ESTUDIO SOBRE APLICACIÓN DE CONTROLES EN SEGURIDAD DE LA INFORMACIÓN PARA GARANTIZAR LA PROTECCIÓN DE USO DE DATOS PERSONALES DE ACUERDO CON LA LEGISLACIÓN Y NORMATIVIDAD EN EL TERRITORIO COLOMBIANO

RICARDO RUFINO RAMIREZ RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

ESTUDIO SOBRE APLICACIÓN DE CONTROLES EN SEGURIDAD DE LA INFORMACIÓN PARA GARANTIZAR LA PROTECCIÓN DE USO DE DATOS PERSONALES DE ACUERDO CON LA LEGISLACIÓN Y NORMATIVIDAD EN EL TERRITORIO COLOMBIANO

RICARDO RUFINO RAMIREZ RIVERA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Mg. LUIS FERNANDO ZAMBRANO
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

“NOTA DE ACEPTACIÒN”

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., septiembre 20 de 2022

DEDICATORIA

Expreso mi agradecimiento al ser supremo Dios, bastión central presente en mi vida y mi familia y, quien con su bendición llena siempre mis esperanzas y proyectos.

Dedico este trabajo y les expreso mi gran sentido de agradecimiento a mi esposa e hijos, quienes siempre estuvieron acompañándome, dándome fuerza y animo en el desarrollo de este camino que emprendí en realizar la presente especialización.

.

AGRADECIMIENTOS

Por último, deseo expresar mi gratitud a la Universidad Nacional Abierta y a Distancia – UNAD y en especial a todos mis tutores y director Luis Fernando Zambrano, quienes con su dedicación y enseñanza fueron un factor de crecimiento personal y profesional durante el proceso académico y el desarrollo del presente trabajo.

CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AUTORIZACIÓN: la ley 1581 de 2012 para la protección de datos personales la define como consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.[1]

BASE DE DATOS PERSONALES: la ley 1581 de 2012 para la protección de datos personales la define como un conjunto organizado de datos personales que sea objeto de Tratamiento.[2]

CONTROLES DE SEGURIDAD: Son los diferentes mecanismos, medidas, actividades y procedimientos entre otros que se ejecutan o implementan para salvaguardar y proteger los datos personales de los titulares, haciendo uso de buenas prácticas y normatividad.

DATO PERSONAL: de acuerdo con la ley 1581 de 2012 la define como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[3]

DERECHO DE HABEAS DATA: de acuerdo con definición por la Superintendencia de Industria y Comercio la define como el derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.[4]

[1] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 2.
[2] Ibid.
[3] Ibid.
[4] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manejo de Información personal, “Habeas data”. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/manejo-de-informacion-personal

ENCARGADO DEL TRATAMIENTO: de acuerdo con la ley 1581 de 2012 se refiere a la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.[5]

INTIMIDAD: Según la corte constitucional de Colombia en la sentencia C-640/10 lo reconoce como un derecho fundamental que permite a las personas manejar su propia existencia como a bien lo tengan con el mínimo de injerencias exteriores.[6]

PRIVACIDAD: se refiere al entorno de la vida personal de una persona o individuo, en un ambiente reservado o confidencial de la misma el cual se encuentra fuera del alcance de las demás personas o la sociedad.

PROTECCION DE DATOS: se refiere a la ejecución de métodos o mecanismos, actividades para salvaguardar los datos personales de los titulares.

RESPONSABILIDAD DEMOSTRADA: Se refiere a que todo responsable o encargado del tratamiento de datos personales a un requerimiento de una autoridad delegada debe demostrar o comprobar que ha implementado mecanismo o medidas para garantizar la confidencialidad y seguridad de los datos personales de los titulares, así como el cumplimiento a las disposiciones dispuestas por la superintendencia de Industria y Comercio – SIC.[7]

---

[5] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 2.

[6] CORTE CONSTITUCIONAL DE COLOMBIA. Sentencia C-640/10. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.corteconstitucional.gov.co/relatoria/2010/C-640-10.htm#:~:text=C%2D640%2D10%20Corte%20Constitucional%20de%20Colombia&text=Desde%201992%2C%20la%20Corte%20Constitucional,el%20m%C3%ADnimo%20de%20injerencias%20exteriores.

[7] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manejo de Información personal, “Habeas data”. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

RESPONSABLE DEL TRATAMIENTO: la ley 1581 de 2012 para la protección de datos personal la define como 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.[8]

TITULAR: la ley 1581 de 2012 para la protección de datos personales lo define como la persona natural cuyos datos personales sean objeto de Tratamiento.[9]

TRATAMIENTO: la ley 1581 de 2012 para la protección de datos personales la define como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.[10]

[8] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 2.
[9] Ibid.
[10] Ibid.

RESUMEN

Este documento monográfico presenta un análisis de las medidas y controles en seguridad para la protección de datos personales con referencia en las normatividades y legislaciones en protección y privacidad de los mismos de la Unión Europea y los gobiernos de España, México, Perú, Chile y Colombia, en el documento se realiza una identificación y evaluación de las debilidades o la ausencia de controles en seguridad de la información para la salvaguardar los datos personales existentes en las normativas y disposición en mención; así mismo valora entre otras, cuales fuentes originaron sanciones por la Superintendencia de Industria y Comercio (SIC) durante los últimos tres años. Finalmente presenta las recomendaciones en medidas y controles de seguridad, con el fin que las entidades minimicen el riesgo de amenazas en vulnerabilidades que puedan comprometer la integridad, disponibilidad o confidencialidad de los datos personales tratados por las mismas en el territorio colombiano y evitar sanciones pecuniarias de ley. El estudio toma como referencia las normas internacionales ISO/IEC 27001:2013 e ISO/IEC 27002:2015, que describen requisitos para la implementación de controles para la seguridad la información; la Ley estatutaria 1581 de 2012 y el Decreto 1377 de 2013 que dictan disposiciones para la protección de los datos personales, así como las disposiciones, manuales y guías que emite la Superintendencia de Industria y Comercio (SIC) como entidad delegada para la vigilancia en la gestión de los datos personales en el territorio colombiano. Este documento va dirigido en general a todos los sectores que deben cumplir con una normatividad en cada uno de los países y en especial en el estado colombiano con la ley 1581 de 2012, la cual busca la protección en el uso y tratamiento de los datos personales, así como el respeto a la privacidad de los titulares.

Palabas claves: Datos personales, controles en seguridad, legislación, protección, sanciones.

ABSTRACT

This monographic document presents an analysis of the security measures and controls for the protection of personal data with reference to the regulations and legislation on protection and privacy of the same of the European Union and the governments of Spain, Mexico, Peru, Chile and Colombia. , in the document an identification and evaluation of the weaknesses or the absence of information security controls is made to safeguard the existing personal data in the regulations and provision in question; Likewise, it assesses, among others, which sources originated sanctions by the Superintendence of Industry and Commerce (SIC) during the last three years. Finally, it presents the recommendations on security measures and controls, so that entities minimize the risk of threats in vulnerabilities that may compromise the integrity, availability or confidentiality of personal data processed by them in Colombian territory and avoid financial penalties of law. The study takes as reference the international standards ISO/IEC 27001:2013 and ISO/IEC 27002:2015, which describe requirements for the implementation of information security controls; Statutory Law 1581 of 2012 and Decree 1377 of 2013 that dictate provisions for the protection of personal data, as well as the provisions, manuals and guides issued by the Superintendence of Industry and Commerce (SIC) as a delegated entity for surveillance in the management of personal data in Colombian territory. This document is directed in general to all sectors that must comply with regulations in each of the countries and especially in the Colombian state with Law 1581 of 2012, which seeks protection in the use and treatment of personal data. , as well as respect for the privacy of the owners.

Keywords: Personal data, security controls, legislation, protection, sanctions.

INTRODUCCIÓN

El progreso de las tecnologías de la información ha modificado la forma de vivir, influyendo en las diferentes actividades y labores diarias que realizan las personas; el empleo de herramientas informáticas, sistemas de información y plataformas de tecnología, ayudan en la resolución de problemas, igualmente automatizar y dinamizar procesos, todos encaminados en facilitarle y hacerle la vida mejor al ser humano y la sociedad en general.

Ahora, la información, es el insumo principal en las Tecnologías de la Información (TI), siendo de gran valor entre otros los datos personales, los cuales son tratados en actividades comerciales, financieras, académicas, laborales y la salud entre un sinnúmero de operaciones que se realizan en las actividades del ser humano y la sociedad.

Esta globalización y masificación de las TI van de la mano con el delito, en especial el robo de bases de datos personales, con el ánimo de realizar fraudes y cometer delitos informáticos, lo que requiere que las entidades que recolectan datos personales implementen o mejoren sus medidas de control en seguridad informática, así mismo den cumplimiento a la normatividad y leyes vigentes para la salvaguarda de los datos personales.

Las entidades por normatividad internacional y particularmente en el territorio colombiano deben implementar programas, mecanismos y medidas que permitan gestionar la salvaguarda de los datos personales de los titulares, y terceros entre otros, mediante la implementación de controles técnicos en seguridad, procedimientos, manuales e instructivos que permitan mitigar el riesgo de materialización del riesgo en protección de datos personales, así como minimizar las sanciones dispuestas en la ley 1581 de 2012.

Ahora bien, se requiere por parte de las entidades, realizar mejoras o implementar controles que permitan gestionar la infraestructura tecnológica y la seguridad de las redes que soportan el uso de los datos personales a los que dan tratamiento, mediante el empleo de herramientas de software, la administración, operación, seguridad y mantenimiento de redes para su óptimo funcionamiento, así como la implementación de marcos de control y buenas prácticas en seguridad de la información.

El realizar un análisis de los controles de seguridad de la información usados para la protección de los datos personales, contrastar la información relacionada con marcos de referencia y legislación enfocada en la protección de los mismos, y estimar las causas que originaron las sanciones por la Superintendencia de Industria y Comercio – SIC durante los últimos tres años, permitirá plantear a las entidades, recomendaciones en gestion de infraestructura tecnológica y seguridad de redes que contribuyan en minimizar el riesgo de incumplimiento de los controles de seguridad para la protección de datos personales.

1 FORMULACION DEL PROBLEMA

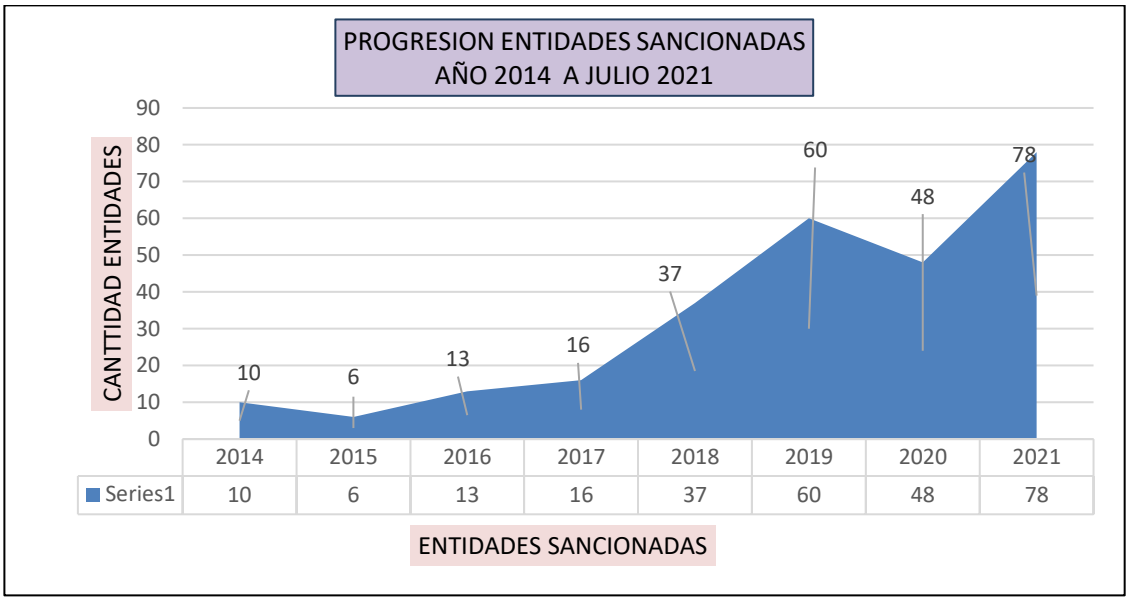
1.1 ANTECEDENTES DEL PROBLEMA

La jurisprudencia colombiana vigente dispuso la ley estatutaria 1581 de 2012 dictando disposiciones generales para la protección de datos personales, dispone en el artículo "*1o. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*.[11]"

Iniciada en firme la ley, la Superintendencia de Industria y Comercio (SIC), entidad que regula y dicta disposiciones al respecto; como resultado de este control desde el año 2014 al año 2021, ha emitido resoluciones de sanción en protección de datos personales[12] a 268 entidades, la ilustración 1 presenta una progresión de las entidades sancionadas, que aún presentaron debilidades o no fortalecieron sus controles en seguridad y los procedimientos en protección para dar cumplimiento la ley 1581 de 2012.

[11] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 2.
[12] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Ilustración 1. Entidades sancionadas por el SIC año 2014 a julio 2021



Fuente: Adaptación con información de la SIC - decisiones administrativas 2019, 2020 y 2021.[13]

1.2 FORMULACIÓN DEL PROBLEMA

Aunque para cumplir la ley 1581 de 2012 hay publicaciones referentes a la misma y las acciones que deberían realizar las entidades para cumplirla, estas se hacen desde el aspecto jurídico y no se evidencia a la fecha un instrumento técnico de fácil comprensión y uso por las entidades que les sirva de guía para el análisis y evaluación de los riesgos, vulnerabilidades técnicas y de cumplimiento, igualmente su integración con un Sistema de Gestión de Seguridad de la Información (SGSI) y un Programa Integral de Gestión de Datos Personales (PIGDP) que les permita mejorar y tener un control de la gestión de la salvaguarda de los datos personales de sus titulares.

[13] Ibid.

La ley 1581 de 2012, se enmarca entre las leyes estatutarias[14], dictando normativas para la protección de datos personales, el artículo 2. Ámbito de aplicación dispone entre otras disposiciones:

> *"Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales…"*[15]

Por lo cual, las entidades, se ven abocadas a dar cumplimiento a esta ley, lo que conlleva que deben generar estrategias para la implementación de diferentes mecanismos como: herramientas tecnológicas, evaluación de riesgos, controles en seguridad, procedimientos, medidas y políticas en seguridad de la información, entre otras, para dar observancia a la normatividad que reglamenta la protección de datos personales en Colombia.

Ahora bien, de acuerdo con la ley 1581 de 2012, un incumplimiento a las disposiciones fijadas en la misma conlleva a que estas entidades se vean inmersas a sanciones de tipo pecuniario hasta dos mil (2000)[16], salarios mínimos vigentes, suspensión de actividades, cierre temporal o en caso más críticos el cierre inminente y total de la actividad relacionados con el tratamiento de datos de tipo sensible.

¿Cómo el análisis de los controles de seguridad para la protección de datos personales permite generar recomendaciones que al ser aplicadas contribuyen en reducir o anular sanciones de entes de control como la SIC?

---

[14] Ibid. p. 2
[15] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 2.
[16] Ibid. p. 11.

2 JUSTIFICACIÓN

El alto riesgo de exposición de datos personales de los titulares y sus posibles consecuencias para las entidades desde el aspecto jurídico y sanciones pecuniarias por la SIC, las coloca en la posición de evaluar sus controles para salvaguardas de seguridad y cumplimiento, además de fortalecer con los empleados una cultura de adopción y apropiación en seguridad de la información y “protección de datos personales”.

La presente monografía tiene como propósito realizar un estudio de seguridad de la información que permita efectuar una evaluación de las amenazas que pongan en riesgo la protección de los datos personales en las entidades, diagnosticar el estado de vulnerabilidad, validar los controles en seguridad existentes y determinar que salvaguardas técnicas y procedimentales se deben aplicar para garantizar el cumplimiento de la ley 1581 de 2012, así mismo salvaguardar la confidencialidad, integridad y privacidad de los datos personales de titulares que tratan las entidades.

Este estudio permite a las entidades, la alta dirección y el oficial de cumplimento o sección comisionada de la protección de los datos personales, un marco de referencia, práctica, dinámica, de fácil entendimiento y uso para la evaluación de vulnerabilidades, mitigar el riesgo y asegurar la confidencialidad, integridad y privacidad de los datos personales de los titulares a los cuales les da tratamiento.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los controles de seguridad de la información usados para la protección de los datos personales teniendo como referente la ley 1581 de 2012 y las directrices emitidas por la Superintendencia de Industria y Comercio (SIC).

3.2 OBJETIVOS ESPECÍFICOS

Contrastar información relacionada con marcos de referencia y legislación enfocada en la protección de datos personales, que permita reconocer debilidades o falencias presentas en la implementación de los controles de seguridad.

Estimar las causas que originaron sanciones por la Superintendencia de Industria y Comercio (SIC) debido a la mala implementación o ausencia de controles de seguridad para la protección de datos personales durante los últimos tres años.

Plantear recomendaciones que contribuyan en minimizar el riesgo de incumplimiento de los controles de seguridad para la protección de datos personales.

4 MARCO REFERENCIAL

Para el desarrollo del estudio desde la parte jurídica como interpretación al cumplimiento de protección de datos personales se referencia, la ley 1581 de 2012, el decreto 1377 de 2013, las disposiciones emitidas por la SIC y desde el ámbito en seguridad información, igualmente el estándar ISO/IEC 27001:2013 encaminado a los Sistemas Gestión de la Seguridad de la Información que apoya a las entidades en la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos, la norma ISO/IEC 27002:2013 que presenta lineamientos en aplicación de medidas viables en la administración de la seguridad de la información y la norma ISO 31000 para la gestión de riesgos. Los postulados y recomendaciones propuestos en estos documentos se tomarán como línea base para integrarlos, estructurarlos e ir generando las recomendaciones de acuerdo con los objetivos propuestos.

4.1 MARCO TEÓRICO

Como lo manifiesta Arellano[17], el comienzo de la legislación de la protección de los datos personales se ubica en la cronología del mundo con el inicio de la sociedad de la información en los años setenta, época en que la industrialización los acogió como una política pública y de interés para los gobiernos con el crecimiento y desarrollo de las tecnologías de la información (TI).

Este auge y desarrollo de las TI, hizo prestar relevancia ya que para la época de los años setenta las medidas en tratamiento de la información general mediante el uso de las TI no eran reguladas.

[17] ARELLANO LÓPEZ, Christian Alberto. El derecho de protección de datos personales. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-55452020000200009&lang=es

En este sentido, las TI vinieron a revolucionar la industria debido a su potencial de aumentar los ingresos económicos al realizar el tratamiento de la información que contenía datos personales que realizaban en sus procesos comerciales.

Ahora bien, los gobiernos identificaron, que, con el uso de las TI y el poder preferencial de ejercer el control sobre la sociedad, lo emplean (hoy por hoy escudándose en el ejercicio de la seguridad nacional lo siguen haciendo) para una invasión de la vida privada del ser humano, violando un principio derecho fundamental de los ciudadanos en su intimidad personal.

Este exceso de la invasión a la intimidad de las personas por parte de los gobiernos y la industria conllevó a que se comenzaran a desarrollar propuestas y se promulgaran las primeras normativas o leyes relacionadas con la protección de los datos personales.

Como resultado de esta evolución se pueden encontrar dos ámbitos principales entre otros: El primero hace relación a que por parte de los estados y naciones se dicten disposiciones y lineamientos de orden estatutario con el objetivo de un uso reglado del tratamiento de los datos personales por parte de las entidades sin importar su naturaleza pública o privada y el segundo se enfoca a proteger la persona en su privacidad e intimidad en el uso de la información personal.

Como antecedentes de relevancia en el desarrollo y evolución de leyes en diversas naciones y organizaciones como lo describen Sánchez y Rojas[18] la protección de datos personales se remonta a 1948, cuando la Asamblea General de las Naciones

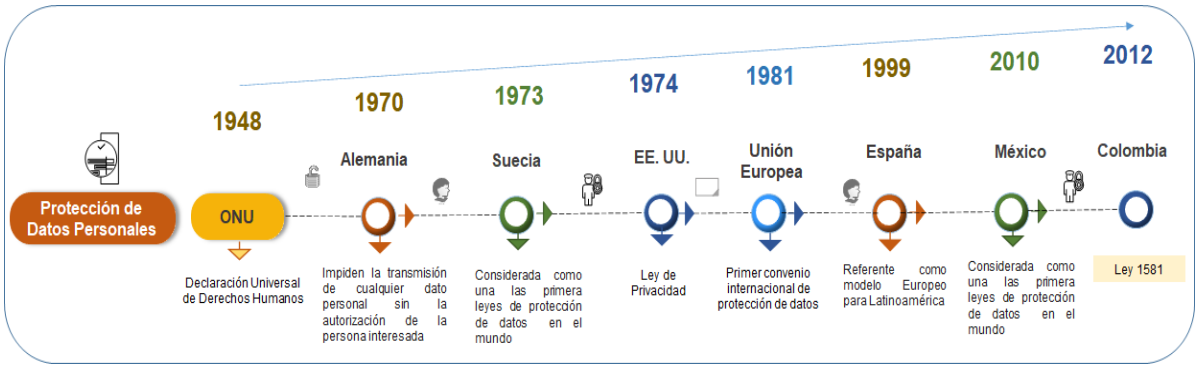
[18] SÁNCHEZ PÉREZ, Gabriel y ROJAS GONZÁLEZ, Isai. Leyes de protección de datos personales en el mundo y la protección de datos biométricos – parte I. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

Unidas adopta el documento conocido como *Declaración Universal de Derechos Humanos*, en este documento se expresan los derechos humanos conocidos como básicos…" el artículo 12 dispone:

> *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*.[19]

La siguiente ilustración presenta una evolución de las siguientes naciones y organizaciones entre otras, que incorporan la protección de datos en sus legislaciones y disposiciones desde la proclamación de la Declaración Universal de los Derechos Humanos, hasta la ley 1581 de 2012 en el estado colombiano:

Ilustración 2. Evolución de legislación datos personales



Fuente: Autor

Como lo manifiesta Remolina[20], a partir de 1985 la mayoría de las constituciones de los países latinoamericanos han tratado los datos personales como una clase de

[19] NACIONES UNIDAS. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://www.un.org/es/about-us/universal-declaration-of-human-rights

[20] UNIANDES. Revista Internacional de Protección de Datos Personales. Aproximación constitucional de la protección de datos personales en Latinoamérica. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

información constitucionalmente protegida, lo que a la fecha ha concedido a los titulares derechos y el ejercicio del cumplimiento constitucional del habeas data[21] para un uso adecuado del tratamiento de sus datos personales que conlleven a evitar una vulneración a sus derechos constitucionales.

En el estado colombiano la protección de datos personales se fundamenta entre otras disposiciones legislativas como: la constitución política de Colombia de 1991 en lo dispuesto en los artículos 15 y 20[22], la ley 1266 de 2008[23], el decreto 1377 de 2013[24], decreto 1074 de 2015[25] y las disposiciones que dicta la Superintendencia de Industria y Comercio (SIC) en protección de datos personales.

Ahora bien, como lo manifiestan Ayala y González[26], en la actualidad con más frecuencia se hace notoria la propagación de nuevos medios de información y comunicación a través de los cuales se divulgan datos de diverso contenido, allí se pueden apreciar los datos personales de cada sujeto, estas grandes fuentes de información son conocidas como nuevas tecnologías de la información y comunicación, es innegable que hoy en día las TI son los medios que utilizan las

[21] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manejo de información personal, 'Habeas data'. El derecho de hábeas data es aquel que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://www.sic.gov.co/manejo-de-informacion-personal

[22] CONSTITUCIÓN POLÍTICA DE COLOMBIA, Asamblea Constituyente de Colombia de 1991, (04, julio, 1991). Consultado el 01 de octubre de 2021. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Documents/Constitucion-Politica-Colombia.pdf.

[23] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1266 (31, diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. El Congreso, p. 1.

[24] COLOMBIA, MINISTERIO DE COMERCIO, INDUSTRIA Y COMERCIO, Decreto 1377 (27, junio, 2013). por el cual se reglamenta parcialmente la Ley 1581 de 2012.

[25] COLOMBIA, MINISTERIO DE COMERCIO, INDUSTRIA Y COMERCIO, Decreto 1074 (26, mayo, 2015). "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

[26] POLITECNICO GRACOLOMBIANO. SISTEMA NACIONAL DE BIBLIOTECAS SISNAB. La protección de datos en la era digital: Colombia-España. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://alejandria.poligran.edu.co/bitstream/handle/10823/2142/Articulo%20Proteccion%20de%20datos%20%20en%20la%20era%20digita%20Colombia-Espa%C3%B1a%20Nov.%2029.pdf?sequence=1&isAllowed=y

entidades para recolectar, tratar y almacenar los datos personales de los titulares, entre los que se encuentran: Internet, redes, computación en la nube, blockchain, bases de datos, sistemas de información, herramientas tecnológicas colaborativas, servidores, portales web, sistemas de videovigilancia y biométricos entre otros medios electrónicos y digitales empleados, lo que conlleva nuevos retos en medidas de seguridad que deben implementar las entidades encaminadas a dos premisas esenciales: la primera son medidas en cumplimiento a la normatividad de la legislación dispuestas por las naciones o estados y la segunda que controles de seguridad deben implementar para la protección de los datos personales de los titulares con el fin de no incurrir en presuntas violaciones o afectaciones en las garantías constitucionales que le asisten a las personas en sus derechos fundamentales.

4.2 MARCO CONCEPTUAL

Para la elaboración de la monografía se presentan los siguientes conceptos del ámbito de la seguridad de la Información relacionados con la protección de los datos personales entre otros:

- NORMA ISO/IEC 27001:2013.

  Define los requisitos que deben implementarse en un SGSI, especifica que controles en seguridad se deben implementar.[27]

[27] ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-6.

- NORMA ISO/IEC 27002:2013

  Presenta una buena guía en buenas prácticas para implementar los requisitos definidos por la ISO/IEC 27001:2013, recomienda con más profundidad que acciones se deben seguir en la implementación de los controles de seguridad. [28]

- MAGERIT

  Marco de referencia para el tratamiento de riesgos e, alineados en la identificación de amenazas y el análisis del impacto que se genere por las infracciones a la seguridad, que puedan afectar las entidades[29].

- MARCO DE CIBERSEGURIDAD DEL NIST – CYBER SECURITY FRAMERWOK - SP 800-53, REV.5

  El Marco de trabajo NIST SP 800-53, REV.5 (del inglés “National Institute of Standards and Technology”) Es un conjunto de controles basado en estándares y buenas prácticas para gestionar y minimizar los riesgos en ciberseguridad[30], fue definido por el gobierno de Estados Unidos enfocado a la protección de las infraestructuras críticas entre las cuales se encuentran las tecnologías de la información, debido a la completitud e integridad de los controles ha sido adoptado por diversas organizaciones en la industria. Se desarrolló tomando como referencia entre otros estándares: COBIT 5, ISO/IEC 27001:2013, CIS

[28] ICONTEC. Guía Técnica Colombiana GTC-ISO/IEC 27002. Técnicas Seguridad. Código de Práctica para Controles de Seguridad de la información (consultado junio 2021). ISBN impreso 978-958-8585-53-6.

[29] ESQUEMA NACIONAL DE SEGURIDAD. MAGERIT – VERSIÓN 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[30] NIST. Special Publication 800-53. Revision 5. Security and Privacy Controls for Information Systems and Organizations. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

CSC, NIST y SP 800-53 Rev.4. Una de las características que ha permitido la adopción de este marco de referencia por la industria y las organizaciones es que ayuda a la gobernanza de la ciberseguridad, permitiendo llevar de forma práctica la estrategia de TI a los objetivos y necesidades del negocio de las organizaciones.

- CONFIDENCIALIDAD.

  Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados, así como la no divulgación de información a individuos, entidades o procesos no autorizados y garantizar el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.[31]

- INTEGRIDAD.

  Propiedad de la información relativa a su exactitud y completitud, que busca mantener los datos libres de modificaciones no autorizadas para conservar con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.[32]

- VULNERABILIDAD.

  Debilidad de un activo o control que puede ser explotada por una o más amenazas y que pueden ser utilizadas por atacantes (personas o usuarios) internos o externos para causar daño, comprometiendo la integridad, disponibilidad o confidencialidad de la información. [33]

[31] ISO27000.ES. Glosario. [en línea]. Consultado el 28 de febrero de 2022. Disponible en Internet: https://www.iso27000.es/glosario.html
[32] Ibid.
[33] Ibid.

- RIESGO

  Efecto de la incertidumbre sobre los objetivos, un posible evento que podría causar daño o pérdidas, o afectar la habilidad de alcanzar objetivos, asociado al impacto y probabilidad de ocurrencia, así como el potencial que una amenaza específica explote las debilidades de un activo o grupo de activos de información para ocasionar pérdida y/o daño a los activos se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.[34]

- OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

  Lista amplia de objetivos y controles para el tratamiento de riesgos de la seguridad de la información, relacionados en el Anexo “A” de la norma ISO/IEC 27001:2013.[35]

- AUTORIZACIÓN.

  La ley estatutaria 1581 de 2012 lo define en el artículo 3. a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;[36]

- BASE DE DATOS.

  La ley estatutaria 1581 de 2012 lo define en el artículo 3. Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;[37]

[34] Ibid.
[35] ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.
[36] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 2.
[36] Ibid. p. 2.
[37] Ibid. p. 2.

- DATO PERSONAL.

  La ley estatutaria 1581 de 2012 lo define en el artículo 3. c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;[38]

- ENCARGADO DEL TRATAMIENTO.

  La ley estatutaria 1581 de 2012 lo define en el artículo 3. Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento;[39]

- RESPONSABLE DEL TRATAMIENTO

  La ley estatutaria 1581 de 2012 lo define en el artículo 3. e) responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;[40]

- TITULAR.

  La ley estatutaria 1581 de 2012 lo define en el artículo 3. f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;[41]

- TRATAMIENTO.

  La ley estatutaria 1581 de 2012 lo define en el artículo 3. g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.[42]

[38] Ibid. p. 2.
[39] Ibid. p. 2.
[40] Ibid. p. 2.
[41] Ibid. p. 2.
[42] Ibid. p. 2.

4.3 MARCO LEGAL

En el marco Internacional se encuentran diversas legislaciones y disposiciones para la protección de los datos personales, se reseñan los de más notoriedad y que han tenido impacto o son de referencia para el estado colombiano en la promulgación de los mismos, igualmente para el marco regulatorio en el estado colombiano se relaciona en orden cronológico las más relevantes de la legislación existente en la materia, resaltando que las que no se enuncien no dejan de ser importantes, que no son independientes, deben armonizarse y darles cumplimiento.

En legislación o disposiciones Internacionales se relacionan entre otras:

- DECLARACIÓN UNIVERSAL DE LOS HUMANOS – NACIONES UNIDAD

  Proclama la presente Declaración Universal de los Derechos Humanos[43] como ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promuevan, mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos, tanto entre los pueblos de los Estados Miembros como entre los de los territorios colocados bajo su jurisdicción.

- LEY ORGÁNICA 3/2018 – ESPAÑA

  Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. En

[43] NACIONES UNIDAS. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://www.un.org/es/about-us/universal-declaration-of-human-rights

la actualidad se encuentra en vigor la Ley Orgánica 3/2018[44], de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), por la que se deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como cualquier otra disposición de igual o inferior rango que contradiga, se oponga o resulte incompatible con lo dispuesto en el RGPD y en la LOPDGDD.

- REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) – 2016 UNION EUROPEA

  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)

- LEY ORGÁNICA 3/2018 - ESPAÑA

  Protección de Datos Personales y garantía de los derechos digitales. pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones.

- ESTANDARES DE PROTECCION DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS

  XIV Encuentro Iberoamericano de Protección de Datos celebrado el 8 de junio de 2016 en Santa Marta Colombia en el marco del IV Congreso Internacional de Protección de Datos Personales organizado por la Superintendencia de Industria

[44] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

y Comercio[45], los países miembro de la Red Iberoamericana de Protección de Datos acordaron la elaboración de los Estándares Iberoamericanos, con el fin de brindar una herramienta que contenga las directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos en aquellos países de la región iberoamericana que no cuentan con estos ordenamientos o que sean referentes para la modernización y actualización de las legislaciones existentes.[46]

En la legislación colombiana se relacionan las siguientes leyes, decretos y resoluciones entre otras:

- CONSTITUCION POLITICA DE COLOMBIA DE 1991

  La protección de datos personales se fundamenta en los ARTÍCULOS 15 Y 20 presentados a continuación:[47]

> *"TITULO II. DE LOS DEERECHOS, LAS GARANTIA Y LOS DEBERES. CAPITULO 1. DE LOS DERECHOS FUNDAMENTALES. ARTICULO 15. FUNDAMENTALES. Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."*
>
> *"TITULO II. DE LOS DERECHOS, LAS GARANTIA Y LOS DEBERES. CAPITULO 1. DE LOS DERECHOS FUNDAMENTALES. ARTICULO 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar*

[45] RED IBEROAMERICANA. XIV Encuentro Iberoamericano: Santa Marta, Colombia 8,9,10 de junio de 2016 [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.redipd.org/es/actividades/encuentro/xiv-encuentro-iberoamericano-santa-marta-colombia-8-9-y-10-de-junio-de-2016

[46] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/colombia-participo-en-la-elaboracion-de-los-estandares-de-proteccion-de-datos-de-los-estados-iberoamericanos

[47] CONSTITUCIÓN POLÍTICA DE COLOMBIA, Asamblea Constituyente de Colombia de 1991, (04, julio, 1991). Consultado el 01 de octubre de 2021. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Documents/Constitucion-Politica-Colombia.pdf.

> *y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres* y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura."

