DOCENTE:

EDGAR SALAZAR COBO

ESTUDIANTE:
María Del Mar Henao Llanos

ÁREA:
TRABAJO DE GRADO II

PRÁCTICA ESTUDIANTIL

ANÁLISIS DE CLÁUSULA ESTANDAR DE PROTECCÍON DE DATOS PERSONALES

PONTIFICIA UNIVERSIDAD JAVERIANA DE CALI

PERIODO
2026-1

CALI, VALLE DEL CAUCA

Tabla de contenido

INTRODUCCIÓN

La presente sistematización de la práctica profesional surge a partir de la experiencia desarrollada en la XYZ organización colombiana de carácter privado dedicada al desarrollo, implementación, consultoría y soporte de soluciones de planificación de recursos empresariales (Enterprise Resource Planning – ERP). Con más de cuatro décadas de trayectoria en el mercado tecnológico latinoamericano, XYZ ha consolidado una posición estratégica al atender a más de 10.000 organizaciones pertenecientes a sectores como manufactura, comercio, retail, salud, servicios y hospitalidad, y al contar con un equipo humano que supera los 1.000 colaboradores distribuidos en Colombia, Ecuador y Perú.

La actividad misional de la compañía se orienta a impulsar procesos de transformación digital y optimización operativa en las organizaciones clientes, mediante la implementación de soluciones tecnológicas integrales que implican el procesamiento permanente de información empresarial y de datos personales. En este contexto, el manejo masivo y sistemático de información genera responsabilidades jurídicas específicas que trascienden el ámbito del derecho comercial tradicional y se insertan en el régimen especial de protección de datos personales y regulación del entorno digital.

Dentro de este marco normativo adquieren particular relevancia la Ley 527 de 1999, relativa al comercio electrónico y los mensajes de datos, y la Ley 1581 de 2012, que desarrolla el derecho fundamental al habeas data y establece el régimen general de protección de datos personales en Colombia. Estas disposiciones imponen a las empresas tecnológicas la obligación de adoptar medidas técnicas, administrativas y contractuales dirigidas a garantizar la seguridad, confidencialidad, integridad y legalidad del tratamiento de la información. De manera especial, el ordenamiento jurídico colombiano incorpora el principio de responsabilidad demostrada (accountability), el cual exige a los responsables del tratamiento no solo cumplir formalmente la normativa, sino estar en capacidad de acreditar de manera objetiva, verificable y proporcional la implementación de mecanismos efectivos de protección, acordes con el nivel de riesgo que implique el tratamiento de los datos personales.

En el desarrollo de la práctica profesional, particularmente en las labores de custodia contractual, organización de repositorios documentales por verticales de negocio y gestión de contratos, anexos y otrosíes a través de la plataforma DocuSign, se identificó una problemática jurídica relevante asociada a la utilización de una cláusula estándar de protección de datos personales aplicada de manera uniforme a la totalidad de los contratos celebrados por la compañía. Esta estandarización contractual no distingue entre la naturaleza de los datos tratados, los sectores económicos atendidos ni los niveles diferenciados de riesgo jurídico, lo cual puede generar vacíos normativos y limitar la eficacia real del sistema de cumplimiento.

En efecto, no resulta jurídicamente equivalente el tratamiento de datos personales en sectores como comercio o pequeñas y medianas empresas (PYMES), donde predomina información de carácter comercial y financiero, frente al manejo de datos altamente sensibles en clínicas, hospitales y entidades del sector salud, donde se procesan historias clínicas, diagnósticos médicos, tratamientos, exámenes especializados y datos biométricos. En este último escenario, el tratamiento involucra información íntimamente vinculada con la dignidad humana, la intimidad y la autodeterminación informativa, lo que exige estándares reforzados de seguridad, minimización, proporcionalidad y control de acceso.

La aplicación uniforme de una cláusula genérica, sin adecuación al perfil sectorial ni al nivel de sensibilidad de la información, puede contravenir los lineamientos establecidos

por la Superintendencia de Industria y Comercio, autoridad nacional encargada de la vigilancia y control en materia de protección de datos personales. Dicha entidad ha reiterado que el principio de responsabilidad demostrada implica la adopción de medidas diferenciadas y proporcionales al riesgo, así como la implementación de mecanismos contractuales que reflejen de manera concreta la gestión sectorial del tratamiento de datos. En este sentido, la ausencia de cláusulas predeterminadas pero modulables expone a la empresa a eventuales riesgos de responsabilidad administrativa, civil y reputacional.

A partir de este hallazgo empírico, la presente sistematización tiene como objetivo general analizar la cláusula estándar de protección de datos personales utilizada por XYZ, con el fin de verificar su adecuación al marco normativo colombiano vigente y al principio de responsabilidad demostrada, identificando posibles vacíos jurídicos y oportunidades de mejora conforme a los distintos sectores económicos atendidos por la compañía.

Desde el punto de vista metodológico, la investigación se enmarca en un enfoque cualitativo, de carácter jurídico-analítico y descriptivo, orientado a la sistematización crítica de una experiencia práctica profesional. Se emplea el método deductivo, partiendo del marco constitucional y legal general del derecho fundamental al habeas data para descender hacia su desarrollo jurisprudencial, doctrinal y administrativo, y finalmente contrastarlo con la práctica contractual concreta de la empresa. Como técnica principal se utilizó el análisis documental, aplicado a fuentes normativas (Constitución, leyes y decretos), jurisprudenciales (sentencias de la Corte Constitucional), administrativas (resoluciones, circulares y guías emitidas por la autoridad de control) y documentos internos de la compañía, especialmente modelos contractuales y cláusulas estándar. Este diseño metodológico permite articular teoría y práctica, evaluar la suficiencia jurídica de un instrumento contractual específico y formular propuestas de mejora basadas en criterios normativos verificables.

En coherencia con los objetivos específicos planteados, el trabajo se estructura en tres capítulos complementarios. El primer capítulo responde al primer objetivo específico mediante la descripción y análisis del marco normativo, conceptual y doctrinal que regula la protección de datos personales en Colombia, con énfasis en la Ley 1581 de 2012, sus decretos reglamentarios y los principios rectores del régimen de habeas data. El segundo capítulo desarrolla el segundo objetivo específico a través del estudio sistemático de la jurisprudencia constitucional y de los lineamientos administrativos adoptados por la Superintendencia de Industria y Comercio, particularmente en relación con la validez de las cláusulas contractuales y la materialización del principio de responsabilidad demostrada. Finalmente, el tercer capítulo da cumplimiento al tercer objetivo específico al contrastar la normativa y doctrina analizadas con la cláusula estándar utilizada por XYZ, evaluando su suficiencia frente a la diversidad sectorial y los distintos niveles de sensibilidad de la información tratada, con el propósito de formular una propuesta de reformulación contractual ajustada a los estándares legales vigentes.

De esta manera, la sistematización no se limita a describir una experiencia profesional, sino que construye un análisis jurídico aplicado que permite fortalecer el modelo de cumplimiento corporativo, aportar a la gestión integral del riesgo legal y contribuir a la consolidación de buenas prácticas contractuales en el ecosistema tecnológico colombiano.

OBJETIVO GENERAL

Analizar la cláusula estándar de protección de datos personales utilizada por la empresa XYZ, con el fin de verificar su adecuación al marco normativo colombiano vigente y al principio de responsabilidad demostrada, identificando posibles vacíos jurídicos y

oportunidades de mejora conforme a los distintos sectores económicos atendidos por la compañía.

OBJETIVOS ESPECÍFICOS

- Describir el marco normativo, conceptual y doctrinal que regula la protección de datos personales en Colombia, con énfasis en la Ley 1581 de 2012, sus decretos reglamentarios y los principios rectores del régimen de habeas data.
- Identificar y analizar las principales decisiones administrativas, lineamientos y criterios interpretativos adoptados por la Superintendencia de Industria y Comercio (SIC), como autoridad competente en materia de protección de datos personales, en relación con las cláusulas contractuales y el principio de responsabilidad demostrada.
- Contrastar la normativa vigente y la doctrina administrativa con la cláusula estándar de protección de datos personales utilizada por XYZ, evaluando su suficiencia jurídica frente a la diversidad de sectores económicos atendidos y los distintos niveles de sensibilidad de la información tratada.

CAPÍTULO PRIMERO: Análisis Normativo y Conceptual (Método Deductivo)

El presente capítulo tiene como finalidad desarrollar el marco normativo y conceptual que regula la protección de datos personales en el ordenamiento jurídico colombiano, en cumplimiento del primer objetivo específico de la investigación. Para ello, se realiza un recorrido sistemático que parte de los fundamentos constitucionales del derecho fundamental al habeas data y avanza hacia su desarrollo estatutario, reglamentario, jurisprudencial y doctrinal, con el propósito de construir una base teórica sólida que permita comprender el alcance, los principios rectores y la clasificación jurídica de los datos personales.

Este análisis resulta indispensable para el desarrollo del estudio, en tanto proporciona los criterios normativos y conceptuales que servirán como parámetro de contraste frente a la cláusula contractual de protección de datos utilizada por XYZ. En otras palabras, antes de evaluar la suficiencia jurídica del instrumento contractual, es necesario delimitar con precisión qué exige el ordenamiento jurídico colombiano en materia de tratamiento de datos personales, cuáles son los estándares de diligencia aplicables a los responsables y encargados, y qué implicaciones se derivan del principio de responsabilidad demostrada en contextos empresariales con tratamiento sectorial diferenciado. De esta manera, el capítulo no se limita a una exposición normativa descriptiva, sino que construye el andamiaje conceptual que permitirá, en los capítulos posteriores, efectuar un análisis crítico aplicado al caso concreto objeto de estudio.

1. Marco normativo colombiano de la protección de datos personales

1.1. Fundamento constitucional

El derecho a la protección de datos personales encuentra su consagración expresa en el artículo 15 de la Constitución Política de Colombia, adoptada por la Asamblea Nacional Constituyente en 1991, el cual reconoce el derecho fundamental al habeas data y faculta a todas las personas para conocer, actualizar y rectificar la información que sobre ellas repose en bases de datos o archivos de entidades públicas y privadas (Constitución Política de Colombia, 1991). Esta disposición constitucional no solo garantiza la autodeterminación informativa, sino que también establece límites claros al tratamiento de datos, en salvaguarda de la intimidad, el buen nombre y la dignidad humana.

El artículo 20 superior, además, garantiza la libertad de expresar y difundir el pensamiento y las opiniones, así como el derecho a informar y recibir información veraz e imparcial. No obstante, esta garantía no es absoluta, pues debe armonizarse con los derechos fundamentales a la intimidad, al buen nombre y al habeas data. La Corte Constitucional ha sostenido que la circulación de información encuentra límites cuando afecta injustificadamente la dignidad humana o vulnera la autodeterminación informativa de los titulares de los datos. En la Sentencia T-058 de 2013, el alto tribunal reiteró que la libertad de información debe ejercerse conforme a los principios de veracidad, imparcialidad y responsabilidad, especialmente cuando involucra datos personales susceptibles de afectar derechos fundamentales. De igual forma, en la Sentencia C-748 de 2011, al examinar la constitucionalidad del régimen estatutario de protección de datos personales, la Corte precisó que el habeas data constituye un derecho fundamental autónomo que impone límites tanto al Estado como a los particulares en el tratamiento de información personal, consolidando así un modelo de protección basado en la autodeterminación informativa y en la responsabilidad de los responsables del tratamiento.

