Análisis de la Protección de Datos Personales en las Relaciones Contractuales entre EPS e IPS en el Sector Salud Colombiano: Desafíos y Recomendaciones para el Fortalecimiento de la Seguridad y Privacidad.

Manuela Varela Arévalo

Trabajo de grado presentado para optar al título de abogada

Director

Carlos Andrés Gómez García, Magíster (MSc) en Bioética y Bioderecho

Universidad Pontificia Bolivariana

Escuela de Derecho y Ciencias Políticas

Derecho

Medellín, Antioquia, Colombia

2025

El contenido de este documento no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en esta o en cualquiera otra universidad.

TABLA DE CONTENIDO

RESUMEN

Este trabajo de investigación analiza cómo se protegen los datos personales en las relaciones contractuales entre Entidades Promotoras de Salud (EPS) e Instituciones Prestadoras de Salud (IPS) en Colombia. Su objetivo es identificar desafíos regulatorios y proponer recomendaciones para mejorar la privacidad y seguridad de los datos sensibles de los pacientes. El estudio nace de la preocupación cada vez mayor por la vulnerabilidad de la información personal en el sector salud, donde la transmisión constante de datos médicos demanda altos niveles de protección.

La investigación se basa en un enfoque cualitativo y documental, fundamentado en el análisis de regulaciones como la Ley 1581 de 2012, la jurisprudencia de la Corte Constitucional y la doctrina especializada. Se examinan las políticas actuales de tratamiento de datos, además de la eficacia de los mecanismos de seguridad que las EPS e IPS han establecido. Asimismo, se detectan lagunas normativas y problemas prácticos que impiden el cumplimiento de los principios de transparencia, privacidad y autodeterminación en la información.

Los hallazgos demuestran que la falta de consistencia en las prácticas contractuales y la falta de protocolos concretos incrementan el peligro de accesos no permitidos, pérdida o mal uso de la información. Se proponen recomendaciones que incluyen crear protocolos claros, usar tecnologías seguras y aplicar cláusulas en los contratos que refuercen la responsabilidad de las partes. Esto es para proteger mejor los derechos fundamentales de los pacientes en situaciones comunes y críticas.

Palabras Clave: Protección de datos personales, EPS, IPS, sector salud, relaciones contractuales, privacidad…

ABSTRACT

This research work examines the protection of personal data in contractual relationships between Health Promoting Entities (EPS) and Health Service Providers (IPS) in Colombia, with the aim of identifying regulatory challenges and suggesting recommendations to enhance the privacy and security of patients' sensitive data. The study arises from growing concern over the vulnerability of personal information in the healthcare sector, where the continuous transmission of medical data demands high levels of protection.

The research is based on a qualitative and documentary approach, grounded in the analysis of regulations such as Law 1581 of 2012, Constitutional Court jurisprudence, and specialized legal doctrine. Current data processing policies are reviewed, along with the effectiveness of the security mechanisms implemented by EPS and IPS. In addition, regulatory gaps and practical issues that hinder compliance with the principles of transparency, privacy, and informational self-determination are identified.

The findings show that inconsistencies in contractual practices and the absence of concrete protocols increase the risk of unauthorized access, loss, or misuse of information. In summary, the paper recommends creating clear guidelines, using secure technologies, and adding contract clauses that strengthen the responsibilities of all parties. This will help better protect patients' essential rights in both regular and emergency situations.

Keywords: Personal data protection, EPS, IPS, health sector, contractual relationships, privacy.

INTRODUCCIÓN

Este trabajo trata un asunto crucial en el sector sanitario de Colombia: la gestión y protección de los datos personales en las relaciones contractuales entre las Entidades Promotoras de Salud (EPS) y las Instituciones Prestadoras de Salud (IPS). En este escenario, la relación estrecha entre ambas entidades conlleva el intercambio continuo de datos privados vinculados con la salud de los pacientes, que incluyen desde registros clínicos hasta diagnósticos y tratamientos. Dada la importancia y sensibilidad de estos datos, su correcta gestión es crucial para asegurar la privacidad y proteger los derechos básicos de los propietarios. Debido a la naturaleza delicada de estos datos, su correcta administración resulta esencial para garantizar la privacidad y la protección de los derechos fundamentales de quienes los poseen.

En Colombia, hay leyes que protegen los datos personales, especialmente la Ley 1581 de 2012 y sus regulaciones, como el Decreto 1377 de 2013, además de decisiones importantes de la Corte Constitucional. Sin embargo, la manera en que está organizado este derecho es bastante compleja. Aún persisten interrogantes sobre su alcance y aplicación, lo que evidencia la necesidad de un análisis más profundo para delimitar su forma y contenido de manera precisa. Este estudio tiene como objetivo examinar a fondo los retos relacionados con la protección de información sensible en el sector sanitario. No solo se evaluará el cumplimiento de las regulaciones, sino que también se buscarán oportunidades para mejorar la privacidad y seguridad en la protección del derecho a la salud.

Desde una perspectiva ética, es esencial mantener la privacidad y la confidencialidad para construir una relación sólida y de confianza entre pacientes e instituciones, ya que una administración inadecuada de su información más delicada puede afectar su dignidad y la confianza en el sistema. Por lo tanto, este estudio tiene como objetivo proporcionar un análisis crítico que detecte áreas de mejora tanto en la legislación como en las prácticas de operación vinculadas al manejo de datos personales en este sector. Una correcta protección de los datos no solo favorece a los pacientes asegurando su privacidad, sino que también

fortalece la imagen institucional y promueve una cultura organizativa enfocada en el respeto a los derechos personales.

En este marco, se plantean las cuestiones esenciales de investigación que guían este análisis: ¿Cómo se implementa la protección de la información personal en las relaciones contractuales entre EPS e IPS en el sector de la salud en Colombia? ¿Cuáles son los desafíos legales y prácticos actuales? ¿Qué recomendaciones se pueden aportar para mejorar la seguridad y privacidad de los datos sensibles de los pacientes?

La hipótesis central de este estudio sostiene que la protección de los datos personales en las relaciones contractuales entre EPS e IPS en Colombia es insuficiente. Esto se debe a la falta de regulaciones concretas y prácticas consistentes en la administración de información sensible en salud, lo que representa peligros significativos para la privacidad y seguridad de los pacientes. Se sugiere que, al crear y usar protocolos claros de seguridad y confidencialidad, basados en principios como el derecho a decidir sobre la información, la transparencia y la responsabilidad, se puede mejorar mucho la protección de los derechos de los pacientes. Además, se mejorará la observancia de las regulaciones actuales, especialmente en situaciones críticas y de alto riesgo en el ámbito de la salud. Adicionalmente, se considera que la normativa actual y los enfoques teóricos como el hábeas data y el derecho a la intimidad no se aplican de manera óptima en las relaciones EPS-IPS, puesto que los contratos actuales no garantizan plenamente la protección de los datos personales, evidenciando una necesidad de regulación y práctica mejorada.

Para abordar el problema planteado y verificar la hipótesis, se han definido los siguientes objetivos: El objetivo general es examinar la protección de datos personales en el tratamiento de datos entre EPS e IPS en Colombia, identificando los desafíos normativos y prácticos en la aplicación de políticas de seguridad y privacidad, y proponiendo recomendaciones para optimizar la protección de los datos sensibles de los pacientes en estas relaciones contractuales. Este objetivo principal se divide en los siguientes objetivos concretos: 1) Examinar las leyes, regulaciones y políticas actuales con base a las relaciones contractuales entre EPS e IPS en Colombia, poniendo especial atención en la seguridad de

los datos personales en el ámbito sanitario; 2) Valorar las prácticas vigentes de tratamiento y protección de datos personales entre EPS e IPS, evaluando su eficacia y nivel de cumplimiento a las normativas nacionales; y 3) Sugerir sugerencias para la elaboración y/o transformación de protocolos concretos en el marco contractual EPS-IPS, que potencien la transparencia, privacidad y responsabilidad en el manejo de datos personales, asegurando la protección de los derechos de los pacientes y la observancia de las regulaciones en circunstancias habituales y críticas.

En cuanto al enfoque de investigación, este estudio se llevará a cabo mediante un método documental cualitativo de carácter documental. El método implica un examen exhaustivo de leyes reguladoras, fallos (principalmente de la Corte Constitucional y la Superintendencia de Industria y Comercio en lo que respecta a hábeas data) y doctrinas pertinentes, además de investigaciones contemporáneas sobre la protección de datos en el sector salud. Se utilizará el método de análisis documental para descifrar los principios de protección de datos y establecer su idoneidad en la gestión de información sensible en situaciones contractuales y en situaciones críticas como emergencias sanitarias. Este procedimiento posibilita profundizar en el marco legal y normativo sin intervención directa, proporcionando una base sólida práctica y normativa, y simplificando la comparación de leyes.

Para finalizar, este trabajo se organiza en capítulos que tratan de manera secuencial los objetivos fijados. El primer capítulo se enfoca en sentar las bases teóricas y contextuales, examinando las leyes, regulaciones y políticas actuales, revisando los reglamentos y jurisprudencias anteriores, forjando un sólido marco teórico a través de la definición de conceptos esenciales y la identificación de la legislación correspondiente, y evaluando el estado presente de la protección de la información personal en el ámbito sanitario. Los próximos capítulos, fundándose en los objetivos específicos, se centrarán en la valoración de las prácticas vigentes de tratamiento de datos entre EPS e IPS, además de proponer sugerencias específicas para reforzar la protección de datos sensibles, la transparencia, la privacidad y la responsabilidad en estas relaciones contractuales.

CAPÍTULO 1: ANÁLISIS DE LA PROTECCIÓN DE DATOS EN LAS RELACIONES CONTRACTUALES EPS-IPS EN COLOMBIA

El capítulo inicial de este trabajo se enfoca en la elaboración de esta base teórica y contextual, examinando las leyes, normativas y políticas actuales. Luego, se muestra un resumen en forma de cuadro que reúne los elementos clave del marco legal correspondiente, incluyendo las leyes esenciales, los principios que deben guiar el manejo de la información, los derechos de los titulares de la información y las responsabilidades de los proveedores de servicios y responsables de su tratamiento.

Regulación	Año	Tema
Ley 1266 de 2008	2008	Régimen general sobre hábeas data financiero y protección de datos personales.
Ley 1581 de 2012	2012	Establece el régimen general de protección de datos personales en Colombia. Introduce principios como legalidad, finalidad, libertad, veracidad, acceso, y seguridad.
Ley 1751 de 2015 (Ley Estatutaria de Salud)	2015	Reconoce el derecho fundamental a la salud. Señala que el acceso, uso y manejo de datos en salud debe respetar el derecho a la intimidad y a la confidencialidad.
Decreto 1377 de 2013	2013	Reglamenta parcialmente la Ley 1581/12, especialmente en lo relativo al manejo de datos recolectados antes de la expedición de la ley.
Decreto 1074 de 2015	2015	Decreto Único Reglamentario del Sector Salud, incluye disposiciones sobre protección de datos.
Sentencia C-748 de 2011 (Corte Constitucional)	2011	Declara exequible el proyecto de Ley 1581 de 2012. Destaca la autonomía del habeas data como derecho fundamental.

