El Alcance del Principio de Responsabilidad Demostrada en cuanto al Responsable del Tratamiento de Datos Personales a partir de las Decisiones Administrativas de la Superintendencia de Industria y Comercio en los años 2014 – 2019 en Colombia.

Alejandra Jaramillo Londoño

Pontificia Universidad Javeriana

Facultad de Humanidades y Ciencias Sociales

Maestría en Derecho Empresarial

Cali

2020

El Alcance del Principio de Responsabilidad Demostrada en cuanto al Responsable del Tratamiento de Datos Personales a partir de las Decisiones Administrativas de la Superintendencia de Industria y Comercio en los años 2014 – 2019 en Colombia.

Alejandra Jaramillo Londoño

Trabajo de Grado

Director: Luis Félix Barriga Palomino

Profesor Departamento Ciencia Jurídica y Política

Pontificia Universidad Javeriana

Facultad Humanidades y Ciencias Sociales

Maestría en Derecho Empresarial

Cali

2020

Índice

Introducción

El marco jurídico de la protección de datos personales o derecho al *habeas data* en Colombia está contemplado en la Ley Estatutaria 1581 de 2012 y reglamentado por el Decreto Único 1074 de 2015 (que compiló, entre otras normas, el Decreto 1377 de 2013) y por el Capítulo V de la Circular Única de la Superintendencia de Industria y Comercio (en adelante SIC), normas que comprenden la normatividad aplicable a la protección de datos personales en Colombia. En ellas se dispuso que la entidad encargada de la vigilancia de la protección de datos personales en Colombia es la SIC (Ley 1581, 2012, art. 19). Para la aplicación de la ley, por Datos Personales se entiende "*cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*" (Ley 1581, 2012, art. 3, lit. c); a dichas personas naturales se les denomina Titulares, los cuales son los propietarios de sus datos personales; estos pueden estar organizados en conjuntos, a los cuales se les denomina Bases De Datos. Adicionalmente, hay una categoría especial de datos personales llamados Datos Sensibles que son "*aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación*" (Ley 1581, 2012, art. 5). El sistema de protección de datos personales regula la forma y condiciones en que debe realizarse su Tratamiento, entendido este como "*cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*." (Ley 1581, 2012, art. 3, Lit. g), por parte de los Responsables y encargados del Tratamiento; estos, a su vez, son quienes realizan el Tratamiento, ya sean personas naturales o jurídicas; por su parte los Responsables son los que "*deciden sobre las bases de datos y/o el Tratamiento de los datos*" (Ley 1581, 2012, art. 3, Lit. e), y los Encargados son terceros que realizan el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Sumado a lo anterior, el Artículo 2.2.2.25.6.1. del Decreto 1074 de 2015 establece el Principio de Responsabilidad Demostrada frente al Tratamiento de Datos Personales, el cual implica a los Responsables: (i) la obligación de estar en capacidad de demostrar, a petición de la SIC, que ha *"implementado medidas apropiadas y efectivas"* para cumplir con sus obligaciones, de manera proporcional con unos criterios generales establecidos en la norma; y (ii) la obligación de que, ante un requerimiento de la SIC, pueda suministrar evidencia de la implementación efectiva de *"medidas de seguridad apropiadas"*. Por su parte, el Artículo 2.2.2.25.6.2 del mismo decreto indica que, respecto de dichas medidas apropiadas y efectivas, debe garantizarse que: (i)

son consistentes con las instrucciones que la SIC imparta; (ii) exista una estructura proporcional al interior del Responsable para su adopción e implementación; (iii) se han adoptado mecanismos internos para ponerlas en práctica, incluyendo herramientas de implementación, entrenamiento y educación; y (iv) se han adoptado procesos para la atención de peticiones, consultas y reclamos de los titulares. La verificación del cumplimiento con el Principio de Responsabilidad Demostrada será tenida en cuenta a la hora de evaluar la imposición de sanciones por la infracción al régimen de protección de datos personales.

De la lectura de las normas se puede extraer, que el Principio de Responsabilidad Demostrada tiene dos facetas para los Responsables del Tratamiento de Datos Personales: la primera es un mandato adicional o complementario en materia de sus obligaciones para el Tratamiento, que les precisa la implementación y la capacidad de demostración de *"medidas apropiadas y efectivas"*; la segunda es que la demostración del cumplimiento de los estándares del Principio de Responsabilidad Demostrada será tenida en cuenta al momento de evaluar la imposición de sanciones por el incumplimiento de las obligaciones en materia de Tratamiento. Así, el Principio de Responsabilidad Demostrada implica entonces que los Responsables deben estar en capacidad de demostrar ante la SIC que han adoptado medidas apropiadas y efectivas para dar cumplimiento a la normativa, por lo cual no bastará con comprobar la elaboración de políticas en papel o limitarse a dar cumplimiento a las obligaciones iniciales establecidas en la Ley 1581.

Así, el Principio de Responsabilidad Demostrada ha cobrado gran relevancia en la protección de datos por cuanto

"su real y debida implementación no sólo redundará en beneficio de la protección de los derechos de titulares de los datos personales sino que beneficiará muy positivamente a las organizaciones porque les permitirá maximizar el uso inteligente de la información, aumentar su nivel de competitividad y consolidar su buena reputación empresarial o institucional." (Remolina, N. & Alvarez, M.F. 2018. p. 7). A su vez, el reto de las organizaciones, en materia de Responsabilidad Demostrada es "*probar que lo que están haciendo funciona bien y se ajusta a la ley."* (Remolina, N. 2013. p. 287).

De esta manera, la Responsabilidad Demostrada implica garantizar la aplicación efectiva y práctica de lo ordenado en las normas de protección de datos, y si bien es necesario expedir reglamentaciones que regulen el tema en las organizaciones, esto no es suficiente pues los esfuerzos deben concentrarse en que los objetivos de dichas regulaciones sean reales, concretos y

no simplemente formales. Es en esta materialización de los objetivos que cobra especial importancia la Responsabilidad Demostrada pues esta *"exige que los Responsables y encargados del tratamiento implanten medidas apropiadas, efectivas y verificables que le permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales."* (Remolina, N. & Tenorio, M.M. & Quintero G.A. 2018. p. 186.)

Ahora, si bien existe un mandato positivo de implementar el Principio de Responsabilidad Demostrada en el Tratamiento de Datos Personales, no hay una norma que establezca cuáles son las obligaciones, requisitos o criterios específicos que deben cumplir los Responsables del Tratamiento para demostrar el cumplimiento de este Principio ante la SIC lo cual resulta problemático pues para los destinatarios de la norma no resulta claro cuáles son las obligaciones que se les imponen. Dado lo anterior el presente trabajo pretende identificar cuál es el alcance que se le ha dado al Principio de Responsabilidad Demostrada para los Responsables del Tratamiento de Datos Personales en las decisiones administrativas de la SIC pues como se verá más adelante esta ha sido una de las bases estudiadas y bajo las cuales la SIC ha fundamentado sus decisiones en las investigaciones a los Responsables relacionadas con sus obligaciones en materia de protección de datos personales. Este tema es relevante para el derecho empresarial en Colombia por cuanto todas las empresas que realicen el Tratamiento de Datos Personales, que son prácticamente todas, están obligadas a dar cumplimiento a las normas en materia de protección de datos y al Principio de Responsabilidad Demostrada.

En desarrollo de lo anterior, el tema será abordado a través de cuatro objetivos específicos. Se partirá del análisis la definición del rol del Responsable en materia de datos personales conforme a la normatividad colombiana, sus deberes, obligaciones y los principios cuyo respeto debe garantizar en el Tratamiento; así mismo, se estudiará el contenido del Principio de Responsabilidad Demostrada según ha sido abordado en las normas colombianas sobre protección de datos, la doctrina nacional y los referentes internacionales. Posteriormente se realizará el análisis de las decisiones administrativas de la Superintendencia de Industria y Comercio en el periodo 2014- 2019 para identificar cómo ha abordado la autoridad la aplicación del principio de Responsabilidad Demostrada en la operación de los Responsables del Tratamiento de Datos Personales e identificar las pautas que ha dado sobre la adopción de medidas que resulten adecuadas y suficientes bajo el principio de Responsabilidad Demostrada. Finalmente se presentaran las conclusiones del trabajo.

Capítulo I – El Responsable en el Régimen de Protección de Datos Personales y el Principio de Responsabilidad Demostrada

1. El Responsable del Tratamiento de Datos Personales

El Responsable del Tratamiento de Datos Personales es la *"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"* (Ley 1581, 2012, art. 3, Lit. e), al respecto la Sentencia C-748 explica esa capacidad de decisión que caracteriza al Responsable como *"la posibilidad de definir –jurídica y materialmente- los fines y medios del tratamiento"* (Corte Constitucional, C-748, 2011). En desarrollo de lo anterior, tiene un rol preponderante en el régimen de protección de datos por cuanto es el principal llamado a dar cumplimiento a los principios que se erigen en la norma para el Tratamiento, es el destinatario principal de las obligaciones contenidas en la norma y es quien debe garantizar el pleno ejercicio de los derechos de los Titulares y los Principios para el Tratamiento. Precisó la Corte Constitucional que los Responsables son los principales llamados a garantizar el derecho fundamental al *habeas data* y las condiciones de seguridad para impedir cualquier tratamiento ilícito de los datos (Corte Constitucional, C-748, 2011).

1.1. Los deberes del Responsable.

La Ley 1581 le asigna unos deberes especiales al Responsable frente al Titular consistentes en:

(i) garantizar el pleno y efectivo ejercicio del *habeas data*;

(ii) solicitar y conservar copia de la autorización otorgada y actuar conforme a los límites de dicha autorización;

(iii) informar debidamente sobre la finalidad de la recolección y los derechos que le asisten; tramitar sus consultas, reclamos y solicitudes de información;

(iv) conservar la información bajo condiciones de seguridad;

(v) garantizar la calidad de la información que se suministre al Encargado, mantenerla actualizada, rectificarla cuando sea el caso, exigir la seguridad y privacidad;

(vi) adoptar un manual interno de políticas y procedimientos para garantizar el cumplimiento de la ley y en especial, para la atención de consultas y reclamos;

(vii) informar a la SIC de violaciones a la seguridad y riesgos en la administración de la información; y cumplir las instrucciones y requerimientos de la SIC (Ley 1581, 2012, art. 17).

