados del nivel de educación preescolar, las instituciones educativas, oficiales y privadas, únicamente solicitarán copia o fotocopia de los siguientes documentos: 1. Registro civil de nacimiento del educando. 2. Certificación de vinculación a un sistema de seguridad social, de conformidad con lo establecido en la ley. Si al momento de la matrícula, los padres de familia, acudientes o protectores del educando no presentaren dichos documentos o uno de ellos, de todas maneras, se formalizará dicha matrícula. La respectiva institución educativa propenderá por su pronta consecución, mediante acciones coordinadas con la familia y los organismos pertinentes. Parágrafo. Si el documento que faltare fuese el certificado de vinculación a un sistema de seguridad social, el educando deberá estar protegido por un seguro colectivo que ampare en general su salud, como en particular su atención inmediata en caso de accidente, situaciones que deberán preverse en el reglamento o manual de convivencia”.

- Identificar los datos sensibles a los cuales se les de tratamiento por parte de la IEPBM.
- Identificar los puntos de recolección de dichos datos sensibles.
- Identificar los fines de la recolección de dichos datos sensibles.
- Implementar en los formatos de solicitud de autorización con el lleno de los requisitos legales.

4.3. Respetto del deber de conservar la información bajo condiciones de seguridad y de garantizar la reserva de la información

Un aspecto de especial relevancia para las IEPBM en materia de tratamiento de datos personales es el manejo del expediente académico, toda vez que el mismo contiene información que identifica todo el proceso académico del alumno, la cual es diversa teniendo en cuenta las diferentes etapas del ciclo académico, y actividades que involucran al alumno en la IEPBM.

El primer factor a tener en cuenta es determinar si el expediente se va a manejar de manera física o digital, pues de eso dependerá el tratamiento que se le dé con relación a la conservación y la reserva de la información. En el primer caso lo recomendable es designar un sistema de gestión de archivo , en virtud del cual se pueda garantizar los mayores estándares de protección y conservación de la información; por otro lado, si se trata de un expediente digital, es preferible contar con un software especializado para el efecto, cuyos estándares cumplan cuando menos los estándares mínimos de protección nacional y se cuente con una debida implementación de sistemas de seguridad informática, pudiendo para el efecto implementar en el marco de la implementación de un sistema de cumplimiento de protección de datos, el adquirir licencias de software que cumplan los lineamientos de la norma técnica ISO 27001¹⁰.

Cabe mencionar que existe una gran posibilidad de que se incorporen datos sensibles al expediente académico, tales como portes médicos o psicológicos, limitaciones físicas o condiciones especiales de aprendizaje, lo cual exige por parte de la IEPBM un mayor nivel de protección.

¹⁰ Norma Técnica elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

Para implementar medidas efectivas con relación al punto anterior es necesario identificar qué agentes del entorno interactúan con el expediente académico, de manera que en las políticas y manuales internos de tratamiento de datos personales se incluyan limitaciones para únicamente a las actividades o gestiones que correspondan al respectivo agente. La implementación de expedientes digitales hará más sencillo el control y medición de este aspecto, pues bastaría con que el software cuente con la posibilidad de crear distintos perfiles con distintos permisos de acceso, de manera que se pueda dar trazabilidad al uso que se haga a los datos allí contenidos, garantizando así la seguridad y la reserva de la información. Adicionalmente deben implementarse en sus procesos de contratación la inclusión de cláusulas de confidencialidad en los contratos de sus empleados.

Por lo mencionado, es recomendable que las IEPBM implementen un manual de funciones y un protocolo de acceso a la información contenida en el expediente académico, y un sistema de respaldo de los expedientes académicos, donde se incluya una actualización periódica, de manera que se facilite su reconstrucción o reposición en caso de destrucción o pérdida del mismo.