Regulación	Año	Tema
Sentencia T-414 de 1992 (Corte Constitucional)	1992	Introduce el concepto de habeas data y resalta su importancia frente al derecho a la intimidad.
Sentencia T-578 de 1998 (Corte Constitucional)	1998	Define criterios para la protección del dato sensible, especialmente en salud.
Sentencia T-398 de 2023 (Corte Constitucional)	2023	Reconoce la finalidad informativa y administrativa de bases de datos como "Justicia Siglo XXI". Reafirma la importancia de la gestión adecuada y protección de bases de datos públicas con datos sensibles.
Sentencia T-456 de 2023 (Corte Constitucional)	2023	Protege derechos de personas con enfermedades sensibles frente a actos discriminatorios en atención médica. Refuerza el derecho a la no discriminación en el acceso a servicios médicos.
Circular Externa 02 de 2015 (SIC)	2015	Ofrece lineamientos para el tratamiento de datos sensibles, especialmente en el ámbito de la salud.
Sentencia T-402 de 2024 (Corte Constitucional)	2024	Protege la confidencialidad de los datos personales sensibles en salud. Declara vulnerados los derechos fundamentales de una paciente cuya información sobre IVE fue filtrada por la IPS a terceros, reafirmando la obligación de salvaguardar la privacidad y confidencialidad en el sector salud.

En el cuadro anterior, el marco normativo en Colombia establece un conjunto integral de reglas, principios y obligaciones para el tratamiento de datos personales, reconociendo el derecho al manejo correcto de los datos como un derecho fundamental con facultades inequívocas para los titulares. Sin embargo, la mera existencia de este reglamento no garantiza su aplicación efectiva y no abordar completamente las complejidades efectivas no aborda plenamente las complejidades inherentes a la gestión de datos sensibles en el contexto particular de las relaciones contractuales EPS e IPS. La siguiente sección de este capítulo se centrará en conectar estos conceptos teóricos y normativos con las limitaciones y la potencial

falta de efectividad normativa y prácticas encontradas en este campo, definiendo con precisión el problema de investigación que guiará los siguientes capítulos del estudio.

Este primer capítulo se enfoca en establecer los fundamentos teóricos y contextuales para el estudio que trata el problema esencial de la protección de la información personal en el marco de las relaciones contractuales entre las Entidades Promotoras de Salud (EPS) y las Instituciones Prestadoras de Salud (IPS) en el sector de la salud en Colombia. El propósito principal es examinar minuciosamente las leyes, reglamentos y políticas actuales que regulan la protección de la información personal en este escenario particular, poniendo especial atención en la seguridad de la información sensible vinculada a la salud.

Se llevará a cabo un análisis exhaustivo del escenario global del asunto, tanto a nivel nacional como a nivel particular de las relaciones EPS-IPS. Se analizarán los precedentes legales y jurídicos que han dado forma al marco actual. Se construirá un sólido marco teórico a través de la definición exacta de conceptos esenciales, la exposición de doctrinas y teorías pertinentes, y la identificación de la legislación correspondiente. Finalmente, se examinará el estado actual de los datos personales en Colombia, enfocándose especialmente en el ámbito de la salud. Se establecerá un vínculo claro y coherente entre las teorías actuales y el problema de investigación que motiva este análisis. Finalmente, se presentará una conclusión que condensa los puntos clave discutidos en este primer capítulo, preparando el escenario para el análisis posterior.

Para establecer este fundamento, se iniciará con el reconocimiento del derecho fundamental a la protección de datos personales. Este derecho se basa en el artículo 15 de la Constitución Política de 1991, que establece el derecho de hábeas data, lo que permite a las personas conocer, actualizar y rectificar los datos recopilados sobre ellas en bases de datos y archivos públicos y privados. La Corte Constitucional ha sido fundamental en su desarrollo jurisprudencial, elevando el habeas data a la categoría de derecho fundamental autónomo. Primero establecida por la Ley 1266 de 2008 para datos financieros y comerciales, la Ley 1581 de 2012 estableció un marco general que rige la recopilación, almacenamiento, uso y tratamiento de datos personales por organismos públicos y privados. Esta ley, junto con sus

regulaciones, como el Decreto 1377 de 2013 y el Decreto 886 de 2014, impone la obligación legal a las entidades de definir políticas requeridas para la administración y tratamiento de datos personales, estableciendo objetivos y recursos fundamentales.

En el marco teórico, se tratará la definición de los datos personales y, para el análisis en particular, los datos sensibles. Se consideran datos sensibles aquellos que amenazan la privacidad del poseedor o cuyo uso inadecuado puede provocar discriminación, incluyendo de manera evidente los datos relacionados con la salud en esta categoría. Esto incluye historiales de salud, diagnósticos, tratamientos y cualquier otra información relacionada con el estado físico o mental de un individuo.

La Ley 1581 de 2012 y el Decreto 1377 de 2013 dictan que estos datos solo pueden ser administrados con la autorización explícita del propietario y bajo rigurosos criterios de seguridad. Principios fundamentales como la legalidad, finalidad, libertad, veracidad, acceso restringido, seguridad y confidencialidad son rectores en el tratamiento en el manejo de datos personales, siendo cruciales en el sector salud debido a la delicadeza de la información. También se destacarán como principios fundamentales la transparencia y la reducción de datos. El derecho a la autodeterminación informativa ha sido reconocido por la doctrina y la jurisprudencia como el núcleo del hábeas data. La seguridad en el manejo de datos se presenta como una teoría esencial, proponiendo la necesidad de poner en marcha acciones técnicas, físicas y administrativas para minimizar riesgos.

El estudio de la situación presente en la protección de datos personales en el sector sanitario, especialmente en las relaciones EPS-IPS, mostró un panorama que se distingue por la presencia de un marco legal general con normativas y regulaciones prácticas pertinentes. Las relaciones contractuales entre EPS e IPS implican un flujo constante de datos personales sensibles, vitales para la prestación de servicios. Aunque las instituciones tienen el deber de documentar procedimientos y garantizar la seguridad y privacidad, existe una carencia de eficacia en el ámbito legal y práctico. Esto se debe, en cierta medida, a la falta de una regulación específica que trate las especificidades del manejo de datos delicados en salud en el marco bilateral EPS-IPS, junto con la ausencia de prácticas uniformes y estandarizadas.

Esta circunstancia provoca peligros latentes para la privacidad y protección de la información de los pacientes, impactando derechos esenciales. La Superintendencia Nacional de Salud desempeña funciones de supervisión y tiene la potestad de aplicar sanciones, con el objetivo de prevenir y rectificar transgresiones, en particular las que crean obstáculos de acceso o afectan a individuos de protección especial.

La conexión entre los conceptos teóricos y el asunto de investigación se basa en que el marco legal, los principios esenciales y el contexto presente han configurado las dinámicas de las relaciones contractuales entre las EPS y las IPS. En este contexto, se presenta un conflicto crucial: por un lado, la exigencia de divulgar información delicada para asegurar una correcta prestación de servicios sanitarios y, por otro, el deber de resguardarla mediante rigurosas medidas de privacidad y seguridad. En este escenario, la protección de los datos personales es insuficiente debido a la atención, las regulaciones específicas y la ausencia de prácticas uniformes que garanticen su uso eficiente, lo que implica riesgos significativos para los dueños de la información. El propósito de esta investigación es examinar estos desafíos y proponer soluciones que contribuyan a fortalecer la protección de los datos sensibles en las relaciones contractuales EPS-IPS.

Este primer capítulo sienta los cimientos al definir los principios y conceptos esenciales del derecho a la protección de datos en Colombia; define los conceptos y principios esenciales, en particular los relacionados con los datos sensibles en salud, y expone el panorama actual del sector sanitario y los desafíos específicos en las relaciones contractuales EPS-IPS. Al reconocer los retos y la falta de regulaciones y prácticas en este campo, se define el problema de investigación que orientará el análisis en los capítulos posteriores, que se enfocarán en la valoración de las prácticas vigentes y en la elaboración de sugerencias de mejora.

1.1 PANORAMA Y ANTECEDENTES DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

En Colombia, la protección de los datos personales no es una idea reciente, sino el resultado de una progresión normativa y jurisprudencial que abarca el valor ascendente de la información personal en la sociedad actual y los riesgos vinculados a su gestión. Esta protección se basa en la Constitución Política de 1991. El artículo 15 desarrolló por vez primera el derecho esencial al hábeas data, otorgándole a cada persona la facultad de conocer, actualizar y rectificar la información que se haya recolectado sobre la persona en particular en archivos y bancos de datos de naturaleza pública o privada. Este mandato constitucional sentó las bases para el desarrollo normativo posterior y estableció un estándar mínimo de protección, exigiendo que en la recolección, tratamiento y circulación de datos se respeten la libertad y demás garantías consagradas en la Constitución.

La jurisprudencia de la Corte Constitucional ha desempeñado un papel crucial en la definición de los alcances y limitaciones de la protección de datos personales en Colombia. La Corte ha sido fundamental para ampliar el concepto, contenido, alcance y finalidad del derecho al hábeas data, estableciendo precedentes importantes.

Los antecedentes jurisprudenciales relevantes incluyen:

- Considerada como un progreso inicial, la Sentencia T-414 de 1992 estableció la importancia del derecho a la privacidad y el hábeas data. En este contexto, la Corte hizo hincapié en que la gestión de datos personales podría suponer un "encarcelamiento del alma", valorando el artículo 15 superior y sus cambios como fundamentales para regular y controlar el "poder informático".
- La Sentencia SU-082 de 1995, al igual que precedentes como la T-414 de 1992, enfatizó la relevancia del hábeas data en el sector salud, protegiendo la privacidad de los datos de los pacientes y asegurando que la gestión de dicha información se lleve a cabo con los estándares de confidencialidad más elevados. Estas sentencias ratificaron que el hábeas data permite a los ciudadanos reclamar por el uso inadecuado

de sus datos y solicitar que sean tratados de acuerdo con la ley y sus expectativas de privacidad. La Corte Constitucional ha establecido, interpretando el hábeas data, que el titular de los datos personales tiene la facultad de exigir el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en su divulgación, publicación o cesión, conforme a los principios que regulan la administración de datos personales.

- La Sentencia T-729 de 2002 es significativa, ya que reconoce la necesidad de una protección reforzada para los datos sensibles vinculados a la salud. Además, establecieron principios rectores fundamentales que deben orientar la administración de esta información y validar la legitimidad de la acción de tutela como la herramienta legal apropiada para proteger este derecho frente a eventuales violaciones.

Estas sentencias son el fundamento jurídico que sostiene la protección de datos en el sector salud en Colombia, estableciendo los derechos de los titulares.

La evolución legislativa del hábeas data comenzó con la Ley Estatutaria 1266 de 2008, centrada principalmente en la protección de datos en el sector financiero y crediticio. Luego, debido a la demanda de una normativa más extensa y general, se promulgó la Ley Estatutaria 1581 de 2012, denominada "por la cual se dictan disposiciones generales para la protección de datos personales". Esta normativa es la regla general que establece para proteger la información personal y rige el derecho esencial de hábeas data de los individuos, protegiendo sus medidas personales almacenadas en cualquier base de datos gestionada por organismos públicos y/o privados. Define el "Tratamiento" de manera amplia, abarcando cualquier operación o conjunto de operaciones sobre datos personales, como la recolección, almacenamiento, uso, circulación o supresión.

La Ley 1581 de 2012 estableció principios rectores como la legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. El principio de libertad exige que el tratamiento solo podrá realizarse con el consentimiento previo, expreso e informado del titular. La Ley 1581 de 2012 fue objeto de control de constitucionalidad por la Corte Constitucional (Sentencia C-748 de 2011). En este

control, la Corte determinó, por ejemplo, que el legislador limitó desproporcionadamente el ejercicio del derecho fundamental de hábeas data al condicionar la supresión del dato a que la Superintendencia de Industria y Comercio (SIC) hubiera determinado una conducta contraria a la ley. La Corte precisó que el individuo es libre de decidir qué información desea que continúe o que sea excluida, salvo mandato legal u obligación contractual que imponga su permanencia. Además, la confidencialidad de la información de salud, reconocida en la Ley 1751 de 2015, fue hallada conforme a la Constitución durante el control previo de la Ley 1581 de 2012. La Ley 1581 de 2012 también define los datos sensibles, incluyendo los datos de salud, los cuales requieren una protección reforzada.