Los anteriores deberes tienen como finalidad garantizar dos puntos básicos, el primero es el ejercicio pleno del derecho al *habeas data* por parte de los Titulares y el segundo son los principios para el Tratamiento, los cuales se estudiarán más adelante. A este respecto la Corte Constitucional expresó que el Responsable tiene:

"Responsabilidades claras, concretas y precisas frente al titular del dato, por cuanto ambos sujetos, en los términos de los preceptos en análisis, están obligados a garantizar el ejercicio pleno y efectivo del derecho al habeas data, el cual se irradia por todos los principios que rigen el tratamiento de datos" (Corte Constitucional, C-748, 2011).

Así, teniendo en cuenta que el rol del Responsable en cuanto a la delimitación de sus deberes en materia del Tratamiento y el Principio de Responsabilidad Demostrada está directamente relacionado con el cumplimiento de sus deberes conforme al Artículo 17 y los principios para el Tratamiento ("los Principios"), es necesario abordar su estudio.

1.2. Los Principios para el Tratamiento de Datos Personales

El Artículo 4 de la Ley 1581 contiene un aspecto medular de la regulación de Protección de Datos Personales en Colombia pues establece los Principios para el Tratamiento, así mismo en la sentencia C-748 de 2011 la Corte introdujo una serie de principios adicionales. Los Principios son un aspecto medular de la regulación de *habeas data* pues su observancia se erige como una de las principales obligaciones que deben cumplirse en el Tratamiento de Datos Personales y los deberes específicos establecidos en el Artículo 17 son una concreción de ellos. En palabras de Remolina (2018, pág. 52) *"El desconocimiento de dichos principios implica, además de una infracción de la ley, una vulneración del debido proceso en el tratamiento de los datos."*

Los Principios tienen entonces varias funciones dentro de la Ley, permiten garantizar el respeto a los derechos de los Titulares, imponen los límites al Tratamiento en el sentido de establecer que esta deberá realizarse en total cumplimiento de ellos y funcionan como una

herramienta interpretativa para la aplicación correcta de la normativa de datos personales (Remolina, N., Tenorio, M.M. & Quintero, G.A. 2018. pág. 53.). En este sentido, los Principios son un elemento muy importante a la hora de analizar el rol del Responsable y las obligaciones a las cuales este está sujeto, pues el Tratamiento de los Datos Personales deberá realizarse en cumplimiento de todos y cada uno de estos Principios, convirtiéndose entonces en verdaderas obligaciones positivas que deben cumplirse.

Los principios establecidos en la Ley 1581 de 2012 son:

(i) Legalidad: El Tratamiento debe darse en estricto cumplimiento de lo establecido en la Ley 1581 y las demás disposiciones que la desarrollen (Ley 1581, 2012, art. 4, Lit. a). Este principio encierra entonces el principal objetivo de la norma que es someter el Tratamiento a las normas y sus disposiciones (Corte Constitucional, C-748, 2011);

(ii) Finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular (Ley 1581, 2012, art. 4, Lit. b). Lo anterior significa que el Tratamiento debe realizarse con un propósito legítimo, específico y explícito, que fue previamente informado al Titular y autorizado por este. Así mismo, los Datos solamente deben ser tratados de la manera que el Titular pudo haber previsto cuando otorgó su autorización. Adicionalmente, el principio de finalidad impone un límite temporal al Tratamiento pues este solamente podrá realizarse por el periodo de tiempo necesario para alcanzar la necesidad con que se obtuvo el dato y a su vez impone un límite material, pues exige que solamente se recauden Datos Personales que sean estrictamente necesarios para el cumplimiento de las finalidades autorizadas (Corte Constitucional, C-748, 2011);

(iii) Libertad: El Tratamiento solamente puede llevarse a cabo después de obtener el consentimiento previo, expreso e informado del Titular. Para la obtención o divulgación de datos personales debe existir una autorización previa del Titular o un mandato legal o judicial que releve el consentimiento (Ley 1581, 2012, art. 4, Lit. c). El consentimiento expresado en la autorización es la instrucción específica e informada que el Titular libremente otorga para el Tratamiento y en este sentido, se convierte en un límite material y temporal del Tratamiento para los Responsables.

(iv) Veracidad o Calidad: Los datos sujetos a Tratamiento deben ser veraces, completos, exactos, comprobables y comprensibles. El Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error (integridad del dato personal) está prohibido (Ley 1581, 2012, art. 4, Lit. d).

(v) Transparencia: Impone el deber de garantizar el derecho de los Titulares a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan (Ley 1581, 2012, art. 4, Lit. e). Al desarrollar este principio, la Corte estableció que cuando de la inclusión en una base de datos se derive una situación provechosa para el Titular, el Responsable no podrá negarse injustificadamente a su inclusión. Así mismo, dio alcance a la información mínima que debe estar disponible en todo momento para los Titulares: *"**(i)** información sobre la identidad del controlador de datos, **(ii)** el propósito del procesamiento de los datos personales, **(iii)** a quién se podrán revelar los datos, **(iv)** cómo la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y **(v)** toda otra información necesaria para el justo procesamiento de los datos."* (Corte Constitucional, C-748, 2011).

(vi) Acceso y Circulación Restringida: El Tratamiento estará limitado por la naturaleza de los datos personales, las disposiciones legales y la Constitución. Así, el Tratamiento solamente podrá hacerse por quienes estén autorizados por el Titular y/o por las personas previstas en la ley (Ley 1581, 2012, art. 4, Lit. f).

(vii) Seguridad: Los Datos Personales deberán manejarse con las medidas técnicas, humanas y administrativas que sean necesarias para dar seguridad, evitando su adulteración, pérdida, y consulta, uso o acceso no autorizado o fraudulento (Ley 1581, 2012, art. 4, Lit. g).

(viii) Confidencialidad: Los intervinientes en el Tratamiento de Datos Personales que no tengan naturaleza pública deben garantizar la reserva de la información, su suministro o comunicación solamente podrá realizarse cuando corresponda al desarrollo de las actividades autorizadas en la Ley (Ley 1581, 2012, art. 4, Lit. h).

Los principios introducidos en el régimen de Protección de Datos Personales por la Sentencia C-748 de 2011 por la Corte Constitucional[1] son:

(ix) Prohibición de discriminación: Se prohíbe la discriminación con base en las informaciones recaudadas en las bases de datos.

(x) Interpretación integral de los derechos constitucionales: De conformidad con la Corte

[1] En la Sentencia de Constitucionalidad, la Corte incluyó esta serie de principios que, en sus palabras, *"se entienden incluidos"* en la Ley 1581 de 2012 por estar derivados directamente de la Constitución Política de 1991 o por derivarse directamente del núcleo temático de dicha ley.

"la administración de datos personales deberán, en todo caso, subordinarse a la eficacia de los derechos fundamentales del individuo." Corte Constitucional, C-748, 2011).

(xi) Obligación de indemnizar perjuicios: Los perjuicios causados por fallas en el Tratamiento deberán ser indemnizados.

(xii) Proporcionalidad del establecimiento de excepciones: Si bien existen materias que se consideran exceptuadas del régimen establecido en la Ley 1581 de 2012 de conformidad con su ámbito de aplicación, ese tratamiento especial deberá "*estar justificado en términos de proporcionalidad y responder a los estándares internacionales de protección*" (Corte Constitucional, C-748, 2011).

(xiii) Autoridad independiente: La autoridad que dentro de la estructura del Estado está encargada de garantizar el respeto de los principios anteriormente desarrollados debe garantizar imparcialidad e independencia.

(xiv) Exigencia de estándares de protección equivalentes para la transferencia internacional de datos: Existe una prohibición de transferencia internacional a países que no proporcionen niveles adecuados de protección de datos.

2. El Principio de Responsabilidad Demostrada

2.1. Normatividad colombiana

El Principio de Responsabilidad Demostrada no se incluyó dentro de la Ley 1581 de 2012, ni fue mencionado en la sentencia de constitucionalidad C-748 de 2011, sino que fue introducido en la normatividad de Protección de Datos colombiana por medio del Decreto Reglamentario 1377 de 2013, que posteriormente fue compilado en el Decreto 1074 de 2015. No obstante, este Principio guarda total armonía con la Ley 1581 de 2012 y con el desarrollo que de ella realizó la Corte Constitucional pues, como se verá, hace énfasis en la realización efectiva de los Principios que informan el sistema de Protección de Datos Personales, el cumplimiento real de los deberes de los Responsables y la garantía de los derechos de los Titulares para que estos no se queden simplemente en la norma, sino que sean efectivamente llevados a la práctica. Esto último guarda total armonía con el alcance que la Sentencia C-748 les dio a los demás principios, aquellos incluidos en el Art. 4 de la Ley 1581, en el sentido de exponer cómo estos son verdaderas obligaciones para los Responsables en el Tratamiento de Datos Personales.

El Artículo 2.2.2.25.6.1. del Decreto 1074 de 2015, al instituir el Principio de Responsabilidad Demostrada, establece que este implica para los Responsables dos obligaciones principales:

a) la obligación de estar en capacidad de demostrar, a petición de la SIC, que ha *"implementado medidas apropiadas y efectivas"* para cumplir con sus obligaciones, de manera proporcional a los siguientes criterios establecidos en la norma:
    - La naturaleza jurídica del Responsable y su tamaño empresarial, de acuerdo con la normativa vigente.
    - La naturaleza de los datos personales objeto del Tratamiento.
    - El tipo de Tratamiento.
    - Los riesgos potenciales que referido Tratamiento podría causar sobre los derechos de los titulares.
b) la obligación de que, ante un requerimiento de la SIC, puedan suministrar evidencia de la implementación efectiva de *"medidas de seguridad apropiadas"*.

Por su parte, el Artículo 2.2.2.25.6.2 del mismo Decreto indica que, respecto de dichas medidas apropiadas y efectivas, debe garantizar que:

a) Son consistentes con las instrucciones que la SIC imparta;
b) Existe una estructura proporcional al interior del Responsable para su adopción e implementación;
c) Ha adoptado mecanismos internos para ponerlas en práctica, incluyendo herramientas de implementación, entrenamiento y educación; y
d) Ha adoptado procesos para la atención de peticiones, consultas y reclamos de los Titulares.

De igual manera establece que la verificación del cumplimiento del Principio de Responsabilidad Demostrada será tenida en cuenta a la hora de evaluar la imposición de sanciones por la infracción al régimen de protección de datos personales.