- LEY 527 DE 1999

  Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.[48]

- LEY 1273 DE 2009

  Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[49]

- LEY 1266 DE 2008

  Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.[50] Su finalidad es proteger a las personas

[48] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. El Congreso, p. 1.
[49] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1273 (5, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. El Congreso, p. 1.
[50] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. El Congreso, p. 1.

del uso indebido del empleo de la información personal, de servicios y comercial o lo que se denomina el historial crediticio de los titulares, igualmente las disposiciones de esta ley regulan de forma exclusiva al habeas data financiero. Igualmente, el tratamiento de la información que lo titulares entregan a entidades y centrales de riesgos para el tratamiento de su información en cuanto a al estado del cumplimiento de sus obligaciones financieras

- LEY 1581 DE 2012

Compone el referente jurídico en protección de los datos personales en Colombia, regula el derecho fundamental que tienen todas las personas naturales en lo relacionado al tratamiento de sus datos personales desde que se recolectan, se almacenan, se usan y eliminan, así mismo el derecho que tienen los titulares de actualizar y rectificar la información que tratan las organizaciones.[51], Esta ley busca proteger el derecho a las que tienen las personas en conocer, actualizar y rectificar los datos personales que se hayan recolectado sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada, igualmente dispones los principios generales aplicables a cualquier tipo de tratamiento de Datos Personales, incluyendo datos sensibles y datos de menores de edad, los deberes y obligaciones del Responsable y Encargado del tratamiento de la información, las consideraciones relativas a la solicitud de autorización o consentimiento de los titulares de la información y establece las reglas relacionadas con la transferencia de Datos Personales. Solamente al tratamiento de Datos Personales realizados en territorio colombiano o siempre que un responsable o Encargado de la información que no se encuentre localizado en Colombia, se encuentre sujeto a la legislación colombiana de conformidad con los tratados internacionales aplicables.

[51] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 1.

- DECRETO 1377 DE 2013.

  Es el acto administrativo que reglamenta parcialmente la ley 1581 de 2012, con el fin de normalizar o reglar disposiciones más concretas para las salvaguardas de los datos personales[52].

- DECRETO 1074 DE 2015

  Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Capítulos 25 Reglamenta parcialmente la ley 1581 de 2012, capitulo 26 Registro Nacional de bases de datos, capitulo 27 contenido mínimo de historias crediticias, capitulo 28 Se reglamentan los artículos 12 y 13 de la ley 1266 de 2008.[53]

- DECRETO 620 DE 2020

  Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.[54]

---

[52] COLOMBIA, MINISTERIO DE COMERCIO, INDUSTRIA Y COMERCIO, Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

[53] COLOMBIA, MINISTERIO DE COMERCIO, INDUSTRIA Y COMERCIO, Decreto 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

[54]COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Decreto 620. (2, mayo, 2020). Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- CIRCULAR ÚNICA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO – SIC – TITULO V – PROTECCION DATOS PERSONALES.

  Cómo órgano nombrado para la vigilancia de los datos de personas reglamenta en el título V disposiciones a las entidades públicas y privadas en lo relacionado al cumplimiento para la protección de los datos de personas.[55]

- RESOLUCIÓN 462 DE 2019 PROCURADURIA GENERAL DE LA NACIÓN

  Se adicionan funciones disciplinarias: Adelantar en primera instancia las actuaciones disciplinarias que correspondan por conductas relacionadas en el incumplimiento de las obligaciones contenidas en la Ley 1581 de 2012 y demás disposiciones que la desarrollen, modifiquen y reglamenten a cargo de los sujetos vinculados con las autoridades públicas, para lo cual asumirá las funciones de los literales a), b), c), k), l), m) y n) del numeral 1, así como la de los numerales 4, 5, 6, 10 y 11 del artículo 25 del Decreto Ley 262 de 2000 y las demás que se deriven del ejercicio propio de los asuntos de esa competencia.[56]

[55] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular Única – Protección de datos Personales. [en línea]. Consultado el 04 de enero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/normatividad/052020/Ti%CC%81tulo%20V%20Proteccion%20Datos%20Circular%2003%20del%2030%20de%20marzo%202020%29.pdf

[56] PROCURADURIA GENERAL DE LA NACIÓN. Resolución 462 (26, abril, 2019). Por medio de la cual se asignan funciones a una procuraduría delegada - se adicionan funciones disciplinarias. [en línea]. Consultado el 04 de enero de 2022. Disponible en Internet: https://www.procuraduria.gov.co/relatoria/media/file/flas_juridico/2380_PGN%20Resoluci%C3%B3n%20462%20de%202019%20.pdf.

5 DESARROLLO DE LOS OBJETIVOS

5.1 DESARROLLO OBJETIVO 1

Con referencia al objetivo No. 1 Contrastar información relacionada con marcos de referencia y legislación enfocada en la protección de datos personales, que permita reconocer debilidades o falencias presentadas en las disposiciones de medidas en la implementación de los controles de seguridad, se abordarán fuentes documentales como artículos, trabajos de grado, legislaciones y normatividad entre otros, que permitan dilucidar el problema abordado en la presente monografía.

De acuerdo con el artículo publicado por Nelson Remolina *"Aproximación constitucional de la protección de datos personales en Latinoamérica"*[57], presenta un estudio general de veinte naciones latinoamericanas, en lo referente a la protección de los datos personales, también destaca la importancia que las constituciones latinoamericanas confieren a los datos personales, al habeas data y a la protección de las personas respecto del tratamiento de su información. El siguiente cuadro el resumen del estudio.

Cuadro 1. Resumen estudio artículo publicado por Nelson Remolina

Aspectos sobre protección de datos personales	País y artículo de la Constitución que explícitamente se refiere a cada aspecto
Mención de dato personal, información personal o dato	Argentina (Art. 43), Bolivia (Art.130), Brasil (Art. 5, LXXII), Colombia (Art. 15), Ecuador (Art. 94), Honduras (Art. 182), México (Arts. 6,16 y 20 lit. C -V-), Nicaragua (Art. 26), Panamá (Arts. 42 y 44), Paraguay ((Art. 135), Perú (Art. 2, No. 6), República Dominicana (Art. 44, No.2), Venezuela (Art.28).
Derecho a la protección de datos personales	México (Art. 16) y Panamá (Art. 42).

[57] UNIANDES. Red Académica Internacional. Aproximación constitucional de la protección de datos personales en Latinoamérica. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

Aspectos sobre protección de datos personales	País y artículo de la Constitución que explícitamente se refiere a cada aspecto
Derecho a conocer datos contenidos en bases de datos públicos y privados	Argentina (Art. 43), Bolivia (Art.130), Colombia (Art. 15), Ecuador (Art. 94), Honduras (Art. 182), México (Art. 16), Panamá (Arts. 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, No.2), Venezuela (Art. 28).
Derechos a conocer datos contenidos solamente en bases de datos públicos	Brasil (Art. 5, LXXII), Guatemala (Art. 31), México (Art. 6), Nicaragua (Art. 26).
Derecho a conocer la finalidad del uso de los datos	Argentina (Art. 43), Ecuador (Art. 94), Guatemala (Art. 31), Nicaragua (Art. 26), Paraguay (Art. 135), República Dominicana (Art. 44, No.2), Venezuela (Art.28).
Derecho a conocer el uso que se le da a los datos	Paraguay (Art. 135), República Dominicana (Art. 44, No.2), Venezuela (Art.28).
Derecho a exigir actualización de los datos	Argentina (Art. 43), Colombia (Art. 15), Ecuador (Art. 94), Guatemala (Art. 31), Honduras (Art. 182), Panamá (Arts. 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, No.2 y 70), Venezuela (Art. 28).
Derechos a solicitar rectificación o corrección	Argentina (Art. 43), Bolivia (Art.130), Brasil (Art. 5, LXXII), Colombia (Art. 15), Ecuador (Art. 94), Guatemala (Art. 31), Honduras (Art. 182), México (Arts. 16, 16), Panamá (Arts. 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, No.2, 70), Venezuela (Art.28).
Derecho a solicitar supresión, eliminación, destrucción o cancelación del dato	Argentina (Art. 43), Bolivia (Art.130), Ecuador (Art. 94), Honduras (Art. 182), México (Arts. 16), Panamá (Arts. 42 y 44), Paraguay (Art. 135), República Dominicana (Art. 44, No.2), Venezuela (Art.28).
Derecho a exigir confidencialidad sobre los datos	Argentina (Art. 43), Honduras (Art. 182), Panamá (Arts. 44), República Dominicana (Art.70),
Derecho a impedir transmisión o divulgación de la información	Honduras (Art. 182)
Derecho de oposición	México (Art 16), República Dominicana (Art. 44, No.2),
Tratamiento de datos	Colombia (Art. 16), República Dominicana (Art. 44, No.2)
Recolección de datos	Colombia (Art. 15), Panamá (Arts. 42)
Recolección con consentimiento del titular	Panamá (Arts. 42)

Aspectos sobre protección de datos personales	País y artículo de la Constitución que explícitamente se refiere a cada aspecto
Recolección por disposición de autoridad competente	Panamá (Arts. 42)
Circulación de datos	Colombia (Art. 15)
Acción o garantía de habeas data	Brasil (Art. 5, LXXII), Ecuador (Art. 94), Honduras (Art. 182), Panamá (Arts. 44), Paraguay ((Art. 135), Perú (Art. 200, No. 3), República Dominicana (Art. 70), Venezuela (Art.281).
Acción de amparo	Argentina (Art. 43)
Acción de protección privada	Bolivia (Art.130)
Principio de calidad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de licitud en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de lealtad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de seguridad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de finalidad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2), Panamá (Arts. 42),

Fuente: Adaptación del artículo publicado por Nelson Remolina en UNIANDES. Red Académica Internacional. Aproximación constitucional de la protección de datos personales en Latinoamérica.[58]

Tomando como referencia el cuadro anterior, en el siguiente cuadro se referencia la constitución de Colombia relacionada con los aspectos en protección de datos personales, de 25 aspectos, presenta 7 de los mismos conexos a la protección de datos, que se encuentran implícitamente en el artículo 15 de la misma.

[58] UNIANDES. Red Académica Internacional. Aproximación constitucional de la protección de datos personales en Latinoamérica. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

Cuadro 2. Constitución de Colombia protección de datos personales

#	Aspectos sobre protección de datos personales	Constitución
1	Mención de dato personal, información personal o dato	Colombia (Art. 15)
2	Derecho a conocer datos contenidos en bases de datos públicos y privados	Colombia (Art. 15)
3	Derecho a exigir actualización de los datos	Colombia (Art. 15)
4	Derechos a solicitar rectificación o corrección	Colombia (Art. 15)
5	Tratamiento de datos	Colombia (Art. 15)
6	Recolección de datos	Colombia (Art. 15)
7	Circulación de datos	Colombia (Art. 15)

Fuente: Adaptación del artículo publicado por Nelson Remolina en UNIANDES. Red Académica Internacional. Aproximación constitucional de la protección de datos personales en Latinoamérica.[59]

Igualmente, en el siguiente cuadro se resaltan aquellos aspectos relevantes que desde el enfoque en seguridad de la información merecen atención en la aplicación de buenas prácticas por parte de las entidades para el cumplimiento de la legislación y normatividad que han establecido las naciones en cumplimiento de sus constituciones en los aspectos de la protección y seguridad de los datos personales de los ciudadanos.

Cuadro 3. Aspectos protección de datos personales con la seguridad

#	Aspectos sobre protección de datos personales
1	Derecho a la protección de datos personales
2	Derecho a conocer datos contenidos en bases de datos públicos y privados
3	Derechos a conocer datos contenidos solamente en bases de datos públicos
4	Derecho a exigir confidencialidad sobre los datos
5	Derecho a impedir transmisión o divulgación de la información
6	Recolección de datos
7	Circulación de datos
8	Principio de calidad en el tratamiento de datos personales
9	Principio de seguridad en el tratamiento de datos personales

Fuente: Autor.

[59] Ibi.

El siguiente cuadro, presenta una correlación de los aspectos en protección de datos personales contemplados en las constituciones y los controles en seguridad de la información; considerando entre otros en especial la protección en accesos y uso no autorizados durante el tratamiento de los datos personales durante su ciclo de vida**.**

Cuadro 4. Protección datos personales vs. Controles en Seguridad

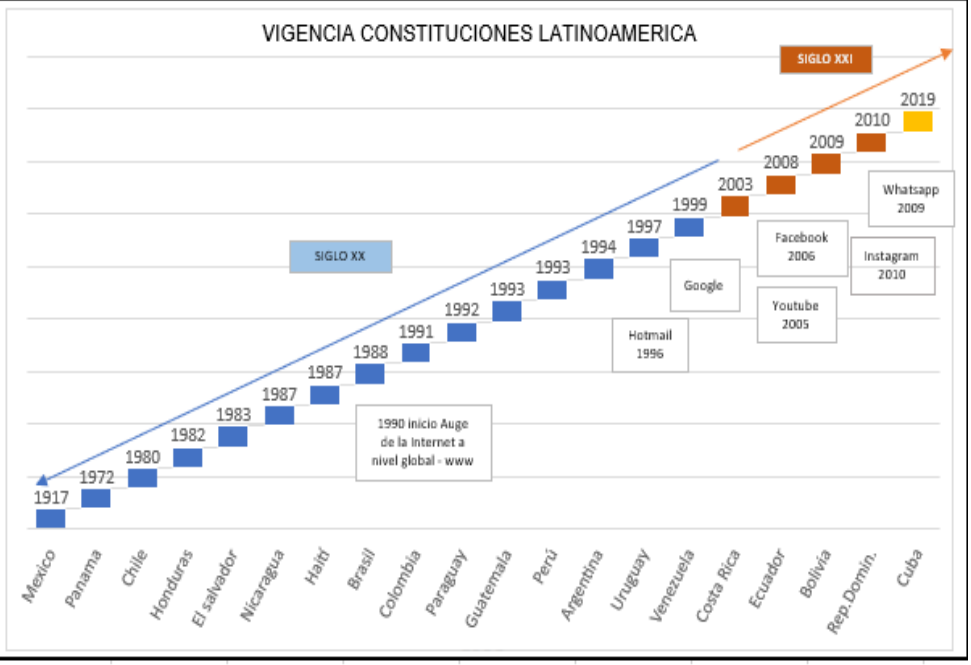
#	Aspecto en protección y privacidad de datos personales	Controles en seguridad de la información
1	Derecho a impedir transmisión o divulgación de la información	Controles en transmisión de datos, en los diferentes canales de comunicación
2	Circulación de datos	
3	Principio de seguridad en el tratamiento de datos personales	Controles procedimentales, técnicos y humanos, para evitar pérdida, adulteración, accesos o consultas no autorizadas,
4	Derecho a la protección de datos personales	
5	Recolección de datos	Controles para asegurar que los datos se recolecten de forma segura y solamente para la finalidad requerida
6	Recolección con consentimiento del titular	Procedimientos y Controles en mecanismos físicos y electrónicos para recolección de los datos
7	Recolección por disposición de autoridad competente	
8	Acción de protección de privacidad	Controles en acceso a la información
9	Derecho a exigir confidencialidad sobre los datos	
10	Principio de calidad en el tratamiento de datos personales	Controles para garantizar la integridad
11	Derecho a conocer datos contenidos en bases de datos públicos y privados	Control de acceso solo al usuario autorizado
12	Derecho a conocer datos contenidos solamente en bases de datos públicos	
13	Derecho a solicitar supresión, eliminación, destrucción o cancelación del dato	Procedimientos y Controles en el ciclo de vida del dato

Fuente: Autor.

De acuerdo con la información presentada por el portal web DW.com[60], en el siguiente cuadro se presentan las vigencias de las 20 constituciones referenciadas desde la más antigua hasta la más reciente.,

Cuadro 5. Vigencias de las Constituciones en Latinoamérica

#	Estado	Vigencia
1	Mexico	1917
2	Panama	1972
3	Chile	1980
4	Honduras	1982
5	El salvador	1983
6	Nicaragua	1987
7	Haití	1987
8	Brasil	1988
9	Colombia	1991
10	Paraguay	1992
11	Guatemala	1993
12	Perú	1993
13	Argentina	1994
14	Uruguay	1997
15	Venezuela	1999
16	Costa Rica	2003
17	Ecuador	2008
18	Bolivia	2009
19	Rep.Domin.	2010
20	Cuba	2019



Fuente: Autor adaptación de DW.com[61]

Del cuadro anterior se relaciona las siguientes consideraciones con las constituciones analizadas por el portal web DW.com[62]:

- En color azul se resaltan las del siglo pasado (XX) para un total de 15, siendo la más antigua la de la nación de México (1917) y las del siglo presente (XXI) para un total de 5, cuatro en color naranja y una en color amarillo siendo la más reciente la nación de Cuba (2019),

[60] DW. Las Constituciones de América Latina. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.dw.com/es/las-constituciones-de-am%C3%A9rica-latina/g-50480635
[61] Ibid.
[62] Ibid.

- El 75% (15) de las constituciones de Latinoamérica que encuentran vigentes pertenecen al siglo pasado

- Solo el 25 % (5) de las constituciones de Latinoamérica han sido actualizadas o entraron en vigor en el siglo actual (XXI).

- Ubicando la evolución del Internet y la masificación de las diferentes aplicaciones para el mismo en la era digital actual podemos observar que el auge de las mismas y su masificación a nivel global comenzó en el Siglo XXI, como las redes sociales de Facebook (2006), YouTube (2005), Instagram (2010) WhatsApp (2009), de acuerdo con el último informe Digital 2021 elaborado por We Are Social en colaboración con Hootsuite[63], Facebook tiene un promedio de 2740 millones usuarios, le sigue YouTube con 2291 millones y WhatsApp con 2000 millones, sumando los usuarios da un promedio alrededor de 8000 mil millones de usuarios con sus datos personales almacenados digitalmente, sin contar los demás sitios de la industria como bancos, organizaciones y en general el sector público y privado.

- Las constituciones emitidas con vigencia en el siglo pasado (XX), si bien, concibieron el amparo adecuado al tratamiento de los datos personales, la evolución de la era digital no era relevante o de impacto en los años de 1900 a 1990, con el auge de las TI en especial el Internet se fue masificando a nivel global, es decir fueron concebidas para un mundo físico y territorial, sin contemplar el desarrollo de las TI y el alto impacto de globalización que comenzarían a tener en el siglo XXI.

[63] WE ARE SOCIAL. DIGITAL REPORT 2021: EL INFORME SOBRE LAS TENDENCIAS DIGITALES, REDES SOCIALES Y MOBILE. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://wearesocial.com/es/blog/2021/01/digital-report-2021-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/

- Es de reflexión si las constituciones latinoamericanas y en especial la de Colombia se alinean a los requerimientos de las actuales y nuevas tecnologías que nos depara el futuro y si las mismas responden o dictan directrices a las exigencias en medidas y mecanismos de seguridad de la información en la protección de los datos personales de los titulares en un mundo globalizado e interconectado donde los datos personales juegan un papel importante para las diferentes actividades de la sociedad.

- El cuadro 5 presenta una evolución y vigencia de las constituciones iniciando con la de México en 1917 y su paso en el tiempo con el inicio del internet en 1993, las redes sociales entre 1996 y 2009 con la constitución más vigente de Cuba reformada en el 2009.

En el “Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respeta 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) (Texto relevante a efectos del EEE)”[64], se resaltan en el siguiente cuadro entre otras las siguientes normas relativas a la seguridad y riesgos de los datos personales:

[64] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Cuadro 6. Normas en seguridad de datos personales Reglamento UE

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
CAPÍTULO II, Principios, Artículo 5, Principios relativos al tratamiento	1. Los datos personales serán: f). Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
CAPÍTULO II, Principios, Artículo 25, Protección de datos desde el diseño y por defecto	1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. 3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente a

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal.
Sección 2, Seguridad de los datos personales, Artículo 32 Seguridad del tratamiento	1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: a) la seudonimización y el cifrado de datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. 2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. 4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.
Artículo 33	Notificación de una violación de la seguridad de los datos personales a la autoridad de control. 1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. 2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento. 3. La notificación contemplada en el apartado 1 deberá, como mínimo: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. 5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.
Artículo 34	Comunicación de una violación de la seguridad de los datos personales al interesado. 1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. 2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d). 3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. 4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Fuente: Adaptado del Reglamento UE 2016/679[65].

En la ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[66], del Gobierno de España, se resalta en el siguiente cuadro, entre otras las siguientes normas relativas a la seguridad y riesgos de los datos personales:

Cuadro 7. Normas en seguridad de los datos personales Gobierno de España

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
PREÁMBULO IV	Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación

[65] Ibid.
[66] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	digital de nuestra sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía. Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales.
Artículo 82	Derecho a la seguridad digital. Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.
Artículo 84.	Protección de los menores en Internet.
Artículo 85.	Derecho de rectificación en Internet
Artículo 86.	Derecho a la actualización de informaciones en medios de comunicación digitales.
Artículo 87	Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
Artículo 88.	Derecho a la desconexión digital en el ámbito laboral.
Artículo 89	Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
Artículo 90	Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
Artículo 91	Derechos digitales en la negociación colectiva
Artículo 92	Protección de datos de los menores en Internet
Artículo 93	Derecho al olvido en búsquedas de Internet
Artículo 94	Derecho al olvido en servicios de redes sociales y servicios equivalentes
Artículo 95	Derecho de portabilidad en servicios de redes sociales y servicios equivalentes
Artículo 96	Derecho al testamento digital

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
Disposición adicional novena	Tratamiento de datos personales en relación con la notificación de incidentes de seguridad. Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.
Disposición adicional undécima	Privacidad en las comunicaciones electrónicas

Fuente: Adaptación de la ley Orgánica 3/2018 del Gobierno de España[67]

En la Ley 19628 SOBRE PROTECCION DE LA VIDA PRIVADA MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA[68], de la república de Chile, se resaltan en el siguiente cuadro, entre otras las siguientes normas relativas a la seguridad y riesgos de los datos personales:

Cuadro 8. Normas en seguridad de los datos personales Gobierno de Chile

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
Artículo 5	El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

[67] Ibid.
[68] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
Artículo 11	El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

Fuente: Adaptación de la Ley 19628 SOBRE PROTECCION DE LA VIDA PRIVADA MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA[69], de la república de Chile[70]

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES[71], de los Estados Unidos Mexicanos, se resaltan en el siguiente cuadro entre otras, las siguientes normas relativas a la seguridad y riesgos de los datos personales:

Cuadro 9. Normas en seguridad de los datos personales Gobierno de México

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
CAPÍTULO II De los Principios de Protección de Datos Personales Artículo 19	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

[69] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

[70] Ibid.

[71] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
Artículo 20	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos

Fuente: Adaptación de la LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES[72], de los Estados Unidos Mexicanos

En la Ley PROTECCION DE LOS DATOS PERSONALES 25.326, Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales[73], del gobierno Argentina, se resalta en el siguiente cuadro entre otras las siguientes normas relativas a la seguridad y riesgos de los datos personales:

Cuadro 10. Normas en seguridad Gobierno de Argentina

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
ARTICULO 9° (Seguridad de los datos).	1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

[72] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[73] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.
ARTICULO 12	1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.
ARTICULO 21 (Registro de archivos de datos. Inscripción).	2. El registro de archivos de datos debe comprender como mínimo la siguiente información: g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
ARTICULO 29 (Órgano de Control).	1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: d) Controlar la observancia de las normas sobre integridad y Seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

Fuente: Adaptación de la Ley PROTECCION DE LOS DATOS PERSONALES 25.326 del gobierno de Argentina[74]

[74] Ibid.

En la LEY DE PROTECCIÓN DE DATOS PERSONALES N.º 29733[75], del Gobierno de Perú, se resaltan en el siguiente cuadro, entre otras las siguientes normas relativas a la seguridad y riesgos de los datos personales:

Cuadro 11. Normas en seguridad datos personales Gobierno de Perú

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
TÍTULO PRELIMINAR DISPOSICIONES GENERALES Artículo 2. Definiciones	12. Nivel suficiente de protección para los datos personales. Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.
Artículo 9. Principio de seguridad	El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.
Artículo 11. Principio de nivel de protección adecuado	Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia.
Artículo 16. Seguridad del tratamiento de datos personales	Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.

[75] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.
Artículo 17. Confidencialidad de datos personales	El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.
TÍTULO III DERECHOS DEL TITULAR DE DATOS PERSONALES Artículo 18	…. Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables. ….. Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado de tratamiento de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias, según ley, las que deben informar que se encuentra en trámite cualquiera de los mencionados procesos.
Artículo 35. Confidencialidad	El personal de la Autoridad Nacional de Protección de Datos Personales está sujeto a la obligación de guardar confidencialidad sobre los datos personales que conozca con motivo de sus funciones. Esta obligación subsiste aun después de finalizada toda relación con dicha autoridad nacional, bajo responsabilidad.
DISPOSICIONES COMPLEMENTARIAS FINALES Segunda.	La Autoridad Nacional de Protección de Datos Personales elabora la directiva de seguridad de la información administrada por los bancos de datos personales en un plazo no mayor de ciento veinte días

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
Directiva de seguridad	hábiles, contado a partir del día siguiente de la publicación de la presente Ley. En tanto se apruebe y rija la referida directiva, se mantienen vigentes las disposiciones sectoriales sobre la materia.

Fuente: Adaptación de la LEY DE PROTECCIÓN DE DATOS PERSONALES N.º 29733[76], del Gobierno de Perú[77]

En la LEY ESTATUTARIA 1581 DE 2012 por la cual se dictan disposiciones generales para la protección de datos personales[78], del gobierno de Colombia, se resaltan en el siguiente cuadro, entre otras las siguientes normas relativas a la seguridad y riesgos de los datos personales:

Cuadro 12. Normas en seguridad datos personales Gobierno de Colombia

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
TÍTULO II PRINCIPIOS RECTORES Artículo 4°.	f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

[76] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf
[77] Ibid.
[78] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.
Artículo 11.	Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.
TÍTULO VI DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO	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: d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
Artículo 18.	Deberes de los Encargados del Tratamiento Los Encargados 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: b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley; h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal; k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
TÍTULO VIII TRANSFERENCIA DE DATOS A TERCEROS PAÍSES Artículo 26.	Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

Fuente: Adaptación de la LEY ESTATUTARIA 1581 DE 2012 del gobierno de Colombia[79]

DECRETO 1377 DE 2013[80] Por el cual se reglamenta parcialmente la Ley 1581 de 2012**,** del gobierno de Colombia, se resaltan en el siguiente cuadro entre otras, las siguientes normas relativas a la seguridad y riesgos de los datos personales:

[79] Ibid.

[80] COLOMBIA, MINISTERIO DE COMERCIO, INDUSTRIA Y COMERCIO, Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

Cuadro 13. Normas seguridad datos personales Gobierno de Colombia

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
Artículo 7°. Modo de obtener la autorización.	….. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización……
Artículo 8°. Prueba de la autorización.	Los responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.
Artículo 19. Medidas de seguridad.	La Superintendencia de Industria y Comercio impartirá las instrucciones relacionadas con las medidas de seguridad en el Tratamiento de datos personales.
Artículo 22. Del derecho de actualización, rectificación y supresión.	En desarrollo del principio de veracidad o calidad, en el tratamiento de los datos personales deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes……
CAPÍTULO VI Responsabilidad demostrada frente al tratamiento de datos personales Artículo 26. 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 este decreto, en una manera que sea proporcional a lo siguiente: 4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas.
Artículo 27. Políticas internas efectivas	En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con

Artículo	Aspecto que se resalta relativo a la seguridad de los datos personales
	las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar: La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto.

Fuente: Adaptación del decreto 1377 DE 2013[81] del gobierno de Colombia

Contrastando la normativa de las medidas de seguridad de la información identificadas y más relevantes para la protección y privacidad de los datos personales dispuestas en el reglamento del parlamento de la Unión Europea y las leyes de los gobiernos de España, Chile, México, Argentina, Perú y Colombia con respecto a los controles de seguridad para cumplimiento de requisitos legales para la protección de los datos y privacidad de la información personal, los cuadros 14, 15, 16, 17, 18, 19 y 20, presentan una agrupación con respecto a: 1. La integridad y confidencialidad, 2. Medidas técnicas y físicas, 3. Medidas en gestión de los riesgos, 4. Medidas para la gestión de los incidentes de seguridad, 5. Medidas en transmisión y transferencias, 6. Medidas en el Internet y medios digitales y 7. Almacenamiento y conservación de los datos personales; que identifican un panorama de como las disposiciones de la Comisión Europea y las leyes de los Gobiernos en mención dan a las medidas en seguridad de la información para salvaguardar los datos personales:

[81] Ibid.

Cuadro 14. Medidas de seguridad en integridad y confidencialidad

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
Medidas en integridad y confidencialidad	Seguridad en protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).	1						
	Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	1						
	El personal de la Autoridad Nacional de Protección de Datos Personales está sujeto a la obligación de guardar confidencialidad sobre los datos personales que conozca con motivo de sus funciones						1	
	El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.						1	
	Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento							1
		2	**0**	**0**	**0**	**0**	**2**	**1**

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[82] , y los gobiernos de España[83] , Chile[84] , México[85] , Argentina[86] , Perú[87] y Colombia[88].

Cuadro 15. Medidas de controles de seguridad técnicas y físicas

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
controles de seguridad técnicas y físicas	Establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.				1			
	Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.					1		
	Adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado					1		
	Para fines del tratamiento de datos personales, el titular del banco de datos						1	

[82] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf
[83] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3
[84] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599
[85] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares
[86] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto
[87] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf
[88] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
	personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.							
	El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.						1	
	Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.						1	
	Principio de seguridad: La información sujeta Tratamiento por el responsable del ratamiento o Encargado del Tratamiento a ue se efiere la presente ley, se deberá manejar con as medidas técnicas, humanas y dministrativas que sean necesarias para torgar seguridad a los registros evitando su dulteración, pérdida, consulta, uso o acceso o autorizado o fraudulento;							1
	Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;							1
	Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;							1
		0	**0**	**0**	**1**	**2**	**3**	**3**

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[89] , y los gobiernos de España[90] , Chile[91] , México[92] , Argentina[93] , Perú[94] y Colombia[95].

Cuadro 16. Medidas de controles de seguridad en gestión de riesgos

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
Medidas para la gestión de los riesgos de os datos personales	Evaluar la adecuación del nivel de seguridad los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.	1						
	Aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.	1						
	Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias				1			

[89] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf
[90] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3
[91] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599
[92] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares
[93] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto
[94] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf
[95] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
	para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.							
	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. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.							1
	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. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.							1
		2	0	0	1	0	0	2

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[96] , y los gobiernos de España[97] , Chile[98] , México[99] , Argentina[100] , Perú[101] y Colombia[102].

[96] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[97] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

[98] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

[99] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[100] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

[101] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

[102] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Cuadro 17. Medidas de controles de seguridad en incidentes de seguridad

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia	
Medidas para gestionar los incidentes de seguridad en datos personales	Notificación de una violación de la seguridad de los datos personales a la autoridad de control y al interesado	1							
	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos				1				
	Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.							1	
	Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares							1	
		1	0	0	1	0	0	2	

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[103] , y los gobiernos de España[104] , Chile[105] , México[106] , Argentina[107] , Perú[108] y Colombia[109].

[103] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[104] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

[105] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

[106] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[107] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

[108] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

[109] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Cuadro 18. Medidas de controles de transmisiones y transferencias

Requisitos en Seguridad de la Información	Aspectos Normativo-relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
Medidas en seguridad para transmisiones y transferencias de datos personales	Derecho a la seguridad digital. Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.		1					
	Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.					1		
	Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos							1
	Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia.						1	
	Establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes			1				
		0	1	1	0	1	1	1

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[110] , y los gobiernos de España[111] , Chile[112] , México[113] , Argentina[114] , Perú[115] y Colombia[116].

Cuadro 19. Medidas de controles en Internet y medios digitales

[110] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[111] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

[112] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

[113] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[114] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

[115] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

[116] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
Medidas en el Internet y medios digitales	Protección de los menores en Internet.		1					
	Derecho de rectificación en Internet		1					
	Derecho a la actualización de informaciones en medios de comunicación digitales.		1					
	Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.		1					
	Derecho a la desconexión digital en el ámbito laboral.		1					
	Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.		1					
	Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.		1					
	Derechos digitales en la negociación colectiva		1					
	Protección de datos de los menores en Internet		1					
	Derecho al olvido en búsquedas de Internet		1					
	Derecho al olvido en servicios de redes sociales y servicios equivalentes		1					
	Derecho de portabilidad en servicios de redes sociales y servicios equivalentes		1					
	Derecho al testamento digital		1					
	Privacidad en las comunicaciones electrónicas		1					
	Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser						1	

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
	fácilmente accesibles e identificables							
	Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley							1
		0	13	0	0	0	1	1

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[117] , y los gobiernos de España[118] , Chile[119] , México[120] , Argentina[121] , Perú[122] y Colombia[123].

[117] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[118] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

[119] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

[120] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[121] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

[122] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

[123] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Cuadro 20. Mmedidas de controles en almacenamiento y conservación

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
Medidas de protección en almacenamiento y conservación de bases de datos personales	El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.			1				
	Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales						1	
	La Autoridad Nacional de Protección de Datos Personales elabora la directiva de seguridad de la información administrada por los bancos de datos personales						1	
	En desarrollo del principio de veracidad o calidad, en el tratamiento de los datos personales deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes……							1
	Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no							1

Requisitos en Seguridad de la Información	Aspectos Normativos relevantes relacionados con medidas de seguridad	Unión Europea	España	Chile	México	Argentina	Perú	Colombia
	autorizado o fraudulento							
	Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.							1
		0	0	1	0	0	2	3

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[124] , y los gobiernos de España[125] , Chile[126] , México[127] , Argentina[128] , Perú[129] y Colombia[130].

