

**Entre la reserva y el acceso: Desafíos en la aplicación del régimen de protección de
datos en la práctica hospitalaria**

Trabajo de Grado: Sistematización de la práctica

PRESENTADO POR:

Valentina Sandoval Ospina y Julieta Villacote Sarasty

Estudiantes de Derecho

Facultad de Humanidades y Ciencias Sociales

Dpto. de Ciencia Jurídica y Política

Pontificia Universidad Javeriana Cali

DIRECTOR:

Luis Félix Barriga Palomino



Santiago De Cali, 09 de junio de 2026

RESUMEN

La presente sistematización de prácticas, con enfoque en el área de la salud, pretende analizar las tensiones jurídicas y operativas existentes respecto a la protección de los datos sensibles, de manera más específica en el deber de reserva de la historia clínica y el derecho al acceso a la información sensible y privada que se maneja en una Institución Prestadora de Salud (IPS) de Nivel IV. El trabajo está fundamentado en la práctica profesional realizada en el área jurídica de dicha institución, por ende, el análisis se basará en la gestión de Derecho de Petición y en la proyección de respuestas a Acciones de Tutela, se implementó un enfoque cualitativo y socio-jurídico, dado que, se investiga como la autonomía del paciente y su autodeterminación informativa se materializan dentro del área de la salud. Uno de los mayores retos que se pretende evaluar es la validación de la legitimación en la causa ante terceros y sus familiares, la protección al derecho de la intimidad en los pacientes fallecidos o personas en condición de discapacidad, y los retos que trae consigo la transformación digital en la nueva era tecnológica bajo el marco de la Historia Clínica Electrónica interoperable regulada por la Ley 2015 de 2020 y la Resolución 1888 de 2025.

El estudio finaliza con la construcción de un modelo denominado “hospitalidad informativa” el cual tiene como objetivo la búsqueda del equilibrio respecto al rigor estipulado por el Habeas Data junto con la humanización del servicio, buscando de esta manera garantizar que los datos clínicos sean tratados como un atributo esencial de la dignidad humana de los pacientes y no solo como un objeto de insumo administrativo para la gestión institucional.

Palabras clave: Habeas Data, Historia Clínica, Datos Sensibles, Interoperabilidad, Dignidad Humana, tecnología, Salud.

ÍNDICE

1. Introducción	4
2. Capítulo I. Régimen Estatutario de Protección de Datos en Salud.....	8
1.1. El derecho fundamental al Habeas Data en el ordenamiento jurídico colombiano	10
1.2. Concepto y alcance de los datos personales sensibles en el sector salud.....	12
1.3. Marco legal.....	14
1.4. Principios rectores del tratamiento de datos personales.....	16
1.5. Obligaciones de las IPS como responsables del tratamiento.....	17
1.6. La Historia Clínica como documento reservado y dato sensible.....	20
3. Capítulo II. Desafíos operativos y barreras percibidas	22
2.1. La legitimación en la causa como punto de inflexión	22
2.2. Conflictos entre la celeridad asistencial y la protección de datos personales.....	25
2.3. Identificación de “barreras de acceso” desde la percepción del usuario	28
2.4. Riesgos de la gestión: entre la sanción de la sic y la vulneración del paciente.....	30
4. Capítulo III. Sistematización de la experiencia en la IPS.....	32

3.1. El entorno de la práctica: gestión de la intimidad en una IPS de alta complejidad.....	32
3.2. La aplicación del filtro de legitimación: entre el deber ser y la percepción del usuario.....	35
3.3. Nudos críticos en la gestión de casos sensibles: fallecidos e incapaces.....	37
3.4. Reflexiones finales: la humanización del dato como estrategia de excelencia.....	39
5. Capítulo IV: Conclusiones	41
6. Bibliografía	44

INTRODUCCIÓN

Una Institución Prestadora de Salud (IPS) diariamente se enfrenta a diversos desafíos materiales y jurídicos, los cuales deben resolverse bajo unos altos estándares de calidad, por lo cual, en este entorno, la gestión de los datos personales sobrepasa el simple cumplimiento administrativo para ser un factor determinante de la seguridad del paciente.

La presencia de servicios como oncología, imágenes diagnósticas avanzadas y trasplantes en el ámbito de la medicina crítica exige un flujo continuo y preciso de información. Sin embargo, esta exigencia de estar disponible inmediatamente suele entrar en conflicto con la estricta normativa de protección de datos personales que dicta la Ley 1581 del año 2012, debido a la gran cantidad diaria de pacientes y solicitudes. En otras palabras, esto exige que la clínica disponga de una infraestructura legal robusta, capaz de garantizar la confidencialidad sin poner en riesgo el momento oportuno en el cuidado asistencial.

La gestión diaria de una empresa privada en el ámbito de la salud evidencia que la protección de datos no es un término inalterable, sino una administración de tensiones constantes entre derechos fundamentales. Pese a que el sistema de Hábeas Data impone límites de seguridad indispensables para proteger la privacidad, las normativas sanitarias necesitan fluidez para garantizar la vida. Esta dualidad convierte el ejercicio del derecho en un procedimiento técnico de valoración

Por lo tanto, para comprender los desafíos concretos que han sido detectados en el tratamiento de tutelas y PQR, es fundamental analizar el marco jurídico que apoya dicha relación. Esto significa que se debe examinar cómo las obligaciones de reserva chocan con los mandatos de acceso y eficacia dentro del sistema de salud en Colombia.

PLANTEAMIENTO DEL PROBLEMA JURÍDICO

Para proteger el derecho fundamental de los pacientes a recibir una atención digna, oportuna y de calidad en una organización privada del sector salud, frente a obstáculos como la negativa a otorgar citas, medicamentos o tratamientos, mediante la administración de Peticiones, Quejas y Reclamos (PQR), esta gestión se enfoca en validar que el paciente tenga legitimidad para acceder a su información clínica. Su propósito es brindar una respuesta rápida y con información exacta, para así poder ofrecer al usuario una solución efectiva y clara a su solicitud.

Este procedimiento no es solo formal, sino que supone de un análisis ponderado para prevenir la violación del derecho a la intimidad en respuesta a las peticiones de terceros o familiares. El trabajo consiste en valorar si los poderes de representación son suficientes y si las excepciones legales a la reserva son aplicables, garantizando que la transmisión de historias clínicas o resultados paraclínicos respete los principios de finalidad y circulación restringida. De esta manera, se disminuyen los peligros de sanción por parte de la Superintendencia de Industria y Comercio (SIC).

Por otra parte, cuando el paciente siente que sus derechos fundamentales están siendo violados, la acción de tutela es el principal mecanismo legal que utiliza. Una organización del sector privado de la salud recibe cada día una gran cantidad de estos recursos. Por esta razón, el propósito del área jurídica es ofrecer una respuesta técnica y oportuna que esté en línea con lo que el paciente solicita, evaluando siempre la viabilidad asistencial y legal de proveer el servicio requerido.

En la actualidad, implementar herramientas tecnológicas para el manejo de documentos representa un desafío más: garantizar que la privacidad por diseño no se vea comprometida

por la innovación, asegurando que cumplir con el régimen de protección de datos en la IPS sea un hecho tangible y no solo una formalidad administrativa.

Sin embargo, para poder ofrecer una respuesta honesta y clara a las solicitudes de asistencia y jurídicas, la circulación de información y datos personales de los usuarios se mantiene en un flujo continuo por medio de los distintos servicios administrativos y clínicos. Esta dinámica transversal significa que la información sensible no está contenida en un compartimento estanco, sino que se mueve desde la admisión hasta el alta médica, yendo por laboratorios, áreas de apoyo y especialistas.

La movilidad constante de la información hace que sea aún más necesario un control de accesos estricto, en el que la trazabilidad del dato sea el único medio capaz de equilibrar la rapidez que requiere la prestación del servicio sanitario con la obligación de reserva establecida por las leyes colombianas.

Teniendo en cuenta la gestión interna de la institución con respecto a las soluciones ofrecidas a los usuarios por medio del departamento jurídico, es apropiado plantear la siguiente pregunta: ¿Es el cumplimiento del régimen de protección de datos en una IPS una garantía efectiva y tangible, o se ha convertido solo en un conjunto de exigencias formales que dificultan la obtención de información y la prestación puntual del servicio?

Dicha respuesta requiere un análisis que lleve a analizar cómo las regulaciones colombianas, tales como lo son la **Ley 1581 de 2012** (Régimen General de Protección de Datos Personales), la **Ley Estatutaria 1751 de 2015** (Derecho Fundamental a la Salud) y la **Ley 2015 de 2020** (Historia Clínica Electrónica Interoperable), junto con la **Resolución 1995 de 1999**, se materializan en el día a día de una institución de alta complejidad.

OBJETIVO GENERAL

Se pretende identificar cuál es el régimen aplicable del tratamiento de datos personales en las Instituciones Prestadoras de Salud (IPS), desde la normativa general de protección de datos personales, hasta la legislación específica de la materia, señalando los retos y dificultades que estas instituciones presentan a la hora de la aplicación de las mismas frente a la atención de los pacientes usuarios.