2.2. Referentes Internacionales

Con el fin de ilustrar la importancia del Principio de Responsabilidad Demostrada, a continuación, se presentarán algunos referentes internacionales que muestran cómo este principio es considerado un elemento fundamental para la garantía efectiva de los derechos protegidos y los fines perseguidos por los regímenes generales de protección de datos personales. Así mismo, estos referentes internacionales son de gran utilidad para estudiar cuál es el contenido y qué criterios específicos deben alcanzar los Responsables para dar cumplimiento a este Principio.

2.2.1. Organización para la Cooperación y el Desarrollo Económico -OCDE-

La OCDE cuenta con las *Guías sobre Protección de la Privacidad y los Flujos Transfronterizos de Información* de la Organización para la Cooperación y el Desarrollo Económicos -OCDE- que fueron adoptadas como una recomendación del Consejo de la OCDE a sus países miembros, en aras de propender por los tres principios base de la organización: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas (Organisation for Economic Cooperation and Development [OECD]. 2013). Estas Guías traen como uno de sus elementos la Responsabilidad Demostrada (*accountability* en Inglés), que consiste en un principio en materia de protección de datos personales según el cual el Responsable del Tratamiento de Datos Personales debe considerarse responsable de cumplir con medidas que materialicen los demás principios del régimen de Protección de Datos Personales (Organisation for Economic Cooperation and Development [OECD]. 2013).

Al respecto, para la implementación de la Responsabilidad Demostrada las Guías de la OCDE establecen que el Responsable:

a) Deberá implementar un sistema de administración que:
   - Materialice las guías para todos los Datos Personales bajo su control;
   - Esté diseñado a la medida de la estructura, escala, volumen y sensibilidad de sus operaciones;
   - Provea salvaguardas apropiadas basadas en evaluaciones de riesgo de privacidad;
   - Esté integrado a su estructura de gobernanza y establezca mecanismos de supervisión internos;
   - Incluya planes para responder a consultas e incidentes;
   - Sea actualizado a la luz de monitoreos constantes y evaluaciones periódicas.

b) Deberá estar preparado para demostrar que su sistema de administración es apropiado, en particular ante un requerimiento en este sentido de la autoridad de protección de datos personales.
c) Informar a la autoridad de protección de datos personales cuando haya habido una brecha de seguridad significativa que afecte los Datos Personales. Cuando la brecha posiblemente afecte a los Titulares, el Responsable deberá notificar a los Titulares afectados.

(Organization for Economic Cooperation and Development [OECD]. 2013).

2.2.2. Reglamento General de Protección de Datos Personales -RGDP- de la Unión Europea

En 2016 se expidió el Reglamento 2016/679 o Reglamento General de Protección de Datos Personales (en adelante le "RGDP") en la Unión Europea, regulación que al estar contenida en un reglamento es de aplicación directa en todos los países miembros de la unión y no requiere medidas adicionales de implementación dentro de cada país (Voigt, P. & Bussche, A., 2017. pág. 2). Una de las novedades que el Reglamento implementó con respecto a la normatividad anterior de protección de datos personales en la unión europea, fue precisamente el énfasis explícito en el Principio de Responsabilidad Demostrada, llamado responsabilidad proactiva (*accountability*), así, en el Numeral 2 de su Artículo 5 el RGDP establece que: *"El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)."* (Reglamento 679, 2016, Artículo 5). Así, este principio se compone de dos elementos, primero el deber del Responsable de garantizar el cumplimiento con el RGDP y segundo, la habilidad del Responsable de probar dicho cumplimiento a las autoridades supervisoras. La Responsabilidad Demostrada es un verdadero mandato y su cumplimiento es exigible por derecho propio y en ese sentido, es exigible de manera directa, teniendo las autoridades de protección de datos la facultad de imponer multas por su incumplimiento conforme al Artículo 83 del RGDP.

De esta manera, el Principio de Responsabilidad Demostrada en el RGDP persigue el objetivo de fortalecer el entendimiento y el compromiso del Responsable en la práctica para implementar medidas organizacionales apropiadas para garantizar el cumplimiento de la norma de protección de datos, en especial sus principios y el respeto a los derechos de los titulares. En palabras de Voigt y Bussche: *"Medidas apropiadas incluyen la adopción de políticas internas, el*

uso de programas escalables para implementar los principios de protección de datos."[2] (Voigt, P. & Bussche, A., 2017. pág. 32). Adicionalmente, se reconoce también en el RGDP la importancia que tiene la relación entre el cumplimiento del Principio de Responsabilidad Demostrada con la materialización efectiva de los demás principios de Tratamiento, lo anterior pues bajo la Responsabilidad Demostrada los Responsables deben estar en capacidad de probar el cumplimiento del RGDP y la única forma de hacerlo es probar el cumplimiento de los demás principios bajo los cuales debe llevarse a cabo el Tratamiento conforme al RGDP.

> *"Bajo requerimiento de la autoridad supervisora, los responsables deben estar en capacidad de probar su cumplimiento con el RGDP bajo el principio de responsabilidad proactiva. Esta obligación se refiere explícitamente a los principios básicos para el tratamiento bajo el Art. 5 Sec. 1 RGDP, tales como la legalidad y transparencia del tratamiento o el principio de minimización de los datos. Sin embargo, en tanto estos principios están concretados en las diferentes obligaciones materiales y organizacionales bajo el RGDP, las entidades deben ser capaces de demostrar su cumplimiento con todos ellos."*[3] (Voigt, P. & Bussche, A., 2017. pág. 32).

2.3. Doctrina Nacional

2.3.1. Superintendencia de Industria y Comercio -SIC-

Es importante tener en cuenta, que en el año 2015 la SIC, en lo que ha sido considerado por la misma entidad como un esfuerzo por dar claridad a los Responsables del Tratamiento sobre cómo materializar el Principio de Responsabilidad Demostrada en sus operaciones, publicó en el año 2015 su *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability) (*"en adelante la "Guía Accountability"). Al respecto, esta establece que en la

[2] Texto en Inglés *"Suitable measures include the adoption of internal policies, the use of scalable programs to implement data protection principles."* (Voigt, P. & Bussche, A. 2017. p. 32).
[3] Texto en inglés *"Upon request of Supervisory Authorities, controllers must be able to prove their compliance with the GDPR under the accountability principle. This obligation explicitly refers to the basic principles for processing under Art. 5 Sec. 1 GDPR, such as the lawfulness and transparency of processing or the principle of data minimization (see Sect. 4.1 for details). However, as these principles are specified by the different material and organizational obligations under the GDPR, entities must be able to demonstrate compliance with all of them."* (Voigt, P. & Bussche, A. 2017. p. 32).

inclusión de este principio en la normatividad colombiana y la manera en que la SIC ha diseñado su sistema de supervisión se *"privilegia la gestión del riesgo y la asignación de Responsabilidades en cabeza del Responsable del Tratamiento"* (Superintendencia de Industria y Comercio. 2015). Al referirse a la faceta atenuante del Principio, se indica que este es un desarrollo novedoso y que significa que la autoridad debe realizar un reconocimiento expreso de aquellas organizaciones que, ante una falla en el Tratamiento, puedan demostrar que se trata de una situación aislada dentro de un Programa Integral de Gestión de Datos Personales (uno de los elementos de la Responsabilidad Demostrada según la SIC el cual se abordará más adelante).

Así, la SIC indica que el punto de partida fundamental para el cumplimiento de la exigencia de adoptar políticas internas efectivas en materia de protección de datos es el desarrollo de un Programa Integral de Gestión de Datos Personales (en adelante **Programa Integral de Gestión**) y como punto fundamental, la capacidad de probar no solamente el diseño de este programa sino su efectiva implementación. Para el efecto, este Programa Integral de Gestión debe tener como partida un proceso de debida diligencia al interior de la organización del Responsable e incorporar políticas que respondan a los *"ciclos internos de gestión de datos de la organización y generen resultados medibles que le permitan probar ese grado de diligencia especial"* (Superintendencia de Industria y Comercio. 2015. p. 8). Los elementos esenciales del Programa Integral de Gestión son:

a. Compromiso de la Organización: se requiere de una cultura de respeto a la protección de datos y el compromiso desde la alta dirección. Así mismo, es fundamental la asignación de recursos económicos y humanos para la implementación, incluyendo la designación de un oficial de protección de datos que asuma la función de protección de datos y de trámite a las solicitudes de los Titulares. Adicionalmente, deben implementarse mecanismos de reporte internos para hacer seguimiento a la ejecución del Programa.
b. Controles del Programa Integral de Gestión: el segundo paso, luego de haber adelantado la debida diligencia, es la implementación de controles que permitan al Oficial de Protección de Datos o al área encargada desarrollar el Programa Integral de Gestión que asegure que las políticas se implementen al interior de la organización. Lo anterior implica asegurarse de que los procedimientos internos operacionales sean consistentes con las políticas de tratamiento de datos personales, mantener un inventario actualizado de las bases de datos que

contienen Datos Personales y los procesos en los cuales se recolectan dichos datos. Adicionalmente, será necesario que se generen y documenten políticas internas que implementen los Principios que rigen el Tratamiento de Datos Personales y que reglamenten los procedimientos que impliquen operaciones de Tratamiento de Datos Personales, las cuales deben ser divulgadas en la organización.

Por otra parte, debe desarrollarse un sistema de administración de riesgos asociados al Tratamiento de Datos Personales que permita *"identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en el desarrollo del cumplimiento de las normas de protección de datos personales."* (Superintendencia de Industria y Comercio. 2015 p. 16). Este sistema debe contar con las etapas de identificación, medición, control y monitoreo de los riesgos asociados.

De igual manera, será necesario contar con programas de formación en la materia, protocolos de respuesta ante violaciones e incidentes de seguridad, gestión de los encargados del Tratamiento, así como de las transferencias y transmisiones internacionales de Datos Personales y procedimientos de comunicación externa a los Titulares.

Por último, la SIC indica que los Responsables deben garantizar dentro del Programa Integral de Gestión, la evaluación y revisión continua del mismo mediante el desarrollo de un plan de supervisión y revisión.

Si bien la Guía Accountability no es una norma vinculante, ni de obligatorio cumplimiento, la SIC ha indicado que esta constituye un criterio orientador que podrá ser tenido en cuenta para dar cumplimiento a la normatividad de datos personales y así, los parámetros contenidos en ella son mencionados en las decisiones administrativas de la SIC cuando se está evaluando el cumplimiento del Principio de Responsabilidad Demostrada. Sobre la naturaleza jurídica de este documento la SIC ha dicho *"Es esta, quizá, una manifestación de la tendencia del derecho público*

a acercarse al concepto de 'soft law', normas cuasi legales que no son coercitivas a pesar de que pueden estar construidas como reglas, pero que, en todo caso, buscan influir en la conducta de sus destinatarios." (Superintendencia de Industria y Comercio. Resolución 39298 de 2016).

