Diseño de un modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia

Andrés Fabian Rodríguez Peña - Cod 100198444
Brayan Andrés Tafur Pabón – Cod 100241708

Trabajo de grado – Maestría En Gerencia De Proyectos
Institución Universitaria Politécnico Grancolombiano
Bogotá D.C.
2024

Diseño de un modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia

Andrés Fabian Rodríguez Peña - Cod 100198444
Brayan Andrés Tafur Pabón – Cod 100241708

Director
Sebastián Alberto Peláez Gómez

Trabajo de grado para optar al título de Maestría En Gerencia De Proyectos

Institución Universitaria Politécnico Grancolombiano
Maestría En Gerencia De Proyectos
Bogotá D.C.
2024

Índice

Índice e índice de tablas y figuras

Introducción

Enfrentando los desafíos éticos y legales de la inteligencia artificial en la medicina: Un modelo de gestión para la protección de datos en Colombia

Este proyecto se propone examinar de manera objetiva los nuevos retos que presenta la protección de datos personales y su legislación en el contexto del uso de la inteligencia artificial (IA) en los ámbitos de la medicina y la bioética. Se hace hincapié en el hecho de que las nuevas tecnologías de la información y la comunicación (TIC) administrados en la prestación de servicios de Salud que, por medio de la recopilación de información en la historia clínica, generan un sinfín de accesos a datos por parte de terceros, lo que podría poner en riesgo los derechos fundamentales de las personas.

En primer lugar, se presenta un resumen conciso de los conceptos actuales relacionados con la IA, seguido de un análisis crítico que resalta la urgencia de que en Colombia se legisle sobre su uso.

El objetivo final del proyecto es diseñar un modelo de gestión para la protección de datos personales en la prestación de servicios de salud que utilicen IA en Colombia. Este modelo se basará en la normativa vigente referente a la protección de datos personales y la historia clínica en Colombia, así como en las mejores prácticas.

Contextualización

En Colombia, la ley contempla que los datos personales son cualquier información relacionada con una persona, ahora refiriéndonos a la definición de persona, según el Código Civil Colombiano son

personas: *"Todos los individuos de la especie humana, cualquiera que sea su edad, sexo, estirpe o condición"* (Art. 74).

La Superintendencia de Industria y Comercio complementa esta definición, precisando en el artículo publicado en la página web "*Sobre la protección de datos personales",* que los datos personales son aquellos que permiten identificar a una persona:

> Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos. (Superintendencia de Industria y Comercio, 2024, abril 10).

La protección de datos personales se encuentra reconocida en la Constitución Política de Colombia y en la Ley 1581 de 2012 donde se establece el marco legal para la protección de datos personales en Colombia, siendo este el derecho fundamental que tienen las personas a controlar cómo se recopilan, usan, almacenan y divulgan sus datos personales.

Los datos de salud, por su naturaleza íntima y personal, refieren que la protección de datos personales requieres un especial cuidado en su tratamiento representado un reto importante en la prestación de servicios de salud con el uso de la IA. Como se ha referido anteriormente, los datos de la salud de la persona son especialmente sensibles, garantizar la protección de estos datos es una responsabilidad crucial e indelegable por parte de los prestadores de servicios de salud con la información de sus pacientes cuando utilizan la IA.

El uso de IA en los servicios médicos es un tema muy poco abordado en Colombia, pese a la coyuntura actual y los cambios de gobierno que vivimos, el sistema de salud se encuentra en un alto grado de incertidumbre por las amplias reformas que se han empezado a discutir al interior del país, si bien el clamor por un cambio en el sistema de salud es cada vez más sonoro, tras años de deterioro en la calidad de la atención, la liquidación de varias de las EPS más grandes con presencia en el territorio, clínicas, hospitales y demás prestadores de servicios, el gobierno ha olvidado dar una mirada a los cambios que trae el uso de nuevas tecnologías y la inminente necesidad de implementación que se requiere.

Según el Registro Especial de Prestadores de Servicios de Salud - REPS, con corte a abril de 2024, existen alrededor de 11.389 Instituciones Prestadoras de Servicios de Salud (IPS) habilitadas para operar en el territorio nacional, y más de 48.000 profesionales independientes también habilitados y que desempeñan sus labores en este sector.

En Colombia, no existe un registro centralizado de las demandas por errores en el tratamiento de datos personales. Sin embargo, según las cifras reportadas por la Superintendencia de Industria y Comercio entre los años 2018 al 2022, se recibieron 63.830 quejas ciudadanas, se impusieron 368 multas y emitieron alrededor de 5.502 órdenes administrativas. En su publicación del NotiSIC, indican que se reciben *"Más de 2.300 quejas al mes recibe la Superintendencia de Industria y Comercio por temas relacionados con infracciones al régimen de protección de datos personales"*. (Superintendencia de Industria y Comercio, enero 2024).

La Corte Suprema de Colombia ha reconocido, en varias sentencias, el derecho a la protección de datos personales. Además, ha ordenado a las entidades responsables del tratamiento de datos personales compensar económicamente a las personas afectadas por el manejo indebido de su información. No

estando tan lejos, en 2023 el país sufrió un hackeo en las bases de datos de varias de las entidades del estado, según lo informado por el periódico EL País, en dentro de las principales afectadas se encontraban *"la rama Judicial, el Ministerio de Salud, la Superintendencia de Industria y Comercio y la Superintendencia de Salud"*. (Ownby R. El País, 2023)

En otros países de la Unión Europea ya se ha advertido de ello, Para Ramón Fernández:

> Otro de los aspectos que hemos analizado es la vinculación de la inteligencia artificial con el big data. La minería de datos que se genera con los datos masivos y el empleo de los algoritmos plantea un reto entorno a la privacidad que la doctrina ya ha puesto de manifiesto (Castellanos Claramunt, 2020: 61). Es por ello por lo que la normativa también tiene que adaptarse a dicha circunstancia y tener en cuenta las aplicaciones de móviles y programas informáticos en el ámbito de la salud, la utilización de datos personales y el respeto a los derechos fundamentales. (Ramón Fernández, F. 2021: 329-351)

Es inminente que se considere desde ya la llegada de nuevas tecnologías que, aunque ya hace varios años existen, no han sido del todo implementadas en la prestación de los servicios de la salud ofertados en Colombia, quizás por negligencia, por desconocimiento e incluso por falta de interés de los actores (socios, dueños, inversionistas) en acceder a estas tecnologías que mejoran notablemente la calidad de los servicios prestados.

Sin descuidar los retos que trae ello consigo, la privacidad y protección de la información, el uso responsable y adecuado de la misma, la necesidad de crear y regular todos estos aspectos que son tan necesarios para que su uso no genere riesgos significativos para la sociedad y sobre todo para los usuarios del sistema de salud.

A partir de lo anterior, se hace evidente la necesidad de crear un modelo que aborde las deficiencias normativas en Colombia relacionadas con la prestación de servicios de salud utilizando Inteligencia Artificial. Este modelo servirá como marco para desarrollar soluciones a dicha problemática. Por ello se ha planteado la siguiente pregunta del problema de investigación y los objetivos definidos para el diseño del modelo planteado: **¿De qué manera logramos proteger los datos personales de los Colombianos en el uso de la inteligencia artificial en la prestación de servicios de salud?.** Planteada la misma, se propone entonces el diseño de un modelo que se desarrollará conforme los objetivos planteados a continuación:

Objetivo General

Diseñar un modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia.

Objetivos Específicos

- Enmarcar los principales fundamentos teóricos sobre el uso de la inteligencia artificial en la prestación de servicios de salud en Colombia.

- Establecer un marco legal y normativo para la protección de datos personales en Colombia referentes a la historia clínica de las personas que acceden a la prestación de servicios de salud con IA.
- Definir los datos o información sensible contenidos en la historia clínica de las personas que acceden a la prestación de servicios de salud con IA.

- Documentar el modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia.

Capítulo I: DESCRIPCIÓN DEL PROYECTO

Antecedentes de Investigación

Para empezar, es importante conocer la definición de IA pero en este caso no desde un enfoque tecnológico, más bien desde una visión legal del término, definiéndola como *"en el campo jurídico no hay una definición concreta en razón de que la IA tiene múltiples aplicaciones por especialidad, las principales aplicaciones son: 1. Argumentación y la toma de decisiones, 2.clasificación y extracción de textos jurídicos (jurisprudencia, doctrina y normativa), 3. constitución y proyección de un sistema legislativo"*. (Rissland, Ashley, & Loui, 2003, citado por Guerrero, Pag 4, 2021).

Para Vill alba Gómez (2016) la dinámica del crecimiento en la construcción tecnocientífica alrededor de la ampliación de las capacidades humanas, entendidas estas mediante la generación, construcción e implementación de inteligencia artificial o enfoques biotecnológicos en robótica y sistemas expertos, se convierten en el escenario emergente de análisis y reflexión filosófica, para que la bioética (mediante la germinación de un contexto propio enmarcado en una bioética de la tecnología) sea la llamada a identificar y analizar, desde la protección de la vida humana, los posibles juzgamientos éticos que se puedan presentar en la conjunción de esta dinámica.

El uso de las Nuevas Tecnologías por parte de todos los que tenemos acceso a ellas, crea un panorama diferente de lo que podemos concebir como realidad, para Rolando V, Jiménez Domínguez y Onofre Rojo A.:

> No se podrá negar que la ciencia y la tecnología han contribuido enormemente para mejorar la vida de los seres humanos, pero si se analizan estos resultados en el sentir y humor de la gente pareciera que no todo ha sido para felicidad humana. Los valores y metas de la sociedad postindustrial difieren notablemente de los de hace dos o tres generaciones, estableciéndose la "brecha generacional" con muy poca comunicación por lo que respecta a los valores. La nueva cultura con base tecnológica está para quedarse y avanzar del lado técnico. Los que han probado alguna vez el desarrollo tecnológico tardan en reaccionar ante sus otras consecuencias. (2008)

En pocas palabras, el panorama de la realidad en la que vivimos conectados en la actualidad, las facilidades de acceso a la información por parte de algunos, todo aquello que nos brindan las tecnologías y las comunicaciones, han dejado como resultado un cambio social y ético en la forma en cómo nos relacionamos con los demás, pero también en el uso de la información que puedan contener, conservar, generar o analizas dichas “nuevas tecnologías”.

Se observa cada día que, con la llegada de la era tecnológica y las comunicaciones, las nuevas generaciones cada vez tienen un mayor acceso a un sin número de datos en tiempo real (información) que genera a su vez un gran riesgo pues en su mayoría, no tenemos certeza de que la fuente de dicha información cumpla con estándares de confiabilidad y protección, es decir, que su uso no genere un daño directo (uso propio) o indirecto (vulnerar la información de otros).

Garzón Fierro, V. (2020), en su tesis sobre La inteligencia artificial en Colombia, plantea un reto muy contundente para el panorama jurídico pues es a todas luces una realidad, identificando como desafío “la falta de comprensión de las formas legales por parte de los titulares del dato. En este sentido, se presentan situaciones en donde los titulares otorgan la autorización al tratamiento de datos

sin entender cuál es el alcance de la misma.”. Cuantas personas no firman en señal de aceptación un documento referente al tratamiento de los datos personales desconociendo totalmente el contenido de este.

Tal como se ha venido abordando en los párrafos anteriores, cada día se hacen más necesarias las regulaciones frente al uso de la información, situación que resuena en países europeos como se destaca en la denominada Declaración de Barcelona para la Inteligencia Artificial que fue elaborada por un grupo de expertos en inteligencia artificial (IA) que establece un conjunto de principios y recomendaciones para el desarrollo y uso responsable de la IA en Europa:

> El documento destaca la gran importancia de la IA en el devenir de la economía y de las sociedades, si bien también muestra su inquietud por el posible uso inapropiado, precipitado o doloso de las nuevas tecnologías. En este sentido, plantea un código de conducta centrado en la cautela, la confianza, la transparencia, la rendición de cuentas, la limitación de la autonomía y el rol humano. (International Center for Scientific Debate Barcelona, 2017, citado por Gerrero Arevalo, Pag 13, 2021).

Guerrero Arévalo finiquita su escrito indicando que:

> Ha presentado una visión general de cómo la inteligencia artificial va a influir en muchos aspectos de la vida cotidiana y su puesta en práctica debe ser reglamentada a través de un parámetro normativo fundamentado en los principios éticos que tienen por objeto la tutela de los derechos humanos fundamentales, y con ello prevenir la posibilidad de que su acelerado avance pueda generar un riesgo a la población por la excesiva dependencia que existe hacia estos sistemas de carácter autónomo, por lo que mediante un adecuado ejercicio de precaución y responsabilidad, podrá generarse la conciencia necesaria respecto del poder de la inteligencia artificial y de sus inesperadas consecuencias. (Gerrero Arevalo, Pag 19, 2021)

Ratificando con esto la necesidad que vemos muchos de los profesionales en Colombia de estar preparados para los nuevos cambios, y que los mismos no deben ser tratados de una forma interdisciplinar para ser afrontados en debida forma.

La legislación Colombiana considera en Ley de Protección de Datos Personales o Ley 1581 de 2012 tiene por Objeto: *"desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"*. (Art. 1)

Existen diversos intentos por parte de la administración pública que han removido o generado normativas y regulaciones generales respecto del uso de las nuevas tecnologías, Ospina, M. R., y Zambrano, K.J. (2023) en su artículo Gobierno digital e inteligencia artificial, una mirada al caso colombiano, realizan una importante reunión de todo este marco normativo y regulatorio que se ha adelantado al interior de las entidades de gobierno con el fin de enmarcar la implementación de la IA en el territorio colombiano de una forma segura desde el punto de vista legal, y sin dejar los derechos de las personas.