OBJETIVOS ESPECÍFICOS

- I. Analizar la normatividad propia de la protección de datos personales en el sector de la salud, incluyendo los principios de legalidad, finalidad y responsabilidad demostrada.
- II. Evidenciar los asuntos relacionados con la protección de datos personales dentro de las Instituciones Prestadoras de Salud (IPS), señalando los retos y dificultades frente a la entrega de información de los pacientes usuarios de las mismas, y cómo los pacientes, familiares y/o terceros pueden considerar qué se están instalando barreras para el acceso de la información.
- III. Relacionar la normatividad con la experiencia laboral en una organización privada del sector de la salud, identificando los retos y dificultades en la aplicación y materialización de la misma.

METODOLOGÍA

El presente escrito se realizará mediante un enfoque cualitativo con metodología de sistematización de experiencias, el cual se encontrará orientado en reconstruir, interpretar y analizar las situaciones observadas durante el tiempo de práctica en la gestión de peticiones, quejas y reclamos (PQR), Derecho de Petición y tutelas dentro del área jurídica de una Institución Prestadora de Salud (IPS) de nivel IV. Se basa en un estudio jurídico-analítico que

evidencia las decisiones institucionales con el régimen aplicable de protección de datos personales, el derecho fundamental a la salud y el marco de IHCE, así como con la jurisprudencia constitucional en materia de intimidad, habeas data y reserva.

CAPÍTULO I. RÉGIMEN ESTATUTARIO DE PROTECCIÓN DE DATOS EN SALUD: MARCO NORMATIVO, PRINCIPIOS Y DESAFÍOS DE LA GESTIÓN DE INFORMACIÓN EN IPS.

En las instituciones de salud la información no es solamente un recurso operativo, sino también una marca digital de la dignidad humana, por lo tanto, estas instituciones tienen el reto de lograr un equilibrio entre el acceso legítimo a la información por parte del paciente, sus familiares o terceros, y la protección de la privacidad de la información del paciente, esto es lo que se evidencia en el título del presente documento “entre la reserva y el acceso”. Asimismo, la **sentencia SU-355 de 2022** indica que el derecho a la intimidad significa tener el control sobre la información personal, por lo mismo, existe un límite legal al manejo de la información por parte de terceros en lo que se refiere a la reserva hospitalaria.

El literal c) del artículo 3 de la **Ley 1581 de 2012** define el dato personal como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. En la práctica clínica un dato aislado puede no identificar a una persona, no obstante, la identificabilidad surge del entrecruzamiento de rasgos que permiten individualizar al sujeto, es decir que toda información que permita rastrear la identidad del paciente debe someterse al régimen de protección de datos.

Por ende, existe una clasificación que gradúa niveles de acceso y reserva de los datos:

- I. **DATO PÚBLICO:** Es la información no semiprivada ni privada, los cuales pueden ser tratados sin autorización previa del titular según el artículo 10 de la **Ley 1581 de 2012**, tales como el estado civil, registros públicos, entre otros.

- II. **DATO SEMIPRIVADO:** Es aquel que no es íntimo, reservado, ni público, y el cual le puede interesar tanto al titular como a un sector específico; en salud, incluye datos de afiliación requeridos por las EPS para auditoría, bajo flujo regulado.
- III. **DATO PRIVADO:** Se trata de información íntima relevante sólo para el titular y en dado caso para su entorno cercano.
- IV. **DATO SENSIBLE:** Definido en el artículo 5 de la ley mencionada anteriormente, donde se indica que es aquel que afecta la intimidad o cuyo uso indebido puede generar discriminación, incluyendo datos de salud, vida sexual y biométricos.

La forma en la que se manejan los datos sensibles es el núcleo del conflicto que nos compete en este escrito.

Por otro lado, debemos tener presente que la Corte Constitucional ha manifestado que se admite la entrega de los datos sensibles de una persona incapacitada o fallecida a sus familiares o terceros, siempre y cuando se cumplan con los requisitos necesarios, como por ejemplo, la certificación del parentesco, una carta de autorización, entre otros. La institución debe evaluar la situación y decidir sobre la pertinencia de la entrega de la información, esto teniendo en cuenta que la incapacidad del titular para acceder a la misma, no significa que la misma se vuelva de carácter público y se extinga automáticamente la reserva del dato médico, pues aún se continúa protegiendo la intimidad familiar.

En conclusión, el ordenamiento colombiano ha logrado un equilibrio en el que la reserva y el acceso a la información no se excluyen, sino que se articulan de manera armónica, sin embargo, el desafío para la institución consiste en asegurar que el uso de la información, indispensable para la atención médica y la gestión administrativa, se realice con pleno respeto

por la autonomía y la libertad del paciente, de modo que ninguna actuación comprometa la intimidad del mismo y su entorno.

1.1. EL DERECHO FUNDAMENTAL AL HABEAS DATA EN EL ORDENAMIENTO JURÍDICO COLOMBIANO

El artículo 15 de la **Constitución Política de Colombia** contiene tres derechos fundamentales que protegen la esencia del ser humano, estos son: derecho a su intimidad personal y familiar, a su buen nombre y al habeas data. Estos derechos son compatibles, debido a que se encuentran totalmente relacionados con la dignidad humana, la cual actúa como base que coloca a la persona como el propósito final de toda actuación estatal y privada, garantizando de esta manera su libre desarrollo de la personalidad; por lo tanto, se procede a realizar un pequeño contexto de los derechos mencionados anteriormente:

En primera instancia, tenemos el derecho a la Intimidad Personal y Familiar, el cual se basa en la existencia de un núcleo íntimo que debe permanecer libre de la intervención del Estado o de intervenciones injustificadas de la sociedad. Este derecho permite que una persona mantenga su vida personal, espiritual y cultural sin intervenciones sin fundamento, tal como lo ha señalado la Corte Constitucional en la **Sentencia C-913 de 2010**. En el ámbito clínico, este núcleo se traduce en el deber de confidencialidad; sin embargo, es importante anotar que este derecho no es absoluto, pues se permite el acceso ante imperativos de seguridad nacional, salud pública o administración de justicia, siempre que se cuente con los documentos que motiven la solicitud de los mismos.

En igual sentido, el derecho al **buen nombre** protege la reputación y la percepción pública de la persona frente a la sociedad. Su relevancia es tal que la formulación de acusaciones deshonrosas constituye el delito de injuria, previsto en el artículo 220 de la **Ley 599 de 2000**. En el ámbito de la gestión de datos personales, un manejo inadecuado de la información puede

dar lugar a actuaciones de hecho que afecten la honra y el patrimonio del titular. Por esta razón, el examen de responsabilidad en las instituciones de salud debe comprender las esferas civil, administrativa y sancionatoria, en la medida en que un dato incorrecto puede alterar gravemente la estabilidad social y personal del paciente.

Por otro lado, se encuentra el **Hábeas Data** como derecho fundamental autónomo, el cual, con el paso del tiempo la Corte Constitucional dejó claro que este derecho, el cual se encuentra regulado en el segundo inciso del artículo 15 de la **Constitución Política de Colombia**, no es una simple garantía accesorio, sino que se trata de un derecho fundamental autónomo de cada individuo, el cual le otorga a toda persona tres facultades principales frente a su información personal: conocer (Solicitar y obtener información sobre los datos personales), actualizar (Facultad que dispone para la información cuando sea incompleta o desactualizada) y rectificar (Solicitar la corrección de la información cuando sea errónea o inexacta)

De igual forma, se ha indicado en varias ocasiones que este derecho no se limita únicamente a corregir errores, sino que también permite agregar información que sea necesaria para verificar la situación real del titular de la misma, especialmente en contextos financieros o crediticios.

En el área de la salud, esto significa que el paciente no es un simple “espectador” de su historia clínica, por el contrario, tiene el derecho de asegurarse de que cada registro que se realice sea veraz, completo y actualizado, manteniendo así el control sobre su propia información médica.

Finalmente, como consecuencia natural del habeas data aparece el llamado **Derecho al Olvido**, que impone una obligación clara a quien administra bases de datos. De acuerdo con la Corte Constitucional, la información negativa o aquella que ya perdió la finalidad para la cual fue recolectada no puede mantenerse de forma indefinida. Cuando el titular lo solicita y se cumplen los requisitos legales, el responsable debe eliminar los datos y cualquier registro que permita seguir vinculando a la persona con esa información.

Visto desde una perspectiva más humana, este conjunto de derechos parte de una idea sencilla: los datos personales hacen parte de la dignidad de la persona. La protección de esa información no es un privilegio, sino algo que corresponde a todo individuo por el hecho de existir. En el entorno hospitalario, esto se traduce en entender que la relación médico-paciente es un espacio de confianza y diálogo. Por eso, manejar la información con claridad y responsabilidad no es sólo una exigencia legal, sino la manera de proteger la autonomía del paciente frente al poder informático que hoy tienen las instituciones.

1.2. CONCEPTO Y ALCANCE DE LOS DATOS PERSONALES SENSIBLES EN EL SECTOR SALUD

En concordancia con lo anterior, la **Ley 1581 de 2012** en artículo 5 define que los datos sensibles son aquellos que repercuten en la intimidad del titular. Ahora bien, dentro del tema que nos compete, cuando se trata de una institución de alta complejidad, su definición adquiere una dimensión crítica, toda vez que, como lo hemos venido planteando, la información que se tiene en juego no solo revela los estados de salud sino que puede poner en velo la dignidad, la autonomía y la integridad futura de los pacientes.

