UNIB.E
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

FACULTAD DE JURISPRUDENCIA

CARRERA: DERECHO

TÍTULO

ANÁLISIS DEL TRATAMIENTO DE LOS DATOS DE SALUD DE ACUERDO AL MARCO JURÍDICO ECUATORIANO

Trabajo de Integración Curricular para la obtención del Título de Abogada

Autor (a):
Cinthia Liseth Parra Vega

Tutor (a):
Estefanía Pamela Ortega Flores, Mgst.

Quito, Ecuador
Agosto, 2024

DECLARACION DE AUTORÍA Y AUTORIZACIÓN PARA LA DIFUSIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

UNIB.E
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

DECLARACIÓN DE AUTORÍA Y AUTORIZACIÓN PARA LA DIFUSIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

1. Yo, Cinthia Liseth Parra Vega, declaro en forma libre y voluntaria, que los criterios emitidos en el presente Trabajo de Integración Curricular, titulado: "ANÁLISIS DEL TRATAMIENTO DE LOS DATOS DE SALUD DE ACUERDO AL MARCO JURÍDICO ECUATORIANO", previo a la obtención del título profesional de Abogada, así como también los contenidos, ideas, análisis, conclusiones y propuestas son exclusiva responsabilidad de mi persona, como autor/a.

2. Declaro, igualmente, tener pleno conocimiento de la obligación que tiene la Universidad Iberoamericana del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT, en formato digital una copia del referido Trabajo de Integración Curricular para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública, respetando los derechos de autor.

3. Autorizo, finalmente, a la Universidad Iberoamericana del Ecuador a difundir a través del sitio web de la Biblioteca de la UNIB.E (Repositorio Digital Institucional), el referido Trabajo de Integración Curricular, respetando las políticas de propiedad intelectual de la Universidad Iberoamericana del Ecuador.

Quito, DM., a los 02 días del mes de agosto de 2024.

Cinthia Liseth Parra Vega
1727085779

CONSTANCIA DE APROBACION DEL DIRECTOR DE TRABAJO DE TITULACIÓN

UNIB.E
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

AUTORIZACIÓN DE PRESENTACIÓN FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR POR PARTE DEL TUTOR

Mgtr. Mayra Alejandra Guerra Sánchez
Director(a) de la Carrera de Derecho
Presente. -

Yo, **ESTEFANÍA PAMELA ORTEGA FLORES, Mgtr,** Tutor(a) del Trabajo de Integración Curricular realizado por la estudiante **CINTHIA LISETH PARRA VEGA** de la carrera de **DERECHO** informo haber revisado el presente documento titulado **"ANÁLISIS DEL TRATAMIENTO DE LOS DATOS DE SALUD DE ACUERDO AL MARCO JURÍDICO ECUATORIANO"**, el mismo que se encuentra elaborado conforme a lo establecido en el Reglamento de Titulación y el Manual de Estilo de la Universidad Iberoamericana del Ecuador, UNIB.E de Quito, por lo tanto, autorizo la entrega del Trabajo de Integración Curricular a la Unidad de Titulación para la presentación final ante el tribunal evaluador.

Atentamente,

Mgtr. Estefanía Pamela Ortega Flores
Tutora

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

UNIB.E
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Facultad: Jurisprudencia

Carrera: Derecho

Modalidad: Híbrida

Nivel: 3er nivel de Grado

En el Distrito Metropolitano de Quito a los diecisiete días del mes de septiembre del 2024 (17-09-2024) a las 09H00 (09:00), ante el Tribunal de Presentación Oral, se presentó la señorita: **PARRA VEGA CINTHIA LISETH**, titular de la cédula de ciudadanía No. **1727085779** a rendir la evaluación oral del Trabajo de Integración Curricular: **"ANÁLISIS DEL TRATAMIENTO DE LOS DATOS DE SALUD DE ACUERDO AL MARCO JURÍDICO ECUATORIANO.**", previo a la obtención del Título de Abogada. Luego de la exposición, la referida estudiante obtiene las calificaciones que a continuación se detallan:

	Calificación
Lectura del Trabajo de Integración Curricular	9 /10
Evaluación Oral del Trabajo de Integración Curricular	8,2 /10
Calificación Final del Trabajo de Integración Curricular	8,6 /10

Para constancia de lo actuado, los miembros del Tribunal de Presentación Oral del Trabajo de Integración Curricular, firman el presente documento en unidad de acto, a los diecisiete días del mes de septiembre del 2024 (17-09-2024).

UNIB.E
FACULTAD DE JURISPRUDENCIA

Dr. Thelman Cabrera
DECANO DE LA FACULTAD DE JURISPRUDENCIA

Mgst. Mayra Guerra
DIRECTORA DE LA CARRERA DE DERECHO

UNIB.E
SECRETARÍA ACADÉMICA GRADO

Mgst. Estefanía Ortega
TUTOR

Mgst. Roberto Zurita
LECTOR

DEDICATORIA

Quiero dedicar este trabajo, principalmente a mi persona por no rendirme y llegar hasta el último semestre de esta hermosa carrera, que, aunque tiene su lado complicado, también tiene muchas puertas abiertas en cualquier rama en la que quiera ejercer. También le dedico mi trabajo, a mis padres y amigas

Agradecimiento

Primero quiero agradecer a Dios y a mis padres por ser mi guía en este arduo camino, por ser mi soporte y apoyo en momentos buenos y malos.

También quiero agradecer a mis amigas Alisson y Patricia por su linda amistad. Soy muy afortunada de coincidir con ellas en este camino universitario. Son de esas personas que se conocen una vez en la vida y te dejan una huella imborrable en el alma y el corazón. Gracias por escucharme, por sus consejos, por las miles de sonrisas que sanan un poquito la vida y te recargan de energía, también por los momentos en que nos ponemos sentimentales y lloramos juntas por ser mis compañeras de aventuras, gracias por aguantar mi carácter un poquito complicado. Espero que nuestra amistad vaya más allá de 4 paredes de universidad y sigamos acompañándonos en el futuro exitoso que nos espera. No me alcanzan las palabras para describir lo que significan para mi y no quiero llorar. Las amo.

Le agradezco infinitamente a mi tutora, MSc. Estefanía Ortega, por su paciencia, por su guía y ayuda en este trabajo. Es una excelente docente y una gran abogada.

ÍNDICE

Tabla 1 Cuadro comparativo de la normativa de protección de datos personales

CINTHIA LISETH PARRA VEGA. ANÁLISIS DEL TRATAMIENTO DE LOS DATOS DE SALUD DE ACUERDO AL MARCO JURÍDICO ECUATORIANO. DERECHO UNIVERSIDAD IBEROAMERICANA DEL ECUADOR. QUITO.20-SEPTIEMBRE-ECUADOR 2024. (81 HOJAS)

RESUMEN

Este trabajo de titulación abarca el análisis del tratamiento de los datos de salud y su aplicación en Ecuador, de acuerdo con el marco jurídico vigente. Dentro del mismo se desprende la vulneración del derecho a la privacidad, derivado de la inadecuada infraestructura tecnológica en los centros de salud, acompañado de la deficiencia en relación a las políticas internas para el tratamiento de los datos de salud, que abarca desde la recolección, registro, conservación, utilización y destrucción de los mismos. De esto se desprende que los datos de salud están comprometidos nuevas a modalidades de ciberataques, para el robo de la información altamente sensible. La metodología propone un paradigma jurídico dogmático e interpretativo, con enfoque cualitativo y diseño hermenéutico para interpretar profundamente la normativa legal. El principal resultado de la investigación radica en que se identifican deficiencias significativas en las políticas internas de protección de datos en los centros de salud, especialmente en relación con el Art. 38 de la normativa de protección de datos, que exige medidas para enfrentar riesgos y accesos no autorizados a los datos de salud. Se concluye que el estado actual de la protección de datos de salud en Ecuador es deficiente, ya que los centros de salud no cuentan con las medidas de seguridad adecuadas para la protección y tratamiento de datos de salud.

Palabras clave: salud, tratamiento, vulneración, privacidad, protección, políticas internas.

INTRODUCCIÓN

En la era digital actual, donde los avances tecnológicos han permeado todos los ámbitos de la vida, la protección de los datos personales se ha convertido en un tema de suma relevancia. Esto cobra especial importancia cuando se trata de información sensible como los datos relativos a la salud de las personas. Estos datos, que revelan aspectos íntimos sobre el estado físico y mental de un individuo, requieren de los más altos estándares de protección y confidencialidad.

En Ecuador, pese a que el derecho a la protección de datos personales fue reconocido en la Constitución de la República del Ecuador de 2008, no fue hasta el año 2021 que se promulgó la Ley Orgánica de Protección de Datos Personales. Esta ley sienta las bases legales para regular el tratamiento adecuado de la información personal de los ciudadanos, estableciendo principios, derechos, obligaciones e instituciones encargadas de velar por su cumplimiento.

El presente trabajo de titulación se enfoca en analizar el tratamiento de los datos de salud en el contexto ecuatoriano, a la luz del marco jurídico vigente. Se aborda esta temática debido a la sensibilidad y vulnerabilidad inherente a este tipo de información, cuyo manejo inadecuado puede derivar en graves violaciones a la privacidad de los pacientes, así como en discriminación y menoscabo de sus derechos fundamentales.