De acuerdo con lo expuesto, el Responsable del Tratamiento de Datos es entonces aquella persona (natural o jurídica) que decide sobre los Datos Personales y el Tratamiento que se les dará. Como tal tiene entonces un rol de vital importancia para la Protección de Datos puesto que es el destinatario principal de los mandatos contenidos en las normas (deberes y principios para el Tratamiento) y es quien está llamado a respetar los derechos de los Titulares. Por su parte, el Principio de Responsabilidad Demostrada fue introducido en las normas de Protección de Datos Personales en un esfuerzo por garantizar que los principios para el Tratamiento, los deberes de los Responsables y Encargados, pero sobre todo los derechos de los Titulares no se quedarían en el papel, sino que serían llevados a la práctica. Lo anterior, mediante la creación de procedimientos al interior de cada organización que respondan a sus características propias y las de sus actividades de Tratamiento y su materialización con la efectiva implementación.

Capítulo II – El Desarrollo del Principio de Responsabilidad Demostrada en las Decisiones Administrativas de la SIC en los años 2014-2019

1. Alcance del capítulo y caracterización de las decisiones administrativas objeto de revisión

En el presente capítulo se reseñarán y analizarán las decisiones administrativas de la Superintendencia de Industria y Comercio en el periodo 2014 - 2019 para identificar cómo ha abordado la autoridad la aplicación del principio de Responsabilidad Demostrada en la operación de los Responsables del Tratamiento de Datos Personales y qué pautas ha dado sobre la adopción de medidas que resulten adecuadas y suficientes bajo el principio de Responsabilidad Demostrada.

Es importante comenzar precisando que las decisiones administrativas de la SIC en materia de Protección de Datos Personales se emiten en razón a las facultades que le otorgan el Artículo 19 de la Ley 1581 de 2012, que la designa como autoridad de protección de datos para ejercer la vigilancia del cumplimiento normativo en la materia y el Artículo 21 que, entre otras, le asigna la función de adelantar las investigaciones y ordenar las medidas que sean necesarias para hacer efectivo de derecho de *habeas data* (Ley 1581, 2012, arts. 19 y 21). Al tratarse de resoluciones sancionatorias administrativas los efectos de las mismas, en principio, se limitan al investigado. No obstante, el estudio de las decisiones de Protección de Datos Personales de la SIC es importante en tanto la entidad es la autoridad en la materia y sus decisiones constituyen precedente administrativo, el cual se encuentra consagrado en el artículo 10 de la Ley 1437 de 2011, Código de Procedimiento Administrativo y Contencioso Administrativo, que establece que las autoridades administrativas al momento de resolver asuntos de su competencia deberán aplicar la Constitución, la ley y las disposiciones reglamentarias *"de manera uniforme a situaciones que tengan los mismos supuestos fácticos y jurídicos"* (Ley 1437, 2011, art. 10). Así, esta norma se ha entendido como la obligación que tienen las autoridades administrativas de dar una aplicación uniforme a las normas cuando las situaciones tengan los mismo presupuestos facticos y jurídicos (Corte Constitucional, C-634, 2011) (Moreno, L. 2016.) (Quecán, R., 2020.).

Para efectos de abordar los objetivos de este Capítulo, se realizó la revisión preliminar de la totalidad de las decisiones administrativas, un total de noventa y nueve (99), de primera instancia en materia de protección de datos personales disponibles en la página web de la SIC[4] y se realizó una selección de todas aquellas que abordan el estudio del Principio de Responsabilidad Demostrada, en total veintitrés (23) las cuales se enuncian y caracterizan de manera general en la Tabla 1 siguiente. Se utilizó esta metodología para la búsqueda y selección de las decisiones objeto de estudio dado el carácter en general amplio de la pregunta de investigación y por cuanto el número de resoluciones disponibles no se consideró demasiado voluminoso. Luego, se estudió a profundidad y se realizó el análisis de cada una de esas veintitrés (23) resoluciones identificadas como de interés para el presente trabajo, proceso mediante el cual se encontró que existen distintos frentes desde los cuales la SIC ha abordado el estudio y la aplicación del Principio de Responsabilidad Demostrada en sus resoluciones, los cuales se pueden esquematizar de la manera indicada en la Tabla 2 al final de este capítulo.

[4] A la fecha no se encuentran disponibles decisiones administrativas correspondientes al año 2020.

TABLA 1

Identificación y caracterización de las Resoluciones de la SIC en las cuales el Principio de Responsabilidad Demostrada es estudiado y aplicado

Resolución No.	Entidad Investigada	Sector Económico de la Entidad Investigada	Origen de la Investigación	Fecha de Apertura de la Investigación	Fecha de la Resolución
36863 de 2014	Almacenes Éxito S.A.	Comercio al por menor y al por mayor	Queja	12 de febrero de 2014	30 de mayo de 2014
39298 de 2016	Colmédica Medicina Prepagada S.A.	Salud	Queja	11 de noviembre de 2015	21 de junio de 2016
78899 de 2017	Inversiones CMR S.A.S.	Plataforma tecnológica de domicilios	Queja	31 de marzo de 2016	30 de noviembre de 2017
27708 de 2017	Centro Comercial Oviedo PH	Centro comercial	De oficio	30 de septiembre de 2015	22 de mayo de 2017
	Ripley Compañía de Financiamiento S.A.[5]	Entidad Financiera			
83882 de 2018	Linio Colombia S.A.S.	Comercio al por menor realizado a través de internet	Queja	25 de enero de 2016	15 de noviembre de 2018[6]
64902 de 2018	Instituto de Diagnóstico Médico S.A.	Salud	Queja	23 de abril de 2018	4 de septiembre de 2018
63316 de 2018	Corporación Universidad De La Costa	Educación	De oficio	26 de marzo de 2018	30 de agosto de 2018
61062 de 2018	Colmédica Medicina Prepagada S.A.	Salud	Queja	11 de noviembre de 2015	24 de agosto de 2018
51290 de 2018	Universidad de San Buenaventura	Educación	De oficio	29 de septiembre de 2017	23 de julio de 2018
48813 de 2018	Provincia Nuestra Señora De La Gracia De Colombia - Liceo Cervantes El Retiro	Educación	De oficio	28 de noviembre de 2017	12 de julio de 2018

[5] Ripley Colombia S.A.S. no fue sancionada.

[6] La Resolución 83882 de 2018 resuelve el recurso de apelación interpuesto por la investigada en contra de la Resolución 28373 emitida el 26 de abril de 2018, mediante la cual se le impuso sanción. En la Resolución 28373 el Principio de Responsabilidad Demostrada no se menciona en el análisis hecho por la SIC.

Resolución No.	Entidad Investigada	Sector Económico de la Entidad Investigada	Origen de la Investigación	Fecha de Apertura de la Investigación	Fecha de la Resolución
44026 de 2018	Almacenes Éxito S.A.	Comercio al por menor y al por mayor	Queja	30 de noviembre de 2017	25 de junio de 2018
45743 de 2018	Starmedia Group S.A.S.	Comunicaciones	Queja	31 de octubre de 2017	29 de junio de 2018
30906 de 2018	Mall Express S.A.S.	Call center	Queja	31 de mayo de 2017	07 de mayo de 2018
10414 de 2018	Internacional de Vehículos S.A.	Comercio de vehículos	Queja	25 de enero de 2016	16 de febrero de 2018
1321 de 2019	Facebook Colombia S.A.S.	Red social	De oficio	N/A[7]	24 de enero de 2019
4082 de 2019	Bancolombia S.A.	Entidad Financiera	Queja	30 de abril de 2018	21 de febrero de 2019
4086 de 2019	Bancolombia S.A.	Entidad Financiera	Queja	11 de septiembre de 2018	21 de febrero de 2019
	BRM S.A.	Call center			
9766 de 2019	Banco Falabella S.A.	Entidad Financiera	Queja	11 de septiembre de 2018	25 de abril de 2019
9800 de 2019	Rappi S.A.S.	Plataforma tecnológica de domicilios	Queja	26 de marzo de 2018	25 de abril de 2019
6074 de 2019	Contacto Solutions Ltda.	Call y contact center	Queja	1 de noviembre de 2018	18 de marzo de 2019
5477 de 2019	Socialatom Colombia S.A.S.	Consultoría	De oficio	8 de agosto de 2018	7 de marzo de 2019
5848 de 2019	Centro Educativo Superior Interamericano S.A.S.	Educación	Queja	17 de septiembre de 2018	14 de marzo de 2019
21478 de 2019	Uber Technologies, Inc.	Plataforma tecnológica de transporte	De oficio	N/A[8]	17 de junio de 2019
	Uber Colombia S.A.S.				
	Uber B.V.				

De lo anterior se evidencia que las entidades investigadas se dedican a diversas actividades y están involucradas en diversos sectores así: cinco (5) se dedican a actividades de comercio, cuatro (4) son entidades financieras, cuatro (4) están en el sector de educación, tres (3) en el de salud, tres (3) son plataformas tecnológicas, tres (3) desarrollan actividades de call center, dos (2) son redes

[7] La Resolución 1321 de 2019 no cuenta con un antecedente de apertura de investigación por cuanto no fue el resultado de una investigación administrativa sancionatoria, sino una decisión de impartir ordenes preventivas tomada por la SIC dentro de sus facultades como autoridad en materia de protección de datos personales.
[8] La Resolución 21478 de 2019 no cuenta con un antecedente de apertura de investigación por cuanto no fue el resultado de una investigación administrativa sancionatoria, sino una decisión de impartir ordenes preventivas tomada por la SIC dentro de sus facultades como autoridad en materia de protección de datos personales.

sociales y una (1) presta servicios de consultoría. Así, no se observó que ningún sector de la economía predominara sobre los demás pero sí que se trata de actividades que por lo general implican contacto con el público o con un gran número de personas y por lo tanto, suelen tratar un gran volumen de datos personales. Adicionalmente, se observa que de veintitrés (23) resoluciones: dieciséis (16) tuvieron su origen en una queja, esto es el setenta por ciento (70%) y siete (7) fueron iniciadas de oficio por la SIC, esto es el treinta por ciento (30%) lo cual evidencia que los titulares de los datos personales están ejerciendo sus derechos. Por último, en aquellas resoluciones estudiadas que resolvieron una investigación administrativa en primera instancia, el procedimiento administrativo tuvo una duración de seis (6) meses o menos en el veinticinco por ciento (25%), de entre seis (6) y (12) meses en el cincuenta por ciento (50%) y mayor a doce (12) meses en el veinticinco por ciento (25%) restante.