La siguiente ilustración presenta un resumen compilado del análisis de los aspectos en disposiciones de sus artículos en medidas de seguridad de la información contrastadas con las disposiciones de ley del parlamento Europeo y las leyes en protección de datos persónales de los gobiernos estudiadas, sin embargo es de anotar que los gobiernos emiten las leyes en concordancia a sus constituciones políticas, cumplimiento de tratados internacionales y medidas internas entre otros

[124] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[125] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

[126] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

[127] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

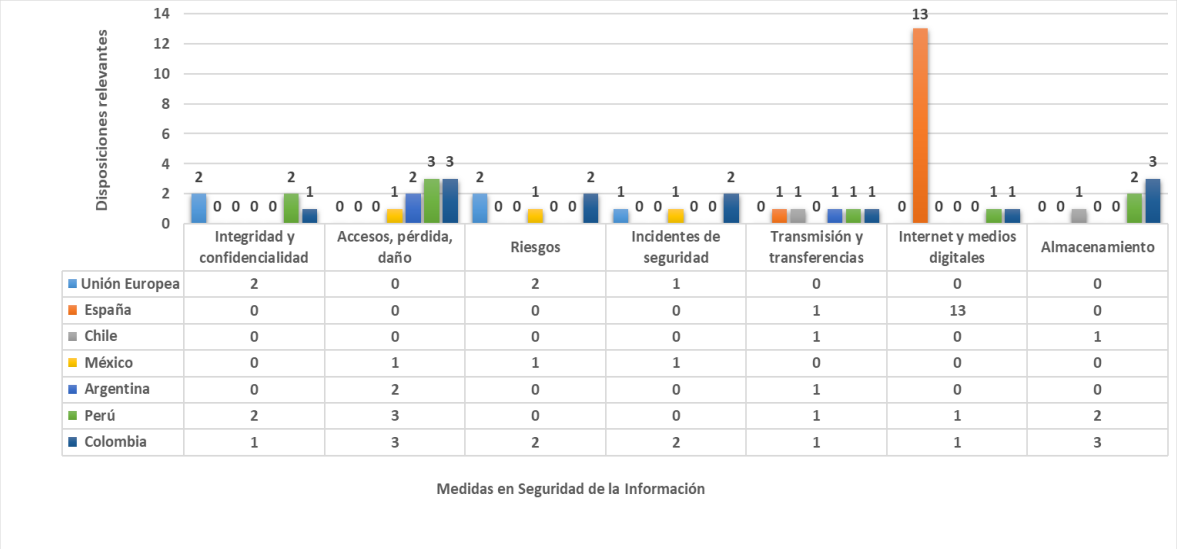
[128] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

[129] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

[130] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

ámbitos, con el fin de regular su cumplimiento, así mismo asignan o delegan las responsabilidades de su cumplimiento y supervisión a las entidades oficiales internas de cada gobierno quienes a su vez también dictan disposiciones como complemento a la ley, igualmente a su vez también emiten decretos para reglamentar parcialmente las leyes emitidas y facilitar su implementación y cumplimiento.

Ilustración 3. Medidas de seguridad en protección de datos personales



	Integridad y confidencialidad	Accesos, pérdida, daño	Riesgos	Incidentes de seguridad	Transmisión y transferencias	Internet y medios digitales	Almacenamiento
Unión Europea	2	0	2	1	0	0	0
España	0	0	0	0	1	13	0
Chile	0	0	0	0	1	0	1
México	0	1	1	1	0	0	0
Argentina	0	2	0	0	1	0	0
Perú	2	3	0	0	1	1	2
Colombia	1	3	2	2	1	1	3

Fuente: Adaptación de controles de seguridad y disposiciones en protección de datos personales la UE[131] , y los gobiernos de España[132] , Chile[133] , México[134] , Argentina[135] , Perú[136] y Colombia[137].

[131] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[132] GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

[133] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

[134] GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[135] GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

[136] GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

[137] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en

De la Ilustración anterior se relacionan las siguientes apreciaciones y consideraciones:

- Para el ámbito de medidas en seguridad en el aspecto de la integridad y confidencialidad, 3 de las 7 legislaciones, la Unión Europea, Perú y Colombia la señalan en los artículos de sus disposiciones o leyes o al menos es de más relevancia para ellas; El principio de confidencialidad integridad de los datos personales son el factor importante y base para el cumplimiento normativo en la protección y privacidad de los datos personales y se garanticen medidas de seguridad adecuadas para el tratamiento no autorizado o ilícito, así mismo para que los responsables empleen medidas para garantizar que los datos no puedan ser alterados por personas no autorizadas.

- Para el ámbito de medidas en seguridad en el aspecto de accesos, pérdida y daño de datos personales, 4 de las 7 legislaciones, Argentina, Perú y Colombia la señalan en los artículos de sus disposiciones o leyes o al menos es de más relevancia para ellas y se resalta en su jurisprudencia.

- Para el ámbito de medidas en seguridad para los riesgos en datos personales, 3 de 7 de las legislaciones, la Unión Europea, México y Colombia la señalan en los artículos de sus disposiciones o leyes o al menos es de más relevancia para ellas, resaltando la gestión de los riesgos en las medidas de protección y privacidad de los datos.

- Para el ámbito de medidas en seguridad en el aspecto de transmisión y transferencias de datos personales, 5 de 7 legislaciones, España, Chile,

línea]Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Argentina, Perú y Colombia son más relevantes y explícitos en estas disposiciones.

- Para el ámbito de medidas en seguridad en el aspecto de incidentes de seguridad en datos personales, 3 de 4 legislaciones, la Unión Europea, México y Colombia la señalan en los artículos de sus disposiciones o leyes o al menos es de más relevancia para ellas, destacándose la obligación de la gestión de los incidentes de seguridad de la información en protección de datos personales como un requisito de cumplimiento en sus legislaciones.

- Para el ámbito de medidas en seguridad en el aspecto de Internet y medios Digitales, 3 de 7 legislaciones, entre las que se destaca las disposiciones emitidas por España resaltando los derechos y la protección de los datos personales, es de anotar que esta ley orgánica fue emitida en el año de 2018 dando cumplimiento al reglamento (UE) 2016/679 del parlamento europeo del cual hace parte, la disposición el uso actual de la tecnología y la importancia de legislar en estos aspectos para proteger la privacidad de las personas. También se resalta que Colombia y Perú también incorporan este aspecto en sus legislaciones.

- Para el ámbito de medidas en seguridad en el aspecto de almacenamiento y conservación de los datos personales tratados por las entidades, 3 de las 7 legislaciones, se destaca que Colombia, Perú y Chile hacen referencia en este aspecto, es de destacar que este ámbito es de importancia desde el aspecto de asegurar que las autorizaciones de los titulares deben estar debidamente almacenadas, custodiadas y disponibles para consultas y requerimientos de las autoridades ya que la autorización es la entrada para el tratamiento y recolección de datos personales de los titulares.

Como conclusión contrastando las legislaciones en aspectos de medidas de seguridad que se deben implementar para la protección de la privacidad de los datos

personales de las personas, aún las legislaciones estudiadas en el presente documento solo cubren un total del 43% quedando un faltante de 57% por cubrir en sus disposiciones y recomendaciones de relevancia que permitan a las entidades obligadas a cumplirlas definir y estructurar medidas claras y concisas en aspectos de seguridad de la información, dejando a las autoridades internas delegadas en protección de datos el cumplimiento e igualmente a las entidades definir de acuerdo a su libre albedrío la implementación de las medidas de seguridad ya sean técnicas, normativas o de procedimientos en el cumplimiento de la legislación.

Ahora bien, para la legislación colombiana en protección de datos personales se encuentran libros, monografías, que tratan el cumplimiento a la ley 1581 de 2012 que deben cumplir las entidades públicas o privadas, pero lo hacen desde del ámbito jurídico, pero no en medidas técnicas con enfoque a la seguridad de la información o informática.

En resumen, se referencia que en el ámbito colombiano y en general los documentos relacionados con el habeas data postulan el debe en seguridad, pero no hay un instrumento que integre la observancia de la ley con las medidas y controles en seguridad de la información como referencia práctica a las partes interesadas de las entidades para su análisis, evaluación, diagnostico e implementar medidas de protección a datos personales a los que dan tratamiento.

5.2 DESARROLLO OBJETIVO 2.

Con referencia al objetivo 2. *“Estimar las causas que originaron sanciones por la Superintendencia de Industria y Comercio (SIC) debido a la mala implementación o ausencia de controles de seguridad para la protección de datos personales durante los últimos tres años”*. Se realiza una evaluación de causas a los controles en seguridad tomando como referencia y fuente de información las entidades de los últimos 3 años a julio de 2021 a las que la SIC les emitió disposiciones sancionatorias por incumplimiento a la ley 1581 de 2012 para la protección de datos personales.

De acuerdo con los registros de decisiones administrativas por la SIC en su portal web durante los últimos 3 años al mes de diciembre de 2021 se han presentado 186 resoluciones sancionatorias a entidades, relacionadas con la protección de datos personales, por lo que resulta relevante estudiar y evaluar cuales son las vulnerabilidades técnicas y procedimentales que conllevaron al comprometimiento de la seguridad de los datos personales de los titulares y proponer diferentes mecanismos y lineamientos en seguridad de la información que deberían mejorar y tener en cuenta las organizaciones para dar cumplimiento a la ley 1581 de 2012 y a las instrucciones y requerimientos que emite la SIC y obviar sanciones pecuniarias, legales y a una suspensión o cierre de sus actividades.

Así mismo un estudio realizado en 2019 por la Policía Nacional y la Cámara Colombiana de Informática y Telecomunicaciones[138] reveló que la violación de datos personales es el segundo ciberdelito más cometido en Colombia, superado únicamente por el hurto a través de medios informáticos", este estudio permite razonar que las entidades están expuestas a este tipo de delitos y como resultado las acciones judiciales y sanciones pecuniarias a las que están expuestas, seguidamente se relacionan las vulnerabilidades y los riesgos que se pueden materializar por falta de controles de seguridad para la protección de los datos personales de la entidad.

Entre las vulnerabilidades y riesgos en seguridad a los que están expuestas las entidades se referencian entre otras:

- Recolección de datos personales por medios electrónicos y físicos sin el aviso de privacidad.

[138] UNIVERSIDAD SERGIO ARBOLEDA. Protección De Datos Personales: Qué es y cómo mitigar riesgos [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: "https://www.usergioarboleda.edu.co/noticias/proteccion-de-datos-personales-que-es-y-como-mitigar-riesgos/"

- No contar con un procedimiento y aplicativos que permita registrar y llevar la trazabilidad de las solicitudes de los titulares
- No contar con medidas de seguridad para almacenamiento físico y electrónico de las bases de datos de los titulares.
- No contar mecanismo de IDS/IPS para la prevención y detección de intrusos, así como fuga de datos.
- Acceso no autorizado a las bases de datos personales.
- Exposición de datos no autorizados en sitios web y redes sociales.
- Sanciones pecuniarias.
- Afectaciones reputacionales.
- Demandas judiciales por daños y perjuicios.
- Indisponibilidad de las de datos.
- Pérdida o destrucción de las de datos.
- Modificación no autorizada de datos.
- Transmisión de datos personales si las medidas de seguridad.
- Uso indebido de datos sensibles (de menores de edad, biométricos)

En el Anexo A presenta un cuadro de relación con un total de 60 entidades con resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2019[139], el título sancionatorio, la disposición o normativa más relevante que no cumplió y que se encuentran definidas en los tipos y detalle de reclamo a la ley 1581 de 2012 definidas en el Manual de usuario del Registro Nacional de Bases de Datos – RNDB[140] de la SIC que presentaron los

[139] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

[140] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

titulares y la correspondencia con el control o medida de seguridad de la información con la norma ISO/IEC 27001:2013.

De las 60 entidades sancionadas por la SIC para el año 2019 relacionadas, el siguiente cuadro presenta un resumen en cantidades y porcentajes por cantidad, tipo y detalle de los reclamos a la ley 1581 de 2012 más relevante por parte de los titulares.

Cuadro 21. Entidades sancionas por tipo y detalle de reclamos 2019

Causa origen de sanción SIC	Cantidad	%
2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	18	30%
13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	9	15%
4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	8	13%
14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	5	8%
21 CONTRA EL RESPONSABLE - RESPECTO DE LA RECOLECCIÓN DE INFORMACIÓN	3	5%
8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	3	5%
1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	2	3%
15 CONTRA EL RESPONSABLE - RESPECTO DEL AVISO DE PRIVACIDAD	2	3%
16 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN SENSIBLE	2	3%
17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES	2	3%
3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	2	3%
24 CONTRA EL ENCARGADO - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	1	2%
25 CONTRA EL ENCARGADO - RESPECTO DE LA RECTIFICACIÓN O SUPRESIÓN DE LA INFORMACIÓN	1	2%
9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	1	2%
20 CONTRA EL RESPONSABLE - RESPECTO DE LA LIMITACIÓN TEMPORAL AL TRATAMIENTO	1	2%
Total, general	**60**	**100%**

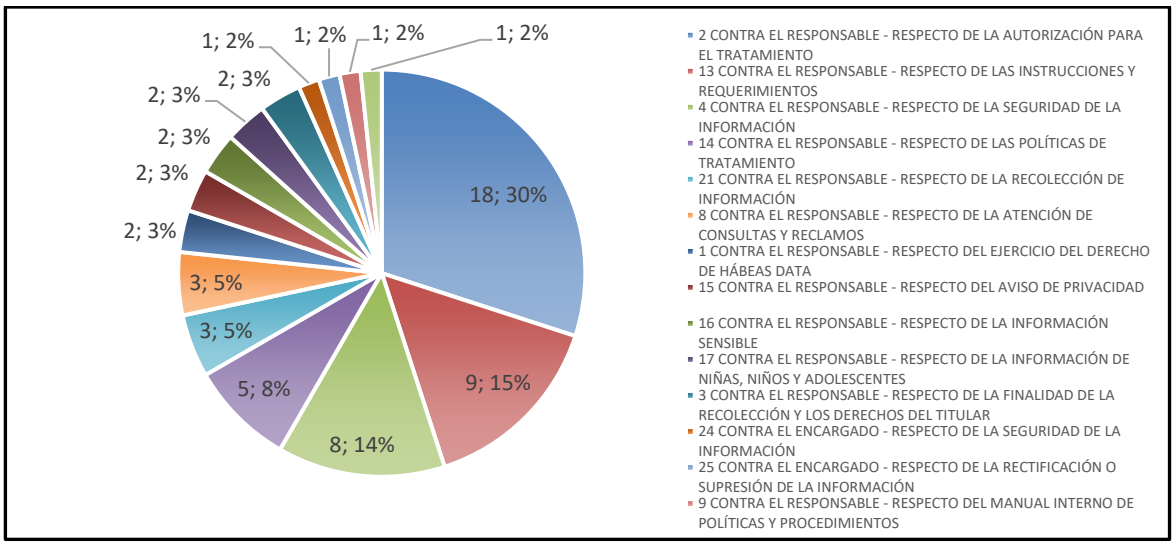
Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[141] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2019.[142]

[141] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[142] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

La siguiente Ilustración presenta la distribución circular en porcentajes y cantidades de las entidades sancionas por la sic en 2019[143]

Ilustración 4. Porcentajes entidades sancionas por el SIC año 2019



Fuente: Adaptación de resoluciones decisiones administrativas SIC 2019[144]

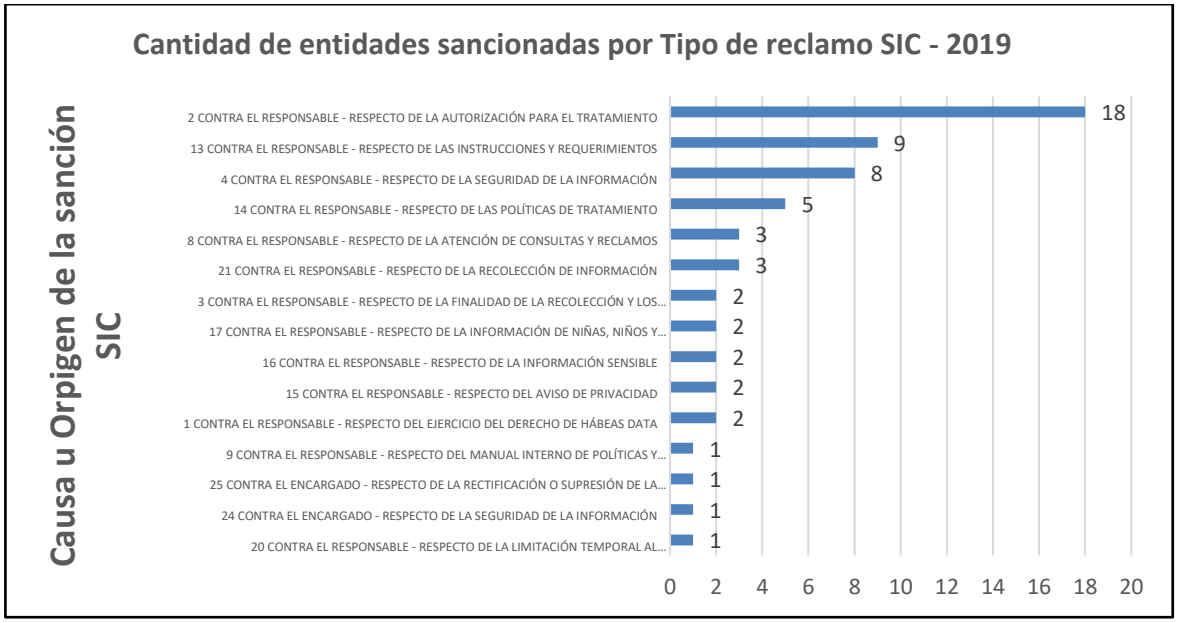
En la ilustración anterior se referencia que 18 entidades fueron sancionadas siendo el origen más relevante tipo de reclamo más relevante: *"2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO"* presentando el porcentaje más alto con el 30 % de entidades sancionadas, 9 entidades con el reclamo *"13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS"* con un porcentaje del 15 %, 8 entidades con el reclamo *"4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN"* con un porcentaje de 13 %, 5 entidades con el reclamo *"14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO"* con un porcentaje del 8 %, 3 entidades con el reclamo *"14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO"* con un porcentaje de 5 %, 3 entidades con el reclamo "*8 CONTRA*

[143] Ibid.
[144] Ibid.

EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS" con un porcentaje de 5 %, sumando 46 entidades sancionadas en un porcentaje del 76 % y las 14 entidades demás restantes con un porcentaje del 14%.

La siguiente ilustración presenta en barras apiladas las entidades sancionadas en el año 2019 por la SIC[145], desde el reclamo top de los titulares con más cantidades, hasta el menor comparados entre sí, siendo el de más cantidades el tipo de reclamo más relevante: *"2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO".*

Ilustración 5. Entidades sancionadas SIC 2019 por reclamos titulares



Fuente: Adaptación de decisiones administrativas SIC 2019[146]

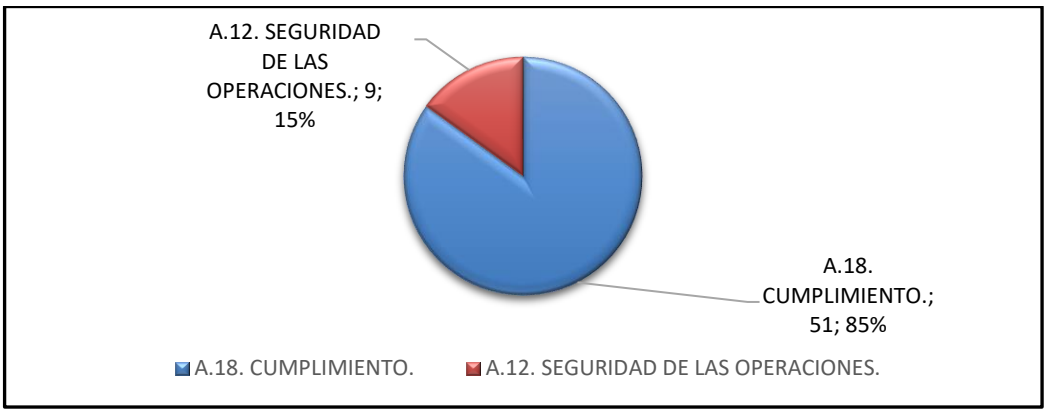
La ilustración anterior presenta la escala de mayor a menor por tipos de reclamos de entidades sancionadas por la SIC para el año 2019.

Con respecto a la correspondencia con el control o medida de seguridad de la información con la norma ISO/IEC 27001:2013, la siguiente ilustración presenta la

[145] Ibid.
[146] Ibid.

relación de las ausencias o debilidades en medidas y controles en seguridad de la información que las entidades sancionadas en el año 2019 debieron haber implementado o mejorar en sus Sistemas de Seguridad de la Información si lo tenían o dado el caso para las entidades que no lo tenían haberlos definido en sus políticas de seguridad de la información, como lo define la SIC en sus instrucciones y requerimientos para el cumplimiento de la ley 1581 de 2012, presentadas en la siguiente ilustración :

Ilustración 6. Medidas ausentes o débiles entidades sancionadas SIC 2019



Fuente: Autor.

Se referencia en la ilustración anterior 51 entidades que el 85 % de las causas u orígenes de sanciones a la entidad fue por no implementar o fortalecer medidas en seguridad de la información referenciadas en el Anexo de “A” del dominio A.18 cumplimiento de la norma ISO/IEC 27001:2013, y 9 entidades el 9 % con respecto al dominio A.12 en controles de Seguridad en las Operaciones relacionadas con medidas técnicas para la protección de los datos personales.

En lo referente para el año 2020, en el Anexo B se presenta un cuadro con un total de entidades con resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC[147], el título sancionatorio, la disposición o

[147] Ibid.

normativa más relevante que no cumplió y que se encuentran definidas en los tipos y detalle de reclamo a la ley 1581 de 2012 definidas en el Manual de usuario del Registro Nacional de Bases de Datos – RNDB[148] de la SIC que presentaron los titulares y la correspondencia con el control o medida de seguridad de la información con la norma ISO/IEC 27001:2013.

Resumiendo, de las 48 entidades sancionadas por la SIC para el año 2020, el siguiente cuadro presenta un resumen en cantidades y porcentajes por cantidad, tipo y detalle de los reclamos a la ley 1581 de 2012 más relevante por parte de los titulares.

Cuadro 22. Entidades sancionas por tipo y detalle de reclamos 2020

Causa origen de sanción SIC	Cantidad	%
2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	17	35%
8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	8	17%
4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	7	15%
1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	6	13%
13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	5	10%
3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	2	4%
23 CONTRA EL ENCARGADO - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	1	2%
17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES	1	2%
9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	1	2%
Total, general	48	100%

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[149] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2020.[150]

[148] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[149] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

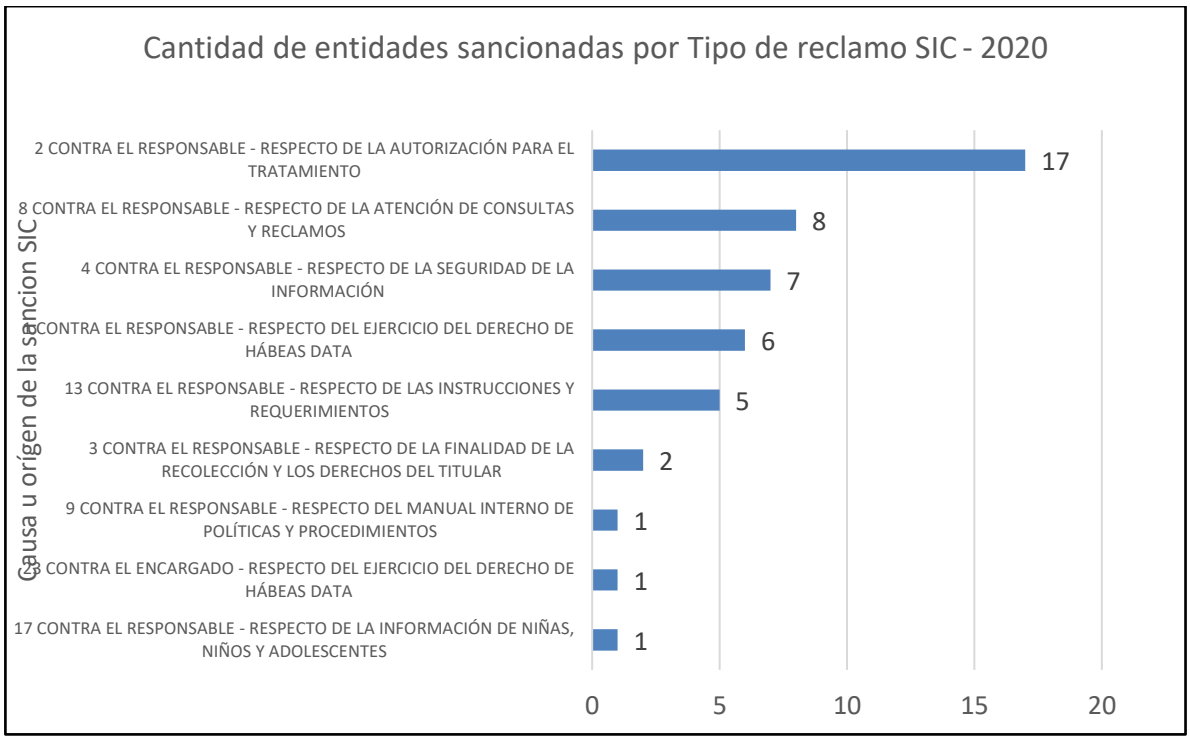
[150] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Del cuadro anterior se referencia que 17 entidades fueron sancionadas siendo el origen más relevante tipo de reclamo *"2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO"* presentando el porcentaje más alto con el 35% de entidades sancionadas, 8 entidades con el reclamo *8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS"* con un porcentaje del 17 %, 7 entidades con el reclamo "*4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN"* con un porcentaje de 13 %, 5 entidades con el reclamo *"1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA"* con un porcentaje del 10 %, 2 entidades con el reclamo *"23 CONTRA EL ENCARGADO - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA"* con un porcentaje de 4 %, 3 entidades con el reclamo "*8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS"* con un porcentaje de 5 %, sumando 45 entidades sancionadas en un porcentaje del 94% y las 3 entidades demás restantes con un porcentaje del 6%.

La siguiente ilustración presenta en barras apiladas las entidades sancionadas por la SIC en el año 2020[151], desde el reclamo top de los titulares con más cantidades, hasta el menor comparados entre sí, siendo el de más cantidades el tipo de reclamo más relevante: *"2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO".*

[151] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Ilustración 7. Entidades Sancionadas por la SIC en el año 2020



Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[152] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2020.[153]

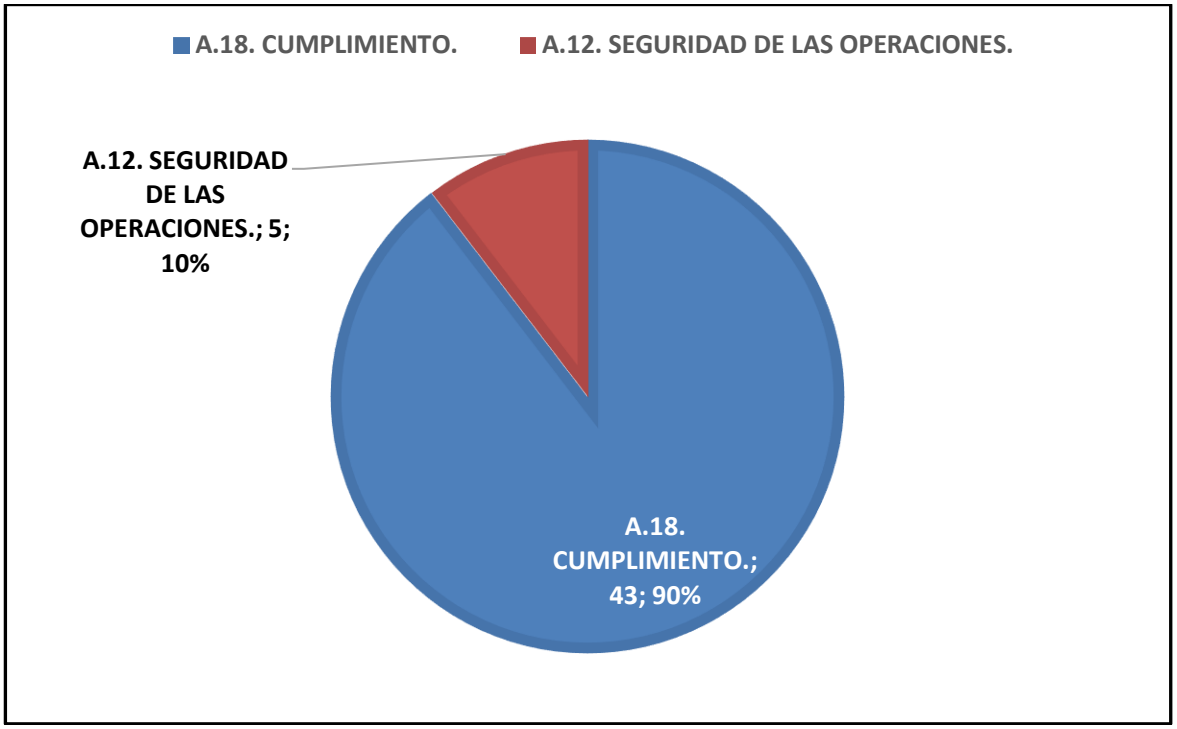
Con respecto a la correspondencia con el control o medida de seguridad de la información con la norma ISO/IEC 27001:2013, la siguiente ilustración presenta la relación de las ausencias o debilidades en medidas y controles en seguridad de la información que las entidades sancionadas en el año 2020 debieron haber implementado o mejorar en sus Sistemas de Seguridad de la Información si lo tenían o dado el caso para las entidades que no lo tenían haberlos definido en sus políticas de seguridad de la información, como lo define la SIC en sus instrucciones y

[152] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[153] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

requerimientos para el cumplimiento de la ley 1581 de 2012, presentadas en la siguiente ilustración:

Ilustración 8. Medidas ausentes entidades sancionadas SIC 2020



Fuente: Autor

Como se puede observar en la ilustración anterior de las 43 entidades, el 90% de las causas u orígenes de sanciones fue por no implementar o fortalecer medidas en seguridad de la información referenciadas en el Anexo de “A” del dominio A.18 cumplimiento de la norma ISO/IEC 27001:2013, y 5 entidades el 10 % con respecto al dominio A.12 en controles de Seguridad en las Operaciones relacionadas con medidas técnicas para la protección de los datos personales.

En lo referente para el año 2021, en el Anexo C se presenta un cuadro con un total de 78 entidades con resolución sancionatoria emitida por la delegatura para la

protección de datos personales de la SIC[154], el título sancionatorio, la disposición o normativa más relevante que no cumplió y que se encuentran definidas en los tipos y detalle de reclamo a la ley 1581 de 2012 definidas en el Manual de usuario del Registro Nacional de Bases de Datos – RNDB[155] de la SIC que presentaron los titulares y la correspondencia con el control o medida de seguridad de la información con la norma ISO/IEC 27001:2013.

En el siguiente cuadro se presenta un resumen en cantidades y porcentajes por cantidad, tipo y detalle de los reclamos a la ley 1581 de 2012 más relevante por parte de los titulares de las 78 entidades sancionadas por la SIC para el año 2021[156].

Cuadro 23. Entidades sancionas por tipo y detalle de reclamos 2021

Causa origen de sanción SIC	Cantidad	%
13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	18	**23%**
2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	16	**21%**
9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	15	**19%**
1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	8	**10%**
14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	4	**5%**
3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	4	**5%**
4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	4	**5%**
8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	2	**3%**
10 CONTRA EL RESPONSABLE - RESPECTO DE LA INSCRIPCIÓN DE LA LEYENDA	1	**1%**
11 CONTRA EL RESPONSABLE - RESPECTO DEL DEBER DE INFORMAR A LOS TITULARES COMO SE ESTÁ UTILIZANDO SU INFORMACIÓN	1	**1%**
16 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN SENSIBLE	1	**1%**

[154] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sanciones-proteccion-datos-personales-2021
[155] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manual de Usuario del Registro Nacional de Bases de Datos- RNBD. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Manual-de-Usuario-5-RNBD-01032017.pdf
[156] Ibid.

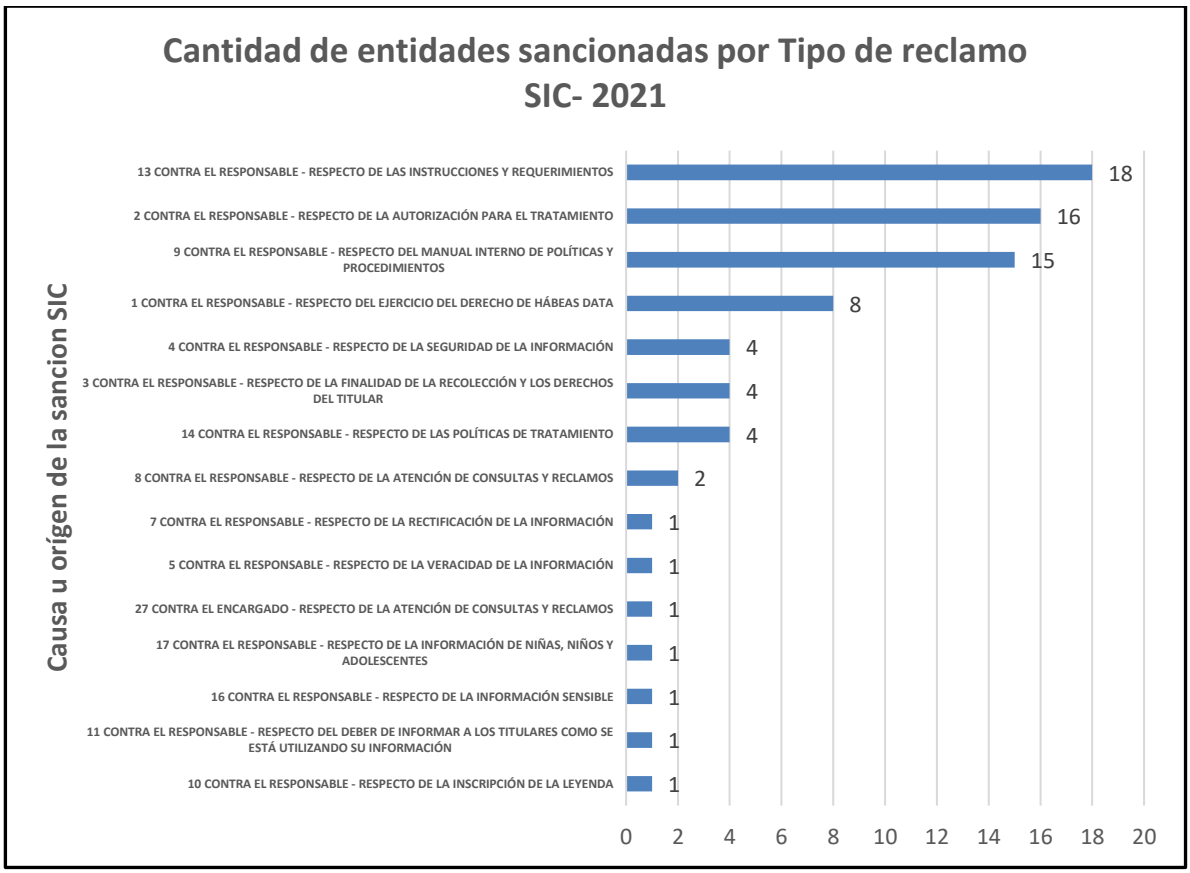
Causa origen de sanción SIC	Cantidad	%
17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES	1	**1%**
27 CONTRA EL ENCARGADO - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	1	**1%**
5 CONTRA EL RESPONSABLE - RESPECTO DE LA VERACIDAD DE LA INFORMACIÓN	1	**1%**
7 CONTRA EL RESPONSABLE - RESPECTO DE LA RECTIFICACIÓN DE LA INFORMACIÓN	1	**1%**
Total, general	**78**	**100%**

Fuente: Adaptación de las entidades sancionadas por la SIC - 2021[157]

Del cuadro anterior en la siguiente ilustración se presenta la relación de entidades y porcentajes, se estima que 18 entidades fueron sancionadas siendo el origen más relevante tipo de reclamo *"13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS"* presentando el porcentaje más alto con el 23% de entidades sancionadas, 16 entidades con el reclamo "*2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO"* con un porcentaje del 21%, 15 entidades con el reclamo "*9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS"* con un porcentaje de 19%, 8 entidades con el reclamo *"1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA"* con un porcentaje del 10%, 4 entidades con el reclamo *"3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR"* con un porcentaje del 5%, 4 entidades con el reclamo *"4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN"* con un porcentaje de 5 %, 2 entidades con el reclamo "*8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS"* con un porcentaje de 3%, sumando 71 entidades sancionadas en un porcentaje del 91% y las 7 entidades demás restantes con un porcentaje del 9%.

