PROTECCIÓN DE DATOS Y RIESGOS EN LA HISTORIA CLÍNICA

LORENA BEDOYA AGUILAR

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE ABOGADA

DIEGO MARTÍN BUITRAGO BOTERO

ASESOR

FACULTAD DE DERECHO

UNIVERSIDAD CES

2025

PROTECCIÓN DE DATOS Y RIESGOS EN LA HISTORÍA CLÍNICA.

1. Planteamiento Del Problema

En Colombia, la transformación digital del sistema de salud se ha intensificado en los últimos años, especialmente con el impacto generado a raíz de la pandemia del COVID-19. La optimización de los procesos administrativos ha promovido la implementación de herramientas tecnológicas que permiten almacenar, gestionar y compartir de manera digital la información clínica de los pacientes. Estos avances han contribuido a mejorar la eficiencia en la prestación de los servicios de salud, sin embargo, también han generado retos en materia de protección de datos personales, en particular aquellos catalogados como sensibles, que comprometen la intimidad del titular o cuyo uso inapropiado podría generar discriminación por su vinculación con la dignidad humana según la Ley 1581 de 2012 (Congreso de la República, 2012).

La Resolución 1995 de 1999, modificada por la Resolución 839 de 2017, regula el manejo de las historias clínicas en Colombia y establece que este documento es de carácter privado, reservado y sujeto a condiciones de confidencialidad y veracidad (Ministerio de Salud, 1999). Estas disposiciones se complementan con la Ley 1581 de 2012 (Congreso de la República, 2012) , que regula el tratamiento de datos personales e incorpora principios como la legalidad, finalidad, libertad, calidad de la información, transparencia, acceso restringido, seguridad y confidencialidad, aplicables también a los datos sensibles vinculados con la salud. La integración de estas normas puede reflejar el riesgo de que la información contenida en la

historia clínica, especialmente cuando se gestiona a través de sistemas electrónicos, sea divulgada sin autorización, con posibles consecuencias negativas para la vida en sociedad del paciente, como se ve reflejado en la Resolución No 4548 de 2025, (Superintendencia de Industria y Comercio, 2025), en donde se impuso sanciones a una entidad de salud por violar lo establecido en la Ley 1581 de 2012 (Congreso de la República, 2012) sobre el régimen de protección de datos de manera específica, la entidad sancionada divulgó sin autorización la historia clínica de un afiliado, incluyendo su diagnóstico de VIH, a directivos de su empleador, pese a que la entidad reconoció la infracción y atribuyó el hecho a un error humano, se evidenció que sus medidas de seguridad eran insuficientes, además porque la sanción también se fundamentó en el impacto emocional y laboral que sufrió el titular.

En este contexto, la Ley 1581 de 2012 (Congreso de la República, 2012) impone a los responsables y encargados del tratamiento de datos la obligación de aplicar medidas técnicas, humanas y administrativas destinadas a garantizar la seguridad de la información, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado. Este deber resulta especialmente relevante en el sector salud, donde la información sensible exige salvaguardas reforzadas. Además, la norma establece la obligación de conservar los datos bajo condiciones adecuadas de seguridad y de informar a la autoridad de control en caso de presentarse incidentes que comprometan la protección de la información (Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos Personales, 2020).

El marco normativo se amplía con la Ley 1266 de 2008 (Congreso de la República, 2008), que regula el tratamiento de la información financiera y crediticia, e introduce principios como

la seguridad y la confidencialidad, igualmente aplicables al manejo de información personal asociada tanto a la atención de servicios de salud como a las transacciones económicas relacionadas con esta (Congreso de la República, 2008)

Sin embargo, los informes de la Superintendencia de Industria y Comercio (en adelante, "SIC) muestran deficiencias que persisten en la implementación de medidas de seguridad por parte de los responsables del tratamiento, además se evidenció que el 54,6% de las organizaciones no cuentan con políticas específicas para regular el acceso a información sensible y que el 61% no dispone de un sistema integral de gestión de seguridad de la información. Estos hallazgos reflejan la necesidad de fortalecer la cultura de protección de datos en todos los sectores y, de manera prioritaria, en el ámbito de la salud, dado que la vulneración de la confidencialidad de la información clínica puede generar afectaciones graves a los derechos fundamentales de los titulares (Escuela de Privacidad, 2023).