Para esta investigación, es importante la categorización de los tipos de datos sensibles que se pueden presentar, después de analizar el alcance que una organización privada del sector de la salud tiene respecto a la información personal de los usuarios que recibe día a día, encontramos tres aspectos multidimensionales los cuales es pertinente identificar: Primero tenemos los datos biométricos y genéticos (huellas, iris, ADN), estos gozan de una protección reforzada teniendo en cuenta su carácter inmutable, como segundo eje contamos con la información clínica y paraclínica, dentro de esta categoría nos referimos a registro en la historia clínica, ya sean diagnósticos, información respecto a la evolución, resultados, imágenes diagnósticas y reportes de laboratorio, por último están los datos de especial vulnerabilidad, se

denomina así a toda información que se relacione con la vida sexual, orientación e identidad de género o condiciones de salud estigmatizadas, donde la reserva es la barrera frente a la exclusión social.

Como podemos evidenciar, al tener la necesidad de categorizar los tipos de datos sensibles que se presentan, podemos decir que, el alcance de estos datos en la práctica hospitalaria no es estático y requiere de mayor atención por parte de los trabajadores de la institución; si bien es cierto, los datos personales siempre han sido un tema a tratar y por lo tanto la busca de regulaciones está en constante cambio, con la implementación de tecnologías de análisis y gestión de datos, surge el concepto de "dato inferido", es decir, al contar con una información parcial de un paciente, existe la capacidad de utilizar la información de que disponemos para aplicarla o procesarla con la posibilidad de emplearla de una manera nueva o diferente.

Esto significa que información que parece técnica o administrativa, se puede convertir en una herramienta permite deducir el estado de salud real del titular y como consecuencia de esto, se pone en juego todos los datos sin excepción alguna de los usuarios, dado que esta información no solo pasa por manos de una sola persona sino que, varios servicios dentro de la institución la tienen en su poder, por lo tanto, el alcance que se defiende en este capítulo sostiene que todo dato tratado en el entorno clínico que permita reconstruir la esfera íntima del paciente debe ser blindado bajo el régimen de protección reforzada, independientemente de si se encuentra en un soporte físico o digital.

Por lo anterior, es por lo tanto pertinente hablar sobre las limitaciones al tratamiento de los datos personales y las excepciones que la ley nos plantea, bajo la premisa del Artículo 6 de la **Ley 1581 de 2012**, el tratamiento de estos datos está proscrito, salvo excepciones taxativas.

Tratándose de temas con fines de salud, el alcance de esta prohibición se flexibiliza bajo dos escenarios operativos fundamentales en una organización privada del sector de la salud:

- I. **URGENCIA VITAL:** Considerando los escenarios de urgencia vital donde la vida de una persona puede estar en riesgo dentro de la institución, el manejo de los datos personales adquiere un carácter primordial. En estos casos, la gestión de la información debe priorizar la salvaguarda del interés vital del afectado, permitiendo un tratamiento excepcional de los datos para garantizar una intervención médica oportuna y efectiva.
- II. **FINALIDADES MÉDICAS:** El uso del tratamiento necesario para la prevención, diagnóstico médico o gestión de servicios de salud, siempre que sea realizado por profesionales sujetos al secreto profesional.

En conclusión, el alcance de los datos personales sensibles en el ámbito hospitalario trasciende la simple recopilación de información médica; se configura como la custodia de la biografía íntima del sujeto.

En una institución de alta complejidad, la interconexión de datos clínicos, genéticos y biométricos crea un perfil de vulnerabilidad que exige una protección reforzada, no solo desde la óptica legal de la **Ley 1581 de 2012**, sino desde la ética médica y la seguridad digital.

1.3. MARCO LEGAL

La gestión de datos en una organización privada del sector de la salud se encuentra estructurada bajo una jerarquía normativa que integra derechos fundamentales, leyes estatutarias y disposiciones técnicas de obligatorio cumplimiento. Es este marco jurídico el que delimita el alcance de la reserva de la información y el derecho de acceso a la misma.

- I. **Ley 1581 de 2012:** El eje central del tratamiento de datos es la **Ley 1581 de 2012**, la cual dicta las disposiciones generales para la protección de datos personales en Colombia. Esta norma establece que cualquier tratamiento de información debe contar

con la autorización previa, expresa e informada del titular, salvo excepciones específicas como la urgencia médica o sanitaria.

- II. **Ley 1751 de 2015:** Esta Ley regula el derecho fundamental a la salud, en su artículo 10, esta ley consagra el derecho del paciente a que su historia clínica sea tratada de manera confidencial y reservada, y a recibir información clara sobre su estado de salud, esto evidencia la primera gran tensión legal: mientras la Ley protección de datos personales protege el flujo de datos bajo principios de libertad, la Ley que regula el derecho fundamental a la salud impone una muralla de confidencialidad que solo puede ser levantada bajo parámetros estrictos.
- III. **Resolución 1995 de 1999:** Es la norma principal que establece los criterios para la organización, manejo y conservación de la historia clínica, está la define como un documento privado, obligatorio y sometido a reserva, al cual solo pueden acceder el usuario, el equipo de salud, las autoridades judiciales y las personas autorizadas por ley. La **Resolución 839 de 2017** modifica la anterior mencionada en cuanto a los tiempos de retención, establece que la historia clínica debe conservarse por un periodo mínimo de 15 años (5 años en el archivo de gestión y 10 años en el archivo central), tras los cuales se puede proceder a su disposición final o eliminación segura, siempre que no tenga valor histórico o científico.
- IV. **Ley 2015 de 2020:** Introduce la Historia Clínica Electrónica Interoperable, un gran avance el cual facilita el intercambio de datos clínicos relevantes entre prestadores para garantizar la continuidad asistencial, bajo los más altos niveles de seguridad y confidencialidad.
- V. **Estándares Internacionales y Éticos:** Una organización privada del sector de la salud, al ser parte de un grupo prestigioso, integra estándares internacionales como los de la **Joint Commission International (JCI)**. Estos estándares exigen que la institución demuestre, mediante el principio de **Responsabilidad Demostrada (Accountability)**,

que cuenta con medidas técnicas y administrativas para evitar el acceso no autorizado a los datos sensibles.

Esta estructura normativa no tiene únicamente como propósito evitar sanciones, sino que su finalidad última es proteger los derechos, la dignidad y la confianza del paciente en el sistema.

1.4. PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS PERSONALES

Los principios de la protección de datos, los cuales se aplicarán de manera armónica e integral, son de vital importancia para comprender este derecho y se encuentran regulados en el artículo 4 de la **Ley 1581 de 2012**:

- I. PRINCIPIO DE LEGALIDAD:** la protección de datos debe estar regulada por la ley.
- II. PRINCIPIO DE FINALIDAD:** debe responder a una finalidad legítima que debe conocer el titular y que sea conforme a la **Constitución Política de Colombia** y la ley.
- III. PRINCIPIO DE LIBERTAD:** el tratamiento únicamente puede realizarse con el consentimiento previo, expreso e informado del titular, es decir, los datos personales no podrán ser expuestos sin previa autorización, salvo ciertas excepciones.
- IV. PRINCIPIO DE VERACIDAD O CALIDAD:** La información objeto de tratamiento debe poder ser objeto de validación, es decir, debe ser exacta, íntegra, actualizada, verificable y clara.
- V. PRINCIPIO DE TRANSPARENCIA:** En el desarrollo del tratamiento debe asegurarse el derecho del titular a solicitar y obtener, en cualquier momento y sin limitaciones, información sobre la existencia de datos personales que le concierne, ya sea ante el responsable o el encargado del tratamiento.

- VI. PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA:** El tratamiento está sometido a los límites que derivan de la naturaleza de los datos personales, así como de lo dispuesto en la ley y en la **Constitución Política de Colombia**. En consecuencia, sólo podrá ser realizado por personas autorizadas por el titular o por aquellas expresamente habilitadas por la ley.
- VII. PRINCIPIO DE SEGURIDAD:** La información objeto de tratamiento por parte del responsable o del encargado deberá ser gestionada mediante la adopción de medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los registros, evitando su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- VIII. PRINCIPIO DE CONFIDENCIALIDAD:** Toda persona que intervenga en el tratamiento de datos personales que no sean públicos tiene el deber de mantener la confidencialidad de la información, incluso después de haber finalizado su vínculo con las actividades relacionadas con dicho tratamiento. Sólo podrá suministrar o comunicar datos personales cuando ello esté autorizado por la ley y dentro de los límites establecidos en ella.

1.5. OBLIGACIONES DE LAS IPS COMO RESPONSABLES DEL TRATAMIENTO

La **Ley 1581 de 2012** en su artículo 17, establece que la Institución Prestadora de Servicios de Salud (IPS) asume el rol de responsable del tratamiento, toda vez que es quien decide sobre la recolección, almacenamiento y uso de los datos personales de los pacientes.

Dentro de una organización privada del sector de la salud se logra evidenciar que, estas obligaciones adquieren una connotación de "diligencia calificada" debido a la sensibilidad de la

información gestionada, es decir, debe existir un compromiso con la investigación minuciosa de cada caso, con el fin de garantizar una información veraz.

Ahora bien, es responsabilidad de las IPS garantizar al titular, en todo momento, el pleno y efectivo ejercicio del derecho de Hábeas Data. Esto implica que la clínica debe contar con canales verificables para que el paciente o sus causahabientes puedan:

- I. Conocer su información clínica.
- II. Actualizar datos demográficos o de contacto.
- III. Rectificar información errónea (siempre bajo los protocolos de historia clínica).