Como parte de las conclusiones emitidas en su artículo, Ospina, M. R., y Zambrano, K.J. indican que:

> El Estado colombiano, ha venido evolucionando en sus modelos de gestión pública acorde con las tendencias, necesidades sociales y voluntades políticas de sus gobernantes, por ejemplo, actualmente las entidades públicas operan con el MIPG (Modelo Integrado de Planeación y

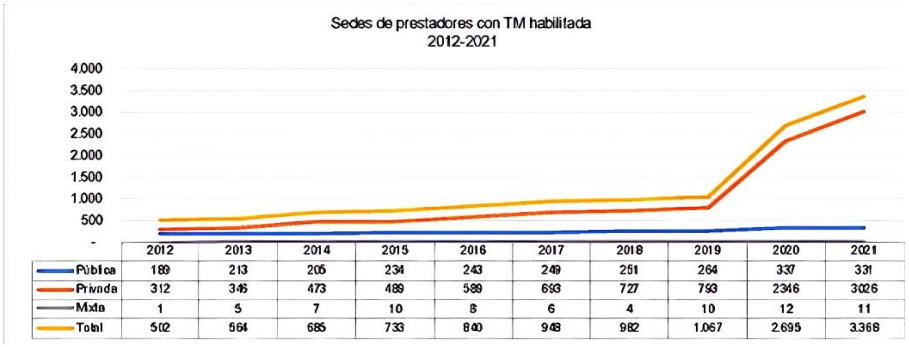
> Gestión), así mismo, se ha pasado de un enfoque de gobierno electrónico a una política de gobierno digital, sin embargo, hay asimetrías en esta transformación digital entre las diferentes entidades tanto del orden nacional como territorial. (2023)

Lo anterior como preámbulo legal para ser considerado, si bien se ha venido describiendo una serie de argumentos y premisas frente al uso de las nuevas tecnologías, la salud, el acceso a la información, todo ellos para llegar al punto de hablar sobre qué puede pasar cuando en Colombia empecemos a implementar el uso de nuevas tecnologías e inteligencia artificial en la prestación de servicios de salud, ¿qué garantías tienen los pacientes sobre el uso de su información personal? ¿quién va a poder tener accesos a esta información? ¿de qué forma se va a custodiar y quién va a responder en un caso de filtración de datos? estas y muchas otras preguntas son las que debemos considerar con el fin de regular todos estos temas que son tan novedosos para países como el nuestro.

En los últimos años, diversas empresas del sector salud han tenido acercamiento con la inteligencia artificial y el internet de las cosas, está claro que es una tecnología que llegó para quedarse, esto a pasos acelerados en el sector de la Salud.

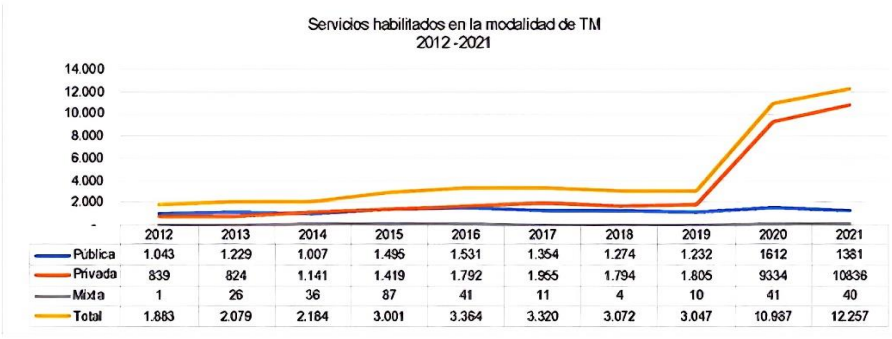
Con el paso de la última pandemia que vivió el país con el COVID-19 que generó un estado de emergencia sanitaria y que trajo consigo la aceleración del uso de nuevas tecnologías y un acceso general a servicios como la Telemedicina, de acuerdo con el boletín de prensa No 203 de 2022 emitido por el Ministerio de Salud, "*entre diciembre de 2020 y diciembre de 2021, se observó incremento de la oferta de servicios habilitada en la modalidad de telemedicina, 25 % en las sedes de prestadores que ofrecen TM y 12 % en los servicios habilitados"*. (2022)

Tabla 1.



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Pública	189	213	205	234	243	249	251	264	337	331
Privada	312	346	473	489	589	693	727	793	2346	3026
Mixta	1	5	7	10	8	6	4	10	12	11
Total	502	564	685	733	840	948	982	1.067	2.695	3.368

Tabla 2.



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Pública	1.043	1.229	1.007	1.495	1.531	1.354	1.274	1.232	1612	1381
Privada	839	824	1.141	1.419	1.792	1.955	1.794	1.805	9334	10836
Mixta	1	26	36	87	41	11	4	10	41	40
Total	1.883	2.079	2.184	3.001	3.364	3.320	3.072	3.047	10.987	12.257

Fuente: Registro Especial de Prestadores de Servicios de Salud diciembre 31 de 2021

Figura 1. Estadísticas telemedicina pos-COVID

(recuperado de https://www.minsalud.gov.co/Paginas/Dos-anos-de-posicionamiento-de-la-telemedicina-en-Colombia.aspx)

Vesga Ferreira, J. C.; Contreras Higuera, M. F.; Vesga Barrera, J. A. (2021), concluyeron que:

> La convergencia de la telemedicina y del Internet de las cosas (IoT), junto con los nuevos paradigmas que demanda el sector salud y el mundo globalizado, han abierto todo un panorama de retos para la investigación en diferentes áreas del conocimiento. Sin embargo, la falta de estándares relacionados con el desarrollo de soluciones y las restricciones desde el punto de vista normativo en Colombia, se han convertido en un obstáculo para avanzar libremente en el campo de telemedicina y la prestación de servicios. (Pag 15, 2021)

Teniendo en cuenta lo anterior, y evidenciando los diversos retos y oportunidades que enfrentan las entidades que prestan servicios de salud al interior del territorio colombiano, son muchas las necesidades que sales a la luz en materia de regulación o incluso de estandarización de procesos.

En el trabajo desarrollado por Alfaro Orozco, Z. y Suarez Ramírez, C. sobre la empresa SENTECOL S.A., que tiene como objetivo "*Proponer un modelo de negocio basado en herramientas tecnológicas en inteligencia artificial (IA) para la óptima trasmisión de información entre instituciones prestadoras de servicio de salud y sus usuarios durante los procesos de agendamiento, confirmación y seguimiento de citas médicas"* (Pag 21, 2023), se da cuenta del uso de inteligencia artificial basado en Machine Learning, sistema que en todo caso se evidencia hace uso de datos personales para la administración de la información objetivo.

Habiendo referenciado lo anterior, se da muestra que en diversos temas del sector salud, se han venido adelantando desarrollos, actividades e investigaciones que dan cuenta de la disposición y necesidad que se tiene en el uso de inteligencia artificial en diversos procesos del sector y por supuesto es claro que en la prestación de servicios es inminente su uso.

Ahora, haciendo referencia a uno de los documentos que mayor cantidad de información sensible contienen y que es generado por la prestación de servicios de salud es la Historia Clínica, Rojas Camargo, la resume en investigación como "*uno de los pilares fundamentales, en el sistema de información en salud en nuestro país y además la importancia que tiene esta al ser electrónica, en la identificación de las patologías, la evolución y tratamiento que se brinda a los pacientes en las instituciones de salud"*. (2021)

Contreras, A., hace un Marco normativo de la historia clínica electrónica y su incidencia en el ámbito de la protección de datos personales en Colombia, en el que define:

> La historia clínica uno de los principales insumos con los que cuentan los profesionales de la salud para la prestación adecuada del servicio, está en condiciones de adecuar su presentación al uso de las nuevas tecnologías, aprovechando las ventajas que brindan los sistemas de información, entre estos, la confidencialidad e integridad de los datos contenidos en el historial médico-asistencial de los pacientes, no solo para conseguir una mayor eficacia sino también para preservar y garantizar derechos fundamentales de los titulares de los datos, tales como el derecho a la salud, el derecho a la intimidad y el habeas data. (Pag 112, 2020)

Con respecto a los datos personales, "*La Historia Clínica está conformada por datos de información personal (nombre y apellidos, dirección, teléfono, documento nacional de identidad, número de tarjeta sanitaria, etc.) y datos de salud (pruebas diagnósticas, cirugías, medicamentos, etc.) No se puede concebir una historia clínica sin tener en cuenta los datos. La Historia Clínica Electrónica (HCE) debe ser proactiva, más inteligente, con una interfaz amigable e intuitiva que asegure la confidencialidad y seguridad de la información"*. (Medinaceli Díaz, Silva Choque. 2021. Impacto y regulación de la Inteligencia Artificial en el ámbito sanitario)

Bajo las perspectivas expuestas, se tiene que la IA (Inteligencia Artificial) está revolucionando el sector de la salud, sin embargo, el uso de datos personales en los sistemas de IA plantea importantes desafíos éticos y legales, especialmente en lo que respecta a la protección de la privacidad usada en la prestación de servicios de salud que comprende del uso de los datos personales para su alimentación o funcionamiento principalmente contenidos en la historia clínica.

Dado lo expuesto anteriormente, se hace imprescindible establecer un mecanismo o modelo de gestión que ajuste los procedimientos y la información de tal manera que asegure la forma de mantener protegidos los datos personales de los pacientes, las principales responsabilidades de los actores dentro del proceso y que a su vez brinde mecanismos de garantía mínimos de los derechos de los titulares de los datos; teniendo presente que se trata de información y datos sensibles que requieres un alto nivel de confidencialidad debido que revelan el estado de salud de los pacientes y que su uso indebido puede generar consecuencias catastróficas para los titulares como la discriminación, el robo de identidad e incluso hasta fraude.

Capítulo II: METODOLOGÍA

Estrategia General

Se realizará mediante un enfoque cualitativo, recopilando información por medio de la revisión de literatura y el análisis de documentos, en 2 fases:

1. Diagnóstico de la situación actual
2. Diseño del modelo de gestión

En la siguiente estructura de desglose del trabajo EDT, se definen las actividades principales para el cumplimiento de los objetivos definidos:

EDT	Diseñar un modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia
1	Diagnóstico de la situación actual

EDT	Diseñar un modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia
1.1	**Enmarcar los principales fundamentos teóricos sobre el uso de la inteligencia artificial en la prestación de servicios de salud en Colombia**
1.1.1	Revisar el concepto de inteligencia artificial y sus aplicaciones en el sector salud.
1.1.2	Analizar los beneficios y riesgos del uso de IA en la prestación de servicios de salud
1.1.3	Identificar los desafíos éticos y legales del uso de IA en la prestación de servicios de salud
1.2	**Establecer un marco legal y normativo para la protección de datos personales en Colombia referentes a la historia clínica de las personas que acceden a la prestación de servicios de salud con IA**
1.2.1	Reunir el marco normativo de protección y tratamiento de datos personales den Colombia
1.2.2	Analizar los principios rectores de la protección de datos personales en el contexto de la IA
1.2.3	Determinar las obligaciones de los prestadores de servicios de salud en materia de protección de datos personales
2	**Diseño del modelo de gestión**
2.1	**Definir los datos o información sensible contenidos en la historia clínica de las personas que acceden a la prestación de servicios de salud con IA**
2.1.1	Clasificar los tipos de datos personales presentes en la historia clínica
2.1.2	Identificar los datos sensibles que requieren un mayor nivel de protección
2.1.3	Establecer criterios para el tratamiento de datos sensibles en la prestación de servicios de salud con IA
2.2	**Documentar el modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia**
2.2.1	Establecer procedimientos claros y accesibles para que los titulares de datos personales puedan ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad
2.2.2	Definir como se informa a los titulares de datos personales sobre sus derechos y la forma de ejercerlos
2.2.3	Definir la política de tratamiento de datos personales sugerida en contexto con la prestación de servicios de salud con IA

Tabla 1. EDT del proyecto
Fuente de Elaboración Propia

En el presente trabajo también se ejecuta una investigación exploratoria, logrando determinar que no se han efectuado investigaciones anteriores sobre el tratamiento de los datos personales en la prestación de servicios de salud en Colombia que hubiese derivado un modelo como el propuesto.

De igual forma se emplea un método que parte de lo concreto que en este caso sería la protección de los datos personales, para llegar a conclusiones más amplias con un modelo general como el que se plantea en la presente investigación. Esto significa que primero se examinan detenidamente las causas específicas que conducen al problema de investigación. Se analizan los detalles y particularidades para comprender a fondo cómo surge el problema y cuáles son sus implicaciones en un contexto específico, en este caso, la protección de datos personales en los servicios de salud con inteligencia artificial en Colombia.

En resumen, este método inductivo-deductivo permite una comprensión profunda y completa del problema de investigación, desde sus causas específicas hasta sus implicaciones generales y su aplicación en el diseño del modelo propuesto.

Participantes

Para la Ejecución de la presente investigación, participan Andrés Fabian Rodríguez Peña y Brayan Andrés Tafur Pabón como Coinvestigadores y Ejecutores del proyecto con el fin de lograr el diseño del modelo propuesto.

Técnicas o estrategias de recolección de información

De conformidad con el alcance de los objetivos y la delimitación de actividades realizada en cada una de las fases determinadas para el diseño del modelo de gestión propuesto, se proponen 3 estrategias:

La primera se concentra en la Revisión de Literatura principalmente enfocada a la protección de datos personales en el sector de la salud, para ellos se estudiaron diversas fuentes como artículos de estudio, libros, informes y otros documentos o fuentes que develan la información requerida respecto del tema concreto sobre la protección de datos, inteligencia artificial y los servicios de salud con el fin de obtener un estado del arte que brinde un panorama general para la propuesta del modelo.

La segunda enfocada a la revisión y análisis de sitios web de algunas instituciones prestadoras de servicios de salud, así como de entidades gubernamentales en Colombia tanto en el sector de la salud como del sector de industria y comercio, siento estos últimos quienes brindan pautas importantes para el desarrollo de los procesos de tratamiento de datos, con el fin de identificar la políticas y mejores prácticas aplicables a la protección de datos en la prestación de servicios de salud con inteligencia artificial.

Por último, dar una revisión de las leyes y normas vigentes que regulan la materia de protección de datos personales, información sensible e historia clínica en Colombia, con el fin de fortalecer el modelo propuesto con el sustento legal adecuado y poder determinar partiendo de esto, las obligaciones y derechos de las diferentes involucradas en el proceso.

Técnicas o estrategias de organización de la información recolectada

Con el fin de abordar el desarrollo de las actividades delimitadas en al EDT del proyecto, se realizará la creación de una matriz de datos que se consolidará en el desarrollo de cada uno de los puntos, esto con el fin de tener un índice durante el desarrollo de la investigación y el diseño de la propuesta siendo herramienta fundamental de uso interno de los investigadores, incluyendo la fuente (Literaria, Sitios Web, Legal), la fecha de recolección y la dirección de acceso para su consulta.