Normativas complementarias, como el Decreto 1377 de 2013 (integrado en el Decreto 1074 de 2015), controlan de manera parcial la Ley 1581 de 2012, detallando aspectos fundamentales como las condiciones para el consentimiento y las pautas para las políticas de tratamiento de la información, e incluyendo el principio de Responsabilidad Demostrada.

El Registro Nacional de Bases de Datos (RNBD) está regulado por el Decreto 886 de 2014. Incluso antes de la Ley 1581 de 2012, existían directrices sectoriales para la gestión de la historia clínica, como la Resolución Ministerial 1995 de 1999, con el objetivo de proteger la privacidad de este documento privado y obligatorio. Otra legislación, como la Ley 1712 del 2014, también aborda asuntos relacionados con el acceso a la información, incluyendo datos personales. El derecho a la información, definido en el artículo 20 de la Constitución Política, se encuentra en consonancia con el principio de publicidad y representa una dimensión del acceso al derecho a la salud. Sin embargo, debe asegurarse sin disminuir el derecho de hábeas data acerca de la información sanitaria. La Superintendencia de Industria y Comercio (SIC) cumple un rol de vigilancia y sanción, habiendo emitido directrices e investigado casos de datos sensibles, lo que subraya la necesidad de cumplimiento. La Superintendencia Nacional de Salud (Supersalud) también tiene un papel en la supervisión en el sector salud.

A pesar de que se reconoce el derecho esencial al hábeas data (que abarca componentes fundamentales de la protección de datos personales) y la sensibilidad de la

información en salud, la protección de los datos personales en el marco particular de las relaciones contractuales entre Entidades Promotoras de Salud (EPS) e Instituciones Prestadoras de Servicios de Salud (IPS) se encuentra con retos considerables. Estos retos comprenden la ausencia de un marco normativo específico y unificado para la administración de datos sensibles en salud en este marco contractual, la falta de prácticas consistentes, protocolos uniformes, y la necesidad de aclarar las obligaciones contractuales en la gestión de datos sensibles, creando riesgos latentes para la privacidad y seguridad de los pacientes.

1.2 CONCEPTOS FUNDAMENTALES Y EL DATO SENSIBLE EN SALUD

El análisis de la protección de datos personales en las relaciones contractuales entre las EPS e IPS en Colombia requiere la comprensión de varias nociones esenciales. Un elemento esencial en esta investigación es la aceptación de que la información de salud constituye una categoría particular de datos sensibles.

El derecho a la protección de datos personales es un derecho fundamental que concede a las personas un tipo particular de libertad, otorgándoles la facultad de gestionar y supervisar su información personal. Este derecho es ambiguo y no se encuentra totalmente claro en su estructura y contenido, lo que exige un intenso trabajo de argumentación para su protección y justificación. No obstante, se fundamenta en principios que respaldan su presencia, reconocimiento y respeto obligatorio.

Dentro de este derecho fundamental, un componente significativo, aunque no el único, es el hábeas data o hábeas scriptum. Este incluye las capacidades más recientes del titular para conocer, actualizar, rectificar, suprimir, entre otras, su información. La idea del derecho fundamental al hábeas data se ha desarrollado a través de la jurisprudencia de la Corte Constitucional, enfatizando la importancia de los principios de justicia. Estos principios actúan como mecanismos a través de los cuales se logra la protección de los derechos fundamentales de las personas frente al tratamiento de sus datos personales.

Las restricciones que el ordenamiento jurídico impone al tratamiento de datos, especialmente a través de estos principios y las obligaciones de responsables y encargados, son elementos integrantes del contenido y alcance del derecho fundamental a la protección de datos personales. Un principio significativo en el ámbito de la salud es el respeto de que los datos personales relacionados con la salud sean manejados de manera confidencial. Se considera que la información sanitaria es sensible y, por lo tanto, requiere una protección reforzada. El carácter de estos datos, que abarcan registros clínicos y diagnósticos, sugiere que su manejo debe cumplir con altos estándares de seguridad y, con el permiso explícito del titular.

La jurisprudencia de la Corte Constitucional ha sido crucial para dar forma a estas ideas en Colombia. Específicamente, la decisión T-729 de 2002 es notable por establecer principios rectores fundamentales que deberían dirigir el manejo de datos sensibles relacionados con la salud. Esta decisión también confirmó el papel de la tutela como el mejor método legal para proteger este derecho fundamental contra posibles vulneraciones. La acción de tutela, dirigida por principios como la prevalencia del derecho sustancial y la solidaridad, tiene como objetivo asegurarse de que las personas puedan gozar completamente sus derechos a la salud, incluidos los tratamientos de atención completa y continuos, sin necesidad de múltiples acciones judiciales por cada servicio. El marco legal del hábeas data busca la protección más efectiva de su núcleo fundamental y principios, incluso en circunstancias de crisis.

El concepto de "tratamiento" de datos personales juega un papel crucial en el campo de la protección jurídica de la información. Su definición es amplia e incluye todas las acciones que se puedan llevar a cabo con la información, como la recolección, almacenaje, uso, circulación o supresión. Este carácter expansivo implica que el tratamiento no se limita a prohibidas o restringidas, sino que también puede ser acciones legales permitidas y promovidas, siempre que se realice conforme a los principios rectores establecidos por la ley vigente, tales como la legalidad, la finalidad, la libertad, la veracidad, la transparencia, la seguridad y la confidencialidad.

Si bien no existe un marco jurídico general y jurisprudencial en materia de protección de datos y específicamente de datos sanitaria sensible, se han identificado desafíos importantes y hay una evidente falta de legislación específica y de un enfoque consistente para abordar adecuadamente las particularidades del intercambio bilateral de datos sensibles que tiene lugar dentro de la relación contractual entre EPS e IPS. La falta de uniformidad y regulación precisa en esta circunstancia particular pone en peligro la privacidad y la seguridad del paciente, lo que resalta la necesidad de investigación en esta área.

La protección de la información médica es un derecho fundamental al hábeas data. El carácter perceptible de estos hechos exige una protección reforzada, sustentada en principios específicos y sostenida por la jurisprudencia de la Corte Constitucional y mecanismos como la acción de tutela. Sin embargo, la exitosa aplicación de estas ideas y principios en el complejo flujo de datos entre EPS e IPS presenta desafíos que requieren un análisis exhaustivo.

1.3 ESTADO ACTUAL Y PROBLEMÁTICA EN LAS RELACIONES CONTRACTUALES EPS-IPS

Los datos en el sector salud en Colombia suponen un desafío importante. Esto se debe principalmente a la naturaleza sensible de la información manejada y a la gran cantidad de datos intercambiados entre EPS e IPS. Estas organizaciones tienen el deber de trabajar juntas y a su vez garantizar que todos los afiliados tengan acceso oportuno a los servicios de salud en todo el país. Para cumplir con esta función fundamental, las EPS e IPS establecen relaciones contractuales que implican inevitablemente la transmisión y tratamiento continuado de información personal y médica de los pacientes.

Si bien este intercambio de datos es esencial para una atención médica oportuna y adecuada, existen graves riesgos para la privacidad y la seguridad de la información. Es aquí donde radica la raíz del problema. Existe un conflicto inherente entre la urgente necesidad de intercambiar datos sensibles para la prestación eficiente de servicios y la obligación ineludible de garantizar la estricta confidencialidad y seguridad de estos datos.

A pesar de que Colombia dispone de un marco legal general, como la Ley 1581 de 2012 y sus decretos reglamentarios, junto con directrices de la Superintendencias Nacional de Salud, la Superintendencia de Industria y Comercio y diversa jurisprudencia consistente de la Corte Constitucional, todavía persisten barreras prácticas y jurídicas que complican su desarrollo.

La dificultad se agudiza especialmente en el marco contractual entre EPS e IPS. En este contexto, el carácter y propósito del tratamiento de datos requieren elevados niveles de protección para evitar accesos no permitidos, pérdidas o abuso asociado a la información sensible. Un elemento que las EPS, para desempeñar su papel de aseguradoras, deben establecer acuerdos con las IPS, frecuentemente bajo esquemas como capitación o pago por actividad.

Estos acuerdos requieren la divulgación de información personal. No obstante, se ha detectado una insuficiencia percibida y una falta de un marco regulatorio unificado y específico que contemple las especificidades de la gestión de datos sensibles en salud en el marco específico de las relaciones contractuales entre EPS e IPS. Esto sugiere que las normas actuales no cubren todos los requisitos específicos para manejar datos sensibles en los contratos de servicios de salud. La falta de una regulación cuidadosa y unificada se suma al hecho de que las diferentes partes del sistema no tienen las mismas reglas y prácticas para procesar datos. La falta de protocolos homogéneos para la transferencia y protección de datos entre EPS e IPS propicia inconsistencias en las prácticas de tratamiento de datos e incrementa la probabilidad de infracciones de seguridad, lo que ha resultado en incidentes.

El análisis de diversas acciones administrativas pone de manifiesto que las peticiones formuladas por los sujetos en relación con la gestión de sus datos personales no siempre son atendidas de manera integral, apropiada o dentro del marco legal. En numerosas instancias, los errores en la respuesta, la falta de claridad o la exigencia de que el titular persista en su insistencia para obtener una resolución, ponen de manifiesto las deficiencias en la diligencia exigida a los responsables del tratamiento. Estos problemas no sólo afectan el derecho

fundamental al hábeas data, sino que también violan directamente los derechos del titular. Las autoridades han subrayado que la obligación de los responsables trasciende la formalidad o el procedimiento, orientándose hacia el resultado: deben garantizar que la solicitud sea atendida de forma clara, integral y oportuna. No es aceptable retrasar o pedir más información sin una buena razón, ya que esto supone una carga injusta para el titular.

Además, la ausencia de criterios uniformes en el manejo de situaciones críticas como las emergencias sanitarias agrava estos problemas, aumentando la demanda de información junto con el riesgo de incumplimiento de los estándares de protección. Esto plantea interrogantes sobre la suficiencia del marco actual para proteger datos en contextos de alto riesgo.

1.4 CONEXIÓN CON EL PROBLEMA DE INVESTIGACIÓN

Contamos con un marco legal y judicial que reconoce como un derecho fundamental la protección de datos personales. Este derecho, plasmado en el artículo 15 de la Constitución Política, consagrado como hábeas data, confiere a los ciudadanos la capacidad de acceder, actualizar y rectificar la información contenida en bases de datos asociadas a ellos. Este derecho ha experimentado una transformación a través de la Ley Estatutaria 1581 de 2012 y sus sucesivos decretos reglamentarios (Decreto 1377 de 2013, Decreto 886 de 2014), los cuales definen normas generales, mecanismos de control y principios fundamentales. La jurisprudencia de la Corte Constitucional ha jugado un papel fundamental en la delimitación del alcance de este derecho y los principios fundamentales, considerándolas como elementos fundamentales del contenido y la extensión del derecho fundamental al hábeas data constitucional.