También deben tener en cuenta que El Ministerio de Educación, analizando las disposiciones de la ley 594 del 2000¹¹, concluyó que las Instituciones de educación preescolar, básica y media,

“deben conservar en todo momento, el archivo de los documentos que contengan información académica de los estudiantes que han tenido matriculados, en razón a que dichos documentos son prueba del servicio público prestado, lo cual es de interés para las autoridades públicas así como para las personas que recibieron este servicio educativo (...) En esa medida, y teniendo en cuenta que los documentos que producen las instituciones educativas son un medio probatorio que evidencia la forma como éstas realizan sus actividades, es claro que se trata de una herramienta con la cual las entidades territoriales pueden ejercer sus funciones de inspección y vigilancia sobre dichas instituciones”(Ministerio de Educación, Concepto 39801, 2015, p. 2).

Así, en síntesis de las recomendaciones, las IEPBM deben tener en cuenta lo siguiente:

¹¹ Ley General de archivo

- Identificar y determinar la conservación de la información contenida en documentos (matrícula, expediente académico, entre otros) se realizará en formato físico o en formato digital.
- Identificar los agentes que interactúan entorno a la información personal contenida tanto en el expediente académico como en bases de datos y demás documentos contentivos de datos personales.
- Establecer limitaciones para únicamente a las actividades o gestiones que correspondan al respectivo agente.
- Implementar en sus procesos de contratación la inclusión de cláusulas de confidencialidad en los contratos de sus empleados.
- Implementar un manual de funciones y un protocolo de acceso a la información contenida en el expediente académico, y un sistema de respaldo de los expedientes académicos, donde se incluya una actualización periódica, de manera que se facilite su reconstrucción o reposición en caso de destrucción o pérdida del mismo.

4.4. Respecto del deber de contar con un manual interno de políticas y procedimientos para garantizar, en especial, la atención de consultas y reclamos y con ello garantizar el pleno y efectivo ejercicio del derecho de *habeas data*

Como se evidenció del análisis de las resoluciones de la SIC y de la obligación contenida en el literal k) del artículo 17 de la ley 1581, corresponde a los Responsables y Encargados del tratamiento adoptar manuales internos de políticas y procedimientos en el que se expliquen claramente todos los parámetros y reglas que utilizará la organización para garantizar el correcto tratamiento de los datos personales, en especial, el procedimiento que la organización utilizará para atender las quejas, consultas y reclamos presentados por los Titulares en ejercicio de su derecho de *habeas data*.

Además de sus requisitos mínimos legales, se recomienda que dicho manual documente los procedimientos relacionados con:

- a. Recolección, almacenamiento, uso, circulación, supresión o disposición final de la información personal

- b. El acceso y corrección de datos personales
- c. La conservación y eliminación de información personal
- d. El uso responsable de la información, incluyendo controles de seguridad administrativos, físicos y tecnológicos
- e. Inclusión en todos los medios contractuales de la Institución de una cláusula de confidencialidad
- f. Procedimiento para la atención de peticiones, quejas, denuncias y reclamos

Es decir, todos los aspectos hasta el momento mencionados deben estar contemplados y documentados en los manuales internos de políticas y procedimientos, de manera que sean de conocimiento de todas las personas que se encuentran relacionadas con el tratamiento de datos personales al interior de las IEPBM, para garantizar así que los manuales sean implementados.

Adicionalmente se reitera el deber de poner a disposición de los Titulares las políticas de tratamiento de datos, lo cual se puede lograr mediante un enlace de acceso desde su web o mediante un aviso de privacidad, de conformidad con lo establecido en el Decreto Único Reglamentario.

En síntesis, se debe diseñar e implementar unas políticas de tratamiento de datos personales y un manual interno que cumpla a cabalidad, por lo menos, con los requisitos legales mínimos exigidos, incorporando los resultados de las recomendaciones precedentes para las obligaciones que en su calidad de Responsable le corresponden.

4.5. Otras recomendaciones y aspectos relevantes a tener en cuenta en los Manuales Internos de Políticas y Procedimientos

4.5.1. Designación de un oficial de protección de datos personales

El decreto 1377 de 2013, en su Artículo 23. Designa que todo “Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente Decreto.”

Con la finalidad que esta persona se encargue de verificar todas aquellas actividades que se desarrollen dentro de la corporación y sean referentes al tratamiento de datos. A su vez, esta persona debe dar respuesta de manera inmediata frente a cualquier queja o reclamo que realicen los Titulares del derecho *habeas data*, o cualquier entidad que realice actividades de control y vigilancia.