[157] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Ilustración 9. Entidades Sancionadas SIC - 2021



Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[158] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2021.[159]

Con respecto a la correspondencia con el control o medida de seguridad de la información con la norma ISO/IEC 27001:2013, el siguiente cuadro presenta la relación de las ausencias o debilidades en medidas y controles en seguridad de la información que las entidades sancionadas en el año 2020 debieron haber implementado o mejorar en sus Sistemas de Seguridad de la Información si lo tenían

[158] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[159] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

o dado el caso para las entidades que no lo tenían haberlos definido en sus políticas de seguridad de la información, como lo define la SIC en sus instrucciones y requerimientos para el cumplimiento de la ley 1581 de 2012, presentadas en el siguiente cuadro:

Cuadro 24. Medidas ausentes o débiles entidades sancionadas 2020

Control o medida de seguridad norma ISO/IEC 27001:2013	Cantidad	%
A.18. CUMPLIMIENTO.	76	**97%**
A.12. SEGURIDAD DE LAS OPERACIONES.	2	**3%**
Total, general	**78**	**100%**

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[160] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2021.[161]

Como se puede observar en el cuadro anterior, de 76 entidades el 97% de las causas u orígenes de sanciones a la entidad fue por no implementar o fortalecer medidas en seguridad de la información referenciadas en el Anexo de "A" del dominio A.18 cumplimiento de la norma ISO/IEC 27001:2013, y 2 entidades el 3% con respecto al dominio A.12 en controles de Seguridad en las Operaciones relacionadas con medidas técnicas para la protección de los datos personales.

Realizando una evaluación de las entidades sancionadas por la SIC en los últimos tres años el siguiente cuadro presenta el resumen del mayor a menor causal relevante de incumplimiento a la ley 1581 por parte de las entidades.

[160] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[161] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Cuadro 25. Causales de sanciones de entidades por parte de la SIC

Causa origen de sanción SIC	2019	2020	2021	Total	%
2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	18	17	16	51	27%
13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	9	5	18	32	17%
4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	8	7	4	19	10%
9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	1	1	15	17	9%
1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	2	6	8	16	9%
8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	3	8	2	13	7%
14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	5		4	9	5%
3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	2	2	4	8	4%
17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES	2	1	1	4	2%
16 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN SENSIBLE	2		1	3	2%
21 CONTRA EL RESPONSABLE - RESPECTO DE LA RECOLECCIÓN DE INFORMACIÓN	3			3	2%
15 CONTRA EL RESPONSABLE - RESPECTO DEL AVISO DE PRIVACIDAD	2			2	1%
10 CONTRA EL RESPONSABLE - RESPECTO DE LA INSCRIPCIÓN DE LA LEYENDA			1	1	1%
11 CONTRA EL RESPONSABLE - RESPECTO DEL DEBER DE INFORMAR A LOS TITULARES COMO SE ESTÁ UTILIZANDO SU INFORMACIÓN			1	1	1%
27 CONTRA EL ENCARGADO - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS			1	1	1%
5 CONTRA EL RESPONSABLE - RESPECTO DE LA VERACIDAD DE LA INFORMACIÓN			1	1	1%
7 CONTRA EL RESPONSABLE - RESPECTO DE LA RECTIFICACIÓN DE LA INFORMACIÓN			1	1	1%
20 CONTRA EL RESPONSABLE - RESPECTO DE LA LIMITACIÓN TEMPORAL AL TRATAMIENTO	1			1	1%
23 CONTRA EL ENCARGADO - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA		1		1	1%

Causa origen de sanción SIC	2019	2020	2021	Total	%
24 CONTRA EL ENCARGADO - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	1			1	1%
25 CONTRA EL ENCARGADO - RESPECTO DE LA RECTIFICACIÓN O SUPRESIÓN DE LA INFORMACIÓN	1			1	1%
Total	60	48	78	186	100%

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[162] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2021.[163]

De acuerdo con el cuadro anterior se presenta que la causal de sanción más relevante es la *"2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO", con 61 entidades y un porcentaje de 27%, le sigue la "13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS"* con 32 entidades y un porcentaje de 17%, la causal *"4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN"* con 19 entidades y un porcentaje 10%, la causal *"9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS"* con 17 entidades y un porcentaje de 9%, la causal *"8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS"* con 13 entidades y un porcentaje de 7 %, la causal *"14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO"* con 9 entidades y un porcentaje del 5 %, la causal *"3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR"* con 8 entidades un porcentaje del 4%, la causal *"17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES",* con 4 entidades y un porcentaje del 2 %, siendo las

[162] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[163] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

causales de más sanciones con 169 entidades y un porcentaje del 91%, y los demás causales con 17 entidades y un porcentaje del 9 % restante.

Se destacan las 5 primeras causales relevantes y de importancia en las sanciones de las entidades de la SIC para los últimos tres años[164], presentadas en el siguiente cuadro:

Cuadro 26. Top 5 de causales de sanción entidades SIC

Causal de reclamo	Top
2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	1
13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	2
4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	3
9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	4
1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	5

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[165] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC.[166]

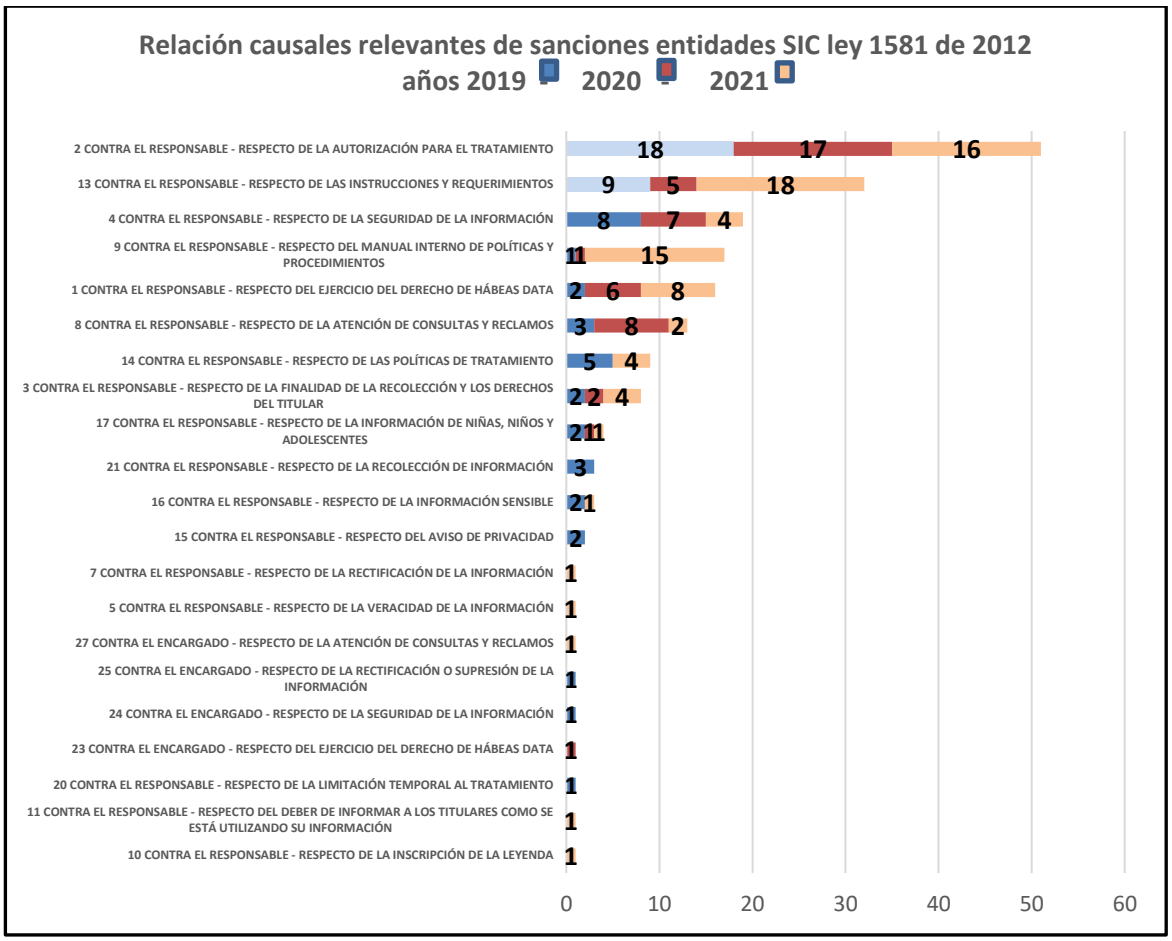
La siguiente ilustración presenta en barras apiladas las entidades sancionadas vs causales, presenta el aspecto *"2 CONTRA EL RESPONSABLE – RESPECTO DE LA AUTORIZACIÓN PARA ELTRATAMIENTO"* como el top número uno con 51 reclamos de los titulares con más cantidades, hasta el menor comparados entre sí.

[164] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

[165] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[166] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Ilustración 10. Top de cáusales más relevantes de sanciones SIC



Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[167] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2019, 2020 y 2021.[168]

En lo relacionado con los controles en seguridad de la información con referencia a la norma ISO/IEC 271001:2013 más relevantes en las causales de los reclamos y sanciones de las entidades por la SIC el siguiente cuadro presenta un resumen de los últimos tres años.

[167] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[168] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

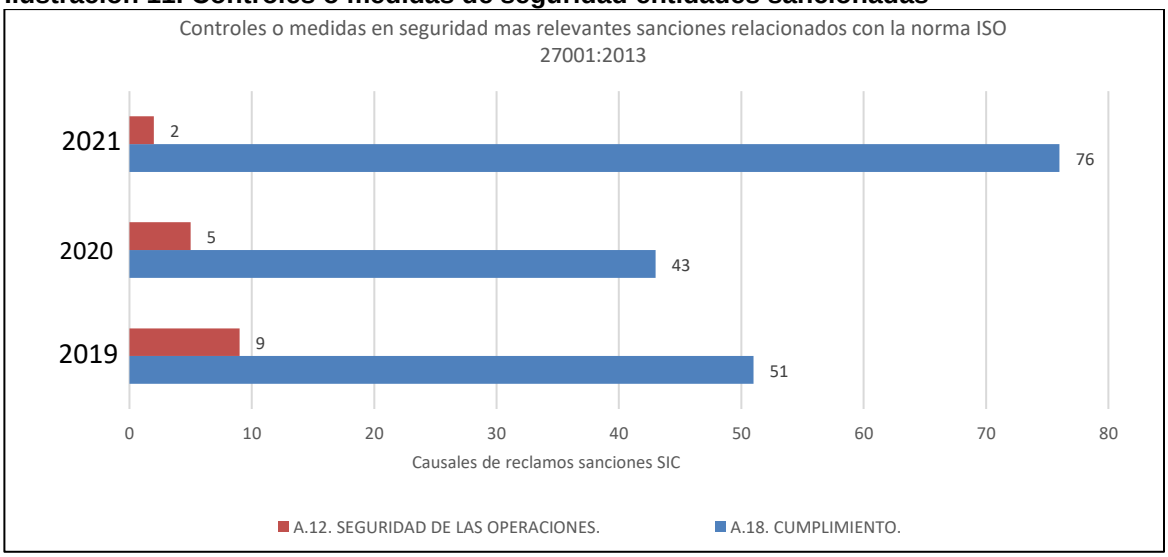
Cuadro 27. Controles medidas de seguridad en sanciones de la SIC

Control o medidas de seguridad norma ISO/IEC 27001:2013	2019	2020	2021	SUMAN	%
A.18. CUMPLIMIENTO.	51	43	76	170	91%
A.12. SEGURIDAD DE LAS OPERACIONES.	9	5	2	16	9%
Total, general	**60**	**48**	**78**	**186**	**100%**

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[169] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2019, 2020 y 2021.[170]

La siguiente ilustración presenta en barras apiladas los controles en seguridad más relevantes de las entidades sancionadas comparados entre sí.

Ilustración 11. Controles o medidas de seguridad entidades sancionadas



Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[171] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2019, 2020 y 2021.[172]

[169] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[170] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

[171] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[172] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

La anterior ilustración presenta que el causal en controles de seguridad de la información de más relevancia fue el “A.18 Cumplimiento” con 170 entidades y un porcentaje del 91%, seguido del control “A.12 Seguridad de las Operaciones” con 16 entidades con un porcentaje del 9%. Relacionados con la norma ISO/IEC 27001:2013.

5.3 DESARROLLO OBJETIVO 3.

Con respecto a disposiciones y obligaciones para la protección de los datos personales en la ley 1581 de 2012 se referencian dos aspectos de relevancia entre otros, que se relacionan y corresponden con medidas de seguridad de la información, el primero que se refiere al artículo 4. *“Principios para el Tratamiento de datos personales. g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;”* y el segundo aspecto que se refiere al 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: d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;”* que las entidades deberían considerar en mejorar o implementar en observancia al cumplimiento de las obligaciones dispuestas en la ley 1581 de 2012 y normativas para la protección de los datos personales;

En lo referente en medidas de seguridad para la protección y privacidad de los datos personales, se referencian tres aspectos de relevancia entre otros, que se relacionan y corresponden con el Anexo A - Objetivos de control y controles de referencia en la norma ISO/IEC 27001:2013, el dominio 1: A.9 Control de acceso,

el dominio 2: A.12 Seguridad de las operaciones y el dominio 3. A.18 Cumplimiento, [173] que las entidades deberían considerar en mejorar o implementar en observancia al cumplimiento de las obligaciones dispuestas en la ley 1581 de 2012 y normativas para la protección de los datos personales.

En lo que respecta sobre el Régimen General de Protección de Datos Personales la Superintendencia de Industria y Comercio – SIC, en su portal web ha publicado una serie de documentos como apoyo a los sujetos obligados a dar cumplimiento a la ley 1581 de 20212, decretos reglamentarios y disposiciones emitidas por la misma, relacionadas en siguiente cuadro presenta una relación entre otras de los mismos más relevante que se les recomienda a las entidades revisarla y adoptarla como buena práctica y una vez implementados les permitirá disminuir el riesgo de sanciones por parte de la SIC.

Cuadro 28. Documentos SIC cumplimiento protección datos personales

#	Documentos
1	Cartilla Formato modelos para el cumplimiento de obligaciones, establecidas en la ley 1581 de 2012[174]
2	Manual de usuario del Registro Nacional de Bases de Datos - RNBD[175]
3	Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES[176]

[173] NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-6.

[174] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

[175] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[176] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

#	Documentos
4	Guía para la implementación del principio de responsabilidad demostrada (Accountability)[177]
5	Guía Sobre el Tratamiento de datos personales estatales[178]
6	Guía sobre el tratamiento de datos personales en la propiedad horizontal[179]
7	Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales[180]
8	Guía sobre el tratamiento de datos personales para fines de Marketing y Publicidad[181]
9	Guía Protección de datos personales en sistemas de videovigilancia[182]
10	Guía sobre el tratamiento de las fotos como datos personales[183]
11	Guía para solicitar la declaración de conformidad sobre transferencias internacionales de datos personales[184]

Fuente: Autor

Del anterior cuadro se destaca una cartilla con formatos de modelos y plantillas, el manual de registro de Bases de datos personales que indica como se inscriben y los campos que deben diligenciar, el cuestionario de diagnóstico de cumplimiento que le permite a la entidad evaluar cómo está en cumplimiento, le sigue la guía de

[177] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

[178] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2021/SIC%20(2021)%20Gu%C3%ADa%20sobre%20el%20tratamiento%20de%20datos%20personales%20en%20las%20entidades%20estatales.pdf

[179] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_prop_horizontal_NOV12_OK%20(1).pdf

[180] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

[181] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf

[182] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf

[183] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Gu%C3%ADa%20tratamiento%20de%20datos%20fotos%20FINAL%2014%20diciembre(1).pdf

[184] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Guia_para_solicitar_la_declaracion_de_conformidad_sobre_las_trasferencias_internacionales_de_datos_personales.pdf

implementación para el principio de responsabilidad demostrada, este documento es de vital importancia porque emite recomendaciones de como la entidad debe generar un programa Integral de gestión de datos personales y sus requisitos, además, que una vez implementada le permite a le entidad demostrar ante la SIC el cumplimiento de la ley 1581 de 2012 y por último le siguen una serie de guías todas a encaminadas a la evaluación, aplicación de acciones de cumplimiento y las medidas de seguridad para la protección y privacidad de los datos personales.

Para el registro de una base de datos personal en el aplicativo de la SIC-RNBD página 59[185], se encuentra en el paso 6 la opción de responder las *"Medidas de Seguridad de la Información"* con que cuenta o tiene implementada la entidad que registra la base de dato personal, hay que tener en cuenta que son los controles actuales y no las que piensa implementar y ser muy diligentes en contestarlas debidamente, ya que la SIC en sus revisiones las analiza y si visita la entidad las va a contrastar con las respuestas registradas, se recomienda que las medidas ausentes se deben omitir en el check de verificación y colocarla en una lista de pendientes e incorporarlas en el plan de implementación de la entidad a la ley 1581 de 2012, en el Anexo D presenta una relación de las 26 preguntas, el bloque temático en seguridad, la posible causa de reclamo por el titular por no implementarse y su correspondencia con la medidas o controles en seguridad del anexo "A" de la norma ISO/IEC 27001:2013.

En el Anexo D se presenta un cuadro que permite a la entidad tener una visión general de la seguridad de la información para los datos personales y de cómo aplicar los controles del Anexo "A" de la norma ISO/IEC 27001:2013 a las preguntas de medidas de seguridad del RNBD de la SIC.

El siguiente cuadro presenta un resumen por preguntas al formulario de la SIC-RNBD y porcentajes de los 8 bloques temáticos.

[185] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://rnbd.sic.gov.co/sisi/login

Cuadro 29. Preguntas medidas de seguridad formulario SIC-RNBD

Bloque temático preguntas SIC	Cantidad	%
SEGURIDAD DE LA INFORMACION	5	19%
PROCESAMIENTO DE INFORMACIÓN PERSONAL	5	19%
SEGURIDAD DE LA INFORMACIÓN	5	19%
SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL	4	15%
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL	2	8%
AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL	2	8%
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	2	8%
SEGURIDAD DE LA INFORMACIÓN PERSONAL EN TORNO AL RECURSO HUMANO	1	4%
Total	**26**	**100%**

Fuente: Adaptación del Sistema de la SIC- RNBD[186] y anexo "A" de la norma ISO/IEC 27001:2013[187]

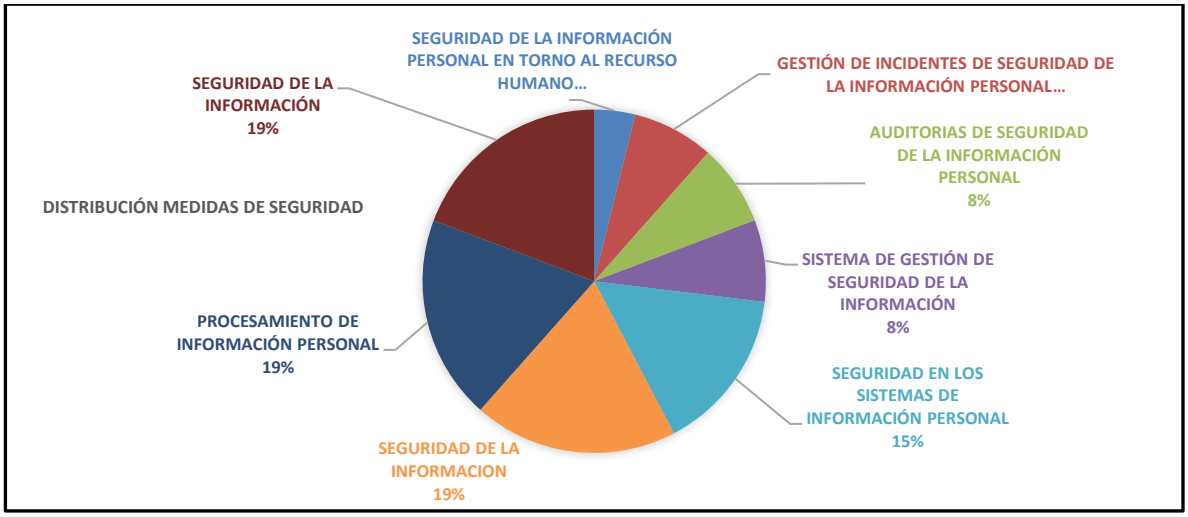
En el cuadro anterior los bloques temáticos de Seguridad de la Información, procesamiento de la información y seguridad de la Información, presentan cada uno un total de 5 preguntas por bloque cada uno, le sigue seguridad de la información con 4 preguntas sumando 19 preguntas y los restantes bloques con 7 preguntas,

La siguiente ilustración presenta un resumen por porcentajes de preguntas al formulario de la SIC-RNBD.

[186] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://rnbd.sic.gov.co/sisi/login

[187] ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-6.

Ilustración 12. Preguntas medidas de seguridad formulario SIC-RNBD



Fuente: Adaptación del Sistema de la SIC- RNBD[188] y anexo "A" de la norma ISO/IEC 27001:2013[189]

En la ilustración anterior se presenta los bloques temáticos de Seguridad de la Información, procesamiento de la información y seguridad de la Información, presentan cada uno un porcentaje de 19% cada uno, le sigue seguridad de la información con el 15 %, sumando el 73% de las preguntas y los restantes bloques con el 27 %.

El siguiente cuadro presenta su correspondencia a la norma ISO/IEC 27001:2013 por dominios del anexo "A" de la norma ISO 271001:2013 y las preguntas a las medidas de seguridad del formulario RNBD-SIC.

Cuadro 30. Controles norma ISO/IEC 27001:2013 Vs. formulario RNBD-SIC

Ámbito Anexo "A" controles Norma ISO/IEC 27001:2013	Cantidad	%
A.12. SEGURIDAD DE LAS OPERACIONES.	9	35%
A.9. CONTROL DE ACCESO.	4	15%
A.13. SEGURIDAD DE LAS COMUNICACIONES.	3	12%

[188] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://rnbd.sic.gov.co/sisi/login

[189] ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-6.

Ámbito Anexo "A" controles Norma ISO/IEC 27001:2013	Cantidad	%
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	3	12%
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	2	8%
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	2	8%
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	1	4%
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	1	4%
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	1	4%
TOTAL	26	100%

Fuente: Adaptación del Sistema de la SIC- RNBD[190] y anexo "A" de la norma ISO/IEC 27001:2013[191]

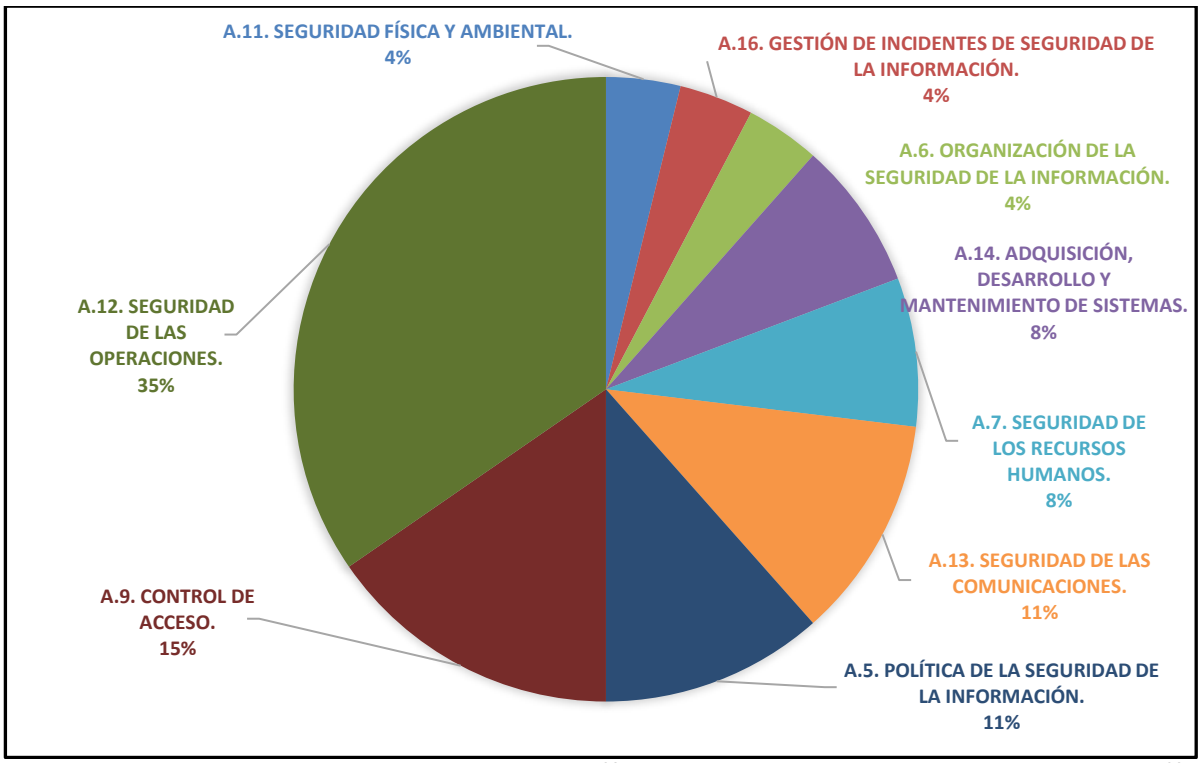
En el cuadro anterior el dominio "*A.12. SEGURIDAD DE LAS OPERACIONES"*. presenta 9 preguntas, le siguen "*A.9. CONTROL DE ACCESO"* con 4 preguntas, luego *"A.13. SEGURIDAD DE LAS COMUNICACIONES*" y "*A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN*" con 3 preguntas cada uno, luego los dominios "*A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS"* y "*A.7. SEGURIDAD DE LOS RECURSOS HUMANOS"* con 2 preguntas cada uno para un total de 23 preguntas y los restantes dominios con 3 preguntas.

La siguiente ilustración presenta un resumen por porcentajes de dominios de la norma ISO/IEC 27001:2013 con referencia a medidas de seguridad de formulario de la SIC-RNBD.

[190] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://rnbd.sic.gov.co/sisi/login

[191] ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-6.

Ilustración 13. Dominios norma ISO/IEC 27001:2013 formulario RNBD-SIC.



Fuente: Adaptación del Sistema de la SIC- RNBD[192] y anexo "A" de la norma ISO/IEC 27001:2013[193]

En la ilustración anterior el dominio "*A.12. SEGURIDAD DE LAS OPERACIONES*". presenta el porcentaje top del 35%, le sigue "*A.9. CONTROL DE ACCESO*" con 15%, luego "*A.13. SEGURIDAD DE LAS COMUNICACIONES*" y "A.5. *"POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN"* con 12% cada uno, luego los dominios "A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS" y "A.7. SEGURIDAD DE LOS RECURSOS HUMANOS" con 8% cada uno para un total de 88% y los restantes dominios con el 12%.

Ahora bien, en el decreto 1377 de 2013, referencia un aspecto notable en lo concerniente a la responsabilidad demostrada frente al tratamiento de los datos en

[192] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://rnbd.sic.gov.co/sisi/login
[193] ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-6.

el artículo 26. “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…”, que las entidades deberían considerar en mejorar o implementar en observancia al cumplimiento de las obligaciones dispuestas en la ley 1581 de 2012 y normativas para la protección de los datos personales.

La Superintendencia de Industria y Comercio – SIC, dispuso la cartilla guía “Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES”[194] con dos listados. El primer listado mediante el cual las entidades deben aplicar para cotejar el cumplimiento de los principios y deberes establecidas en la ley 1581 de 2012, y el segundo listado con el cual las entidades al aplicarlo su resultado les permitirá establecer y determinar el nivel de avance en la implementación del principio de responsabilidad demostrada en concordancia con la “Guia para la implementación del principio de responsabilidad demostrada (Accountability)”[195].

El Anexo D, presenta un cuadro con las preguntas del primer listado que le permite a la entidad verificar el cumplimiento de los principios y deberes establecidos en la ley 1581 de 2012, que deben ser evaluados e implementar para minimizar el riesgo de sanción por parte de la SIC ante un probable incumplimiento a la protección de datos personales.

[194] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

[195] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

En el siguiente cuadro se presenta un resumen, por preguntas del listado por ámbitos de comprobación del régimen de protección de datos personales al formulario de la SIC-RNBD y porcentajes de 14 ámbitos temáticos del listado referenciados en la guía "Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES"[196].

Cuadro 31. Listado de comprobación del régimen de la SIC-RNBD

#	Lista Formulario SIC	CANTIDAD	%
1	ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES	12	14%
2	TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES	10	12%
3	GESTIÓN DE ENCARGADOS DEL TRATAMIENTO	9	11%
4	POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES	8	9%
5	AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES	7	8%
6	AVISO DE PRIVACIDAD	7	8%
7	PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES	6	7%
8	TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD	6	7%
9	RESPONSABILIDAD DEMOSTRADA	6	7%
10	DERECHOS DE LOS TITULARES DE LA INFORMACIÓN	5	6%
11	INFORMACIÓN MÍNIMA A LOS TITULARES	5	6%
12	SUMINISTRO DE LA INFORMACIÓN PERSONAL	2	2%
13	REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD	1	1%
14	REGISTRO NACIONAL DE BASES DE DATOS	1	1%
TOTAL		85	100%

Fuente: Adaptación de la guía Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las Mipymes de la SIC[197]

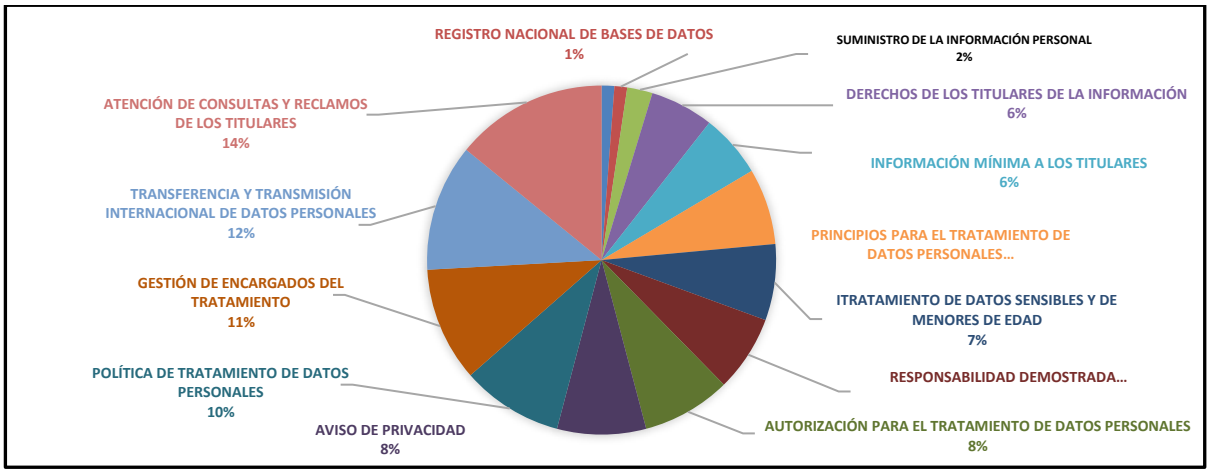
En cuadro anterior el ámbito que presenta más relevancia y top es *"ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES",* presenta 12 preguntas, le siguen *"TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES"* con 10 preguntas, el ámbito "*GESTIÓN DE ENCARGADOS DEL TRATAMIENTO"* con 9 preguntas, *"POLÍTICA DE TRATAMIENTO DE DATOS*

[196] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

[197] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

PERSONALES" con 8 preguntas, *"AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES" y "AVISO DE PRIVACIDAD"* con 7 preguntas cada uno, luego los ámbitos *"PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES"*, "*TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD"* y *"RESPONSABILIDAD DEMOSTRADA"* con 6 preguntas cada uno, para un total de 71 preguntas y los restantes ámbitos con 14 preguntas, sumando un total de 85 preguntas del formulario guía "Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES", en lo referente al cumplimiento de los principios y deberes establecidos en la ley 1581 de 2012. Lo que permite recomendar que las entidades deben generar estrategias para dar cumplimiento ir implementando las respectivas medidas y mecanismos a los 14 ámbitos del formulario, además que deben cubrirlos todos ya que uno solo que no cumple es un referente para la SIC en el incumplimiento a la protección de datos personales. La siguiente ilustración presenta un resumen por porcentajes porcentajes de los 14 ámbitos temáticos del listado referenciados en la guía "Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES".

Ilustración 14. Resumen porcentajes ámbitos medidas de seguridad



Fuente: Adaptación de la guía Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las Mipymes de la SIC[198]

[198] Ibid.