En el marco general, se pone énfasis en la categoría de datos de naturaleza sensible, siendo la información médica un ejemplo primordial. Debido a la naturaleza de estos datos, es necesario protegerlos estrictamente y debe cumplir con más altos estándares de privacidad y seguridad. Este marco general, concebido para un amplio espectro de procesamiento de datos, resulta complejo aplicarlo a la dinámica particular y compleja de las relaciones de las

EPS e IPS. Estos organismos, con el objetivo de garantizar la prestación puntual de servicios sanitarios, instauran acuerdos contractuales que conllevan un flujo constante y un volumen significativo de intercambio y tratamiento continuo de información personal y médica de los pacientes. Este intercambio es fundamental para la prestación de servicios de salud; sin embargo, inherentemente, implica riesgos considerables para la privacidad y la seguridad.

Por consiguiente, el principal desafío de la investigación reside en la percepción de insuficiencia en la protección de datos personales en este contexto particular. Pese a la presencia de regulaciones generales y jurisprudencia, persisten obstáculos considerables en su implementación efectiva en el sector sanitario.

Este contexto, propicia inconsistencias operativas que, más que ser meras deficiencias administrativas, se manifiestan como vulnerabilidades tangibles para los titulares. Frecuentemente, cada entidad interpreta y aplica de manera diferente los principios de protección de datos, lo cual obstaculiza la instalación de una línea coherente y clara en la protección de los derechos de los pacientes. Esta deficiencia normativa genera un vacío que obstaculiza la aplicación apropiada de las normas generales a circunstancias particulares y altamente sensibles que se manifiestan diariamente en el funcionamiento del sistema médico.

Esta situación se ve agravada por una tensión estructural insoluble entre la necesidad operativa de divulgar información clínica de forma rápida y eficiente —esencial para asegurar la continuidad y la calidad de la atención— y la obligación legal y ética de proteger rigurosamente la confidencialidad y la integridad de dicha información. Esta dualidad, en caso de no ser tratada de manera explícita en los marcos contractuales y normativos, compromete tanto la eficacia del sistema como los derechos fundamentales del usuario. Los datos de los pacientes pueden ser accesibles a personas no autorizadas, filtrados, perdidos o incluso utilizados sin permiso, lo que pone en riesgo su privacidad y puede tener consecuencias graves, no solo legales, sino también humanas.

Un elemento crucial a considerar es la ambigüedad presente en la definición de obligaciones contractuales y la distribución de responsabilidades. Numerosos acuerdos entre

las EPS e IPS no definen con precisión suficiente quién debe asumir la responsabilidad de elementos cruciales del procesamiento de la información, generando así áreas grises de corresponsabilidad. Esta falta de claridad podría dificultar el seguimiento de las decisiones, el establecimiento de protocolos de seguridad e incluso rastrear respuestas a incidentes, lo que reduciría la confianza en el sistema y dejaría a los pacientes sin protección efectiva.

Finalmente, la implementación práctica de los derechos otorgados por la legislación —como la rectificación, actualización o supresión de datos— persiste en confrontar barreras considerables. Es habitual identificar circunstancias en las que estos derechos son inexistentes en la práctica o se administran de manera insuficiente o tardía, lo cual evidencia una ausencia de diligencia por parte de las organizaciones responsables. El derecho fundamental al hábeas data exige una respuesta integral, clara y puntual a cada petición, sin imponer al solicitante la responsabilidad de perseverar para lograr lo que según la legislación le corresponde.

CAPÍTULO 2: EVALUACIÓN DE LAS PRÁCTICAS ACTUALES Y ÁREAS DE RIESGO EN EL TRATAMIENTO DE DATOS PERSONALES ENTRE EPS E IPS

Evaluar las prácticas actuales y encontrar áreas de riesgo en el manejo de datos personales entre EPS e IPS es clave para garantizar que la información sensible de los usuarios del sistema de salud de Colombia se mantenga segura. Este capítulo se centra en cómo se manejan los datos personales en el marco de las relaciones contractuales entre estas entidades, teniendo en cuenta los principios legales de finalidad, legalidad, consentimiento informado y seguridad consagrados en la Ley 1581 de 2012 y sus normas complementarias.

Asimismo, se examinan las deficiencias y brechas presentes en la implementación de estas prácticas, que pueden poner en riesgo la privacidad, la integridad y los derechos fundamentales de los pacientes, especialmente en el manejo de datos sensibles como la información clínica y de menores de edad. Las áreas fundamentales no solo contribuyen a la comprensión de los retos contemporáneos, sino que también establecen los fundamentos para la formulación de protocolos contractuales específicos que optimizarán la protección de datos en el sector de salud.

Este estudio se fundamenta en políticas institucionales en vigor, manuales de tratamiento de datos y directrices regulatorias, con el objetivo de proporcionar una perspectiva exhaustiva y contemporánea sobre el estado actual del tratamiento de datos personales en las Entidades Prestadoras de Salud (EPS) e Instituciones de Seguridad Social (IPS), y las consecuencias que esto conlleva para la confianza y seguridad de los usuarios del sistema sensible, como la información clínica y de menores de edad. Las áreas fundamentales no solo facilitan la comprensión de los retos contemporáneos, sino que también establecen los fundamentos para la formulación de protocolos contractuales específicos que potencian la protección de datos en el sector sanitario.

2.1. EL FLUJO DE DATOS PERSONALES EN LAS RELACIONES CONTRACTUALES EPS-IPS: UNA DESCRIPCIÓN DE LAS PRÁCTICAS IDENTIFICADAS

El flujo de datos personales en las relaciones contractuales entre las Entidades Promotoras de Salud (EPS) y las Instituciones Prestadoras de Salud (IPS) es una parte importante del funcionamiento del sistema de salud colombiano. Este flujo se compone de procesos regulados y sistematizados, prácticas reguladas, sistematizadas y de alta seguridad y estándares legales que buscan asegurar el adecuado manejo de los datos personales y los usuarios, especialmente aquellos considerados sensibles, como estado de salud, historial clínico, diagnósticos, tratamientos y otra información requerida.

En este contexto, el intercambio de datos personales entre EPS e IPS se fundamenta en la necesidad de atender obligaciones contractuales que se derivan del aseguramiento de la salud, la prestación efectiva de los servicios médicos, la facturación, la auditoría de los servicios y la continuidad de la atención. Todo esto se hace bajo la protección del derecho fundamental al habeas data, que está regulado principalmente por la Ley 1581 de 2012, el Decreto Reglamentario 1377 de 2013 y otras disposiciones específicas como la Ley 1751 de 2015 (Ley Estatutaria de Salud), que reafirman la protección de los datos en el marco del derecho a la salud. Prácticas que se han encontrado en este flujo:

RECOLECCIÓN Y TRANSMISIÓN DE DATOS

La IPS es la primera línea de atención y es la responsable de recoger los datos personales de los usuarios cuando se presta el servicio. Los datos se registran en la historia clínica y pueden incluir información general (nombre, identificación, contacto), información sensible (diagnósticos, tratamientos, historial clínico) y, en algunos casos, datos especialmente protegidos (como los relacionados con la salud mental, enfermedades de transmisión sexual o discapacidad).

Luego, estos datos se envían a las EPS a través de canales electrónicos seguros, interoperables y que cumplen con los estándares normativos y técnicos establecidos por el Ministerio de Salud y Protección Social, como el Plan Nacional de Interoperabilidad en Salud. Este intercambio permite a las EPS llevar a cabo la gestión del riesgo en salud, realizar procesos de autorización, facturación, validación de servicios, seguimiento de tratamientos y actividades de control y auditoría.

AUTORIZACIÓN Y CONSENTIMIENTO

El consentimiento informado es uno de los principios que rigen el tratamiento de datos personales. la Ley 1581 de 2012 y en concordancia con el artículo 15 de la Constitución Política de Colombia.

Cuando se trata de datos sensibles, como los relacionados con la salud, o de titulares que pertenecen a poblaciones vulnerables (menores de edad, personas en situación de discapacidad), se exige una autorización especial y reforzada. La ley colombiana exige que se brinde información clara y suficiente sobre la finalidad del tratamiento, los derechos del titular y los mecanismos disponibles para ejercerlos.

RESPONSABILIDAD Y SEGURIDAD:

Tanto la EPS como LA IPS son ambas responsables del manejo de datos personales, pero lo hacen de diferentes maneras en distintos puntos del flujo de información. Estas medidas incluyen el uso de tecnologías de seguridad administrativas, autenticación de usuarios, protocolos de respaldo y recuperación, auditorías periódicas y formación del personal en protección de datos. Además, las entidades deben cumplir con los principios de transparencia, acceso restringido, circulación limitada, seguridad y confidencialidad establecidos por la regulación de Colombia.

Deben garantizarse a los titulares de los datos el ejercicio efectivo de sus derechos, como:

- Conocer la información que se posee sobre ellos.
- Solicitar la actualización, corrección o eliminación de datos incorrectos o inapropiados.
- Revocar el consentimiento otorgado para el tratamiento, salvo que exista una obligación legal o contractual que lo impida.

Una consideración a tener en cuenta es que el flujo de datos entre EPS e IPS también está sujeto a principios de finalidad y necesidad, lo que significa que los datos recolectados y compartidos deben ser estrictamente los requeridos para cumplir los fines previamente informados al titular, sin exceder el tratamiento necesario para tal propósito.

También es importante tener presente la evolución jurisprudencial de la Corte Constitucional, que ha subrayado reiteradamente que la historia clínica es un documento privado y que su divulgación no autorizada puede vulnerar derechos fundamentales como la intimidad, la dignidad y el acceso a la atención sanitaria. Es importante tener en cuenta los avances jurisprudenciales de la Corte Constitucional, que ha subrayado reiteradamente que la historia clínica es un documento privado y que su divulgación no autorizada puede vulnerar derechos fundamentales como la intimidad, la dignidad y el acceso a la atención sanitaria.

2.2. EVALUACIÓN DE LA CONFORMIDAD Y EFECTIVIDAD DE LAS PRÁCTICAS FRENTE A LA NORMATIVA: BRECHAS SIGNIFICATIVAS EN EL SGSSS

El análisis de la protección de datos personales en las relaciones contractuales entre las EPS y las IPS dentro del marco del Sistema General de Seguridad Social en Salud (SGSSS) pone en evidencia la existencia de brechas normativas y operativas que dificultan la aplicación efectiva del régimen de protección de datos personales en Colombia, particularmente en el ámbito de la salud.

A pesar de que la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 establecen principios básicos como legalidad, libertad, finalidad, veracidad, transparencia, seguridad y

acceso limitado, su implementación en la práctica aún enfrenta serios problemas estructurales y culturales en las EPS e IPS, que afectan directamente los derechos fundamentales de los usuarios del sistema de salud. Se identifican las siguientes brechas principales:

CONSENTIMIENTO INFORMADO INSUFICIENTE O DEFICIENTE

La falta de consentimiento para el tratamiento de datos personales es uno de los errores más comunes en la práctica. En algunos casos, este se obtiene de manera genérica, implícita o vaga sin proporcionar al titular una explicación clara, detallada y comprensible sobre la finalidad del tratamiento. Esto viola el principio de libertad, especialmente cuando se trata de datos sensibles, como los relativos a la salud, tratamientos médicos, discapacidades, entre otros.

En entornos donde el usuario se encuentra en un estado de urgencia o vulnerabilidad, dar el consentimiento puede convertirse más en una formalidad que en un acto voluntario, informado y consciente, debilitando la base legal para el tratamiento de datos.

FALTA DE TRANSPARENCIA Y DEFICIENCIAS EN EL ACCESO A LA INFORMACIÓN

No siempre se garantiza adecuadamente el derecho de los titulares a conocer, acceder, actualizar y rectificar sus datos. La mayoría de las EPS e IPS no tienen canales accesibles, claros y oportunos para que los usuarios puedan ejercer estos derechos, lo que va en contra del principio de transparencia que se establece en el artículo 4 de la Ley 1581.