Se encuentra en cabeza del oficial de privacidad, así conocido en materia internacional, “la estructuración, diseño, y administración de un programa que permita a la organización cumplir con todas aquellas normas sobre protección de datos personales, así como establecer determinados controles para los programas que se realicen, su evaluación y revisión permanente” (Superintendencia de Industria y Comercio, 2013, p,11).

En consecuencia, la función de un oficial de privacidad es crucial para el desarrollo de una corporación en materia de responsabilidad demostrada, debido a que permiten promover e implementar controles que buscan administrar debidamente el riesgo a la hora de tratar los datos, sirviendo como canal directo de comunicación con el personal por medio de auditorías que permiten obtener el análisis de desempeño de la corporación. A su vez está sirviendo como puente entre el exterior, al poder brindar respuestas directas, claras y contundentes a la hora de cualquier tipo de reclamo por parte de una entidad de control y vigilancia, o los Titulares del derecho.

4.5.2.Sistema Integrado de Matrícula -SIMAT-

Con relación al tema de matrículas, las IEPB oficiales, deben considerar como punto clave en sus manuales internos de políticas y procedimientos de tratamiento de datos la inclusión y armonización con el uso del Sistema Integrado de Matrícula (SIMAT) del Ministerio de Educación, cuyas directrices se encuentran contenidas en la Circular No. 09 de 2012 de la misma entidad. El Ministerio de Educación define la matrícula como (...) El proceso de matrícula es el conjunto de procedimientos y actividades que permiten garantizar la continuidad de los alumnos antiguos y el ingreso de alumnos nuevos en el sistema educativo del país. Para el control y desarrollo efectivo de este proceso el Ministerio de Educación Nacional, tiene a disposición de los establecimientos educativos y de las secretarías de educación el Sistema Integrado de Matrículas SIMAT, el cual facilita la inscripción de alumnos nuevos, la

actualización de datos del estudiante y la IEPBM, el reporte de novedades de los alumnos registrados, y la generación de reportes y obtención de informes asociados a fenómenos como la deserción. (Ministerio de Educación, Concepto 405, 2018, p. 2). El Ministerio de Educación describe al SIMAT como:

“una herramienta que permite organizar el proceso de matrícula en todas sus etapas, así como tener una fuente de información única oportuna, confiable y disponible para la gestión, la toma de decisiones, la formación, seguimiento y evaluación de la política sectorial y la distribución eficiente de los recursos del Sistema General de Participaciones para educación”. (Ministerio de Educación, 2018, p. 2).

4.5.3. Gobierno Escolar

El Ministerio de Educación se refirió a la ley 115 de 1994, la cual impone la obligación a todas las instituciones de educación, públicas o privadas, de contar con un gobierno escolar¹². También se hizo mención al artículo 2.3.3.1.4.1. del Decreto 1075 de 2015¹³, concluyendo que las IEPBM deben contar con un gobierno escolar en virtud del cual se garantice la participación de todos los órganos que componen la comunidad educativa. Disponiéndose además que en las IEPBM privadas el gobierno escolar debe estar integrado al menos por el Consejo Directivo, el Consejo Académico y el Rector, sin perjuicio de que puedan incluir otros órganos que consideren necesarios de acuerdo con su proyecto educativo institucional (Ministerio de Educación, 2020, p. 3).

¹² “Artículo 142. Conformación del gobierno escolar. Cada establecimiento educativo del Estado tendrá un gobierno escolar conformado por el rector, el Consejo Directivo y el Consejo Académico. Las instituciones educativas privadas establecerán en su reglamento, un gobierno escolar para la participación de la comunidad educativa a que hace referencia el artículo 68 de la Constitución Política. En el gobierno escolar serán consideradas las iniciativas de los estudiantes, de los educadores, de los administradores y de los padres de familia en aspectos tales como la adopción y verificación del reglamento escolar, la organización de las actividades sociales, deportivas, culturales, artísticas y comunitarias, la conformación de organizaciones juveniles y demás acciones que redunden en la práctica de la participación democrática en la vida escolar. Los voceros de los estamentos constitutivos de la comunidad educativa, podrán presentar sugerencias para la toma de decisiones de carácter financiero, administrativo y técnico-pedagógico. Tanto en las instituciones educativas públicas como privadas, la comunidad educativa debe ser informada para permitir una participación seria y responsable en la dirección de las mismas”.