2. Justificación Del Problema

El desarrollo del tema en cuestión permitirá crear un planteamiento para identificar cuáles son los puntos de relacionamiento entre las normas de la historia clínica (Resolución 1995 de 1999, modificada por la Resolución 839 de 2017 y la ley 2015 de 2020) y las de Tratamiento de Datos Personales (en adelante, "TDP"), en la Ley 1581 de 2012 (Congreso de la República, 2012) para así, ilustrar a los pacientes de la necesidad de entendimiento total de cara al suministro de la información médica, teniendo presente el cumplimiento constitucional del Artículo 15 (Constitución Política de Colombia,1991) , para el derecho a la intimidad y seguridad de la información. Por tanto, se plantea indagar cómo prevenir y mitigar

los riesgos inherentes al tratamiento de datos sensibles en la historia clínica, considerando la aparente ausencia de mecanismos de defensa específicos dentro de la norma, sin abandonarlo dispuesto en la Ley 23 de 1981(Congreso de la República, 1981) código de ética médico.

En este sentido, resulta de gran relevancia profundizar el tema, no sólo respecto a la atención que brindan las instituciones sino a la información que queda depositada de manera posterior, y la actualización de datos con la que debe cumplirse en función del habeas data. A su vez, crea la necesidad del cuestionamiento y proyección de soluciones para el eventual escenario de una divulgación no deseada de datos personales, y el fortalecimiento de sistemas de protección y seguridad de la información.

Además, para el campo del Derecho, permitirá suministrar información relevante y contribuir a mecanismos robustos para la proyección de los datos sensibles según la Ley 1581 de 2012 (Congreso de la República, 2012) y expandir los planteamientos alrededor del tema teniendo en cuenta un contexto de digitalización acelerada, la cual crea desafíos en cuanto a la privacidad y la seguridad de la información de los pacientes, educándolos sobre la importancia sobre el manejo de su información médica.

De igual manera, la viabilidad del presente trabajo se fundamenta en la posible vulnerabilidad de datos médicos sensibles ante la digitalización, exponiendo a los pacientes a riesgos de divulgación interna y externa con grave impacto en su privacidad y relacionamiento social. Además, la necesidad de fortalecer el marco legal, específicamente la Ley 1581 de 2012 (Congreso de la República, 2012), para adaptarla a los desafíos únicos del sector,

promoviendo así una gestión ética de la información médica, y finalmente, la necesidad de garantizar la confidencialidad de la historia clínica.

3. Descripción del público al que va dirigido

El presente trabajo se dirige de manera específica al sector salud, tanto para los profesionales que intervienen en la prestación de los servicios, como para los pacientes que son titulares de los datos personales objeto de tratamiento. Para los primeros, se busca ofrecer una guía clara que contribuya a suplir los vacíos operativos que puedan presentarse en la aplicación práctica de la normativa vigente, permitiendo a médicos, instituciones prestadoras de salud (IPS), entidades promotoras de salud (EPS) y demás actores del sistema implementar protocolos que sean coherentes con los estándares legales y éticos en materia de protección de datos, y para los segundos el propósito es brindar la comprensión suficiente que les permita ejercer de manera efectiva sus derechos en relación con su información sensible.

4. Marco Referencial

Resulta importante realizar un análisis y conceptualizar el contenido del Artículo 4, de la Ley 1581 de 2012 (Congreso de la República, 2012), que establece los principios rectores para el tratamiento de datos, y el Artículo 3, de la Resolución 1995 de 1999 (Ministerio de Salud, 1999) que enmarca las características de la Historia Clínica (en adelante, “HC”), en el siguiente sentido:

El Principio de **Legalidad**, se relaciona de manera directa con la característica de integralidad, toda vez que la recolección, almacenamiento y uso de la información clínica

debe enmarcarse en lo dispuesto por la normativa vigente, lo que implica que los datos contenidos solo pueden ser tratados conforme a las disposiciones legales aplicables.

Con el Principio de **Finalidad**, se puede encontrar su relación con la racionalidad científica y la disponibilidad de la HC, debido a que el fin último del tratamiento de la información clínica es la atención integral en salud y la investigación clínica, lo que impide su uso para actividades o divulgación no autorizada, y que pueda garantizar que su acceso y uso respondan a un propósito legítimo.

En cuanto al Principio de **Libertad**, se identifica su relación con la oportunidad en el diligenciamiento de la HC, en donde debe contarse con la autorización previa, expresa e informada del titular de la información, dándole el deber al Médico Tratante de registrar la información de manera precisa y clara.