Además, muchas entidades escriben su política de tratamiento de datos en un lenguaje técnico o legal que no se entiende muy bien, lo que hace que el usuario no sepa qué datos se recogen, cómo se usan, con quién se comparten y por cuánto tiempo se conservan.

DEBILIDADES EN LAS MEDIDAS DE SEGURIDAD TÉCNICAS Y ADMINISTRATIVAS

Si bien la ley exige el uso de mecanismos consolidados para proteger la información personal, la realidad en muchas IPS, especialmente las más pequeñas o las de zonas rurales, es que no gastan mucho en sistemas de seguridad digital ni en protocolos administrativos de protección de datos. Esto incluye:

- Uso de software obsoleto.
- Acceso no controlado al historial médico.
- Manipulación de documentos sin el almacenamiento adecuado.
- Administración de documentos físicos sin custodia apropiada

Todos estos elementos aumentan enormemente las posibilidades de pérdida de datos, robo de identidad, fugas de información y otros eventos que afectan la confidencialidad, integridad y disponibilidad de la información.

AUSENCIA DE AUDITORÍA INTERNA Y SUPERVISIÓN AFECTIVA

Muchas de estas organizaciones no realizan auditorías rutinarias ni establecen sistemas centralizados de evaluación y control para garantizar el cumplimiento de las normas de protección de datos. La ausencia de un sistema de monitoreo interno dificulta la pronta identificación de errores o violaciones, afectando la capacidad de la institución para responder a los riesgos o violaciones.

Esto se agrega a la ausencia de capacidad de supervisión externa por parte de la Superintendencia de Industria y Comercio (SIC), la entidad responsable de supervisar el cumplimiento del régimen de hábeas data. En un sistema sanitario complejo y con un amplio número de actores, la supervisión gubernamental se torna restringida ante la magnitud de los retos a enfrentar.

2.3. IDENTIFICACIÓN DE ÁREAS DE MAYOR RIESGO PARA LA PRIVACIDAD

El marco de las relaciones contractuales entre EPS e IPS y las áreas críticas que representan mayores riesgos para la privacidad de los datos personales permiten ver los puntos débiles del sistema que necesitan una intervención estratégica inmediata. A pesar de la existencia de diferentes regulaciones en donde se establecen obligaciones claras y expresas frente al manejo de datos personales, aún existen vulnerabilidades estructurales, técnicas y humanas que ponen en riesgo la privacidad de los pacientes dentro del Sistema General de Seguridad Social en Salud (SGSSS). Principales áreas de riesgo identificadas:

FILTRACIÓN DE ACCESO NO AUTORIZADO A DATOS PERSONALES SENSIBLES

Los datos sobre la historia clínica, el estado de salud, los diagnósticos, los tratamientos y los medicamentos son clasificados como datos personales sensibles, lo que significa que deben ser protegidos de acuerdo con el artículo 6 de la Ley 1581 de 2012. Sin embargo, hay muchos casos documentados de acceso no autorizado por personal no habilitado para dicha facultad, filtraciones intencionadas o negligentes y divulgaciones indebidas a terceros no autorizados. Estos eventos pueden resultar en transgresiones severas de derechos fundamentales como la intimidad, la dignidad y la igualdad, impactando de manera directa a individuos que podrían experimentar repercusiones como la discriminación en el ámbito laboral, la estigmatización social, el hostigamiento o las perturbaciones emocionales.

La Corte Constitucional ha declarado que el principio de confidencialidad de la información médica representa un elemento fundamental del derecho a la salud, y su violación puede acarrear consecuencias jurídicas para las partes implicadas (Sentencia T-414 de 1992, entre otras).

DEBILIDADES EN LA APROPIACIÓN E IMPLEMENTACIÓN DE POLÍTICAS INTERNAS

Aunque numerosas Entidades Prestadoras de Salud (EPS) e Instituciones Prestadoras de Salud (IPS) han implementado políticas de gestión de datos personales y manuales de buenas prácticas en conformidad formal con la Ley 1581 de 2012, la aplicación efectiva de dichas medidas aún se encuentra limitada. En la ejecución práctica, se verifican:

- Insuficiencia en la formación del personal respecto al contenido y la extensión de dichas políticas.
- La ausencia de protocolos específicos y operativos para la administración diaria de la información.
- La violación del mandato de privacidad por parte de empleados.

La discrepancia entre las regulaciones y las prácticas operativas favorece un entorno propicio para errores, omisiones y prácticas inapropiadas. La protección de la información no debe limitarse a los archivados, sino que debe transformarse en una cultura organizativa viva, fundamentada en la educación continua, la evaluación de riesgos y la rendición de cuentas internas.

2.4. PROFUNDIZACIÓN DEL ANÁLISIS: EL IMPACTO DE LAS PRÁCTICAS DEFICIENTES EN LOS DERECHOS FUNDAMENTALES

Un análisis detallado de los efectos del manejo indebido de datos personales en las relaciones contractuales entre Entidades Promotoras de Salud (EPS) e Instituciones Prestadoras de Salud (IPS) revela un conjunto de afectaciones que van más allá de la privacidad y afectan directamente derechos fundamentales como la dignidad humana, la integridad personal, el derecho a saber y el acceso efectivo a la atención en salud.

A partir de estos descubrimientos, se puede señalar la presencia de un entramado sistémico de riesgos que no solo pone de manifiesto deficiencias normativas y operativas en

la administración de la información clínica, sino que exige una respuesta coordinada e inmediata por parte del Estado, los proveedores de servicios de salud y la ciudadanía.

Un detallado análisis de las consecuencias del manejo indebido de datos personales en las relaciones contractuales entre Entidades Promotoras de Salud (EPS) e Instituciones Prestadoras de Salud (IPS) revela un conjunto de vulneraciones que van más allá de la privacidad y afectan directamente derechos fundamentales como la dignidad humana, la integridad personal, la autodeterminación informativa y el acceso efectivo a la salud. Con base en estos hallazgos, queda claro que existe una red sistémica de riesgos que no sólo muestra fallas en las normativas y operaciones de gestión de la información clínica, sino que también requiere una respuesta inmediata y coordinada del Estado, los proveedores y la ciudadanía.

Una de las afectaciones encontradas es que el derecho a la salud y a una vida digna se ve afectado cuando errores en el procesamiento de datos imposibilitan el acceso oportuno a servicios médicos esenciales. Un caso crítico es cuando se niegan servicios por errores administrativos o tecnológicos relacionados con la actualización o integridad de la información del paciente. La Corte Constitucional ha documentado momentos en los que, por mala gestión de datos de personas que viven con VIH, se retrasó la entrega de medicamentos antirretrovirales, poniendo en peligro su vida e integridad. Esta situación se agrava en comunidades marginadas como migrantes y personas transgénero, que enfrentan barreras adicionales debido a inconsistencias en sus registros personales, como el nombre o el sexo autopercibido que no se actualiza, lo que hace que sea más difícil seguir recibiendo atención médica.

El derecho a no ser discriminado se viola cuando la filtración de información sensible, como diagnósticos psiquiátricos o enfermedades de transmisión sexual, conduce a prácticas estigmatizadoras. Según el Estudio Ponemon del año 2024, el 67% de las filtraciones de datos en el sector de la salud conducen a comportamientos discriminatorios que afectan desproporcionadamente a las mujeres embarazadas y a las personas LGBTIQ+. Las consecuencias de estas filtraciones incluyen la pérdida de empleo, la violencia institucional,

la exclusión social y la revictimización dentro del mismo sistema de salud, lo que demuestra que el tratamiento indebido de datos sensibles no solo es una infracción legal, sino una puerta de entrada a vulneraciones estructurales de derechos fundamentales.

También es importante mencionar la preocupación en la afectación al derecho de la autodeterminación informativa, que es un principio consagrado en la Ley 1581 de 2012, cuya vigencia se ve seriamente comprometida por la imposibilidad que tienen muchos pacientes de ejercer control sobre sus datos personales. Un análisis realizado muestra que el 42% de las IPS evaluadas no permiten corregir errores en las historias clínicas, lo que constituye una grave violación al principio de veracidad y pone en riesgo la calidad del diagnóstico, la pertinencia y la capacidad de ejercer otros derechos, como el acceso a la justicia y la defensa jurídica, en los procesos en que el historial médico es una pieza esencial de evidencia.

A todo esto, se le agrega la vulneración al derecho de la intimidad al usar datos personales para fines que no son atención médica. Un ejemplo de ello es el uso de bases de datos clínicas para comercializar medicamentos, lo que va en contra del principio de finalidad. La Superintendencia de Industria y Comercio multó a 15 entidades de salud por realizar esta práctica entre 2023 y 2024. Las multas sumaron más de $1.800 millones de pesos. Estas acciones demuestran que los datos clínicos no están siendo tratados con el respeto que merecen por su naturaleza sensible, sino que están siendo usados como activos transaccionales sin el consentimiento ni conocimiento de los titulares.

Uno de ellos es la judicialización creciente: en 2023, el 38% de las acciones de tutela en salud estuvieron relacionadas con errores o negligencias en el manejo de datos personales, según la Defensoría del Pueblo. Esto demuestra que los usuarios se ven obligados a recurrir a la vía judicial para arreglar problemas que deben ser solucionados por la administración, lo que causa congestión en las instituciones y desconfianza en la ciudadanía.

Del mismo modo, se ha producido una pérdida de confianza en las instituciones. Encuestas realizadas arrojaron que el 61% de los usuarios evitan compartir información clínica completa con su EPS o IPS por temor a filtraciones o uso indebido. Esto reduce la

calidad del diagnóstico, imposibilita la elaboración de planes de salud integrales y reduce la eficacia de las intervenciones médicas. Asimismo, el incumplimiento de la Ley 1581 de 2012 ha traído una creciente inseguridad jurídica para estas entidades. Las sanciones han aumentado en un 200%, incluyendo la suspensión temporal de contrataciones con el Estado para tres EPS en 2024. Esto afecta la continuidad del servicio y genera incertidumbre en las relaciones contractuales del sistema.

Ante esta situación, es necesaria una intervención multinivel que integre acciones regulatorias, institucionales y culturales para asegurar la efectiva protección de los datos personales de salud. La implementación de auditorías cruzadas entre EPS e IPS para garantizar la trazabilidad y cumplimiento normativo en la transmisión de datos sensibles; la adopción de protocolos de anonimización en toda transferencia de información clínica, especialmente en contextos de interoperabilidad o análisis estadístico; el desarrollo de sistemas de alerta temprana para identificar y contener accesos indebidos en tiempo real; y la capacitación obligatoria del personal médico y administrativo en ética de datos y derechos fundamentales, con enfoque práctico y diferencial para poblaciones vulnerables.

En conclusión, los resultados muestran que la protección de datos personales en las relaciones contractuales EPS-IPS no solo debe ser vista como una obligación legal, sino también como una condición estructural para garantizar el núcleo de derechos fundamentales en el sistema de salud de Colombia. La información no puede ser tratada como una variable operativa más, sino como parte central de la dignidad humana, la autonomía personal y la confianza en las instituciones. Por tanto, el cumplimiento de la ley debe integrarse a una ética del cuidado centrada en el paciente como sujeto de derechos y no como objeto de gestión administrativa.