1.2. Marco estatutario

La Ley 1581 de 2012 constituye el eje central del sistema general de protección de datos personales en Colombia. Expedida como ley estatutaria en desarrollo del artículo 15 de la Constitución Política, esta norma establece el marco jurídico aplicable al tratamiento de datos personales por parte de entidades públicas y privadas. La constitucionalidad de su contenido fue examinada de manera integral por la Corte Constitucional en la Sentencia C-748 de 2011, decisión en la cual el alto tribunal precisó que el habeas data es un derecho fundamental autónomo que comprende no solo la facultad de conocer, actualizar y rectificar información, sino también el poder de autorizar, controlar y limitar su tratamiento, consolidando así el principio de autodeterminación informativa como eje estructural del sistema.

En cuanto a su contenido, la Ley 1581 define el dato personal como toda información vinculada o que pueda asociarse a una persona natural determinada o determinable, configurando un concepto amplio que abarca formas de identificación directa e indirecta. Asimismo, organiza el régimen de protección sobre tres pilares fundamentales: (i) los derechos de los titulares, (ii) los deberes y responsabilidades de los responsables y encargados del tratamiento y (iii) un conjunto de principios rectores que orientan cualquier actividad de recolección, almacenamiento, uso, circulación o supresión de datos personales.

Esta norma se erige como parámetro obligatorio para compañías tecnológicas como XYZ, al exigir la implementación de medidas administrativas, técnicas y humanas destinadas a garantizar la seguridad, confidencialidad, integridad y legalidad del tratamiento de la información, en aplicación del principio de responsabilidad demostrada.

Por su parte, la Ley 1266 de 2008 regula de manera especial el tratamiento de datos financieros, crediticios, comerciales y de servicios, estableciendo un régimen particular aplicable a centrales de riesgo y operadores de información. Su constitucionalidad fue analizada en la Sentencia C-1011 de 2008, decisión en la cual la Corte reconoció el habeas data financiero como una manifestación específica del derecho fundamental consagrado en el artículo 15 superior, precisando los límites entre el derecho a la información económica y la protección del buen nombre. Posteriormente, en la Sentencia C-282 de 2021, el tribunal reiteró la naturaleza fundamental del derecho al habeas data en el ámbito financiero y examinó las modificaciones legislativas introducidas al régimen, enfatizando la necesidad de equilibrio entre la inclusión financiera y la protección efectiva de los titulares.

En conjunto, estas decisiones consolidan un bloque de constitucionalidad jurisprudencial que refuerza la estructura del sistema colombiano de protección de datos personales, imponiendo estándares de legalidad, proporcionalidad y razonabilidad que deben reflejarse no sólo en políticas internas, sino también en los instrumentos contractuales utilizados por las organizaciones.

1.3. Marco reglamentario

El desarrollo reglamentario de la Ley 1581 se consolida principalmente en el Decreto 1377 de 2013, compilado posteriormente en el Decreto Único Reglamentario 1074 de 2015. Este decreto regula aspectos esenciales como la autorización del titular, los avisos de privacidad, la transferencia y transmisión internacional de datos, el principio de responsabilidad demostrada (accountability) y la implementación de programas integrales

de cumplimiento normativo (Congreso de la República, 2013, 2015). El principio de responsabilidad demostrada, en particular, requiere que los encargados del tratamiento implementen acciones adecuadas y eficaces para asegurar el acatamiento de la normativa. Estas deben ser proporcionales a la naturaleza de los datos y al nivel de riesgo vinculado a su procesamiento.

Este enfoque resulta especialmente relevante para empresas del sector tecnológico, donde el volumen, la sensibilidad y la circulación internacional de la información incrementan sustancialmente la exposición a riesgos jurídicos y operativos. Adicionalmente, El RNBD, que es el Registro Nacional de Bases de Datos, se encuentra regulado por el Decreto 886, promulgado en 2014. Mediante este registro, la Superintendencia de Industria y Comercio realiza tareas de vigilancia, control e inspección sobre las bases de datos administradas por personas naturales y jurídicas, fortaleciendo así los mecanismos institucionales de supervisión (Congreso de la República, 2014).

1.4. Concepto integral de datos personales

El dato personal debe comprenderse desde una perspectiva integral que articule dimensiones lingüísticas, legales y doctrinales, permitiendo una aproximación teórica completa al fenómeno de la información en el ámbito digital, en tanto los datos no constituyen meros elementos técnicos, sino construcciones jurídicas, sociales y culturales vinculadas directamente con la identidad, la dignidad y la autodeterminación informativa de las personas (Martínez et al, 2025).

1.4.1. Dimensión lingüística

Desde el punto de vista lingüístico, Los datos personales son definidos por el Diccionario Panhispánico del Español Jurídico de la Real Academia Española como "toda información gráfica, acústica, fotográfica, alfabética o numérica que se refiere a personas físicas identificadas o que pueden ser identificables” (RAE, 2023). Etimológicamente, el término “dato” alude a la unidad mínima de información que permite conocer un hecho o deducir sus consecuencias, mientras que “personal” remite a aquello propio y particular de un individuo. En conjunto, el dato personal constituye la pieza informativa que permite construir la identidad de una persona y describir sus circunstancias individuales, en la medida en que los elementos lingüísticos y semánticos que lo conforman actúan como marcadores identitarios capaces de individualizar, categorizar y representar simbólicamente a los sujetos dentro de los sistemas sociales y comunicativos contemporáneos (Comb, 2024).

1.4.2. Dimensión legal

En el plano normativo, la Ley 1581 de 2012 consolida una definición amplia y funcional del dato personal, orientada a garantizar una protección efectiva en relación con los peligros derivados del tratamiento automatizado de información. Esta conceptualización no se limita a datos de identificación directa, sino que abarca cualquier elemento que, mediante asociación razonable, permita individualizar a una persona natural (Congreso de la República, 2012). Desde esta perspectiva, el dato personal adquiere la condición de objeto de tutela jurídica reforzada, al integrarse al núcleo fundamental del derecho a habeas data. Esta concepción impone a las organizaciones un deber reforzado de diligencia, responsabilidad y proporcionalidad en el tratamiento de la información.

1.4.3. Dimensión doctrinal

La doctrina contemporánea ha destacado la evolución del dato personal como un activo estratégico en los modelos de negocio actuales. Quintero Riveros (2023) sostiene

que el dato ha trascendido su concepción estrictamente ius fundamental para convertirse en un insumo productivo esencial dentro de la economía digital, lo cual incrementa la necesidad de establecer sistemas robustos de protección jurídica. Por su parte, Osuna Carreño (2024) señala que el artículo 15 constitucional no debe entenderse únicamente como un límite al poder estatal, sino como una garantía activa que faculta al ciudadano para controlar el flujo de su información en entornos digitales complejos.

Esta visión fortalece el carácter dinámico del habeas data, al concebir al titular como un agente activo en la gestión de su información personal. En la misma línea, Garriga (2016) afirma que la salvaguarda de datos personales es un derecho esencial autónomo, cuyo ejercicio efectivo exige la implementación de estructuras normativas, técnicas y organizacionales capaces de garantizar la autodeterminación informativa frente a los riesgos propios de la computación ubicua, la inteligencia artificial y el big data.

1.5. Principios rectores de la protección de datos personales

La Ley 1581 de 2012 consagra un conjunto de principios que orientan la interpretación y aplicación del régimen de protección de datos, entre los que sobresalen: seguridad, confidencialidad, transparencia, veracidad, libertad, finalidad, legalidad y acceso y circulación limitados (Congreso de la República, 2012, art. 4). Estos principios cumplen una función estructural dentro del sistema jurídico, al establecer límites claros al tratamiento de la información y fijar estándares mínimos de comportamiento para responsables y encargados. En particular, el principio de seguridad exige la adopción principio de confidencialidad, medidas administrativas, humanas y técnicas que se requieren para prevenir el uso, acceso, consulta, pérdida o adulteración no autorizados, mientras que el principio de confidencialidad impone un deber permanente de reserva, incluso después de finalizada la relación contractual. La SIC ha señalado que la correcta aplicación de estos principios exige una aproximación diferencial según la naturaleza del dato y el sector económico involucrado, lo cual refuerza la necesidad de cláusulas contractuales adaptables a los distintos contextos empresariales (SIC, 2023).

1.6. Clasificación de los tipos de datos personales

El ordenamiento jurídico colombiano clasifica los datos personales en cuatro categorías principales: públicos, semiprivados, privados y sensibles (Congreso de la República, 2012. Los datos públicos son aquellos que no están sujetos a confidencialidad y cuyo acceso es permitido por la ley, como los contenidos en registros públicos. Los datos semiprivados se refieren a información que, si bien no es íntima, interesa a un grupo determinado de personas, como los datos financieros y crediticios. Los datos privados corresponden a información íntima o reservada cuyo acceso sólo es posible mediante autorización del titular.

Para concluir, los datos sensibles son la categoría que tiene el nivel más alto de protección. Incluyen información vinculada a la raza, las creencias religiosas, la salud, la orientación sexual, los datos biométricos y la afiliación política o sindical. La gestión de esta clase de información requiere protocolos de seguridad rigurosos, cláusulas contractuales especializadas y salvaguardas reforzadas, debido a que está íntimamente relacionada con la dignidad humana y los derechos fundamentales (Congreso de la República, 2012; SIC, 2023; Kunst et al., 2024). Esta clasificación resulta especialmente relevante para el análisis del caso XYZ, en tanto la empresa gestiona información perteneciente a múltiples sectores económicos, incluyendo el sector salud, lo cual impone la obligación jurídica de diferenciar los niveles de protección y seguridad aplicables según la naturaleza del dato tratado.

CAPÍTULO SEGUNDO: Estudio Jurisprudencial y Doctrinal

2.1. Enfoque general y delimitación analítica

El presente capítulo tiene como finalidad desarrollar el segundo objetivo específico de la investigación, consistente en analizar el desarrollo jurisprudencial y administrativo del derecho fundamental al habeas data en Colombia, con especial énfasis en los criterios interpretativos adoptados por la autoridad nacional de protección de datos personales y su incidencia en la configuración de las cláusulas contractuales. A diferencia del capítulo anterior, centrado en la construcción normativa y conceptual del régimen jurídico, este apartado se orienta a examinar cómo dicho marco ha sido interpretado, aplicado y concretado por los órganos de control constitucional y administrativo.