En el caso en particular se evidencia que la organización privada del sector de la salud, cumple con todos estos canales, de esta forma fortalece la buena comunicación con los usuarios y garantiza en la medida de sus posibilidades entregar el mejor y oportuno servicio para cada uno de los casos.

Por otro lado, de acuerdo con el **literal (c) del artículo 17 de la ley** nombrada anteriormente, la IPS debe informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten, deben existir dos parámetros claves, la autorización expresa puesto que, al tratarse de datos sensibles, la autorización debe ser previa, expresa e informada. y el aviso de privacidad, es decir que, la clínica debe disponer de avisos de privacidad visibles y políticas de tratamiento de información (PTI) de fácil acceso, que detallen el uso que se dará a los datos.

Desde el área jurídica, se hace especial énfasis en estos dos puntos fundamentales. Es imperativo que todos los servicios de la institución tengan pleno conocimiento de que, previo a cualquier procedimiento, se debe informar y asegurar exhaustivamente al paciente sobre el tratamiento de sus datos personales y el seguimiento de sus procesos asistenciales.

Asimismo, dentro de las obligaciones se encuentra la seguridad y reserva de la información, esta es quizás la obligación más operativa en la práctica hospitalaria. Según los literales (a) y (d) del artículo 17 de la **Ley 1581 de 2012**, la IPS debe:

- I. **RESERVA:** Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data
- II. **SEGURIDAD:** Implementar las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado.

Por último, en el **Decreto 1377 de 2013** el cual se encuentra incorporado en el **Decreto Único 1074 de 2015**, nos afirma una vez que las IPS deben ser capaces de demostrar que han implementado medidas útiles y efectivas para cumplir con la ley. Esto incluye:

- I. La designación de un Oficial de Protección de Datos.
- II. La realización de auditorías internas.
- III. El Registro Nacional de Bases de Datos (RNBD) ante la Superintendencia de Industria y Comercio (SIC).

Basándonos en la jurisprudencia anterior y los parámetros legales que presenta para las IPS, la organización privada del sector de la salud por medio de la innovación ha logrado cumplir con las expectativas respecto a la protección de datos, sin embargo, se requiere un análisis que lleve a confrontar cómo las regulaciones colombianas, imponen una carga que supera el simple archivo de documentos y cómo esto puede afectar a la hora de llevar todos los procesos sin ningún margen de error.

En conclusión, la responsabilidad de una organización privada del sector de la salud como prestador de nivel IV no se agota en la atención médica, sino que se extiende a la gobernanza de la información. El incumplimiento de estas obligaciones no solo acarrea sanciones onerosas por parte de la SIC, sino que vulnera la confianza del paciente y la integridad del Sistema General de Seguridad Social en Salud. Así, el marco de obligaciones se convierte en el estándar mínimo de calidad sobre el cual se edifica la seguridad del paciente en la era digital.

1.6. LA HISTORIA CLÍNICA COMO DOCUMENTO RESERVADO Y DATO SENSIBLE

La **Resolución 1995 de 1999** nos indica que la historia clínica es un documento privado, obligatorio y sometido a reserva, el cual no es únicamente un registro médico, sino una biografía médica de un individuo, en la cual podemos llegar a conocer datos relevantes los cuales lo identifican y le dan identidad. El artículo 74 de la **Constitución Política de Colombia** indica que el secreto profesional es inviolable, por lo cual, se garantiza lo confiado a los médicos dentro de las instituciones prestadoras de salud (IPS) y que lo informado permanezca bajo reserva absoluta para proteger la dignidad del paciente.

Asimismo, la **Ley 2015 de 2020** por medio de la cual se crea la historia clínica electrónica interoperable, reforzó el hecho de que cada persona es titular de su historia clínica, mientras que las IPS actúan únicamente como responsables de la custodia, seguridad y mantener la integridad de lo contenido en él. Tener clara la distinción nombrada anteriormente es fundamental, debido a que con ello se logra entender las obligaciones de las Clínicas frente a lo relacionados con la tenencia y administración del historial clínico de los paciente, esto se rige bajo el principio de Responsabilidad Demostrada, el cual se encuentra en el **Decreto 1377 de 2013** el cual se encuentra incorporado en el **Decreto Único 1074 de 2015**, que nos indica que se debe probar que se hayan implementado las medidas técnicas y administrativas necesarias para evitar que se tenga acceso a información del paciente por personas no autorizadas. El

tratamiento de este documento debe regirse bajo los principios mencionados anteriormente, tales como finalidad, circulación restringida y seguridad.

Sin embargo, es en la aplicación de estos principios y normatividad donde surgen los conflictos con familiares y terceros, ya que, por el cuidado excesivo que se debe tener al manejo de la información, el entorno del paciente podría considerar que se está restringiendo de forma injustificada los datos solicitados. Por esta razón, la **sentencia T- 182 de 2009** señala que la reserva de la información de la historia clínica no desaparece con el fallecimiento o incapacidad del titular, dado que, solamente los familiares o terceros autorizados puede continuar accediendo a ella, por los conflictos que podrían surgir dentro del entorno del paciente, no obstante, para la entrega de esta información, debe verificarse la acreditación de quien lo solicita, para no incurrir en la vulneración de derechos por la divulgación de la misma. Las Clínicas enfrentan un gran reto como se ha mencionado en varias ocasiones dentro de este escrito, pues la reserva no debe convertirse en un muro incruzable para los que rodean al individuo, ni el acceso puede incurrir en una vulneración a los derechos, memoria y sobre todo a la dignidad del titular de la información, por lo tanto, buscar este equilibrio es lo que define la ética por medio de la cual se realiza la gestión de los datos que se encuentran dentro de la Institución en la actualidad, es decir, el reto consiste en buscar una armonía entre ambos intereses, garantizando que se realice una gestión que contribuya con la protección de los derechos sin perjudicar la autonomía y la dignidad humana.

CAPÍTULO II. DESAFÍOS OPERATIVOS Y BARRERAS PERCIBIDAS: LA Tensión ENTRE LA RESERVA LEGAL Y EL ACCESO A LA INFORMACIÓN EN LA PRÁCTICA HOSPITALARIA

2.1. LA LEGITIMACIÓN EN LA CAUSA CÓMO PUNTO DE INFLEXIÓN

La legitimación en la causa no es un simple concepto o trámite, está es realmente un primer “filtro de seguridad” de la información del paciente, es decir, es la que define quiénes son las personas realmente acreditadas para poder proporcionar la información sensible, reservada y confidencial, qué se encuentra en la Historia Clínica, este concepto es el Principio de Libertad el cual se encuentra en el artículo 4 de la **Ley 1581 de 2012**, según el cual el tratamiento de datos solo procede con el consentimiento del titular. Sin embargo, este “filtro” puede llegar a percibirse cómo una traba al acceso de la información frente a los ojos de las personas que la solicitan, esto se debe a que las Instituciones Prestadoras de Salud (IPS), deben registrarse bajo el **Decreto 1377 de 2013** el cual se encuentra incorporado en el **Decreto Único 1074 de 2015** en el cual se encuentra el principio de **Responsabilidad Demostrada**, donde se evidencia que estas instituciones están obligadas a pedir la documentación necesaria para poder verificar quién está debidamente legitimado para obtener dicha información, y quien aunque quisiera obtenerla, no puede debido a la protección de datos personales del usuario, ya que si la Institución Prestadora de Salud (IPS) proporciona la información a una persona no autorizada, está incurriendo en una divulgación de información sensible de una paciente y se enfrentaría a una falta grave según la **Ley 2015 de 2020**.

Uno de los desafío operativo más crítico surge día a día en las Instituciones Prestadoras de Salud (IPS), debido a que estas se enfrenta al reto de analizar las personas correspondientes a las cuales es posible suministrarles información del paciente y/o hacer entrega de la Historia Clínica, esto se debe a que muchos familiares y terceros realizan solicitudes para recibir

información correspondiente al estado de salud de una persona en particular, sin embargo, al momento de qué la Institución solicita una documentación que lo acredite, ya sea: copia del documento de identidad, registro civil de nacimiento, acta de matrimonio, carta de autorización, poder debidamente autenticado, entre otros, el solicitante frecuentemente expresa una barrera interpuesta por parte de la institución a la información que ellos consideran es su derecho que le sea entregada. Si bien debemos tener en cuenta que la entrega de dichos documentos a las personas legitimadas si es un derecho, se debe poner en la mesa también la reserva legal de la información la cual se pretende entregar, por lo tanto, la entidad encargada de la información debe actuar como una "notaría expés", validando que los documentos aportados sean verídicos, todo esto en un entorno de inmediatez asistencial, esto basándose en la **Resolución 1995 de 1999 en su artículo 14**, la cual limita el acceso a la información sensible al usuario, al equipo de salud y a las autoridades judiciales.

Otro de los momentos más difíciles en la gestión de datos médicos sensibles ocurre cuando un paciente fallece o se encuentra en estado de incapacidad, por lo cual, no le es posible acceder a los documentos que necesita por sí mismo. Por ende, en este escenario la protección de datos personales se encuentra frente a un dilema ético y moral, ya que como se indicó en el primer capítulo de este texto y lo manifiesta igualmente la **Sentencia T-182 de 2009**, la reserva de dichos documentos no se extingue con la incapacidad del titular de acceder a ellos o de decidir qué desea hacer con los mismo, esto con el fin de proteger la intimidad tanto del titular del documento como a su núcleo familiar frente a la exposición de la información contenida al público; por lo cual, el deber de las Instituciones Prestadoras de Salud (IPS) de mantener la reserva de estos documentos (aun en la defunción o incapacidad) y la necesidad de los familiares y/o terceros de acceder a la misma, chocan de tal manera que se convierte en una odisea, de la cual se deriva el conflicto interno de la entidad de querer complacer a los acompañantes del paciente con una excelente atención al usuario, con el deber de reservar los

documentos sensibles y no compartirlos con cualquier persona que lo solicite, sin antes verificar los documentos que lo acrediten como persona legitimada para lo mismo.