CAPÍTULO 3: PROPUESTA DE PROTOCOLOS CONTRACTUALES ESPECÍFICOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA RELACIÓN EPS-IPS

Como parte del análisis de las vulnerabilidades en el manejo de datos personales en el sistema de salud en Colombia, es necesario proponer un conjunto integral de protocolos contractuales entre las Entidades Promotoras de Salud (EPS) y las Instituciones Prestadoras de Salud (IPS) que no solo aseguren el estricto cumplimiento del marco legal vigente —especialmente la Ley 1581 de 2012 y el Decreto 1074 de 2015—, sino que también brinden una protección sustancial de los derechos fundamentales de los titulares.

Dado que la relación EPS–IPS tiene un carácter dual, con responsabilidades compartidas y diferencias en el grado de control sobre la información, la estructuración de cláusulas contractuales específicas debe responder a un enfoque de responsabilidad proactiva y colaborativa. Este enfoque no sólo frena conflictos y sanciones, sino que también genera confianza institucional, fortalece la interoperabilidad técnica con garantías y ayuda a construir una cultura organizacional basada en la ética de los datos personales.

3.1. DEFINICIÓN PRECISA DE RESPONSABILIDADES

Un componente esencial en la elaboración de acuerdos contractuales eficaces entre Entidades Prestadoras de Salud (EPS) e Instituciones de Protección de Datos (IPS) es la definición precisa, meticulosa y legalmente vinculante de las obligaciones de cada parte en relación con la administración de datos personales. Esta determinación no puede apoyarse en el azar o en interpretaciones ambiguas, dado que se fundamenta en una identificación precisa de las obligaciones jurídicas, el régimen penal correspondiente y la salvaguarda efectiva de los derechos de los poseedores de la información.

Los términos responsables y encargados del tratamiento tienen implicaciones legales distintas en el marco normativo de Colombia, específicamente en lo estipulado en la Ley

1581 de 2012. La parte responsable es el encargado de tomar decisiones respecto al tratamiento, delineando los objetivos y componentes claves de este. Por otro lado, el encargado opera en representación del responsable, llevando a cabo el tratamiento de acuerdo con sus directrices. Esta distinción, recogida también en el Decreto 1074 de 2015 y en las directrices de la Superintendencia de Industria y Comercio, debe trasladarse de manera explícita al texto contractual que regula la relación entre EPS e IPS.

En ese sentido, el contrato debe identificar a la EPS como responsable del tratamiento, dado que esta entidad —por su rol dentro del sistema de salud— tiene la facultad de determinar los fines del tratamiento de los datos personales, en tanto coordina la afiliación, administración del riesgo en salud y la autorización de servicios. Es la IPS del tratamiento en general y sigue las instrucciones de la EPS para ofrecer servicios de asistencia médica eficaces. Esto significa que la IPS tiene que seguir estrictamente funciones como llevar un registro de las consultas, diligenciar los registros clínicos y reporte de información médica importante.

Sin embargo, es importante tener en cuenta que esta asignación no es estática ni automática. En algunos casos, la IPS también puede actuar como responsable del tratamiento, como cuando gestiona directamente el historial clínico de un paciente y decide por sí misma si lo conserva o lo comparte. Por consiguiente, en el contrato es imperativo prever la eventualidad de responsabilidades compartidas o concurrentes, especificando con precisión las estipulaciones que definen los supuestos bajo los cuales cada entidad asume el papel de responsable, encargado o corresponsable.

La definición de responsabilidades en el contrato debe incluir obligaciones específicas y verificables, como las siguientes:

- El deber de implementar políticas internas de protección de datos.
- La obligación de contar con registros de actividades de tratamiento.
- La designación de oficiales de protección de datos (DPO o su equivalente).

- La adopción de procedimientos para la atención de solicitudes de los titulares. La colaboración mutua para atender requerimientos de la Superintendencia de Industria y Comercio.

Esta demarcación funcional de separación no sólo sigue el principio de responsabilidad demostrada (accountability) establecido en la Ley 1581 de 2012, sino que también ayuda a reducir el riesgo de lagunas legales o desacuerdos entre las partes en caso de incidentes de seguridad, fugas de información o demandas por violaciones a derechos fundamentales.

Además, una definición precisa de las responsabilidades contractuales fomenta la rastreabilidad de las acciones y el monitoreo de las obligaciones legales. En situaciones de reclamación o incidente, resulta imprescindible identificar con exactitud a la entidad encargada de la protección de la información, quién concedió la autorización para su procesamiento y las condiciones bajo las cuales fue transmitida o almacenada. De no contar con esta claridad, ambas entidades pueden ser objeto de investigaciones y sanciones administrativas, con consecuencias no solo económicas, sino también reputacionales.

Por lo tanto, el primer paso para garantizar la protección de los datos personales en la relación EPS–IPS es dejar consignada en el contrato —mediante cláusulas expresas, inequívocas y operativas— la estructura de responsabilidades, ajustada al flujo real de la información, a los sistemas tecnológicos involucrados y a la autonomía funcional que cada parte ejerce. Solo de este modo se logra una protección integral de los derechos de los pacientes, una adecuada distribución de riesgos y una gestión contractual coherente con los principios del régimen de hábeas data en Colombia.

3.2. CLÁUSULAS ESPECIFICAS SOBRE CONSENTIMIENTO Y FINALIDAD

Uno de los elementos cruciales para la protección de los datos personales en los contratos entre las EPS e IPS es la estricta adhesión al principio del consentimiento del titular y la definición precisa de los propósitos para los cuales se recopila, usa y comparte la

información. En ese sentido, todo protocolo contractual debe incluir cláusulas específicas que garanticen que el tratamiento de datos personales —especialmente aquellos considerados sensibles, como los datos clínicos— se realice exclusivamente con el consentimiento previo, expreso e informado del titular, de conformidad con lo establecido en la Ley 1581 de 2012, el Decreto 1377 de 2013 y el Decreto Único Reglamentario 1074 de 2015.

El consentimiento, entendido como la expresión de la voluntad libre y autónoma del sujeto, no debe ser interpretado como un procedimiento meramente formal o generalizado. En contraposición, su validez se encuentra condicionada porque sea otorgado de forma informada, es decir, que el usuario del sistema de salud tenga pleno conocimiento acerca de cuáles datos serán recopilados, con qué finalidad, qué duración, con quién serán compartidos y cuáles derechos le son asignados en relación con su información personal. En este caso, dentro de las condiciones contractuales, deberán exigir a EPS, como responsable del tratamiento, que asegure las garantías para obtener y conservar pruebas documentales físicas o digitales del consentimiento otorgado por los usuarios. Esto es fundamental para efectos probatorios en situaciones de reclamaciones y sanciones.

Los contratos deben especificar las finalidades legítimas y necesarias del tratamiento, limitándolas solo a las que estén directamente relacionadas con la prestación del servicio de salud. Esto incluye, por ejemplo, la programación de citas, el seguimiento clínico, la facturación por servicios prestados, la remisión de pacientes entre diferentes niveles de atención y la comunicación con entidades establecidas para cumplir con obligaciones legales. La información nunca debe utilizarse para fines distintos de aquellos para los que el propietario ha dado permiso, como enviar anuncios de medicamentos, elaborar perfiles para fines comerciales o proporcionar datos a terceros sin el permiso explícito del propietario.

De hecho, la inclusión de cláusulas que prohíban expresamente el uso de datos personales con fines secundarios o no autorizados se convierte en un blindaje contractual ante posibles desviaciones del principio de finalidad. Esta disposición es en especial importante porque recientemente la Superintendencia de Industria y Comercio ha sancionado a varias personas del sector salud por utilizar datos personales de los usuarios para fines

comerciales sin base legal ni consentimiento explícito, lo que vulnera gravemente el derecho a la privacidad y el control de la información por parte del titular.

Además, las cláusulas sobre el consentimiento y la finalidad deben tener en cuenta situaciones excepcionales, como los tratamientos legalmente permitidos para emergencias, la monitorización epidemiológica o la ejecución de mandatos judiciales o administrativos, en las que el consentimiento puede no ser necesario de acuerdo con la legislación vigente. No obstante, resulta crucial que el contrato establezca explícitamente estas circunstancias para prevenir interpretaciones que faciliten la implementación de prácticas que puedan infringir los derechos.

Las cláusulas contractuales relacionadas con el consentimiento y el propósito del tratamiento representan una protección esencial frente a prácticas invasivas, desproporcionadas o arbitrarias en la gestión de la información de los usuarios del sistema de salud. Además de prevenir sanciones legales, la inclusión y ejecución adecuadas también promueven el respeto a la autonomía individual, la confianza en las instituciones y la legitimidad en el uso de datos en un campo tan sensible como el sector de salud. Y al realizar los contratos entre EPS e IPS, se debe dar máxima prioridad a la precisión técnica, jurídica y operativa de esas disposiciones.

3.3. MEDIDA DE SEGURIDAD Y CONFIDENCIALIDAD

En relación con las medidas de seguridad y confidencialidad que deben ser incorporadas en los contratos entre EPS e IPS, es esencial que dichas estipulaciones se diseñen con un elevado grado de especificidad técnica y jurídica. Estas estipulaciones deben evidenciar un compromiso colectivo para asegurar la integridad, confidencialidad y disponibilidad de los datos personales, particularmente aquellos de naturaleza delicada vinculados con la salud. Conforme al principio de seguridad estipulado en la Ley 1581 de 2012, los contratos deben establecer, como responsabilidad de ambas partes, la implementación de protocolos técnicos, físicos y administrativos apropiados para los riesgos detectados en el procesamiento de datos clínicos. Esto significa, en primer lugar, que se debe

instalar un cifrado sólido de la información, tanto en tránsito como en reposo, con el objetivo de minimizar la probabilidad de accesos no autorizados o interceptaciones malintencionadas durante las transacciones de datos entre entidades.

Además, es fundamental incluir la responsabilidad de instalar controles de acceso basados en niveles jerárquicos, mediante sistemas de autenticación especializados y la asignación individual de credenciales. Esto asegura que solo el personal con el permiso adecuado pueda acceder a la información clínica de los pacientes. Es muy importante que estas herramientas de control se utilicen con sistemas de auditoría electrónica que registren automáticamente todas las acciones realizadas sobre los datos, incluyendo consultas, modificaciones o estos controlan, identificando al usuario responsable, el momento de la acción y su naturaleza. Es imperativo que estos registros sean resguardados de manera segura, sometidos a inspecciones regulares y mantenidos accesibles para su inspección por parte de las entidades encargadas de su control y supervisión.

Un elemento fundamental de dichas cláusulas debería ser la responsabilidad contractual de instaurar procesos de formación continua y educación del personal, tanto médico como administrativo, que interactúa con información personal. Esta formación debe cubrir no sólo los aspectos técnicos de la gestión segura de la información, sino también los principios éticos relacionados con la privacidad, la confidencialidad y el deber de proteger los datos de los pacientes. En el contexto actual, es esencial que las cláusulas contractuales estipulen que cualquier individuo que acceda a datos clínicos debe firmar previamente acuerdos de confidencialidad vinculantes, cuya violación constituye una causal de sanción disciplinaria o contractual.

La violación de estas disposiciones de seguridad y confidencialidad debería resultar en repercusiones explícitas, previamente estipuladas en el contrato. Por lo tanto, es necesario establecer mecanismos internos de vigilancia, junto con procedimientos punitivos proporcionales en caso de infracción. Incluir desde sanciones internas hasta rescisión anticipada del contrato, dependiendo de la gravedad de la infracción. Asimismo, es imperativo que exista un compromiso contractual para cooperar con las autoridades

pertinentes, particularmente con la Superintendencia de Industria y Comercio, en caso de que se instalen investigaciones por posibles infracciones al régimen de protección de datos individuales.