2. Análisis del Principio de Responsabilidad Demostrada en las Resoluciones de la SIC

De las resoluciones estudiadas pudo observarse que la SIC abordó el estudio y la aplicación del Principio de Responsabilidad Demostrada de varias maneras, las cuales fueron esquematizadas en las seis (6) categorías que se exponen a continuación.

2.1. Como Una Obligación Autónoma

La primera decisión que aborda profundamente el estudio del Principio de Responsabilidad Demostrada como una obligación autónoma es la Resolución 83882 de 2018, que resuelve el recurso de reposición interpuesto contra la Resolución 28373 mediante la cual se sancionó a la investigada por el incumplimiento de varios de sus deberes emanados del Art. 17 de la Ley 1581 de 2012. De igual manera, en las Resoluciones 1321 de 2019 y 21478 de 2019, cuyas investigaciones se iniciaron por fallas a los deberes de seguridad del Responsable en organizaciones cuyo impacto en el Tratamiento son considerables dado el alto número de Datos Personales que tratan, la SIC realiza el estudio a profundidad del Principio de Responsabilidad Demostrada remitiéndose a los argumentos y consideraciones establecidos en la Resolución 83882. Así, la SIC sustenta la Responsabilidad Demostrada como un principio autónomo bajo el entendido de que, según la jurisprudencia de la Corte Constitucional, quienes administren datos personales tienen el deber constitucional de hacerlo correctamente y protegiendo los archivos y bases de datos. Bajo esta obligación, los Responsables deben poder probar que han tomado

medidas *"adecuadas, útiles y eficaces para cumplir la regulación"* lo cual significa que no basta con adoptar cualquier tipo de política o herramienta, sino que aquellas deben servir para que "*los postulados legales no sean meras elucubraciones teóricas sino realidades verificables"* (Superintendencia de Industria y Comercio. Resolución 83882 de 2017).

En el estudio de fondo del Principio de Responsabilidad Demostrada que la SIC hace en sus resoluciones, la SIC remite a la Guía Accountability, indicando que ella es un criterio orientador que podrá ser tenido en cuenta para dar cumplimiento a la normatividad de datos personales y al respecto precisa que esta se denomina también guía de 'accountability', término inglés que en el ámbito de protección de datos se refiere *"al modo como una organización debe cumplir en la práctica las regulaciones sobre el tema y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente"* (Superintendencia de Industria y Comercio. Resolución 83882 de 2017).

Las obligaciones emanadas del Principio de Responsabilidad Demostrada implican para la SIC (i) la implementación de acciones de distinta naturaleza para garantizar el correcto cumplimiento de las obligaciones en materia de Tratamiento de Datos Personales; (ii) la implementación de medidas apropiadas, efectivas y verificables que le permitan demostrar el cumplimiento de dichas obligaciones; y (iii) la revisión y evaluación permanente de la eficacia de las medidas tomadas y el grado de cumplimiento de las obligaciones (Superintendencia de Industria y Comercio. Resolución 83882 de 2017).

Así, el Principio de Responsabilidad Demostrada implica que las obligaciones en materia de Tratamiento de Datos Personales van más allá de la expedición de documentos y políticas porque implican la exigencia de la demostración del cumplimiento real y efectivo en la práctica de su operación. Con lo anterior se busca que los mandatos legales sean una realidad verificable, lo cual exige que los Responsables sean proactivos y que adopten medidas estratégicas con la capacidad de garantizar los derechos de los Titulares.

De igual manera, este Principio se articula con el concepto de cumplimiento o '*compliance*' con el cual las organizaciones deben garantizar que cumplen con las normas, generando evidencias de sus esfuerzos para alcanzar dicho cumplimiento y disponen sanciones para quienes a su interior no logran dicho cumplimiento; este tipo de sistemas implica la creación de funciones específicas y metodologías concretas para el cumplimiento. De esta manera, con base en el '*compliance'*, para la Responsabilidad Demostrada será de vital importancia la identificación, clasificación de riesgos y la adopción de medidas para mitigarlos.

Si bien la organización investigada aportó material probatorio que permitía constatar que contaba con políticas y procedimientos, así como con capacitaciones a sus funcionarios sobre protección de Datos Personales, en la Resolución 4086 de 2019 la SIC estimó que este esfuerzo probatorio resultaba insuficiente si la organización no probaba también que esos procedimientos fueron efectivamente implementados. En este caso, la evidencia de la implementación debió haberse constituido mediante la documentación que permitiera constatar que, en el caso concreto dichos procedimientos habían sido puestos en práctica a la fecha. Así, la SIC dejó claro que el Principio de Responsabilidad Demostrada se basa principalmente en la implementación real de las medidas tomadas por las organizaciones.

2.2. En relación con el Principio de Seguridad

Las resoluciones relacionadas con el principio de seguridad representan el 21,3% del total analizado. En las Resoluciones 39298 de 2016, 78899 de 2017 y 10414 de 2018 se estudia la infracción de las organizaciones investigadas como Responsables del Tratamiento a la obligación de informar a la autoridad cualquier violación de los códigos de seguridad (Ley 1581 de 2012. Art. 17. Lit. n), ante lo cual las organizaciones alegaron la vaguedad de las disposiciones normativas para argumentar que el hecho ocurrido no estaba constituido específicamente como una violación a un código de seguridad por la norma. En este contexto, la autoridad comienza con un análisis de dicha obligación en armonía con el Principio de Seguridad y con la obligación del Responsable de mantener la información en *"condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"* (Ley 1581 de 2012. Art. 17. Lit. d). Lo anterior por cuanto considera que los principios en materia de datos personales *"permean la interpretación"* de todo el régimen legal de protección de Datos Personales y que estos *"se encuentran plenamente armonizados con los derechos de los titulares del dato y los deberes de los sujetos obligados de la ley."* (SIC. Resolución 39298 de 2016).

Al respecto, la SIC establece que ni el principio de seguridad, ni las obligaciones legales en esta materia establecen específicamente cuáles son las medidas que deben adoptar los Responsables para cumplir sus obligaciones, pero que sí señalan que estas medidas deben ser las que resulten necesarias. Es en este contexto, bajo el Principio de Responsabilidad Demostrada les corresponde a los Responsables demostrar a la SIC que *"dispusieron de las medidas de seguridad apropiadas para la conservación de la información que es objeto de los tratamientos por ellos*

definidos, por lo que son estos quienes definirían tales controles" de acuerdo con los cuatro criterios de proporcionalidad definidos bajo el artículo 2.2.2.25.6.1.[9] En este sentido, si bien en las obligaciones del Principio de Seguridad no se establecieron específicamente las medidas que deben adoptarse por parte de los Responsables, bajo el Principio de Responsabilidad Demostrada no les está permitido a los Responsables alegar una supuesta vaguedad en las normas para abstraerse de sus obligaciones, pues este implica que no están obligados únicamente a cumplir con los mínimos de la ley sino a adoptar medidas apropiadas y efectivas, que por lo demás deben ser determinadas por ellos mismos.

De otra parte, en la Resolución 61062 de 2018 la SIC determinó que al no tener documentado un manual de políticas de seguridad de la información no solo se incumple el Principio de Seguridad sino también el Principio de Responsabilidad Demostrada pues no se *"evidencia la implementación de medidas y procedimientos de seguridad apropiados y proporcionales al tamaño de la sociedad, que garantizara una adecuada protección de los datos personales."* (Superintendencia de Industria y Comercio. Resolución 61062 de 2018).

En la Resolución 10414 de 2018, frente al estudio de una infracción al Principio de seguridad por el uso no autorizado de los Datos Personales por parte de un subalterno del Responsable, la SIC determina que es sobre los Responsables que recae la responsabilidad de los actos de las personas que tengan acceso a los Datos Personales, pues en virtud del Principio de Responsabilidad Demostrada están obligados a adoptar e implementar medidas apropiadas y efectivas que garanticen el cumplimiento de la Ley 1581 de 2012. (Superintendencia de Industria y Comercio. Resolución 10414 de 2018).

2.3. En Relación con el Deber legal de contar con un Manual Interno de Políticas y Procedimientos

[9] Decreto 1074 de 2015. Artículo 2.2.2.25.6.11. *"Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y capítulo, 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 una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. tipo de Tratamiento.
4. Los riesgos potenciales que referido tratamiento podrían causar sobre los derechos de los titulares".

Las resoluciones relacionadas con este tópico fueron las más frecuentes y representaron el 39,1% de los casos analizados. En las Resoluciones 64902 de 2018, 63316 de 2018, 51290 de 2018, 45743 de 2018, 30906 de 2018, 6074 de 2019, 5477 de 2019 y 5848 de 2019 cuando se estudia la infracción de las investigadas como Responsables del Tratamiento a su deber de adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial para la atención de consultas y reclamos (Ley 1581 de 2012. Art. 17. Lit. k)[10], la SIC relaciona de manera directa el incumplimiento de esta obligación con el incumplimiento al Principio de Responsabilidad Demostrada.

En las Resoluciones 63316 de 2018 y 51290 de 2018, en tanto durante el curso de la investigación no se evidenció que las investigadas contaran con este manual, la SIC concluye y enfatiza que al no constatar evidencia de la adopción de dicho manual, las organizaciones investigadas incumplieron no solo su deber derivado del literal k) del Artículo 17 sino también sus obligaciones bajo el Principio de Responsabilidad Demostrada, pues este establece que las medidas y procedimientos adoptados por los Responsables deben encontrarse documentados para efectos de demostrar la implementación de dicho Principio, sobre todo en lo atinente a la implementación de *"un mecanismo para la medición y control de riesgos que puedan presentarse frente al derecho de los titulares."* (Superintendencia de Industria y Comercio. Resolución 63316 de 2018). La SIC ha dejado entendido que el deber de contar con este manual tiene relación directa con la obligación que impone el Principio de Responsabilidad Demostrada en cuanto a la adopción de procedimientos internos y el desarrollo de políticas internas efectivas que demuestren el cumplimiento de sus obligaciones emanadas de la Ley 1581 de 2012 y el Decreto 1974 de 2015 (Superintendencia de Industria y Comercio. Resolución 51290 de 2018). En la misma línea, en la Resolución 5477 de 2019 la autoridad concluye que cuando el Responsable no cuenta con un manual de políticas y procedimientos en la materia, infringe directamente el Principio de Responsabilidad Demostrada (Superintendencia de Industria y Comercio. Resolución 5477 de 2019).