Así mismo, se plantea la elaboración de fichas resumen para uso interno que permitan sintetizar la información contenida en las fuentes recolectadas, destacando los hallazgos y las conclusiones que son instrumento importante para la construcción del marco referencial del proyecto. Y la construcción en este mismo sentido de una matriz que contenga las principales leyes y normativas aplicables en Colombia referentes al tratamiento de datos personales y en conexidad con esto la historia clínica asumiendo que en esta última se concentran los datos recolectados de los pacientes que asisten a la prestación de servicios de salud con inteligencia artificial.

Técnicas o estrategias de análisis de la información recolectada

La propuesta del modelo de gestión está planteada para desarrollase desde el análisis ético y técnico desde el punto de vista legal sobre las implicaciones que tiene el uso de la inteligencia artificial con un enfoque especial en lo que puede suceder con los datos de los pacientes que se generan, administran y almacenan por medio del uso de estas nuevas tecnologías dando especial énfasis en la protección de esos datos sensibles y el impacto que puede generar su uso.

Metodología aspectos éticos

La presente investigación ha tenido en cuenta estudios: teorías, conceptos, imágenes y gráficos por diferentes autores; debido a ello cada una de las citas posee su referencia bibliográfica redactada según la norma APA. La información o referencias tomadas han sido usadas de manera honesta y transparente, sin manipular o falsificar datos.

En el desarrollo, tanto el tutor de la asignatura como los investigadores desarrollaron sus actividades de forma independiente y con respetos hacia las consideraciones del otro dentro de un entorno colaborativo. No se ejecutaron actividades que afectaran la integridad de los participantes de la investigación, así como tampoco la intervención de otros procedimientos en organismos vivos.

En cuanto al material de estudio, fue tomado de fuentes digitales en las que se encuentra conservado, sin la generación de desechos y aplicando la iniciativa de **cero papel** que contribuye con la protección del medio ambiente.

Capítulo III: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

3.1 Principales fundamentos teóricos sobre el uso de la inteligencia artificial en la prestación de servicios de salud en Colombia

3.1.1 Revisar el concepto de inteligencia artificial y sus aplicaciones en el sector salud

En esta sección, se realiza una revisión bibliográfica más detallada y se amplía el análisis de los fundamentos teóricos que sustentan el concepto de la inteligencia artificial (IA) ya referidos en el

marco teórico del proyecto, enfocándolos en el ámbito de la salud en Colombia. Para ello, se han consultado fuentes adicionales, entre las que se destacan:

- Ministerio de Salud y Protección Social de Colombia (2020). Estrategia Nacional de Salud Digital 2020-2024.
- Organización Mundial de la Salud (OMS) (2023). La OMS esboza las cuestiones que cabe tener en cuenta a fin de regular la inteligencia artificial para la salud
- Zabala Leal, T y Zuluaga Ortiz, P. (2021). Los retos jurídicos de la inteligencia artificial en el derecho en Colombia

Con base en la revisión bibliográfica extendida, se propone una definición la Inteligencia Artificial (IA) en el contexto de la salud como el uso de los sistemas información para replicar la inteligencia humana en el ámbito de la atención médica, incluyendo el análisis de datos, el diagnóstico de enfermedades, la sugerencia de decisiones clínicas y la creación de nuevas tecnologías para mejorar la salud y el bienestar de los pacientes.

Del mismo modo, se desarrollan algunas de las principales aplicaciones de la inteligencia artificial en la prestación de servicios de salud:

- En los servicios de Diagnóstico médico, en especial en cuanto al análisis de imágenes diagnosticas (tomografías, radiografías, etc.) contribuyendo en el apoyo diagnóstico a los profesionales de la salud con la detección de anomalías y/o enfermedades con una mayor precisión y rapidez.
- En cuanto a los servicios de Telemedicina en conde es posible el desarrollo e implementación de servicios para la atención médica de forma remota.

- En la prestación de servicios por medio de Asistentes virtuales para pacientes, por medio de la creación y uso de chat-bots, asistentes virtuales, u otras herramientas con el fin de resolver preguntas básicas de los pacientes e incluso extender su uso para la programación de citas médicas y otros servicios de salud.
- En la revisión y análisis de datos de salud, permitiendo con el uso de IA el desarrollo y uso de herramientas que analicen grandes volúmenes o conjuntos de datos para identificar patrones, tendencias y aumentar incluso la comprensión de enfermedades.
- En el desarrollo de fármacos, el uso de algoritmos y sistemas con inteligencia artificial pueden ser una herramienta importante a la hora de producir nuevos medicamentos, con un amplio panorama técnico en el que se puede incluir la identificación de todos sus compuestos, la predicción de su eficacia, y la correlación con historiales de tratamientos y resultados documentados con su uso.

De conformidad con el concepto de inteligencia artificial sugerido, una vez profundizado el mismo y las los principales usos o aplicaciones de estas nuevas tecnologías, centrándonos específicamente en el contexto colombiano, dentro de las cuales se logró identificar el amplio potencial que trae el uso de IA que incluso se puede correlacionar directamente con la mejora en la eficiencia, la precisión y la accesibilidad de la prestación de los servicios de salud en Colombia.

3.1.2 Analizar los beneficios y riesgos del uso de IA en la prestación de servicios de salud

Es claro en este punto que el uso de nuevas tecnologías está en auge, en especial es uso de Inteligencia Artificial (IA), en el campo de la salud dichas tecnologías están revolucionando, ofreciendo alternativas o herramientas para el diagnóstico, tratamiento y seguimiento de pacientes. Sin embargo, como todo lo novedoso, es necesario considerar que su implementación puede conlleva tanto

beneficios como riesgos, siendo de gran importancia darle una continua evaluación y seguimiento de preferencia bajos los principios del PHVA (Planear, Hacer, Verificar, Actuar) con el fin de que sean gestionados de la mejor forma, y de la mitigación adecuada de su materialización.

Surtidas las definiciones anteriores y la ampliación de los contextos literarios, se procede a realizar la respectiva argumentación de los posibles beneficios y riesgos del uso de la IA en el sector salud:

Beneficios:

- Mejora de la precisión diagnóstica: el uso de inteligencia artificial en los procesos de diagnóstico puede apoyar al personal de la salud en el diagnóstico de enfermedades con un mayor nivel de precisión y rapidez teniendo la oportunidad de procesar mayores cantidades de datos médicos, historial de los pacientes, correlación de diagnósticos similares, entre otros.
- Personalización de la atención médica: estas nuevas tecnologías permiten el desarrollo de algoritmos y procedimientos de análisis que consideren el historial del paciente, permitiendo una prestación del servicio más personalizada considerando además de esto otros factores de correlación con patrones o diagnósticos similares y la creación de tratamiento personalizados.
- Mejora del acceso a la atención médica: con el apoyo de la inteligencia artificial, puede ampliarse el espectro de cobertura incluso a lugares remotos o con acceso limitado a la atención médica tradicional, mejorando así la calidad y eficiencia de los servicios de atención en salud.

- Reducción de costos: con la IA es posible administrar de forma adecuada los posibles costos de atención médica al mejorar la eficiencia de los servicios prestados y encaminar los mismos a la prevención enfermedades, además de significar un soporte en la gestión de los recursos que intervienen en la prestación del servicio de salud, la planificación de cirugías y demás tratamientos.

Riesgos:

- Sesgos algorítmicos: el uso de sistemas basados en IA, puede en determinado punto pueden verse afectados seriamente por los sesgos existentes en los datos con los que los alimentan, siendo la fuente de información para el apoyo que brinda esta tecnología en la prestación del servicio, lo que puede implicar un mayor riesgo en la definición de diagnósticos y tratamientos.
- Falta de transparencia: a menudo, estas nuevas tecnologías se basan en desarrollos robustos o complejos que puede dificultar tanto a los usuarios (personal de la salud), como a los desarrolladores la adecuada gestión de estos afectando en gran medida la toma de decisiones durante la prestación de los servicios de salud.
- Preocupaciones éticas: en cuando al uso de la IA en la prestación de los servicios de salud, varios autores ha expresado su alto grado de preocupación a nivel ético, como el alto potencial de deshumanización de la atención médica e incluso la posible pérdida de autonomía del paciente em cuanto a las decisiones que pueda tomar este en especial en la aceptación de tratamiento.
- **Privacidad y seguridad de los datos**: en cuanto a los datos, es importante establecer que todos los sistemas de información son vulnerables a ataques cibernéticos, esto no excluye

en todo caso a sistemas que hagan uso de la Inteligencia Artificial durante su ejecución, significando esto que existe un riesgo de acceso no autorizado y/o uso indebido de la información personal de salud de los pacientes. Es por esto que juega un papel fundamental el diseño, desarrollo, ejecución, evaluación y adaptación de mecanismos que garanticen en gran medida la protección de estos datos debido a su naturaleza sensible.

Es esencial adoptar un enfoque equilibrado y responsable al implementar la inteligencia artificial (IA) en el ámbito de la salud en Colombia, por ellos anteriormente se reconocen algunos de sus posibles beneficios como los riesgos asociados. Mantener la transparencia en los procesos de toma de decisiones, proteger la privacidad de los datos, fomentar la ética en el desarrollo y uso de la IA, y mantener una vigilancia constante sobre posibles riesgos, son elementos cruciales para asegurar que la IA se convierta en una herramienta poderosa para mejorar la prestación de servicios de salud y el bienestar de las personas, sin comprometer los principios éticos, la calidad de la atención y la protección de los datos de los pacientes.

3.1.3 Identificar los desafíos éticos y legales del uso de IA en la prestación de servicios de salud

Abarcados los puntos anteriores, no dejando pasar por alto que uno de los principales riesgos definidos está relacionado con la Privacidad y seguridad de los datos, se evaluaron la existencia de leyes y normativas nacionales relacionadas con la protección de datos personales y el uso de inteligencia artificial en el ámbito de la salud, también se examinaron las implicaciones éticas asociadas con el empleo de inteligencia artificial en la atención médica.

Desafíos éticos:

- Privacidad: La inteligencia artificial depende de grandes volúmenes de datos personales, lo que genera inquietudes sobre la privacidad y la seguridad de dicha información.
- Consentimiento informado: Es esencial obtener el consentimiento informado de los pacientes antes de utilizar sus datos en sistemas de inteligencia artificial, **asegurando que los pacientes comprendan y aprueben el uso de su información**.
- Autonomía del paciente: La inteligencia artificial no debe emplearse para tomar decisiones que sustituyan la autonomía del paciente.
- Equidad: La IA debe usarse de manera que sea justa y equitativa para todos los pacientes, independientemente de su origen o condición socioeconómica, esto queriendo decir que debe guardar un principio de la salud que trata de la universalidad en el acceso.
- Responsabilidad profesional: Se deben establecer mecanismos claros para determinar la responsabilidad en caso de que un sistema de IA sugiera una decisión que cause daño a un paciente.

Desafíos legales:

- Marco regulatorio: es necesario realizar una revisión y adecuación de los marcos regulatorios, con el fin de que los mismos sean claros y permitan garantizar el adecuado uso de la inteligencia artificial en la prestación de servicios de salud, sin dejar a un lado los aspectos bioéticos que se deban contemplar. Es por ello tan necesaria una supervisión estricta por parte del gobierno, y de los entes de tanto regulatorios como de control para

garantizar que los sistemas de IA usados en la prestación de servicios de salud se implementen y utilicen respetando las normas y lineamientos aplicables.

- Protección de datos: se hace fundamental la implementación de medidas robustas que protejan la confidencialidad e integridad de los datos de salud de los pacientes, ellos con el fin de garantizando los derechos de los titulares de los datos en cuanto a su uso responsable y ético en el ámbito de la atención en salud basados en leyes y regulaciones aplicables relacionadas con la privacidad y protección de los datos.
- Acceso a los datos: es deber de los intervinientes en el proceso de prestación de servicios, en especial de los proveedores de servicios de salud, el establecer mecanismos que ofrezcan a los investigadores y/o desarrolladores de tecnologías basadas en inteligencia artificial aplicada a los servicios de la salud para que tengan acceso a los datos necesarios, confiables y que le probar sus sistemas de manera responsable, protegiendo siempre los titulares de los datos (pacientes) y demás información sensible.

Habiendo ampliado la revisión bibliográfica y el análisis realizado, cada vez se itera sobre la gran necesidad de establecer procesos, procedimientos y un marco normativo específico que aborde los desafíos éticos y legales que puede presentar el uso de la inteligencia artificial en la prestación de servicios de salud en Colombia. En otros lugares como los países europeos, se ha logrado basándose en diversas recomendaciones y desarrollos por parte de expertos en la materia junto que demuestran el papel fundamental que significa proteger los derechos de los pacientes y garantizar una implementación segura y ética de esta tecnología en el sector salud, lo que pone de manifiesto la urgencia de regular de forma específica para el sector su uso en Colombia.

3.2 Establecer un marco legal y normativo para la protección de datos personales en Colombia referentes a la historia clínica de las personas que acceden a la prestación de servicios de salud con IA

3.2.1 Reunir el marco normativo de protección y tratamiento de datos personales en Colombia

Para establecer un marco legal y normativo adecuado para la protección de datos personales especialmente contenidos en la historia clínica de pacientes que acceden a servicios de salud con IA en Colombia, es fundamental comprender el contexto legal vigente en el país. A continuación, se presenta una matriz jurídica que resume las principales normas:

Norma	Descripción	Aspectos Clave
Constitución Política de Colombia	Establece los derechos fundamentales de las personas, incluyendo el derecho a la intimidad y el habeas data.	Todos los ciudadanos colombianos
Resolución 1995 de 1999	Reglamenta el manejo de la historia clínica. Establece los requisitos para su elaboración, custodia y acceso	Confidencialidad, seguridad de los datos de salud
Ley 1581 de 2012	"Ley estatutaria de protección de datos personales y habeas data". Define los principios rectores para la protección de datos personales, establece los derechos de los titulares de los datos y las obligaciones de los responsables y encargados del tratamiento de datos	Derechos de los titulares, obligaciones de los responsables del tratamiento
Decreto 1377 de 2013	Reglamenta la Ley 1581 de 2012. Establece los requisitos para el tratamiento de datos personales sensibles, incluyendo la historia clínica	Medidas de seguridad, procedimientos específicos

Norma	Descripción	Aspectos Clave
Decreto 1074 de 2015	"Decreto único reglamentario del sector de las Tecnologías de la Información y las Comunicaciones". Establece los requisitos para el tratamiento de datos personales en el ámbito de las TIC, incluyendo la seguridad de la información y la protección de datos	Medidas de seguridad, procedimientos específicos
CONPES 3975 de 2019	Transformación digital e IA	Lineamientos para el uso responsable de IA y protección de datos
Ley 1955 de 2019	Crea el Sistema Nacional de Información en Salud (SNIS). Regula el manejo de datos en salud	Prestadores de servicios de salud y entidades del sector salud
Resolución 866 de 2021	Interoperabilidad de datos clínicos	Seguridad y confidencialidad en el intercambio de datos

Tabla 2. Marco Normativo

Fuente de Elaboración Propia

Este marco fue elaborado en consonancia con la Constitución Política de Colombia, que establece los derechos fundamentales, incluyendo el derecho a la intimidad y el habeas data, partiendo de allí se relacionan entre otras, todas las normas que regulan el manejo, tratamiento y protección de los datos personales en Colombia, especialmente en el ámbito de la salud. La implementación efectiva de estas normativas garantizará la confidencialidad, seguridad y privacidad de los datos de salud de los ciudadanos colombianos, así como la promoción de un uso responsable de la IA en el sector de la salud.