¹³ “Artículo 2.3.3.1.5.2. Obligatoriedad del Gobierno Escolar. Todos los establecimientos educativos deberán organizar un Gobierno para la participación democrática de todos los estamentos de la comunidad educativa, según lo dispone el artículo 142 de la Ley 115 de 1994”.

4.5.4. Enfermería

Por otra parte, el Ministerio de Educación ha determinado que si bien es cierto la prestación de servicios de emergencia en salud escapa de la competencia de las IEPBM, es su deber y tienen la responsabilidad de tomar todas las medidas pertinentes de seguridad y cuidado de sus educandos y establecer dentro de sus reglamentos protocolos para atención de casos relativos a la salud, o eventos que representen daños a la salud física garantizando la atención inmediata y la remisión a las entidades pertinentes (Ministerio de Educación, 2019, p. 5).

De manera que las IEPBM que opten por disponer de servicios de enfermería en sus establecimientos, deben tener presente que la actividad de enfermería se encuentra regulada en la ley 911 de 2004, la cual dispone en su artículo 6 el deber del profesional de enfermería de informar y solicitar el consentimiento de la persona o familia previa a realización de intervenciones de cuidado de enfermería y; el artículo 37 de la citada ley exige al profesional de enfermería adoptar los formatos y medios de registro que respondan a las necesidades de información que se deba mantener acerca de los cuidados de enfermería que se prestan a los sujetos de cuidado.

Por lo que la disposición de servicios de enfermería representa para la IEPBM un punto relevante en materia de tratamiento de datos personales, lo cual debe ser tenido en cuenta por las respectivas Instituciones a efectos de incluir la labor de la enfermería en sus manuales internos.

De esta manera, las propuestas realizadas posibilita en principio a las IEPBM la inclusión de estos aspectos y aspectos propios de cada institución en sus políticas de tratamiento de datos personales y sus manuales internos de políticas y procedimientos, para lograr en las mismas un nivel adecuado de cumplimiento del régimen de tratamiento de datos personales articulado con las obligaciones propias que como IEPBM tienen a su cargo y que implican necesariamente el tratamiento de datos personales. Otorgando en consecuencia un mayor nivel de protección de datos personales de los Titulares y que los mismos tengan un conocimiento previo y claro del tratamiento que se le dará a sus datos personales.

REFERENCIAS

- Remolina Angarita N, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16. *International Law, Revista Colombiana de Derecho Internacional*, 489-524 (2010)
- Remolina Angarita N (julio-diciembre 2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales*. Recuperado de https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_- Nelson-Remolina.pdf
- Remolina Angarita, Nelson. Álvarez Zuluaga, Luisa Fernanda. (2018). Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability– en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos. Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58.
- Remolina Angarita, N. (2013). Tratamiento de datos personales. 1a ed. Bogotá, Colombia: Legis
- Pérez Fernández, O. E. (2017). El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia
- Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *IDP. Revista de Internet, Derecho y Política*, (5), 47-61. Recuperado de <http://www.redalyc.org/html/788/78812861005/>
- Galvis Cano, L. (2012) *Revista Lebret. Protección de Datos en Colombia Avances y Retos*, (4), 195-214. Recuperado de <http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336/336>
- Bautista Avellaneda, M. E. (2015). Marco legal en Colombia, la Ley Estatutaria de Protección de Datos y el tratamiento penal. En: M. E. Bautista Avellaneda. *El derecho a la intimidad y su disponibilidad pública* (pp. 41-51). Bogotá: Universidad Católica de Colombia