Por otro lado, puntualiza la SIC que el manual de políticas internas es el documento mediante el cual las organizaciones deben disponer de los procedimientos adecuados para la aplicación de

[10] Ley 1581 de 2012. "*ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:* (…) *k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;"*

las normativas de Datos Personales. Adicionalmente, que estos procedimientos deben ser puestos en conocimiento de los funcionarios que dentro de sus actividades estén destinados a aplicarlos y que los Titulares tengan acceso a los mismas para que conozcan plenamente las finalidades del Tratamiento, sus derechos y los medios para ejercerlos (Superintendencia de Industria y Comercio. Resolución 30906 de 2018).

2.4. Alcance e interpretación del concepto de *"medidas apropiadas y efectivas".*

Es necesario recordar que, según se abordó en el primer capítulo de este trabajo, el concepto de "*medidas apropiadas y efectivas"* tiene una importancia central en el Principio de Responsabilidad Demostrada, pues la obligación principal que de este principio se deriva es precisamente adoptar medidas que resulten apropiadas y efectivas para cumplir con las obligaciones en materia de protección de datos personales. Estas medidas no se encuentran definidas de manera precisa en la norma, sino que se establece que deben ser proporcionales a unos criterios generales establecidos ella. En este sentido, en tanto la norma no es precisa en establecer cuáles son las medidas que deben adoptarse en virtud del Principio de Responsabilidad Demostrada, es importante conocer qué ha entendido la SIC por medidas apropiadas y efectivas que logren superar o cumplir con la exigencia de este principio.

Los casos relacionados con el concepto de *"medidas apropiadas y efectivas"* constituyeron el 21,7% del total estudiado. En la Resolución No. 36863 de 2018 se refieren a: la inclusión de la política de tratamiento de datos personales en los principales sitios web del grupo empresarial; atención de Peticiones, Quejas y Reclamos (PQRs) relacionados con datos personales a través de correo electrónico; capacitación sobre la Ley 1581 de 2012 al personal de las áreas de atención al cliente; creación de dos áreas responsables de la protección de datos personales como encargadas de impartir instrucciones y atender los asuntos relacionados; creación de comités para protección al consumidor y para la implementación de sus obligaciones en materia de protección de datos personales conformados por las áreas de operaciones, comercial, informática y tecnología, procesos y negocios complementarios; conformación de un comité de gobierno de la información; contratación de asesoría externa para el diagnóstico del manejo de la información de los clientes; creación de una política de seguridad informática y establecimiento de métodos para el resguardo y la garantía de acceso autorizado a los datos personales de los clientes (Superintendencia de Industria y Comercio. Resolución 36863 de 2014). En el presente caso y al analizar el argumento

presentado por la organización investigada, según el cual, con la implementación de medidas correctivas y el acatamiento de las normas de Protección de Datos Personales de conformidad con el Decreto 1074 de 2015 ha implementado medidas apropiadas y efectivas para cumplir con sus obligaciones, la SIC encuentra *"de elevada importancia las medidas que ha tomado e implementado al interior de su organización la sociedad investigada, teniendo en cuenta su tamaño empresarial"* (Superintendencia de Industria y Comercio. Resolución 36863 de 2014). Sin embargo, cuestionó que dado el gran tamaño empresarial de la organización investigada y la gran cantidad de datos personales que trata, solamente hubiese habilitado un canal (correo electrónico) para la recepción de quejas y reclamos de los titulares

En las Resoluciones 39298 de 2016 y 78899 de 2017, al estudiar el incumplimiento al Principio de Seguridad y sus obligaciones correlativas, la SIC establece que si bien la Guía Accountability no es una norma vinculante, sí constituye un criterio de orientación que busca influir en la conducta de sus destinatarios a partir de lo anterior, establece que el contenido de dicho documento *"es un criterio que pudo -y debió- ser tenido en cuenta"* y así mismo, que aunque no tiene fuerza vinculante, "*al tratarse de un criterio orientador proferido por la Autoridad de Protección de Datos, el mismo, en un ejercicio de diligencia, debió al menos ser revisado por la investigada".* Al respecto indica además la SIC que cuando los destinatarios de las normas buscan criterios que les permitan definir y comprender el alcance de sus obligaciones en materia de Protección de Datos Personales, lo lógico es revisar los documentos expedidos por el ente de control, como en este caso es la Guía Accountability.

De lo anterior puede entenderse entonces que, para la SIC, la Guía Accountability constituye una clara herramienta que define cuáles son las medidas apropiadas y efectivas que deben tomar los Responsables para cumplir con el Principio de Responsabilidad Demostrada; herramienta que, por lo demás, es tenida en cuenta a la hora de determinar en una investigación administrativa si las medidas adoptadas del Responsable han sido o no suficientes.

En la Resolución 27708 de 2017 la entidad investigada demostró que venía trabajando en la implementación de un Programa Integral de Gestión de Datos Personales (PIGDP) *"para cumplir con los estándares fijados por esta Superintendencia mediante las guías para la implementación del principio de responsabilidad demostrada publicadas en mayo de 2015."* (Superintendencia de Industria y Comercio. Resolución 27708 de 2017) y aportó pruebas que permiten inferir las siguientes medidas implementadas dentro de ese Programa Integral: entrega de información a la gerencia sobre el tratamiento de datos personales de los clientes; plan de

auditoría y acta de revisión del programa; instructivo de procedimientos para diligenciar Peticiones, Quejas y Reclamos (PQR's) y para el retiro de información de las bases de datos; nombramiento de un Oficial de Protección de Datos; instructivo de procedimientos e indicadores de medición del tratamiento de datos personales; guion para los recolectores de datos sobre el tratamiento; formato de recepción de PQRs; formato de autorización para el tratamiento; modelos de control de entrega de documentos. Al analizar estas pruebas la SIC concluyó que estas medidas resultan pertinentes a la luz del Principio de Responsabilidad Demostrada.

En la Resolución 44026 de 2018 la SIC consideró que la investigada logró acreditar su compromiso con incrementar sus estándares de Protección de Datos y la implementación de un programa de gestión de datos personales cumpliendo con los estándares del Principio de Responsabilidad Demostrada. Dentro de las pruebas que se aportaron y que permitieron a la autoridad llegar a la anterior conclusión se encuentran: actas de la junta directiva y del comité de auditoría y riesgos; informes del comité de auditoría y riesgos; las Políticas de Protección de Datos Personales; registros de asistencia y modelos de exámenes de capacitaciones internas en protección de datos; boletines de cumplimiento para comunicar al interior de la organización las novedades en la materia; manual de seguridad de la información; procedimiento de gestión de incidentes de seguridad de la información; procedimiento de gestión de bases de datos de personas naturales; inclusión de cláusulas de protección de datos y confidencialidad en los contratos laborales.

2.5. Criterio de Atenuación en la Graduación de la Sanción

En el 26,1% de las resoluciones analizadas el principio fue utilizado por la SIC como criterio de atenuación en la graduación de la sanción interpuesta a los investigados por la violación de otras normas en materia de tratamiento de datos personales. Así, en estos casos la SIC encontró probado el incumplimiento de las obligaciones como Responsable (obligaciones distintas al Principio de Responsabilidad Demostrada) y en ese sentido impuso la sanción correspondiente, no obstante, al encontrar que el investigado también demostró estar tomando medidas apropiadas y efectivas en desarrollo de dicho principio, decidió reducir el monto de la sanción impuesta.

De esta manera, en la Resolución No. 36863 de 2018 la investigada utiliza el Principio de Responsabilidad Demostrada como su principal argumento de defensa ante su incumplimiento a la obligación de dar respuesta en término a las solicitudes de los titulares, indicando que: (i) se

trató de un caso aislado de error de la funcionaria del chat y (ii) destacando el intenso trabajo que viene realizando como organización para cumplir con sus obligaciones establecidas en la ley 1581 de 2012. Así, se enfoca en demostrar las medidas que ha implementado en aras de superar cualquier eventual desconocimiento de sus obligaciones como Responsable del Tratamiento. Si bien la SIC impuso una sanción por el incumplimiento de sus obligaciones como Responsable a la entidad investigada y claramente indicó que la implementación de medidas apropiadas y efectivas no la exoneran del cumplimiento de sus obligaciones, redujo la sanción que inicialmente fue tasada en cien salarios mínimos mensuales legales vigentes (100 smmlv) en cuarenta salarios mínimos mensuales legales vigentes (40 smmlv) en razón a que (i): la organización investigada reconoció la infracción y demostró haber *"implementado previamente a los hechos materia de investigación, medidas apropiadas y efectivas encaminadas a demostrar el compromiso en la protección de datos personales"*. (Superintendencia de Industria y Comercio. Resolución 36863 de 2014).

En la Resolución 27708 de 2017 la entidad investigada utiliza como uno de sus argumentos el de que venía trabajando en la implementación de un Programa Integral de Gestión de Datos Personales (PIGDP) *"para cumplir con los estándares fijados por esta Superintendencia mediante las guías para la implementación del principio de responsabilidad demostrada publicadas en mayo de 2015."* (Superintendencia de Industria y Comercio. Resolución 27708 de 2017) y aportó pruebas de las medidas implementadas, sobre las cuales la SIC concluyó que eran pertinentes a la luz del Principio de Responsabilidad Demostrada. Si bien la SIC procedió a imponer la sanción por la violación de los literales a) y b) del Artículo 17 de la Ley 1581 de 2012, la sanción fue reducida de sesenta salarios mínimos mensuales legales vigentes (60 smmlv) en treinta salarios mínimos mensuales legales vigentes (30 smmlv) teniendo en cuenta varios factores atenuantes, entre ellos el Principio de Responsabilidad Demostrada.