En la ilustración anterior el ámbito que presenta más relevancia y top es “ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES”, presenta un porcentaje del 14 %, de preguntas le siguen “TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES” con el 12% de preguntas, el ámbito “GESTIÓN DE ENCARGADOS DEL TRATAMIENTO” con 11% de preguntas, “POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES” con 9% preguntas, “AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES” y “AVISO DE PRIVACIDAD” con 8% de preguntas cada uno, luego los ámbitos “PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES”, “TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD” y “RESPONSABILIDAD DEMOSTRADA” con 7% preguntas cada uno, para un total de 85% de preguntas y los restantes ámbitos con un porcentaje de 15 % de preguntas, sumando un total de 100% de preguntas del formulario guía “Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES”, en lo referente al cumplimiento de los principios y deberes establecidos en la ley 1581 de 2012. Lo que permite referenciar a las entidades que ámbitos tienen más porcentajes de preguntas para diseñar e implementar estrategias y aplicar controles y medidas de seguridad para dar cumplimiento del régimen de protección de datos personales.

El Anexo F presenta un cuadro con el segundo listado correspondiente a la lista de verificación para medir el avance de implementación del principio de responsabilidad demostrada por parte de las entidades para la protección de datos personales dispuesta en la cartilla guía “Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES”[199]

El siguiente cuadro presenta un resumen de las preguntas agrupadas en 3 ámbitos: 1. Compromisos de la Organización, 2. Controles del programa y 3. Evaluación y

[199] Ibid

revisión continua, del listado en la cartilla guía “Cuestionario de Diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES”[200]

Cuadro 32. Preguntas principio de responsabilidad demostrada

LISTA DE VERIFICACION - MEDIR AVANCE DE IMPLEMENTACION DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA		
1. COMPROMISOS DE LA ORGANIZACIÓN	**CANTIDAD**	**%**
1.1. DESDE LA ALTA DIRECCIÓN	**10**	**32%**
1.2. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	**17**	**55%**
1.3. PRESENTACIÓN DE INFORMES	**4**	**13%**
SUMAN	**31**	**32%**
2. CONTROLES DEL PROGRAMA	**CANTIDAD**	
2.1. PROCEDIMIENTOS OPERACIONALES	**1**	**2%**
2.2. INVENTARIO DE BASES DE DATOS CON INFORMACIÓN PERSONAL	**16**	**30%**
2.3. POLÍTICAS	**8**	**15%**
2.4. SISTEMA DE ADMINISTRACIÓN DE RIESGOS	**7**	**13%**
2.5. FORMACIÓN Y EDUCACIÓN	**4**	**8%**
2.6. PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES DE SEGURIDAD	**6**	**11%**
2.7. GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES.	**7**	**13%**
2.8. COMUNICACIÓN EXTERNA	**4**	**8%**
SUMAN	**53**	**54%**
3. EVALUACIÓN Y REVISIÓN CONTINUA	**CANTIDAD**	
3.1. PLAN DE SUPERVISIÓN Y REVISIÓN	**2**	**2%**
3.2 EVALUACIÓN Y REVISIÓN DE LOS CONTROLES DEL PROGRAMA	**12**	**12%**
SUMAN	**14**	**14%**
TOTAL	**98**	**100%**

Fuente: Adaptación de la guía Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las Mipymes de la SIC[201]

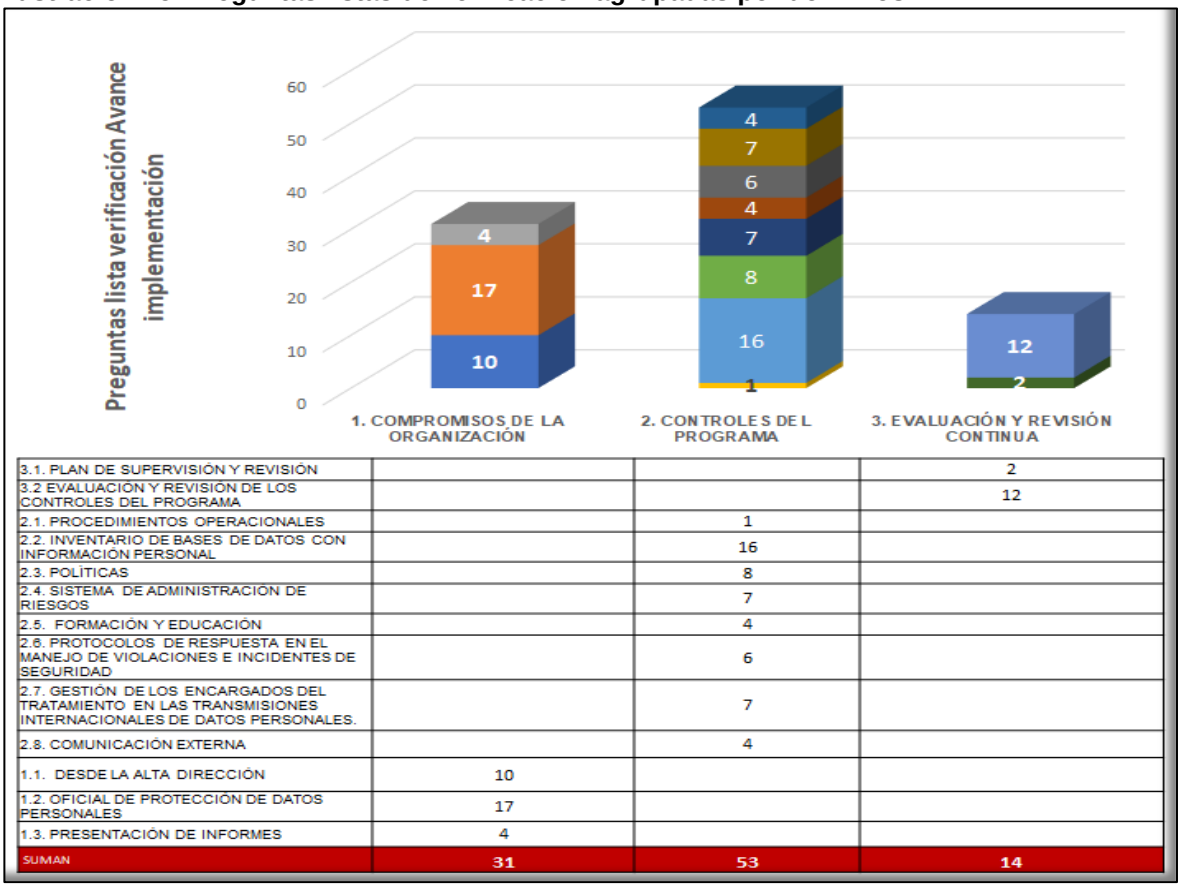
En el cuadro anterior el dominio “Controles del Programa” compuesto por 8 agrupaciones representa la mayor cantidad de con un total del 32 % y 53 preguntas, lo que permite identificar que las entidades que den observancia en mecanismos e implementación de requisitos a este ámbito, será un avance considerativo en el cumplimiento de la responsabilidad demostrada a la ley 1581, le sigue el dominio “Compromisos de la organización” con tres agrupaciones con el 32% y 31 preguntas y por último “Evaluación y revisión continua” con 2 agrupaciones para un

[200] Ibid
[201] Ibid.

total del 14% y 14 preguntas, este dominio toma importancia una vez se hayan implementado los dos primeros ámbitos ya que corresponde al seguimiento, control y mejora en la revisión y evaluación de controles que se implementan que permiten a la entidad medir su estad de eficacia en la implementación de controles en seguridad y de cumplimiento para la protección y privacidad de datos personales.

La siguiente ilustración nos presenta los dominios por grupos de preguntas apilados por dominios.

Ilustración 15. Preguntas listas de verificación agrupadas por dominios.



3.1. PLAN DE SUPERVISIÓN Y REVISIÓN			2
3.2 EVALUACIÓN Y REVISIÓN DE LOS CONTROLES DEL PROGRAMA			12
2.1. PROCEDIMIENTOS OPERACIONALES		1	
2.2. INVENTARIO DE BASES DE DATOS CON INFORMACIÓN PERSONAL		16	
2.3. POLÍTICAS		8	
2.4. SISTEMA DE ADMINISTRACIÓN DE RIESGOS		7	
2.5. FORMACIÓN Y EDUCACIÓN		4	
2.6. PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES DE SEGURIDAD		6	
2.7. GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES.		7	
2.8. COMUNICACIÓN EXTERNA		4	
1.1. DESDE LA ALTA DIRECCIÓN	10		
1.2. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	17		
1.3. PRESENTACIÓN DE INFORMES	4		
SUMAN	31	53	14

Fuente: Adaptación de la guía Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las Mipymes de la SIC[202]

La ilustración anterior presenta los tres dominios por 13 grupos de preguntas, siendo el de más relevancia el dominio “Controles del Programa” con 54 % y 53 preguntas.

[202] Ibid.

6 CONCLUSIONES

Lo expuesto en el desarrollo de la presente monografía permite referenciar las siguientes conclusiones:

En primera instancia, contrastada la información relacionada con la legislación en aspectos relativos a las medidas de seguridad en protección de datos personales de la Unión Europea y de los gobiernos de España, México, Chile, Perú y Colombia, con los estándares ISO 27001:2013 e ISO/IEC 27002:2015 para la Seguridad de la Información, se encuentra que en las legislaciones se encuentra de forma implícita al menos un ítem en medidas de seguridad, no obstante lo hacen de forma muy generalizada, dejando su interpretación e implementación a las entidades y a las respectivas autoridades que delegan para la supervisión, quienes emiten disposiciones acordes a su interpretación del entorno del estado, lo que no permite a las entidades tener muy claro como implementar estos controles haciendo uso de un Sistema de Gestión de Seguridad de la Información, que les permita tener un control y supervisión de los controles y medidas en seguridad implementados o que deban implementar y responder a las necesidades y requerimientos de ley.

En segunda instancia estimadas las causas de las sanciones emitidas en las resoluciones sancionatorias por la Superintendencia de Industria y Comercio para los últimos tres años (2019, 2020,2021), se evidencia que las mismas de debieron a la ausencia de controles en seguridad de la información, bien sea de orden procedimental, técnico o desconocimiento por parte de los responsables del tratamiento de las entidades en el cumplimiento a la normatividad de la ley 1581 de 2012 y las disposiciones emitidas por la SIC en lo referente a la protección de datos personales, reflejándose que las mismas no aplican un Sistema de Seguridad de la Información o no le hacen seguimiento y control al mismo.

Y por último en tercera instancia, contrastadas las legislaciones estudiadas en el presente documento con las medidas en seguridad de la información y evaluadas las entidades sancionadas por la SIC en lo referente a protección de datos personales, se concluye que la incorporación de buenas prácticas mediante un Sistema de Gestión de Seguridad de la información (SGSI) correlacionándolo con las disposiciones, manuales y guías emitidas por la SIC para el cumplimiento de la ley 1581 de 2012, permitirá a las entidades gestionar los riesgos de seguridad de la información y minimizar las multas por parte de la SIC o posibles demandas de los por la no protección de los datos personales de los titulares.

7 RECOMENDACIONES

Las entidades deben contemplar fortalecer sus buenas prácticas en la aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI) incorporando mecanismos y controles buscando proteger los datos personales y la privacidad de los titulares.

Los Oficiales de Protección de Datos Personales o el área encargada de la entidad, deben mantener actualizada las disposiciones, normativas, manuales y guías entre otras emitidas por la Superintendencia de Industria y Comercio para la protección de datos personales y a su vez integrarlas y aplicarlas en los controles de seguridad del SGSI.

Los Oficiales de Protección de Datos Personales o el área encargada de la entidad, así como la alta dirección deben evaluar en primera instancia las causales de sanción más representativas por parte de la SIC, con el fin que gestionen una matriz de riesgos y generen planes de acción que les permita priorizar los controles de alta criticidad que se deben implementar o remediar.

La legislación del gobierno de España es la más actualizada a la fecha en protección de dato personales en línea con la de la Unión Europea entró en vigencia en el año 2018, además incorpora medias relacionadas con el Internet y medios digitales, igualmente otros gobiernos de Latinoamérica han generado o actualizado sus legislaciones referenciándola; se recomienda a los Oficiales de Protección de Datos Personales o el área encargada su revisión e integrar las medidas en seguridad que no se relacionen en las disposiciones de la ley 1581 de 2012 y de la SIC, acciones que permiten a las entidades ampliar más el espectro en control de medidas de seguridad para a protección de los datos personales de las entidades

BIBLIOGRAFÍA

ARELLANO LÓPEZ, Christian Alberto. El derecho de protección de datos personales. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-55452020000200009&lang=es

BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.bcn.cl/leychile/navegar?idNorma=141599

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1266 (31, diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. El Congreso, p. 1.

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1273 (5, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. El Congreso, p. 1.

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. 1.

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. El Congreso, p. 1.

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley estatutaria 1581 (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. El Congreso, p. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

COLOMBIA, MINISTERIO DE COMERCIO, INDUSTRIA Y COMERCIO, Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Decreto 620 (2, mayo, 2020). Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

CONSTITUCIÓN POLÍTICA DE COLOMBIA, Asamblea Constituyente de Colombia de 1991, (04, julio, 1991). Consultado el 01 de octubre de 2021. Disponible en Internet: http://wsp.presidencia.gov.co/Normativa/Documents/Constitucion-Politica-Colombia.pdf.

DW. Las Constituciones de América Latina. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.dw.com/es/las-constituciones-de-am%C3%A9rica-latina/g-50480635

ESQUEMA NACIONAL DE SEGURIDAD. MAGERIT – VERSIÓN 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

GOBIERNO DE ARGENTINA. Protección de los datos personales Ley 25.326. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/doue/2016/119/L00001-00088.pdf

GOBIERNO DE ESPAÑA. Agencia estatal Boletín Oficial del estado. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.boe.es/eli/es/lo/2018/12/05/3

GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

GOBIERNO DE MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

GOBIERNO DE PERU. Normas legales. Ley 29733. Ley de protección de datos personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-
ISO27000.ES. Glosario. [en línea]. Consultado el 28 de febrero de 2022. Disponible en Internet: https://www.iso27000.es/glosario.html

NACIONES UNIDAS. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://www.un.org/es/about-us/universal-declaration-of-human-rights

NIST. Special Publication 800-53. Revision 5. Security and Privacy Controls for Information Systems and Organizations. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-

POLITECNICO GRACOLOMBIANO. SISTEMA NACIONAL DE BIBLIOTECAS SISNAB. La protección de datos en la era digital: Colombia-España. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://alejandria.poligran.edu.co/bitstream/handle/10823/2142/Articulo%20Proteccion%20de%20datos%20%20en%20la%20era%20digita%20Colombia-Espa%C3%B1a%20Nov.%2029.pdf?sequence=1&isAllowed=y

PROCURADURIA GENERAL DE LA NACIÓN. Resolución 462 (26, abril, 2019). Por medio de la cual se asignan funciones a una procuraduría delegada - se adicionan funciones disciplinarias. [en línea]. Consultado el 04 de enero de 2022. Disponible en Internet: https://www.procuraduria.gov.co/relatoria/media/file/flas_juridico/2380_PGN%20Resoluci%C3%B3n%20462%20de%202019%20.pdf.

RED IBEROAMERICANA. XIV Encuentro Iberoamericano: Santa Marta, Colombia 8,9,10 de junio de 2016 [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.redipd.org/es/actividades/encuentro/xiv-encuentro-iberoamericano-santa-marta-colombia-8-9-y-10-de-junio-de-2016

SÁNCHEZ PÉREZ, Gabriel y ROJAS GONZÁLEZ, Isai. Leyes de protección de datos personales en el mundo y la protección de datos biométricos – parte I. [en línea]. Consultado el 01 de octubre de 2021. Disponible en Internet: https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/colombia-participo-en-la-elaboracion-de-los-estandares-de-proteccion-de-datos-de-los-estados-iberoamericanos

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular Única – Protección de datos Personales. [en línea]. Consultado el 04 de enero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/normatividad/052020/Ti%CC%81tulo%20V%20Proteccion%20Datos%20Circular%2003%20del%2030%20de%20marzo%202020%29.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2021/SIC%20(2021)%20Gu%C3%ADa%20sobre%20el%20tratamiento%20de%20datos%20personales%20en%20las%20entidades%20estatales.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_prop_horizontal_NOV12_OK%20(1).pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Gu%C3%ADa%20tratamiento%20de%20datos%20fotos%20FINAL%2014%20diciembre(1).pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Guia_para_solicitar_la_declaracion_de_conformidad_sobre_las_trasferencias_internacionales_de_datos_personales.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://rnbd.sic.gov.co/sisi/login

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

UNIANDES. Red Académica Internacional. Aproximación constitucional de la protección de datos personales en Latinoamérica. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

UNIANDES. Red Académica Internacional. Aproximación constitucional de la protección de datos personales en Latinoamérica. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

WE ARE SOCIAL. DIGITAL REPORT 2021: EL INFORME SOBRE LAS TENDENCIAS DIGITALES, REDES SOCIALES Y MOBILE. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://wearesocial.com/es/blog/2021/01/digital-report-2021-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/

ANEXOS

Anexo A. Entidades con resolución sancionatoria año 2019

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
COMUNICATION TECH Y TRANSPORTE S.A "Cotech S.A"	2019	La Política de Tratamiento de Información (PTI) debe redactarse con un lenguaje claro y sencillo, teniendo en cuenta el tipo de audiencia, en particular si se tratan de niños, niñas o adolescentes, personas con alguna discapacidad, mayores adultos, o personas que no hablen el idioma castellano. La PTI debe diferenciarse claramente de aquella no relacionada con la protección de datos, como disposiciones contractuales o términos generales de uso.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.
Facebook Inc., Facebook Colombia S.A.S. y Facebook Ireland Limited	2019	La Ley Estatutaria 1581 de 2012 es aplicable a Facebook Inc. porque recolecta Datos personales en el territorio de la República de Colombia a través de cookies que instala en los equipos o dispositivos de las personas residentes o domiciliadas en Colombia. El Principio de Responsabilidad Demostrada (Accountability) le impone a Facebook Inc. el deber de probar que ha adoptado medidas apropiadas y efectivas para garantizar la seguridad de la información de sus usuarios. En el ciberespacio no desaparecen los derechos humanos ni la ciberseguridad.	24 CONTRA EL ENCARGADO - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
ABASTECIMIENTO, ASESORÍAS Y ACOMPAÑAMIENTO GAS NATURAL SAS	2019	El tratamiento de datos personales semiprivados de clientes, prospecto de clientes y empleados requiere de autorización previa, expresa e informada por parte de los Titulares, quienes deben ser informados previamente respecto de la finalidad o finalidades del tratamiento al que serán sometidos los datos recolectados.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
BANCOLOMBIA S.A.	2019	El Responsable del tratamiento de los datos debe atender las solicitudes, peticiones, quejas y reclamos de manera debida, oportuna, de fondo, completa y demostrable. No es aceptable que el ciudadano tenga que realizar varias solicitudes y que deba esperar más de un (1) año para que su petición sea respondida -artículo 15 de la ley 1581 de 2012-.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
BANCOLOMBIA S.A. /BRM S.A	2019	Se vulneran los derechos fundamentales de protección de datos y de petición del titular cuando no se responde una solicitud de supresión de la información dentro de los siguientes quince (15) días hábiles a su realización -artículo 15 ley 1581 de 2012-.	25 CONTRA EL ENCARGADO - RESPECTO DE LA RECTIFICACIÓN O SUPRESIÓN DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
DIRECTV COLOMBIA LTDA	2019	Las respuestas automatizadas, preestablecidas y estandarizadas que no se refieran al caso específico del ciudadano no son útiles para cumplir debidamente la atención de consultas o reclamos del Titular del dato. No es aceptable que el Titular de la información tenga que realizar reiteradas peticiones al Responsable solicitando la eliminación de sus datos.	20 CONTRA EL RESPONSABLE - RESPECTO DE LA LIMITACIÓN TEMPORAL AL TRATAMIENTO	A.18. CUMPLIMIENTO.
CENTRO EDUCATIVO SUPERIOR	2019	Tratamiento de datos sensibles y de niños niñas y adolescentes: en los formularios utilizados por las instituciones educativas en los que se recolecten datos de niños, niñas y adolescentes y datos	17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
INTERAMERICANO S.A.S.		sensibles se debe informar a los titulares que por tratarse de datos sensibles y de menores de edad no están obligados a autorizar su tratamiento e informar de manera explícita y previa cuáles de los datos que recolecta son sensibles, la finalidad del tratamiento, así como obtener su consentimiento expreso.	NIÑAS, NIÑOS Y ADOLESCENTES	
CONTACTO SOLUTIONS LTDA.	2019	El uso de procesos tecnológicos automatizados para el tratamiento de los datos no está exento de cumplir el deber legal de solicitar y conservar copia de la autorización previa y expresa de la persona Titular del dato. Los formularios preestablecidos y el diligenciamiento obligatorio de ciertos campos para permitir un proceso en línea no satisfacen, per se, dicho requisito -artículo 9 de la ley 1581 de 2012-.	21 CONTRA EL RESPONSABLE - RESPECTO DE LA RECOLECCIÓN DE INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
CENTRAL MOTOR AMÉRICA S.A.S	2019	No toda información es un dato personal, ni todo dato personal requiere de la autorización para ser tratado. Una dirección de correo electrónico no es, per se, un dato personal y algunas direcciones de correo electrónico son datos personales de naturaleza pública. La recurrente no adoptó las medidas de seguridad necesarias para evitar que 196 direcciones de correo electrónico fuesen conocidas indebidamente por terceros.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
GALVIS ARQUITECTOS EU	2019	La omisión de responder los requerimientos emitidos por la SIC por parte de los Administradores, Responsables y Encargados, es un incumplimiento al régimen de protección de datos personales, incluso cuando omiten responder de forma completa y suficiente los requerimientos de la entidad.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
INCOTEL - MÒVIL S.A.S	2019	La omisión de responder los requerimientos remitidos por la Superintendencia da lugar a la imposición de sanción, incluso cuando omiten responder de forma completa y suficiente los requerimientos de la entidad. De conformidad con lo dispuesto en el literal o) del artículo 17 de la ley 1581 de 2012.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
BANCO FALABELLA S.A.	2019	Los Titulares de los datos tienen el derecho de solicitar al Responsable del Tratamiento la exclusión o supresión de sus datos personales. Esta solicitud debe ser atendida oportuna y debidamente sin que el ciudadano tenga que insistir para hacer valer sus derechos.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
RAPPI S.A.S	2019	Rappi incumplió el deber de solicitar y conservar copia de la autorización del Titular del dato y se demoró más de 22 meses en suprimir datos de una persona que tuvo que presentarle dos peticiones para dicho efecto. Los derechos de las personas se deben garantizar oportunamente sin que el ciudadano tenga que rogarles o insistirles a las empresas. La creación de un usuario en una plataforma tecnológica no significa, per se, que él autorizó el tratamiento de sus datos personales. Al utilizarse herramientas o procesos tecnológicos en páginas web o aplicaciones (APP) es imprescindible que el Responsable establezca la real identidad del Titular del dato; evitando que terceros o suplantadores de identidad autoricen el tratamiento.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
TRAVEL LINK S.A.S.	2019	La recolección de datos personales acudiendo al mecanismo de "referidos" no habilita al responsable para realizar tratamiento de datos personales en la medida en que se requiere la autorización previa, expresa e informada del Titular cuyos datos van a ser tratados. La responsabilidad jurídica y económica frente al tratamiento de datos personales radica no sólo en la persona jurídica, sino también en cabeza de sus Administradores.	21 CONTRA EL RESPONSABLE - RESPECTO DE LA RECOLECCIÓN DE INFORMACIÓN	A.18. CUMPLIMIENTO.
ACORAL CONSTRUCTORA S.A.S	2019	La política de tratamiento de datos debe cumplir con los requisitos mínimos establecidos en la ley 1581 de 2012, por cuanto: i) debe describir de manera clara y sencilla los procedimientos mediante los cuales los Titulares pueden ejercer sus derechos, ii) informar el término de vigencia de cada una de sus bases de datos y, iii) acreditar el haber puesto a disposición de los Titulares está información.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.
PASH S.A.S	2019	El Responsable debe recolectar los datos personales habiendo solicitado de manera previa y expresa la autorización del titular para realizar el tratamiento y conservar copia de esta. Adicionalmente, el Responsable deber darles el trámite correspondiente a las solicitudes interpuestas por el quejoso, implementando un procedimiento de atención de consultas y reclamos que garantice el derecho de habeas data.	21 CONTRA EL RESPONSABLE - RESPECTO DE LA RECOLECCIÓN DE INFORMACIÓN	A.18. CUMPLIMIENTO.
ROYAL FILMS S.A.S	2019	Los Responsables del Tratamiento de la información de los ciudadanos tienen la obligación de mantener la información bajo condiciones de seguridad idóneas, eficaces, oportunas y demostrables, que impidan la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales de las personas -literal d) del artículo 17 de la Ley 1581 de 2012.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
COMUNICACIÓN CELULAR S A COMCEL S.A	2019	El deber de garantizar el ejercicio efectivo del derecho al habeas data, se viola cuando no se le permite al titular revocar la autorización; también se vulnera este derecho fundamental cuando el administrador no tramita los requerimientos del Titular.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
RED MÁS 365 S.A.S	2019	Deber de solicitar autorización: el número telefónico de uso personal es un dato personal de carácter semiprivado, lo que significa que sólo puede ser tratado cuando se cuente con la autorización previa, informada y expresa.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
UNE EPM TELECOMUNICACIONES S.A	2019	El deber de solicitar y conservar copia de la autorización previa, se viola cuando el Responsable recolecta datos personales como números telefónicos y correos, sin adelantar el procedimiento para obtener la autorización previa, expresa e informada.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
MERVICOL S.A.S	2019	Debe ser respetuoso de la regulación de datos personales cualquier tratamiento de números telefónicos mediante "marcadores predictivos", robocalls, inteligencia artificial y otras tecnologías o procedimientos automatizados para contactar personas.	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
ASISTENCIA UNIVERSAL S.A.S	2019	El Responsable debe solicitar y conservar copia de la autorización previa, expresa e informada del titular y cumplir con el deber de informar al Titular la finalidad del tratamiento de sus datos personales. El consentimiento puede verse viciado cuando no se especifica la finalidad del tratamiento de los datos.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
FOTOGRAFO	2019	La foto que capta la imagen del rostro de una persona es un dato personal sensible porque trata datos biométricos (Artículo 5 de la Ley 1581 de 2012). Para la recolección y uso de este tipo de datos deben observarse las reglas especiales señaladas en el artículo 6 del decreto 1377 de 2013 en concordancia con lo dispuesto en los artículos 9 y 12 de la citada ley. La autorización puede obtenerse mediante cualquiera de los mecanismos autorizados por la ley y sus normas reglamentarias, pero el Responsable debe asegurarse de conservar copia de esta para suministrarla al Titular del dato cuando la requiera en virtud del literal b) del artículo 8 de la citada ley y para dar cumplimiento al literal b) del artículo 17 de la misma.	16 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN SENSIBLE	A.18. CUMPLIMIENTO.
DIEZ MEDELLIN S.A.S	2019	Para usar fotos con fines de publicidad o marketing y que captan la imagen facial de una persona, es necesario que el Responsable del Tratamiento solicite la autorización previa, expresa e informada a que se refiere la Ley Estatutaria 1581 de 2012. Esta se puede obtenerse mediante cualquiera de los mecanismos autorizados por la ley y sus normas reglamentarias, pero el Responsable debe asegurarse de conservar copia de esta para suministrarla al Titular del dato cuando la requiera en virtud del literal b) del artículo 8 de la citada ley y para dar cumplimiento al literal b) del artículo 17 de la misma.	16 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN SENSIBLE	A.18. CUMPLIMIENTO.
PAZ RODRIGUEZ S.A.S	2019	El Responsable debe cumplir con las órdenes y requerimientos que imparta la SIC, relacionadas con posibles instrucciones o modificaciones solicitadas frente al Registro Nacional de Base de Datos.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
COLEGIO RAFAEL POMBO	2019	El Tratamiento de datos personales de menores de edad exige mayor responsabilidad y cuidado. Se deben implementar procesos de seguridad de la información, así como la adopción de un Manual Interno de Políticas y Procedimientos. El cumplimiento de estos debe ser monitoreado con el fin de garantizar que sean útiles, oportunas, idóneas, efectivas y demostrables.	17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES	A.18. CUMPLIMIENTO.
UNE EPM TELECOMUNICACIONES S.A	2019	No es necesario que el ciudadano presente más de una solicitud para que supriman o eliminen sus datos. Los derechos del Titular del dato deben garantizarse oportunamente. Los Responsables del Tratamiento deben obrar de manera muy profesional, diligente e implementar la responsabilidad demostrada (accountability) en esta materia.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
CASA EDITORIAL EL TIEMPO S.A CON SIGLA CEET S.A	2019	Las medidas de seguridad de los datos deben ser idóneas, oportunas, demostrables y efectivas cuando se realiza el tratamiento de esa información. No basta expedir documentos o	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		políticas, sino que es necesario asegurar que lo escrito en el papel se cumpla en la práctica.		
NSTALACIONES HIDROSANITARIAS FUENTES S.A.S	2019	El Responsable debe cumplir con las órdenes y requerimientos que imparta la SIC, relacionadas con posibles instrucciones o modificaciones solicitadas frente al Registro Nacional de Base de Datos.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
COLOMBIA TELECOMUNICACIONES S. A E.S.P	2019	COLOMBIA TELECOMUNICACIONES S.A. E.S.P. incluyó a la Titular del dato en una "lista negra"; actuación que está prohibida por constituir un ejercicio abusivo y desproporcionado de la facultad legal de administración de los datos personales, y que es contraria a los principios de libertad, finalidad y legalidad en el tratamiento de dichos datos, ya que constituye un uso no autorizado de la información de los ciudadanos.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
DIRECTV COLOMBIA LTDA	2019	DIRECTV COLOMBIA LTDA no demostró haber adoptado medidas apropiadas y efectivas para cumplir el principio y el deber de seguridad, pues permitió que un tercero no autorizado conociera información privada de otra persona. Por el contrario, sólo ha implementado medidas formales de seguridad, las cuales son insuficientes para garantizar un tratamiento seguro de los datos personales. Sin seguridad no existe debido tratamiento de datos personales y la seguridad no se logra con la mera redacción de políticas, sino con la implementación real de las mismas en todas las actividades que involucran tratamiento de datos personales.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
UBER	2019	UBER B.V. usa “cookies” para recolectar o tratar datos personales en el Territorio de la República de Colombia, las cuales instala en los equipos o dispositivos de las personas residentes o domiciliadas en Colombia, razón por la cual debe cumplir la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias. Por su parte, Uber Colombia S.A.S. realiza una actividad que involucra el Tratamiento de Datos Personales, en particular, utilizando los Datos de los usuarios de Uber para prestar sus servicios de publicidad. En esa medida, Uber Colombia S.A.S. es corresponsable del Tratamiento de Datos Personales de los usuarios de la plataforma en Colombia y, por tanto, debe ser muy responsable, diligente y muy profesional con el Tratamiento seguro de dichos datos.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
TRAVELS INTERNATIONAL S.A.S	2019	El responsable del tratamiento debe adoptar los procedimientos adecuados para solicitar y conservar la copia de la autorización del titular, e informar los datos que serán recolectados junto con las finalidades específicas, para los cuales se va a obtener el consentimiento del titular. Por otra parte, los Responsables deben acreditar el deber de desarrollar e implementar un manual para la atención de consultas y reclamos, un manual de políticas de seguridad y un manual para la recolección, uso almacenamiento circulación y supresión de la información.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
PAZ RAMÍREZ S.A.S	2019	Los Responsables del Tratamiento de datos de los ciudadanos tienen el deber de acatar de manera debida y oportuna las instrucciones que imparte esta Superintendencia - literal o) del artículo 17 de la Ley 1581 de 2012-. Omitir el cumplimiento de dichas órdenes, requerimientos o instrucciones es una actuación negligente e inaceptable que presta mérito para ser sancionado.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
AROLEDA Y CIA S.A.S	2019	Los Responsables del tratamiento, aun cuando no estén obligados a la inscripción de sus bases de datos en el RNBD, tienen que adoptar una política de TDP o de manera subsidiaria un aviso de privacidad que debe conocer el Titular a más tardar al momento de la recolección de sus datos personales, en concordancia con el principio de transparencia, que describa la política de TDP, y los mecanismos que permitan el ejercicio del derecho de habeas data.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.
PROMOTORA DEINVERSIONES Y COBRANZAS S.A.S	2019	La falta de controles sobre la veracidad de la información que le suministran terceros al Responsable del Tratamiento, puede generar el uso y circulación de información errónea. En caso en que se presente una falla de seguridad que afecte datos personales, los Responsables del Tratamiento deben implementar las medidas necesarias para remediar el incidente y mitigar los posibles efectos o consecuencias negativas para los Titulares concernidos, así como con las medidas correctivas para evitar que ese tipo de fallas vuelvan a suceder a futuro.)	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
ROMAL ARQUITECTURA Y CONSTRUCCIÒN S.A.S	2019	El responsable del tratamiento, aun cuando no esté obligado a la inscripción de sus bases de datos en el RNBD, tienen el deber de adoptar una política de TDP o de manera subsidiaria un Aviso de Privacidad que describa la existencia de esta y la forma de ejercer sus derechos, la cual se debe dar a conocer a los titulares, al momento de la recolección de sus datos personales, en concordancia con el principio de transparencia y legalidad.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.
CREACIONES IRUNA Y CIA. LIDA.	2019	El deber de informar por medio de un Aviso de Privacidad a los Titulares sobre la existencia de la política de tratamiento de datos personales se vulnera cuando no es oportuno, es decir, cuando no se realiza a más tardar al momento de la recolección de los datos personales, y es sancionable cuando la SIC imparte órdenes e instrucciones al respecto y el responsable las omite.	15 CONTRA EL RESPONSABLE - RESPECTO DEL AVISO DE PRIVACIDAD	A.18. CUMPLIMIENTO.
TCC S.A.S	2019	Transcribir o parafrasear lo que dice la ley no cumple con lo ordenado por el literal k) del artículo 17 de la Ley 1581 de 2012 porque en el Manual Interno se deben establecer las "políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley". Adicionalmente, lo mencionado en dicho Manual debe ser útil, oportuno, idóneo y demostrable para proteger los derechos de los Titulares de la información.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
CREDIMPORTACIONES BOGOTA LTDA	2019	El Responsable tiene el deber de solicitar la autorización previa, expresa e informada del Titular, antes de dar tratamiento a sus datos personales mediante llamadas a su teléfono celular, de igual manera, al momento de la recolección se debe informar la finalidad especifica del tratamiento.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
SABEL HENAO DE MENESES E HIJOS CIA S. EN C.	2019	Deber de implementar y desarrollar un Aviso de privacidad, para dar a conocer la existencia de políticas de tratamiento de información.	15 CONTRA EL RESPONSABLE - RESPECTO DEL AVISO DE PRIVACIDAD	A.18. CUMPLIMIENTO.
WORKING BUSINESS S.A.S	2019	Deber de contar con una autorización previa y expresa por parte de los titulares de la información, para no vulnerar su derecho a la autodeterminación informática y decidir sobre su tratamiento. Deber de adoptar una "política de tratamiento de datos personales" para garantizar la seguridad de la información.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
CAJA COLOMBIANA DE SUBSIDIO FAMILIAR - COLSUBSIDIO	2019	Deber de cumplir las observaciones y requerimientos realizados por la SIC, aportando prueba técnica de la supresión de la información del titular.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
IMPULSADORA HOTELERA Y TURISTICA LTDA. HOTURIS LTDA.	2019	Es deber de los Responsables de contar con una política (o manual) interno para la atención de consultas y reclamos que presenten los Titulares de la Información - literal k) del artículo 17 de la Ley 1581 de 2012-. Dicha política debe incluir un mecanismo de monitoreo para evaluar su efectividad en la práctica y cumplir el principio de responsabilidad demostrada (accountability)	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
AMERICAN BUSSINES S.A.S	2019	AMERICAN BUSSINES realizó el tratamiento de datos personales, sin acreditar que contaba con la autorización previa, expresa e informada del Titular; lo cual restringió su derecho a la autodeterminación informática y a decidir sobre el tratamiento de sus datos personales. Desde luego, el Responsable tampoco contaba con la copia de la autorización, pese a que esta se debe conservar mientras subsista en tratamiento.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
SAMARA REPRESENTACIONES HOTELERAS S.A.S	2019	SAMSARA REPRESENTACIONES HOTELERAS S.A.S. al momento de recolectar los datos personales de los titulares de manera virtual, no solicitó su autorización, ni informó las finalidades específicas del tratamiento. El Responsable debe dar respuesta oportuna a los requerimientos de la SIC, puesto que de lo contario estaría obstaculizando la facultad de inspeccionar y velar por el cumplimiento del Régimen de protección de datos personales.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
ASEGÚRATE FÁCIL LTDA	2019	Asegúrate Fácil LTDA no demostró que había solicitado y conservada prueba del consentimiento previo, expreso e informado del Titular para tratar los datos personales que le conciernen. El silencio, las casillas “pre marcadas” por defecto y la inacción no constituye consentimiento bajo la Ley 1581 de 2012. Al utilizarse herramientas en páginas web o aplicaciones tecnológicas, resulta imprescindible que el Responsable verifique que la persona que autorizará el Tratamiento es realmente quien dice	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.12. SEGURIDAD DE LAS OPERACIONES.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		ser y no que se trata de un tercero o de un suplantador de identidad.		
VIA PACIFICO S.A.S	2019	VÍA PACIFICO SAS debe informar las finalidades del Tratamiento de la información personal de los Titulares, en los formatos de autorización previa. Así mismo, en su política de tratamiento de DP debe señalar el periodo de vigencia de las bases de datos que utiliza dentro de sus operaciones.	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.
ENTIDAD PROMOTORA DE SALUD SERVICIO OCIIDENTAL DE SALUD S.A. SOS	2019	La Entidad Promotora de Salud Servicio Occidental de Salud S.A. SOS, no respondió de manera completa la solicitud del Titular del Dato. Dicha entidad, como Responsable del Tratamiento de la información de los ciudadanos, tiene el deber de atender y responder de manera completa, debida, de fondo y oportuna, las solicitudes de los Titulares de la información, conforme lo estable el artículo 17 de la Ley 1581 de 2012.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
TRAVELS LINE S.A.S	2019	El incumplimiento del deber de atender los requerimientos e instrucciones de la SIC referentes al tratamiento de datos personales; permite concluir que TRAVELS LINE SAS no cuenta con: a) una política de tratamiento de datos personales con los requisitos mínimos establecidos en la ley 1581 de 2012, b) no solicitó y ni conservó copia de la autorización del Titular para el tratamiento de datos personales c) tampoco acreditó la implementación de un manual de políticas de seguridad, ni un manual para la atención de consultas y reclamos.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
CAJA DE COMPENSACIÓN FAMILIAR COMFENALCO SANTANDER	2019	El principio de seguridad y confidencialidad se vulnera cuando se remite un correo electrónico que permite a una o varias personas ver o conocer las direcciones de correo electrónico de los destinatarios de dicho mensaje. En el tratamiento de datos personales de naturaleza pública se deben aplicar los principios rectores del artículo 4 de la ley 1581 de 2012, salvo los de libertad y confidencialidad.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
WINNER GROUP S.A	2019	La Autorización y/o consentimiento que exige la Ley 1581 de 2012 para el Tratamiento de los datos de los ciudadanos es calificado, esto es, debe ser previo, expreso e informado; características anteriores que deben acreditarse y demostrarse por el Responsable del Tratamiento aún en el supuesto de que dicho consentimiento sea otorgado por el Titular a través de conductas inequívocas, lo que en el caso concreto no demostró la sociedad Winner Group S.A. La autorización mediante conductas inequívocas también debe ser previa e informada.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
GRUPO REDDIAL S.A.S	2019	GRUPO REDDIAL SAS, no solicitó ni conservó copia de la autorización de los Titulares para el tratamiento de datos personales, situación que impide el ejercicio del derecho de autodeterminación informática en concordancia con el principio de libertad, según el cual los Titulares son quienes autorizan que su información personal sea incluida en alguna base de datos.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
STAR SEGUROS VIP LTDA	2019	El tratamiento de datos personales sólo puede ser autorizado por el Titular de estos para una finalidad específica, por lo tanto, el Responsable debe adoptar los procedimientos adecuados para solicitar y conservar copia de la autorización del Titular e informar los datos que serán recolectados junto con las finalidades de su uso.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
ENTIDAD PROMOTORA DE SALUD SAITAS S.A.S - E.P.S SANITAS S.A.S	2019	La adulteración del formulario de afiliación del Titular bajo custodia de la E.PS SANITAS S.A.S, sin su autorización, además de ilegal, constituye una vulneración al literal d) del artículo 16 de la Ley Estatuaria 1581 de 2012, que ordena "conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento". Una empresa que se dedica a la prestación del servicio de salud (derecho fundamental) como la E.P.S. Sanitas S.A.S., y que trata Datos de más de cuarenta y tres millones y medio (43'500.000) de personas, debe ser extremadamente diligente y garantizar la efectividad real (no formal) de los derechos de los Titulares de los Datos.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
PAYMENT SOLUTION S.A.S	2019	Deber de solicitar la respectiva autorización otorgada por el Titular: los Responsables no pueden conformar sus bases de datos a través del sistema de referidos, pues la autorización debe ser previa al tratamiento, y con el hecho de utilizar el número telefónico por primera vez se estaría realizando tratamiento del dato anterior al otorgamiento de la autorización.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
RAPPI S.A.S	2019	La autorización otorgada por el Titular en virtud del contrato laboral suscrito con el Responsable vulneró sus derechos de habeas data y autodeterminación informática, puesto que no autorizó de manera expresa la difusión de su imagen/fotografías para fines publicitarios. Por consiguiente, la autorización para el tratamiento de datos personales no debe generar confusión, por el contrario, dicho documento debe informar claramente los datos que serán recolectados y las finalidades del tratamiento	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
CREDIVALORES CREDISERVICIOS S.A	2019	Los datos personales no podrán ser obtenidos ni divulgados sin previa autorización del titular, o en ausencia de mandato legal o judicial que releve el consentimiento. Esto impide que la información ya registrada de un ciudadano, obtenida bajo su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos a los autorizados inicialmente, puesto que el titular tiene el derecho a determinar cuáles de sus datos dar a conocer como parte de su imagen corporativa.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
PREPAGO DE COLOMBIA PREPACOL S.A.S	2019	El Responsable debe cumplir las órdenes emitidas por la SIC referentes a la inscripción de las bases de datos en el Registro Nacional de Bases de Datos, así mismo es su deber atender de forma integral los requerimientos realizados por dicha autoridad.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
CONJUNTO RESIDENCIAL HACIENDA	2019	Los edificios de oficinas o conjuntos residenciales que se someten al régimen de propiedad horizontal son personas jurídicas Responsables del Tratamiento de los datos personales que	2 CONTRA EL RESPONSABLE - RESPECTO DE LA	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
PEÑALISA OCOBO		recolectan, almacenan o usan sobre todas las personas que ingresan a sus instalaciones. Por lo tanto, están obligados a obtener la autorización previa e informada de las personas de las cuales realicen tratamiento de datos, y deben demostrar que informaron todo lo que ordena el artículo 12 de la Ley 1581 de 2012.	AUTORIZACIÓN PARA EL TRATAMIENTO	