En este sentido, el análisis se concentra, de una parte, en la evolución jurisprudencial de la Corte Constitucional en materia de autodeterminación informativa, principios rectores del tratamiento de datos personales y límites a la libertad contractual cuando se encuentran en juego derechos fundamentales. De otra parte, se estudian los lineamientos, resoluciones y guías emitidas por la Superintendencia de Industria y Comercio, en su calidad de autoridad nacional de protección de datos personales, a fin de identificar los estándares exigibles en materia de consentimiento informado, proporcionalidad, gestión del riesgo y responsabilidad demostrada.

Este capítulo parte de la premisa según la cual la cláusula de protección de datos personales no constituye un elemento accesorio dentro de los contratos civiles y comerciales, sino un instrumento jurídico estructural mediante el cual se materializa la garantía efectiva del derecho fundamental al habeas data. Por ello, la interpretación jurisprudencial y administrativa adquiere un papel determinante en la delimitación de su contenido mínimo, su alcance y sus límites, especialmente en contextos empresariales caracterizados por la alta complejidad tecnológica y la gestión intensiva de información, como ocurre en el sector del software y los servicios digitales.

2.2. Análisis jurisprudencial constitucional del derecho fundamental al habeas data

La construcción dogmática del derecho fundamental al habeas data en Colombia no ha sido estática ni meramente declarativa, sino el resultado de una evolución jurisprudencial progresiva desarrollada por la Corte Constitucional. A través de decisiones de constitucionalidad y tutela, el tribunal ha definido el contenido esencial del derecho, sus principios estructurantes y los límites aplicables al tratamiento de datos personales, consolidando una línea jurisprudencial coherente orientada a garantizar la autodeterminación informativa.

Como punto de partida estructural, la Sentencia T-414 de 1992 sentó las bases conceptuales del derecho a la autodeterminación informativa, al reconocer que el titular debe conservar un control real y efectivo sobre sus datos personales. En esta decisión, la Corte sostuvo que el habeas data no se limita al acceso formal a la información, sino que implica la facultad de conocer, actualizar, rectificar y decidir sobre su uso y circulación, estableciendo así el núcleo esencial del derecho.

Posteriormente, en ejercicio del control previo de constitucionalidad del proyecto que dio origen a la Ley 1581 de 2012, la Corte profirió la Sentencia C-748 de 2011, decisión que constituye un referente estructural del régimen colombiano de protección de datos. En esta providencia, el tribunal reconoció expresamente la autonomía del habeas data como derecho fundamental independiente y sistematizó los principios rectores que orientan su ejercicio: legalidad, finalidad, libertad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Asimismo, enfatizó que el tratamiento de datos sensibles exige medidas reforzadas de protección debido a su estrecha relación con la dignidad humana.

La consolidación de esta línea encuentra un punto de inflexión en la Sentencia T-058 de 2013, que puede considerarse sentencia hito en la materia. En esta decisión, la Corte articuló de manera sistemática el derecho al habeas data con la libertad de información y el derecho al buen nombre, estableciendo que la circulación de datos personales debe superar un juicio de veracidad, imparcialidad y proporcionalidad. El tribunal precisó que el consentimiento del titular no puede entenderse como una habilitación ilimitada, y que el tratamiento debe estar estrictamente vinculado a finalidades legítimas, específicas y previamente informadas. Con ello, la Corte reforzó la idea de que el derecho a la autodeterminación informativa impone límites materiales tanto a particulares como a autoridades públicas.

Esta línea se profundizó en la Sentencia T-197 de 2014, en la cual el alto tribunal desarrolló el alcance del principio de finalidad, advirtiendo que las autorizaciones amplias o indeterminadas vulneran el derecho fundamental cuando permiten tratamientos desproporcionados o no relacionados con el objeto legítimo que justificó la recolección de la información. De manera complementaria, la Sentencia T-063 de 2017 profundizó en la protección reforzada de los datos sensibles, estableciendo que su tratamiento debe superar un estricto test de proporcionalidad, necesidad y razonabilidad, y que cualquier habilitación contractual debe justificar la indispensabilidad del dato y prever salvaguardas técnicas y organizativas adecuadas.

De este modo, la línea jurisprudencial puede sintetizarse en tres ejes estructurales: (i) la consolidación del habeas data como derecho fundamental autónomo basado en la autodeterminación informativa; (ii) la exigencia de proporcionalidad y finalidad específica en todo tratamiento de datos; y (iii) la protección reforzada de los datos sensibles mediante estándares estrictos de seguridad y consentimiento informado. Bajo estos parámetros, la validez constitucional de las cláusulas contractuales de protección de datos personales depende de su capacidad real para garantizar estos principios, lo cual resulta incompatible con esquemas de estandarización rígida, genérica o descontextualizada.

Estos criterios jurisprudenciales constituyen el marco interpretativo esencial para evaluar, en el capítulo siguiente, la suficiencia jurídica de la cláusula utilizada por XYZ, particularmente en escenarios de tratamiento sectorial diferenciado y gestión intensiva de información.

2.3. La Superintendencia de Industria y Comercio como autoridad nacional de protección de datos personales

El régimen colombiano de protección de datos personales no se agota en su dimensión normativa y jurisprudencial, sino que se estructura institucionalmente a través de

un sistema de inspección, vigilancia y control cuyo eje central es la Superintendencia de Industria y Comercio (SIC). En virtud de la Ley 1581 de 2012 y su desarrollo reglamentario en el Decreto 1074 de 2015, esta entidad fue designada como Autoridad Nacional de Protección de Datos Personales, con competencia para garantizar el cumplimiento del régimen general de habeas data en el territorio colombiano.

En ejercicio de esta función, la SIC no solo impone sanciones administrativas ante vulneraciones al régimen legal, sino que también ejerce facultades preventivas y orientadoras mediante la emisión de circulares, conceptos jurídicos y lineamientos técnicos que precisan los estándares exigibles a responsables y encargados del tratamiento. Esta doble dimensión correctiva y pedagógica ha permitido consolidar un cuerpo doctrinal que desarrolla en la práctica los principios constitucionales de legalidad, transparencia, finalidad y responsabilidad demostrada.

Desde el punto de vista competencial, la SIC puede ordenar la adopción de medidas correctivas, imponer multas, exigir la modificación o supresión de bases de datos, ordenar la implementación de políticas internas y verificar el cumplimiento de obligaciones como el consentimiento informado y las medidas de seguridad. Además, administra el Registro Nacional de Bases de Datos (RNBD), instrumento que fortalece la supervisión del tratamiento de información personal bajo el régimen general.

La actuación reciente de la SIC evidencia la concreción de estas facultades. En octubre de 2025, la Dirección de Investigaciones de Protección de Datos Personales sancionó con el cierre inmediato y definitivo de las operaciones de tratamiento de datos personales de las sociedades World Foundation y Tools for Humanity Corporation en Colombia, tras comprobar que estas recolectaron y trataron datos biométricos sensibles sin cumplir las obligaciones legales de información, consentimiento y seguridad exigidas por la Ley 1581 de 2012. La autoridad ordenó además la supresión de los datos recolectados, reafirmando la protección del derecho fundamental al habeas data frente a actividades comerciales que vulneran la normativa de protección de datos personales (SIC, 2025).

En un caso similar, en 2025 la SIC impuso a Mercado Libre Colombia Ltda. una multa de más de 214 millones de pesos por condicionar el acceso de usuarios al suministro de datos biométricos mediante reconocimiento facial, violando los principios constitucionales y legales del tratamiento de información sensible (SIC, 2025). A su vez, la Delegatura de Protección de Datos de la SIC reportó en agosto de 2025 el inicio de más de cien investigaciones y la imposición de multas que superan los cinco mil millones de pesos por vulneraciones al régimen de protección de datos personales, lo que revela una intensificación de la función de inspección, vigilancia y control en los últimos años (SIC, 2025).

A pesar de lo anterior, el sistema institucional colombiano no es absolutamente concentrado. Existen regímenes especiales en los que la competencia se distribuye sectorialmente según la naturaleza de la información tratada. En particular, el dato financiero y crediticio se encuentra regulado por la Ley 1266 de 2008, conocida también como la Ley de Habeas Data Financiero, cuyo control respecto de entidades vigiladas corresponde a la Superintendencia Financiera de Colombia. Según información oficial de la SIC, por regla general la vigilancia de los operadores, las fuentes y usuarios de información crediticia y comercial es ejercida por la propia SIC, “sin embargo, cuando la fuente, usuario u operador sea una entidad vigilada por la Superintendencia Financiera, será esta última la entidad que ejerza dicha vigilancia”(SIC, s/f).

En desarrollo de este régimen especial, en 2024 y 2025 la Superintendencia Financiera estableció plazos específicos para la atención de peticiones, quejas y reclamos relacionados con el derecho de habeas data por parte de entidades vigiladas, obligando a que estos se resuelvan en un máximo de quince días hábiles. Esta medida busca garantizar que la atención a los titulares de información financiera se haga de manera oportuna y efectiva, frente al aumento de quejas vinculadas con el fraude y la vulneración de derechos de los consumidores financieros (Saavedra, 2024).

Esta distinción no implica una fragmentación del derecho fundamental, sino una diferenciación funcional dentro del sistema de control. Mientras la SIC actúa como autoridad nacional bajo el régimen general de la Ley 1581 de 2012, la Superintendencia Financiera ejerce funciones sectoriales respecto del habeas data financiero en entidades vigiladas bajo la Ley 1266 de 2008. Por tanto, el análisis jurídico necesario para evaluar la conformidad de una cláusula de protección de datos personales debe partir de la identificación de la naturaleza de la información tratada y del régimen que le es aplicable. Si se trata de datos personales en general, y no de información financiera regulada, se aplicarán los estándares y obligaciones definidos por la SIC bajo el régimen general. Si, por el contrario, la información es financiera o crediticia y se trata en el contexto de entidades vigiladas, los lineamientos y tiempos de respuesta definidos por la Superintendencia Financiera para Habeas Data Financiero serán determinantes.

2.4. Desarrollo doctrinal y administrativo: hacia un modelo flexible y contextualizado de cláusula contractual

La doctrina administrativa de la SIC ha consolidado un modelo flexible, dinámico y contextualizado de cláusula de protección de datos personales, orientado a superar la concepción formalista del cumplimiento normativo. En la Guía sobre el tratamiento de datos personales con fines de marketing y publicidad, la SIC enfatiza que el consentimiento informado solo puede considerarse válido cuando el titular comprende claramente qué datos serán recolectados, con qué finalidad, durante cuánto tiempo y bajo qué medidas de seguridad, descartando expresamente las cláusulas genéricas y promoviendo una redacción clara, específica y sectorial (SIC, 2019).

Por su parte, la Guía de Responsabilidad Demostrada (Accountability) introduce un cambio paradigmático al establecer que las organizaciones deben demostrar de manera verificable el cumplimiento normativo, mediante la adopción de políticas internas, auditorías periódicas, análisis de riesgos, protocolos de seguridad y programas de capacitación. En este marco, la cláusula contractual adquiere un valor probatorio esencial, al constituir uno de los principales instrumentos mediante los cuales la empresa acredita su diligencia y su compromiso con la protección válida de los derechos de los titulares (SIC, 2022).