El presente trabajo de titulación aborda un tema de gran relevancia en el ámbito jurídico y de la salud pública: el análisis del tratamiento de los datos de salud de acuerdo con el marco jurídico ecuatoriano, por lo que es fundamental garantizar la adecuada protección de estos datos sensibles para salvaguardar los derechos fundamentales de los pacientes, como la privacidad, la intimidad y la no discriminación. Este estudio exhaustivo examina las leyes, normativas y regulaciones vigentes en Ecuador relacionadas con el manejo de los datos de salud, evaluando su aplicación práctica y su alineación con los estándares internacionales en materia de protección de datos personales.

En el capítulo I, se presenta el planteamiento del problema, el cual gira en torno a la vulneración del derecho a la privacidad derivado de la inadecuada infraestructura tecnológica en los centros de salud. Se exponen los objetivos generales y específicos que guiarán la investigación, así como la justificación que respalda la importancia y relevancia del estudio desde diversas perspectivas, incluyendo el aspecto social, académica, jurídica y metodológica.

El capítulo II se enfoca en el marco teórico o jurídico del trabajo, donde se abordan los antecedentes de la investigación y se establecen las bases teóricas fundamentales. Aquí se exploran conceptos clave como el origen de la protección de datos personales, las definiciones de dato personal, dato de salud, anonimización o técnica de tratamiento de datos y tratamiento de datos. Además, se presentan los actores principales involucrados en la protección de datos relativos a la salud y se analizan las bases legales aplicables, como la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales y otras normativas relevantes.

En el capítulo III, se detalla la metodología de la investigación empleada en el presente trabajo. Se describe la naturaleza de la investigación, el paradigma jurídico dogmático e interpretativo adoptado, así como el enfoque cualitativo utilizado. Además, se explica el diseño de investigación hermenéutico, la unidad de análisis seleccionada y las técnicas de recolección y análisis de datos aplicadas, como la revisión documental y el uso de fichas de registro.

En el capítulo IV se elabora el análisis de resultados de los objetivos específicos planteados. La discusión de los resultados se enriquece mediante la incorporación de información pertinente extraída de diversas fuentes. Se hace especial énfasis en la integración de elementos normativos y doctrinales relevantes, que proporcionan un sólido respaldo legal a las interpretaciones presentadas.

El capítulo V constituye la culminación del trabajo de titulación, presentando los hallazgos y reflexiones derivadas de la exhaustiva investigación realizada. Este apartado sintetiza los hallazgos más relevantes y propone acciones concretas basadas en el análisis efectuado.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

En el Ecuador, el primer acercamiento hacia el reconocimiento de la protección de datos personales se dió en la Constitución de la República del Ecuador a través de la reforma constitucional realizada en 1996, que modificó la Constitución de 1976. Esta reforma sentó las bases iniciales para el resguardo legal de la información privada de los ciudadanos ecuatorianos. Fue hasta el año 2008 en que el país reconoció constitucionalmente el derecho a la protección de datos personales, desde un enfoque europeo, que defiende elevados estándares de salvaguarda. En ese orden de ideas, la Constitución de la República del Ecuador en el artículo 66 numeral 19 estipula que:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución de la República del Ecuador, 2008, art 66 num.19).

Este derecho fundamental se ha consolidado en las legislaciones modernas como un mecanismo esencial para salvaguardar la privacidad y la autodeterminación informativa de las personas en el contexto del tratamiento masivo de datos personales. Además, este derecho a la protección de datos personales busca equilibrar los intereses legítimos de los responsables del tratamiento con los derechos y libertades fundamentales de los titulares de los datos, fomentando un entorno de confianza y respeto a la privacidad en el manejo de la información personal.

Consecuentemente, con la promulgación de la Ley Orgánica de Protección de Datos Personales (en adelante LOPDP) en 2021 introdujo nuevas obligaciones para organizaciones públicas y privadas en todo el país. Uno de los propósitos de esta ley es aprovechar de manera legítima el potencial de los datos y reducir el riesgo de su mal uso o acceso ilegal.

La ley también contempla efectos territoriales que protegen los datos personales de los ciudadanos ecuatorianos, incluso si son procesados en otros países. De igual modo, la ley establece que el consentimiento válido del titular para el tratamiento de sus datos personales debe ser libre, específico, informado e inequívoco. En otras

palabras, se le otorga al ciudadano la capacidad de decidir quién, cómo, cuándo y para qué se procesará su información personal. Además, la norma estipula que todo procesamiento de datos personales deberá tener fines legítimos, los cuales podrán ser revisados por la Autoridad de Protección de Datos Personales.

En ese sentido, el artículo 4, de la ley en mención LOPDP(2021), establece que el dato personal es:

> El dato que identifica o hace identificable a una persona natural, directa o indirectamente". De manera que, la unidad mínima objeto de tutela puede ser de diverso contenido y naturaleza y, puede estar disponible en cualquier formato; ya que, la condición esencial es que permita identificar a su titular, con o sin la ejecución de procedimientos informáticos.

Además, la normativa en cuestión establece cuatro tipos especiales de datos personales que reciben un tratamiento restringido o prohibido. Dicha clasificación incluye los datos sensibles, datos de niñas, niños y adolescentes, datos de personas con discapacidad y de sus sustitutos relativos a la discapacidad y siendo uno de ellos el objeto de estudio, datos relativos a la salud. La Ley Orgánica de Protección de Datos Personales en el art. 30 define a los datos relativos a la salud como: "aquellos relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

Esta definición legal sienta las bases para el tratamiento de los datos relativos a la salud en Ecuador, estableciendo claramente qué información se considera parte de esta categoría especial y, por lo tanto, debe cumplir con los requisitos y garantías adicionales que establece la normativa para salvaguardar los derechos y libertades de los titulares de estos datos sensibles.

Así mismo, el Artículo 32 de la Constitución ecuatoriana establece que:

> la salud es un derecho garantizado por el Estado y que su realización está vinculada al ejercicio de otros derechos fundamentales, como el derecho a la intimidad, ya que este derecho es considerado un bien personal, un derecho subjetivo que no se transfiere ni se negocia, en virtud que la persona decide qué aspectos de su vida admite compartir y cuáles no. Desde la intimidad, se puede llegar al honor, imagen, fama reputación, reserva, confidencialidad, secreto, derecho al olvido, verdad, entre otros.

Los datos relativos a la salud son especialmente protegidos debido a que refieren aspectos íntimos y sensibles del individuo. Por lo cual, la normativa vigente ha calificado a los datos de salud como datos sensibles que necesitan un tratamiento adecuado para su protección.

En torno a que la sensibilidad de los datos personales se evalúa según el perjuicio o daño que podría causarle a una persona si esa información fuera expuesta públicamente. En otras palabras, los datos personales que reciben una protección especial o que se consideran categorías especiales siendo uno de ellos los datos relativos a la salud que, de ser manejados inadecuadamente, afectan directamente la privacidad del individuo e impactan en el ejercicio de otros derechos fundamentales.

Gracias al notable avance de las tecnologías informáticas y de comunicación, los usuarios pueden acceder a todo tipo de datos desde cualquier lugar y en cualquier momento. La problemática central gira en torno a que se vulnera derecho a la privacidad, derivado de infraestructura tecnológica inadecuada en muchas instituciones de salud, ya que no existe una protección y tratamiento de los datos de salud que sea seguro. Angarita (2019) manifiesta que: “a pesar de la existencia de un marco legal, muchos centros médicos del Ecuador, carecen de sistemas informáticos modernos y seguros que establece la LOPDP para llevar a cabo el tratamiento de los datos de salud.

Así mismo González (2020) asegura que: “muchos profesionales de la salud y personal administrativo no están suficientemente familiarizados con las mejores prácticas en seguridad de la información o con las implicaciones legales del manejo inadecuado de datos sensibles”. Esta falta de conocimiento puede llevar a errores humanos que comprometan la confidencialidad de los datos de los pacientes, incluso sin intención maliciosa.

En lo que respecta a la vulneración del derecho a la privacidad, se debe entender que es el derecho a la privacidad, por lo que Altamirano (2000) al referirse a este derecho manifiesta que es: “un derecho fundamental que protege la esfera personal y familiar de las personas, así como el resguardo de su información y datos personales”. Este derecho abarca la facultad de las personas de controlar la recolección, uso, almacenamiento y divulgación de su información personal. La privacidad en el ámbito de la salud es fundamental para mantener la confianza entre pacientes y profesionales médicos. Cuando se comprometen los datos de salud y se viola directamente este derecho esencial, los pacientes pueden sentirse expuestos y vulnerables, lo que podría llevarlos a ocultar información importante a sus médicos en el futuro, comprometiendo así la calidad de su atención médica. Las consecuencias de que se

vulnere el derecho a la privacidad trae una serie de factores como: la discriminación, robo de identidad médica, extorsión.

En lo que refiere a la discriminación Alcalá (2006) manifiesta que se considera como "un trato desigual hacia individuos o grupos, cuando esta discriminación se basa en criterios prohibidos, como el sexo, la etnia, entre otros."