La elaboración de estas disposiciones no puede restringirse a un ajuste formal o simbólico del marco jurídico. En contraposición, esto debería materializarse en una arquitectura contractual que establezca una infraestructura de seguridad auténtica para el procesamiento de datos personales en el sector sanitario, adaptada a las especificidades del contexto tecnológico, los riesgos operativos de las entidades implicadas y la sensibilidad de la información procesada. Esta infraestructura debe caracterizarse por su dinamismo, susceptible de evaluación y ajuste constante, y constituir una garantía efectiva de los derechos fundamentales de los poseedores, trascendiendo la mera observancia normativa. Por consiguiente, la aplicación meticulosa de estas estipulaciones en los contratos EPS-IPS constituye un requisito indispensable para fomentar una cultura institucional de respeto por la privacidad, la ética en la gestión de información y la protección efectiva de los datos personales en el sistema sanitario colombiano.

3.4. PROCEDIMIENTOS PARA EL EJERCICIO DE DERECHOS DE LOS TITULARES

Para lograr este objetivo, es imperativo que los contratos integren la instalación de canales de atención específicos para los titulares, tanto físicos como virtuales, que permitan presentar sus solicitudes de manera directa y sin la necesidad de intermediarios. Es esencial que estos canales estén respaldados por protocolos internos que garanticen una respuesta precisa y significativa, en consonancia con lo estipulado en la normativa, y que promuevan la supervisión de cada caso desde su presentación hasta su resolución final. Además, es imperativo definir plazos máximos de respuesta, en consonancia con lo estipulado en los artículos 14 y 15 de la Ley 1581, y en consonancia con los principios de celeridad y eficacia de la función administrativa, evitando prácticas dilatorias o evasivas que puedan infringir el derecho fundamental de autodeterminación de información.

Además, los contratos deben incorporar la obligación para las EPS e IPS de colaborar de manera coordinada en situaciones donde la información requerida por el titular se encuentra parcialmente en cada una de las entidades, de tal manera que se asegura una respuesta holística y se previene la fragmentación del procedimiento. Esta responsabilidad de cooperación activa adquiere una relevancia particular en situaciones donde los datos personales, particularmente aquellos de naturaleza sensible, se encuentran disgregados entre diversos actores del sistema, tales como laboratorios, centros de diagnóstico, profesionales autónomos o terceros contratistas. Por lo tanto, las estipulaciones contractuales deben anticipar situaciones de interoperabilidad asistida, en las que se establecen obligaciones compartidas para garantizar que el solicitante obtenga una respuesta completa, auténtica y coherente a su solicitud.

En cuanto a la rectificación y actualización de la información, es crucial subrayar que toda petición presentada por el titular en este contexto debe ser gestionada con un estándar de diligencia estricta. Los errores en la historia clínica o en los datos administrativos pueden influir directamente en el acceso a tratamientos, diagnósticos precisos o decisiones clínicas precisas. Por consiguiente, los acuerdos contractuales deben definir no solo el procedimiento para gestionar dichas solicitudes, sino también los mecanismos de verificación interna que deben ser activados cuando la alteración de los datos pueda comprometer la continuidad del tratamiento médico u originar obligaciones médicas. Esta regulación contractual no solo protege los derechos del titular, sino que también brinda seguridad jurídica a las entidades participantes al establecer cómo deben actuar en caso de conflictos sobre la veracidad o integridad de la información documentada.

En el presente escenario, resulta esencial que los contratos establezcan la normativa que regula el derecho a la supresión de datos, particularmente en circunstancias en las que la relación con el titular haya cesado. A pesar de que el derecho a la supresión presenta restricciones cuando se refiere a datos cuyo almacenamiento se rige por obligaciones legales (como las historias clínicas que deben ser preservadas por un período específico), el contrato debe definir explícitamente los criterios que dictan este derecho, los mecanismos de anonimización cuando sea factible y las condiciones técnicas que aseguran que la supresión

no conlleve la pérdida de información esencial para propósitos estadísticos o epidemiológicos autorizados por la legislación.

La regulación contractual que rige el ejercicio de los derechos de los titulares en el contexto de la EPS-IPS debe superar una simple declaración de compromiso con la legislación vigente y convertirse en disposiciones operativas, minuciosas y verificables que garantizan que cada usuario del sistema de salud pueda ejercer sus derechos de forma eficaz, oportuna y sin dificultades, conforme a las normas constitucionales y legales de protección de datos personales en Colombia. Este aspecto es muy importante no sólo para la legitimidad del sistema, sino también para garantizar que el tratamiento de datos se realice de forma ética y respetuosa con la dignidad humana.

3.5. OBLIGACIÓN DE NOTIFICACIÓN DE INCIDENTES

Este deber está directamente relacionado con el principio de transparencia establecido en la Ley 1581 de 2012 y con los estándares internacionales de protección de datos personales. Es también muy importante para manejar los riesgos que conlleva el manejo de información sensible en el sector salud.

En virtud de esta obligación, debe establecerse que tanto EPS como IPS están en la responsabilidad de comunicar, de forma oportuna, cualquier situación anómala que pueda derivar en una pérdida, acceso no autorizado, divulgación no consentida o alteración indebida de los datos personales bajo su custodia. La notificación debe realizarse no solo entre las partes contratantes, sino también al titular afectado y, cuando sea procedente, a la autoridad de control competente, en este caso la Superintendencia de Industria y Comercio, conforme a las facultades de supervisión y sanción establecidas en el régimen general de protección de datos en Colombia.

Esta cláusula no puede entenderse de forma genérica o abstracta. El contrato debe contener una regulación precisa que defina los canales de comunicación oficiales para la notificación de incidentes, los cuales deben ser seguros, accesibles y previamente

establecidos, con el fin de evitar dilaciones o ambigüedades en la reacción institucional. Además, es crucial fijar tiempos límite para la notificación, de manera que se efectúe en un período razonable desde que se revela el incidente. Esto contribuirá a prevenir que los perjuicios se intensifiquen y simplificará la implementación de acciones correctivas inmediatas.

Además del deber de informar, deben existir procedimientos detallados para contener y reducir el incidente. Esto significa que el contrato debe incluir la existencia de protocolos de respuesta rápida, que estén formados por equipos técnicos y jurídicos elegidos por cada entidad, que permitan evaluar la magnitud del impacto, identificar las causas, contener la propagación del riesgo y definir acciones correctivas o compensatorias hacia los titulares afectados. En esta misma línea, debe incluirse el compromiso de documentar cada incidente, con un reporte detallado de lo ocurrido, las acciones ejecutadas y los resultados obtenidos, con el fin de alimentar procesos de mejora continua y auditoría interna.

Por otra parte, resulta esencial establecer que, en aquellos eventos en los que el incidente pueda afectar derechos fundamentales de los titulares —como la salud, la intimidad, la no discriminación o la autodeterminación informativa—, las partes tienen la carga reforzada de comunicar de forma directa, clara y comprensible al titular afectado lo sucedido, indicándole las posibles consecuencias, así como las medidas adoptadas para remediar el hecho y prevenir su repetición. Este factor humaniza la respuesta institucional y consolida la confianza del usuario en el sistema de salud.

En última instancia, el contrato debe contemplar la responsabilidad de notificar a la Superintendencia de Industria y Comercio cuando el incidente constituya una amenaza severa a los derechos de los titulares, de acuerdo con las directrices y circulares emitidas por dicha entidad. Este informe debe incluir la información mínima requerida, que abarca la descripción del incidente, la fecha y método de identificación, el volumen y la categoría de datos comprometidos, el impacto proyectado y las medidas implementadas por la entidad correspondiente. Así, se asegura la interacción entre los participantes del sistema de salud y

el ente de supervisión, facilitando una respuesta coordinada y eficaz frente a los riesgos vinculados al tratamiento inapropiado de información personal delicada.

La inclusión de una cláusula sólida para la notificación de incidentes en los contratos entre EPS e IPS no solo cumple una función regulatoria, sino que se convierte en un instrumento de control digital, administración de crisis y protección sustantiva de los derechos fundamentales de los titulares. La formulación adecuada ayuda a reducir el impacto de eventos adversos, aumentar la responsabilidad y respetar la privacidad en el campo de la salud.

CONCLUSIÓN

El objetivo principal de este estudio fue examinar la protección de datos personales en el contexto de las relaciones contractuales entre las Instituciones Prestadoras de Salud (IPS) y las Entidades Promotoras de Salud (EPS) en Colombia. En este contexto, se realizó de las leyes vigentes las restricciones legales que conlleva el manejo de datos de pacientes. que vienen con el manejo de datos de pacientes se realizó. Posteriormente se formularon recomendaciones para mejorar la privacidad, confidencialidad y seguridad de esos datos. El estudio se centró en el análisis de leyes fundamentales, como la Ley 1581 de 2012, la jurisprudencia de la Corte Constitucional y las contribuciones de la doctrina especializada. Este análisis se complementó con una revisión de la eficacia de las medidas de seguridad actualmente implementadas en el sector salud.

Los hallazgos respaldan la hipótesis principal, que afirma que, a pesar del marco jurídico general de Colombia que reconoce la protección de datos personales como un derecho fundamental y clasifica la información médica como dato sensible, esta protección resulta insuficiente en el contexto específico de las relaciones contractuales entre Entidades Prestadoras de Salud (EPS) e Instituciones Prestadoras de Salud (IPS). Esta insuficiencia se debe principalmente a la falta de directrices normativas específicas y coherentes que se puedan aplicar a estas relaciones, así como a la falta de prácticas estandarizadas, consistentes y protocolizadas para la gestión de datos médicos sensibles.

Los principales problemas identificados son: la falta de protocolos específicos y uniformes para la gestión de la información; la necesidad de definir y aclarar con precisión las obligaciones contractuales; la falta de atención a las solicitudes y derechos de los titulares de los datos; y la inconsistencia en las prácticas contractuales entre las partes implicadas. Estas preocupaciones no son solo técnicas o administrativas; afectan directamente los derechos fundamentales de los pacientes, poniendo en riesgo su privacidad, su salud, su dignidad y su confianza en el sistema de salud. En vista de esto, el estudio sugiere que los protocolos contractuales deberían ser para regular el manejo de datos personales en las

relaciones entre las EPS e IPS. Renaciendo, estas situaciones pueden hacer que la privacidad sea más riesgosa si no se toman las medidas preventivas adecuadas.

Se propuso la implementación de mecanismos eficaces para asegurar el ejercicio completo y puntual de los derechos de los titulares, tales como la consulta, corrección, actualización o eliminación de su información personal. Es necesario que todos los organismos involucrados trabajen en conjunto para llevar a cabo estos protocolos, así como las autoridades competentes, como la Superintendencia de Industria y Comercio y la Superintendencia Nacional de Salud, estén pendientes de la situación. Y así, garantizar una gestión rigurosa, legítima y responsable que respeta los derechos fundamentales, la dignidad humana y la confianza de los pacientes en el sistema de salud de Colombia, incluyendo la protección de datos como un elemento transversal y esencial en las relaciones contractuales para su adecuada transformación.