Esta “barrera” de reserva, si bien protege la memoria del difunto, no puede convertirse en un muro completamente incruzable, el cual aumente el sufrimiento de su núcleo familiar, es por esto, que reiteradas jurisprudencias, incluyendo la **Sentencia T-182 de 2009**, fijaron cuatro (4) requisitos, los cuales se deben cumplir para poder acceder a la información sensible de un paciente fallecido, y por ende, deben ser validados por la entidad encargada de archivar dichos documentos:

1. La persona quien desea le sean suministrados los documentos debe demostrar que el paciente ha fallecido, esto se podía demostrar con el Registro Civil de Defunción.
2. Deberá acreditar la condición de familiar con el titular de la historia clínica, esto podría ser demostrado mediante acta de matrimonio, Registro Civil de Nacimiento, entre otros.
3. La solicitud debe ser motivada, es decir, el peticionario debe explicar las razones por la cual solicita la información, ya sea para proteger su derecho a la salud por antecedentes genéticos, para trámites y/o para verificar posibles fallas en el servicio.
4. Por último, debe indicarse que quien recibe la información asume la responsabilidad de mantenerla en reserva, es decir, no hacerla pública, esto con el fin de respetar la memoria del difunto y que la misma no sea divulgada.

Teniendo en cuenta lo anterior, podemos evidenciar que el acceso a la Historia Clínica puede ser indispensable para los familiares quienes consideren se enfrentan a una falla del servicio, y únicamente con los registros de la Historia Clínica pueden acercarse un poco más a qué le pasó a su ser querido, y con esta información, puedan defender sus derechos, tal como se evidencia en la **Sentencia T-373 de 2025**, donde un paciente sufrió un brote psicótico y falleció

tras lanzarse por una ventana dentro de las instalaciones de una Institución Prestadora de Salud (IPS), por lo cual, el familiar alega una negligencia médica por la ausencia de medidas de seguridad, por ende, solicitaba la Historia Clínica del paciente para sustentar el hecho, y asimismo, la demanda.

2.2. CONFLICTOS ENTRE LA CELERIDAD ASISTENCIAL Y LA PROTECCION DE DATOS PERSONALES

En el día a día de una clínica, el tiempo se mide en segundos, mientras que el equipo médico corre para atender una urgencia, el **Habeas Data** exige una pausa para verificar quién es el titular, pedir una firma y asegurar que el dato no termine en manos equivocadas. En este punto analizaremos precisamente ese enfrentamiento, cuando la necesidad de ser rápidos (celeridad asistencial) se encuentra con la “barrera” de requisitos que exige la **Ley 1581 de 2012**.

En las Instituciones Prestadoras de Salud el elemento más importante es el consentimiento, esto debido a que según la **Sentencia C-748 de 2011** nadie puede tocar la información de un paciente sin que este haya dado su permiso previo, expreso e informado, sin embargo, en una situación de emergencia, pedirle a una persona que se debate entre la vida y la muerte que firme algún documento, podría considerarse cómo un acto fuera de toda lógica humana.

Por lo tanto, el **artículo 10 de la Ley 1581 de 2012** para resolver el conflicto establece una excepción vital, es decir, en casos de urgencia médica o sanitaria, el hospital puede tratar los datos sin necesidad de autorización previa, con lo cual se permite que la vida prevalezca sobre el trámite administrativo, sin embargo, el problema real surge cuando la urgencia pasa y el paciente entra en la fase administrativa, es entonces cuando el rigor de la ley vuelve a aparecer, y lo que antes era rapidez se convierte en lo que muchos familiares perciben como una "barrera administrativa" para obtener una cita, un resultado de laboratorio, un traslado e incluso la misma entrega de la misma información integrada en la Historia Clínica.

Asimismo, se ha detectado que a veces el exceso de trámites para validar la identidad o la protección de datos se convierte en un obstáculo que impide que el paciente reciba su atención a tiempo, por lo tanto, el reto para las Instituciones Prestadoras de Salud (IPS) no es dejar de proteger el dato, sino simplificar el proceso para que la seguridad de la información no castigue la salud del usuario.

En este sentido, la **Sentencia SU-124 de 2018** es muy clara al decir que los problemas administrativos de una institución no pueden ser una excusa para negar o retrasar un servicio, asimismo, humanizar el Habeas Data en la práctica hospitalaria significa entender que el dato sensible (el diagnóstico, el examen, la nota de enfermería) es la herramienta que el médico necesita para curar. Por lo tanto, si el sistema de protección de datos es tan rígido que impide que el médico acceda a la información cuando más la necesita, el derecho al Habeas Data termina irónicamente lesionando el derecho fundamental a la salud.

Es por lo tanto que la gestión de datos en el hospital no debe ser vista como una tarea ajena a la medicina, ya qué, proteger la privacidad es una forma de cuidar al paciente, pero facilitar el acceso rápido es una forma de salvarlo. El desafío operativo radica en convertir el cumplimiento legal en un proceso invisible pero seguro, que acompañe la rapidez del acto médico sin restarle la garantía de reserva que todo ser humano merece.

Asimismo, debemos tener en cuenta que la evolución es la base de la vida, por lo tanto, entre estos cambios que se han evidenciado en estos años, tenemos la digitalización de los documentos, entre estos, la Historia Clínica, está ya no es una carpeta de papel guardada en un sótano, ahora podemos tener nuestra Historia Clínica en nuestros celulares, es decir, se convirtió en una “biografía médica digital”, la cual inclusive puede ser pedida por estos medios, sin tener que desplazarte hasta la institución donde se encuentra archivada. Sin embargo, por el mismo flujo de información, las instituciones obtienen un “poder” sobre la misma, el cual

debe tener límites claros, con el fin de qué no se convierta al paciente en un simple dato procesable, sino qué siempre se respete su dignidad y el derecho al Habeas Data.

En el ámbito jurídico, este cambio ingresó con la **Ley 2015 de 2020**, mediante la cual se creó la Historia Clínica Electrónica Interoperable, en donde se especifica qué el paciente es el único dueño de su información y qué las entidades donde reposen esos archivos son únicamente “guardianes” de los mismos. Por lo tanto, si bien este avance se creó con el fin de que paciente pueda tener a la mano su información médica y pueda salvar su vida en cualquier lugar, el desafío se encuentra en lograr qué esta información no se pierda en el camino y caiga en manos equivocadas, las cuales puedan generarle un perjuicio al paciente o en su defecto a sus allegados.

Es por lo mismo que, para el acceso a la Historia Clínica la **Resolución 1995 de 1999** faculta al usuario, al Equipo de Salud, a las autoridades judiciales y de Salud en los casos previstos en la Ley y a las demás personas determinadas en la ley, siempre y cuando demuestren su acreditación (incluyendo al usuario), sin embargo, la **Resolución 1888 de 2025**, especifica qué el equipo de salud, incluyendo a los médicos, únicamente pueden evidenciar de la Historia Clínica lo que realmente necesitan para la atención del usuario, evitando qué se divulgue información sensible o privada quedando expuesta sin necesidad. Por esta razón, el sistema interno de cada institución debe tener un control, el cual registre exactamente que personal entro a evidenciar la información, debido a qué si lo hacen sin autorización o simplemente por “curiosear”, puede generarse una falta gravísima según la **Ley 2015 de 2020** en su artículo 12, la cual podría llevar incluso a la pérdida de la tarjeta profesional o sanciones disciplinarias severas.

Es por lo mismo, qué las entidades “guardianas” de la información de los pacientes, no deben verse sólo cómo un administrador de sistemas, sino también cómo un garante de la dignidad

del individuo, incluso en un entorno virtual. Por lo tanto, el acceso a la Historia Clínica digital es un avance innegable, sin embargo, aumenta el desafío de permitir que la información no llegue a manos equivocadas y sea divulgada, afectando así la dignidad del titular y su entorno familiar, es decir, el mayor reto para las instituciones es lograr que cada consulta de información, incluyendo las digitales sea un acto de cuidado integral, donde el sistema actúe como un escudo de la intimidad, sin llegar a vulnerar el acceso, y garantice que la información clínica del paciente sea tratada como un atributo esencial de su libertad personal.

2.3. IDENTIFICACIÓN DE “BARRERAS DE ACCESO” DESDE LA PERCEPCIÓN DEL USUARIO

Ahora bien, la operatividad diaria y masiva de una IPS, evidencia que la protección de datos no es meramente un concepto, sino que es una gestión diría que genera tensiones entre la normativa de salud que exige fluidez en los procesos para garantizar eficacia en los procesos y el régimen de habeas data que impone barreras de seguridad necesarias para proteger la intimidad.

En este contexto, se genera una brecha administrativa y las expectativas del paciente quien a menudo percibe los protocolos de seguridad como obstáculos administrativos que dificultan el acceso a su información clínica.