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[203] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2019[204].

Anexo B. Entidades con resolución sancionatoria año 2020

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
SCOTIABANK COLPATRIA S.A	2020	Es deber del Responsable del Tratamiento conservar copia de la autorización previa, expresa e informada otorgada por el Titular, para temas de prospección comercial, con el fin de demostrar que el Responsable está facultado para transferir información personal a sus aliados comerciales.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
INVERSIONES GODESTEA S A	2020	El Responsable del tratamiento debe responder a los requerimientos de la SIC de manera oportuna, demostrando el cumplimiento del Régimen de Protección de Datos Personales, con la descripción detallada de los procedimientos usados para la recolección de datos personales, y las finalidades de su uso.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
COLOMBIA MOVIL S.A. ESP	2020	El Responsable del Tratamiento debe garantizar el ejercicio del derecho de habeas data del Titular, a través de los canales de atención de quejas y reclamos que le permitan suprimir o revocar la autorización otorgada.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
AGRUPACION DE VIVIENDA RINCON DE MANDALAY	2020	El Responsable debe informar la finalidad del tratamiento de los datos personales del Titular al momento de la recolección y solicitud de autorización previa, expresa e informada. Así mismo debe informar los derechos que le asisten como Titular de la información.	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.
CONJUNTO RESIDENCIAL CIUDADELA PARQUE CENTRAL DE OCCIDENTE SEGUNDA ETAPA-PROPIEDAD HORIZONTAL	2020	El Responsable debe demostrar que cuenta con la autorización previa, expresa e informada otorgada por el Titular para el tratamiento de datos personales, e informar la finalidad de la recolección de manera clara y especifica.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

[203] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[204] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
AMARILO S.A.S.	2020	La Autorización y/o consentimiento que exige la Ley 1581 de 2012 para el Tratamiento de los datos de los ciudadanos es calificado, esto es, debe ser previo, expreso e informado; características anteriores que no fueron acreditadas por la sociedad AMARILLO S.A.S. En particular, porque no demostró haber conservado en condiciones óptimas y verificables, copia de la Autorización que en su momento hubiera otorgado el Titular de la información para el debido Tratamiento de sus Datos.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
ALMACENES EXITO S.A.	2020	Los Responsables y Encargados deben garantizar el ejercicio del derecho de habeas data y el derecho de petición de los Titulares sin dilaciones ni atrasos, de manera completa y de fondo; atendiendo efectivamente y de forma oportuna las solicitudes de supresión de información en todas sus bases de datos.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
CREDIVALORES - CREDISERVICIOS S.A	2020	El derecho de habeas data otorga la facultad al Titular de los datos personales de exigir el acceso, corrección, actualización y eliminación de su información personal, por lo que se deben tramitar las peticiones de fondo por parte de los Responsables del Tratamiento respecto de los datos y direcciones de correo electrónico asociados al registro individual de los Titulares.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
GENERAL SERVICE DE COLOMBIA S.A.S	2020	El Responsable de la información debe solicitar la autorización previa, expresa e informada del Titular previamente al tratamiento de sus datos personales por lo cual, no puede realizar llamadas telefónicas para solicitar datos personales sin antes haber obtenido la debida autorización.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
EXPEDIENTES SAS	2020	El Responsable debe garantizar el ejercicio del derecho de habeas data del Titular a través del derecho de petición mediante el cual los Titulares ejercen el control sobre el manejo de sus datos personales.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
COPERATIVA AUTONOMA DE SEGURIDAD C.T.A. COAUTOMA C.T.A.	2020	El Responsable debe desarrollar y documentar un manual interno a través del cual se describan los procedimientos para garantizar la seguridad en la custodia de la información personal incluyendo archivos físicos, digitales y magnéticos.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
CRC OUTSOURCING S.A.S.	2020	La recolección, uso, circulación y el tratamiento de los datos personales privados, semiprivados y sensibles sólo puede realizarse cuando exista la autorización previa, expresa e informada del Titular, tal y como lo establece el principio de libertad definido en el literal c) del artículo 4 de la Ley 1581 de 2012. La sociedad OUTSOURCING S.A.S. actuó ilegalmente, porque no acreditó dicha autorización -artículo 9 de la Ley 1581 de 2012-	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
PROPIEDAD HORIZONTAL CONJUNTO RESIDENCIAL PLAZUELAS DE SANTA ANA	2020	El Responsable tiene el deber de tratar la información que se encuentra almacenada en su base de datos bajo medidas de seguridad idóneas, que garanticen la custodia de los datos personales que tiene a su cargo, por lo cual se deben establecer las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros y datos personales de los residentes y propietarios.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
FITNESS PEOPLE CENTRO MÉDICO DEPORTIVO S.A.S	2020	El Responsable no atendió de manera oportuna y dentro de los 10 días hábiles siguientes la petición presentada por la Titular, vulnerando su derecho fundamental de habeas data. Aunque atendió la integridad de las peticiones, no cumplió con el termino legal impidiéndole al Titular conocer, actualizar y rectificar su información personal.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
BANCO POPULAR S.A	2020	El Responsable vulnero el ejercicio del derecho de habeas data al no atender oportunamente su solicitud de supresión de datos personal con el fin de no continuar recibiendo mensajes de texto y correos electrónicos de prospección comercial, tampoco otorgo respuesta en el término legal a la solicitud de supresión.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
SODIMAC COLOMBIA S.A.	2020	La autorización mediante conductas inequívocas es jurídicamente válida siempre y cuando sea previa e informada. SODIMAC COLOMBIA S.A. no cumplió con el deber de informar al Titular todo lo que ordena la ley, razón por la cual la autorización que manifiesta haber obtenido no	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		cumple los requisitos legales. Los avisos de privacidad no suplen la autorización previa, expresa e informada del Titular de la información. No es una buena práctica en materia de tratamiento de datos personales utilizar mecanismos de obtención del consentimiento en los que tenga el mismo efecto que la persona ACEPTE o NO ACEPTE. No es sensato que dé lo mismo aceptar o no aceptar. Eso es irrespetuoso con los seres humanos porque no importa la autonomía de las personas, ni su voluntad.		
MADERFORMAS SAS	2020	El Responsable incumplió con el deber de cumplir con los requerimientos e instrucciones que imparta la SIC de manera oportuna, al no dar atender la orden impartida de cargar los archivos de RNBD sin clave de lectura.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
CONJUNTO RESIDENCIAL PARQUE CENTRAL BONAVISTA ETAPA II PROPIEDAD HORIZONTAL	2020	El Responsable debe dar trámite a las consultas y reclamos realizadas por el Titular frente al tratamiento de su información personal contenida en bases de datos, que considere que debe ser objeto de corrección actualización o supresión.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
GRUPO INNOVA INTERNATIONAL S.A.S	2020	Las direcciones de correo electrónico que se encuentren a disposición del público deben ser tratadas con posterioridad a la solicitud de autorización, previa, expresa e informada del Titular, especialmente cuando son obtenidas mediante referidos recomendados por terceros.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
CONJUNTO RESIDENCIAL ALMEIRA TORRES 1,2,3,4 Y 5 PROPIEDAD HORIZONTAL	2020	El Responsable debe solicitar la autorización, previa, expresa e informada de los Titulares antes de realizar el tratamiento de sus datos personales como el envío de correos electrónicos masivos, y conservar copia de esta, así mismo debe informar al momento de la recolección la finalidad específica del tratamiento.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
EDITORA RED PREFERENCIAL S.A.S.	2020	Las Sociedades deben implementar un mecanismo efectivo para obtener la autorización previa expresa e informada de los Titulares; y suprimir, de manera definitiva, de sus bases de datos la totalidad de los datos personales que no hayan sido obtenidos y tratados con el consentimiento de su respectivo Titular.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
COMSERVICE ASISTENCIA S.A.S	2020	Las Sociedades deben implementar un mecanismo efectivo para obtener la autorización previa expresa e informada de los Titulares; y suprimir, de manera definitiva, de sus bases de datos la totalidad de los datos personales que no hayan sido obtenidos y tratados con el consentimiento de su respectivo Titular.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
GENERAL SERVICE DE COLOMBIA S.A.S	2020	La Responsables deben informar previamente a los Titulares sobre las finalidades del tratamiento de la información y adoptar un Manual de Políticas de seguridad con las medidas apropiadas y efectivas para que la información de los Titulares permanezca bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado.	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.
CCG SOLUCIONES SAS	2020	Las Sociedades deben suprimir, de manera definitiva, de sus bases de datos la totalidad de los datos personales que no hayan sido obtenidos y tratados con el consentimiento de su respectivo Titular y adoptar un Manual de Políticas de seguridad para evitar el acceso de terceros no autorizados.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
SOLUCIONES VIDA FÁCIL SAS	2020	Información personal como el número telefónico, dirección de residencia y datos de la tarjeta de crédito son datos semiprivados, que requieren autorización previa, informada y expresa del Titular, la cual debe ser de consulta posterior, antes de realizar el tratamiento	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
PROVINCIA DE NUESTRA SEÑORA DEL ROSARIO DE LA CONGREGACIÓN DE DOMINICAS DE SANTA CATALINA DE SENA - COLEGIO NUESTRA SEÑORA DEL ROSARIO FUNZA	2020	Es deber del Responsable realizar todos los actos tendientes a obtener la autorización para el tratamiento de datos personales por parte del Titular, y conservar prueba de esta, independientemente del medio por el que se recolectó.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
BANCO DE BOGOTÁ S.A	2020	El Responsable debe abstenerse de hacer uso del sistema de referidos para hacer gestiones de cobros de obligaciones de terceros, sin contar con la autorización previa, expresa e informada, puesto que el tratamiento de los datos de referidos consiste en verificar la identidad de sus contratantes y su comportamiento con las obligaciones adquiridas.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
MARÍA FERNANDA MARTÍNEZ PORTILLA -HOTEL VILLA DE LEYVA PLAZA	2020	Los Responsables del tratamiento deben atender los diferentes llamados de la Superintendencia y demostrar el cumplimiento de los deberes de protección de datos personales, a través de los requerimientos, ordenes e instrucciones que emite la entidad.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
ALMACENES ÉXITO E INDUSTRIAS ÉXITO S.A.S	2020	El Responsable debe contar con la autorización previa, expresa e informada del Titular antes de suministrar información al Encargado, la cual debe ser de consulta posterior, por lo que el uso de aplicaciones electrónicas debe ajustarse a los parámetros de tratamiento de datos personales, garantizando la opción de autorización expresa del TDP	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
ÉXITO INDUSTRIAS S.A.S.	2020	El Encargado debe garantizar el ejercicio del derecho de habeas data del Titular, con mecanismos gratuitos, útiles, de fácil acceso y efectivos que le permitan solicitar la supresión de la dirección de correo electrónico, y resolver oportunamente y de fondo sus quejas y reclamos de supresión o revocatoria de la autorización.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
GIROS & FINANZAS COMPAÑÍA DE FINANCIAMIENTO S.A.	2020	El Responsable debe garantizar el ejercicio del derecho de supresión de la información de sus bases de datos, cuando el Titular solicite la eliminación de sus datos personales para fines publicitarios o de prospección comercial de manera inmediata, y con certeza de la fecha en que se ejecutó la eliminación.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
IMPERIAL TOUR S.A.S.	2020	Los Responsables deben garantizar el cumplimiento de las ordenes de eliminación de datos personales que emite la SIC, mediante procedimientos de eliminación de datos personales efectivos debidamente certificados, en aras de evitar que se vulnere reiteradamente el derecho fundamental de habeas data.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
COBROACTIVO S.A.S.	2020	Los Encargados del tratamiento deben garantizar el ejercicio del derecho de habeas data y de petición, suministrando una solución dotada de claridad y congruencia entre lo pedido y lo resuelto, que la respuesta sea oportuna y que sea puesta en conocimiento del Titular. De igual forma, el Encargado debe informarle al interesado acerca del traslado de la solicitud al Responsable.	23 CONTRA EL ENCARGADO - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
COOPERATIVA BELEN AHORRO Y CRÉDITO	2020	Los canales dispuestos para la atención de quejas y reclamos no deben crear barreras para el ejercicio de los derechos de los Titulares, pues los procedimientos deben ser accesibles para que el ejercicio del derecho de habeas data sea real y efectivo y no formal y solemne.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
TENNIS S.A. EN REORGANIZACIÓN	2020	El Responsable debe solicitar la autorización previa, expresa e informada del Titular, para el envío de prospección comercial a su dirección de correo electrónico personal y al número de línea móvil. De igual manera, debe garantizar el ejercicio del derecho de habeas del Titular y respetar su voluntad en cuanto no continuar recibiendo publicidad.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
ACIERTOS RECREATIVOS S.A.S.	2020	El Responsable debe tener especial cuidado frente al tratamiento de datos personales de menores de edad, por lo que debe solicitar la autorización previa, expresa e informada de sus representantes legales e informar las finalidades específicas del tratamiento, como es el caso del uso de fotografías de menores con fines publicitarios, en virtud del derecho de seguridad y privacidad.	17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES	A.18. CUMPLIMIENTO.
TOUR VACATION HOTELES AZUL S A S	2020	El Responsable debe garantizar el derecho a la supresión y rectificación de la información personal de los Titulares, con procedimientos efectivos de eliminación de datos personales que impidan el envío de información de prospección comercial no deseada, o información personal de terceros no autorizados.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
RAPPI S.A.S.	2020	Los Responsables deben garantizar el derecho de habeas data de los Titulares en cuanto a la supresión de sus datos personales de manera diligente, efectiva y oportuna, sin que el Titular deba insistir sobre el respeto de sus derechos con más de una solicitud.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
CONJUNTO RESIDENCIAL EL TESORO I-PROPIEDAD HORIZONTAL	2020	Los Responsables deben adoptar medidas apropiadas y pertinentes para evitar que los correos electrónicos personales sean difundidos masivamente y conocidos indiscriminadamente por todos los destinatarios. Es necesaria la implementación de medidas de seguridad para impedir la consulta y acceso no autorizado.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
BANCA DE SERVICIOS FINANCIEROS SAS	2020	Los Encargados deben implementar y poner en conocimiento de sus trabajadores las medidas de seguridad necesarias para evitar el envío de correos electrónicos masivos con información personal registrada en sus bases de datos a terceros no autorizados, que expongan dicha información a riesgos de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
FONDO DE EMPLEADOS GRANFONDO - FEG	2020	Los Responsables deben exigir a los Encargados el respeto en todo momento a las condiciones de seguridad y privacidad de la información del Titular; garantizando que la misma sea manejada con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros. Por otra parte, debe informar a la Autoridad de Protección de Datos los eventos en que se presenten violaciones a los códigos de seguridad y posibles riesgos en la administración de datos personales.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
SCOTIABANK COLPATRIA S.A	2020	Es deber del Responsable del Tratamiento garantizar, en todo tiempo el pleno y efectivo goce del derecho fundamental de habeas data a los Titulares de la información, atendiendo efectivamente las solicitudes de supresión de información en sus bases de datos, sin que el Titular deba reiterar sus solicitudes por diferentes medios electrónicos por falta de diligencia por parte del Responsable.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
CASA EDITORIAL EL TIEMPO S A	2020	Los Responsables deben adoptar procedimientos, políticas y medidas idóneas para la atención de consultas y reclamos relacionadas con el ejercicio del derecho de Habeas Data. Las peticiones sobre supresión de datos personales y revocación de autorización del tratamiento se deben contestar oportunamente y de manera precisa, suprimiendo la información personal en el momento en que el Titular lo solicite con eficacia real y verificable.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
CÁMARA DE COMERCIO DE BOGOTÁ	2020	En virtud del principio de confidencialidad, los Responsables deben mantener la reserva de los datos personales que no son considerados públicos, a través de medidas de seguridad efectivas e idóneas, con el propósito de evitar la filtración de información mediante correos electrónicos masivos, que permiten el acceso y consulta por parte de terceros no autorizados.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
FARROW COLOMBIAS.A.	2020	El Responsable del tratamiento debe atender a los requerimientos impartidos por la autoridad de protección de datos personales de manera oportuna y cumplir con las instrucciones (ordenes) impartidas por las autoridades de seguimiento y vigilancia por mandato legal.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
FARROW MÉXICO S.A.P.I. de C.V	2020	Los Responsables de las aplicaciones deben implementar mecanismos para solicitar la autorización previa, expresa e informada de los Titulares antes de su registro. Es inadmisible la incorporación de datos personales con solo un "clic" sin informar, al momento de la recolección, la finalidad del tratamiento. Así mismo, deben ser especialmente diligentes en la solicitud y conservación de las autorizaciones de los representantes legales de menores de edad y advertir acerca del carácter facultativo en el otorgamiento de datos sensibles o datos de menores de edad.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
FARROW VENTURES INC	2020	Titulares antes su registro. Es inadmisible la incorporación de datos personales con solo un "clic" sin informar al momento de la recolección la finalidad del tratamiento. Así mismo, deben ser especialmente diligentes en la solicitud y conservación de las autorizaciones de los representantes legales de menores de edad y advertir acerca del carácter facultativo en el otorgamiento de datos sensibles o datos de menores de edad.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
A2P COLOMBIA S.A.S.	2020	Frente al tratamiento de números telefónicos de los usuarios que han solicitado la portabilidad de su número de un operador de telefonía a otro, al ser éste un dato semiprivado que no es público se debe solicitar y conservar la autorización previa, expresa e informada de los Titulares antes de realizar labores de marketing mediante el acceso a bases de datos con información personal. El Responsable del tratamiento de datos personales viola el Régimen General de Datos Personales cuando no ha adoptado una Política de Tratamiento de Datos, no ha documentado e implementado un Manual de Seguridad de la información y cuando incumple las instrucciones impartidas por la Autoridad de Protección de Datos Personales	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[205] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2020.[206]

Anexo C. Entidades con resolución sancionatoria SIC 2021

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
INVESMENT DE COLOMBIA S.A.S	2021	Las Responsables del tratamiento deben cumplir con los siguientes deberes:1. El deber de solicitar y conservar, copia de la respectiva autorización otorgada por el Titular de la información para el tratamiento de su información personal.2. Informar a los Titulares sobre la finalidad de la recolección y los derechos que les asisten en virtud de la autorización otorgada.3. Deber de tramitar las peticiones presentadas por los titulares de forma oportuna. 4. Deber de contar con un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581 del 2012 y, en especial, para la	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.