Asimismo, el Principio de **Transparencia** se armoniza con la disponibilidad y el derecho del titular de la información a conocer la existencia y contenido de su HC.

El Principio de **Acceso y Circulación Restringida**, si bien no tiene una relación directa con alguna de las características descritas en la Resolución 1995 de 1999, sí resulta importante por su nexo con la reserva legal de la HC, ya que sólo las personas autorizadas por la ley pueden acceder a los datos del titular de la información con la intención de preservar su carácter privado, como bien se define a continuación según el Artículo 1, Resolución 1995 de 1999:

"*La Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley"(Ministerio de Salud, 1999).*

Por último, los Principios de **Seguridad** y **Confidencialidad** constituyen un eje central importante para la protección de la información de la HC y para el desarrollo del presente trabajo, no sólo por el deber de adopción de medidas técnicas, humanas y administrativas posibles para prevenir pérdidas, accesos o divulgaciones no autorizadas, sino también por la obligación de reserva incluso después de terminada la relación médico-paciente.

Lo anterior arroja un tema relevante de cara a la mención del consentimiento informado del titular de la información y la implementación de la historia clínica electrónica (en adelante HCE), regulada en la Ley 2015 de 2020 que se convierte en un pilar para poder legitimar el tratamiento de datos personales en el sector salud. Sin embargo, en la práctica el consentimiento es un formalismo que el paciente debe aceptar y manifestar para poder recibir atención médica y un registro que cuente con el respaldo suficiente para protegerse y no divulgarse.

5. Contenido de la Cartilla

Se comparte el enlace de la cartilla, en donde se deposita el contenido del presente trabajo, construido desde cero, y con apoyo de Inteligencia Artificial sólo en la creación de las imágenes:

https://www.canva.com/design/DAG2eWEn060/-o_088hEtjgehFixeO-low/edit?utm_content=DAG2eWEn060&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

6. Análisis de los aportes que el proceso tuvo a la formación profesional

El desarrollo del presente trabajo de grado ha sido una gran experiencia para mi formación profesional, dado que mi interés por el tema surge de la conexión entre la digitalización y la necesidad de proteger los derechos fundamentales en un entorno cada vez más interconectado. El estudio y la investigación me ha permitido consolidar y ampliar mi perspectiva, con una mayor comprensión de las complejidades vinculadas a la protección de datos en el ámbito de la historia clínica.

Desde un punto de vista teórico, el proceso me obligó al estudio profundo de un marco normativo en constante evolución, en donde la precisión en la interpretación de cada principio, y concepto me permitió entender la importancia de compartir este tema para el conocimiento de las áreas específicas.

Asimismo, desde el ámbito práctico, la investigación expone la realidad de los posibles retos que enfrentan las organizaciones en la implementación de medidas de seguridad, y me ayudó a reflexionar de manera crítica sobre la importancia de conocer la ley y promover la implementación de mecanismos idóneos para la protección de los datos sensibles.

Por último, la elaboración de un trabajo de esta magnitud ha fortalecido mi confianza en las habilidades de investigación, argumentación y redacción jurídica. La exigencia de precisión

en cada afirmación, la necesidad de mantener coherencia en la estructura y la búsqueda de claridad en la exposición de ideas han sido aspectos que logré perfeccionar a lo largo de este proceso. Este trabajo no solo refleja la aplicación de los conocimientos adquiridos, sino también la apertura hacia un campo que me inspira y en el cual deseo generar un impacto positivo como futura abogada.

7. **Conclusión**:

El análisis de la gestión de la información contenida en las historias clínicas, a la luz de la Ley 1581 de 2012 y la Resolución 1995 de 1999, permite evidenciar que los datos de salud constituyen información sensible que requiere un régimen de protección reforzado. Su tratamiento debe estar limitado a situaciones específicas como la urgencia médica, defensa judicial o fines científicos y sustentado en medidas tecnológicas y administrativas que garanticen la confidencialidad, la trazabilidad y el acceso restringido a la información.

La gestión adecuada de los datos personales en el sector salud no debe entenderse únicamente como una obligación legal, sino como un compromiso ético y una práctica de gobernanza que reconoce el valor humano de la información clínica. Por ello, resulta necesario fortalecer la cultura organizacional en torno a la privacidad, la seguridad digital y la responsabilidad institucional.