Finalmente, el Concepto 14-064430 de 2014, relativo al tratamiento de datos en entornos de computación en la nube, resulta especialmente relevante para empresas proveedoras de software, al establecer que la externalización de infraestructuras tecnológicas no exime de responsabilidad al encargado del tratamiento, quien debe garantizar niveles adecuados de seguridad, confidencialidad y control, incorporando estas exigencias de manera expresa en las cláusulas contractuales.

2.5. Análisis del precedente administrativo: Resolución 16582 de 2025 (Mercado Libre Colombia Ltda.)

El estudio del precedente administrativo en materia de protección de datos personales exige identificar no sólo la existencia de decisiones sancionatorias, sino el criterio jurídico que éstas consolidan dentro de la línea interpretativa de la autoridad nacional. En los últimos años, la Superintendencia de Industria y Comercio ha venido fortaleciendo una postura estricta frente al tratamiento de datos sensibles, particularmente en entornos digitales donde el acceso a servicios se condiciona a la entrega de información biométrica.

Dentro de esta evolución, la Resolución 16582 de 2025, proferida contra Mercado Libre Colombia Ltda., constituye un hito administrativo relevante. Antes de esta decisión, la SIC ya había sostenido que el principio de libertad implica que el consentimiento debe ser previo, expreso e informado, y que el tratamiento de datos sensibles exige estándares reforzados de proporcionalidad y necesidad. Sin embargo, esta resolución profundiza el análisis al aplicar dichos principios a un esquema de autenticación biométrica obligatoria en una plataforma digital de uso masivo.

En el caso concreto, la autoridad determinó que la empresa condicionaba el acceso a su plataforma al suministro obligatorio de datos biométricos (específicamente reconocimiento facial) sin ofrecer alternativas razonables de autenticación. La SIC consideró que esta práctica vulneraba los principios de libertad, legalidad y proporcionalidad, al imponer un tratamiento de datos sensibles sin demostrar su estricta necesidad ni garantizar un consentimiento verdaderamente libre, en la medida en que el usuario no contaba con opciones reales para negarse sin perder el acceso al servicio.

La relevancia del precedente radica en la regla que se desprende de la decisión: ninguna organización puede supeditar el acceso a bienes o servicios a la entrega obligatoria de datos sensibles cuando existan mecanismos menos invasivos que permitan alcanzar la misma finalidad. En este sentido, la autoridad no solo impuso una sanción económica por valor de $214.405.120 COP, sino que ordenó la supresión de los mecanismos obligatorios de autenticación biométrica y la implementación de sistemas alternativos respetuosos del derecho fundamental al habeas data.

Este pronunciamiento consolida tres criterios estructurales dentro de la doctrina administrativa: (i) el consentimiento no es válido cuando se encuentra condicionado de manera desproporcionada; (ii) el tratamiento de datos sensibles debe superar un juicio estricto de necesidad y proporcionalidad; y (iii) las cláusulas contractuales o términos y condiciones no pueden legitimar prácticas que, en la realidad operativa, vacían de contenido la autodeterminación informativa del titular.

Desde la perspectiva del presente estudio, este precedente resulta especialmente significativo, pues demuestra que la autoridad administrativa evalúa no solo la redacción formal de las cláusulas, sino su impacto material en los derechos de los titulares. En consecuencia, cualquier modelo contractual que incorpore habilitaciones amplias, genéricas o que no contemple alternativas diferenciadas según el nivel de sensibilidad del dato tratado, puede ser considerado insuficiente frente a los estándares actuales de control administrativo.

2.6. Tendencias sancionatorias y criterios de graduación y absolución en la doctrina administrativa

El análisis sistemático de las decisiones administrativas publicadas por la Superintendencia de Industria y Comercio en materia de protección de datos personales permite identificar una línea doctrinal consolidada que trasciende la resolución de casos particulares y configura verdaderos criterios estructurales de responsabilidad administrativa. La revisión de los actos sancionatorios, decisiones de archivo y órdenes correctivas evidencia que la autoridad ha venido construyendo un modelo de control cada vez más sustancial, orientado a verificar no solo la existencia formal de políticas y cláusulas contractuales, sino su eficacia real para garantizar el derecho fundamental al habeas data.

2.6.1. Endurecimiento progresivo del estándar sancionatorio

En los últimos años se observa un fortalecimiento significativo del ejercicio de la potestad sancionatoria por parte de la SIC, particularmente frente a conductas relacionadas con el tratamiento de datos sensibles sin consentimiento expreso, la implementación deficiente de medidas de seguridad, la ausencia de políticas de tratamiento debidamente adoptadas, el uso de cláusulas contractuales amplias o genéricas y el incumplimiento del deber de reporte de incidentes de seguridad. La práctica administrativa demuestra que la autoridad ha adoptado una postura más rigurosa cuando se constata que el responsable del tratamiento no ha implementado mecanismos proporcionales al nivel de riesgo asociado a la información recolectada.

Las decisiones recientes revelan, además, que el control administrativo ya no se limita a la imposición de multas económicas, sino que incorpora órdenes estructurales de corrección orientadas a transformar la gestión interna de las organizaciones. Entre estas órdenes se encuentran la modificación obligatoria de cláusulas contractuales, la implementación de políticas diferenciadas según el tipo de dato tratado, la supresión de bases de datos recolectadas sin autorización válida, el rediseño de mecanismos de autenticación y la adopción de programas permanentes de capacitación en protección de datos. Este giro evidencia que el análisis de la autoridad es sustancial y no meramente formal, pues evalúa si el tratamiento cumple efectivamente con los principios de finalidad, libertad, proporcionalidad y responsabilidad demostrada.

2.6.2. Criterios de graduación de la sanción

El examen comparado de las resoluciones administrativas permite advertir que la graduación de la sanción responde a un juicio de proporcionalidad que articula la gravedad objetiva de la conducta con el nivel de diligencia desplegado por el responsable del tratamiento. En este sentido, la autoridad valora la naturaleza del dato comprometido, imponiendo mayores sanciones cuando se trata de datos sensibles; considera el número de titulares afectados; analiza la existencia de reincidencia; examina el grado de diligencia demostrado por la organización durante la investigación; y verifica si existían previamente políticas internas, análisis de riesgo y protocolos documentados. Asimismo, la colaboración con la autoridad durante el trámite administrativo constituye un elemento relevante para la determinación de la sanción, ya sea como atenuante o como indicador de buena fe. De esta manera, la SIC aplica un modelo de responsabilidad administrativa que integra elementos preventivos y correctivos, privilegiando la proporcionalidad y la evaluación contextual de cada caso.

2.6.3. Criterios de absolución o archivo

No todas las investigaciones culminan con la imposición de sanciones. El estudio de decisiones de archivo o exoneración demuestra que la autoridad absuelve cuando la organización logra acreditar, de manera documentada y verificable, la existencia de autorizaciones válidas, políticas internas implementadas de forma efectiva, análisis de riesgos actualizados, protocolos técnicos de seguridad y programas de capacitación periódica en materia de protección de datos. Igualmente, la atención oportuna y completa de los requerimientos formulados por los titulares y por la autoridad administrativa constituye un elemento determinante en la valoración de la responsabilidad. En estos escenarios, el principio de responsabilidad demostrada opera como eje estructural del sistema, en tanto el cumplimiento normativo no se presume, sino que debe acreditarse mediante evidencia objetiva. La práctica administrativa confirma, por tanto, que la ausencia de documentación y trazabilidad suele derivar en sanción, mientras que la implementación verificable de un programa integral de protección de datos puede constituir eximente o atenuante de responsabilidad.

2.6.4. Regla estructural derivada de la práctica administrativa

El análisis sistemático de la doctrina administrativa permite formular una regla general aplicable al diseño de cláusulas contractuales: la validez jurídica de una cláusula de protección de datos no depende exclusivamente de su existencia formal en el contrato o en los términos y condiciones, sino de su coherencia con el modelo de gestión del riesgo adoptado por la organización. En consecuencia, una cláusula genérica, no diferenciada por sector económico, tipo de dato o finalidad específica del tratamiento, difícilmente podrá superar el escrutinio administrativo si no se encuentra acompañada de políticas, protocolos y medidas técnicas proporcionales al nivel de sensibilidad de la información tratada. Esta conclusión se articula con la línea jurisprudencial constitucional consolidada por la Sentencia C-748 de 2011, la Sentencia T-058 de 2013 y la Sentencia T-063 de 2017, así como con los lineamientos administrativos contenidos en la Circular Única y en las guías de responsabilidad demostrada expedidas por la autoridad de control.

Tabla 1

Síntesis jurisprudencial, administrativa y doctrinal sobre cláusulas de protección de datos personales en Colombia

Documento / Decisión	Regla jurisprudencial o administrativa	Criterio aplicable a cláusulas
Sentencia C-748 de 2011	Constitucionalización del habeas data y desarrollo de principios estructurales del tratamiento	Las cláusulas deben reflejar finalidad específica, legalidad y proporcionalidad

Sentencia T-058 de 2013	El consentimiento no puede ser amplio ni indeterminado; debe ser proporcional a la finalidad	Prohíbe habilitaciones genéricas o ilimitadas
Sentencia T-063 de 2017	Protección reforzada de datos sensibles	Exige diferenciación contractual según nivel de riesgo
Circular Única – Título V (SIC)	Gestión integral de seguridad y cumplimiento	Impone cláusulas alineadas con medidas técnicas y organizacionales
Guía de Responsabilidad Demostrada (SIC, 2022)	Accountability verificable y documentada	La cláusula debe ser coherente con un sistema integral de gestión
Resolución 16582 de 2025	Prohibición de tratamiento biométrico obligatorio desproporcionado	Impide condicionamiento contractual abusivo y exige alternativas menos invasivas

Nota. Elaboración propia

El estudio jurisprudencial y administrativo desarrollado en este capítulo demuestra que el régimen colombiano de protección de datos personales ha evolucionado hacia un modelo de control sustancial, en el cual la autoridad no se limita a verificar la presencia formal de cláusulas contractuales, sino que evalúa su coherencia con la gestión real del riesgo y con la garantía efectiva de la autodeterminación informativa. La tendencia sancionatoria evidencia un endurecimiento frente a tratamientos desproporcionados, genéricos o carentes de soporte técnico, mientras que los criterios de absolución confirman que la implementación documentada de programas de cumplimiento puede mitigar o incluso excluir la responsabilidad administrativa.

Este marco interpretativo refuerza la hipótesis central del presente trabajo: la utilización de cláusulas estándar rígidas y no contextualizadas resulta potencialmente insuficiente frente a los estándares actuales de control. En consecuencia, el capítulo siguiente desarrollará el análisis aplicado de la cláusula utilizada por XYZ, con el fin de identificar vacíos, evaluar su adecuación normativa y proponer una reformulación jurídica alineada con los criterios de proporcionalidad, diferenciación y responsabilidad demostrada exigidos por la autoridad colombiana de protección de datos personales.