En la Resolución 44026 de 2018 la investigada reconoce el incumplimiento a la obligación de eliminar los Datos Personales de manera extemporánea luego de la solicitud recibida del Titular y utiliza como su defensa que esto se trató de una situación aislada debida a un error humano ajeno a las buenas prácticas y procedimientos implementados dentro de un programa integral de protección de datos personales conforme a las pautas dadas por la Guía Accountability de la SIC. Al respecto, la autoridad indica que el Artículo 2.2.2.25.6.2 establece que la implementación de políticas y procedimientos en materia de datos personales debe ser tenida en cuenta como criterio para evaluar la imposición de sanciones por parte de la SIC, siendo deber del Responsable

demostrar la debida diligencia en el Tratamiento y *"que tales procesos son apropiados y efectivos tanto al interior de la organización como en la atención de consultas, peticiones y reclamos de los titulares"* (Superintendencia de Industria y Comercio. Resolución 44026 de 2018). Dentro de la investigación, la SIC consideró suficientes las pruebas aportadas por la entidad investigada para acreditar que cuenta con procesos para demostrar su compromiso con el incremento de estándares de Protección de Datos, a pesar de que dichos procedimientos no fueron efectivos en el caso concreto pues no se siguieron en debida forma. Si bien la SIC procedió a imponer la sanción por la violación de los literales a) del Artículo 17 y e) del Artículo 18 de la Ley 1581 de 2012, la sanción fue reducida de doscientos cincuenta salarios mínimos mensuales legales vigentes (250 smmlv) en ciento sesenta salarios mínimos mensuales legales vigentes (160 smmlv) teniendo en cuenta como único factor atenuante la aplicación del Principio de Responsabilidad Demostrada.

En la Resolución 4082 de 2019 la organización investigada informó que había desarrollado un Programa Integral de Protección de Datos Personales basado en el Principio de Responsabilidad Demostrada y en la Guía Accountability de la SIC. No obstante, la autoridad constató que el documento mediante el cual se implementaron mediadas para garantizar a los Titulares su derecho a la supresión del Dato Personal se creó con posterioridad a los hechos que dieron lugar a la investigación, motivo por el cual este argumento no fue tenido en cuenta para la atenuación de la sanción.

En la Resolución 4086 de 2019 la entidad investigada utiliza como parte de sus argumentos de defensa el Principio de Responsabilidad Demostrada, aportando material probatorio que permitiría demostrar la implementación de medidas y políticas al interior de su organización en aras de dar cumplimiento a sus obligaciones. No obstante, no aportó las pruebas sobre cómo se implementaron dichos procedimientos en el caso concreto bajo estudio, motivo por el cual la autoridad decidió no tener en cuenta este argumento para la atenuación de la sanción pues si bien se aportaron pruebas documentales, la organización investigada no logró demostrar la implementación de las políticas y medidas en la práctica operativa de la misma.

2.6. Aplicación en la orden que se da al investigado.

En el 17,4% de los casos analizados en la sección resolutiva de la decisión la SIC emitió ordenes administrativas fundadas en el Principio de Responsabilidad Demostrada y encaminadas

a que las investigadas logren garantizar que los hechos materia de investigación no se presenten nuevamente. De esta manera, en la Resolución 83882 de 2018, posterior al análisis de fondo que la SIC hace sobre el contenido y las implicaciones que tiene el Principio de Responsabilidad Demostrada para los Responsables del Tratamiento, decidió en la parte Resolutiva exhortar a la organización investigada a adoptar medidas *"pertinentes, útiles, efectivas y verificables"* para evitar que se repitan hechos similares a los que dieron origen a la investigación; garantizar el respeto a los derechos de los Titulares; dar estricto cumplimiento a la normatividad de Datos Personales; aplicar el Principio de Responsabilidad Demostrada observando las orientaciones de la Guía Accountability, haciendo énfasis en los mecanismos de monitoreo y control que permitan verificar la efectividad de las medidas implementadas; y hacer efectivo el pleno respeto del derecho al *habeas data.*

En la Resolución 51290 de 2018, cuando se analizó el Principio de Responsabilidad Demostrada en conjunto con el incumplimiento de la obligación de adoptar un Manual Interno de Políticas y Procedimientos, se ordenó a la organización investigada implementar manuales internos de políticas y procedimientos para la atención de quejas, consultas y reclamos de los Titulares, así como medidas que garanticen la seguridad apropiada de los Datos Personales y una estructura administrativa adecuada para garantizar los derechos de los Titulares.

En las Resoluciones 9766 de 2019 y 9800 de 2019 no se analizó de fondo el Principio de Responsabilidad Demostrada, ni se le mencionó en relación con alguna otra de las obligaciones de los Responsables. No obstante, se sancionó a las entidades investigadas por incumplir varias de sus obligaciones bajo el régimen de protección de Datos Personales y con base en el Principio de Responsabilidad Demostrada y en virtud del mismo se ordenó que en un término de dos (2) meses la entidad investigada debía adoptar medidas efectivas, apropiadas y verificables para: evitar que las situaciones que dieron lugar a imposición de la sanción volviesen a ocurrir e implementar mecanismos de monitoreo permanente respecto de la efectividad de dichas medidas. En cuanto a la demostración del cumplimiento de lo anterior se ordenó presentar a la autoridad una certificación de cumplimiento expedida por un tercero e imparcial y especializado en los temas de que trata este asunto y aportar los resultados de una auditoría externa enfocada en la verificación de la aplicación de las medidas.

3. Conclusiones del Capitulo

Del análisis de las resoluciones se pudo establecer que, en general, las actuaciones administrativas no se iniciaron para efectos de abordar el estudio del Principio de Responsabilidad Demostrada sino que iniciaron por una Queja de un Titular o en un hecho noticioso de gran difusión en el que la autoridad evidencia la presunta violación general o de otros deberes específicos del Responsable o de los derechos del Titular, mas no por el Principio de Responsabilidad Demostrada como tal. No obstante, en las resoluciones que se reseñan en el presente trabajo, es posible extraer el abordaje que ha realizado la SIC del Principio de Responsabilidad Demostrada dentro de una de las siguientes categorías temáticas que se muestran en la Tabla 2, enfatizando adicionalmente que la mayor frecuencia de eventos correspondió al incumplimiento de la obligación de contar con un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581 de 2012.

TABLA 2

Resoluciones de la SIC en las cuales el Principio de Responsabilidad Demostrada es aplicado **Resolución No.**	**Se analiza como una obligación autónoma**	**Se analiza en relación con el Principio de Seguridad**	**Se analiza en relación con la obligación de contar con un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581**	**Se define en qué consisten las medidas apropiadas y efectivas**	**Se analiza como criterio de atenuación en la graduación de la sanción**	**Se aplica en la orden que se da al investigado**
36863 de 2014				•	•	
39298 de 2016		•		•		
78899 de 2017		•		•		
27708 de 2017				•	•	
83882 de 2018	•					•
64902 de 2018			•			
63316 de 2018		•	•			
61062 de 2018		•			•	
51290 de 2018			•			•
48813 de 2018			•			
44026 de 2018				•	•	

Resoluciones de la SIC en las cuales el Principio de Responsabilidad Demostrada es aplicado **Resolución No.**	**Se analiza como una obligación autónoma**	**Se analiza en relación con el Principio de Seguridad**	**Se analiza en relación con la obligación de contar con un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581**	**Se define en qué consisten las medidas apropiadas y efectivas**	**Se analiza como criterio de atenuación en la graduación de la sanción**	**Se aplica en la orden que se da al investigado**
45743 de 2018			•			
30906 de 2018			•			
10414 de 2018		•				
1321 de 2019	•					
4082 de 2019					•	
4086 de 2019	•				•	
9766 de 2019						•
9800 de 2019						•
6074 de 2019			•			
5477 de 2019			•			
5848 de 2019			•			
21478 de 2019	•					

Conclusiones

El Responsable del Tratamiento de Datos Personales tiene un papel de suma importancia dentro del sistema de protección de datos personales por cuanto es quien tiene el poder de decisión sobre el Tratamiento de los Datos Personales y las bases de datos. En consecuencia, es el principal destinatario de las normas de Protección de Datos Personales que establecen Principios para el Tratamiento, obligaciones para los Responsables y los derechos de los Titulares, con el objetivo de garantizar el pleno ejercicio y la protección del *habeas data*. Por su parte, el Principio de Responsabilidad Demostrada se encuentra presente en varios referentes internacionales y significa un esfuerzo hacia la materialización de las normas de Protección de Datos Personales. En este sentido dicho Principio propende porque los principios para el Tratamiento, las obligaciones de

los Responsables y los derechos de los Titulares tengan verdadera aplicación práctica y no se queden en el papel. Igualmente, imponen la necesidad de establecer medidas que se ajusten a las características propias de cada organización, realizando un esfuerzo permanente y proactivo por implementar y supervisar el cumplimiento de las mismas.

La SIC ha abordado el estudio y aplicación del Principio de Responsabilidad Demostrada en sus investigaciones administrativas iniciadas a raíz de quejas recibidas de los Titulares, de hechos noticiosos de amplia difusión en las que se ha evidenciado el posible incumplimiento de las normas de Protección de Datos Personales por parte de los Responsables y en actuaciones iniciadas de oficio. A la fecha, ninguna de las investigaciones se inició por el Principio de Responsabilidad Demostrada como tal, sino que al existir evidencia del incumplimiento de otras de las obligaciones del Responsable dentro de la investigación, la SIC entró a estudiar las medidas que había tomado el Responsable en materia de Protección de Datos Personales y su cumplimiento bajo el umbral que impone el Principio de Responsabilidad Demostrada. En este contexto, se establecen seis (6) categorías temáticas bajo las cuales la SIC abordó el estudio y dio aplicación al Principio de Responsabilidad Demostrada.

De conformidad con las Resoluciones estudiadas puede concluirse que el Principio de Responsabilidad Demostrada es para la SIC una obligación autónoma en sí misma, sobre la cual debe poder demostrarse el cumplimiento por los Responsables, y por la cual podrán ser sancionados sin necesidad de que se pruebe el incumplimiento a otras obligaciones del régimen de Protección de Datos Personales. Así, para la SIC esta obligación está relacionada con el concepto de cumplimiento o "*compliance*" en cuanto a que su contenido implica que los Responsables deben generar evidencias de sus esfuerzos por cumplir con toda la normativa de Protección de Datos Personales, demostrando la disposición de recursos, creando funciones, estructuras y metodologías concretas para asegurar dicho cumplimiento; priorizando la identificación, clasificación y adopción de medidas de mitigación de riesgos.