- Bautista Avellaneda, M. E. (2015). Marco constitucional y jurisprudencia constitucional del derecho a la intimidad. En: M. E. Bautista Avellaneda. El derecho a la intimidad y su disponibilidad pública (pp. 29-38). Bogotá: Universidad Católica de Colombia
- Quiroga, A (26 de septiembre de 2014). Asuntos: legales. Recuperado de <https://www.asuntoslegales.com.co/analisis/andres-felipe-quiroya-511176/aplicacion-del-principio-de-responsabilidad-demostrada-2173831>
- Aguilar, M. A. (2018). LA LEY DE PROTECCIÓN DE DATOS EN COLOMBIA: SUS INICIOS Y EXAMEN DE SUS PRINCIPALES POSTULADOS. *Universidad Católica de Colombia*, 18. <https://repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Protección%20De%20Datos%20En%20Colombia.pdf>
- Deloitte. (2015). Guía para la implementación del principio de responsabilidad demostrada en el tratamiento de datos personales. *Boletín Sector Público*. Recuperado de <https://www2.deloitte.com/content/dam/Deloitte/co/Documents/legal/Boletin%20002%20-%20Protección%20de%20datos%20personales%20V1.pdf>
- Goyes, A. (2014). La educación: Derecho fundamental o servicio público ¿Dicotomía o integralidad? *Revista Universitaria*, 3(2), 1-17.
- Menéndez, J., y Gayo, M. (2014). Derecho e informática. Ética y legislación. *Librería Bosch*.
- Pérez, A. (1992). Del habeas corpus al habeas data. *Informática y derecho*, 153-161.
- Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum jus*, 8(1), 107-139.

REFERENCIAS LEGALES:

- Ministerio de Educación. (2016). *La educación en Colombia*. Recuperado de https://www.mineduacion.gov.co/1759/articles-356787_recurso_1.pdf
- Ministerio de Educación. (2018). Planeación básica. Recuperado de <http://bi.mineduacion.gov.co:8380/portal/web/planeacion-basica/zona-de-atencion1>

Superintendencia de Industria y Comercio. (s.f). *Guía para el tratamiento de datos personales para el sector de la educación pública y privada*. Recuperado de https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Guia_datos_educacion_publica_nov27.pdf

Superintendencia de Industria y Comercio. (s.f) *Guía para la implementación del principio de responsabilidad demostrada (Accountability)*. Recuperado de <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

Resolución Número 48813 de 2018. (12 de julio de 2018). Superintendencia de Industria y Comercio.

Resolución Número 5848 de 2019. (14 de marzo de 2019). Superintendencia de Industria y Comercio.

Resolución Número 51290 de 2018. Bogotá (23 de julio de 2018). Superintendencia de Industria y Comercio.

Resolución Número 44029 de 2018. (25 de junio de 2018). Superintendencia de Industria y Comercio.

Resolución Número 63316 de 2017. (30 de agosto de 2018). Superintendencia de Industria y Comercio.

Resolución Número 85323 de 2016. (12 de diciembre de 2016). Superintendencia de Industria y Comercio.

Resolución Número 46693 de 2016. (16 de julio de 2016). Superintendencia de Industria y Comercio.

Sentencia T-414, Ref: expediente T – 534 (1992, 16 de junio). Corte Constitucional (Cristina Pardo, M,P).

Sentencia SU-624, T-216801 (1999, 25 de agosto). Corte Constitucional

Sentencia T-002, T-664 (1992, 8 de mayo). Corte Constitucional (Alejandro Martínez, M,P).

Sentencia T-1101, T-300.968 (2000, 18 de agosto). Corte Constitucional (Vladimir Naranjo, M,P).

Sentencia T-429, T-1011 (1992, 24 de junio de 1992). Corte Constitucional (Ciro Angarita, M,P).

Concepto 405 de 2018.(2018, 3 de enero). Ministerio de Educacion Nacional.

Concepto 14292 de 2019. (2019, abril 9). Ministerio de Educacion Nacional.

Concepto 39801 de 2015. (2015, abril 28). Ministerio de Educacion Nacional.

Concepto 68108 de 2016. (2016, junio 1). Ministerio de Educacion Nacional.

Concepto 37329 de 2019. (2019, marzo 27). Ministerio de Educacion Nacional.

Concepto 25642 de 2019. (2020, febrero 13). Ministerio de Educacion Nacional.