CAPÍTULO TERCERO: Contraste de la cláusula estándar con la ley 1581 y el principio de responsabilidad demostrada Accountability

El presente capítulo constituye el núcleo central de la investigación, en tanto permite confrontar el marco normativo vigente en materia de protección de datos personales con la realidad contractual aplicada por XYZ. A partir del examen de los modelos contractuales utilizados por la empresa, se analiza de manera específica la cláusula estándar de tratamiento de datos personales, con el propósito de evaluar su idoneidad jurídica frente a las exigencias previstas en la Ley 1581 de 2012, el Decreto 1074 de 2015 y los lineamientos fijados por la Superintendencia de Industria y Comercio.

Este contraste permite determinar si la estructura contractual actualmente implementada resulta coherente con los principios de legalidad, finalidad, proporcionalidad, seguridad y, especialmente, con el principio de responsabilidad demostrada (accountability), entendido como la obligación de implementar y acreditar medidas efectivas, proporcionales y verificables en función del riesgo asociado al tratamiento de datos personales. En este sentido, el capítulo se orienta a identificar eventuales vacíos jurídicos y tensiones estructurales derivadas del uso de cláusulas estandarizadas en contextos sectoriales heterogéneos.

3.1. Descripción de las funciones desarrolladas en la práctica profesional

La práctica profesional se realizó entre el 2 de septiembre de 2025 y el 28 de febrero de 2026, en virtud de un contrato de aprendizaje celebrado con la empresa XYZ, con una duración total de seis meses. La vinculación se efectuó en el área legal y de cumplimiento (compliance), unidad estratégica encargada de asegurar que las actividades empresariales se ejecuten en conformidad con el ordenamiento jurídico vigente y con los estándares internos de control normativo. Desde una perspectiva organizacional, el cumplimiento normativo constituye un componente esencial de la gobernanza corporativa, orientado a prevenir riesgos legales, operativos y reputacionales mediante la adopción de políticas, procedimientos y mecanismos de supervisión sistemática (Ramos & Weiss, 2018; Rincón & Valbuena, 2021).

En este contexto, las funciones desarrolladas se orientaron principalmente al apoyo jurídico, documental y administrativo en los procesos contractuales, contribuyendo a la estructuración, control y seguimiento de los instrumentos legales que regulan las relaciones de la empresa con clientes, proveedores y aliados estratégicos. Estas labores incluyeron la elaboración de conceptos jurídicos internos, la revisión formal de contratos, la gestión documental contractual, la actualización de repositorios digitales, el seguimiento de procesos de firma electrónica mediante la plataforma DocuSign, así como el control de contratos pendientes de suscripción, modificación o vencimiento.

La gestión documental ocupó un lugar central dentro de las actividades desarrolladas, en tanto permitió garantizar la trazabilidad, integridad y disponibilidad de los documentos contractuales. La literatura especializada destaca que la adecuada administración de archivos jurídicos constituye un elemento clave del compliance empresarial, al facilitar los procesos de auditoría, control interno y respuesta ante requerimientos administrativos y judiciales (Gómez & Sánchez, 2019; Ponce & Rodríguez, 2020). En este sentido, establecimiento y la preservación de bases de datos contractuales organizadas ayudaron a robustecer los sistemas de control interno y a reducir el riesgo jurídico.

Asimismo, se realizó un acompañamiento constante en los procesos de firma digital, validando la correcta suscripción electrónica de los contratos conforme a los lineamientos establecidos en la Ley 527 de 1999, el Decreto 2364 de 2012 y las directrices de la Superintendencia de Industria y Comercio (SIC). La utilización de plataformas de firma electrónica responde a la tendencia contemporánea de digitalización contractual, la cual exige garantizar la autenticidad, integridad, no repudio y trazabilidad de los documentos electrónicos, especialmente en contextos empresariales de alta complejidad tecnológica (Camacho & López, 2018; SIC, 2023).

De igual forma, se brindó apoyo en la elaboración de respuestas a peticiones, quejas, reclamos y sugerencias (PQRS), incorporando criterios jurídicos orientados a la protección de los derechos de los usuarios, la observancia del principio de legalidad y el fortalecimiento de la confianza institucional. Diversos estudios subrayan que los sistemas de atención al usuario constituyen un indicador fundamental del cumplimiento normativo, en tanto permiten evidenciar el grado de diligencia empresarial frente a los derechos de los titulares de la información y los consumidores (Molina & Hernández, 2020; Rojas & Pérez, 2022).

Desde una perspectiva formativa, la práctica permitió el fortalecimiento de competencias profesionales en derecho contractual, protección de datos personales, cumplimiento normativo y gestión documental, integrando conocimientos teóricos con su aplicación práctica en entornos empresariales reales. Esta metodología ayudó a que se desarrollara una perspectiva crítica acerca de cómo las normas jurídicas se concretan realmente en la dinámica organizacional, especialmente con respecto a la implementación de políticas para el manejo de datos personales y la escritura de cláusulas contractuales.

Como resultado del ejercicio profesional, fue posible identificar tensiones relevantes entre la teoría normativa y la práctica contractual, especialmente en lo concerniente al uso de cláusulas estandarizadas de protección de datos personales. Si bien la estandarización contractual favorece la eficiencia operativa, la doctrina contemporánea advierte que su aplicación indiscriminada puede generar vacíos jurídicos y riesgos de incumplimiento cuando no se ajusta a las particularidades sectoriales y al nivel de sensibilidad de la información tratada (Montoya & Pineda, 2019; Rodríguez & Uprimny, 2021). Esta observación empírica constituyó el punto de inicio para plantear el problema de investigación, orientado a analizar los riesgos jurídicos derivados de la utilización de una cláusula uniforme en escenarios contractuales heterogéneos, particularmente en empresas tecnológicas que gestionan información en sectores altamente diferenciados.

3.2. Tipología contractual utilizada por XYZ

En coherencia con su objeto social, centrado en el desarrollo, comercialización, implementación, consultoría y soporte de soluciones de planificación de recursos empresariales (ERP), XYZ parte de una tipología amplia, dinámica y flexible, orientada a responder a la diversidad de necesidades operativas, tecnológicas y estratégicas de sus clientes. La creación de estructuras contractuales complejas es un instrumento fundamental para la distribución de riesgos, la salvaguarda de activos intangibles y la garantía de seguridad jurídica en entornos digitales que cambian con frecuencia, dentro del derecho empresarial contemporáneo (Camacho & López, 2018; Montoya & Pineda, 2019).

Dentro de los principales instrumentos contractuales empleados por la compañía se destacan, en primer lugar, los contratos de licencia de uso de software, mediante los cuales XYZ otorga a sus clientes derechos limitados, no exclusivos, intransferibles y temporales para la utilización de sus plataformas tecnológicas, conservando la titularidad plena de los

derechos patrimoniales de autor sobre los desarrollos informáticos. Este tipo contractual responde a los lineamientos establecidos por el régimen de propiedad intelectual colombiano, particularmente por la Decisión Andina 351 de 1993 y la Ley 23 de 1982, así como por la doctrina especializada que concibe el software como una obra protegida cuya explotación económica puede ser objeto de licenciamiento sin transferencia del dominio (Rengifo, 2017; Vargas & Correa, 2020).

En segundo lugar, XYZ celebra contratos de prestación de servicios tecnológicos, los cuales comprenden actividades de consultoría, instalación, parametrización, capacitación, mantenimiento evolutivo y soporte técnico. Estos contratos resultan fundamentales para garantizar la correcta implementación, operación y optimización de las soluciones ERP, permitiendo adaptar las plataformas a los procesos internos de cada cliente. La literatura jurídica y administrativa ha señalado que este tipo de contratos se inscribe dentro de una categoría híbrida que combina elementos del arrendamiento de servicios, la consultoría especializada y la asistencia técnica, lo que exige una regulación contractual detallada en materia de alcance, niveles de servicio (SLA), responsabilidad, confidencialidad y protección de datos (Camacho & López, 2018; Ponce & Rodríguez, 2020).

Además, la empresa firma contratos de confidencialidad (NDA) y acuerdos para el tratamiento de datos personales. Estos están enfocados en salvaguardar la información delicada que se intercambia durante las relaciones comerciales y en fijar los compromisos particulares que resultan del régimen de protección de datos personales. En el ámbito empresarial, estos instrumentos adquieren una importancia particular, donde el flujo constante de información empresarial, financiera, operativa y personal incrementa de manera sustancial los riesgos asociados a la pérdida, filtración o uso indebido de los datos. En este sentido, la doctrina contemporánea sostiene que la adecuada estructuración contractual en cuanto a la reserva y protección de datos constituye un eje central del compliance digital, en tanto permite materializar los principios de legalidad, seguridad, confidencialidad y responsabilidad demostrada (Montoya & Pineda, 2019; Rincón & Valbuena, 2021).

En el ámbito interno, XYZ celebra contratos laborales y de prestación de servicios profesionales con su personal técnico, administrativo y comercial, incorporando cláusulas específicas sobre confidencialidad, propiedad intelectual, protección de datos y uso adecuado de las plataformas de gestión de información . Estas estipulaciones contractuales buscan prevenir conflictos jurídicos relacionados con la apropiación indebida de desarrollos tecnológicos, la fuga de información estratégica y el incumplimiento de las políticas internas de seguridad. Diversos estudios destacan que la incorporación de cláusulas de compliance en los contratos laborales fortalece la cultura organizacional, promueve la autorregulación y contribuye a la mitigación del riesgo legal y reputacional (Ramos & Weiss, 2018; Gómez & Sánchez, 2019).

Finalmente, en atención a su presencia internacional, particularmente en Perú y Ecuador, la empresa celebra contratos de distribución, comercialización y representación, los cuales incorporan cláusulas especiales sobre ley aplicable, jurisdicción competente, solución de controversias, protección transfronteriza de datos y transferencia internacional de información personal. En estos escenarios, la complejidad jurídica se incrementa de manera significativa, dado que confluyen distintos regímenes normativos en materia contractual, comercial, tecnológica y de protección de datos, lo que exige una cuidadosa armonización de las obligaciones legales y contractuales. La doctrina especializada ha subrayado que la correcta estructuración de contratos internacionales en entornos digitales

requiere una visión integral del derecho comparado, la regulación transfronteriza de datos y los estándares internacionales de salvaguarda de los datos (Delgado & Puyana, 2020; Uprimny & Sánchez, 2021).