Uno de los principales desafíos identificados es la comunicación jurídica, el rigor técnico con el que se manejan los procesos es un obstáculo para poder generar una comunicación asertiva con el usuario. Lo que para la institución constituye un ejercicio de ponderación técnica para evitar la vulneración de la intimidad, para el usuario se manifiesta como una barrera burocrática que impide el flujo de información necesario para su atención.

En este sentido, se considera que el problema empieza en el momento en el que las solicitudes son negadas bajo los conceptos de “legitimación en la causa” entre otros. Mientras el abogado entiende que estas restricciones son imperativos legales para mitigar riesgos ante la Superintendencia de Industria y Comercio (SIC), el paciente, a menudo en una situación de vulnerabilidad, interpreta el lenguaje jurídico como una negación del servicio o una falta de humanidad.

Esta desconexión convierte el cumplimiento normativo en una "muralla de confidencialidad" que el usuario no logra comprender, generando la percepción de que la clínica instala obstáculos injustificados para la entrega de resultados o documentos médicos.

En consecuencia, si bien es cierto la clínica trabaja de manera rigurosa con el cumplimiento de la **Ley 1581 de 2012**, es desafío que se presenta consiste en la transformación en donde la visión puramente formalista pueda generar un lenguaje levemente más fluido con el fin de que todas las partes puedan entender el porqué de las decisiones que se toman.

Por lo tanto, la acción de tutela y el sistema de Peticiones, Quejas y Reclamos (PQR) constituyen el principal mecanismo de medición sobre cómo la aplicación del régimen de protección de datos impacta la experiencia del usuario. Dentro de una organización privada del sector de la salud, se recibe diariamente un alto volumen de estos recursos, podemos decir que esto no solo es un trámite administrativo, sino que, es un síntoma entre el rigor legal de los procesos y la necesidad de los pacientes de tener acceso a su servicio de salud completo. Cuando el área jurídica exige requisitos estrictos de legitimación para la entrega de información, el usuario, al considerar que se vulneran sus derechos fundamentales de dignidad y oportunidad, recurre al amparo constitucional como la vía más expedita para derribar lo que percibe como una barrera burocrática.

Mientras que la IPS tiene la obligación de actuar de manera oportuna para proteger datos sensibles y evitar riesgos ante la Superintendencia de Industria y Comercio (SIC), el paciente interpreta la rigurosidad como un obstáculo para su tratamiento médico. Por ello, el objetivo de la gestión jurídica en estos casos es brindar una respuesta técnica y oportuna que sea congruente con la solicitud, sin embargo, en ciertas ocasiones no es suficiente para el paciente recibir este tipo de respuestas, lo que obliga a la institución a realizar una ponderación constante entre beneficiar al paciente o cumplir con la obligación legislativa.

En última instancia, el descontento manifestado en las tutelas y PQR refleja que el cumplimiento del régimen de protección de datos en las IPS suele reducirse a una formalidad que el paciente no logra asimilar como una garantía material de su propia privacidad. La labor consiste, entonces, en analizar críticamente estas situaciones para identificar si los protocolos actuales, aunque legales, están operando como muros injustificados. Buscar una armonía entre la agilidad en la prestación del servicio y el deber de reserva es el reto ético y jurídico que define hoy la gestión de datos en una institución de alta complejidad.

2.4. RIESGOS DE LA GESTIÓN: ENTRE LA SANCIÓN DE LA SIC Y LA VULNERACIÓN DEL PACIENTE

La institución no solo presta servicios de salud, sino que como lo hemos venido mencionando, el tema de la información hacia el paciente juega un papel muy importante, por ende, el área jurídica y su gestión diaria se convierte en un proceso de ponderación técnica donde el riesgo de incumplimiento normativo frente a los entes de control debe equilibrarse con el respeto a la dignidad y autonomía del paciente.

En el área jurídica de una organización privada del sector de la salud por medio de las diferentes áreas como lo son laboral, comercial, tutelas y litigios, se busca mitigar los riesgos sancionatorios ante la SIC, esta presión administrativa genera la necesidad de que cada trámite

que se realice se haga de manera precisa, por ende existe siempre el miedo de que los datos proporcionados respecto a los pacientes sean los correctos y sobre todo, se debe conocer muy bien los límites, es decir, si bien es cierto los datos sensibles que se proporcionan son con fines netamente informativos, no en todos los casos se pueden proporcionar o incluso algunos datos no se pueden brindar aunque sean solicitados.

Es por ende que, se debe trabajar muy de la mano con el tema de la responsabilidad demostrada, probando de manera interna y externa que se han implementado las medidas técnicas, humanas y administrativas necesarias para evitar accesos no autorizados. Sin embargo, es importante entender que es imposible no tener errores dentro de los procesos, puede generar un fenómeno de hiper-cumplimiento, donde la protección del dato se vuelve tan rígida que colisiona con la oportunidad asistencial. Así, la gestión jurídica se encuentra en una encrucijada: cumplir con el estándar mínimo de calidad que exige la ley para proteger la confianza del paciente, sin que el miedo a la sanción administrativa se convierta en una barrera que vulnere el derecho a la salud del titular.

Por otro lado, es importante entender la manera en cómo los procesos se manejan, en la actualidad donde prima la tecnología es claro que todo se maneja por medio de un sistema digital dinámico, esto lleva a que conozcamos nuevos conceptos como lo son “el dato inferido” que se refiere a aquella información que no es suministrada directamente por el paciente, sino que la clínica deduce o genera a través de procesos analíticos, diagnósticos avanzados o algoritmos de inteligencia de datos.

El reto se encuentra en poder balancear el tema respecto a que muchos de los datos sensibles no son suministrados directamente del paciente, sino que la clínica por medio de sus diligencias internas través de procesos analíticos, diagnósticos avanzados o algoritmos de inteligencia de datos. El desafío jurídico radica en que, aunque el paciente no haya entregado

esa información de manera consciente, el resultado sigue siendo un dato sensible que describe su estado de salud y, por ende, goza de una protección reforzada.

Al ser una clínica de alta complejidad, se debe garantizar que la tecnología no avance más rápido que las actuaciones legales, es decir, el riesgo principal se encuentra en la trazabilidad de los datos sensibles, esta, pasa por varias áreas asistenciales y administrativas de la institución desde el ingreso hasta el egreso del paciente, en este flujo constante es sumamente importante asegurar que solo el personal autorizado accede a los datos proporcionados esto es vital para evitar filtraciones que puedan derivar en discriminación o vulneraciones a la intimidad.

Por lo tanto, podemos decir que, la protección de los datos personales en este entorno tecnológico no puede limitarse a la custodia de la historia clínica tradicional sino que se debe blindar toda la información que llegue de la misma manera, una de las maneras más efectiva para hacerlo es la innovación en las herramienta del sistema tecnológico de la institución, La seguridad de la información debe evolucionar a la par de la tecnología médica, asegurando que cada dato generado automáticamente sea tratado con la misma rigurosidad y reserva que los datos sensibles recolectados de forma presencial.

CAPÍTULO III. LA MATERIALIZACIÓN DEL DERECHO AL HABEAS DATA EN LA PRÁCTICA CLÍNICA: SISTEMATIZACIÓN DE LA EXPERIENCIA EN EL ÁREA JURÍDICA DE UNA ORGANIZACIÓN PRIVADA DEL SECTOR DE LA SALUD

3.1. EL ENTORNO DE LA PRÁCTICA: GESTIÓN DE LA INTIMIDAD EN UNA IPS DE ALTA COMPLEJIDAD

Para la investigación actual, es fundamental entender el origen de la organización privada en el sector salud. Su historia es un ejemplo de consolidación institucional: desde su establecimiento en 1976, ha destacado por un desarrollo continuo hacia una alta complejidad médica y la

seguridad del paciente. Este progreso local, respaldado por estándares internacionales como la acreditación de la Joint Commission International, hizo posible que la institución superará el campo regional y se estableciera como un activo estratégico en el sector de salud de América Latina.

Desde 2019, la clínica establece una relación con un grupo prestigioso, transformándola de esta manera en una institución de IV Nivel a nivel internacional. Por lo mencionado, es posible demostrar que la organización privada del sector de la salud tiene un gran significado en el campo donde se lleva a cabo, clasificándose como una de las más destacadas, con servicios y herramientas médicas que no están disponibles en otras partes.

Aunque la trayectoria de la institución supone un apoyo positivo y de gran prestigio para la organización privada del sector sanitario, es fundamental examinar las consecuencias que este posicionamiento tiene en el trato con los usuarios. Siendo clasificada como una institución de IV Nivel, el acceso a la prestación de servicios está sometido a estrictas auditorías de verificación y trazabilidad interna.

Este modelo de gestión de calidad requiere que se verifique, en primer lugar, que la EPS con la que el paciente está afiliado conserve un contrato activo con la clínica. Una restricción operativa se origina de este proceso: la severidad en la elección de socios estratégicos. La clínica no mantiene acuerdos con todas las EPS del mercado, ya que las aseguradoras requieren que se cumplan los pagos y los procesos administrativos de manera eficaz. Esta política tiene como objetivo asegurar que los estándares de calidad se mantengan sostenibles, aunque en la práctica limite el acceso a los usuarios cuyos organismos no satisfacen las condiciones institucionales establecidas con anterioridad.

Lo mencionado con anterioridad está directamente vinculado con el elevado número de acciones de tutela y derechos de petición que la institución recibe. En la mayoría de las situaciones, no poder ofrecer el servicio solicitado proviene de las restricciones contractuales y de convenio que se mencionaron anteriormente.