La discriminación resultante de la filtración o mal uso de datos de salud es una preocupación seria que subraya la importancia de una protección robusta de esta información. Cuando los datos médicos personales caen en manos equivocadas o son utilizados de manera inapropiada, pueden conducir a diversas formas de trato desigual y prejuicioso contra los individuos afectados.

En el ámbito laboral, por ejemplo, un empleador podría negar oportunidades de empleo o promoción basándose en información médica confidencial obtenida de manera ilícita. Esto podría afectar particularmente a personas con condiciones crónicas, enfermedades genéticas o historiales de salud mental. En el contexto social, la divulgación no autorizada de información médica sensible puede llevar al estigma y la exclusión, especialmente en casos de enfermedades como el VIH/SIDA o ciertas condiciones de salud mental. Esta discriminación no solo viola los derechos fundamentales de las personas, sino que también puede tener impactos negativos duraderos en su calidad de vida y oportunidades futuras.

De igual manera, Razza (2021) manifiesta que el robo de identidad médica ocurre cuando:

> "alguien usa la información personal de otra persona (como el nombre, fecha de nacimiento, información de seguro médico, etc.) para obtener productos o servicios médicos o utiliza la información de la víctima para realizar reclamaciones falsas sobre productos o servicios médicos"

Una de las formas más comunes de robo de identidad médica ocurre cuando el perpetrador utiliza la información del seguro médico de la víctima para obtener tratamientos o medicamentos. Esto puede resultar en cambios en el historial médico de la víctima, lo que podría llevar a diagnósticos erróneos o tratamientos inadecuados en el futuro. Por ejemplo, si el ladrón de identidad recibe tratamiento para una condición que la víctima no tiene, esto podría quedar registrado en el historial médico y confundir a futuros proveedores de atención médica.

Además del impacto en la atención médica, el robo de identidad médica puede tener graves consecuencias financieras para la víctima. Las facturas por servicios médicos no autorizados pueden acumularse rápidamente, y la víctima puede encontrarse luchando contra deudas sustanciales que no incurrió. En algunos casos, esto puede llevar a problemas de crédito si las facturas no pagadas son enviadas a agencias de cobro.

En lo referente a la extorsión, la posesión de información médica confidencial por parte de actores malintencionados puede llevar a situaciones de extorsión. Los delincuentes pueden amenazar con revelar información médica sensible a menos que se les pague. Esto puede ser particularmente devastador cuando se trata de condiciones estigmatizadas o información que el paciente desea mantener en privado. La extorsión no solo tiene un impacto financiero, sino que también causa un estrés psicológico significativo, ya que las víctimas viven con el temor constante de que su información personal sea expuesta. Este tipo de amenaza puede afectar gravemente la salud mental y el bienestar general de la persona.

En lo concerniente a riesgos para la vida de los pacientes (Angarita, 2019) dice que “la consecuencia más grave de la violación de datos de salud es el riesgo directo para la vida de los pacientes”.

Si los registros médicos son alterados o no están disponibles debido a un ataque cibernético, los médicos podrían tomar decisiones basadas en información incorrecta o incompleta. Esto puede llevar a errores en el diagnóstico, prescripción de medicamentos inadecuados o incompatibles, o retrasos en tratamientos críticos. En situaciones de emergencia, donde el acceso rápido a información médica precisa es crucial, la falta de disponibilidad de estos datos debido a un ataque cibernético podría tener consecuencias fatales.

En este sentido, la norma mencionada indica que, los datos relacionados con la salud deben ser previamente anonimizados o seudonimizados. No obstante, establece que cualquier tratamiento de este tipo de datos anonimizados debe ser autorizado previamente por la Autoridad de Protección de Datos Personales. Para ello, la persona interesada debe presentar ante dicha autoridad un protocolo técnico que garantice la

protección de los datos y que cuente con un informe favorable previo emitido por la Autoridad Sanitaria.

Así mismo, la protección de datos personales a nivel internacional, está adquiriendo una importancia creciente. Diversos países han establecido o se encuentran en proceso de establecer sus propias normativas de protección de datos o de actualizar y fortalecer las ya existentes, tomando como referencia, en gran medida, el modelo sentado por el Reglamento General de Protección de Datos de la Unión Europea.

Como se mencionó, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea establece la normativa internacional de protección de datos más rigurosa y estricta, lo cual la ha convertido en un modelo a seguir para muchas otras leyes de protección de datos en distintos países. Por lo tanto, cada vez es más común encontrar similitudes entre las legislaciones de protección de datos de otros países y el RGPD.

Si bien hay marcos legales vigentes que regulan la protección de datos, las evidencias a nivel mundial señalan que los riesgos y amenazas cibernéticas están aumentando a un ritmo vertiginoso, en paralelo con los avances en las tecnologías de la información y las comunicaciones. Esta situación resulta especialmente alarmante cuando se trata del manejo de datos sensibles vinculados con la salud de las personas.

Es imperativo que las regulaciones sobre protección de datos se mantengan actualizadas y se implementen rigurosamente para proteger la confidencialidad de la información médica. Uno de los principales doctrinarios que ha definido y conceptualizado la regulación de la protección de datos personales es el jurista español Lombarte (2019) y manifiesta que:

> "La protección de datos personales aparece configurada como un derecho fundamental autónomo que dispone de un objeto y contenido propio, el cual no se agota en la estricta privacidad de los datos personales, sino que se proyecta en un haz de facultades que la norma atribuye a los ciudadanos para oponerse a que determinados datos sean tratados o, en su caso, imponer el consentimiento para dicho tratamiento". (pág. 10)

Según Lombarte (2019), la regulación de la protección de datos personales: "consiste en un derecho fundamental que faculta a las personas a controlar y decidir sobre el tratamiento de sus datos personales por parte de terceros".

Es por ello que la protección de datos se ha convertido en un tema importante en el Ecuador. De manera especial cuando se trata de datos sensibles, como los datos relativos a la salud. Debido a que esta información refiere a ámbitos muy delicados de la intimidad de una persona (Esto implica que, los centros sanitarios en los que se tratan datos personales de categoría especial, deben velar por la protección de los derechos y los datos de los pacientes.

Pregunta central de la investigación

¿Cómo se protegen los datos de salud en Ecuador, en concordancia con el marco jurídico vigente?

Objetivos de la investigación

Objetivo general.

Analizar la protección y tratamiento de datos de salud y su aplicación en el Ecuador.

Objetivos específicos

- Evaluar las políticas internas para el tratamiento de datos de salud aplicadas en los centros de salud del Ecuador
- Analizar el rol del superintendente de protección de datos personales en el ámbito de la salud
- Realizar un análisis comparativo de la normativa sobre la protección de datos personales entre Ecuador, España y Argentina.

Justificación de la investigación

La realización de esta investigación sobre el "Análisis del Tratamiento de los Datos de Salud de Acuerdo al Marco Jurídico Ecuatoriano" se justifica por diversas razones de relevancia tanto en el ámbito de la salud como en el de la protección de datos personales. Desde la perspectiva legal, es fundamental profundizar en el análisis del tratamiento de los datos de salud, ya que se trata de información altamente sensible y confidencial, cuyo manejo inadecuado puede derivar en graves violaciones a los derechos fundamentales de los pacientes, como la privacidad, la intimidad y la no discriminación.

El marco jurídico ecuatoriano, particularmente la Ley Orgánica de Protección de Datos Personales, establece principios, derechos, obligaciones e instituciones encargadas de velar por la protección de estos datos. Sin embargo, es necesario examinar a fondo la aplicación efectiva de esta normativa en el sector de la salud, identificar posibles vacíos legales o desafíos en su implementación, y proponer mejoras o reformas que garanticen una adecuada salvaguarda de la información médica de los ciudadanos.

La investigación propuesta tiene un valioso aporte social, ya que busca proteger uno de los derechos fundamentales más preciados de los ciudadanos: la privacidad y confidencialidad de su información médica. Al analizar el tratamiento de los datos de salud y proponer mecanismos para su adecuada protección, se contribuye a salvaguardar la dignidad y la integridad de los pacientes, evitando situaciones de discriminación, estigmatización o vulneración de su intimidad personal. Esto, a su vez, fomenta la confianza de la sociedad en el sistema de salud y en el manejo ético y responsable de sus datos sensibles, lo cual es crucial para garantizar el acceso equitativo a los servicios médicos y el pleno ejercicio del derecho a la salud.

Desde el ámbito académico, este trabajo de titulación representa una contribución significativa al campo del derecho, particularmente en el área de la protección de datos personales y el derecho a la intimidad. Al abordar una temática de gran actualidad y relevancia jurídica, como es el tratamiento de los datos de salud, se generan nuevos conocimientos y se profundiza en el análisis de la normativa vigente y su aplicación práctica. Además, al realizar un análisis comparativo con otros países, se enriquece el debate académico y se fomentan espacios para el intercambio de experiencias y buenas prácticas a nivel internacional. Este trabajo puede servir como referencia y punto de partida para futuras investigaciones en el campo de la protección de datos y los derechos fundamentales en el ámbito de la salud.