REFERENCIAS

1. Andrés Fernández de Castro. (2024). Privacidad de pacientes: pilar fundamental de los servicios médicos. Ámbito Jurídico. https://www.ambitojuridico.com/noticias/litigios-con-gp/constitucional-y-derechos-humanos/privacidad-de-pacientes-pilar
2. Comité de Derechos Económicos, Sociales y Culturales. (2000). Observación General 14 (2000). El derecho al disfrute del más alto nivel posible de salud (artículo 12 del Pacto Internacional de Derechos Económicos, Sociales y Culturales). E/C.12/2000/4. https://www.refworld.org/es/leg/coment/cescr/2000/es/36991
3. Congreso de la República de Colombia. (1971). Código de Comercio. Decreto 410 de 1971. Diario Oficial No. 33.339 de 16 de junio de 1971. http://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio.html
4. Congreso de la República de Colombia. (1993). Ley 100 de 1993. Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones. Diario Oficial No. 41.148 de 23 de diciembre de 1993. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5248
5. Congreso 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. Diario Oficial No. 47.595. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488
6. Congreso de la República de Colombia. (2011). Ley 1438 de 2011. Por medio de la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones. Diario Oficial No. 47.957 de 19 de enero de 2011. http://www.secretariasenado.gov.co/senado/basedoc/ley_1438_2011.html
7. Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por medio de la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587 de 17 de octubre de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
8. Congreso de la República de Colombia. (2015). Ley 1751 de 2015. Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones. Diario Oficial No. 49.427 de 16 de febrero de 2015. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60733
9. Congreso de la República de Colombia. (2020). Ley 2015 de 2020. Por medio de la cual se crea y reglamenta el Sistema de Información para la Vigilancia de la Salud Pública - Sivigila y se dictan otras disposiciones. Diario Oficial No. 51.188 de 6 de enero de 2020. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=105472
10. Constitución Política de Colombia [Const. P.]. (1991). Art. 15. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html
11. Corte Constitucional de Colombia. (1992, junio 16). Sentencia T-414 de 1992 [M.P. Ciro Angarita Barón]. http://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

12. Corte Constitucional de Colombia. (1995). Sentencia SU-082 de 1995 [M.P. Jorge Arango Mejía]. https://www.corteconstitucional.gov.co/relatoria/1995/su-082-95.htm
13. Corte Constitucional de Colombia. (1997). Sentencia SU-480 de 1997 [M.P. Alejandro Martínez Caballero]. https://www.corteconstitucional.gov.co/relatoria/1997/su-480-97.htm
14. Corte Constitucional de Colombia. (1998). Sentencia T-578 de 1998 [M.P. José Gregorio Hernández Galindo]. https://www.corteconstitucional.gov.co/relatoria/1998/T-578-98.htm
15. Corte Constitucional de Colombia. (2003). Sentencia T-227 de 2003 [M.P. Eduardo Montealegre Lynett]. https://www.corteconstitucional.gov.co/relatoria/2003/t-227-03.htm
16. Corte Constitucional de Colombia. (2007). Sentencia C-1041 de 2007 [M.P. Manuel José Cepeda Espinosa]. https://www.corteconstitucional.gov.co/relatoria/2007/c-1041-07.htm
17. Corte Constitucional de Colombia. (2008). Sentencia C-1011 de 2008 [M.P. Jaime Córdoba Triviño]. https://www.corteconstitucional.gov.co/relatoria/2008/c-1011-08.htm
18. Corte Constitucional de Colombia. (2008). Sentencia T-760 de 2008 [M.P. Manuel José Cepeda Espinosa]. https://www.corteconstitucional.gov.co/relatoria/2008/t-760-08.htm
19. Corte Constitucional de Colombia. (2011). Sentencia C-748 de 2011. [M.P. Jorge Ignacio Pretelt Chaljub]. https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm
20. Corte Constitucional de Colombia. (2022). Sentencia C-055 de 2022 [M.P. Alberto Rojas Ríos, Antonio José Lizarazo Ocampo]. https://www.corteconstitucional.gov.co/relatoria/2022/c-055-22.htm
21. Corte Constitucional de Colombia. (2022). Sentencia T-143-22 [M.P. Alejandro Linares Cantillo]. https://www.corteconstitucional.gov.co/relatoria/2022/t-143-22.htm
22. Corte Constitucional de Colombia. (2023). Sentencia T-398 de 2023 [M.P. Alejandro Linares Cantillo]. https://www.corteconstitucional.gov.co/relatoria/2023/t-398-23.htm
23. Corte Constitucional de Colombia. (2023). Sentencia T-456 de 2023 [M.P. Alejandro Linares Cantillo]. https://www.corteconstitucional.gov.co/relatoria/2023/t-456-23.htm
24. Corte Constitucional de Colombia. (2024). Sentencia T-351-24 [M.P. Diana Constanza Fajardo Rivera]. https://www.corteconstitucional.gov.co/relatoria/2024/t-351-24.htm
25. Corte Constitucional de Colombia. (2024). Sentencia T-402-24 [M.P. José Fernando Reyes Cuartas]. https://www.corteconstitucional.gov.co/relatoria/2024/t-402-24.htm
26. Departamento Nacional de Planeación. (s.f.). Normativa protección de datos personales. https://colaboracion.dnp.gov.co/CDT/Programa%20Nacional%20del%20Se

rvicio%20al%20Ciudadano/NORMATIVA%20PROTECCI%C3%93N%20DE%20DATOS%20PERSONALES.pdf

27. EPS S.O.S. (2023). Política de tratamiento de datos personales. https://www.sos.com.co/wp-content/uploads/2024/01/POLITICA-DE-TRATAMIENTO-DE-DATOS-PERSONALES-1.docx-1.pdf

28. Hernández, A. (2018). Protección de datos personales en el sector privado de la salud. Revista de Derecho y Salud, 15(1), 83–100. https://www.researchgate.net/publication/340009179_Proteccion_de_datos_personales_en_el_sector_privado_de_la_salud

29. Hidalgo, A. (2016). Protección de datos de carácter personal relativos a la salud del paciente: Fundamentos, protección a la intimidad y comentarios al nuevo reglamento UE 2016/679. Madrid: Ediciones Jurídicas. https://revistas.uned.es/index.php/RDUNED/article/view/18462/15501

30. Huerta, P. (2017). La génesis del derecho fundamental a la protección de datos personales [Tesis doctoral, Universidad Complutense de Madrid]. https://docta.ucm.es/entities/publication/2564d350-dbc9-41c7-b8ec-9f8a47405160

31. Instituto Nacional de Salud. (s.f.). Protección de datos personales. https://www.ins.gov.co/Noticias/Paginas/proteccion-de-datos-personales.aspx

32. INTERCONSULTAS S.A.S. (s.f.). Política general de tratamiento de datos personales. https://www.ipsinterconsultas.com/doc/politicaprivacidad.pdf

33. MEGASALUD IPS SAS. (s.f.). Manual de tratamiento para la protección de datos personales. https://www.megasaludips.com/assets/pdf/manual-tratamiento-de-datos.pdf

34. Ministerio de Salud y Protección Social. (s.f.). Flujos de información entre EPS e IPS. https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/OT/Catalogo-flujos-informacion.zip?ID=15821

35. Ministerio de Salud y Protección Social. (s.f.). Política de privacidad y protección de datos del MSPS. https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/OT/asis04-politica-privacidad-proteccion-datos-msps.pdf

36. Ministerio de Comercio, Industria y Turismo & Superintendencia de Industria y Comercio. (2020). Resolución número 77049 de 2020. Radicación 18-179365. Ratificación de multa a EPS Sanitas por vulneración de datos personales. https://www.sic.gov.co/slider/superindustria-ratifica-multa-eps-sanitas-por-violar-la-ley-de-datos-personales

37. Ministerio de Salud. (1999). Resolución 1995 de 1999. Por la cual se establecen normas para el manejo de la Historia Clínica. https://www.minsalud.gov.co/normatividad_nuevo/resoluci%C3%93n%201995%20de%201999.pdf

38. Ministerio de Salud y Protección Social. (2019). Resolución 3100 de 2019. Por la cual se definen los procedimientos y condiciones de inscripción de los Prestadores de Servicios de Salud y de habilitación de servicios de salud y se adopta el Manual de Inscripción de Prestadores y Habilitación de Servicios de Salud.

https://www.minsalud.gov.co/normatividad_nuevo/resoluci%C3%B3n%20no.%203100%20de%202019.pdf

39. Ministerio de Salud y Protección Social. (2022). Resolución No. 1409 de 2022. https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%201409%20de%202022.pdf

40. Ponemon Institute. (2024). Cost of a Data Breach Report 2024. https://www.ponemon.org/research/cost-of-a-data-breach

41. Presidencia de la República de Colombia. (2014). Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

42. Presidencia de la República de Colombia. (2015). Decreto 1074 de 2015. Por el cual se expide el Decreto Único Reglamentario del Sector Salud y Protección Social. Diario Oficial No. 49.671. http://www.secretariasenado.gov.co/senado/basedoc/decreto_1074_2015.html

43. Presidente 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 de 27 de junio de 2013. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

44. Protección de datos personales en el sector salud. (2022). Protección de datos personales en el sector salud. PROTECDATACOLOMBIA. https://biblioteca.protecdatacolombia.com/wp-content/uploads/2022/03/CONCEPTO-SECTOR-SALUD.pdf

45. PROTECDATACOLOMBIA. (2022). Protección de datos personales en el sector salud. https://biblioteca.protecdatacolombia.com/wp-content/uploads/2022/03/CONCEPTO-SECTOR-SALUD.pdf

46. Serrano, M. (2018). La necesidad de una ley de protección de datos en salud. Bioderecho, (8), 12–30. https://revistas.um.es/bioderecho/article/view/389951/269041

47. Serrano, M. (2020). El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del reglamento general de protección de datos y de la ley de protección de datos personales y garantía de los derechos digitales. Madrid: Editorial Jurídica. https://revista-estudios.revistas.deusto.es/article/view/1952/2397

48. SIES Salud S.A.S. (2023). Política de tratamiento de datos personales de Sies Salud SAS. https://siessalud.com/wp-content/uploads/2023/09/Politica-de-Tratamiento-de-Datos-Personales.pdf

49. Superintendencia de Industria y Comercio. (2015). Circular Externa 02 de 2015. Lineamientos para el tratamiento de datos sensibles, especialmente en el ámbito de la salud. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Circular/30035620

50. Superintendencia de Industria y Comercio. (s.f.). Sobre la protección de datos personales. https://www.sic.gov.co/content/sobre-la-protecci%C3%B3n-de-datos-personales

51. Superintendencia de Sociedades. (2023). Manual interno de políticas y procedimientos para el tratamiento de datos personales. https://www.supersociedades.gov.co/documents/107391/3463418/GC-M-003_ManualTratamientoDatosPersonales.pdf

52. Superintendencia Nacional de Salud. (2014). Resolución 1650 de 2014. Por la cual se desarrolla el procedimiento administrativo sancionatorio aplicable por la Superintendencia Nacional de Salud. https://normograma.adres.gov.co/compilacion/docs/resolucion_supersalud_1650_2014.htm

53. Superintendencia Nacional de Salud. (2023). Anexo Resolución 2023700000003372-6 de 2023: Política sancionatoria. https://docs.supersalud.gov.co/PortalWeb/Juridica/Resoluciones/Anexo%20resoluci%C3%B3n%202023700000003372-6%20de%202023.pdf

54. Superintendencia Nacional de Salud. (2023). Concepto 0935661 de 2023. https://minsalud.gov.co/Normatividad_Nuevo/Concepto%20Jur%C3%ADdico%20%202024116000933561%20de%202024.pdf

55. Universidad Externado de Colombia. (2021). Presente y futuro de la protección de datos personales y big data en el sector de la salud. https://www.uexternado.edu.co/derecho/presente-y-futuro-de-la-proteccion-de-datos-personales-y-big-data-en-el-sector-de-la-salud/