Esta circunstancia involucra directamente al área legal, que se ve forzada a ofrecer respuestas negativas ante las demandas de los usuarios. Esta situación no solo da lugar a la sensación de que existen obstáculos para acceder al servicio de salud, sino que también colma la capacidad operativa del equipo legal. Esto afecta la rapidez con que se responde a otras solicitudes y refuerza una discordancia entre las expectativas del paciente y la estricta aplicación de los protocolos administrativos de la clínica.

Para ejemplificar el problema descrito antes, es apropiado presentar un caso de estudio que sea representativo del conjunto de casos institucionales, teniendo en cuenta que los datos sensibles se han anonimizado a través del empleo de nombres ficticios, cumpliendo estrictamente con la normativa de protección de datos personales y el derecho a la privacidad.

El conflicto jurídico ocurre cuando un ciudadano, que está inscrito en una Entidad Promotora de Salud (EPS) con la que la organización no tiene un vínculo contractual vigente, se presenta ante dicha entidad privada del sector salud para solicitar que su tratamiento oncológico continúe. El usuario basa su argumento en que, en tiempos pasados, la clínica le había ofrecido servicios de programación de citas y gestión de ciclos de quimioterapia, lo cual, según él, crea una razonable expectativa de continuidad.

Conforme a esta premisa, el usuario inicia una acción de tutela, argumentando que sus derechos fundamentales a la vida y la salud en condiciones dignas han sido supuestamente

vulnerados. Su principal objetivo es que la clínica sea obligada por orden judicial a encargarse de ofrecer servicios de IV nivel de complejidad, incluso si no hay un convenio o apoyo administrativo que asegure que su aseguradora actual cubrirá económicamente dicho tratamiento.

En esta circunstancia, el área legal basa su defensa en el principio de legitimidad en la causa por pasiva, sosteniendo que la EPS es la principal responsable y que, por lo tanto, nos enfrentamos a una imposibilidad jurídica y material para proporcionar los servicios necesarios sin autorización previa y pago anticipado.

Finalmente, la solución administrativa y jurídica no se restringe a la negativa, sino que se dirige a la gestión de referencia, proveyendo al usuario con el asesoramiento requerido para que su entidad aseguradora lo envíe a una institución que sí pertenezca a su red de proveedores. Así, se consigue un balance entre garantizar que el paciente obtenga la atención necesaria en el lugar administrativamente competente y proteger la autonomía privada de la clínica, con lo cual se evita una carga excesiva para el equipo legal y financiero de la organización.

3.2. LA APLICACIÓN DEL FILTRO DE LEGITIMACIÓN: ENTRE EL DEBER SER Y LA PERCEPCIÓN DEL USUARIO

El escenario planetario descrito en el anterior apartado puede interpretarse como un proceso sistemático y una tarea ordinaria dentro de la gestión institucional, la ejecución de dicho protocolo en la práctica clínica resulta profundamente retadora.

La operatividad diaria exige navegar sobre la delgada línea que separa el estricto cumplimiento administrativo de la sensibilidad humana, lo cual constituye un desafío ético y profesional de gran envergadura. En la mayoría de los casos, este equilibrio se convierte en una tensión

constante: por un lado, la necesidad de garantizar la viabilidad jurídica y financiera de la clínica y, por otro, la respuesta empática ante la vulnerabilidad del paciente, transformando una gestión técnica en un dilema de responsabilidad humana.

Como integrantes del área jurídica, el marco normativo analizado constituye nuestra guía de actuación imperativa; en consecuencia, la objetividad es uno de los pilares fundamentales para la gestión de los escenarios institucionales diarios. No obstante, en diversas ocasiones, el suministro de una respuesta verídica y técnica ante los despachos judiciales exige trascender la trazabilidad digital.

Este proceso requiere una intervención directa en los servicios asistenciales tales como oncología, UCI, urgencias, maternidad y hospitalización, entre otros lo cual confronta al profesional del derecho con la realidad tangible de los usuarios. En este punto, el expediente administrativo se transforma y ya no es solo lo que inicialmente se visualiza en un documento como un nombre o un número radicado, sino que ahora adquiere rostro e historia, humanizando el análisis legal y evidenciando la complejidad intrínseca de la práctica jurídica en el sector salud.

En consecuencia, surge un conflicto crítico en la comunicación con el usuario. A pesar de la sensibilidad con la que se aborda la información y la comprensión empática de cada caso, nuestra actuación se encuentra estrictamente supeditada al marco legal y normativo vigente.

Esta prevalencia de la ley sobre la voluntad individual suele ser percibida por los pacientes y sus familias como un acto insensible o inhumano. La imposibilidad de ejecutar las solicitudes de manera inmediata o, en ciertos casos, la denegación de las mismas por falta de sustento jurídico o contractual genera una ruptura entre la expectativa de atención del ciudadano y el rigor administrativo que debemos observar, consolidando una barrera de comunicación que trasciende lo meramente jurídico para convertirse en un desafío de gestión humana.

3.3. NUDOS CRÍTICOS EN LA GESTIÓN DE CASOS SENSIBLES: FALLECIDOS E INCAPACES

Dentro de nuestra experiencia en el área jurídica de una organización privada del sector de la salud la gestión de solicitudes de familiares de pacientes fallecidos o en estado de incapacidad se volvió uno de nuestros desafíos más grandes y exigentes, esto debido al nivel de complejidad de verificación de la identidad y el conflicto ético interno de cada uno de nosotros cómo seres humanos frente a la situación. Antes de dar continuidad, consideramos importante reiterar la distinción de responsabilidad entre tramitar un Derecho de Petición y responder a una Acción de Tutela.

En el marco de la **Ley 1581 de 2012** encontramos el artículo 13, mediante el cual se indica quienes son las personas autorizadas para poder suministrarle la información solicitada, esto son : *“a) A los Titulares, sus causahabientes o sus representantes legales; b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial; c) A los terceros autorizados por el Titular o por la ley.”*, cada individuo perteneciente a estos grupos debe acreditar su calidad con un documento correspondiente, sin embargo, el tema se complica un poco más cuando el titular no puede dar su autorización, por lo cual, cómo se indicó anteriormente, en la **Sentencia T-182 de 2009** se fijaron los 4 requisitos qué debe cumplir una persona para acceder a información de un titular fallecido o en estado de incapacidad, recordemos que estos son: 1. demostrar que el paciente se encuentra fallecido o incapacitado, 2. acreditar la condición de familiar, 3. motivación de la solicitud, 4. indicar a la persona qué debe mantener la reserva de la información.

Teniendo clara esta información, podemos evidenciar que frente a la recepción de derechos de Petición, los cuales se encuentran enmarcados en el artículo 23 de la **Constitución Política de Colombia**, la organización privada del sector de la salud actúa cómo la única autoridad qué

valida estos requisitos de reserva legal, al no existir una autoridad legal superior que verifique y autorice la entrega de la información, la carga de "no equivocarse" recae íntegramente sobre la persona encargada de responder estas petición en el área jurídica de la organización privada del sector de la salud, en este caso, nosotras cómo practicantes jurídicas. Por lo tanto, la aplicación de la **Sentencia T-182 de 2009** no es solo una guía, sino un protocolo de seguridad de obligatorio cumplimiento para la protección tanto del titular de la información cómo de su entorno, por lo cual, la labor de verificar que el familiar acredite el parentesco cercano, motive la necesidad para proteger un derecho y se comprometa formalmente al sigilo, se percibe en la oficina como un ejercicio de "debida diligencia", sin embargo, para el familiar en duelo o en una situación de extrema tristeza, esta exigencia se traduce a menudo en una colisión emocional, es decir, ellos ven una barrera administrativa donde nosotros estamos aplicando un escudo para evitar que la información sensible caiga en manos no autorizadas, lo cual constituirá una **falta gravísima** según lo anteriormente indicado a lo largo del texto. Una situación por la cual tuvimos qué atravesar, fue la de Julián, hijo de Roberto (Q.E.P.D), quien estaba solicitando información de un procedimiento realizado a su padre, sin embargo, no adjuntó los documentos correspondientes, por lo cual, nos vimos en la necesidad de comunicarnos con Julián y solicitarle los mismos, en esta situación en específico contamos con la suerte de contar con un persona qué entendía la situación y la necesidad de la verificación, por lo tanto, después de explicarle la situación, con toda la cautela qué la misma amerita, Julián nos remitió todos los documentos solicitados; Este caso en específico es un caso ajeno, debido a que también nos encontramos con Luz, quien reside en Estados Unidos, y solicita desde un largo tiempo el envío de la Historia Clínica de Carlos, su padre (Q.E.P.D.), sin embargo, no ha sido posible remitir la información por la ausencia de los documentos necesarios, y en este punto, nos encontramos en una situación de conflicto con la usuaria, quien considera le estamos negando información a la cual tiene derecho acceder, mientras qué nosotros cómo institución, nos

encontramos protegiendo la información registrada en la Historia Clínica del señor Carlos (Q.E.P.D).