Esta diversidad contractual convierte a la gestión jurídica de XYZ en un eje estratégico para la mitigación de riesgos legales, reputacionales y financieros, en tanto la correcta estructuración de los contratos constituye un mecanismo esencial para asegurar la certeza jurídica, la protección de activos intangibles y la estabilidad de las relaciones comerciales. En particular, la heterogeneidad de los sectores atendidos (que incluye manufactura, comercio, retail, salud, servicios y hospitalidad) impone la necesidad de adoptar modelos contractuales flexibles, diferenciados y adaptables, especialmente en lo concerniente a las cláusulas de protección de datos personales, el cual debe ajustarse a la naturaleza del tratamiento, al tipo de información procesada y al nivel de riesgo asociado (Montoya & Pineda, 2019; SIC, 2022).

Desde esta perspectiva, el análisis de la tipología contractual utilizada por XYZ permite comprender la complejidad operativa y jurídica de su modelo de negocio, así como identificar los desafíos que enfrenta la empresa en materia de cumplimiento normativo, particularmente en lo relativo a la necesidad de superar la estandarización rígida de cláusulas y avanzar hacia esquemas contractuales más dinámicos, sectorizados y acordes con los estándares contemporáneos del derecho digital y del compliance corporativo.

3.3. Cláusulas contractuales estandarizadas relevantes

Dentro del conjunto de contratos utilizados por XYZ, se han identificado una serie de cláusulas estandarizadas de carácter transversal, cuyo propósito principal es garantizar la salvaguarda de los intereses jurídicos, económicos y reputacionales de la compañía, así como asegurar el cumplimiento del marco normativo vigente. Estas cláusulas constituyen herramientas esenciales de gestión del riesgo legal y operan como mecanismos preventivos frente a eventuales contingencias contractuales, regulatorias y sancionatorias. En el ámbito del derecho empresarial contemporáneo, la estandarización de cláusulas responde a la necesidad de optimizar procesos, asegurar uniformidad interpretativa y fortalecer la seguridad jurídica, especialmente en organizaciones con alto volumen de contratación y presencia multisectorial (Camacho & López, 2018; Montoya & Pineda, 2019).

Entre las cláusulas más relevantes se encuentran aquellas relativas a propiedad intelectual, prevención de blanqueo de capitales y financiamiento del terrorismo (SARLAFT), confidencialidad, indemnidad y tratamiento de datos personales, las cuales conforman un núcleo normativo esencial dentro de la arquitectura contractual de la empresa. La cláusula de propiedad intelectual tiene como finalidad principal garantizar que los derechos patrimoniales derivados del desarrollo, modificación, adaptación y actualización del software permanezcan en cabeza de XYZ, aun cuando dichos desarrollos se realicen en el marco de relaciones contractuales con clientes, aliados o proveedores. Esta estipulación encuentra sustento en la Ley 23 de 1982, la Decisión Andina 351 de 1993 y la Ley 1450 de 2011, que reconocen el software como una obra protegida por el derecho de autor y permiten su explotación económica mediante contratos de licencia, sin que ello implique transferencia del dominio. La doctrina ha resaltado que, en el sector tecnológico, la adecuada regulación contractual de la propiedad intelectual resulta indispensable para proteger los activos intangibles, preservar la ventaja competitiva y prevenir conflictos derivados del uso no autorizado o la apropiación indebida del conocimiento (Rengifo, 2017; Vargas & Correa, 2020).

Por su parte, la cláusula de prevención de blanqueo de capitales y financiamiento del terrorismo (SARLAFT) incorpora un conjunto de obligaciones dirigidas a garantizar que los clientes y aliados comerciales adopten medidas razonables de debida diligencia, identificación, verificación y reporte de operaciones sospechosas, conforme a lo dispuesto en el Decreto 830 de 2021 y la Circular Básica Jurídica de la Superintendencia de Sociedades. Esta cláusula se inserta dentro de los modernos sistemas de cumplimiento normativo empresarial, orientados a prevenir riesgos penales, administrativos y reputacionales asociados a la utilización indebida de las plataformas tecnológicas para actividades ilícitas. La literatura especializada destaca que la incorporación de cláusulas SARLAFT en los contratos comerciales fortalece la cultura de cumplimiento, promueve la transparencia y reduce significativamente la exposición jurídica de las organizaciones (Gómez & Sánchez, 2019; Ramos & Weiss, 2018).

En cuanto a la cláusula de confidencialidad, esta busca proteger la información clasificada como reservada, estratégica o sensible, intercambiada durante la ejecución del contrato, estableciendo restricciones claras sobre su uso, divulgación y reproducción. Asimismo, contempla consecuencias jurídicas frente a su incumplimiento, tales como la terminación anticipada del contrato y la obligación de indemnizar los perjuicios causados. Desde la perspectiva doctrinal, la confidencialidad constituye uno de los pilares de la contratación tecnológica, en tanto garantiza la protección del know-how empresarial, los secretos industriales, las bases de datos y la información estratégica, elementos esenciales para la sostenibilidad y competitividad de las empresas en la economía digital (Delgado & Puyana, 2020; Rincón & Valbuena, 2021).

De manera complementaria, la cláusula de indemnidad delimita la responsabilidad civil de XYZ frente a daños ocasionados por actuaciones ajenas a su control directo, trasladando al contratante la obligación de asumir los perjuicios derivados de conductas imputables a su propio actuar o al de terceros bajo su dependencia. Esta estipulación contractual responde al principio de asignación eficiente del riesgo, ampliamente desarrollado en la teoría del derecho contractual, según el cual cada parte debe asumir las consecuencias jurídicas de aquellos eventos que se encuentran dentro de su esfera de control (Ponce & Rodríguez, 2020; Rojas, 2021).

Sin embargo, en el contexto de la investigación actual, la cláusula sobre el tratamiento de datos personales se vuelve esencial, ya que tiene como objetivo concretar la observancia del sistema colombiano de protección de datos. Esto incluye especialmente la Ley 1581 del 2012, el Decreto 1074 del 2015 y las directrices emitidas por la Superintendencia de Industria y Comercio (SIC). Esta cláusula también incluye el principio de responsabilidad demostrada (accountability), que estipula que los encargados del tratamiento no solo tienen que acatar la normativa de forma oficial, sino también evidenciar, de manera objetiva, comprobable y documentada, la implementación de acciones efectivas para asegurar la protección de los datos personales (SIC, 2022).

Desde un punto de vista doctrinal, la cláusula de protección de datos es una herramienta legal clave para el aseguramiento real del derecho fundamental al habeas data, ya que establece los propósitos del tratamiento, determina las obligaciones del encargado y del responsable, reconoce los derechos del titular y determina las medidas técnicas, administrativas y organizativas con el fin de evitar sucesos de seguridad. En el marco de la economía digital, numerosos autores coinciden en que la protección de los datos personales se ha vuelto un elemento esencial del cumplimiento corporativo. Su efectividad depende, en gran medida, de la claridad, calidad y flexibilidad de las cláusulas contractuales que dirigen los flujos de información (Montoya & Pineda, 2019; Uprimny & Sánchez, 2021).

En este sentido, si bien la estandarización de cláusulas ofrece ventajas operativas relacionadas con la eficiencia administrativa y la uniformidad contractual, su aplicación indiscriminada en materia de protección de datos personales resulta problemática, particularmente en organizaciones que operan en múltiples sectores económicos y gestionan distintos tipos de información. La doctrina contemporánea ha advertido que la utilización de cláusulas genéricas desconoce la complejidad real de los flujos de datos, invisibiliza los riesgos específicos asociados a cada actividad y limita la capacidad de demostrar un cumplimiento efectivo del principio de responsabilidad demostrada (Rincón & Valbuena, 2021; SIC, 2022).

Bajo este marco, el análisis crítico de las cláusulas estandarizadas utilizadas por XYZ (y, en especial, de la cláusula de tratamiento de datos personales) permite identificar los vacíos jurídicos derivados de la ausencia de diferenciación sectorial, lo cual constituye el eje central del problema de investigación. Esta aproximación posibilita, además, la formulación de propuestas contractuales orientadas a la construcción de cláusulas predeterminadas, flexibles y modulables, ajustadas al tipo de cliente, la naturaleza del servicio, el perfil poblacional y el nivel de riesgo del tratamiento, en consonancia con los estándares doctrinales y jurisprudenciales vigentes.

3.4. Selección de verticales: sector salud y PYMES

Con el propósito de desarrollar un análisis comparativo riguroso, pertinente y metodológicamente sólido, se seleccionaron dos verticales de negocio con características sustancialmente diferenciadas en términos del tipo de información tratada, nivel de sensibilidad de los datos, riesgo jurídico asociado y exigencias normativas: el sector salud y el sector de pequeñas y medianas empresas (PYMES). Esta elección obedece a la necesidad de evidenciar cómo la aplicación uniforme de una cláusula estándar de protección de datos personales resulta insuficiente para garantizar el cumplimiento efectivo del régimen colombiano de habeas data, especialmente cuando se enfrentan escenarios contractuales heterogéneos.

El vertical de salud se caracteriza por el tratamiento intensivo y sistemático de datos personales sensibles, particularmente aquellos relacionados con la historia clínica, diagnósticos médicos, antecedentes patológicos, tratamientos farmacológicos, exámenes de laboratorio, imágenes diagnósticas y datos biométricos. Conforme a lo establecido en el artículo 5 de la Ley 1581 de 2012, este tipo de información goza de una protección reforzada, dado su potencial para afectar la intimidad, dignidad y autonomía de los titulares. A ello se suma el reconocimiento constitucional del derecho fundamental a la salud y del derecho al habeas data, lo que impone estándares elevados en materia de consentimiento informado, confidencialidad, seguridad de la información, minimización del tratamiento y limitación de finalidades (Congreso de la República, 2012; Corte Constitucional, 2019).

Desde la perspectiva doctrinal, diversos autores han señalado que el tratamiento de datos personales en el sector salud constituye uno de los ámbitos de mayor complejidad jurídica, debido a la convergencia entre derechos fundamentales, deberes éticos, obligaciones contractuales y exigencias tecnológicas. En este sentido, Uprimny y Sánchez (2021) sostienen que la protección de los datos médicos exige esquemas normativos reforzados, sustentados en principios de proporcionalidad, necesidad y seguridad reforzada, orientados a minimizar los riesgos de acceso indebido, fuga de información y uso no autorizado. De igual manera, Montoya y Pineda (2019) destacan que las cláusulas contractuales en el sector salud deben incorporar salvaguardas adicionales, mecanismos estrictos de control de acceso, protocolos de cifrado, auditorías periódicas y procedimientos específicos de gestión de incidentes, dada la alta sensibilidad de la información involucrada.

Adicionalmente, la SIC reiteró, en múltiples pronunciamientos, que el tratamiento de datos sensibles en el sector salud exige una evaluación previa de impacto, medidas técnicas reforzadas y cláusulas contractuales diferenciadas, capaces de demostrar el cumplimiento efectivo del principio de responsabilidad demostrada (SIC, 2022). En consecuencia, cualquier modelo contractual que pretenda regular este tipo de relaciones debe superar la lógica estandarizada, incorporando elementos específicos que respondan al riesgo inherente a la naturaleza de los datos tratados.