3.2.2 Analizar los principios rectores de la protección de datos personales en el contexto de la IA

En el ámbito de la inteligencia artificial (IA) aplicada a la salud, la protección de datos personales adquiere una relevancia fundamental. Esta protección se debe basar en principios rectores esenciales

para garantizar el uso responsable y ético de la IA en especial con lo referente a la protección de datos personales en contexto con la normativa. Estos principios se encuentran compilados por la superintendencia de industria y comercio así:

PRINCIPIO DE LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS:

El tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen. (Superintendencia de Industria y Comercio, 2024)

PRINCIPIO DE FINALIDAD:

El tratamiento de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al Titular. (Superintendencia de Industria y Comercio, 2024)

PRINCIPIO DE LIBERTAD:

El tratamiento de datos personales solo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento. (Superintendencia de Industria y Comercio, 2024)

PRINCIPIO DE VERACIDAD O CALIDAD:

La información personal sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, en este sentido, se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. (Superintendencia de Industria y Comercio, 2024)

PRINCIPIO DE TRANSPARENCIA:

En el tratamiento de datos personales debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin

restricciones, información acerca de la existencia de datos que le conciernan. (Superintendencia de Industria y Comercio, 2024)

PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA:

El tratamiento de datos personales está sujeto a los límites que se derivan de la naturaleza de los mismos, de las disposiciones de ley y la Constitución. En este sentido, su tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en ley. En este sentido, los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la ley. (Superintendencia de Industria y Comercio, 2024)

PRINCIPIO DE SEGURIDAD:

La información personal sujeta a tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. (Superintendencia de Industria y Comercio, 2024)

PRINCIPIO DE CONFIDENCIALIDAD:

Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma. (Superintendencia de Industria y Comercio, 2024)

El análisis realizado sobre los principios rectores de protección de datos personales en el ámbito de la inteligencia artificial (IA) genera una necesidad de adherirse a estos principios fundamentales siendo pilares esenciales para garantizar que el tratamiento de datos personales en la prestación de servicios de salud con IA contenidos principalmente en los datos de la historia clínica de los pacientes para que se lleve a cabo de manera ética, legal y segura.

La implementación de la IA en el sector salud presenta desafíos únicos que exigen un enfoque riguroso de riesgos, dentro de los cuales se ha identificado como uno de los principales lo relativo a la protección de los datos personales de los pacientes. La adhesión a estos principios rectores no solo garantiza la protección de los derechos de los pacientes, sino que también asegura que el uso de la tecnología IA no comprometa la calidad de la atención médica brindada, y mitigue el riesgo latente que existe en cuando al uso de los datos de los pacientes.

Al aplicar correctamente estos principios, se puede fomentar la confianza de los pacientes en la prestación de servicios de salud con IA y promover su adopción responsable y beneficiosa para el sector salud en general.

3.2.3 Determinar las obligaciones de los prestadores de servicios de salud en materia de protección de datos personales

De conformidad con las normas y principios definidos, los prestadores de servicios de salud que utilizan IA en la atención de sus pacientes tienen como consecuente las siguientes obligaciones mínimas en materia de protección de datos personales:

- Obtener consentimiento informado: es necesario e imprescindible por parte de los prestadores de servicios de salud la obtención del consentimiento libre, expreso e informado del paciente para el tratamiento de sus datos personales garantizando siempre que este comprenda la política

dispuesta por la entidad para el tratamiento y protección de los datos, y que los pacientes tengan conocimiento claro de este y de los mecanismos propuestos para la garantía de sus derechos.

- Garantizar la confidencialidad: las instituciones y profesionales independientes prestadores de servicios de salud con el uso de inteligencia artificial, deberán implementar medidas técnicas y organizativas de seguridad adecuadas para garantizar la confidencialidad de los datos personales de los pacientes.
- Capacitar al personal: se deben adoptar medidas bajo los principios de mejora continua que obliguen la adecuada formación de todo el personal de la salud, el personal de apoyo y administrativo, que brinde garantías e información oportuna a a los pacientes sobre el uso adecuado de la información sensible contenida en la historia clínica y el tratamiento de estos datos, así como los mecanismos de garantías de derechos propuestos o ejecutados al interior de la institución prestadora de servicios o el profesional independiente que los brinde.
- Informar a los titulares de los datos: es obligación de prestadores de servicios de salud o profesionales independientes que presten sus servicios haciendo uso de IA, de informar a los pacientes titulares de los datos y/o sus representantes sobre los derechos que tienen en relación con sus datos personales y los procedimientos definidos para garantizar estos derechos.
- Reportar: Reportar públicamente a los interesados y a los titulares de los datos sobre cualquier incidente que afecte la seguridad y protección de los datos personales.

Con el desarrollo de los marcos normativos y la evidencia demostrada de la necesidad de implementar mecanismos y garantías de protección de datos, se evidencia entonces mediante sugerencia incluso de las principales obligaciones de los prestadores de servicios de salud o profesionales independientes bajo las mejores prácticas que es necesario no perder de vista estos puntos para el desarrollo del modelo de gestión a proponer.

Capítulo IV: DISEÑO DEL MODELO DE GESTIÓN

4.1 Definir los datos o información sensible contenidos en la historia clínica de las personas que acceden a la prestación de servicios de salud con IA

4.1.1 Clasificar los tipos de datos personales presentes en la historia clínica

En la prestación de los servicios de salud, se genera un documento o informe de atención que contiene información de los pacientes que acuden, la historia clínica es este elemento generado a partir de la prestación del servicio y que alberga todos los datos del paciente, la información de la atención u toda la información sensible sobre la salud y el historial médico del paciente. Teniendo en cuenta lo anterior, es necesario entonces que las instituciones prestadoras o profesionales independientes realicen una adecuada gestión de estos datos, no solo con los fines de garantizar una atención médica oportuna y de calidad de acuerdo a las necesidades de cada paciente, sino también para proteger los derechos fundamentales de los titulares de los datos y especialmente en lo que respecta a la protección estos en términos de protección y confidencialidad de su información personal.

Es por lo que se hace necesario realizar una adecuada clasificación de cada uno de los tipos de datos personales presentes en la historia clínica siendo un pilar fundamental para diseñar un modelo de gestión adecuado que garantice la adecuada administración de estos. Esta clasificación debe establecer los niveles de seguridad y acceso, de acuerdo con las características de los datos, su nivel de riesgo o posible afectación y en especial atención de aquellos que puedan considerarse como datos sensibles, brindando los lineamientos bases para el aseguramiento y protección de los datos y minimizando el riesgo de acceso no autorizado o uso indebido de los mismos. Este proceso es fundamental para el

desarrollo de un modelo de gestión que garantice la seguridad y confidencialidad de los datos en la prestación de servicios de salud con inteligencia artificial en Colombia

La normativa vigente en materia de protección de datos personales refuerza la importancia de esta clasificación. Estas normas establecen un marco legal de base sólido para la gestión de datos en salud, destacando la necesidad de implementar medidas específicas de protección para los datos sensibles conforme se ha venido desarrollando, en especial cuando trata de servicios de salud prestados con el uso o apoyo de inteligencia artificial.

Para comprender a profundidad la clasificación de datos en las historias clínicas, se hizo una revisión de la normativa aplicable, así como la consideración de algunos proyectos en los que se plantea la unificación de la historia clínica en especial del Diseño del modelo de un prototipo de Historia Clínica Electrónica Unificada (HCEU) en Colombia propuesto por Díaz Peralta, G, Moreno Ángel, J y Pacheco Suárez, J. (2015).

Partiendo del análisis realizado, se propone clasificar los datos presentes en las historias clínicas en las siguientes categorías:

Categoría	Tipo de Datos	Observación
1. Datos de Identificación Personal	- Nombre completo - Documento de identidad - Dirección de residencia - Teléfono de contacto - Correo electrónico	Estos datos son fuente de información base para la adecuada identificación de los pacientes al momento de realizar la prestación del servicio de salud
2. Datos Administrativos	- Número de historia clínica - Información del seguro de salud - Información de contacto de emergencia	Estos campos son necesarios para la adecuada gestión administrativa de quien presta el servicio de salud y la coordinación adecuada de la atención médica

Categoría	Tipo de Datos	Observación
3. Datos de Salud	- Antecedentes médicos y quirúrgicos - Resultados de exámenes y diagnósticos - Planes y registros de tratamiento - Medicamentos prescritos - Notas de evolución médica y de enfermería - Información sobre alergias y reacciones adversas	Estos datos son de vital importancia a la hora de prestar servicios de salud pues son de uso para el diagnóstico, tratamiento y seguimiento del estado de salud del paciente
4. Datos Sensibles	- Información genética - Datos sobre salud mental - Enfermedades Graves - Información sobre salud sexual y reproductiva - Datos sobre abuso de sustancias - Información sobre procesos de violencia - Información sobre procesos de acceso carnal u otros procedimientos legales	Debido a su naturaleza sensible y el potencial daño que podría ocasionar su divulgación no autorizada, estos datos **requieren un nivel de protección más estricto**

Tabla 3. Clasificación de los Datos contenidos en la Historia Clínica
Fuente de Elaboración Propia

La investigación llevada a cabo ofrece una comprensión detallada sobre la clasificación de los datos contenidos en las historias clínicas, dando la relevancia de proteger los datos personales permitiendo identificar de manera precisa qué tipo de información requiere un nivel de protección más elevado.

Además, es claro en este punto que el uso de la inteligencia artificial en la prestación de servicios de salud introduce nuevos desafíos y oportunidades en la gestión de datos, teniendo presente que la clasificación adecuada de los datos no solo facilita la implementación de estas nuevas tecnologías, sino que también asegura que se cumplan las normativas legales y éticas relacionadas con el manejo de información de los pacientes.

En el contexto colombiano, la adopción de tecnologías avanzadas en salud está en crecimiento, esto incluye la creación de políticas claras sobre la protección de datos, la capacitación continua del personal de salud en prácticas de seguridad de la información y la colaboración incluso con expertos en ciberseguridad y otras líneas transversales para desarrollar soluciones innovadoras y efectivas para los pacientes, prestadores y en general para el sistema de salud.

En conclusión, la adecuada clasificación de datos contenidos en las historias clínicas constituye un componente relevante al momento de proponer el modelo que permita garantizar la seguridad y confidencialidad de la información de los pacientes. Al mismo tiempo, es una fuente de base que debe ser considerada en la implementación de la inteligencia artificial en la prestación de servicios de salud en Colombia, asegurando que se pueda garantizar la protección de los derechos y la privacidad de los datos de los pacientes mientras se aprovechan las oportunidades que ofrece el uso de estas nuevas tecnologías de las tecnologías.

4.1.2 Identificar los datos sensibles que requieren un mayor nivel de protección

Habiendo analizado los contenidos e identificado la clasificación sugerida para los datos contenidos en la historia clínica de los pacientes y en especial de los datos sensibles que requieren un mayor nivel de protección debido a su naturaleza y a las posibles consecuencias negativas de su divulgación no autorizada. Adicionalmente, las normas revisadas y relacionadas en el marco jurídico constituyen una fuente primordial a ser consideradas para la protección de estos datos en el entorno general, se hace necesario que existan medidas adicionales como el consentimiento informado y el usos de otras medidas de mitigación de riesgos como la anonimización, seudonimización y las restricciones de acceso.

En consonancia con la literatura revisada, la protección de datos sensibles en el ámbito de la inteligencia artificial en salud se erige como un asunto de especial importancia que demanda un enfoque proteccionista frente a los titulares de la información que brinde mejores garantías y seguridad.

Propuesta la clasificación de los datos presentes en las historias clínicas, se hace especial énfasis en los clasificados como Datos Sensibles sugiriendo las siguientes definiciones para cada uno de los tipos:

- Datos de Salud Mental: esta información incluye los diagnósticos, tratamientos y registros de salud mental de los pacientes. Su sensibilidad radica en el estigma social asociado a estas condiciones.

- Información Genética: esta información comprende los resultados de pruebas genéticas y predisposiciones hereditarias y cualquier otro tipo de dato genético de los pacientes. La información genética constituye datos de especial tratamiento y protección es crítica porque puede revelar información no solo sobre el paciente, sino también sobre sus familiares.

- Enfermedades Graves: esta información comprende los diagnósticos y tratamientos de enfermedades graves o terminales de los pacientes. El mal uso o acceso indebido de este tipo de información puede afectar significativamente la privacidad y el bienestar del titulas de los datos.

- Información de Salud Sexual y Reproductiva: esta información incluye historia obstétrica, urológica, métodos anticonceptivos, abortos y otros datos relacionados con la salud reproductiva además de las enfermedades de transmisión sexual. Estos datos son sensibles debido a su naturaleza íntima y el potencial impacto en la vida personal y social del paciente.

- Datos sobre Abuso de Sustancias: esta información incluye el historial de consumo de drogas y tratamientos de los pacientes. La divulgación o mal uso de esta información puede llevar a la discriminación y estigmatización del paciente.

- Información sobre Violencia: esta información comprende los datos sobre violencia doméstica o abuso. Este tipo de información es extremadamente sensible y requiere un manejo cuidadoso para proteger la seguridad y privacidad del paciente.

- Información sobre Procesos de Acceso Carnal u Otros Procedimientos Legales: esta información incluye información relacionada con procesos legales por delitos sexuales, acusaciones, y detalles de procedimientos judiciales. Estos datos son extremadamente sensibles debido a la naturaleza personal y el potencial estigma social y legal asociado.