Desde una perspectiva científica, este estudio contribuye al avance del conocimiento en un área interdisciplinaria que involucra el derecho, la medicina y las tecnologías de la información y la comunicación. Al analizar el tratamiento de los datos de salud y su protección legal, se abordan aspectos técnicos y científicos relacionados con la gestión de información médica en entornos digitales, la ciberseguridad, la privacidad de datos y la ética en el manejo de información sensible. Esto puede generar nuevos enfoques, metodologías y recomendaciones para el manejo seguro y ético de los

datos de salud, considerando los avances tecnológicos y los desafíos emergentes en este campo.

Desde el punto de vista metodológico, el presente trabajo puede aportar nuevas técnicas y herramientas para el análisis jurídico y la investigación en el campo del derecho. Al combinar métodos cualitativos, como el análisis documental y las entrevistas a expertos, con métodos cuantitativos, como el análisis de datos y estadísticas, se puede obtener una visión integral y multidimensional del problema de investigación. Además, al realizar un estudio comparativo con otros países, se pueden adaptar metodologías y enfoques utilizados en otros contextos legales y culturales.

CAPITULO II

MARCO TEÓRICO O JURÍDICO

Para entender que es el marco teórico, Villamil (2021) manifiesta que:

> "El marco teórico es la presentación ordenada, coherente y articulada de los conceptos, teorías, principios, postulados, investigaciones y antecedentes que permiten fundamentar, analizar e interpretar el objeto de estudio de la investigación. Se construye a partir de la revisión de la literatura especializada y actualizada sobre el tema abordado". (pág. 32)

El marco teórico no es simplemente una recopilación de información, sino una construcción coherente, articulada y fundamentada que permite comprender el objeto de estudio desde una perspectiva teórica sólida. Además, enfatiza la importancia de basarse en fuentes especializadas y actualizadas para asegurar la rigurosidad y pertinencia del sustento teórico de la investigación.

Antecedentes de la investigación

Según Hernández, Fernández y Baptista (2014) es necesario conocer los antecedentes (estudios, investigaciones y trabajos anteriores), especialmente si uno no es experto en los temas o tema que vamos a tratar o estudiar, afirmando:

> Conocer lo que se ha hecho con respecto a un tema ayuda a: No investigar sobre algún tema que ya se haya estudiado a fondo, a estructurar más formalmente la idea de investigación a seleccionar la perspectiva principal desde la cual se abordará la idea de investigación. (p.28)

Conocer esto permitirá elaborar una investigación que sea novedosa, e incluso inédita, así nuestra investigación tendrá una temática con mayor claridad, sustentada de conocimientos científicos previos.

Un primer antecedente es de Vivar (2022), en su artículo científico denominado "Las buenas prácticas para el tratamiento del dato de salud" describe brevemente sobre el dato de salud, el motivo de su sensibilidad, qué datos son vinculados como datos de salud y cuál es el debido tratamiento que se debe de tener con este tipo de dato, el objetivo por el cual realizó este artículo es que todos los lectores se informen respecto a qué engloba el dato de salud, y cómo debe ser este tratado apropiadamente. Así también, explica sobre algunas buenas prácticas para el tratamiento de este dato considerado como sensible, que sobre todo buscan proteger

la intimidad del titular del dato. Los resultados de la investigación es que se mencionan dos buenas prácticas para el tratamiento del dato personal: la práctica del secreto profesional y la anonimización del dato. Respecto de la primera, ésta es inherente al ejercicio profesional del médico, quien a su vez debe garantizar que el personal que trabaje con él, también mantenga la confidencialidad y secreto de la información que recaba del paciente que trata; y, respecto de la segunda, resulta novedosa, puesto que de cierta manera desasocia la identidad del titular del dato y el dato per sé, por lo que no se podría arribar a la conclusión de que determinada persona es la titular de un dato en concreto. No se descartan aquellas no enunciadas aquí o que puedan crearse a lo largo del tiempo, puesto que la imaginación es el límite que permite diseñar técnicas para tratar legítimamente todo dato personal; sin embargo, no hay duda de que ambas prácticas funcionan y cumplen con su finalidad de tratar apropiadamente el dato de salud, por lo que, si nosotros como ciudadanos estamos frente a ellas, podemos estar tranquilos respecto al tratamiento que se les da a nuestros datos en dicho campo.

Este artículo científico expuesto aporta al trabajo de investigación que se desarrolla ya que, dentro del mismo se define que son los datos de salud, dato personal, tratamiento de datos, anonimización de datos y que se lo clasifica como un dato sensible. Por lo cual aporta al marco teórico ya que contiene doctrina de personas expertas en el tema y puedo usarlo para construir las bases teóricas del trabajo de titulación.

Un segundo antecedente es de Jara (2022), el cual se desarrolló en la Universidad Católica de Cuenca, una tesis de maestría titulada “Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano”, cuyo objetivo fue analizar el nivel de cumplimiento de la nueva Ley Orgánica de la Protección de Datos Personales en lo que respecta a los datos relativos a la salud en un integrante de los subsistemas de salud ecuatoriano. La investigación tiene enfoque cualitativo, para el análisis se utilizó la información que se ha recopilado sobre la historia clínica electrónica del desarrollador, se establece el cumplimiento de las garantías legales de los usuarios a la protección de sus datos personales según el marco jurídico vigente. Como resultados, se propusieron mecanismos de acción para que este derecho se garantice. Como conclusión, con la información recopilada se determinó que en la institución objeto de análisis, los sistemas de información no son confiables, existen

brechas de seguridad en la administración de usuarios, no posee la característica de la interoperabilidad entre los sistemas que garanticen la confidencialidad y secreto profesional, no se hallan acuerdos o documentos que comprometan a los usuarios a guardar el estricto nivel de confidencialidad.

La investigación citada aporta al presente trabajo porque analiza el nivel de cumplimiento de la nueva Ley Orgánica de la Protección de Datos Personales en lo que respecta a los datos relativos a la salud en un integrante de los subsistemas de salud ecuatoriano. Es decir, aporta a la problemática planteada en el presente trabajo y cuáles son las consecuencias del incumplimiento establecido en la normativa en lo relativo a la protección de datos de salud ya que las instituciones sanitarias deben disponer de políticas de protección de sus datos informáticos, con el propósito de que usuarios no autorizados no puedan obtener datos de salud de los pacientes.

Un tercer antecedente de Valle (2022), en su tesis doctoral titulada “La Protección De Los Datos Personales Relativos a la Salud. La Historia Clínica Como Eje Vertebrador”, cuyo objetivo fue analizar el escenario regulatorio en el cual se enmarca, en la actualidad, la protección de los datos personales de salud. Para alcanzar los objetivos en dicha investigación se utilizó la metodología descriptiva con técnicas de análisis documental, a partir de la legislación nacional e internacional aplicable a la materia objeto de estudio, así como de los distintos trabajos doctrinales vertidos sobre la misma. Asimismo, se realizó entrevistas a profesionales de la salud. A todo ello se aplica el método deductivo para concluir de lo general a lo particular.

La tesis antes mencionada aporta al trabajo en desarrollo, ya que, analiza el escenario regulatorio en el cual se enmarca la protección de los datos personales de salud, haciendo un recorrido por las fuentes normativas referentes a la tutela de tales datos.

BASES TEÓRICAS

Para entender que son las bases teóricas, Carlino (2021) manifiesta acerca de esto lo siguiente:

> las bases teóricas son las nociones asumidas por el autor del proyecto, procedentes de otros autores con cuyo pensamiento adhiere, y que le sirven para entender el problema que estudiará y/o le servirán para interpretar los datos que recoja. Estos conceptos teóricos funcionan como supuestos, puntos de partida, pero también como lentes, puntos de mira, con los que el investigador aborda el fenómeno que investiga. Dan cuenta de la postura teórica que elige adoptar para pensar su investigación. (pág. 10)

En esta sección se establecerán las bases teóricas, inicialmente, se definirán conceptos clave como dato personal, dato de salud, anonimización de datos y tratamiento de datos, los cuales son esenciales para comprender el tema central. Luego, se identificarán los actores principales involucrados en el derecho a la protección de datos de salud, tales como el titular de los datos, el responsable y encargado del tratamiento, los destinatarios, la autoridad de protección de datos personales y el delegado de protección de datos.

Origen de protección de datos personales

El origen de la protección de datos personales a nivel mundial se remonta a la segunda mitad del siglo XX, surgiendo como respuesta a los avances tecnológicos y la creciente preocupación por la privacidad individual. En la década de 1970, con el auge de las computadoras y el procesamiento automatizado de la información, surgieron las primeras leyes de protección de datos. Razza (2021).

Razza (2021) sostiene que: “Alemania fue pionera con la Ley de Protección de Datos de Hesse en 1970”. Estos primeros esfuerzos reconocían la necesidad de regular la recopilación y el uso de información personal en la era digital. Un hito significativo fue la adopción del Convenio 108 del Consejo de Europa en 1981, Razza (2021) dice que este fue “el primer instrumento internacional jurídicamente vinculante en materia de protección de datos”. Este convenio sentó las bases para muchas leyes nacionales en Europa y más allá.