En este sentido, a continuación, se presenta un **mapa de riesgos** que sintetiza los principales factores de vulnerabilidad identificados durante la investigación:

UNIVERSIDAD CES Un compromiso con la excelencia VIGILADA MINEDUCACIÓN	**Formato Divulgación pública del conocimiento**
	Fecha:
PROCESO	**Trabajo de grado: Lorena Bedoya Aguilar**

#	Riesgo	Factor	Tipo/Clasificación	Descripción	Consecuencia	Probabilidad	Impacto	Severidad (Psl)
1	Divulgación no autorizada de la historia clínica	Interno	Personal y Ética	Compartir información médica sensible (como diagnósticos de VIH o salud mental) sin el consentimiento del paciente vulnera la confidencialidad, puede generar discriminación y expone a la institución a sanciones legales.	Insostenibilidad del sistema en el tiempo; sobrecosto al reemplazar proveedor.	4	5	20
2	Acceso remoto inseguro a los sistemas de información	Externo	Tecnológico	El uso de conexiones sin cifrado fuerte o sin autenticación adecuada facilita el acceso no autorizado, dejando expuestos los datos clínicos a interceptaciones o intrusiones externas.	Riesgo de incumplimiento y retraso en implementación.	4	4	16
3	Ausencia de auditorías periódicas	Externo	Procesos	No realizar revisiones sistemáticas impide detectar accesos indebidos, manipulaciones o brechas de seguridad en los registros clínicos, debilitando el control interno.	Interrupción del servicio, sanciones contractuales.	3	5	15
4	Errores humanos en el manejo de información clínica	Interno	Infraestructura	Acciones involuntarias como enviar datos sensibles al destinatario equivocado pueden comprometer la privacidad del paciente y generar consecuencias legales o reputacionales.	Pérdida de sostenibilidad financiera.	4	5	20
5	Falta de políticas internas claras sobre acceso a datos sensibles	Interno	Infraestructura	La ausencia de directrices específicas para regular quién accede, cómo y en qué condiciones a la información clínica puede derivar en abusos, negligencias o falta de trazabilidad.	Pérdida total de datos clínicos, suspensión de operaciones.	3	4	12
		Niveles	21 y 25 catastrofico	16 y 20 muy alto	11 y 15 alto	6 y 10 moderado	1 y 5 bajo	
				(Cuadro de elaboración propia)				

Referencias

Andes, U. d. (noviembre de 2022). *colev@.uniandes.edu.co*. Obtenido de file:///C:/Users/Usuario/Downloads/Salud%20Digital%20y%20Derechos%20Digitales%20en%20Colombia.pdf

Colombia, R. d. (20 de Julio de 1991). Obtenido de Secretaría del Senado: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Congreso de Colombia. (2012). *Función pública*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Diana Catalina, D. P. (2021). *Sennova*. Obtenido de file:///C:/Users/Usuario/Downloads/Dialnet-ReflexionSobreLaTransformacionDigitalEnSalud-9004392.pdf

Escuela de Privacidad. (2023). *¿Por qué motivos sancionan a las empresas en materia de protección de datos personales?* Bogotá.

Forero, H. S. (Noviembre de 2020). *Politécnico Gran Colombiano*. Obtenido de https://alejandria.poligran.edu.co/bitstream/handle/10823/2134/Trabajo%20de%20grado%20versi%c3%b3n%20final%2001-12-2020.pdf?sequence=3&isAllowed=y

Ministerio de Salud y Protección Social . (23 de Marzo de 2017). *Minsalud.gov.co*. Obtenido de Minsalud.gov.co: https://minsalud.gov.co/Normatividad_Nuevo/Resolucion%20No%20839%20de%202017.pdf

República, C. d. (31 de Diciembre de 2008). *LEY 1266 DE 2008*. Obtenido de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Superintendencia de Industria y Comercio. (31 de Marzo de 2023). *sic.gov.co*. Obtenido de https://www.sic.gov.co/tema/proteccion-de-datos-personales

Superintendencia de Industria y Comercio. (13 de Febrero de 2025). *Sic.gov.co*. Obtenido de https://www.sic.gov.co/

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos Personales. (2020). *Guía para la Gestión de Incidentes de Seguridad*. Bogotá.

UNIR. (2022). Obtenido de https://investigacion.unir.net/documentos/63e1a8a8e824ae619db00ed2?lang=de

Valle, P. C. (2022). *UNIR*. Obtenido de https://investigacion.unir.net/documentos/63e1a8a8e824ae619db00ed2?lang=de