Una vez clasificados los datos y especificado el contenido de los que se determinaron clasificar como sensibles, siendo es un punto crucial y determinante en el diseño del modelo que se complementa de forma transversal con el cumplimiento de las normativas vigentes en cuanto a protección de la información. Con el fin de ampliar este análisis, es importante agregar que lo que comúnmente

conocemos como **consentimiento informado** no solo es una obligación legal, sino también un componente ético que refuerza la autonomía de los pacientes.

Además, el enfoque integral en la protección de datos sensibles, se sugiere incluir otras medidas como la encriptación de datos, controles de acceso estrictos y auditorías regulares, estas estrategias no solo protegen la información de accesos no autorizados y ciberataques, sino que también aseguran que solo el personal debidamente autorizado tenga acceso a los datos sensibles.

4.1.3 Establecer criterios para el tratamiento de datos sensibles en la prestación de servicios de salud con IA

Una vez abordado el contexto de la clasificación y tipificación de los datos contenidos en la historia clínica sobre los cuales se busca proponer el desarrollo del modelo de protección, esta actividad se centra en establecer criterios robustos para el tratamiento de datos sensibles en la prestación de servicios de salud con IA, con esto se busca garantizar la seguridad, confidencialidad y privacidad de la información personal de los pacientes, un aspecto fundamental para la ética médica y sobre todo para la garantía de los derechos de los titulares de la información.

Habiendo identificado las clases y el tipo de datos definido como sensible, así como indagado en diversos materiales académicos ya documentados en este documento y no académicos, a continuación, se proponen los criterios fundamentales para el tratamiento de datos sensibles en el ámbito de la salud con IA en Colombia:

1. Consentimiento Informado: Pilar fundamental

Este consentimiento del que además trata la normativa se resume hoy en día en un documento o texto de aceptación explícita por parte de los pacientes que acceden a los servicios de salud, el cual

debe ser documentado y libremente otorgado del paciente antes de recopilar, utilizar o procesar sus datos sensibles, además de las posibles indicaciones, contraindicaciones o consecuencias que pueda acarrear la prestación del servicio o procedimiento a realizar, en la protección de los datos personales es un paso fundamental en el desarrollo del modelo porque que significa que el paciente debe comprender claramente:

- El propósito específico del tratamiento de sus datos.
- La naturaleza de los datos sensibles que se recopilarán.
- Los riesgos potenciales asociados al tratamiento de sus datos.
- Sus derechos en relación con la información, incluyendo el derecho de acceso, rectificación, oposición y supresión.

El consentimiento informado debe presentarse de forma clara y específica a los pacientes, de modo que por medio de un sistema de comunicación y con el uso de un lenguaje claro, comprensible y adaptado a las características del paciente, se deje además de la constancia, la claridad necesaria por parte del paciente para que si a bien este lo considera pueda ser la fuente base para la protección de su información. Es imprescindible que tanto la información transmitida como la contenida en el documento sea clara y puntual, evitando las cláusulas pre-marcadas o el uso de lenguaje ambiguo que pueda inducir a error o confusión por parte del titular de la información o de quien pueda juzgar su uso.

2. Minimización de Datos: El Principio de Necesidad Estricta

Cuando se hace referencia a datos, además de las limitaciones en cuanto a la capacidad de almacenamiento de estos, se debe considerar la necesidad de la información, al hacer uso de sistemas de información con inteligencia artificial como bien se ha descrito anteriormente son sistemas que

además no sólo contienen la información con el fin de custodiarla si no que en muchos casos es la fuente par diversos usos, en especial el de fuente de apoyo diagnóstico en la prestación de servicios de la salud, a estos sistemas por su naturaleza, se debe limitar la recopilación y utilización de datos sensibles a la mínima cantidad estrictamente necesaria para el propósito definido. Los datos irrelevantes o no esenciales para el objetivo específico del tratamiento no deben ser recopilados ni almacenados.

Este principio es fundamental para mitigar los riesgos inherente que se presentan sobre los datos, su vulnerabilidad frente a posibles al riesgo de violaciones de seguridad, filtraciones de información o incluso el uso indebido de los mismos, es por ello que es necesario delimitar su recopilación, administración y/o uso únicamente en lo que sea estrictamente necesario acceder a los datos, esto permitiendo brindar seguridad a los titulares de los datos.

3. Anonimización y Seudonimización: Escudos para la Privacidad

En el manejo y uso de datos sensibles de salud, resulta fundamental salvaguardar la identidad de los pacientes, en especial en la correlación del uso de la información para otros fines, para ello, se deben aplicar técnicas como la anonimización y la seudonimización, que permiten proteger la privacidad individual mientras se posibilita el uso de la información para fines investigativos y estadísticos. Siempre que sea posible, se deben aplicar estas técnicas para proteger la identidad del paciente:

- Anonimización: La anonimización consiste en la completa disociación o desconexión de los datos clasificados como Datos de Identificación Personal de los demás datos. Esto significa que la información se transforma en un conjunto anónimo, de esta manera, se

garantiza el anonimato absoluto de los pacientes, protegiendo su privacidad al máximo nivel.

- Seudonimización: Sustituye los datos clasificados como Datos de Identificación Personal por un seudónimo o código único, manteniendo la posibilidad de revertir el proceso para identificar al individuo en caso de ser necesario.

4. Acceso Restringido: Caja fuerte Digital

Los datos y en especial los clasificados como sensibles deben contar con especiales políticas de acceso estrictamente limitados, otorgando sólo al personal autorizado que requiera dicha información para cumplir con sus funciones específicas en la prestación del servicio de salud, por esto se hace necesario implementar controles robustos para evitar accesos no autorizados o indebidos. Estos controles de acceso pueden incluir:

- Autenticación: se deben implementar controles de verificación de la identidad de los usuarios que acceden a la información de los pacientes, se sugieren mecanismos como contraseñas, tokens de seguridad o claves cifradas.
- Autorización: la definición de roles y permisos específicos para cada usuario de acuerdo a las funciones que desempeña en la institución prestadora de servicios y/o profesional independiente, limitando el acceso a la información conforme sus necesidades y responsabilidades en la prestación de los servicios de salud.
- Registro de Auditoría: aplicar tanto de forma preventiva como correctiva un monitoreo y seguimiento de los registros de acceso a los datos sensibles por parte de los usuarios de la

información, permitiendo identificar actividades sospechosas y prevenir posibles vulneraciones a los derechos de los titulares de los datos.

5. Auditorías y Controles: Vigilancia Constante

En los procesos de atención de salud es de especial interés la aplicación de políticas enfocadas a la mitigación de los riesgos, en cuanto al tratamiento de datos deben enfocarse los esfuerzos en la evaluación, seguimiento y control de las actividades que se desarrollan y que comprometen de alguna forma el acceso o uso de los datos, siendo fundamental la realización de auditorías periódicas que permitan evaluar el cumplimiento de esas políticas y procedimientos establecidos para garantizar los niveles de seguridad y protección de datos de los pacientes. Estas auditorías deben abarcar:

- Evaluación de riesgos: necesaria para la identificación de los riesgos potenciales asociados a la administración tratamiento de datos de los pacientes, con especial atención en aquellos datos clasificados como Datos Sensibles, incluyendo amenazas internas y externas, vulnerabilidad de los sistemas de información y las posibles fallas de seguridad.
- Análisis de controles: enfocados en la verificación de la efectividad y eficiencia de los controles diseñados para mitigar los riesgos identificados al interior de las instituciones o prestadores de servicios de salud, incluyendo controles de acceso, mecanismos de seguridad y procedimientos de gestión de incidentes.
- Pruebas de violación: realizar simulacros de ataques informáticos y vulneraciones de acceso a la información de los pacientes con el fin de evaluar la robustez de los sistemas y detectar posibles brechas de seguridad.

Es imprescindible que los encargados de realizar las auditorías garanticen su independencia e idoneidad para la ejecución de las actividades encomendadas, y sus resultados deben de estricto análisis para el diseño de los controles y medidas correctivas necesarias, basado especialmente en los ciclos de mejora continua en especial de Verificar y Actuar, en aras de fortalecer y garantizar la protección de los datos de los pacientes.

6. Capacitación del Personal: Recurso humano

Se deben implementar programas de capacitación continua para el personal de la salud, no sólo al quienes intervienen en la prestación de los servicios sino también al personal en general sobre protección de datos y manejo responsable de los datos en el ámbito de la salud. Esta capacitación debe abordar:

- Principios éticos: Sensibilización sobre los principios éticos que rigen el tratamiento de datos sensibles, como el respeto a la privacidad, la confidencialidad y la autonomía del paciente.
- Regulaciones vigentes: Conocimiento de las leyes y normativas aplicables a la protección de datos en el sector salud.
- Mejores prácticas: Actualización constante sobre las mejores prácticas para el manejo seguro y responsable aplicadas al interior de la organización para la protección y garantía de los derechos sobre el tratamiento de datos de los pacientes en el contexto de la IA en salud.

Las capacitaciones deben ser adaptadas a las diferentes funciones y responsabilidades del personal, esto ofreciendo a los pacientes la oportunidad de acceder a los mecanismos o procedimientos establecidos al interior de la organización para la garantía de sus derechos, es recomendable incluir simulaciones prácticas y escenarios realistas para reforzar los conocimientos adquiridos.

7. Encriptación: Blindaje de Datos

La seguridad de la información es primordial, especialmente cuando se trata de datos sensibles, para proteger estos datos contra accesos no autorizados, intercepciones o divulgaciones indebidas, es crucial almacenarlos y transmitirlos de forma encriptada.

Es por esto que la encriptación de los datos tiene como finalidad servir de escudo, transformando la información en códigos indescifrable y de difícil acceso con la finalidad de salvaguardar la información, proteger la integridad de los datos, y garantizar que no sean modificados o alterados de forma inadvertida o maliciosa. Esto de logra por medio del uso de algoritmos de encriptación robustos y protocolos de seguridad confiables que brinden integridad y confidencialidad de los datos de los pacientes.

8. Mecanismos de Denuncia: Canales para la Transparencia

Es fundamental instaurar canales de denuncia claros y accesibles que permitan al personal de la salud, administrativo, de apoyo y a los pacientes reportar cualquier sospecha de uso indebido o violación de la normativa de protección de datos. Estos canales deben garantizar la transparencia y la confianza, asegurando la gestión por parte de un equipo independiente y confiable.

Estos canales de denuncia deben ser gestionados por un equipo independiente y confiable, y los procedimientos para la investigación y resolución de denuncias deben ser claros y transparentes, es importante informar a los titulas de los datos, que en caso de que sus garantías no le sean respetadas puede acudir a instancias jurisdiccionales ante los entes de control, en especial la superintendencia de

industria y comercio quien tiene facultades y mecanismos propios que puedan garantizar la protección requerida.

9. Evaluación de Impacto en la Protección de Datos: Anticipación y Prevención

Es imprescindible establecer, de conformidad con las obligaciones de los prestadores de servicios de salud, que en todos los casos debe anticipar o prevenir futuras afecciones antes de implementar cualquier sistema de IA que involucre el tratamiento de datos de los pacientes, en la que debe realizar una evaluación de impacto en la protección de datos. Esta evaluación debe identificar y analizar los riesgos potenciales asociados al tratamiento de datos, y proponer medidas para mitigar dichos riesgos.

10. Responsabilidad del prestador: Un Marco Sólido

Establecer un marco claro de responsabilidad del prestador es fundamental para garantizar la protección efectiva de datos sensibles en la prestación de servicios de salud con IA. Este marco como mínimo debe abarcar los siguientes aspectos:

a) Definición Clara de Roles y Responsabilidades:

- Designar los responsables de administrar, custodiar y supervisar el cumplimiento de las normas definidas para la protección de datos, asesorar a la organización y actuar como punto de contacto para las autoridades y los interesados.
- Implementar un Comité de Ética en Datos compuesto por expertos en salud, ética, tecnología y protección de datos, responsable de asesorar sobre el uso ético y responsable

de la IA en salud y garantizar el cumplimiento de los principios éticos en el tratamiento de datos de los pacientes.

- Disponer de un Equipo de Seguridad de la Información con personal especializado en protección de datos y ciberseguridad, responsable de implementar y gestionar las medidas de seguridad técnicas y organizativas necesarias para proteger los datos de los pacientes.

b) Políticas y Procedimientos Documentados:

- Política de Protección de Datos: Desarrollar una política integral de protección de datos que establezca los principios, objetivos y compromisos de la organización en materia de protección de datos de los pacientes.

- Procedimientos Específicos: Diseñar e implementar procedimientos específicos para el tratamiento de datos de los pacientes en cada etapa del ciclo de vida de la IA, desde la recolección hasta la eliminación, incluyendo:

    - Obtención de consentimiento informado
    - Minimización de datos
    - Anonimización y seudonimización
    - Control de acceso
    - Seguridad de la información
    - Gestión de incidentes
    - Auditorías y controles
    - Capacitación del personal

c) Implementación Efectiva y Monitoreo Continuo:

- Disponer de los Recursos Suficientes tanto humanos, como financieros y tecnológicos necesarios para implementar y mantener el marco de responsabilidad de manera efectiva.

- Realizar Capacitación y Sensibilización continua al personal sobre el marco de responsabilidad, incluyendo sus roles y responsabilidades específicas en la protección de datos de los pacientes y el cumplimiento de las demás políticas y procedimientos dispuestos para tal fin.

- Ejecutar mecanismos Monitoreo y Evaluación periódicamente que garanticen la efectividad del marco de responsabilidad, identificando áreas de mejora y realizando los ajustes necesarios.

d) Adaptación a Cambios Tecnológicos y Regulatorios:

- Actualización Constante: Mantener el marco de responsabilidad actualizado con los últimos avances tecnológicos y los cambios en las regulaciones de protección de datos.

- Revisiones Periódicas: Realizar revisiones periódicas del marco para garantizar su adecuación a las necesidades cambiantes del entorno y los riesgos emergentes.

e) Cultura de Protección de Datos:

- Fomentar una cultura de protección de datos dentro de la organización, donde la privacidad y la seguridad de la información sean valores prioritarios para todos los empleados.

- Promover la responsabilidad individual en la protección de datos sensibles, empoderando al personal para identificar y reportar posibles riesgos o incumplimientos.

En el argumento de la prestación de servicios de salud con IA, la protección de datos de los pacientes y en especial de aquellos clasificados como Datos Sensibles, es un asunto de máxima prioridad para garantizar la seguridad de estos y por supuestos mitigar posibles riegos que puedan ir en contravía de los intereses de la organización.