En la década de 1990, con la expansión de Internet, la protección de datos adquirió una nueva dimensión. La Unión Europea adoptó la Directiva de Protección de Datos en 1995, que estableció un marco integral para la protección de datos personales en todos los estados miembros. El tratamiento de datos personales se convirtió en un tema central de estas regulaciones. Razza (2021) argumenta que: “se establecieron principios fundamentales como el consentimiento del titular, la limitación de la finalidad, la minimización de datos y la seguridad del tratamiento”. Estos principios buscaban asegurar que los datos personales fueran manejados de manera justa y transparente.

En el siglo XXI, la protección de datos ha ganado aún más relevancia con la explosión de las redes sociales, y la inteligencia artificial. El Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que entró en vigor en 2018, marcó un nuevo estándar global, influyendo en legislaciones de todo el mundo. En Ecuador, la protección de datos personales llegó más tarde que en muchos países desarrollados, La Constitución de 2008 reconoció el derecho a la protección de datos personales como un derecho fundamental. Sin embargo, durante varios años, Ecuador careció de una ley específica que regulara comprehensivamente esta materia.

En 2021, Ecuador dio un paso significativo con la aprobación de la Ley Orgánica de Protección de Datos Personales y el Reglamento General de la Ley Orgánica de Protección de Datos Personales. La ley ecuatoriana aborda aspectos cruciales del tratamiento de datos, incluyendo los principios de licitud, lealtad y transparencia, la limitación de la finalidad, la anonimización de datos, y la seguridad del tratamiento. También establece los derechos de los titulares de los datos y las obligaciones de los responsables y encargados del tratamiento. Un aspecto importante de la ley ecuatoriana es la creación de la Superintendencia de Protección de Datos Personales, como autoridad de control encargada de velar por el cumplimiento de la normativa.

DEFINICIONES

Dato personal

Para comprender que es el dato personal se debe tener en cuenta que según Uivaru (2017), “Los datos personales son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Nos dan identidad, nos describen y precisan”.

La afirmación de que los datos personales son aquella información que se relaciona con nuestra persona, resalta la amplitud de lo que puede considerarse un dato personal, incluyendo desde información básica como: nombres, apellidos, estado civil, dirección domiciliaria, hasta los datos más complejos como patrones de comportamiento e historial médico.

En lo concerniente a los patrones de comportamiento, Araujo (2021) manifiesta que: “se refieren a las formas recurrentes y predecibles en que una persona actúa o interactúa con su entorno”. Estos patrones son muy reveladores sobre la identidad y personalidad de un individuo, ya que incluyen hábitos de navegación en internet, es decir los sitios web que una persona visita regularmente, el tiempo que pasa en ellos, y los tipos de contenido que comparte.

En lo referente al historial médico, Bianchi (2018) sostiene que: “es un conjunto de información altamente personal y sensible que documenta la salud de un individuo a lo largo del tiempo”. Por lo cual, como dato personal el historial médico es particularmente crítico debido a su naturaleza íntima y su potencial impacto en la vida de una persona, porque dentro del mismo se incluye: diagnósticos médicos en los que se establece las condiciones de salud de la persona, enfermedades o trastornos psicológicos.

Así mismo se toma en consideración que el dato personal nos describe, es decir que proporciona un retrato detallado de quiénes somos, ya que incluye aspectos como nuestras características físicas, psicológicas, sociales, económicas y culturales, por ejemplo, nuestro historial de compras puede describir nuestros gustos y hábitos de consumo, mientras que nuestras interacciones en redes sociales pueden ofrecer una visión de nuestra personalidad y relaciones sociales.

Es importante recalcar que debido a que esta información es tan integral para nuestra identidad y puede tener un impacto tan profundo en nuestras vidas, su protección y uso ético, ha llevado al desarrollo de regulaciones de protección de datos en todo el mundo, que buscan salvaguardar la privacidad y los derechos de los individuos sobre la información personal. Consecuentemente, dicha definición presenta a los datos personales no solo como información identificativa, sino como elementos fundamentales que construyen y reflejan nuestra identidad en el mundo moderno. Esta concepción subraya la importancia de proteger y tener un tratamiento adecuado en una sociedad cada vez más digitalizada y conectada.

Dato de salud

Como lo manifiesta León (2000) “Los datos de salud se refieren a la información sobre la salud mental o física de una persona. Revelan información sobre su estado de salud.”

Los datos de salud constituyen un conjunto de información altamente sensible y personal que abarca tanto la salud física como mental de un individuo. Estos datos no se limitan únicamente a diagnósticos médicos específicos, sino que incluyen una amplia gama de información que, directa o indirectamente, puede revelar el estado de salud de una persona.

En el ámbito físico, León (2000) dice que: “los datos de salud pueden incluir registros de consultas médicas, resultados de exámenes clínicos, historiales de tratamientos, prescripciones médicas, e incluso información genética”. Estos datos proporcionan una visión detallada de la condición física de una persona, sus vulnerabilidades y su evolución a lo largo del tiempo.

Por otro lado, en lo que respecta a la salud mental, los datos pueden abarcar registros de terapias psicológicas, diagnósticos de trastornos mentales, historiales de tratamientos psiquiátricos y evaluaciones de estado emocional. Esta información es particularmente delicada, ya que puede tener implicaciones significativas en la vida personal y profesional del individuo.

Es importante destacar que los datos de salud no se limitan a la información generada en entornos médicos tradicionales. Con el avance de la tecnología, ahora incluyen también datos recopilados por dispositivos wearables, es decir, dispositivos electrónicos que se usa en el cuerpo humano, como un reloj inteligente que sirve para transmitir o recoger algún tipo de dato, aplicaciones de salud móviles. Estos nuevos tipos de datos ofrecen una visión más continua y detallada del estado de salud de una persona, pero también plantean nuevos desafíos en términos de privacidad y seguridad.

La protección de los datos de salud es de suma importancia debido a su naturaleza íntima y potencialmente sensible. Su divulgación no autorizada puede tener consecuencias graves, desde discriminación laboral hasta impactos en relaciones

personales. Por lo tanto, el manejo adecuado de estos datos requiere un marco legal robusto y prácticas éticas rigurosas para garantizar su confidencialidad y el respeto a la privacidad del individuo.

Anonimización de datos

(Cano, 2015) denomina a la anonimización como: “una técnica de tratamiento de datos que elimina o modifica los datos personales identificables para obtener datos anónimos que no se pueden asociar con ninguna persona”. En el ámbito de los datos de salud, la anonimización se presenta como una medida de protección adicional para garantizar que la información confidencial sea utilizada de forma legítima y solo con el consentimiento del titular del derecho.

Los datos de salud son extremadamente sensibles y personales. Gómez (2009) sostiene que: “la anonimización permite que esta información valiosa se utilice para investigación, análisis de salud pública o mejora de servicios médicos, sin comprometer la privacidad de los pacientes”. Por ejemplo, se pueden analizar tendencias de enfermedades o efectividad de tratamientos sin revelar la identidad de los individuos involucrados.

En el tratamiento de datos de salud, la anonimización no es un proceso único, sino una estrategia continua que requiere evaluación y ajuste constantes. Implica no solo técnicas de procesamiento de datos. Además Luño (2020) considera que: “la anonimización es como mezclar estas piezas y cambiar su forma para que nadie pueda reconocer la imagen original. Sin embargo, con el tiempo, aparecen nuevas herramientas que pueden ayudar a resolver el rompecabezas más complicado, debido a los avances en tecnología de análisis de datos, ya que estos avances tecnológicos hacen que sea más fácil resolver el rompecabezas de los datos de salud.

Lo que antes parecía imposible de identificar, ahora podría ser descifrado con estas nuevas herramientas, por ejemplo, si antes se pensaba que cambiar el nombre de una persona por un número era suficiente para anonimizar, ahora se sabe que, combinando ese número con otros datos como edad, código postal, se podría identificar a la persona. Por eso, los métodos de anonimización deben actualizarse constantemente, es decir, que los expertos en protección de datos deben estar siempre al tanto de las últimas tecnologías y técnicas de análisis de datos. El objetivo

es mantenerse un paso adelante de las herramientas que podrían usarse para resolver el rompecabezas y revelar información referente a la salud.

Tratamiento de datos

Para Bianchi (2018) el tratamiento es: “cualquier operación o conjunto de operaciones realizadas en datos personales ya sea por procedimientos automatizados o no, como como la recogida, registro, organización, conservación, utilización, destrucción”.

Esta definición ofrece una visión amplia y detallada de las diversas operaciones que pueden realizarse con la información personal, por lo que es fundamental para comprender el alcance y la complejidad del tratamiento de los datos de salud abarcando desde la obtención inicial hasta la eliminación final de la información.

En lo que respecta a la recogida Angarita (2019) sostiene que: “es el punto de partida en el proceso de tratamiento, ya que esta etapa implica la obtención de información directamente de los individuos o de fuentes secundarias”. La forma en que se lleva a cabo esta recogida puede variar desde formularios en línea hasta entrevistas personales. Además de los formularios en línea y las entrevistas personales, existen otros métodos de recolección de datos, como encuestas telefónicas, que para González (2020) “las encuestas telefónicas siguen siendo un método relevante de recolección de datos, especialmente para investigaciones”. Sin embargo, presentan desafíos únicos en cuanto a la verificación de la identidad del encuestado y la obtención de un consentimiento válido. Es importante que los operadores estén bien capacitados en protección de datos y que implementen protocolos claros para el manejo de la información recopilada.