En contraste, el vertical de pequeñas y medianas empresas (PYMES) involucra principalmente el manejo de datos personales de carácter público, semiprivado y privado, relacionados con información comercial, financiera, contable, tributaria, laboral y administrativa. Si bien este tipo de datos se encuentra igualmente protegido por la Ley 1581 de 2012, su nivel de sensibilidad y riesgo jurídico es comparativamente menor que el asociado al sector salud, en tanto no compromete, de manera directa, derechos fundamentales de especial protección, como ocurre con la información médica (Congreso de la República, 2012; Rincón & Valbuena, 2021).

No obstante, la doctrina ha advertido que la gestión de datos en el entorno empresarial también plantea desafíos significativos, particularmente en contextos de transformación digital, automatización de procesos y uso intensivo de plataformas tecnológicas. En este escenario, la protección de la información comercial y financiera resulta clave para la estabilidad económica de las organizaciones, la preservación del secreto empresarial y la mitigación de riesgos asociados al fraude, la suplantación de identidad y el acceso no autorizado (Delgado & Puyana, 2020; Camacho & López, 2018).

La diferencia sustancial entre ambos verticales pone de manifiesto la necesidad de adoptar modelos contractuales diferenciados, capaces de ajustarse a los niveles variables de riesgo, sensibilidad y exposición jurídica. Mientras que el sector salud exige cláusulas altamente especializadas, con salvaguardas técnicas y jurídicas reforzadas, el sector PYMES demanda mecanismos orientados a la protección de la información financiera, comercial y administrativa, bajo parámetros de seguridad adecuados, pero proporcionales al nivel de riesgo.

En este sentido, la literatura especializada coincide en que la estandarización contractual, si bien favorece la eficiencia administrativa, resulta incompatible con un modelo de protección de datos basado en la gestión del riesgo y en el principio de responsabilidad demostrada. Según Rojas (2021), la verdadera eficacia del compliance en materia de protección de datos depende de la capacidad de las organizaciones para identificar los riesgos específicos de cada sector, evaluar su impacto y diseñar respuestas contractuales diferenciadas, coherentes con la naturaleza del tratamiento y el perfil de los titulares.

Bajo este marco, la selección de los verticales de salud y PYMES permite evidenciar, desde una perspectiva comparada, cómo la utilización de una cláusula estándar uniforme desconoce las particularidades propias de cada sector, limita la capacidad de demostrar cumplimiento efectivo y expone a la empresa a riesgos jurídicos significativos. Este contraste constituye, por tanto, un insumo central para el análisis crítico que se desarrollará en los apartados siguientes, orientado a evaluar la adecuación normativa de la cláusula utilizada por XYZ y a formular una propuesta de reformulación contractual ajustada a los estándares legales, doctrinales y jurisprudenciales vigentes.

3.5. Contraste normativo de la cláusula estándar de protección de datos

Se puede determinar que la cláusula estándar empleada por XYZ para manejar los datos personales cumple de manera formal con lo mínimo requerido por la Ley 1581 de 2012, según el análisis. La cláusula, en líneas generales, admite los derechos de los titulares, las obligaciones del encargado y la importancia de llevar a cabo medidas de seguridad administrativas, técnicas y humanas. Sin embargo, un examen detallado revela que dicha cláusula se formula de manera uniforme para todos los contratos, sin atender a las particularidades sectoriales, al tipo de datos tratados ni al nivel de riesgo involucrado. Esta estandarización genera vacíos jurídicos relevantes, especialmente cuando se aplica a verticales como el sector salud, donde el tratamiento de datos sensibles exige mayores garantías.

En este sentido, la aplicación de una cláusula genérica resulta insuficiente para satisfacer los principios de finalidad, proporcionalidad, minimización y seguridad reforzada exigidos por la normativa y la jurisprudencia constitucional. La ausencia de diferenciación contractual puede derivar en escenarios de incumplimiento normativo, incrementando el riesgo de sanciones administrativas, responsabilidad civil y afectación reputacional. Adicionalmente, se evidencia que la cláusula estándar no incorpora de manera explícita mecanismos de evaluación de impacto, protocolos diferenciados de gestión de incidentes, ni esquemas sectoriales de control, lo cual limita la materialización efectiva del principio de responsabilidad demostrada.

3.6. El principio de responsabilidad demostrada (accountability) y su aplicación en XYZ

El principio de responsabilidad demostrada o accountability, el cual fue creado y consolidado por la Superintendencia de Industria y Comercio (SIC), demanda que los encargados del manejo de datos personales no solamente cumplan formalmente con las normativas en vigor, sino que tengan la capacidad de probar, de forma objetiva, documentada y verificable, que han tomado medidas apropiadas y eficaces para asegurar una protección integral de los datos personales. Este principio implica una transformación profunda en la perspectiva convencional del cumplimiento de las normas, pues desplaza el foco de la mera observancia formal de la ley hacia la exhibición constante y activa de una cultura dentro de la organización enfocada en resguardar datos.

La implementación de un sistema integral para manejar la protección de datos es lo que significa aplicar el principio de rendición de cuentas en el ámbito empresarial, que incluya políticas internas claras, programas estructurados de cumplimiento, auditorías periódicas, procesos de capacitación continua del personal, esquemas de gestión de riesgos, mecanismos de trazabilidad documental y protocolos específicos de prevención y respuesta ante incidentes de seguridad. Estas medidas deben ser dinámicas, revisables y adaptables a los cambios tecnológicos, operativos y normativos, garantizando así un cumplimiento sustancial y no meramente declarativo.

Si bien XYZ ha avanzado en la estructuración de políticas internas, manuales operativos y procesos documentales orientados al cumplimiento del régimen de protección de datos personales, el análisis desarrollado en esta investigación evidencia que la estandarización contractual constituye una limitación estructural para la efectividad real del modelo de cumplimiento. En particular, la utilización de una cláusula única, uniforme y genérica para todos los sectores económicos y tipos de clientes impide demostrar, de manera clara y objetiva, que la empresa ha evaluado adecuadamente los riesgos

específicos asociados a cada vertical de negocio y ha adoptado medidas proporcionales y diferenciadas frente a dichos riesgos.

Esta limitación se torna especialmente relevante al considerar que XYZ opera en sectores con naturaleza, sensibilidad y niveles de exposición al riesgo sustancialmente distintos, en los cuales confluyen tratamientos de datos públicos, semiprivados, privados y, eventualmente, sensibles. Durante el proceso de sistematización se evidenció que algunas verticales manejan predominantemente datos públicos, mientras que otras tratan información confidencial, estratégica o sensible, lo cual genera escenarios de riesgo claramente diferenciados, especialmente en lo relativo a la posibilidad de fuga, acceso no autorizado, pérdida, alteración o uso indebido de la información.

En este sentido, la ausencia de una evaluación diferenciada del riesgo de fuga de información, en función del tipo de datos tratados en cada sector, revela una debilidad estructural en la aplicación del principio de responsabilidad demostrada. La estandarización contractual impide reflejar de manera precisa las particularidades técnicas, operativas y jurídicas propias de cada entorno, lo que limita la capacidad de la empresa para demostrar un cumplimiento real, eficaz y proporcional. Así, la cláusula genérica carece de la capacidad necesaria para responder adecuadamente a los distintos niveles de criticidad de la información, lo que afecta la efectividad del sistema de protección de datos y debilita los mecanismos preventivos frente a eventuales incidentes de seguridad.

Por tanto, el principio de accountability exige la superación del enfoque uniforme, promoviendo la adopción de cláusulas predeterminadas pero modulables, estructuradas a partir de matrices de riesgo sectoriales, que permitan adaptar el contenido contractual a las características específicas del tratamiento, al perfil del titular, al sector económico involucrado y al nivel de riesgo asociado. Solo a través de este modelo flexible, contextualizado y verificable es posible garantizar una protección efectiva de los datos personales, fortalecer la trazabilidad documental y consolidar un sistema robusto de cumplimiento normativo acorde con los estándares fijados por la Superintendencia de Industria y Comercio.

3.7. Identificación de vacíos jurídicos y necesidad de reformulación contractual

El contraste entre la normativa vigente y la práctica contractual de XYZ permite identificar un vacío jurídico estructural: la utilización de una cláusula estándar para regular escenarios heterogéneos de tratamiento de datos personales. Esta situación desconoce la diversidad de riesgos inherentes a cada vertical de negocio y limita la eficacia de las medidas de protección implementadas. En particular, el sector salud demanda un régimen contractual reforzado, que incorpore obligaciones específicas en materia de seguridad de la información, control de accesos, cifrado de datos, auditorías periódicas, evaluación de impacto en privacidad y protocolos estrictos de gestión de incidentes.

La omisión de estos elementos dentro de la cláusula estándar incrementa significativamente la exposición jurídica de la empresa. Por el contrario, en el sector PYMES, aunque los riesgos son menores, también resulta necesario incorporar modulaciones contractuales que permitan ajustar las obligaciones de acuerdo con el volumen, la finalidad y la naturaleza de los datos tratados. En este contexto, se propone la sustitución del modelo de cláusula estándar por un esquema de cláusulas predeterminadas sujetas a modificación, estructuradas conforme a matrices de riesgo sectorial, que permitan cumplir de manera efectiva con los principios de legalidad, finalidad, proporcionalidad, seguridad y responsabilidad demostrada.

CONCLUSIONES

El análisis integral desarrollado a lo largo de la presente investigación permitió evidenciar que la cláusula de tratamiento de datos personales empleada por XYZ se ajusta, en términos formales, a las pautas básicas requeridas por la Ley 1581 del año 2012, junto con sus decretos reglamentarios y las instrucciones generales proporcionadas por la Superintendencia de Industria y Comercio. En su forma básica, la cláusula incluye los principios fundamentales del tratamiento, establece los derechos de los titulares y distribuye deberes generales al responsable y al encargado del tratamiento. Sin embargo, el análisis mostró que esta cláusula tiene restricciones significativas si se compara con la complejidad operacional, técnica y sectorial de los diferentes verticales comerciales que la empresa atiende.

En particular, se identificó que el principal problema no radica en la existencia misma de la cláusula, sino en su carácter uniforme, genérico e indiferenciado. La aplicación de un único modelo contractual para contextos altamente heterogéneos, como el sector salud y el sector de pequeñas y medianas empresas (PYMES), desconoce las profundas diferencias en la naturaleza, sensibilidad, volumen y nivel de riesgo jurídico de los datos personales tratados. Mientras que el sector salud involucra el manejo intensivo de datos personales sensibles y exige estándares reforzados de protección, el sector PYMES gestiona, en su mayoría, información de carácter comercial, financiero y administrativo, con perfiles de riesgo diferenciados. Este enfoque estandarizado limita la eficacia real de las medidas de protección y puede derivar en incumplimientos normativos relevantes, especialmente en escenarios de alta exposición jurídica, tal como lo ha reiterado la jurisprudencia constitucional y la doctrina especializada (Garriga, 2016; Osuna Carreño, 2024).