Por el contrario, la **Acción de Tutela** presenta una dinámica jurídica que, de forma irónica, "alivia" la carga de validación por parte de la IPS, esto debido a al inciso C del artículo 13 de la **Ley 1581 de 2012**, donde se autoriza la entrega de esta información por orden judicial. Si bien el término de respuesta es perentorio y genera una presión inmensa, la responsabilidad de la reserva se comparte con la administración de justicia, por lo cual, la verificación de la acreditación por parte nuestra disminuye. Según el **artículo 19 del Decreto 2591 de 1991**, el Juez está plenamente facultado para pedir el expediente o la documentación donde consten los antecedentes del asunto. Al ser una autoridad judicial, se encuentra expresamente habilitada por el **artículo 14 de la Resolución 1995 de 1999** para acceder a la historia clínica, por lo cual, esta obligación de reserva recae íntegramente en estos casos en el órgano judicial a quien se le comparte, debido a que en ese punto el decide si comparte el archivo con el accionante o si es preferible su no entrega. En nuestra práctica observamos que cuando la información se entrega por orden judicial, el "filtro" de legitimación ya ha sido procesado por el juzgado, por lo cual, en estos casos, la Clínica cumple con su deber de custodia entregando el dato al despacho, quien bajo el mandato del **artículo 27 del CPACA**, tiene la obligación legal de asegurar la reserva de los documentos que lleguen a su conocimiento. Esta intermediación judicial reduce el margen de error institucional y garantiza que el acceso a la verdad del familiar sea validado por un garante de derechos fundamentales.

3.4. REFLEXIONES FINALES: LA HUMANIZACIÓN DEL DATO COMO ESTRATEGIA DE EXCELENCIA

La administración de la información en el ámbito hospitalario no debe considerarse como una tarea separada del acto médico, sino como un elemento transversal para garantizar la

seguridad del paciente. La protección de la información personal se convierte en el último nivel de cuidado que la clínica brinda a las personas en una institución de Nivel IV, donde la sensibilidad de los diagnósticos y la seriedad de los acontecimientos asistenciales incrementan el peligro de estigmatización; desde este punto de vista, el dato clínico ya no es simplemente un registro inerte almacenado en un servidor, sino que se considera la biografía médica del sujeto, cuya confidencialidad resguarda su dignidad incluso cuando está inconsciente o después de su muerte.

El estudio de la práctica revela que el conflicto entre el "derecho de acceso" y el "deber de reserva" se trata con eficacia por medio de lo que podemos llamar hospitalidad informativa. Esta táctica se basa en convertir la respuesta jurídica (generalmente considerada como una barrera administrativa) en un procedimiento de acompañamiento pedagógico, por lo cual, la reciente **sentencia T-373 de 2025** destaca que para que las familias tengan claridad frente a situaciones adversas, es necesario acceder a la verdad contenida en la historia clínica. Por ende, el trabajo del área jurídica no debe restringirse a la negativa fundamentada en la ley, sino a orientar al solicitante en la satisfacción de los requerimientos de la **Sentencia T-182 de 2009**, asegurando que el flujo de información sea un acto justo y no una violación a la privacidad.

Además, la aplicación de la Historia Clínica Electrónica Interoperable y el Resumen Digital de Atención (RDA), que está regulada por la **Resolución 1888 de 2025**, requiere reforzar el principio de **Responsabilidad Demostrada (Accountability)**. Para que la asistencia sea excelente, siguiendo normas internacionales como las de **Joint Commission International (JCI)**, es necesario que la seguridad digital no sea visible para el paciente, pero sí infranqueable para terceros no autorizados. Esto significa que el personal administrativo y jurídico debe proceder con un nivel de cuidado elevado, considerando la validación de la identidad y la legitimación no como un procedimiento notarial, sino como un escudo que resguarda la confianza que el paciente ha depositado en la institución.

Por último, la incorporación de la filosofía de **Atención Centrada en la Persona** con el sistema de protección de datos posibilita que la IPS pase a un modelo en el cual la tecnología contribuya a la libertad del ser humano. La comunicación abierta y clara que le explique al usuario la razón por la cual su información es sagrada debe ser promovida en la práctica jurídica de salud, en vez de establecer barreras administrativas sin justificación, en esta línea, la gestión del Habeas Data en situaciones de alta complejidad se caracteriza por un equilibrio continuo: posibilitar que el dato circule rápidamente para curar, pero garantizar que se mantenga reservado para salvaguardar la dignidad y la vida personal del individuo.

CAPÍTULO IV: CONCLUSIONES

Al concluir el desarrollo de este trabajo, se determina que los propósitos planteados fueron alcanzados en su totalidad, ya que se consiguió establecer y examinar el régimen jurídico aplicable a la gestión de datos personales en el ámbito sanitario, especialmente a través de la correlación entre la Ley 1581 del año 2012, la Ley Estatutaria 1751 del año 2015, la Ley 2015 del año 2020 y las normativas reglamentarias relacionadas con la historia clínica. Este análisis demostró que la protección de los datos personales en las Instituciones Prestadoras de Salud (IPS) no es un sistema normativo independiente, sino una red compleja donde se entrecruzan derechos esenciales como la intimidad, el habeas data y la salud; su realización requiere un trabajo constante de ponderación.

Se comprobó, en este contexto, que los principios rectores para el tratamiento de datos personales (como la libertad, la transparencia, la confidencialidad, la seguridad, el acceso y la circulación restringida, la legalidad y la finalidad) cobran un mayor peso en el sector clínico por el carácter delicado de los datos tratados. No obstante, su implementación en situaciones de alta complejidad hospitalaria muestra tensiones estructurales, sobre todo cuando se trata de asegurar que el servicio de salud sea prestado con celeridad. Así pues, se comprobó que

aplicar el régimen de protección de datos no se puede considerar simplemente como un trámite administrativo, sino como una práctica técnica que busca equilibrar la protección de la dignidad humana y la eficiencia asistencial.

Además, se pudo identificar los retos operativos más importantes a los que se enfrentan las IPS, sobre todo en la administración de quejas, peticiones, reclamos y acciones de tutela, mediante la sistematización de la experiencia en el ámbito legal. En estos contextos, la confirmación de la legitimación en la causa se establece como un punto crucial que, aunque obedece a requerimientos legales que provienen del principio de libertad y de la responsabilidad demostrada, es visto por los usuarios como un obstáculo para acceder a la información. Esta tensión revela la exigencia de ir más allá de una perspectiva puramente formalista del derecho, con el objetivo de progresar hacia esquemas de gestión que combinen la observancia normativa con tácticas eficaces de comunicación jurídica.

La práctica, en lo que respecta a la contribución hecha, posibilitó una participación activa en el estudio jurídico de situaciones específicas y favoreció que se aplicara con rigor el régimen de protección de datos personales al tomar decisiones institucionales. Este ejercicio supuso evaluar los requisitos para acceder a la historia clínica, interpretar excepciones legales y formular respuestas desde el punto de vista jurídico con el fin de proteger tanto la confidencialidad de la información sensible como el derecho fundamental a la salud, al tiempo que se disminuían los riesgos de responsabilidad administrativa y sancionatoria ante la Superintendencia de Industria y Comercio.

Desde un punto de vista teórico, el trabajo facilitó la utilización de categorías propias del derecho administrativo y constitucional, especialmente la teoría de ponderación de derechos fundamentales. Esto demostró que no es factible tomar decisiones absolutas en el campo de la salud. En cambio, cada situación requiere un análisis contextual que logre equilibrar el derecho

a acceder a la información con el deber de confidencialidad, reconociendo que ambos son garantías fundamentales de la dignidad humana. En esta línea, se ratifica que el habeas data no solamente salvaguarda la información personal, sino que además restringe el ejercicio del poder institucional sobre la persona.

Finalmente, desde una perspectiva crítica, se determina que uno de los mayores desafíos del sector salud es prevenir que las regulaciones de protección de datos se transformen en un impedimento para la entrega del servicio, sin tener que aflojar indebidamente los estándares de seguridad. Esto requiere una modificación en la cultura de la organización, donde la protección de datos no se vea únicamente como una carga legal, sino que se reconozca como un elemento fundamental de la calidad del servicio y de la confianza del paciente.

Esta experiencia, en el ámbito académico y personal, posibilitó que la comprensión teórica del derecho se trasladara a contextos reales de toma de decisiones, lo cual potenció habilidades como la argumentación, análisis y resolución de conflictos. Por lo tanto, se establece una perspectiva del ejercicio jurídico que no es solo la aplicación de normas, sino también una práctica enfocada en proteger de manera efectiva los derechos fundamentales en situaciones complejas.

BIBLIOGRAFÍA

- ❖ Constitución Política de Colombia de 1991.
- ❖ Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- ❖ Ley Estatutaria 1751 de 2015. Por medio de la cual se regula el derecho fundamental a la salud.
- ❖ Ley 2015 de 2020. Por la cual se crea la Historia Clínica Electrónica Interoperable.
- ❖ Resolución 1995 de 1999. Ministerio de Salud. Normas para el manejo de la Historia Clínica.
- ❖ Resolución 1888 de 2025. Ministerio de Salud. Adopción del Resumen Digital de Atención en Salud (RDA).
- ❖ Resolución 839 de 2017. Ministerio de Salud. Manejo, custodia y tiempo de retención de historias clínicas.
- ❖ Corte Constitucional, Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.
- ❖ Corte Constitucional, Sentencia T-182 de 2009. M.P. Jorge Iván Palacio Palacio.
- ❖ Corte Constitucional, Sentencia SU-355 de 2022. M.P. Cristina Pardo Schlesinger.
- ❖ Corte Constitucional, Sentencia T-373 de 2025. M.P. Paola Andrea Meneses Mosquera.
- ❖ Manual de Estándares de Acreditación JCI, 7ª Edición.