Se establecen criterios claros, que de ser aplicados de manera rigurosa y supervisados constantemente conforme su cumplimiento es una tarea fundamental para garantizar la protección de la privacidad, la seguridad y la integridad de los datos se los pacientes al adoptar un enfoque integral y proactivo en la protección de datos, las entidades de salud pueden generar confianza, calidad y fomentar la innovación responsable en el uso de la IA para mejorar la prestación de servicios de salud.

4.2 Documentar el modelo de gestión para la protección de datos personales en la prestación de servicios de salud con inteligencia artificial en Colombia

4.2.1 Establecer procedimientos claros y accesibles para que los titulares de datos personales puedan ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad

Habiendo propuesto los criterios del tratamiento de los datos, además de su clasificación y la determinación de las obligaciones de los prestadores de servicios de salud en materia de protección de datos personales, se hace necesario entonces realizar la propuesta de los procedimientos mínimos que se deben tener a disposición para que los titulares de datos personales puedan garantizar el ejercicio de sus derechos. En el diseño de procedimientos propuesto, se tiene especial énfasis en actividades que den relevancia al uso y protección de datos, así como la necesidad de garantizar los derechos de los titulares de datos.

Por lo anterior, para facilidad del proceso y pensando en el uso eficiente de los recursos y la información, se propone un formato único de protección de datos personales FUPDP con su respectivo instructivo de diligenciamiento, este formulario se diseñó para ser claro y comprensible, definiendo en su encabezado el tipo de solicitud o trámite y los datos necesarios para la verificación de la información en aras de garantizar la titularidad de la información, y asegurando que los titulares de datos puedan completarlo sin dificultad, el cual debe estar disponible tanto en línea como en formato físico en las oficinas de la institución y/o prestador de salud. La información y los documentos aportados por el solicitante se entenderán como ciertos bajo la gravedad del juramento. A continuación, se visualiza el formato propuesto:

FORMATO ÚNICO DE PROTECCIÓN DE DATOS PERSONALES	Código: FUPDP
	Fecha actualización:
	Versión 1.0

Campo exclusivo para la Institución		
Fecha de radicación:	N° Radicado:	Sede:

1. Tipo de solicitud

Acceso ☐ Rectificación ☐ Cancelación ☐ Oposición ☐ Portabilidad ☐

2. Tipo del solicitante

Nombre propio ☐ Representante ☐

3. Datos del solicitante

Nombre Completo:	T.D	Número de documento:
Dirección:	Municipio/Ciudad:	
Correo electronico:	Teléfono:	

4. Medio de notificación

Correo electrónico ☐ Dirección ☐ ☐ Punto Físico

5. Descripción de la solicitud

Firma

Ilustración 1. Formulario Único de Protección de Datos Personales FUPDP

Elaboración Propia

Instructivo para el diligenciamiento del Formulario Único de Protección de Datos Personales FUPDP

- Estas instrucciones son una guía general para el diligenciamiento del formulario FUPDP, en caso de tener inquietudes sobre su diligenciamiento deberá consultar con el personal autorizado de la institución.

- El solicitante ya sea que actúe a nombre propio o por medio de un representante y/o apoderados deberán estar debidamente facultados y suministrar soporte de su identidad para la aceptación del formulario.

1. Tipo de solicitud: En este campo debe seleccionar el tipo de solicitud que desea realizar de acuerdo con las opciones dispuestas, únicamente deberá seleccionar un tipo de solicitud por formulario, de lo contrario su solicitud podría no ser procesada.

- Solicitud de Acceso: para acceder a sus datos personales, obtener copia y conocer cómo están siendo tratados.
- Solicitud de Rectificación: para la corrección de sus datos personales si estos son inexactos o incompletos.
- Solicitud de Cancelación: para la cancelación o eliminación de sus datos personales cuando ya no sean necesarios para los fines para los cuales fueron recolectados.
- Solicitud de Oposición: para oponerse al tratamiento de sus datos personales por motivos legítimos, y la suspensión de su uso.

- Solicitud de Portabilidad: para la transferencia de sus datos personales a otra entidad de su elección.

2. Tipo de solicitante: En este campo debe seleccionar el tipo de solicitante que eleva la solicitud:

- A nombre propio: cuando la solicitud es realizada directamente por el titular de los datos:
- Representante: cuando la solicitud es realizada por un representante y/o apoderado, debe presentar poder otorgado por el titular de los datos y autenticado de conformidad con las normas aplicables y/o orden judicial expedida por alguna autoridad de la república de Colombia que otorgue facultad para tal fin.

3. Datos del solicitante: En este campo debe indicar los datos de identificación y contacto del solicitante:

- Nombre completo
- T.D o Tipo de Documento
- Número de documento
- Dirección
- Municipio/Ciudad
- Correo electrónico
- Teléfono

4. Medio de notificación: En este campo debe seleccionar el medio de notificación de la respuesta, se sugiere consultar con el personal de la institución y/o prestador de servicios, las solicitudes que seleccionen la opción de envío a la dirección deberán asumir el costo del envío por parte del solicitante:

- Correo electrónico: entrega por mensaje de datos mediante correo electrónico de notificación indicado por el solicitante.
- Dirección: entrega física por medio de correspondencia.
- Punto Físico: entrega física en el punto de solicitud.

5. Descripción de la solicitud: En este campo el solicitante deberá indicar los detalles de su solicitud, especificando los motivos, detalle de los datos y/o información que permitan hacer el respectivo estudio de la solicitud. En caso de inquietud, se recomienda solicitar ayuda con el personal de la institución y/o prestador de servicios.

Una vez planteado el formulario propuesto, a continuación, se detalla el procedimiento sugerido para cada uno de los tipos de solicitud por parte de la institución y/o prestador de servicios de salud

Procedimientos para el ejercicio de derechos:

Se proponen mecanismos para la protección de los derechos que cómo mínimo se deben garantizar a los titulares de los datos en la prestación de los servicios de salud con IA, definiendo como derechos principales los siguientes: acceso, rectificación, cancelación, oposición y portabilidad.

- **Procedimiento de acceso:**

Este procedimiento delimita cómo los titulares de los datos y/o sus representantes pueden acceder a los datos administrados en la prestación de los servicios de salud con IA. Es pertinente establecer que los representantes y/o apoderados deberán estar debidamente facultados para elevar la solicitud mediante poder autenticado de conformidad con las normas

aplicables y/o orden judicial expedida por alguna autoridad de la república de Colombia que otorgue facultad para tal fin. Dicho procedimiento de divide en 3 fases:

1. Solicitud de acceso: los titulares de los datos y/o sus representantes deben solicitar o hacer uso del formulario FUPDP, especificando en el campo designado para tal fin que se trata de una solicitud de acceso, y detallando la información a la cual desea tener acceso.

2. Verificación de identidad: con el fin de garantizar la confidencialidad de los titulares de los datos, el solicitante deberá acreditar la titularidad con la verificación de su documento de identificación válido, en caso de ser representante del titular deberá acreditar el respectivo poder con el cumplimiento de los requisitos legales y/o acreditar la respectiva instrucción por parte de alguna autoridad de la república de Colombia.

3. Entrega de información: el titular de la solicitud y/o su representante deberán indicar el medio idóneo para la entrega de la información, para esto la institución hará entrega de la información solicitada en un formato claro y comprensible dentro de un plazo de 15 días hábiles, disponiendo 3 canales: entrega física en el punto de solicitud, entrega por mensaje de datos mediante correo electrónico de notificación indicado por el solicitante o entrega física por medio de correspondencia para lo cual el solicitante deberá asumir los costos de envío. En todo caso, la responsabilidad sobre la protección de los datos cesará por parte de la institución y/o prestador de salud una vez sea entregada la información requerida por el solicitante.

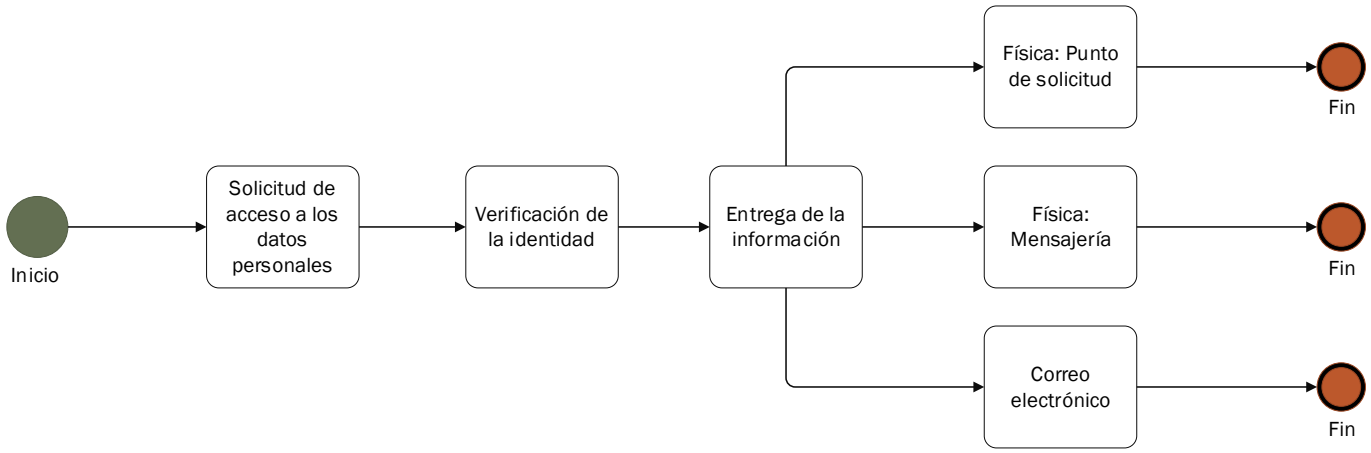


Figura 2. Procedimiento de acceso

Elaboración Propia

- **Procedimiento de rectificación:**

Este procedimiento delimita cómo los titulares de los datos y/o sus representantes pueden solicitar sean rectificados los datos administrados en la prestación de los servicios de salud con IA. Es pertinente establecer que los representantes y/o apoderados deberán estar debidamente facultados para elevar la solicitud mediante poder autenticado de conformidad con las normas aplicables y/o orden judicial expedida por alguna autoridad de la república de Colombia que otorgue facultad para tal fin. Dicho procedimiento de divide en 3 fases:

1. Solicitud de rectificación: los titulares de los datos y/o sus representantes deben solicitar o hacer uso del formulario FUPDP, especificando en el campo designado para tal fin que se trata de una solicitud de rectificación, detallando los datos incorrectos y proporcionando la información correcta.

2. Verificación de identidad y datos: con el fin de garantizar la confidencialidad de los titulares de los datos, el solicitante deberá acreditar la titularidad con la verificación de su documento de identificación válido, en caso de ser representante del titular deberá acreditar el respectivo poder con el cumplimiento de los requisitos legales y/o acreditar la respectiva instrucción por parte de alguna autoridad de la república de Colombia.

3. Actualización de datos: Los datos serán corregidos en un plazo no mayor a 10 días hábiles y el titular y/o su representante será notificado de la actualización disponiendo 2 canales: entrega física en el punto de solicitud o entrega por mensaje de datos mediante correo electrónico de notificación indicado por el solicitante.

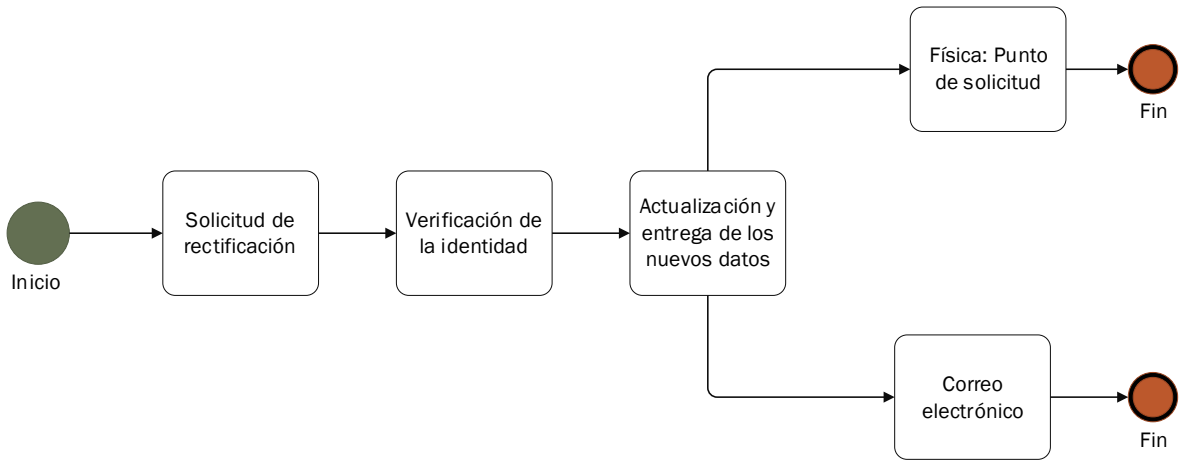


Figura 3. Procedimiento de rectificación

Elaboración Propia

- **Procedimiento de cancelación:**

Este procedimiento delimita cómo los titulares de los datos y/o sus representantes pueden solicitar sean cancelados los datos administrados en la prestación de los servicios de salud con IA. Es pertinente establecer que los representantes y/o apoderados deberán estar debidamente

facultados para elevar la solicitud mediante poder autenticado de conformidad con las normas aplicables y/o orden judicial expedida por alguna autoridad de la república de Colombia que otorgue facultad para tal fin. Dicho procedimiento de divide en 4 fases:

1. Solicitud de cancelación: los titulares de los datos y/o sus representantes deben solicitar o hacer uso del formulario FUPDP, especificando en el campo designado para tal fin que se trata de una solicitud de cancelación, indicando claramente los datos que desean eliminar y el motivo.

2. Verificación de identidad y datos: con el fin de garantizar la confidencialidad de los titulares de los datos, el solicitante deberá acreditar la titularidad con la verificación de su documento de identificación válido, en caso de ser representante del titular deberá acreditar el respectivo poder con el cumplimiento de los requisitos legales y/o acreditar la respectiva instrucción por parte de alguna autoridad de la república de Colombia.

3. Evaluación de solicitud: la institución y/o prestador de salud deberá evaluar si la solicitud cumple con las condiciones legales para proceder con la cancelación, considerando la normativa vigente y los criterios para el tratamiento de datos sensibles, en todo caso de ser viable la solicitud, la responsabilidad sobre la protección de los datos cesará por parte de la institución y/o prestador de salud.