Desde una perspectiva jurídica sustantiva, se concluye que la cláusula estándar resulta formalmente válida, pero materialmente insuficiente. La ausencia de modulaciones contractuales específicas por vertical de negocio genera vacíos normativos relevantes, al no contemplar protocolos diferenciados de gestión del riesgo, esquemas de seguridad reforzada, evaluaciones de impacto, ni mecanismos sectoriales de control y auditoría. Esta omisión contraviene el principio de proporcionalidad en el tratamiento de datos personales, conforme al cual las medidas de protección deben ser acordes con la naturaleza, sensibilidad e impacto potencial de la información procesada (Quintero Riveros, 2023).

Asimismo, el estudio permitió constatar que el principio de responsabilidad demostrada (accountability), aunque formalmente incorporado en las políticas internas de XYZ, no se materializa plenamente en el diseño contractual ni en la arquitectura de cumplimiento corporativo. Este principio exige no solo el acatamiento normativo, sino la capacidad efectiva de probar, de manera objetiva, sistemática y verificable, la implementación de mecanismos idóneos para la protección de los datos personales, incluyendo procesos de evaluación del riesgo, controles técnicos, protocolos documentados y sistemas de mejora continua (Superintendencia de Industria y Comercio, 2020). En este sentido, la estandarización contractual dificulta la demostración de una gestión diferenciada del riesgo, particularmente en sectores de alta sensibilidad como el sanitario.

Ante esta situación, se deduce que la cláusula de tratamiento de datos personales tiene el potencial y la obligación de ser robustecida a través de un modelo contractual dinámico, que se fundamenta en cláusulas preestablecidas pero que permiten modificaciones y son ajustables a las especificidades de cada sector empresarial. Esta perspectiva haría posible incluir normas sectoriales particulares en términos de confidencialidad mejorada, seguridad de la información, minimización del tratamiento,

evaluación del impacto en la protección de datos (PIA), gestión de incidentes y trazabilidad documental, siguiendo las pautas doctrinales y regulatorias actuales (Garriga, 2016; Quintero Riveros, 2023).

Adicionalmente, se recomienda a la empresa implementar procesos internos de mejora continua en materia de cumplimiento, tales como: (i) la creación de una matriz de clasificación de riesgos por tipo de dato y vertical de negocio; (ii) la realización periódica de auditorías internas especializadas en protección de datos; (iii) el fortalecimiento de los programas de capacitación diferenciada para los equipos operativos, técnicos y comerciales; y (iv) la revisión sistemática y actualización permanente de los modelos contractuales y políticas internas. Estas medidas no solo optimizan el cumplimiento normativo, sino que fortalecen la gobernanza corporativa, la confianza digital y la sostenibilidad jurídica de la organización.

En síntesis, la investigación permitió establecer que, si bien XYZ ha avanzado de manera significativa en la adopción de políticas de protección de datos personales, persisten oportunidades estratégicas de mejora en el ámbito contractual y en la gestión integral del riesgo jurídico. La transición desde un modelo de cláusula estándar hacia un sistema de cláusulas predeterminadas, flexibles y modulables constituye una estrategia jurídica idónea para consolidar el principio de responsabilidad demostrada, mitigar contingencias legales, fortalecer la confianza de los clientes y posicionar a la empresa como un referente en cumplimiento normativo dentro del ecosistema tecnológico colombiano.

BIBLIOGRAFÍA

Comb, M., Martin, A. Mining digital identity insights: patent analysis using NLP. *EURASIP J. on Info. Security* 2024, 21 (2024). https://doi.org/10.1186/s13635-024-00172-5

Congreso de la República de Colombia. (1991). Constitución Política de Colombia. Gaceta Constitucional No. 116.

Congreso de la República de Colombia. (1999). 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. Diario Oficial No. 43.673.

Congreso de la República de Colombia. (2008). 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, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Diario Oficial No. 47.219.

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587.

Congreso de la República de Colombia. (2013). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48.834.

Congreso de la República de Colombia. (2014). Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos. Diario Oficial No. 49.203.

Congreso de la República de Colombia. (2015). Decreto 1074 de 2015. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Diario Oficial No. 49.523.

Corte Constitucional de Colombia. (1992). Sentencia T-414 de 1992. M.P. Ciro Angarita Barón.

Corte Constitucional de Colombia. (2011). Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional de Colombia. (2011). Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional de Colombia. (2012). Sentencia T-414 de 2012. M.P. Jorge Iván Palacio Palacio.

Corte Constitucional de Colombia. (2014). Sentencia T-197 de 2014. M.P. María Victoria Calle Correa.

Corte Constitucional de Colombia. (2015). Sentencia C-1011 de 2015. M.P. Gloria Stella Ortiz Delgado.

Corte Constitucional de Colombia. (2017). Sentencia T-063 de 2017. M.P. Gloria Stella Ortiz Delgado.

Corte Constitucional de Colombia. (2018). Sentencia T-063 de 2018. M.P. Carlos Bernal Pulido.

Garriga, A. (2016). El derecho fundamental a la protección de datos: Nuevos retos para la protección de datos personales en la era del Big Data y de la computación ubicua. Dykinson.

González Fuster, G. (2014). The emergence of personal data protection as a fundamental right of the EU. Springer.

Jiménez V., H. C., & Gutiérrez G., J. C. (2022). *Seguridad de la información, datos personales, habeas data dentro del ordenamiento jurídico colombiano 2020–2022 / Information security, personal data, habeas data within the Colombian legal system 2020–2022*.https://repository.unilibre.edu.co/bitstream/handle/10901/28604/Seguridad%20de%20la%20Informacio%CC%81n%2C%20Datos%20Personales%2C%20Habeas%20Data%20Dentro%20del%20Ordenamiento%20Juri%CC%81dico%20Colombiano%202020%20%E2%80%93%202022.pdf?sequence=4

Kunst, M., Luvini, P., & Dias, J. M. (2024). Guía práctica para la clasificación de datos.

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Computer Law & Security Review, 32(2), 238–255. https://doi.org/10.1016/j.clsr.2016.01.014

Martínez, J. J. Z., Moreno, J. A. R., & Ponzo, L. C. H. (2025). Alfabetización digital y derechos de privacidad en la era de las TIC: Análisis documental desde la perspectiva legal y ética del manejo de información. *Revista de Investigación en Tecnologías de la Información*, *13*(29), 71-81.

Montoya, L., & Pineda, J. (2019). Protección de datos personales y responsabilidad empresarial: análisis del principio de accountability en Colombia. Revista de Derecho Privado, 37, 89–115. https://doi.org/10.18601/01234366.n37.05

Osuna Carreño, A. (2024). El derecho fundamental a la protección de datos personales en Colombia: Un análisis del artículo 15 de la Constitución Política. Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/handle/001/16621

Quintero Riveros, M. C. (2023). El dato personal como insumo productivo en la actividad empresarial y su protección jurídica. Revista e-mercatoria, 22(2), 343–406. https://doi.org/10.18601/16923960.v22n2.10

Rallo Lombarte, A. (2018). La protección de datos personales: Derecho fundamental y garantías. Tirant lo Blanch.

Real Academia Española. (2023). Diccionario panhispánico del español jurídico. https://dpej.rae.es

Rodríguez, C., & Uprimny, R. (2010). Interpretación constitucional y protección de derechos fundamentales. DeJusticia.

Rozo Acuña, E. (2017). El derecho a la autodeterminación informativa en Colombia: desarrollo jurisprudencial y límites. Revista Derecho del Estado, 38, 129–165. https://doi.org/10.18601/01229893.n38.06

Saavedra, F. (2024, 27 de febrero). Superintendencia Financiera impone plazo para la protección de datos personales. Infobae.https://www.infobae.com/colombia/2024/02/27/superintendencia-financiera-dio-15-dias-para-contestar-quejas-y-reclamos-por-habeas-data-por-aumento-de-casos

Sistemas de Información Empresarial S.A.S. (SIESA). (2024). Quiénes somos. https://www.siesa.com/quienes-somos/#

Solove, D. J., & Schwartz, P. M. (2020). Information privacy law (7th ed.). Wolters Kluwer.

Superintendencia de Industria y Comercio. (2016). Circular Única – Título V: Protección de datos personales. https://sedeelectronica.sic.gov.co/transparencia/normativa/titulo-v-0

Superintendencia de Industria y Comercio. (2019). Guía para el tratamiento de datos personales con fines de marketing y publicidad. https://protecdatalatam.com/wp-content/uploads/2022/05/Guia-marketing-publicidad-y-tratamiento-de-datos-2019.pdf

Superintendencia de Industria y Comercio. (2020). Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales. https://www.cerlatam.com/wp-content/uploads/2021/01/Gu_a_SIC_1609816469.pdf

Superintendencia de Industria y Comercio. (2022). Guía para la implementación del principio de responsabilidad demostrada (accountability). https://protecdatalatam.com/wp-content/uploads/2022/03/GUIA-DE-RESPONSABILIDAD-DEMOSTRADA.pdf

Superintendencia de Industria y Comercio. (2023). Boletín jurídico de protección de datos personales. SIC.

Superintendencia de Industria y Comercio. (2025). Resolución No. 16582 del 31 de marzo de 2025: Sanción administrativa a Mercado Libre Colombia Ltda. https://sedeelectronica.sic.gov.co/sites/default/files/normativa/Resoluci%C3%B3n%2016582-2025.pdf

Superintendencia de Industria y Comercio. (s. f.). Manejo de información personal – Habeas data.https://www.sic.gov.co/manejo-de-informacion-personal

Superintendencia de Industria y Comercio. (2025). Por violación a las normas de protección de datos personales, la Superintendencia de Industria y Comercio ha iniciado 101 investigaciones e impuesto multas por $5.157 millones en 2025. https://sedeelectronica.sic.gov.co/noticias/por-violacion-las-normas-de-proteccion-de-datos-personales-la-superintendencia-de-industria-y-comercio-ha-iniciado-101-investigaciones-e

Superintendencia de Industria y Comercio. (2025). La SIC sanciona a las sociedades World Foundation y Tools for Humanity Corporation con el cierre inmediato y definitivo de su operación de tratamiento de datos personales en Colombia

https://sedeelectronica.sic.gov.co/comunicado/la-sic-sanciona-las-sociedades-world-foundation-y-tools-humanity-corporation-con-el-cierre-inmediato-y-definitivo-de-su-operacion-de

Tene, O., & Polonetsky, J. (2012). Privacy in the age of Big Data: A time for big decisions. Stanford Law Review Online, 64, 63–69.

Velásquez Posada, O. (2018). Contratos informáticos y protección de datos personales. Universidad del Rosario.

Zuleta Jaramillo, L. F. (2021). Compliance y protección de datos personales: implicaciones jurídicas para la empresa en Colombia. Revista de Derecho Privado, 41, 151–189. https://doi.org/10.18601/01234366.n41.06