Una vez recogidos los datos, viene la etapa de registro que para Fraguío (2018) implica “su incorporación a un sistema y este proceso debe garantizar la precisión y actualización de la información”. El registro adecuado es esencial para mantener la integridad de los datos y facilitar su posterior acceso y uso. Además, es importante implementar medidas de seguridad apropiadas en esta etapa para proteger la información desde el momento en que se ingresa al sistema.

Para Angarita (2019) la organización de los datos personales “es un proceso que permite clasificar y ordenar la información de manera lógica y eficiente”. Esto facilita

su posterior recuperación y análisis. Un aspecto clave de la organización de datos es la categorización. Para Baena (2015) esto “implica agrupar los datos en categorías lógicas basadas en características comunes. Por ejemplo, en un sistema de gestión de historias clínicas electrónicas, los datos podrían organizarse en categorías como información demográfica del paciente, antecedentes médicos, resultados de pruebas diagnósticas, tratamientos prescritos y seguimiento de enfermedades crónicas. Esta categorización facilita la búsqueda y recuperación de información específica cuando sea necesario, lo que es crucial en el ámbito de la salud. Con esto, un médico puede acceder rápidamente al historial ,ya sea de alergias de un paciente antes de prescribir un nuevo medicamento, o revisar los resultados de laboratorio más recientes para evaluar la progresión de un tratamiento.

Así mismo, Herrero (2021) manifiesta que: “La conservación de datos personales se refiere al almacenamiento y mantenimiento de la información durante el tiempo necesario para cumplir con los fines para los que fueron recogidos”. Este aspecto del tratamiento debe equilibrar la necesidad de retener información útil con el principio de limitación del plazo de conservación. La importancia de este proceso radica en su capacidad para garantizar que la información esté disponible cuando se necesite, pero también en asegurar que no se retenga más allá de lo necesario.

En el contexto de la conservación de los datos de salud, el principio de limitación del plazo de conservación es un concepto fundamental. Para Herrero (2021) “este principio establece que los datos no deben mantenerse de forma indefinida, sino que deben ser eliminados o anonimizados una vez que ya no sean necesarios para los fines originales de su recolección”. La esencia de este principio radica en encontrar un equilibrio entre la utilidad de los datos y el respeto a la privacidad de las personas.

Dicho principio reduce el riesgo de que los datos de salud sean utilizados para fines no autorizados o no previstos inicialmente. Cuanto más tiempo se conservan los datos, mayor es la probabilidad de que sean accedidos o utilizados de manera inadecuada, ya sea por error o de forma malintencionada. Además, la limitación del plazo de conservación ayuda a mitigar los riesgos de seguridad. Las amenazas de seguridad son un riesgo constante en la era actual en la que prevalece la tecnología, y cuanto mayor sea el volumen de datos almacenados, más grave puede ser el

impacto de una violación de datos. Al eliminar o anonimizar los datos que ya no son necesarios, se reduce el riesgo potencial para los ciberdelincuentes.

También se toma en consideración la utilización de los datos de salud, que para Reigada (2021) “abarca cualquier operación que se realice con ellos para cumplir con los fines para los que fueron recolectados, esto puede incluir procesamiento, transferencia o cualquier otra forma de uso”. En primer lugar, el procesamiento de datos de salud es una de las operaciones más críticas y potencialmente transformadoras, ya que Reigada (2021) dice que: “incluye la transformación, limpieza y estructuración de la información para hacerla más útil y accesible”. Es decir, la corrección de errores en los registros, o la integración de datos provenientes de diferentes fuentes, como un historial clínico digital, por lo que un procesamiento adecuado es fundamental para garantizar la calidad y fiabilidad de los datos, lo que a su vez se puede considerar para la toma de decisiones clínicas y la investigación médica.

La transferencia de datos de salud es un aspecto relevante. Reigada (2021) manifiesta que esta operación “implica el movimiento de información médica sensible entre diferentes entidades o sistemas, y su importancia radica en la necesidad de mantener la continuidad y calidad de la atención médica, al tiempo que se protege la privacidad de los pacientes.” Por lo que, en el contexto intrahospitalario, la transferencia de datos puede ocurrir entre diferentes departamentos o servicios. Por ejemplo, cuando un paciente es trasladado de urgencias a una unidad de cuidados intensivos, su historial médico, resultados de pruebas y plan de tratamiento deben ser accesibles para el nuevo equipo médico de manera inmediata y precisa.

Por último se encuentra la destrucción de los datos, que para Herrero (2021) “se refiere al proceso mediante el cual se elimina de forma permanente e irreversible la información personal que ya no es necesaria o cuyo período de conservación ha expirado”. Este proceso es esencial para cumplir con el principio de limitación del plazo de conservación, que establece que los datos personales no deben mantenerse más tiempo del necesario para los fines para los que fueron recolectados.

Se debe tener en consideración que para llevar a cabo cada uno de este proceso de tratamiento de datos, hay que contar con el consentimiento informado, Araujo (2021) determina que:

> "es un pilar fundamental en la recogida ética de datos personales. Esto implica proporcionar a los individuos información clara y comprensible sobre qué datos se están recolectando, por qué se están recolectando, cómo se utilizarán, quién tendrá acceso a ellos, y por cuánto tiempo se conservarán" (pág. 90)

Además, es importante manifestar que el consentimiento de conformidad a la Ley Orgánica de Protección de Datos Personales, debe ser libre, específico, informado e inequívoco, y los individuos deben tener la opción de retirar su consentimiento en cualquier momento. En lo que se denomina libre, Araujo (2021) sostiene que: "El consentimiento debe ser otorgado de manera voluntaria, sin ningún tipo de presión". Esto significa que el individuo debe tener una opción real y la capacidad de rechazar o retirar su consentimiento sin sufrir consecuencias negativas.

Lo que refiere a específico, para Araujo (2021) significa que:" El consentimiento debe ser solicitado para cada finalidad específica del tratamiento de datos". Por ejemplo, si una empresa recolecta datos para mejorar sus servicios y también para compartirlos con terceros con fines publicitarios, debe obtener consentimientos separados para cada uno de estos propósitos. Esto permite a los individuos ejercer un control sobre cómo se utilizan sus datos, aceptando algunos usos mientras rechazan otros si así lo desean.

Además, Araujo (2021) sostiene que para que el consentimiento sea válido, "el individuo debe recibir información clara y comprensible sobre qué datos se recogerán, cómo se utilizarán, quién tendrá acceso a ellos, por cuánto tiempo se conservarán". Esta información debe proporcionarse en un lenguaje sencillo, por lo que el objetivo es asegurar que el individuo comprenda plenamente las implicaciones de dar su consentimiento antes de hacerlo.

Así mismo Araujo (2021) dice que: "El consentimiento debe manifestarse mediante una acción afirmativa clara que indique la voluntad del individuo de permitir el tratamiento de sus datos". Por ejemplo, una forma común de obtener un consentimiento inequívoco es mediante un botón de "acepto" que el usuario debe hacer clic activamente.

Integrantes del sistema de protección de datos personales

Para comprender de mejor manera acerca de los integrantes del sistema de protección de datos personales Herrero (2021) manifiesta una idea acerca de esto:

> un sistema de protección de datos personales sólido y efectivo es fundamental para proteger los derechos de los individuos, generar confianza, promover la innovación responsable y facilitar el cumplimiento normativo en un mundo cada vez más digitalizado y orientado a los datos. (pág. 28)

La cantidad de información personal que se genera y comparte a diario a través de plataformas digitales, dispositivos móviles y servicios en línea es abrumadora. Esta realidad hace que un sistema de protección de datos personales robusto sea más crucial que nunca. Baena (2015) manifiesta que “proteger los derechos fundamentales de los individuos, como la privacidad y la autodeterminación informativa, es esencial para salvaguardar su dignidad y libertades en un mundo cada vez más interconectado”. Un sistema sólido de protección de datos garantiza que las personas tengan control sobre su información personal y establece límites claros sobre cómo esta puede ser recopilada, utilizada y compartida por parte de empresas y organismos. En este sentido, según Herrero. (2021) los principales integrantes del sistema de protección de datos personales son: Titular; Responsable del tratamiento; Encargado del tratamiento; Destinatario; Autoridad de Protección de Datos Personales; y, Delegado de protección de datos personales.

Titular de datos

Según Angarita (2019) el titular de datos “Es la persona física a quien pertenecen y refieren los datos personales. Por lo cual el titular de los datos personales es el dueño de los mismos, aunque éstos se encuentren en posesión de un tercero para su tratamiento”. Es importante destacar que la titularidad de los datos personales no se pierde cuando estos son compartidos o transferidos a terceros. Incluso cuando una persona proporciona sus datos a una empresa, institución gubernamental o cualquier otra entidad, sigue siendo el titular de esos datos. Angarita (2019) también dice que “esto implica que el individuo retiene ciertos derechos sobre cómo se utilizan, almacenan y procesan sus datos personales, lo que se conoce comúnmente como derechos del titular de los datos”.