4. Eliminación de datos: si la solicitud es válida, la institución y/o prestador de salud procederá con la eliminación de los datos en un plazo de 15 días hábiles y el titular y/o su representante será notificado de la eliminación disponiendo 2 canales: entrega física en el punto de solicitud o

entrega por mensaje de datos mediante correo electrónico de notificación indicado por el solicitante.

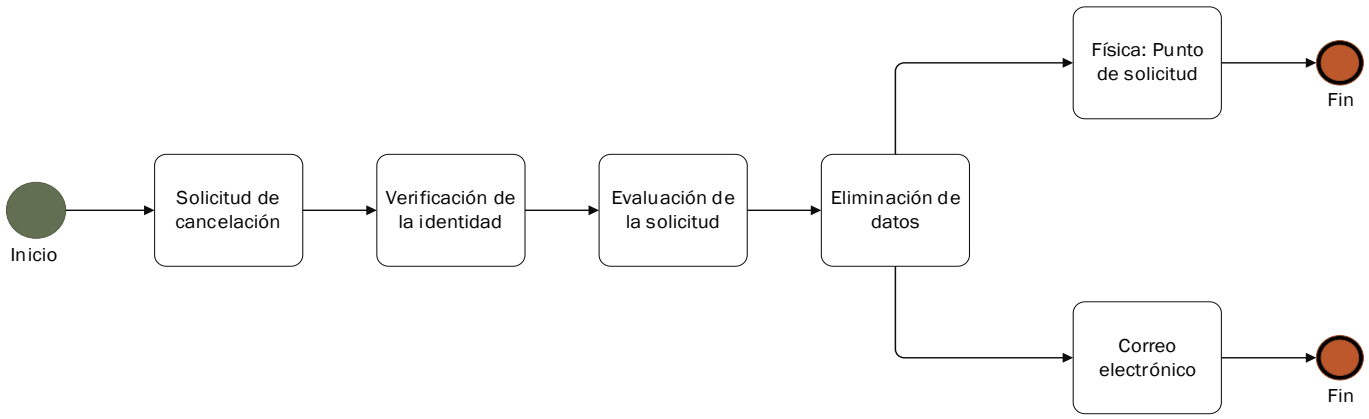


Figura 4. Procedimiento de cancelación

Elaboración Propia

- **Procedimiento de oposición:**

Este procedimiento delimita cómo los titulares de los datos y/o sus representantes pueden solicitar su oposición frente al uso de los datos administrados en la prestación de los servicios de salud con IA. Es pertinente establecer que los representantes y/o apoderados deberán estar debidamente facultados para elevar la solicitud mediante poder autenticado de conformidad con las normas aplicables y/o orden judicial expedida por alguna autoridad de la república de Colombia que otorgue facultad para tal fin. Dicho procedimiento de divide en 4 fases:

1. Solicitud de oposición: los titulares de los datos y/o sus representantes deben solicitar o hacer uso del formulario FUPDP, especificando en el campo designado para tal fin que se trata de una solicitud de oposición al tratamiento de sus datos, especificando las razones.

2. Verificación de identidad y datos: con el fin de garantizar la confidencialidad de los titulares de los datos, el solicitante deberá acreditar la titularidad con la verificación de su documento de identificación válido, en caso de ser representante del titular deberá acreditar el respectivo poder con el cumplimiento de los requisitos legales y/o acreditar la respectiva instrucción por parte de alguna autoridad de la república de Colombia.

3. Revisión de motivos: la institución y/o prestador de salud deberá evaluar si la solicitud cumple con las condiciones legales para proceder con la oposición, considerando la normativa vigente y los criterios para el tratamiento de datos sensibles.

4. Suspensión del tratamiento: si la solicitud es aceptada, la institución y/o prestador de salud procederá con la suspensión del uso de los datos de firma inmediata una vez validada la condición, limitando su uso exclusivamente cuanto el titulas y/o su representante así lo notifiquen, el titular y/o su representante será notificado de la suspensión disponiendo 2 canales: entrega física en el punto de solicitud o entrega por mensaje de datos mediante correo electrónico de notificación indicado por el solicitante.

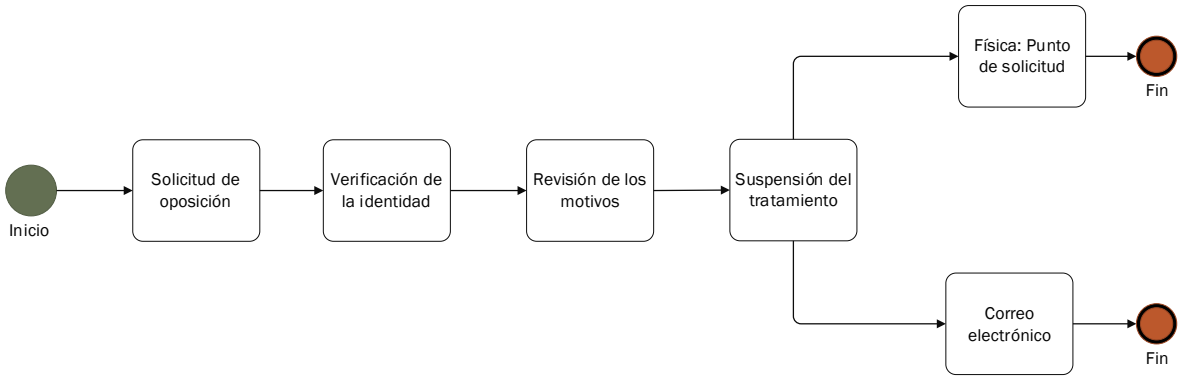


Figura 5. Procedimiento de oposición

Elaboración Propia

- **Procedimiento de portabilidad:**

Este procedimiento delimita cómo los titulares de los datos y/o sus representantes pueden solicitar la portabilidad de sus datos administrados en la prestación de los servicios de salud con IA a otra entidad. Es pertinente establecer que los representantes y/o apoderados deberán estar debidamente facultados para elevar la solicitud mediante poder autenticado de conformidad con las normas aplicables y/o orden judicial expedida por alguna autoridad de la república de Colombia que otorgue facultad para tal fin. Dicho procedimiento de divide en 4 fases:

1. Solicitud de portabilidad: los titulares de los datos y/o sus representantes deben solicitar o hacer uso del formulario FUPDP, especificando en el campo designado para tal fin que se trata de una solicitud portabilidad de sus datos a otra entidad, indicando claramente los datos que desean remitir el medio de entrega.

2. Verificación de identidad y datos: con el fin de garantizar la confidencialidad de los titulares de los datos, el solicitante deberá acreditar la titularidad con la verificación de su documento de identificación válido, en caso de ser representante del titular deberá acreditar el respectivo poder con el cumplimiento de los requisitos legales y/o acreditar la respectiva instrucción por parte de alguna autoridad de la república de Colombia.

3. Evaluación de solicitud: la institución y/o prestador de salud deberá evaluar si la solicitud cumple con las condiciones legales para proceder con la portabilidad, considerando la normativa vigente y los criterios para el tratamiento de datos sensibles, en todo caso de ser viable la solicitud, la responsabilidad sobre la protección de los datos cesará por parte de la

institución y/o prestador de salud una vez sea entregada la información requerida por del solicitante.

4. Transferencia de datos: si la solicitud es válida, la institución y/o prestador de salud procederá con la transferencia de los datos en un plazo de 20 días hábiles y el titular y/o su representante será notificado para su entrega disponiendo 2 canales: entrega física en el punto de solicitud o entrega por mensaje de datos mediante correo electrónico de notificación indicado por el solicitante.

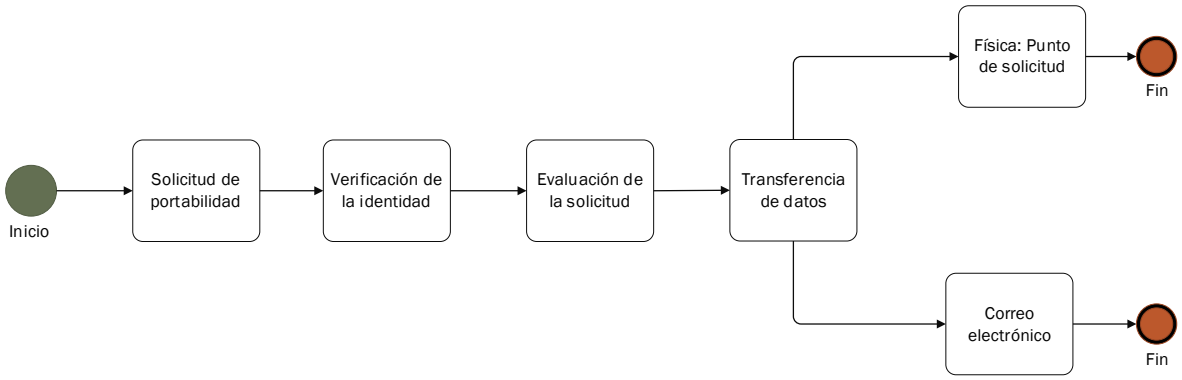


Figura 6. Procedimiento de portabilidad

Elaboración Propia

Los anteriores procedimientos delimitan el accionar de las instituciones y/o prestadores de salud en los mecanismos de acceso, rectificación, cancelación, oposición y portabilidad de los datos propiedad de los pacientes que accedes a la prestación de servicios de salud con IA.

4.2.2 Definir como se informa a los titulares de datos personales sobre sus derechos y la forma de ejercerlos

Con el fin de que los pacientes tengan pleno conocimiento de las políticas de tratamiento de datos adoptadas por la institución y/o prestador de salud, dirigidas a las protección de sus derechos y la forma de ejercerlos, se propone el desarrollo de varias estrategias basadas en los principios definidos en el punto 4.1.3 del informe:

- Sitio web: Se ha creado un portal central dentro del sitio web de la institución, dedicado exclusivamente a los derechos de los usuarios. Este portal ofrece información detallada y actualizada sobre los derechos de los titulares, incluyendo descripciones claras, ejemplos ilustrativos y formularios descargables para facilitar su ejercicio.

- Comunicación Directa:

Capacitación del personal: Se ha implementado un programa de capacitación continuo para el personal de atención al cliente, con el objetivo de brindarles las herramientas y el conocimiento necesarios para informar de manera clara y precisa a los pacientes sobre sus derechos. El personal capacitado puede responder preguntas, aclarar dudas y guiar a los pacientes en el proceso de ejercicio de sus derechos.

Correo electrónico: Se han enviado correos electrónicos informativos a todos los pacientes registrados, proporcionándoles un resumen de sus derechos y los canales disponibles para ejercerlos. Estos correos electrónicos incluyen enlaces directos al portal web y ofrecen la posibilidad de solicitar información adicional o asistencia personalizada.

- Comunicación Visual:

Carteleras informativas: Se han colocado carteleras informativas en áreas visibles de la institución, utilizando un diseño atractivo y llamativo para captar la atención de los pacientes. Las carteleras presentan un resumen visual de los derechos de los titulares, incluyendo íconos, imágenes y lenguaje sencillo, facilitando su comprensión.

- Enfoque Centrado en el Paciente:

Lenguaje claro y accesible: Se ha utilizado un lenguaje sencillo y comprensible en todas las estrategias de comunicación, evitando tecnicismos y jerga médica. La información se presenta de manera organizada, concisa y atractiva para facilitar su comprensión por parte de todos los pacientes, independientemente de su nivel educativo o condición de salud.

- Evaluación y Mejora Continua:

Monitoreo y retroalimentación: Se han implementado mecanismos para monitorear el impacto de las estrategias de comunicación y recopilar retroalimentación de los pacientes. Esta información se utiliza para evaluar la efectividad de las estrategias y realizar mejoras continuas en la comunicación de los derechos de los pacientes.

Actualizaciones periódicas: Se actualiza periódicamente la información en el sitio web, los folletos y las carteleras para garantizar que la información sea precisa, relevante y coherente con las políticas y procedimientos vigentes de la institución.

Las estrategias de comunicación implementadas por la institución demuestran un compromiso con la transparencia, la accesibilidad y el empoderamiento de los pacientes. Al proporcionar información clara y accesible sobre sus derechos, la institución facilita que los pacientes tomen decisiones informadas sobre su atención médica y ejerzan sus derechos de manera efectiva.

4.2.3 Definir la política de tratamiento de datos personales sugerida en contexto con la prestación de servicios de salud con IA

La política de tratamiento de datos personales se diseñó siguiendo los criterios específicos establecidos anteriormente, subrayan la necesidad de mantener la confidencialidad, integridad y disponibilidad de los datos, además de garantizar los derechos de los titulares. La política incluye los siguientes elementos:

Política de Tratamiento de Datos Personales

Objetivo:

Garantizar la protección de los datos personales de los pacientes en el contexto del uso de inteligencia artificial en la prestación de servicios de salud, asegurando la confidencialidad, integridad y disponibilidad de los datos.

Ámbito de Aplicación:

Esta política se aplica a todos los datos personales recogidos, almacenados, tratados y utilizados por la institución o profesional independiente en la prestación de servicios de salud mediante el uso de inteligencia artificial.

Principios:

Legalidad: El tratamiento de datos personales se realizará conforme a la normativa vigente y aplicable en Colombia.

Transparencia: Los titulares de datos serán informados de manera clara y precisa sobre el tratamiento de sus datos personales.

Confidencialidad: Los datos personales serán tratados con la más estricta confidencialidad y únicamente por el personal autorizado.

Seguridad: Se implementarán medidas técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado, la pérdida o la destrucción.

Tratamiento de Datos Personales:

Recolección de Datos: Los datos personales serán recolectados de manera directa del titular, a través de formularios electrónicos o físicos, asegurando que el titular haya otorgado su consentimiento informado.

Uso de Datos: Los datos personales serán utilizados exclusivamente para los fines específicos para los cuales fueron recolectados, incluyendo la prestación de servicios de salud y el uso de sistemas de inteligencia artificial para mejorar la atención médica.

Almacenamiento de Datos: Los datos personales serán almacenados de manera segura, utilizando tecnologías de cifrado y otras medidas de seguridad para proteger la información.

Acceso a Datos: El acceso a los datos personales será restringido y controlado, permitiendo únicamente el acceso al personal autorizado y capacitado.

Transferencia de Datos: La transferencia de datos personales a terceros será permitida únicamente cuando sea necesario para la prestación de servicios de salud y siempre que se cuente con el consentimiento previo del titular.

Derechos de los Titulares:

Acceso: Los titulares tienen derecho a acceder a sus datos personales y conocer cómo están siendo tratados.