[205] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[206] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		atención de consultas y reclamos. 5. Deber de cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio, dando respuesta a los requerimientos y órdenes impartidas por la autoridad de protección de datos personales.		
COOPERATIVA DE AHORRO Y CRÉDITO DE TRABAJADORES DE GOODYEAR DE COLOMBIA	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, las órdenes que se emitan son de obligatorio cumplimiento dentro del plazo establecido por la autoridad, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
FUNDACIÓN MI ALEGRE INFANCIA	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada al tratamiento de datos personales en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de Datos Personales que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos que señale los términos de Ley para que los Titulares hagan efectivo su derecho a habeas data y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
CARDIO GLOBAL LTDA.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo que deben atender las instrucciones y requerimientos efectuados por la Autoridad Nacional de Protección de Datos Personales, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos, así pues, los Responsables y Encargados deben acatar las órdenes impartidas por esta Superintendencia y demostrar el cumplimiento de los deberes a los que se encuentran obligados.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
CONFIABONOS S.A.S	2021	Los Responsables deben garantizar al Titular el derecho que le asiste de solicitar la supresión de su información personal almacenada en sus bases de datos, página web, redes sociales -Facebook e Instagram- y en la Plataforma YouTube, de modo que el derecho de habeas data no sea un asunto meramente formal, sino enteramente material, por lo cual, debe llevarse a cabo la supresión de los datos solicitados por el Titular de forma inmediata. Así mismo, en desarrollo de sus derechos a la	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		autodeterminación informática, los titulares son quienes de forma expresa deben autorizar que la información que sobre ellos sea recaudada pueda ser incluida en una base de datos. Finalmente, la obligación del Responsable del Tratamiento no cesa con la simple resolución del derecho de petición elevado por el titular de la información, es necesario además que dicha solución resuelva sin confusiones el fondo del asunto; que esté dotada de claridad y congruencia entre lo pedido y lo resuelto; e igualmente, que su oportuna respuesta se ponga en conocimiento del solicitante.		
GRAFIVISIÓN EDITORES S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo que deben atender las instrucciones y requerimientos efectuados por la Autoridad Nacional de Protección de Datos Personales, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos, así pues, los Responsables y Encargados deben acatar las órdenes impartidas por esta Superintendencia y demostrar el cumplimiento de los deberes a los que se encuentran obligados.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
URBANIZACIÓN COLORS P.H	2021	Las propiedades horizontales en calidad de Responsables del tratamiento deben cumplir con los siguientes deberes:1. El deber de solicitar y conservar, copia de la respectiva autorización otorgada por el Titular de la información para el tratamiento de su información personal.2. Informar a los Titulares sobre la finalidad de la recolección y los derechos que les asisten en virtud de la autorización otorgada.3. Deber de tramitar las peticiones presentadas por los titulares de forma oportuna. 4. Deber de contar con un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581 del 2012 y, en especial, para la atención de consultas y reclamos. 5. Deber de cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio, dando respuesta a los requerimientos y órdenes impartidas por la autoridad de protección de datos personales.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
CLÍNICA REYES S.A.S.	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada al tratamiento de datos personales en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de Datos Personales que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos que señale los términos de Ley para que los Titulares hagan	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		efectivo su derecho a habeas data y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.		
ESTRIOS S.A.S.	2021	Mediante la recolección de datos privados y/o sensibles a través de formularios y páginas web, se debe requerir y demostrar la autorización previa expresa e informada del Titular, dándole a conocer las finalidades específicas del tratamiento. Así mismo la información personal recolectada en físico o por internet debe ser almacenada bajo estrictas condiciones de seguridad, así mismo se debe poner a disposición de los Titulares las Política de Tratamiento de Datos Personales	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
MIRO SEGURIDAD LTDA	2021	La obligación del Encargado del Tratamiento no cesa con la simple resolución del derecho de petición elevado por el titular de la información, es necesario además que dicha respuesta remedie sin confusiones el fondo del asunto; que este dotada de claridad y congruencia entre lo pedido y lo resuelto; e igualmente, que su oportuna respuesta se ponga en conocimiento del solicitante.	27 CONTRA EL ENCARGADO - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
INVERSIONES E2 S.A.S	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo que deben atender las instrucciones y requerimientos efectuados por la Autoridad Nacional de Protección de Datos Personales, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos, así pues, los Responsables y Encargados deben acatar las órdenes impartidas por esta Superintendencia y demostrar el cumplimiento de los deberes a los que se encuentran obligados.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
SUEÑO ESTÉREO S A S	2021	La autorización para el tratamiento de datos personales capturados en el lector de huella y de niños, niñas y adolescentes, debe cumplir con el requisito de ser informada e indicar las finalidades de su uso, específicamente i) el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes ii) Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento. Los Responsables deben implementar manuales de políticas de seguridad y del ciclo del dato, en el que se describan los procedimientos usados para la recolección, uso, circulación de la información almacenada en sus bases de datos.	17 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES	A.18. CUMPLIMIENTO.
ALMACENES ÉXITO S.A.	2021	El derecho de habeas data, otorga la facultad al Titular de los datos personales de exigir el acceso, corrección, adición, actualización y eliminación de su información, por lo que, los Responsables del Tratamiento, deben proceder de conformidad, implementando las medidas y procedimientos claros, dirigidos a la protección de los datos personales y su adecuado tratamiento, garantizando al Titular de la información el libre acceso y el cumplimiento de las solicitudes que el mismo	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		efectúe respecto de su información, de modo que la supresión de sus datos personales se haga de forma inmediata.		
AEROVÍAS DE INTEGRACIÓN REGIONAL S A	2021	Es un deber de los Responsables y Encargados del Tratamiento garantizar el ejercicio del derecho de hábeas data, el derecho de petición, consulta o reclamación, mediante la atención cada una de las solicitudes de los titulares, sin dilaciones ni retrasos, de manera que las peticiones a través de la red social Facebook, se deben responder a través del mismo medio o gestionar internamente dentro de la compañía para que el área o persona encargada atiendan las solicitudes de los Titulares, al ser esta red social un canal idóneo para la presentación de peticiones, más aún cuando las compañías tiene habilitadas en Facebook las opciones para recibir y enviar comunicaciones. Por otra parte, se deben adoptar medidas de seguridad humanas, técnicas y administrativas necesarias para evitar el uso, consulta o acceso no autorizado de datos personales mediante el envío masivo de correos electrónicos.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
ICL INGENIERÍA DE CORROSIÓN LTDA	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo que deben atender las instrucciones y requerimientos efectuados por la Autoridad Nacional de Protección de Datos Personales, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
CICOMARG - DISTRIBUCIONES S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, las órdenes que se emitan, son de obligatorio cumplimiento dentro del plazo establecido por la autoridad, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
RAPPI S.A.S.	2021	En la Sanción impuesta contra RAPPI S.A.S. se analizó lo siguiente: 1. El deber de garantizar el ejercicio del derecho constitucional al habeas data se concreta cuando el Titular interpone una petición entendida como el medio idóneo para solicitar el amparo efectivo del derecho de los titulares a conocer, actualizar y rectificar la información contenida en las bases de datos públicas y privadas. Por su parte, el deber de tramitar las consultas y reclamos se concreta cuando el ciudadano presenta un reclamo cuya pretensión radica en la supresión de su información personal de la base de datos de la investigada. 2. Es claro que, el ejercicio del derecho fundamental de habeas data permite al Titular requerir la exclusión de información que haya sido recogida en bases de datos, pues este podrá solicitar la supresión del dato, cuando no exista una obligación legal o contractual que imponga el deber de permanecer en la referida base de datos. 3.Aceptar los términos y condiciones o la Política de Tratamiento de la Información no es imperativo para el Titular, ni releva al Responsable del Tratamiento del deber de obtener la autorización previa, expresa e	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		informada por parte de este para el tratamiento de sus datos personales.		
COLOMBIA MÓVIL S A E S P	2021	Los Responsables deben garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, atendiendo las solicitudes de supresión de datos personales de sus bases de datos de manera oportuna; así mismo deben desarrollar, implementar y mantener controles de seguridad que permitan garantizar los estándares de protección consagrados en la Ley estatutaria e informar sin dilación a la Autoridad de Protección de Datos y a los Titulares cuando se presenten incidentes que afecten la confidencialidad, disponibilidad o integridad de los mismos.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
PALMERAS BARBASCAL S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo que deben atender las instrucciones y requerimientos efectuados por la Autoridad Nacional de Protección de Datos Personales, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos, así pues, los Responsables y Encargados deben acatar las órdenes impartidas por esta Superintendencia y demostrar el cumplimiento de los deberes a los que se encuentran obligados.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
ALCALDÍA MAYOR DEL DISTRITO DE BOGOTÁ D.C	2021	Los Responsables y/o Encargados deben actuar con diligencia y cuidado reforzados, frente al Tratamiento de datos personales sensibles, cuya titularidad recae sobre ciudadanos mayores, niños, niñas y adolescentes, utilizando las mejores medidas-humanas, técnicas y administrativas- de seguridad para restringir el acceso, asegurar la confidencialidad, y evitar la circulación de la información personal sensible de salud, incluyendo la relacionada con el control epidemiológico y clínico -historial de vacunación-. De modo que, siempre que se desarrollen nuevas aplicaciones o tecnologías en las que se realice Tratamiento de información personal, se debe incorporar la Privacidad como principio y piedra angular dentro de los procesos de diseño -Privacidad desde el Diseño (PbD)-, y se deben adoptar mecanismos que garanticen el Tratamiento únicamente de los datos que sean necesarios, adecuados y pertinentes para los fines propuestos, y que la extensión de dicho Tratamiento sea estrictamente la necesaria -Privacidad por Defecto (PDpD)-.	16 CONTRA EL RESPONSABLE - RESPECTO DE LA INFORMACIÓN SENSIBLE	A.12. SEGURIDAD DE LAS OPERACIONES.
CMS COLOMBIA LTDA. CORPORACIÓN MÉDICA SALUD PARA LOS COLOMBIANOS	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada al tratamiento de datos personales en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de Datos Personales que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos que señale los términos de Ley para que los Titulares hagan efectivo su derecho a habeas data y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.		
ACEVEDO Y ABOGADOS ASOCIADOS S.A.S.	2021	Deber de comunicar al Titular previamente a efectuar el reporte ante los operadores de la información: La finalidad de esta comunicación es que el Titular pueda realizar el pago de la obligación, así como controvertir aspectos como el monto de la obligación, la cuota o la fecha de exigibilidad; también es una herramienta para actualizar y rectificar sus datos personales. Por consiguiente, la fuente de la información debe adecuar y/o implementar procedimientos con el fin de cumplir con el envío de la comunicación previa según lo establecido en la ley antes de realizar el reporte negativo.	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.
DISTRIBUIDORA LOS COCHES LA SABANA S.A.S	2021	DISTRIBUIDORA LOS COCHES LA SABANA S.A.S. adoptó medidas encaminadas a garantizar la confidencialidad y seguridad de la información; no obstante, estas fueron insuficientes en consideración a que no evitaron la ocurrencia del uso no autorizado de los datos personales del Titular y su divulgación, por lo cual, las medidas implementadas no fueron pertinentes, útiles y efectivas para prevenir el error humano que propició la vulneración del derecho de habeas data y el incidente de seguridad.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
GRUPO VIVIR SUCRE S.A.S.	2021	Así las cosas, es claro para esta Dirección que la consulta realizada por GRUPO VIVIR SUCRE S.A.S. el día 01 de abril de 2019 al historial crediticio del titular contenido en el portal MiDatacredito.com, se realizó de forma indebida sin contar con su autorización, ni acreditar que la sociedad investigada estuviera cobijada por una de las finalidades descritas en el artículo 15 de la Ley 1266 de 2008.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
INVERSIONES AMBER S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo que deben atender las instrucciones y requerimientos efectuados por la Autoridad Nacional de Protección de Datos Personales, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
AGRUPACIÓN DE VIVIENDA RINCÓN DE MANDALAY - PROPIEDAD HORIZONTAL	2021	Los Responsables deben cumplir con el deber de informar la finalidad de la recolección y los derechos que le asisten a los Titulares frente al tratamiento de los datos personales, incluso si están eximidos de solicitar la autorización previa en cumplimiento de un mandato legal. De igual modo, los Responsables deben implementar una Política de Tratamiento de Datos Personales que cumpla con los siguientes requisitos mínimos; (i) nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable (ii)	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		informar al Titular su derecho a presentar quejas ante la SIC (iii) mencionar la fecha de su entrada en vigencia; (iv) mencionar el periodo de vigencia de las Bases de Datos de la sociedad; (iii) los derechos que le asisten como Titular; (iv) la identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento		
CONJUNTO RESIDENCIAL PARQUES DE PRIMAVERA I ETAPAS I Y II PROPIEDAD HORIZONTAL	2021	El Responsable debe solicitar y conservar copia de la autorización previa, expresa e informada de los Titulares para el Tratamiento de los datos que recolecta a través de los formularios que usan en sus plataformas digitales, formatos físicos diligenciables, y sistema de video vigilancia. De igual manera, al momento de la recolección se debe informar a los Titulares las finalidades del uso de su información y los derechos que les asisten, prohibiendo así la recopilación de datos sin la especificación clara acerca de su finalidad. Política de Tratamiento de Datos Personales y un manual interno de políticas y procedimientos para: (i) la atención de consultas y reclamos; y (ii) para el ciclo del dato desde la recolección, desde la recolección, almacenamiento, uso, y disposición final.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
Q10 SOLUCIONES S.A.S.	2021	En virtud del principio de seguridad los Responsables del Tratamiento deben adoptar las medidas de seguridad que describan las medidas humanas técnicas y administrativas para garantizar que la información administrada nos sea divulgada, adulterada, consultada o expuesta de manera inconsulta o no autorizada por su Titular; así mismo deben adoptar un manual interno donde se encuentren los procedimientos para la recolección, almacenamiento, uso, circulación de la información durante el tiempo que sea razonable y necesario de acuerdo con las finalidades que justificaron el tratamiento hasta el momento de la supresión del dato.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
CAJA DE COMPENSACIÓN FAMILIAR DEL HUILA	2021	El deber de veracidad del dato implica que la información que suministre la Fuente a los Operadores de los bancos de datos sea veraz, completa, exacta, actualizada y comprobable, puesto que está destinada a ofrecer a terceros datos útiles para el cálculo de riesgo crediticio. Por otra parte, la Fuente deberá informar al Operador que determinada información se encuentra en discusión por parte del Titular, cuando se haya presentado la solicitud de rectificación o actualización, con el fin de que se incluya en el banco de datos una mención en ese sentido hasta que finalice dicho trámite.	10 CONTRA EL RESPONSABLE - RESPECTO DE LA INSCRIPCIÓN DE LA LEYENDA	A.18. CUMPLIMIENTO.
CAJA DE COMPENSACIÓN FAMILIAR DEL HUILA	2021	Deber de comunicar al Titular previamente a efectuar el reporte ante los operadores de la información: La finalidad de esta comunicación es que el Titular pueda realizar el pago de la obligación, así como controvertir aspectos como el monto de la obligación, la cuota o la fecha de exigibilidad; también es una herramienta para actualizar y rectificar sus datos personales. Por consiguiente, la fuente de la información debe adecuar y/o implementar procedimientos con el fin de cumplir con el envío de la comunicación previa según lo establecido en la ley antes de realizar el reporte negativo.	11 CONTRA EL RESPONSABLE - RESPECTO DEL DEBER DE INFORMAR A LOS TITULARES COMO SE ESTÁ UTILIZANDO SU INFORMACIÓN	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
BIMBO DE COLOMBIA S.A.	2021	Es un deber de los Responsables y Encargados del tratamiento garantizar el ejercicio del derecho de habeas data, para que los titulares conozcan cuáles de sus datos personales han sido recolectados en diferentes bases de datos y el uso que se está haciendo de los mismos; de igual manera, se debe garantizar el pleno y efectivo ejercicio del derecho de petición, consulta o reclamación, atendiendo cada una de las preguntas y solicitudes de los titulares, sin dilaciones ni atrasos, de manera completa y de fondo.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.
CAJIAO OSPINA & CIA S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, las órdenes que se emitan tendientes a la implementación de medidas necesarias para el tratamiento, o las relacionadas con el registro sus bases de datos y la información relacionada con la Política de seguridad en el Registro Nacional de Bases de Datos son de obligatorio cumplimiento dentro del plazo establecido por la autoridad, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
BYLANX S.A	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada al tratamiento de datos personales en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento Personales que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inicio el tratamiento de datos personales y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
OCUPAR TEMPORALES S.A	2021	La regulación en materia de protección de datos personales, exige contar con la autorización previa, expresa e informada del Titular, ya que esta es la expresión de la voluntad inequívoca otorgada por el mismo para que sus datos personales sean recolectados, ingresen a la base de datos y se utilicen para los fines que fueron autorizados pues, de lo contrario, se estaría afectando, el derecho a la autodeterminación informática entendido como el núcleo esencial del derecho al habeas data y, en la práctica, el Titular perdería el control de sus datos personales.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
EL MICO INTERVENTOR S.A.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, las ordenes que se emitan tendientes a la implementación de medidas necesarias para el tratamiento, o las relacionadas con el registro sus bases de datos y la información relacionada con la Política de seguridad en el Registro Nacional de Bases de Datos son de obligatorio cumplimiento dentro del plazo establecido por la autoridad, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
DISTRIBUIDORA NISSI E U	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo que deben atender las instrucciones y requerimientos efectuados por la Autoridad Nacional de Protección de Datos Personales, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
TU CONSULTA COLOMBIA S.A.S.	2021	Respecto de los datos personales que son susceptibles de Tratamiento, independientemente de que sean públicos, privados o semiprivados, el Responsable debe informar las finalidades del Tratamiento al Titular de la información, al momento de la recolección y otorgamiento de la autorización previa, expresa e informada. En este sentido, los formularios de sitios web que soliciten información personal deben informar la finalidad del tratamiento a personar naturales que ejercen actividades comerciales.	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.
CÁMARA DE COMERCIO DE VILLAVICENCIO	2021	El Responsable del tratamiento debe solicitar al Titular de la información la respectiva autorización previa, expresa e informada, por lo que, todo formulario publicado en el sitio web de la sociedad debe implementar la solicitud expresa de la autorización para el tratamiento de datos personales. De igual forma, dicha solicitud debe informar las finalidades del tratamiento y los derechos que le asisten al Titular, y solo podrá ser recolectada aquella información que sea imprescindible para cumplir la finalidad del tratamiento. Por otra parte, la implementación de medidas en materia de protección de datos personales por parte de la sociedad, con posterioridad al incumplimiento que dio origen a la investigación administrativa, no la exonera de responsabilidad.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
CÁMARA DE COMERCIO DE CÚCUTA	2021	El Responsable del tratamiento debe solicitar al Titular de la información la respectiva autorización previa, expresa e informada, por lo que, todo formulario publicado en el sitio web de la sociedad debe implementar la solicitud expresa de la autorización para el tratamiento de datos personales. De igual forma, dicha solicitud debe informar las finalidades del tratamiento y los derechos que le asisten al Titular, y solo podrá ser recolectada aquella información que sea imprescindible para cumplir la finalidad del tratamiento. Por otra parte, la implementación de medidas en materia de protección de datos personales por parte de la sociedad, con posterioridad al incumplimiento que dio origen a la investigación administrativa, no la exonera de responsabilidad.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
CÁMARA DE COMERCIO DE MONTERÍA	2021	El Responsable del tratamiento debe solicitar al Titular de la información la respectiva autorización previa, expresa e informada, por lo que, todo formulario publicado en el sitio web de la sociedad debe implementar la solicitud expresa de la autorización para el tratamiento de datos personales. De igual forma, dicha solicitud debe informar las finalidades del tratamiento y los derechos que le asisten al Titular, y solo podrá ser recolectada aquella información que sea imprescindible para cumplir la finalidad del tratamiento. Por otra parte, la implementación de medidas en materia de protección de datos personales por parte de la sociedad, con posterioridad al incumplimiento que dio origen a la investigación administrativa, no la exonera de responsabilidad.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
WORKING BUSINESS S.A.S	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, las órdenes que se emitan son de obligatorio cumplimiento dentro del plazo establecido por la autoridad, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
COMUNICACIÓN CELULAR S.A. – COMCEL S.A.	2021	Los Responsables del tratamiento deben rectificar y/o suprimir la información personal cuando ésta sea incorrecta y comunicar lo pertinente al Encargado del tratamiento, desde el momento en que el Titular presentó la solicitud. En cumplimiento del deber de seguridad cuya finalidad es evitar el uso o acceso no autorizado por parte de terceros frente a los datos personales del Titular.	7 CONTRA EL RESPONSABLE - RESPECTO DE LA RECTIFICACIÓN DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
COMPULAB SERVICIOS MÉDICOS INTEGRALES S.A.S.	2021	Los Responsables están en el deber de implementar una Política de Tratamiento de Datos Personales que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico, ser puesta en conocimiento de los Titulares, señalar el nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable; el Tratamiento al cual serán sometidos los datos y la finalidad del mismo, los derechos que le asisten como Titular; el procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, rectificar y suprimir su información y revocar la autorización para el tratamiento; y la fecha de entrada en vigencia de la política de tratamiento de la información y el período de vigencia de la base de datos.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.
RAPPI S.A.S.	2021	El Responsable debe solicitar y conservar copia de la autorización previa, expresa e informada de los Titulares para el Tratamiento de los datos que recolecta a través de los formularios que usan en sus plataformas digitales, formatos físicos diligenciables, y sistema de video vigilancia. De igual manera, al momento de la recolección debe informar a los Titulares las finalidades del uso de su información y del carácter facultativo de suministrar sus datos sensibles como la huella dactilar. Con relación a los sistemas de video vigilancia, se debe implementar un Aviso de Privacidad que informe a los Titulares sus derechos y las Políticas de Tratamiento de Datos Personales. Así mismo se debe conservar la información bajo las condiciones de seguridad necesarias para	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, bloqueando el acceso a personas que ya no se encuentran vinculadas con la compañía, y restringiendo el acceso al sistema operativo del sistema de cómputo para prevenir la libre ejecución de programas, que aumenten el riesgo de ataques por software malicioso.		
TIME TO TRAVEL BARRANQUILLA S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, deben atender los diferentes requerimientos e instrucciones emitidas, y demostrar el cumplimiento de los deberes a los que se encuentra obligados. Entre ellos se encuentran la solicitud de autorización previa, expresa en informada para el tratamiento de datos personales, por lo cual, el Responsable del Tratamiento debe estar en capacidad de probar que cuenta con la autorización otorgada por el Titular. Así mismo, el Responsable está obligado a informar la finalidad del tratamiento de los datos personales a los Titulares, y los derechos que le asisten, de forma concomitante al momento de solicitar la autorización.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
CONRED S.A.S.	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de la Información que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inicio el tratamiento de datos personales y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
CENTRO DE IMÁGENES DIAGNÓSTICAS CEDIM I.P.S. S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento, por ende, las instrucciones dictadas por la misma, son de obligatorio cumplimiento, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares. Por otra parte, la atenuación de las sanciones por responsabilidad demostrada, solo opera en la medida en que la investigada demuestre la implementación de una Política de Protección de Datos Personales pertinente, útil, efectiva y verificable con anterioridad a la ocurrencia de los hechos que vulneraron el derecho de habeas data o el régimen de protección de datos personales.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
CONRED S.A.S.	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de la Información que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inicio el tratamiento de datos personales y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
CALZADO TERRANO S.A.S	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, las órdenes que se emitan, son de obligatorio cumplimiento dentro del plazo establecido por la autoridad, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
INSPIRA CONSULTORES S.A.S	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de la Información que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inicio el tratamiento de datos personales y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
CONDIVAL S.A.S.	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, por lo cual, las órdenes que se emitan, son de obligatorio cumplimiento dentro del plazo establecido por la autoridad, y no acatarlas	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.		
COPROPIEDAD VINTAGE PROPIEDAD HORIZONTAL	2021	La autorización para el tratamiento de datos personales puede obtenerse (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que este otorgó la autorización. No debe perderse de vista que el Responsable del Tratamiento debe estar en capacidad de probar que obtuvo el consentimiento previo, expreso e informado del Titular. De igual manera, el silencio, en ningún caso puede ser entendido como el otorgamiento de la autorización, la cual, debe ser calificada y gozar de los elementos señalados. Así mismo, el Responsable está obligado a informar la finalidad del tratamiento de los datos personales a los Titulares, y los derechos que le asisten, de forma concomitante al momento de solicitar la autorización.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
WHATSAPP LLC	2021	WhatsApp LLC deberá implementar un mecanismo o procedimiento apropiado, efectivo y demostrable que, al momento de solicitar la Autorización al Titular, informe en idioma castellano, de manera clara, sencilla y expresa el tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo. De igual forma, deberá crear una Política de Tratamiento de Información que deberá ser puesta en conocimiento de los Titulares de los Datos domiciliados o residentes en el territorio colombiano, y deberá registrar las Bases de Datos en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
COMUNICACIÓN CELULAR S.A. COMCEL S.A.	2021	El deber de veracidad del dato implica que la información que suministre la Fuente a los Operadores de los bancos de datos sea veraz, completa, exacta, actualizada y comprobable, toda vez que la información está destinada a ofrecer a terceros datos útiles para el cálculo del riesgo crediticio, además que la misma debe reflejar el comportamiento de pago del titular, por lo que incluir o reportar información errónea, de la cual no se tiene soportes o certeza, está incompleta, o no corresponde a la realidad, afecta gravemente al Titular de los datos; especialmente cuando se ha demostrado que fue víctima de suplantación de identidad.	5 CONTRA EL RESPONSABLE - RESPECTO DE LA VERACIDAD DE LA INFORMACIÓN	A.18. CUMPLIMIENTO.
MEDINUCLEAR S.A.S.	2021	Los Responsables están en el deber de implementar: (i) una Política de Tratamiento de la información que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los Titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso. Dichos manuales deben ser informados en el Registro Nacional de Bases de Datos.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
RAPPI S.A.S.	2021	Los Titulares tienen el derecho a solicitar la supresión de su información personal cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. Por lo tanto, es imperativo -no facultativo- que los	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		Responsables o Encargados del Tratamiento de datos personales garanticen oportuna y debidamente los derechos constitucionales y legales de los Titulares, atendiendo sus solicitudes de supresión de datos personales dentro del término establecido.		
COLOMBIA RED 365 S.A.S.	2021	Las personas, en desarrollo de sus derechos a la autodeterminación informática y el principio de libertad, son quienes de forma expresa deben autorizar que la información que sobre ellos sea recaudada pueda ser incluida en una base datos, de manera que la recolección de datos personales a través de una llamada telefónica es una forma de tratamiento indebida, puesto que no fue requerida de manera previa la autorización por parte del titular para recibir llamadas comerciales y tampoco se le informó el propósito específico y explícito del tratamiento. Por otra parte, es un deber de los Responsables del Tratamiento, atender los requerimientos de la Autoridad de Protección de Datos Personales.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
SEGURIDAD SUPERIOR LTDA	2021	Uno de los pilares fundamentales de la regulación en materia de protección de datos personales, es la exigencia de contar con la autorización previa, expresa e informada del Titular, ya que esta es la expresión de la voluntad inequívoca otorgada por el mismo para que sus datos personales sean recolectados y divulgados. Así pues, la publicación de fotografías que permitan establecer la identidad de personas naturales determinadas o determinables constituye un tipo de tratamiento de datos personales, por lo tanto, el Responsable debe obtener la autorización previa, expresa e informada y debe estar en la capacidad de demostrar dicho consentimiento.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
AMERICAN BUSINESS S.A.S	2021	La Superintendencia de Industria y Comercio ejerce funciones de vigilancia respecto de los Responsables y Encargados del tratamiento, por lo cual, las instrucciones dictadas por la misma, son de obligatorio cumplimiento, y no acatarlas pone en riesgo los derechos, libertades y garantías constitucionales de los Titulares.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
FUNDACIÓN EDUCACIONAL RUPERTO AGUILERA LEÓN	2021	La implementación de una Política de Tratamiento de Datos Personales no se limita a la creación, aprobación y suscripción de un documento, pues esta se considera efectivamente adoptada cuando es puesta en conocimiento de los Titulares, y cumple con ciertas características como: informar el nombre y domicilio del Responsable, indicar su fecha de entrada en vigencia, e incluirse en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (ii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inició el tratamiento de datos personales y (iii) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida,	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento. Por otra parte, los Responsables deben dar cumplimiento a los requerimientos que realice la Autoridad de Protección de Datos Personales, de manera oportuna y completa.		
GOELEGIDO S.A.S	2021	Los Responsables deben atender de forma eficiente las solicitudes de supresión de datos personales presentadas por los titulares, sin obstaculizar el ejercicio del derecho de habeas data, por tanto, es inadmisible que se generen respuestas dilatorias cuando la solicitud de supresión de los datos es clara. Por otra parte, los Responsables deben implementar mecanismos para solicitar al Titular la autorización para el Tratamiento de sus datos personales, en forma previa al diligenciamiento de los formularios que se encuentran en los sitios web o en la aplicaciones, implementado controles sobre la edad de las personas que llevan a cabo el registro; para el caso de los menores de edad, se debe obtener la autorización de los respectivos representantes legales y/o padres de los menores y conservar prueba de ella.	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.
INTELLIGENT TECHNOLOGY SOLUTIONS S.A.S	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de la Información que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inició el tratamiento de datos personales y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
CENTRO DE RECONOCIMIENTO DE CONDUCTORES SU PASE S.A.S	2021	El Responsable tiene el deber de tratar la información que se encuentra almacenada en su base de datos bajo las medidas mínimas establecidas por el Régimen de Protección de Datos Personales, mediante la implementación de una Política de Tratamiento de la información documentada y puesta en conocimiento de los titulares. Por lo tanto, los Responsables deben elaborar un documento exclusivo para la Política de Tratamiento de Datos Personales y no debe confundirse con otros manuales que cumplen funciones distintas dentro de la organización.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.
ROMLAND S.A.S.	2021	Los Responsables deben atender los diferentes llamados de la Superintendencia de Industria y Comercio y demostrar el cumplimiento de los deberes del Régimen de Protección de Datos Personales, por lo tanto,	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		guardar silencio frente a los requerimientos es un claro incumplimiento que conlleva a una sanción.	Y REQUERIMIENTOS	
SOCIAL, EDUCATIONAL, ENVIRONMENTAL AND DEVELOPMENT FOUNDATION	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (ii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inició el tratamiento de datos personales y (iii) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
BANCO DE BOGOTÁ	2021	Los Responsables del Tratamiento deben implementar medidas de seguridad a efectos de garantizar que la información administrada no sea divulgada, adulterada, consultada o expuesta de manera inconsulta o no autorizada por su Titular, también se deben implementar todos los mecanismos de seguridad necesarios para impedir que terceros tengan acceso a la información personal con el fin de adulterarla, consultarla, usarla o acceder a ella, más aun teniendo en cuenta que la información que maneja un Banco, demanda un grado de diligencia mayor, en la medida en que está dando tratamiento a datos de carácter financiero. Así, por ejemplo, entre las medidas de seguridad que se deben adoptar, está el establecer controles que impidan el uso de cuentas electrónicas que no hayan sido autorizadas directamente por sus titulares para recibir mensajes o que preserven la confidencialidad de los destinatarios de los mensajes respecto del envío de datos semiprivados a través de comunicaciones electrónicas y controlar la información que se encuentra asociada a cada uno de los titulares cuyos datos se está tratando.	4 CONTRA EL RESPONSABLE - RESPECTO DE LA SEGURIDAD DE LA INFORMACIÓN	A.12. SEGURIDAD DE LAS OPERACIONES.
UNE EPM TELECOMUNICACIONES S.A	2021	El ejercicio del derecho fundamental de habeas data permite a los Titulares solicitar la exclusión de la información que haya sido recogida en bases de datos de cualquier entidad privada o pública, por lo cual, el Titular podrá solicitar la supresión del dato cuando, además de que no se respeten los principios, derechos y garantías constitucionales y legales, no exista una obligación legal o contractual que imponga al Titular el deber de permanecer en la referida base de datos y sea su voluntad no permanecer en ella. De igual forma, los Responsables deben atender las peticiones de supresión de datos personales de los Titulares y demostrar técnicamente que se realizó la supresión y/o eliminación de los datos personales del Titular de la base de datos de forma eficiente y dentro de un plazo	1 CONTRA EL RESPONSABLE - RESPECTO DEL EJERCICIO DEL DERECHO DE HÁBEAS DATA	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		razonable, para evitar la vulneración del derecho fundamental de habeas data mediante el envío de mensajes de texto con fines de cobranza.		
HABITAMOS PROPIEDAD RAÍZ S.A.S	2021	El Responsable del Tratamiento debe contar con procedimientos o mecanismos para informar la finalidad a los Titulares de la Información del uso que se le va a dar a sus datos personales, pues no es suficiente que este autorice previa y expresamente el Tratamiento de sus datos, sino que es necesario también que el Titular esté plenamente consciente de los efectos de haber otorgado dicha autorización, así mismo el Responsable del Tratamiento, deberá conservar prueba de la información hecha a los titulares sobre las finalidades del tratamiento de sus datos, antes de empezar a recolectarlos, utilizando un mecanismo que permita la consulta posterior. Por otra parte, los Responsables deben conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento respecto de las bases de datos que almacenan en equipos de cómputo, puertos USB, etc. Así mismo, es obligatoria la implementación de: (i) un manual interno de políticas y procedimiento documentado para la atención de quejas y reclamos, (ii) un manual interno de políticas y procedimientos que describa los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, en donde se señalen las finalidades para las cuales la información es recolectada, (iii) un manual de políticas de seguridad de la información.	3 CONTRA EL RESPONSABLE - RESPECTO DE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS DEL TITULAR	A.18. CUMPLIMIENTO.
ACADEMIA DE COCINA Y ARTES S.A.	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de la Información que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre las finalidades de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inició el tratamiento de datos personales y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.
EDIFICIO LOS NOGALES - PROPIEDAD HORIZONTAL	2021	En virtud del principio de libertad, los Responsables del Tratamiento de datos personales deben requerir la autorización previa, expresa e informada del Titular, y conservar copia de la misma, e informar sobre la finalidad de la recolección y los derechos	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		que le asisten a los residentes de la copropiedad en virtud de la autorización otorgada. De igual modo, el tratamiento de datos sensibles y sobre niños, niñas y adolescentes, tiene una protección especial por parte del legislador estatutario, en ese sentido, el principio de seguridad cobra una relevancia mayor, pues en razón a esa protección especial es imperativo reforzar las medidas técnicas, humanas y administrativas necesarias con el fin de garantizar la seguridad de todos los datos personales de la propiedad horizontal. De igual forma, los Responsables deben implementar: (i) una Manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de las disposiciones establecidas en la Ley 1581 de 2012, (ii) un Manual Interno para la Atención de Consultas y Reclamos para el ejercicio del derecho de habeas data de los Titulares y (iii) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento, (iv) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, (V) una Política de Tratamiento de Datos Personales.		
ECLECTICUS S.A	2021	Es deber del Responsable realizar todos los actos tendientes a obtener el consentimiento previo, expreso e informado de los titulares cuya información recolecta a través de su sitio web, dicho deber no se limita únicamente a solicitar la autorización, sino que el mismo se extiende a conservar copia de la misma en un medio que permita su consulta posteriormente. Sin embargo, no es suficiente que el Titular autorice previa y expresamente el Tratamiento de sus datos, sino es necesario también que esté plenamente consciente de los efectos de haber otorgado dicha autorización. Adicionalmente, el tratamiento de datos personales que se realiza mediante páginas web deben poner a disposición de los titulares las políticas de tratamiento de datos, el Tratamiento al cual serían sometidos y las finalidades del mismo, los derechos que le asisten al Titular, la persona o área responsable de la atención de peticiones, consultas y reclamos, el procedimiento para que los Titulares puedan ejercer sus derechos, la entrada en vigencia de la política y el periodo de vigencia de la base de datos.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
INVERSIONES EL BOSQUE NORTE S.A	2021	Los Responsables tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos y la información relacionada en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar: (i) una Política de Tratamiento de la Información que debe ser redactada en un lenguaje claro y sencillo, constar en un medio físico o electrónico y ser puesta en conocimiento de los titulares, (ii) un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, que incluya una descripción sobre la finalidades	9 CONTRA EL RESPONSABLE - RESPECTO DEL MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		de la recolección y una explicación relativa a la necesidad de recolectar los datos en cada caso, (iii) un Manual Interno para la Atención de Consultas y Reclamos desde el momento en que inició el tratamiento de datos personales y (iv) un Manual Interno de Políticas de Seguridad que garantice la seguridad de la información frente a la administración de los datos personales para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información sujeta a Tratamiento.		
EDIFICIO ESTUDIO 59 - PROPIEDAD HORIZONTAL	2021	Las Propiedades Horizontales al ser Responsables del tratamiento, deben implementar una Política de tratamiento de datos personales que debe ser puesta en conocimiento de los Titulares, así mismo, deben adoptar un manual interno en el cual se definan los procedimientos para la atención de consultas, reclamos y el ejercicio del derecho de habeas data de los titulares. Además de esto, se requiere una mayor diligencia frente al tratamiento de datos personales a través de sistemas de videovigilancia, informando a los Titulares mediante avisos de privacidad acerca de sus derechos y las Políticas de tratamiento de datos personales establecidas para el cumplimiento del Régimen de Protección de Datos Personales.	14 CONTRA EL RESPONSABLE - RESPECTO DE LAS POLÍTICAS DE TRATAMIENTO	A.18. CUMPLIMIENTO.
BLER S.A.S	2021	En virtud del principio de libertad, el Responsable del Tratamiento de datos personales debe requerir la autorización previa, expresa e informada del Titular, y conservar copia de la autorización de Tratamiento otorgada por el mismo. El derecho al habeas data se concreta en la facultad del Titular de la información de decidir, voluntariamente, que la información sobre sí mismo sea sometida a Tratamiento por parte de terceros, por ello, la autorización del Titular debe ser previa al primer contacto vía telefónica, no concomitante ni posterior a la recolección del dato.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
MARKETING PERSONAL S.A	2021	La Fuente debe actuar de manera diligente en la implementación y verificación de mecanismos eficaces que garanticen la veracidad de la información de los Titulares con el fin de evitar una suplantación de identidad, por tanto, debe contar con los documentos que demuestren la existencia de la obligación contraída con el Titular, y conservar copia o evidencia de la autorización otorgada por el Titular de la información con quien entabló una relación contractual. Así mismo, la Fuente debe contar con mecanismos que garanticen que la comunicación previa al reporte negativo sea enviada a los titulares y contestar las peticiones de manera oportuna dentro del término legal establecido.	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.
ASESORES JURÍDICOS E INMOBILIARIOS REMATES Y CESIONES S.A.S	2021	El Responsable debe solicitar el consentimiento previo, expreso e informado para realizar el tratamiento de la información que reposa en sentencias, autos, documentos aportados por las partes, pruebas documentales y expedientes judiciales, puesto que contienen no solo datos públicos sino también semiprivados, privados y sensibles. Adicionalmente, de manera previa a la recolección, almacenamiento y uso de los datos personales se debe informar la finalidad	2 CONTRA EL RESPONSABLE - RESPECTO DE LA AUTORIZACIÓN PARA EL TRATAMIENTO	A.18. CUMPLIMIENTO.

Entidad	Año	Título sancionatorio	Disposición normativa no aplicada ley 1581 de 2012	Control o medida de seguridad - IS0/IEC 27001:2013
		del tratamiento, de lo contrario se incurre en la vulneración del derecho fundamental de habeas data. Por otra parte, los responsables del tratamiento de datos personales tienen el deber de cumplir con las instrucciones y requerimientos impartidos por esta Superintendencia de Industria y Comercio, so pena de hacerse acreedores a las sanciones contempladas en las normas sobre protección de datos personales.		
FUNDACIÓN UNIVERSO DE INTELIGENCIA TECNOLOGÍA Y CULTURA DE COLOMBIA SIGLA UNIVERSITEC DE COLOMBIA	2021	Los Responsables del Tratamiento deben cumplir con las instrucciones y requerimientos impartidos por la Superintendencia de Industria y Comercio entre ellas la inscripción en el Registro Nacional de Bases de Datos, que debe realizarse bajo las formas y en los términos señalados en la Ley. Así mismo, los Responsables deben implementar una Política de Tratamiento de Información Personal que a su vez debe ser puesta en conocimiento de los Titulares, garantizándoles la protección y el amparo de su derecho fundamental de habeas data. De la misma manera, los Responsables deben adoptar un manual interno de políticas y procedimientos para garantizar el cumplimiento de Régimen de Protección de Datos Personales.	13 CONTRA EL RESPONSABLE - RESPECTO DE LAS INSTRUCCIONES Y REQUERIMIENTOS	A.18. CUMPLIMIENTO.
BANCO COMERCIAL AV VILLAS S.A.	2021	La protección del derecho fundamental de Habeas Data se materializa con las peticiones que los titulares interponen ante los Responsables del tratamiento para rectificar, actualizar, suprimir sus datos personales, o advertir el presunto incumplimiento por indebido tratamiento de sus datos personales; por tanto, el Responsable debe dar respuesta oportuna, completa y de fondo a las peticiones presentadas por los Titulares en el ejercicio de su derecho de Habeas Data, dentro del término establecido por la ley. No únicamente con ocasión a un requerimiento de la Autoridad de Protección de Datos Personales.	8 CONTRA EL RESPONSABLE - RESPECTO DE LA ATENCIÓN DE CONSULTAS Y RECLAMOS	A.18. CUMPLIMIENTO.