En este contexto, en sus Resoluciones la SIC da pautas para definir el alcance del Principio de Responsabilidad Demostrada y del significado o contenido de la obligación que de él se deriva de adoptar *"medidas apropiadas y efectivas".* Además de indicar varias medidas que los Responsables investigados han tomado en sus organizaciones y que han resultado suficientes para ser considerados como *"medidas apropiadas y efectivas"*, la pauta principal que establece la

autoridad a este respecto es que los Responsables deben implementar un Programa Integral de Gestión de Datos Personales siguiendo las pautas indicadas en su Guía Accountability. Así, la SIC indica que, si bien este documento no es vinculante como tal, sí es un criterio de orientación para los Responsables que la SIC como autoridad de Protección de Datos Personales ha emitido para hacerle saber a sus supervisados qué se espera de ellos. De las Resoluciones puede concluirse que, definitivamente esta guía es tenida en cuenta por la autoridad para determinar si las medidas tomadas por los responsables son o no *"apropiadas y efectivas".*

Por otro lado, la SIC ha abordado el estudio del Principio de Responsabilidad Demostrada en relación con violaciones al principio de seguridad. Lo anterior por cuanto la obligación que se deriva del principio de seguridad puede resultar amplia en cuanto a que este no establece cuáles medidas o requisitos específicos deben cumplir los Responsables, lo cual además es usado como argumento de defensa por algunas organizaciones investigadas quienes manifiestan que este principio no establece requisitos o mandatos específicos. Así, la SIC hace uso del Principio de Responsabilidad Demostrada para realizar una aproximación a cuáles son las medidas que deben usar los Responsables para mantener la seguridad de los Datos Personales. La SIC indica, entonces, que bajo este principio los Responsables mismos son los encargados de definir dentro de su estructura y su operación qué medidas deben tomarse para garantizar la seguridad de las bases de datos y los Datos Personales, medidas que bajo los estándares de Responsabilidad Demostrada que permea todo el sistema de Protección de Datos Personales deben ser *"apropiadas y efectivas"*. La la SIC indica entonces que, bajo la Responsabilidad Demostrada, para el cumplimiento del Principio de Seguridad, los Responsables deben estar en capacidad de demostrar que han diseñado e implementado medidas proporcionales a su estructura y a su tamaño empresarial para garantizar la seguridad.

Adicionalmente, el Principio es estudiado en relación con el deber de los Responsables de adoptar un manual interno de políticas y procedimientos que garantice el adecuado cumplimiento de la ley 1581 de 2012 (Lit. k, art. 17, Ley 1581 de 2012). La SIC relaciona de manera directa el incumplimiento de este deber con el de la Responsabilidad Demostrada, en cuanto este último establece que los Responsables no solo deben tomar medidas suficientes y adecuadas para cumplir con sus obligaciones, sino que estas medidas deben estar documentadas. Así, la omisión de adoptar el manual de políticas internas no solo resulta en un incumplimiento del literal k del Artículo 17 de la Ley 1581, sino también en un incumplimiento del Principio de Responsabilidad Demostrada en cuanto este exige el desarrollo de políticas internas efectivas que demuestren el cumplimiento

de las obligaciones del Responsable, sería entonces este manual donde dichas políticas deben materializarse.

Además, se observa que la posibilidad que prevé el Artículo 2.2.2.25.6.2 del Decreto 1074 de 2015 de que la verificación del cumplimiento del Principio de Responsabilidad Demostrada sea tenida en cuenta a la hora de evaluar la imposición y tasación de sanciones se ha materializado en las decisiones de la SIC. De igual manera ha sido usada como argumento por las organizaciones investigadas y este ha prosperado. En este sentido, en casos en que se ha comprobado incumplimientos a las obligaciones del régimen de Protección de Datos Personales, cuando la investigada ha demostrado la existencia e implementación previa de procedimientos y medidas que a juicio de la SIC resultan apropiadas y efectivas, esta ha sido la base para una reducción considerable de la sanción que inicialmente se impuso, dándose reducciones del 40%, 50% y hasta el 64%.

Por último, a partir del año 2018 la SIC comienza a introducir el Principio de Responsabilidad Demostrada no dentro del estudio de la conducta de la investigada pero sí al momento de dar las ordenes administrativas que corresponden por el incumplimiento a otras obligaciones del régimen de Protección de Datos Personales, distintas a este principio. Así, se comienza a exhortar a las entidades u organizaciones investigadas a que den verdadero cumplimiento a sus obligaciones en el Tratamiento de Datos Personales bajo el umbral que dispone el Principio de Responsabilidad Demostrada. En este sentido, se ordena la implementación de medidas apropiadas y efectivas en materia de Tratamiento de Datos Personales que aseguren el cumplimiento de sus obligaciones y su demostración a la autoridad mediante la realización de auditorías externas llevadas a cabo por un tercero imparcial, especializado en estos temas, que certifique su adecuado cumplimiento.

Ahora, si bien existe un mandato positivo de implementar el Principio de Responsabilidad Demostrada en el Tratamiento de Datos Personales, no hay una norma que establezca cuáles son las obligaciones, requisitos o criterios específicos que deben cumplir los Responsables del Tratamiento para demostrar el cumplimiento de este Principio ante la SIC lo cual resulta problemático pues para los destinatarios de la norma no resulta claro cuáles son las obligaciones que se les imponen. Con todo lo anterior, se tiene que el estudio y análisis de las Resoluciones de la SIC en materia de protección de datos personales resultan ser un recurso valioso para solucionar el problema de investigación planteado en la introducción y consistente en la falta de mandatos claros y específicos para los responsables a la hora de abordar el cumplimiento del Principio de

Responsabilidad Demostrada. Como se desarrolló a lo largo del trabajo, se observa que el Principio de Responsabilidad Demostrada ha sido objeto de un desarrollo importante en las decisiones administrativas de la SIC, que a su vez está exigiendo a los Responsables el cumplimiento efectivo de este principio. El estudio de estas decisiones permite aproximarse al contenido de la Responsabilidad Demostrada y las exigencias que la autoridad está realizando bajo el mismo a los Responsables. Se observa entonces que, este principio está siendo objeto de verificación por parte de la SIC, haciendo parte importante del análisis que hace la autoridad a la hora de decidir si un Responsable está o no cumpliendo sus obligaciones en materia de Tratamiento de Datos Personales, sirviendo como atenuante de la sanción cuando se presentan fallas y haciendo parte de las órdenes que la entidad imparte a los investigados.

REFERENCIAS

Constitución Política de la República de Colombia. (20 de julio de 1991).

Congreso de Colombia. (17 de octubre de 2012). Por la Cual se Dictan Disposiciones en Materia de Datos Personales. [Ley 1581 de 2012]. DO: 48.587

Corte Constitucional. (6 de octubre de 2011). Sentencia C-748. [MP Jorge Ignacio Pretelt Chaljub]

Corte Constitucional. (24 de agosto de 2011). Sentencia C-634. [MP Luis Ernesto Vargas Silva]

Martínez, A. (2019). *La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales?*, La Propiedad Inmaterial, 27, 5-23. doi: https://doi.org/10.18601/16571959.n27.01

Ministerio de Comercio, Industria y Turismo de Colombia. (26 de mayo de 2015). Decreto Único Reglamentario de Sector Comercio, Industria y Turismo. [Decreto 1074 de 2015].

Moreno, L. (2016). *Precedente judicial y administrativo en la regulación económica colombiana.* Derecho del Estado n.° 37, Universidad Externado de Colombia, julio diciembre de 2016, pp. 165-188. doi: http://dx.doi.org/10.18601/01229893.n37.05

Quecán, R. (2020). *El precedente administrativo en Colombia: implicaciones y dificultades.* Revista Estudios Socio-Jurídicos, 22(1), 353-390.

Organisation for Economic Cooperation and Development [OECD]. (2013). *The OECD Privacy Framework.* Organization for Economic Cooperation and Development [OECD]. doi: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Parlamento Europeo & Consejo Europeo. (27 de abril de 2016). Reglamento (UE) 2016/679. *Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).* DO: L 119/1.

Remolina, N. (2013). *Tratamiento de Datos Personales: Aproximación internacional y comentarios a la Ley 1581 de 2012.* (1ª ed.). Legis Editores.

Remolina, N. & Álvarez, L. F. (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.

Remolina, N., Tenorio, M.M. & Quintero, G.A. (2018). *De la Responsabilidad Demostrada en las Funciones Misionales de la Registraduría Nacional del Estado Civil: Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información.* Registraduría Nacional del Estado Civil. Centro de Estudios en Democracia y Asuntos Electorales (CEDAE).

Superintendencia de Industria y Comercio. (28 de mayo de 2015). *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

Superintendencia de Industria y Comercio. (30 de mayo de 2014). Resolución No. 36863.

Superintendencia de Industria y Comercio. (21 de julio de 2016). Resolución No. 39298.

Superintendencia de Industria y Comercio. (22 de mayo de 2017). Resolución No. 27708.

Superintendencia de Industria y Comercio. (30 de noviembre de 2017). Resolución No. 78899.

Superintendencia de Industria y Comercio. (16 de febrero de 2018). Resolución No. 10414.

Superintendencia de Industria y Comercio. (7 de mayo de 2018). Resolución No. 30906.

Superintendencia de Industria y Comercio. (25 de junio de 2018). Resolución No. 44026.

Superintendencia de Industria y Comercio. (29 de junio de 2018). Resolución No. 45743.

Superintendencia de Industria y Comercio. (12 de julio de 2018). Resolución No. 48813.

Superintendencia de Industria y Comercio. (23 de julio de 2018). Resolución No. 51290.

Superintendencia de Industria y Comercio. (24 de agosto de 2018). Resolución No. 61062.

Superintendencia de Industria y Comercio. (30 de agosto de 2018). Resolución No. 63316.

Superintendencia de Industria y Comercio. (4 de septiembre de 2018). Resolución No. 64902.

Superintendencia de Industria y Comercio. (15 de noviembre de 2018). Resolución No. 83882.

Superintendencia de Industria y Comercio. (24 de enero de 2019). Resolución No. 1321.

Superintendencia de Industria y Comercio. (21 de febrero de 2019). Resolución No. 4082.

Superintendencia de Industria y Comercio. (21 de febrero de 2019). Resolución No. 4086.

Superintendencia de Industria y Comercio. (7 de marzo de 2019). Resolución No. 5477.

Superintendencia de Industria y Comercio. (14 de marzo de 2019). Resolución No. 5848.

Superintendencia de Industria y Comercio. (18 de marzo de 2019). Resolución No. 6074.

Superintendencia de Industria y Comercio. (25 de abril de 2019). Resolución No. 9766.

Superintendencia de Industria y Comercio. (25 de abril de 2019). Resolución No. 9800.

Superintendencia de Industria y Comercio. (17 de junio de 2019). Resolución No. 21478.

Voigt, P. & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR) A Practical Guide.* Springer International Publishing. doi: https://doi.org/10.1007/978-3-319-57959-7