Rectificación: Los titulares pueden solicitar la corrección de sus datos personales si estos son inexactos o incompletos.

Cancelación: Los titulares pueden solicitar la eliminación de sus datos personales cuando ya no sean necesarios para los fines para los cuales fueron recolectados.

Oposición: Los titulares pueden oponerse al tratamiento de sus datos personales por motivos legítimos.

Portabilidad: Los titulares pueden solicitar la transferencia de sus datos personales a otra entidad de su elección.

Responsabilidades:

Oficial de Protección de Datos: Será responsable de supervisar el cumplimiento de esta política y de gestionar las solicitudes de los titulares.

Personal Autorizado: Todo el personal autorizado para tratar datos personales recibirá capacitación adecuada y estará obligado a cumplir con esta política y con las normativas vigentes.

Revisión y Actualización:

Esta política será revisada y actualizada periódicamente para asegurar su adecuación y cumplimiento con las normativas vigentes y las mejores prácticas internacionales.

Conclusiones

Para hablar de la prestación de servicio integral de salud, es necesario no dejar a un lado la protección de los datos personales de los pacientes, especialmente cuando se hace uso de inteligencia artificial (IA) para prestarlos, de conformidad con lo desarrollado en la investigación y elaboración de este proyecto en el que se ha demostrado que dicha información se puede clasificar en diferentes escalas de riesgo y en especial los que son altamente sensibles por lo que un posible manejo o uso inadecuado podría tener consecuencias graves para los titulares de la información (pacientes). Por ello la propuesta de un modelo de gestión que garantice la seguridad y confidencialidad de estos datos, así como los mecanismos de garantías de los derechos, esenciales para dar aplicación a las normativas generales que existen al interior del estado colombiano.

El uso de IA ofrece diversos servicios de apoyo a los profesionales de la salud e instituciones prestadoras de servicios de salud en cuanto a precisión y apoyo diagnóstico, personalización de tratamiento y hasta reducción o control de los costos. Sin embargo, también significa grandes desafíos en materia de posibles sesgos algorítmicos, falta de transparencia e incluso implicaciones éticas que se relacionan con la autonomía y privacidad de los datos de los pacientes, haciendo necesaria la implementación de modelos que busquen minimizar los posibles riesgos mediante la implementación de controles, medidas de seguridad, auditorías y vías de protección de derechos de los pacientes.

Es necesario salvaguardar los derechos de los pacientes abordando estos desafíos que implican el uso de nuevas tecnologías como la IA en la prestación de servicios de salud haciendo uso de los modelos de gestión propuestos. En este mismo sentido el presente estudio dejó en claro la urgencia de que en Colombia se apueste por la creación e implementación de un marco normativo y ético específico

demostrado que regule el uso de la IA en el sector salud colombiano, basado en principios fundamentales y con un enfoque especial en la protección de datos de los pacientes.

El modelo de gestión propuesto enfatiza la adecuada identificación o clasificación de los datos contenidos en la historia clínica de los pacientes que son usados o administrados en la prestación de servicios de salud con IA, con la implementación de técnicas como la anonimización y seudonimización, el uso de controles adecuados enfocados a minimizar los riesgos, la aplicación del ciclo de mejora basado en el PHVA (Planear, Hacer, Verificar, Actuar) con especial énfasis en la realización las evaluaciones periódicas para garantizar en mejor medida la protección de la información de los pacientes, capacitación y otros medios, en aras de garantizarle los derechos a los titulares de la información y en especial la protección de la información.

En cuanto al consentimiento informado de los pacientes, es importante que estos tengan pleno conocimiento de su contenido y sobre todo de las políticas que este contiene en cuanto a la protección de los datos personales en la prestación del servicio de salud con IA, cómo se utilizarán sus datos, los riesgos asociados y los mecanismos de garantía de sus derechos, permitiendo con esto fortalecer la confianza en el sistema de salud y fomentar una colaboración activa entre pacientes y prestadores de servicios de salud.

Finalmente, el uso de un modelo de gestión enfocado en la protección de datos personales de los pacientes en la prestación de servicios de salud con IA en Colombia, aporta en la calidad de la atención prestada, brinda un enfoque ético y responsable en el manejo de datos en especial los clasificados como sensibles, contribuye en la creación de un entorno seguro y confiable en la relación prestados – paciente, y aporta en gran medida al éxito y la sostenibilidad de la integración de la IA en la prestación de servicios de salud.

Conceptos o Glosario

1. IA: El término inteligencia artificial (IA) se refiere a las operaciones de inteligencia ejecutadas por máquinas diseñadas para reproducir las capacidades del cerebro humano por medio de combinaciones de algoritmos.
2. Protección de Datos: es el conjunto de los recursos legales y técnicos que se emplean para que toda la información que se relaciona con una persona, especialmente aquella que permite su identificación, se encuentre salvaguardada.
3. Legislación: es el cuerpo de reglas que permiten ordenar la vida en un territorio.
4. Privacidad: es aquello que una persona lleva a cabo en un ámbito reservado (vedado a la gente en general). Un sujeto, por lo tanto, tiene derecho a mantener su privacidad fuera del alcance de otras personas, asegurándose la confidencialidad de sus cosas privadas.
5. Protección de la Información: es el proceso de salvaguardar información importante contra corrupción, filtraciones, pérdida o compromiso de los datos.

Webgrafía Glosario

1. Editorial, Equipo (14/02/2020). "Qué es la Inteligencia Artificial (IA)". En: Significados.com. Disponible en: https://www.significados.com/inteligencia-artificial/
2. Pérez, J. (21 de septiembre de 202). Protección de datos - Qué es, definición y concepto. Disponible en https://definicion.de/proteccion-de-datos/
3. Pérez Porto J, Merino M. (Actualizado el 8 de agosto de 2022) Legislación - Qué es, definición, ejemplos y tipos. Disponible en https://definicion.de/legislacion/
4. Pérez Porto J, Merino M. (Actualizado el 8 de agosto de 2022) Privacidad - Qué es, definición y concepto. Disponible en https://definicion.de/privacidad/
5. Hefner K, Peterson S, Crocetti P. (Actualizado en agosto de 2021). Protección de datos. ComputerWeekly.es Recuperado de https://www.computerweekly.com/es/definicion/Proteccion-de-datos

Referencias

República de Colombia. (2022). Código Civil de la República de Colombia. En Gaceta de la República de Colombia (No. 42.251, pp. 1-298). Bogotá, D.C.: Imprenta Nacional. Artículo 74, Personas naturales. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil_pr002.html#74

Superintendencia de Industria y Comercio. (2024, Abril 10). Sobre la protección de datos personales. ¿Qué son Datos Personales?. Recuperado de https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Ministerio de Salud y Protección Social. (2024). Registro Especial de Prestadores de Servicios de Salud - REPS. Recuperado de https://prestadores.minsalud.gov.co/habilitacion/

El País. (2023, Septiembre 14). Hackeo masivo en Colombia: la información de millones de personas está en manos de delincuentes en este momento. Recuperado de https://elpais.com/america-colombia/2023-09-21/los-hackeos-en-colombia-no-van-a-parar-y-hay-que-prepararse-para-lo-peor.html

Rolando V, Jiménez Domínguez y Onofre Rojo A. (2008). *CIENCIA, TECNOLOGÍA Y BIOÉTICA: UNA RELACIÓN DE IMPLICACIONES MUTUAS.* Recuperado de http://dx.doi.org/10.4067/S1726-569X2008000200002

Villalba Gómez, J. A. (2016). *Problemas bioéticos emergentes de la inteligencia artificial. Diversitas,* 12(1), 137–147. Recuperado de http://dx.doi.org/10.15332/s1794-9998.2016.0001.10

Garzón Fierro, V. (2020). La inteligencia artificial en Colombia. Universidad de los Andes. Recuperado de http://hdl.handle.net/1992/51660

Contreras P., A. Revista la Propiedad Inmaterial; Bogotá Tomo 29, Marco normativo de la historia clínica electrónica y su incidencia en el ámbito de la protección de datos personales en Colombia,

Universidad Externado de Colombia, enero-junio, 2020, pp. 95-116. Recuperado de https://doi.org/10.18601/16571959.n29.04

Medinaceli Díaz, K., Silva Choque, M. (2021). Impacto y regulación de la Inteligencia Artificial en el ámbito sanitario, 15(48), 77-113. Recuperado de https://www.scielo.org.mx/pdf/rius/v15n48/1870-2147-rius-15-48-77.pdf

Ramón Fernández, F. (2021). *Inteligencia artificial en la relación médico-paciente: Algunas cuestiones y propuestas de mejora.* Revista chilena de derecho y tecnología, 10(1), 329-351. Recuperado de http://dx.doi.org/10.5354/0719-2584.2021.60931

Quintana Hernández, E., Martín Ramírez, A. (2021). *Lineamientos específicos para el tratamiento de datos personales obtenidos desde la historia clínica de los pacientes, hacia la interoperabilidad de sistemas de información en el sector de la salud en Colombia.* Recuperado de https://repository.unipiloto.edu.co/handle/20.500.12277/10070

Ospina, M. R., y Zambrano, K.J. (2023). Gobierno digital e inteligencia artificial, una mirada al caso colombiano. Administración & Desarrollo, 53(1), 1-34. * Documento derivado del curso de Gestión Pública del Programa de Administración de Empresas de la Universidad Militar Nueva Granada (UMNG). Bogotá. Recuperado de https:// doi.org/10.22431/25005227.vol53n1.2

Guerrero Arévalo Wilmer Darío (2021). *Los alcances de la inteligencia artificial (IA) y su responsabilidad frente al derecho y ética.* Recuperado de https://hdl.handle.net/10901/20572

Vesga Ferreira, J. C., Contreras Higuera, M. F., y Vesga Barrera, J. A. (2021). Nuevos desafíos en el desarrollo de soluciones para e-health en Colombia, soportados en Internet de las Cosas (IoT). Revista EIA, 18(36), 36008 pp. 1–19. Recuperado de https://doi.org/10.24050/reia.v18i36.1508

Medinaceli Díaz, Karina Ingrid, & Silva Choque, Moisés Martin. (2021). Impacto y regulación de la Inteligencia Artificial en el ámbito sanitario. Revista IUS, 15(48), 77-113. Epub 14 de marzo de 2022. Recuperado de https://doi.org/10.35487/rius.v15i48.2021.745

Rojas Camargo, J. (2021). Importancia de la Historia Clínica Electrónica como Sistema de Información de Salud en Colombia. Universidad Santo Tomás. Recuperado de https://repository.usta.edu.co/handle/11634/50496

Ministerio de Salud y Protección Social. (2022, 22 de marzo). Dos años de posicionamiento de la telemedicina en Colombia. Recuperado de https://www.minsalud.gov.co/

Superintendencia de Industria y Comercio. (28 de Enero 2022). BALANCE DE GESTIÓN EN PROTECCIÓN DE DATOS (2021). Bogotá, D.C. Recuperado de https://www.sic.gov.co/slider/m%C3%A1s-de-28-mil-quejas-recibi%C3%B3-la-superindustria-en-2021-por-protecci%C3%B3n-de-datos-personales#:~:text=BALANCE%20DE%20GESTI%C3%93N%20EN%20PROTECCI%C3%93N,recibidas%20durante%20el%20a%C3%B1o%202020.

Superintendencia de Industria y Comercio. (2024, 29 de enero). Más de 2.300 quejas al mes recibe la Superintendencia de Industria y Comercio por temas relacionados con infracciones al régimen de protección de datos personales. NotiSIC, 1. Recuperado de https://www.sic.gov.co/NotiSIC/episodio/1/m%C3%A1s-de-2300-quejas-al-mes-recibe-la-superintendencia-de-industria-y-comercio-por-temas-relacionados-con-infracciones-al-r%C3%A9gimen-de-protecci%C3%B3n-de-datos-personales

El País. (2023, 14 de septiembre). Hackeo masivo en Colombia: la información de millones de personas está en manos de delincuentes en este momento. El País América Colombia. Recuperado de https://elpais.com/america-colombia/2023-09-14/hackeo-masivo-en-colombia-la-informacion-de-millones-de-personas-esta-en-manos-de-delincuentes-en-este-momento.html

Alfaro Orozco, Z y Suarez Ramírez, C. (2023). Desarrollo de un modelo de negocio de una herramienta tecnológica en la empresa SENTECOL S.A. basada en inteligencia artificial (IA) para la óptima trasmisión de información entre instituciones prestadoras de servicio de salud y sus usuarios

durante los procesos de agendamiento, confirmación y seguimiento de citas médicas. Corporación Universidad de la Costa. Recuperado de https://repositorio.cuc.edu.co/handle/11323/9968

García-López, Andrea; Girón-Luque, Fernando & Rosselli, Diego (2023). La integración de la inteligencia artificial en la atención médica: desafíos éticos y de implementación. Universitas Médica, 64(3). Recuperado de https://doi.org/10.11144/Javeriana.umed64-3.inte

Zabala Leal, T y Zuluaga Ortiz, P. (2021). Los retos jurídicos de la inteligencia artificial en el derecho en Colombia. Corporación Universidad de la Costa. Recuperado de https://doi.org/10.17981/juridcuc.17.1.2021.17

Consejo Nacional de Política Económica y Social (CONPES). (2019). Política Nacional para la Transformación Digital e Inteligencia Artificial. Documento CONPES 3975. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf

Ministerio de Salud y Protección Social. (1999). Resolución 1995 de 1999. Por la cual se establecen normas para el manejo de la Historia Clínica. Recuperado de https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

Ministerio de Salud y Protección Social. (2021). Resolución 866 de 2021. Por la cual se reglamenta el conjunto de elementos de datos clínicos relevantes para la interoperabilidad de la historia clínica en el país. Recuperado de https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%20866%20de%202021.pdf

República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

República de Colombia. (2013). Decreto Reglamentario 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

República de Colombia. (2015). Decreto 1074 de 2015. Por el cual se compilan y modifican las normas del sector comercio, industria y turismo. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608

República de Colombia. (2016). Decreto 780 de 2016. Por el cual se compilan y modifican las normas del sector salud. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77813

Díaz Peralta, G, Moreno Ángel, J y Pacheco Suárez, J. (2015). Diseño del modelo de un prototipo de Historia Clínica Electrónica Unificada (HCEU) en Colombia. Fundación Universitaria Panamericana. Recuperado de https://repositoriocrai.ucompensar.edu.co/handle/compensar/3207

Jara, J. N. M., & Ycaza, J. C. P. (2022). Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano. Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminalísticas, 7(1), 776-801.