Estos derechos del titular incluyen el derecho de acceso que es poder ver qué datos se tienen sobre uno. Angarita (2019) sostiene que “este derecho permite al titular obtener información sobre qué datos personales suyos están siendo tratados, con qué finalidad, y quiénes son los destinatarios de esta información”. El acceso no solo implica la posibilidad de ver los datos, sino también de obtener una copia de los mismos, además permite en el contexto de los datos de salud, el derecho de acceso puede incluir la revisión de historiales médicos, resultados de pruebas.

Para Araujo (2021) “el derecho de rectificación otorga al titular la facultad de corregir datos inexactos o completar datos incompletos que le conciernen”. Este derecho es particularmente importante porque garantiza la exactitud de la información personal, lo cual es crucial en muchos contextos, especialmente en el ámbito de la salud. Por ejemplo, un error en el historial médico de un paciente podría llevar a decisiones incorrectas sobre su tratamiento.

Así también el derecho de cancelación, también conocido como derecho de supresión o derecho al olvido, para Araujo (2021) “permite al titular solicitar la eliminación de sus datos personales cuando ya no son necesarios para los fines para los que fueron recogidos, cuando se retira el consentimiento, o cuando los datos se han tratado de forma ilícita”. Este derecho es fundamental en la era digital, donde la información puede persistir indefinidamente si no se toman medidas activas para eliminarla. Sin embargo, es importante notar que este derecho no es absoluto y puede estar sujeto a limitaciones, especialmente en el caso de datos de salud que pueden ser necesarios para futuras atenciones médicas o por razones de interés público.

La implementación efectiva de estos derechos requiere que las instituciones de salud, tengan procesos claros y accesibles para que los titulares puedan ejercerlos. Esto puede incluir formularios de solicitud, plazos de respuesta definidos, y personal capacitado para manejar estas solicitudes de manera adecuada y oportuna.

El Responsable

Para entender lo que es responsable respecto a la protección de datos relativos a la salud Angarita (2019) lo define como:

> la persona física o moral o la institución de gobierno que decide sobre el tratamiento de los datos personales, es decir, la que establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión. (pág. 69)

Esta definición subraya que el responsable puede ser una entidad diversa, una persona natural, o jurídica. Esto refleja la realidad del sector salud, donde los datos pueden ser manejados por hospitales privados, clínicas, laboratorios, instituciones de investigación médica, o sistemas de salud pública. También especifica que el responsable establece las finalidades del tratamiento, es decir, determina para qué se utilizarán los datos de salud. En el contexto médico, esto puede incluir propósitos como la prestación de atención médica, la facturación de servicios, la investigación clínica, o la gestión de salud pública.

El poder de decisión que tiene el responsable sobre el tratamiento de los datos personales de salud implica una autoridad significativa que debe ejercerse con sumo cuidado y consideración. Esta capacidad de determinar cómo se utilizará la información médica abarca múltiples aspectos, desde la recopilación inicial hasta el almacenamiento, procesamiento y posible eliminación de los datos. Cada decisión tomada en este proceso puede tener consecuencias de largo alcance para los individuos cuyos datos están siendo manejados.

La responsabilidad ética que acompaña a este poder de decisión es fundamental. El responsable debe considerar constantemente las implicaciones morales de sus acciones con respecto a los datos de salud. Esto incluye respetar la autonomía de los pacientes, mantener la confidencialidad, y asegurar que el uso de los datos siempre sea en beneficio del paciente o para fines de investigación legítimos que hayan sido adecuadamente autorizados. El manejo ético de los datos también implica ser transparente sobre cómo se utilizan y protegen los datos, permitiendo a los individuos tomar decisiones informadas sobre su información personal.

También se toma en cuenta que el responsable determina cómo se obtienen, almacenan y suprimen los datos personales, es decir, que esto abarca todo el ciclo de vida de la información, desde su recopilación hasta su eliminación. En cada una de estas etapas, el responsable debe implementar medidas de seguridad actualizadas. Esto incluye no solo soluciones tecnológicas, sino también políticas y procedimientos claros, capacitación regular del personal, y una cultura organizacional que priorice la

protección de datos. Además, es fundamental realizar evaluaciones de riesgo periódicas y auditorías de seguridad para identificar y abordar posibles vulnerabilidades en el manejo de los datos sensibles de salud.

El Encargado

Para un mayor entendimiento de lo que es el encargado Cano (2015) lo define como:

> la persona física o moral, ajena a la organización del responsable del tratamiento, que trata los datos personales a nombre y por cuenta del responsable. A diferencia de este último, el encargado no decide qué hacer y cómo usar los datos personales, sino que los emplea siguiendo las instrucciones del responsable. (pág. 71)

Un punto fundamental es que el encargado actúa a nombre y por cuenta del responsable. Esto significa que, aunque el encargado tiene acceso y maneja los datos personales, no lo hace para sus propios fines, sino en representación del responsable. Esta relación debe estar claramente definida y documentada, generalmente a través de un contrato de tratamiento de datos que especifique los términos exactos de la relación y las obligaciones del encargado.

Cano enfatiza que el encargado no decide qué hacer y cómo usar los datos personales. Esta es quizás la distinción más crítica entre el responsable y el encargado. El encargado no tiene autonomía en cuanto al propósito o los medios del tratamiento de datos. Su rol se limita a seguir las instrucciones específicas del responsable. Esto tiene implicaciones significativas en términos de responsabilidad legal y ética, ya que el responsable mantiene el control último sobre el uso de los datos.

Es importante notar que, aunque el encargado no toma decisiones sobre el uso de los datos, sí tiene responsabilidades significativas en cuanto a su protección. Debe implementar medidas de seguridad adecuadas, mantener la confidencialidad de la información, y asegurar que su personal cumpla con las mismas obligaciones. Además, el encargado tiene el deber de informar al responsable sobre cualquier brecha de seguridad o incidente que pueda afectar los datos de salud.

Destinatario

Según Angarita (2019) "los destinatarios constituyen un grupo diferente a los responsables y encargados del tratamiento, en la medida en que reciben los datos como resultado de una transmisión o transferencia, para efectos del cumplimiento de

funciones legales o contractuales específicas”. Es fundamental destacar que Angarita establece una clara distinción entre los destinatarios y los roles ya conocidos de responsables y encargados del tratamiento. Esta diferenciación es crucial para entender la complejidad del flujo de datos personales en el mundo actual.

Mientras que los responsables y encargados tienen roles bien definidos en la recolección, procesamiento y gestión de los datos, los destinatarios representan un tercer grupo con características y responsabilidades únicas. Esta categorización ayuda a mapear de manera más precisa cómo se mueven los datos personales entre diferentes entidades y con qué propósito, lo cual es esencial para garantizar una protección integral de la privacidad.

Otro punto clave es es que los destinatarios "reciben los datos como resultado de una transmisión o transferencia". Este punto subraya que los destinatarios no son parte del proceso inicial de recolección o tratamiento de datos, sino que entran en escena en una etapa posterior. Angarita (2019) denomina que “la transferencia implica un movimiento deliberado y controlado de información desde el responsable o encargado hacia el destinatario”. Este proceso debe estar sujeto a rigurosos controles y salvaguardas para asegurar que los datos personales mantengan su integridad y confidencialidad durante el tránsito. Además, la mención explícita de estos términos sugiere que puede haber diferentes modalidades de compartir datos, cada una con sus propias implicaciones legales y de seguridad. Por ejemplo, una transmisión podría referirse a un movimiento de datos dentro de la misma jurisdicción, mientras que una transferencia podría implicar el cruce de fronteras nacionales, lo cual conlleva consideraciones adicionales en términos de normativas internacionales de protección de datos.

Autoridad de Protección de Datos Personales

Según Remolina (2019)Las APD (Autoridades de Protección de Datos Personales) son:

> autoridades públicas independientes que supervisan, mediante los poderes de investigación y correctivos, la aplicación de la legislación sobre protección de datos. Estas ofrecen asesoramiento experto en cuestiones relacionadas con la protección de datos y tramitan reclamaciones presentadas por la violación del Reglamento general de protección de datos y las legislaciones nacionales pertinentes. (pág. 75)

La Autoridad de Protección de Datos Personales desempeña un papel fundamental en la salvaguardia de los derechos y libertades de los ciudadanos en relación con el tratamiento de sus datos personales. Esta entidad, establecida por ley, actúa como un organismo independiente encargado de supervisar y garantizar el cumplimiento de las normativas vigentes en materia de protección de datos. Una de sus principales funciones es investigar posibles infracciones o violaciones a la legislación de protección de datos personales. Para ello, cuenta con poderes de investigación que le permiten acceder a información, realizar inspecciones y solicitar explicaciones a las entidades responsables del tratamiento de datos. Además, tiene facultades correctivas para imponer sanciones y medidas coercitivas en caso de incumplimiento.