Fuente: Adaptación del Manual de usuario del Registro Nacional de Bases de Datos - RNDB[207] y resolución sancionatoria emitida por la delegatura para la protección de datos personales de la SIC para el año 2021.[208]

[207] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/2022/Manual%20de%20UsuarioRNBD%20R-25112020.docx

[208] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales, Decisiones administrativas. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Anexo D. Medidas de Seguridad RNBD Vs. Norma ISO/IEC 27001:2013

#	Requisitos de medidas de seguridad - SIC - formulario RNBD	Bloques temáticos preguntas SIC	Causas de Sanciones de reclamo titulares - SIC	Recomendación Controles seguridad a implementar - ISO/IEC 27001:2013	
I. SEGURIDAD DE LA INFORMACION					
1	¿Ha realizado documentación de procesos en torno a la seguridad de la información personal?	SEGURIDAD DE LA INFORMACION	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.
2	¿Tiene procedimientos de asignación de responsabilidades y autorizaciones en el tratamiento de la información personal?	SEGURIDAD DE LA INFORMACION	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
3	¿Ha implementado acuerdos de confidencialidad con las personas que tienen acceso a la información personal?	SEGURIDAD DE LA INFORMACION	2801 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
4	¿Tiene controles de seguridad en la tercerización de servicios para el tratamiento de la información personal?	SEGURIDAD DE LA INFORMACION	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.2. Transferencia de información.
5	¿Tiene un documento de seguridad de la información personal o general aprobado?	SEGURIDAD DE LA INFORMACION	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
II. SEGURIDAD DE LA INFORMACIÓN PERSONAL EN TORNO AL RECURSO HUMANO					
6	¿Tiene implementados controles de seguridad de la información personal para el Recurso Humano antes de la vinculación y una vez finalizado el contrato laboral?	SEGURIDAD DE LA INFORMACIÓN PERSONAL EN TORNO AL RECURSO HUMANO	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1. Antes de asumir el empleo.
III. CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL					
7	¿Cuenta con un procedimiento para la Gestión de usuarios con acceso a la información personal?	CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.9. CONTROL DE ACCESO.	A.9.2. Gestión de Acceso de Usuarios.
8	¿Ha implementado una política específica para el acceso a la información personal de las bases de datos con información personal sensible?	CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL	902 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.9. CONTROL DE ACCESO.	A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
9	¿Tiene una política implementada de copia de	CONTROL DE ACCESO A LA	903 Adoptar un manual interno de políticas y	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.3. Copias de Respaldo.

#	Requisitos de medidas de seguridad - SIC - formulario RNBD	Bloques temáticos preguntas SIC	Causas de Sanciones de reclamo titulares - SIC	Recomendación Controles seguridad a implementar - ISO/IEC 27001:2013	
	respaldo de la información personal?	INFORMACIÓN PERSONAL	procedimientos para asegurar el cumplimiento de la ley		
10	¿Ha implementado una política de protección para el acceso remoto a la información personal?	CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL	904 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.9. CONTROL DE ACCESO.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.
11	¿Tiene una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico?	CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL	905 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.
IV. SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL					
12	¿Tiene implementados controles de seguridad de la información durante el mantenimiento (Control de cambios) de los sistemas de información personal?	SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL	401 Conservar con la debida seguridad los registros almacenados	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
13	¿Tiene un procedimiento implementado de auditoría de los sistemas de información que contengan datos personales?	SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.7. Consideraciones sobre auditorías de sistemas de información.
14	¿Las bases de datos con información personal poseen Monitoreo de consulta?	SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL	401 Conservar con la debida seguridad los registros almacenados	A.9. CONTROL DE ACCESO.	A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
15	¿Tiene implementado un procedimiento que contemple la definición de especificaciones y requisitos de seguridad de los sistemas de información personal?	SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
V. PROCESAMIENTO DE INFORMACIÓN PERSONAL					
16	¿Cuenta con un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.?	PROCESAMIENTO DE INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.
17	¿Cuenta con un control de seguridad de información para la validación de datos de salida?	PROCESAMIENTO DE INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de

#	Requisitos de medidas de seguridad - SIC - formulario RNBD	Bloques temáticos preguntas SIC	Causas de Sanciones de reclamo titulares - SIC	Recomendación Controles seguridad a implementar - ISO/IEC 27001:2013	
					información o para mejoras a los sistemas de información existentes.
18	¿Cuenta con una política implementada para el Intercambio físico o electrónico de datos (como por ejemplo durante el comercio electrónico para la compra y venta de productos o servicios), transporte y/o almacenamiento de información personal?	PROCESAMIENTO DE INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.
19	¿Tiene un procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción, etc.)?	PROCESAMIENTO DE INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.
20	¿Cuenta con una política implementada para el correcto tratamiento de la información personal en las diferentes etapas del ciclo de vida del dato (recolección, circulación y disposición final)?	PROCESAMIENTO DE INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.
VI. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL					
21	¿Tiene implementada una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados?	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
22	¿Cuenta con una política y procedimientos implementados de gestión de incidentes de seguridad de la información personal?	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
VII. AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL					
23	¿Dentro de las auditorías de seguridad de información personal, tiene en cuenta el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos?	AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
24	¿Tiene una política de auditorías de seguridad de la información personal?	AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar

#	Requisitos de medidas de seguridad - SIC - formulario RNBD	Bloques temáticos preguntas SIC	Causas de Sanciones de reclamo titulares - SIC	Recomendación Controles seguridad a implementar - ISO/IEC 27001:2013	
					las interrupciones en los procesos del negocio.
VIII. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN					
25	¿Tiene implementadas herramientas de gestión de riesgos en el tratamiento de datos personales?	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
26	¿Tiene implementado un sistema de gestión de seguridad de la información o un programa integral de gestión de datos personales?	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	901 Adoptar un manual interno de políticas y procedimientos para asegurar el cumplimiento de la ley	A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.

Fuente: Adaptación del Sistema de la SIC- RNBD[209] y anexo “A” de la norma ISO/IEC 27001:2013[210]

[209] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://rnbd.sic.gov.co/sisi/login

[210] ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. (Consultado junio 2021). ISBN impreso 978-958-8585-53-6.

Anexo E. Lista comprobación protección de datos personales - SIC

	LISTADO DE COMPROBACIÓN RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES	SI/NO
	I. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES	
1	Se recolecto información personal para finalidades legítimas y se informa al titular esas finalidades	
2	Se cuenta con el consentimiento para tratar los datos del titular del cual se recolecta información.	
3	Si hay casos en los que se recolecta o información personal sin el consentimiento de los titulares, existe un mandato legal o judicial que habilite a organización para hacerlo	
4	Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible.	
5	Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.	
6	Se garantiza la confidencialidad de la información por las personas de la organización que interviene en el tratamiento de datos personales, incluso después de que han finalizado si relación con alguna de las labores desempeñadas.	
	II. TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD	
7	Se cuenta con autorización explícita de los titulares para el tratamiento de sus datos sensibles	
8	Se informa al titular que por tratarse de datos sensibles no está obligados a autorizar su tratamiento	
9	Se informa al titular cuáles de los datos serán objeto de tratamiento en su organización son sensibles y para qué finalidad(es) se utilizan	
10	Se efectúa tratamiento de datos personales de menores de edad únicamente para actividades que responden y respetan el interés superior de los menores	
11	En el tratamiento de datos personales de menores de edad se asegura el respeto de sus derechos fundamentales	
12	Se cuenta con la autorización del representante legal del menor de edad para el tratamiento de sus datos	
	III. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN	
13	Se permite el ejercicio del derecho de los titulares a conocer, actualizar y rectificar los datos personales que recolecta	
14	Se da respuesta a las solicitudes presentadas por los titulares dentro de la oportunidad prevista en la ley general de protección de datos personales	
15	Se entrega a los titulares copias de la autorización otorgada por ellos para el tratamiento de sus datos personales cuando así lo solicitan estos.	
16	Se informa a los titulares qué uso les ha dado la organización a sus datos personales cuando así lo solicitan estos	
17	Se permite a los titulares el acceso gratuito a los datos personales que han sido objeto de tratamiento al menos una vez cada mes calendario y cada vez que se hagan modificaciones sustanciales a la política de tratamiento de la información.	
	IV. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES	
18	Se cuenta con la autorización de los titulares de los datos contenidos en las bases de datos que tiene la organización para el tratamiento de estos	
19	Se conocen los casos en los que no es necesario contar con autorización de los titulares para el tratamiento de su información personal	
20	Se cuenta con procedimiento efectivos y eficientes para solicitar, a más tardar en el momento de la recolección de los datos personales, las autorizaciones de los titulares para el tratamiento de estos	
21	Se informa a los titulares qué datos personales serán recolectados y todas las finalidades específicas del tratamiento para las cuales la organización obtiene el consentimiento	
22	Se obtiene nuevas autorizaciones de los titulares, cuando la organización realiza cambios sustanciales en las políticas de tratamiento de información personal	
23	Se estable mecanismos que garantizaran la consulta posterior de la autorización otorgada por los titulares para el tratamiento de sus datos personales	
24	Se ponen a disposición de los titulares mecanismos gratuitos y de fácil acceso para presentar solicitudes de supresión de datos o la revocación de la autorización otorgada	
	V. INFORMACIÓN MÍNIMA A LOS TITULARES	
25	Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, el tratamiento al cual serán sometidos los mismos y la finalidad.	
26	Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, el carácter facultativo de la respuesta a las preguntas que se hacen, cuando se relacionan con datos sensibles a datos de niñas, niños y adolescentes.	
27	Se informa de manera clara expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, los derechos que les asisten.	

LISTADO DE COMPROBACIÓN RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES		SI/NO
28	Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono de responsable del tratamiento	
29	Se conserva prueba de haber informado a los titulares lo mencionado anteriormente.	
VI. SUMINISTRO DE LA INFORMACIÓN PERSONAL		
30	La información personal que se suministra al titular o a quien éste autorice es de fácil lectura, sin barreras técnicas que impidan su acceso y corresponde en un todo a aquella que reposa en la base de datos.	
31	Se suministra únicamente información personal a los titulares, sus causahabientes o sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y a los terceros autorizados por el titular o por la ley.	
VII. ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES		
32	Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención de las consultas y reclamos de los titulares o sus causahabientes.	
33	Se dan a conocer a los titulares e interesados los canales habilitados para la atención de consultas y reclamos en la política de tratamiento de datos personales dispuesta por la organización.	
34	Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información personal presentadas por los titulares, sus causahabientes y las personas autorizadas.	
35	Se informa a los peticionarios el motivo de la no atención oportuna a su consulta de información personal y se señala la fecha de respuesta de la solicitud, sin exceder el término de cinco (5) días adicionales a los (10) días iniciales para contestar.	
36	Se atiende, dentro de los diez (15) días hábiles contados a partir de su recibo, las reclamaciones presentadas por los titulares o sus causahabientes que consideran que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley.	
37	Se informa a los peticionarios el motivo de la no atención oportuna a su reclamo y se señala la fecha de respuesta de la solicitud, sin exceder el término de ocho (8) días adicionales a los quince (15) días iniciales para contestar.	
38	Se adoptan medidas para asegurar que los datos personales que reposan en las bases de datos Dean precisos y suficientes y, cuando así lo solicite el titular o cuando haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento.	
39	Se ha designado a una persona a área para que asuma la función de protección de datos personales y dé trámite a las solicitudes de los titulares para el ejercicio de sus derechos.	
40	Se da a conocer a los titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.	
41	Se incluye dentro de la política de tratamiento de datos personales los procedimientos dispuestos para garantizar el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización.	
42	Se cuenta con un manual interno de políticas y procedimientos para garantizar la atención de consultas y reclamos presentados por los titulares y para garantizar, en general, el adecuado cumplimiento de la ley.	
43	Se han adoptado procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto de tratamiento de sus datos personales.	
VIII. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES		
44	Se cuenta con una política para el tratamiento de los datos personales.	
45	La política para el tratamiento de datos personales consta en medio físico o electrónico, en un lenguaje claro y sencillo, y es puesta en conocimiento de los titulares.	
46	Se cuenta con una política para el tratamiento de los datos personales que incluye el nombre o razón social, domicilio, dirección, correo electrónico y teléfono de la organización.	
47	La política para el tratamiento de datos adoptada por la organización incluye información sobre el tratamiento al cual serán sometidos los datos personales y la finalidad de este.	
48	Incluye la política para el tratamiento de datos personales información sobre los derechos que le asisten a los titulares respecto de su información personal.	
49	Se informa en la política para el tratamiento de datos personales sobre la persona o área responsabilidad de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	
50	Se indica en la política para el tratamiento de datos personales cuál o cuáles son los procedimientos para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.	
51	En la política para el tratamiento de datos personales está incluida la fecha de entrada en vigor y el periodo de vigencia de la o las bases de datos que tiene la organización.	

LISTADO DE COMPROBACIÓN RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES		SI/NO
IX. AVISO DE PRIVACIDAD		
52	Se informa a los titulares la existencia de la política para el tratamiento de datos personales por medio de un aviso de privacidad.	
53	El aviso de privacidad publicado por la organización incluye el nombre o razón social y los datos de contacto de esta.	
54	En el aviso de privacidad publicado se incluye la descripción del tratamiento al cual serán sometidos los datos personales recolectados y la finalidad de tal recolección.	
55	El aviso de privacidad incluye un listado de los derechos que tienen los titulares cuya información es recolectada por la organización.	
56	Se informa a los titulares en el aviso de privacidad publicado, cómo acceder o consultar la política de tratamiento de datos personales dispuesta por la organización.	
57	En el aviso de privacidad publicado se señala expresamente la facultad que tienen los titulares de contestar o no las preguntas que versen sobre datos personales sensibles o sobre los datos de niños, niñas y adolescentes.	
58	Se conserva el modelo de aviso de privacidad utilizado para cumplir con la obligación legal de dar a conocer las políticas de tratamiento de la información personal.	
X. REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD		
	Informa a la Superintendencia cuando se presentan violaciones a los códigos de seguridad que generen riesgos en la administración de la información de los titulares.	
XI. GESTIÓN DE ENCARGADOS DEL TRATAMIENTO		
60	Se han establecidos procedimientos internos para asegurar que los Encargados del tratamiento garanticen la protección de los datos personales que le son entregados y que su tratamiento se haga acorde con los principios y deberes establecidos en la ley.	
61	Se suscriben contratos con los Encargados que incluyen expresamente el tratamiento que éste podrá realizar a los datos personales.	
62	Se suscriben contratos con los Encargados que incluyen cláusulas de confidencialidad de la información entregada.	
63	Se exige a los encargados tener y mantener políticas de seguridad de la información y de tratamiento de datos personales antes de entregar las bases de datos.	
64	Se informa al encargado de forma oportuna todas las novedades respecto de los datos que previamente le fueron suministradas.	
65	Se cuenta con medidas necesarias para que la información suministrada al encargado se mantenga actualizada.	
66	Se comunica al encargado cuando se ha rectificado la información incorrecta.	
67	Se comunica al encargado si determinada información se encuentra en discusión por parte del titular, una vez éste presenta una reclamación y no ha finalizado el trámite respectivo.	
68	Se verifica que el encargado actualice y rectifique la información personal en los términos legales.	
XII. TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES		
69	Se transfieren datos personales a países que garantizan niveles adecuados de protección de datos, según lo establecido en el numeral 3.2 de capítulo tercero del título V de la circular única de la Superintendencia de Industria y Comercio.	
70	Se han implementado medidas a apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia.	
71	Se transfieren datos personales fuera del territorio colombiano con base en alguna de las causales de excepción establecidas en el artículo 26 de la ley 1581 de 2012.	
72	Se transfiere datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia.	
73	Se transfiere datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia.	
74	Se han suscrito contratos con los responsables del tratamiento destinatarios de los datos personales a transferir fuera del territorio colombiano o se implementan otros instrumentos jurídicos en los que se señalen las condiciones que regirán la transferencia Internacional de datos personales, mediante las cuales se garantizará el cumplimiento de los principios que rigen el tratamiento, así como de las obligaciones que tienen a cargo.	
75	Se transmiten datos personales fuera del territorio colombiano a un encargado para que realice el tratamiento indicado por la organización como responsable del tratamiento y para ello han suscrito contratos de transmisión de datos personales en los que se señalen los alcances del tratamiento, las actividades que el encargado realizará y obligaciones de este respecto de los titulares y el responsable.	

LISTADO DE COMPROBACIÓN RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES		SI/NO
76	Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado cláusulas mediante las cuales este se compromete a dar aplicación a las obligaciones del responsable bajo su política de tratamiento de la información y a realizar el tratamiento de datos de acuerdo con la finalidad que los titulares han autorizado y con las leyes aplicaciones	
77	Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación de dar tratamiento, a nombre del responsable, a los datos personales conforme a los principios establecidos en la ley general de protección de datos personales	
78	Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de guardar confidencialidad respecto del tratamiento de los datos personales	
XIII. RESPONSABILIDAD DEMOSTRADA		
79	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a la naturaleza jurídica de la organización y su tamaño empresarial	
80	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a la naturaleza de los datos personales objeto del tratamiento	
81	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional al tipo de tratamiento que realice con los datos personales	
82	Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a los riesgos potenciales que el tratamiento podrías causar sobre los derechos de los titulares.	
83	Se conserva evidencia sobre la implementación efectiva de medidas de seguridad apropiadas para el cumplimiento del régimen de protección de datos personales.	
	Se han adoptado mecanismos internos para poner en práctica las políticas establecidas en los que se incluyan herramientas de implementación, entrenamiento y programas de educación en materia de protección de datos personales.	
XIV. REGISTRO NACIONAL DE BASES DE DATOS		
85	Se han registrado las bases de datos con información personal de la organización en el Registro Nacional de Bases de datos (RNBD) administrado por la Superintendencia de Industria y comercio	

Fuente: Adaptación de la guía Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las Mipymes de la SIC[211]

Anexo F. Lista de verificación del principio de responsabilidad demostrada

LISTA DE VERIFICACION - MEDIR AVANCE DE IMPLEMENTACION DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA		SI/NO
1. COMPROMISOS DE LA ORGANIZACIÓN		
1.1. DESDE LA ALTA DIRECCIÓN		
1	Se cuenta con el compromiso de la organización para la implementación de un programa integral de gestión de datos personales	
2	Existe en la organización una cultura de respeto a la protección de los datos personales que se recogen o tratan	
3	Se han comprometido recursos económicos y de personal en la organización, acorde a su tamaño y estructura, así como al tipo de información a la que se le realiza Tratamiento, para la implementación del Programa Integral de Gestión de Datos Personales	
4	Se cuenta con el apoyo y compromiso de la Alta Dirección para generar una cultura organizacional de respeto a la protección de datos personales	
5	La Alta Dirección de la organización designó a la persona o área que asumirá la función de protección de datos dentro de la organización	
6	La Alta Dirección de la organización aprobó el Programa Integral de Gestión de Datos Personales	
7	La Alta Dirección de la organización realiza un monitoreo del Programa Integral de Gestión de Datos Personales.	
8	La Alta Dirección de la organización informa de manera periódica a los órganos directivos sobre la ejecución del programa Integral de Gestión de Datos Personales	

[211] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales. [en línea]. Consultado el 20 de febrero de 2022. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf

	LISTA DE VERIFICACION - MEDIR AVANCE DE IMPLEMENTACION DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA	SI/NO
9	La Alta Dirección de la organización destina recursos suficientes al área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales para desempeñar sus funciones.	
10	A través del área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales se establecen las responsabilidades específicas para otras áreas de la organización respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan.	
1.2. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES		
11	Se cuenta con una persona o área que asume la función de protección de datos personales y que da trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015.	
12	Se cuenta con una persona o área que vele por la implementación efectiva de las políticas y procedimientos adoptados por la organización para cumplir las normas de protección de datos personales.	
13	Se cuenta con una persona o área que establezca los controles del Programa Integral de Gestión de Datos Personales, así como la evaluación y revisión permanente de dichos controles.	
14	La persona o área que asume la función de protección de datos personales ha promovido la elaboración e implementación de un sistema que permita administrar los riesgos del Tratamiento de datos personales	
15	La persona o área que asume la función de protección de datos personales sirve de enlace y coordina las demás áreas de la organización para asegurar la implementación transversal del Programa Integral de Gestión de Datos Personales.	
16	La persona o área que asume la función de protección de datos personales impulsa dentro de la organización una cultura de protección de datos.	
17	La persona o área que asume la función de protección de datos personales mantiene un inventario de las bases de datos personales en poder de la organización y las clasifica de acuerdo con su tipo.	
18	La persona o área que asume la función de protección de datos personales ha solicitado la declaración de conformidad de las operaciones de transferencia internacional de información personal ante la Superintendencia, cuando ha sido requerida, de conformidad con las instrucciones impartidas por esa entidad.	
19	La persona o área que asume la función de protección de datos personales revisa los contenidos de los contratos de transmisiones internacionales de datos, suscritos por la organización con los Encargados del Tratamiento no residentes en Colombia.	
20	La persona o área que asume la función de protección de datos personales ha diseñado un programa de entrenamiento en protección de datos personales acorde con las responsabilidades de cada cargo de la organización.	
21	La persona o área que asume la función de protección de datos personales realiza un entrenamiento general a todos los empleados y colaboradores de la compañía en protección de datos personales.	
22	La persona o área que asume la función de protección de datos personales realiza un entrenamiento a los nuevos empleados o colaboradores de la organización que, por las condiciones de su empleo, tengan acceso a los datos personales que se gestionan al interior de esta.	
23	La persona o área que asume la función de protección de datos personales integra las políticas de protección de datos personales dentro de las actividades de las demás áreas de la organización.	
24	La persona o área que asume la función de protección de datos personales mide la participación de los empleados y colaboradores en los entrenamientos en protección de datos y califica su desempeño.	
25	La persona o área que asume la función de protección de datos personales acompaña y asiste a la organización en la atención de las visitas y requerimientos realizados por la Superintendencia de Industria y Comercio.	
26	La persona o área que asume la función de protección de datos personales acompaña y asiste a la organización en la atención de las visitas y requerimientos realizados por la Superintendencia de Industria y Comercio.	
27	La persona o área que asume la función de protección de datos personales realiza seguimiento al Programa Integral de Gestión de datos personales	
1.3. PRESENTACIÓN DE INFORMES		
28	Se cuenta con planes de auditoría interna para verificar el cumplimiento de las políticas de Tratamiento de datos personales y señalar el procedimiento a seguir en caso de que se presenten violaciones a los códigos de seguridad o se detecten riesgos en la administración de la información personal de los Titulares.	
29	De define la estructura de la generación de reportes en la que se establezca qué empleado o persona genera qué tipo de reporte y se asignan responsabilidades claras ante una queja de los Titulares o una violación a los códigos de seguridad.	
30	Se documenta el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.	
31	Se generan reportes para los accionistas o socios de manera periódica y se informa a estos el estado del Programa Integral de Gestión de Datos Personales.	
2. CONTROLES DEL PROGRAMA		
2.1. PROCEDIMIENTOS OPERACIONALES		
32	Se cuenta con procedimientos administrativos consistentes con las políticas generales de protección de datos personales y con las disposiciones legales vigentes, para manejar adecuadamente los riesgos inherentes al Tratamiento de datos personales dentro de la gestión operacional.	
2.2. INVENTARIO DE BASES DE DATOS CON INFORMACIÓN PERSONAL		
33	Se tienen identificadas e inventariadas las bases de datos dentro de la organización.	

	LISTA DE VERIFICACION - MEDIR AVANCE DE IMPLEMENTACION DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA	SI/NO
34	Se tiene claridad sobre el medio en el que se conservan las bases de datos al interior de la organización (manual o automatizado). Se tiene claridad de cuántos Titulares o personas naturales existen en cada base de datos.	
35	Se tiene identificado qué tipo de datos personales reposan en cada base de datos (datos de identificación, datos de ubicación, datos sensibles, datos de contenido socioeconómico, etc.)	
36	Se tiene establecido claramente para qué se utiliza cada base de datos y si realmente los datos que allí reposan son necesarios, teniendo en cuenta la finalidad para la que se recolectan.	
37	Se han identificado cómo se obtienen los datos personales en la organización, si se debe solicitar la autorización de los Titulares para obtener esos datos y, de ser así, sí se conserva prueba de tal autorización para su posterior consulta.	
38	Se informa a los Titulares la finalidad de la recolección de sus datos personales y el Tratamiento al que tales datos serán sometidos, así como los derechos que tienen como titulares.	
39	Se protege la calidad de la información personal al momento de su recolección.	
40	Si se recolectan datos de menores de edad, se han imprentado medidas adecuadas para garantizar una protección reforzada de dicha información.	
41	Si se recolectan datos menores de edad, la organización informa al Titular o a quien corresponda (tutores o representantes de los menores), que no existe obligación de suministrar tales datos.	
42	Se ha identificado qué áreas de la organización utilizan los datos personales y de qué forma los utilizan.	
43	Se han implementado medidas de seguridad para tratar y conservar los datos personales recolectados.	
44	Se han implementado procedimientos para actualizar, rectificar y depurar los datos personales en las bases de datos.	
45	Se entregan o comparten las bases de datos con información personal a terceros ubicados dentro o fuera del país.	
46	Se ha identificado para qué entregan o comparte las bases de datos con información personal con terceros dentro o fuera del territorio nacional.	
47	Se ha identificado por cuánto tiempo se conservan los datos personales y qué medios se utilizan para su disposición final (archivo físico, digitalización, eliminación, etc.)	
48	Se cuenta con medidas técnicas que garanticen la seguridad de los datos personales una vez se ha definido cuál será su disposición final.	
2.3. POLÍTICAS		
49	Se cuenta con políticas internas debidamente documentadas e implementadas que incluyan las obligaciones señaladas en la Ley de protección de Datos Personales y se dan a conocer a los empleados o colaboradores.	
50	Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la recolección o recopilación, el mantenimiento, uso y eliminación o disposición final de los datos personales.	
51	Se cuenta con procedimientos debidamente documentados e implementados que establezcan los requisitos para obtener la autorización de los Titulares.	
52	Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la conservación y eliminación de información personal.	
53	Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para el uso Responsables de la información, incluyendo controles administrativos, físicos y tecnológicos que garanticen la seguridad de la información.	
54	Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la inclusión en todos los medios contractuales de la empresa de una cláusula de confidencialidad y de manejo de información, donde se afirme que se conoce la política de la empresa, se acepta, y se permite a la compañía utilizar dicha información de forma Responsable.	
55	Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la presentación de quejas, denuncias y reclamos por parte de los Titulares y la forma de tramitarlas y atenderlas de manera adecuada, congruente y oportuna.	
56	Se incluye en las políticas de la organización, diferentes a la de protección de datos personales (talento humano, contratos, transparencia, etc.), elementos que permitan cumplir las normas sobre protección de datos.	
2.4. SISTEMA DE ADMINISTRACIÓN DE RIESGOS		
57	Cuenta con un sistema de administración de riesgos, acorde con la estructura organizacional, los procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y los tipos de datos personales tratados por la empresa, que le permita identificar, medir, controlar y monitorear aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos los datos personales	
58	Se ha identificado a qué riesgos se ven expuestos los datos personales a los que se realiza Tratamiento al interior de la organización (ej.: riesgo de pérdida o fuga de información, riesgo de mantener información desactualizada o no veraz, riesgo de acceso indebidos a la información, etc.).	
59	Se ha determinado la posibilidad de ocurrencia de los riesgos identificación y el impacto que podría ocasionar la materialización de estos, tanto para los Titulares como para la organización.	
60	Se ha establecidos qué acciones se deben tomar para controlar y/o mitigar los riesgos identificados, con el fin de disminuir la posibilidad y/o el impacto de la materialización de dichos riesgos.	
61	Los controles establecidos son suficientes, efectivos y oportunos para disminuir la posibilidad y/o el impacto de la materialización de los riesgos.	
62	Se realiza seguimiento constante para velar porque las medidas adoptadas sean efectivas	

	LISTA DE VERIFICACION - MEDIR AVANCE DE IMPLEMENTACION DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA	SI/NO
63	Se realiza una evaluación de riesgos constante en la organización y desde el diseño en cada proyecto en él se involucre el Tratamiento de datos personales.	
2.5. FORMACIÓN Y EDUCACIÓN		
64	Se tiene implementado un programa de capacitación para los empleados y contratistas de la organización en materia de protección de datos personales.	
65	Se realizan jornadas de capacitación al personal en materia de protección de datos personales, con periodicidad.	
66	Las capacitaciones realizadas a los empleados, contratistas y colaboradores en general de la organización involucrados directamente en las actividades de Tratamiento de datos personales se adaptan específicamente a las funciones, obligaciones y tareas que tienen a cargo.	
67	Existen dentro de los contratos suscritos por los empleados de la organización acuerdos de cumplimiento de las políticas internas desarrolladas por esta para el adecuado Tratamiento de los datos personales.	
2.6. PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES DE SEGURIDAD		
68	Se cuenta con un procedimiento documentados e implementado y una persona o área encargada de manejar los incidentes o violaciones a los sistemas de información donde se gestionan datos personales y a los archivos físicos.	
69	Los empleados y contratistas de la organización tienen conocimiento sobre qué hacer antes, durante y después de que se presente un incidente de seguridad	
70	Dentro del protocolo de incidentes de seguridad adoptado por la organización está previsto reportar a la Superintendencia de Industria y Comercio la ocurrencia de tales incidentes.	
71	Se cuenta con mecanismos, herramientas o procedimientos para la elaboración de informes internos y para informar tanto a los Titulares como a la Superintendencia de Industria y Comercio cuando se presenten incidentes de seguridad que involucren datos personales.	
72	Se cuenta con mecanismos, herramientas o procedimientos que permitan, además de informar a los Titulares la ocurrencia de un incidente de seguridad con sus datos personales y las posibles consecuencias, dar a conocer opciones o alternativas a dichos Titulares para minimizar el daño potencial o el daño causado.	
73	Se cuenta con mecanismos o procedimientos que permitan informar a la Superintendencia el tipo de incidente ocurrido la fecha en la que ocurrió y la fecha en la que se tuvo conocimiento de este, la causal del incidente, el tipo de datos personales comprometidos y la cantidad de Titulares afectados.	
2.7. GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES.		
74	Se han implementado medidas para asegurar la protección de los datos personales cuyo Tratamiento es realizado por los Encargados.	
75	Los contratos suscritos con los Encargados del tratamiento incluyen requisitos para que estos cumplan las normas colombianas de protección de datos y las políticas de Tratamiento de la información adoptadas por la organización.	
76	Se cuenta con mecanismos para que los Encargados reporten a la organización los incidentes de seguridad de la información que se presentan.	
77	Se verifica si los Encargados del Tratamiento de la información personal cuentan con política de Tratamiento de datos personales y programas de formación o educación en temas de protección de datos para sus empleados.	
78	Se exige la realización de auditoría internas y/o externas a las actividades desarrolladas por el Encargado del Tratamiento	
79	Existen acuerdos con los Encargados y sus empleados o colaboradores aceptando que cumplirán con las políticas y protocolos de Tratamientos de datos de su organización.	
80	Se exige a los Encargados que utilizan subcontratistas que se establezcan obligaciones para éstos de adherencia a las políticas de Tratamiento de la organización.	
2.8. COMUNICACIÓN EXTERNA		
81	Se han implementados procedimientos para informar a los Titulares sus derechos	
82	Se dirigen comunicaciones claras y comprensibles a los Titulares.	
83	Se cuenta con un área o persona encargada de la atención de las quejas y reclamos relacionados con el ejercicio del derecho de hábeas data.	
84	Se informa a los Titulares cuáles son los canales de atención que la organización tiene dispuestos para la presentación de sus reclamaciones o consultas	
3. EVALUACIÓN Y REVISIÓN CONTINUA		
3.1. PLAN DE SUPERVISIÓN Y REVISIÓN		
85	Se ha desarrollado dentro de la organización un plan de supervisión y revisión anual del Programa Integral de Gestión de Datos Personales.	
86	El plan de supervisión y revisión implementado establece las medidas de desempeño e incluye un calendario para las revisiones de las políticas y los controles del Programa Integral de Gestión de Datos Personales, por lo menos una vez al año.	

LISTA DE VERIFICACION - MEDIR AVANCE DE IMPLEMENTACION DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA		SI/NO
3.2 EVALUACIÓN Y REVISIÓN DE LOS CONTROLES DEL PROGRAMA		
87	Se revisan y evalúan periódicamente los controles establecidos para minimizar o evitar la materialización de los riesgos en el Tratamiento de datos personales.	
88	Los controles establecidos tienen en cuenta las nuevas amenazas, los motivos de las quejas más recientes presentadas por los Titulares, los hallazgos en las auditorías o las orientaciones de la autoridad de protección de datos.	
89	Se hace seguimiento a los servicios prestados por la organización que involucran recolección, uso, divulgación y, en general, cualquier Tratamiento de información personal para determinar que estén cumpliendo las políticas y procedimientos adoptados.	
90	Se realizan capacitaciones idóneas y acordes con las políticas y procedimientos dispuestos por la organización.	
91	La persona o área que asume la función de protección de datos personales controla y actualiza el inventario de información personal continuamente para identificar y evaluar nuevas recolecciones, usos y divulgaciones.	
92	La persona o área que asume la función de protección de datos personales revisa las políticas de acuerdo con los resultados de las evaluaciones o auditoría.	
93	La persona o área que asume la función de protección de datos personales mantiene como documentos históricos las evaluaciones de impacto y las de amenazas a la seguridad y riesgos.	
94	La persona o área que asume la función de protección de datos personales revisa y actualiza, en forma periódica, los programas de formación y educación para todos los empleados de la organización como resultado de evaluaciones continuas.	
95	La persona o área que asume la función de protección de datos personales revisa y adapta los protocolos de respuesta al manejo de violaciones e incidentes de seguridad e implementa las mejores prácticas y recomendaciones de las revisiones que se efectúan posterior a la ocurrencia de esos incidentes.	
96	La persona o área que asume la función de protección de datos personales revisa y, si es el caso, modifica los requisitos establecidos en los contratos suscritos por la organización con los Encargados del Tratamiento	
97	La persona o área que asume la función de protección de datos personales actualiza y clara las comunicaciones externas para explicar las políticas de Tratamiento de datos.	
98	La persona o área que asume la función de protección de datos personales reporta semestralmente al representante legal de la empresa la evolución del riesgo, los controles implementados, el monitoreo y, en general, los avances y resultados del Programa Integral de Gestión de Datos Personales.	

Fuente: Adaptación de la guía Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las Mipymes de la SIC[212]

[212] Ibid.