Delegado de protección de datos personales

El delegado de protección según González (2020) es:

> La persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos. (pág. 33)

Ciertamente, el Delegado de Protección de Datos juega un papel crucial en el ámbito de la salud para salvaguardar los derechos y la privacidad de los pacientes y usuarios del sistema de salud, ya que es responsable de velar por el cumplimiento estricto de las leyes y regulaciones de protección de datos en el sector de la salud. Esto implica mantenerse actualizado sobre las normativas vigentes, tanto a nivel nacional como internacional, y asegurarse de que la entidad de salud las cumpla en todas sus operaciones y procesos que involucren el tratamiento de datos personales de pacientes.

Además, desempeña un papel fundamental en la asesoría y capacitación del personal de la entidad de salud. Esto incluye brindar orientación y formación continua sobre las mejores prácticas de protección de datos, las medidas de seguridad necesarias y los procedimientos adecuados para el manejo de información sensible de pacientes. Al sensibilizar y capacitar al personal, se fomenta una cultura de privacidad y se reduce el riesgo de violaciones de datos.

Asimismo, actúa como enlace entre la entidad de salud y la autoridad reguladora de protección de datos. Coopera estrechamente con esta autoridad, respondiendo a

consultas, proporcionando información y gestionando las solicitudes relacionadas con el tratamiento de datos personales de pacientes. Esta colaboración estrecha garantiza una mayor transparencia y rendición de cuentas en el manejo de la información sensible.

Conforme a ello, el Delegado de Protección de Datos en el ámbito de la salud es un guardián clave de los derechos y la privacidad de los pacientes. Su función es fundamental para garantizar el cumplimiento normativo, promover una cultura de privacidad, supervisar las prácticas de tratamiento de datos, capacitar al personal y actuar como enlace con las autoridades reguladoras. Su labor contribuye a fortalecer la confianza de los pacientes en el sistema de salud y a proteger su información sensible de posibles amenazas o violaciones.

Bases legales

Según Villafranca (2018) “Las bases legales no son más que se leyes que sustentan de forma legal el desarrollo del proyecto” explica que las bases legales “son leyes, reglamentos y normas necesarias en algunas investigaciones cuyo tema así lo amerite”.

Por consiguiente, En Ecuador, la protección de datos de salud está respaldada por diversas leyes y regulaciones. Algunas de las principales fuentes legales que pueden fundamentar este análisis incluyen:

La protección de datos personales en la Constitución de la República del Ecuador 2008

El numeral 19 del artículo 66 de la Constitución de la República contempla el reconocimiento de esta categoría de protección en la cual se establece que:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Este derecho fundamental reconoce la facultad de toda persona para acceder y decidir sobre sus datos e información de carácter personal, así como la protección de los mismos. Así mismo, las personas tienen el poder de decisión sobre qué datos suyos pueden ser recolectados y qué uso se les puede dar. También El Estado debe

establecer un sistema jurídico e institucional que garantice la protección efectiva de los datos personales frente a su uso indebido, interferencias arbitrarias o ilegales.

Objeto y Finalidad de la Ley Orgánica de Protección de Datos Personales del Ecuador

El artículo 1 de la presente Ley Orgánica de Protección de Datos Personales (2021) establece el objeto y finalidad, en la cual se establece lo siguiente:

> El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

La Ley Orgánica de Protección de Datos Personales del Ecuador representa un hito significativo en la evolución del marco jurídico del país en materia de privacidad y seguridad de la información. El artículo 1 de esta ley establece de manera clara y concisa su objeto y finalidad, sentando las bases para una protección integral de los datos personales de los ciudadanos ecuatorianos.

En primer lugar, la ley se enfoca en garantizar el ejercicio del derecho a la protección de datos personales. Este enfoque refleja un reconocimiento fundamental de que la protección de datos no es simplemente una cuestión de seguridad técnica, sino un derecho inherente de los individuos, al elevar la protección de datos al nivel de un derecho, la ley subraya la importancia crítica de la privacidad en la era digital. Un aspecto crucial de este derecho, como lo menciona la ley, es el acceso y decisión sobre información y datos de carácter personal. Esto implica que los individuos no solo tienen derecho a que sus datos estén protegidos, sino también a tener control sobre ellos. Este principio de autodeterminación informativa empodera a los ciudadanos, otorgándoles un papel activo en la gestión de su información personal.

La ley va más allá de simplemente declarar estos derechos, al establecer que su finalidad incluye regular, prever y desarrollar principios, derechos, obligaciones y mecanismos de tutela. Esta aproximación holística es fundamental para crear un ecosistema completo de protección de datos. Los principios proporcionan una base ética y conceptual, los derechos otorgan poder a los individuos, las obligaciones aseguran que las entidades que manejan datos actúen responsablemente, y los mecanismos de tutela garantizan que existan vías de recurso en caso de violaciones.

Al abordar tanto los aspectos preventivos como los reactivos de la protección de datos, la ley crea un marco robusto y equilibrado. La prevención se logra a través de la regulación y el establecimiento de principios y obligaciones, mientras que la reacción se maneja mediante los mecanismos de tutela. También es importante destacar que esta ley reconoce implícitamente la naturaleza dinámica de los desafíos relacionados con la protección de datos. Al establecer un marco general en lugar de prescripciones específicas, la ley permite cierta flexibilidad en su aplicación, lo que es crucial en un campo que evoluciona rápidamente debido a los avances tecnológicos.

En este sentido el artículo 1 de la Ley Orgánica de Protección de Datos Personales del Ecuador establece una base sólida para la protección integral de los datos personales en el país. Al combinar la garantía de derechos fundamentales con mecanismos prácticos de implementación y tutela, la ley busca crear un entorno en el que la privacidad y la seguridad de los datos personales sean una prioridad. Este enfoque no solo protege a los individuos, sino que también establece un estándar claro para las organizaciones que manejan datos personales, promoviendo así una cultura de respeto por la privacidad en toda la sociedad ecuatoriana.

Ámbito de aplicación material de la Ley Orgánica de Protección de Datos Personales del Ecuador

El art.2 de la presente Ley Orgánica de Protección de Datos Personales (2021) determina lo siguiente respecto al ámbito de aplicación material:

> La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a: a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas; b) personas fallecidas; c) datos anonimizados, en tanto no sea posible identificar a su titular; d) actividades periodísticas y otros contenidos editoriales; e) datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento; f) datos que identifican o hacen identificable a personas jurídicas de infracciones penales.

El artículo 2 de esta ley define claramente tanto su alcance como sus limitaciones, proporcionando un marco legal integral para la protección de datos personales en el país.

En primer lugar, la ley se aplica al tratamiento de datos personales en cualquier tipo de soporte, ya sean automatizados o no. Esta disposición es crucial en un mundo donde los datos se almacenan y procesan de múltiples formas, desde bases de datos digitales hasta archivos físicos. Al no limitar su alcance a un formato específico, la ley

garantiza una protección amplia y adaptable a las diversas formas de tratamiento de datos existentes y futuras.

Además, la ley extiende su aplicación a toda modalidad de uso posterior de los datos personales. Esta cláusula es particularmente importante en el contexto actual, donde los datos recopilados para un propósito pueden ser reutilizados o reprocesados para otros fines. Al cubrir estos usos posteriores, la ley busca proteger a los individuos contra el uso no autorizado o inesperado de sus datos personales. Sin embargo, la ley también establece excepciones claras a su aplicación, reconociendo que existen situaciones donde una regulación estricta de datos personales podría ser impráctica o innecesaria. La exclusión de datos utilizados en actividades familiares o domésticas reconoce la importancia de la privacidad en el ámbito personal y evita una sobrerregulación de las interacciones cotidianas.

La no aplicación de la ley a personas fallecidas plantea cuestiones interesantes sobre la naturaleza temporal de la protección de datos personales. Esta exclusión sugiere que el derecho a la protección de datos se considera primordialmente un derecho personal que no se extiende más allá de la vida del individuo. La excepción para datos anonimizados es crucial en la era digital. Al permitir el uso de datos que no pueden identificar a individuos específicos, la ley busca un equilibrio entre la protección de la privacidad y la facilitación de investigaciones y análisis que pueden beneficiar a la sociedad en su conjunto.

Así mismo, la exclusión de actividades periodísticas y contenidos editoriales refleja un reconocimiento de la importancia de la libertad de prensa y expresión. Esta excepción busca evitar que la ley de protección de datos se convierta en un obstáculo para el periodismo y la difusión de información de interés público. Por lo que, las excepciones relacionadas con la prevención, investigación y enjuiciamiento de infracciones penales, así como los datos que identifican a personas jurídicas en este contexto, reconocen la necesidad de equilibrar la protección de datos personales con los intereses de seguridad pública y justicia.

Ámbito de aplicación territorial de la Ley Orgánica de Protección de Datos Personales del Ecuador

El art. 3 de la Ley Orgánica de Protección de Datos Personales (2021) establece lo siguiente respecto al ámbito de aplicación territorial en el cual determina que:

> Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando: 1. El tratamiento de datos personales se realice en cualquier parte del territorio nacional; 2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional; 3. Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador; 4. Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional.

La ley reconoce la primacía de los instrumentos internacionales ratificados por Ecuador en materia de protección de datos. Esta disposición demuestra el compromiso del país con los estándares internacionales y asegura que la ley nacional esté en armonía con las obligaciones internacionales del Ecuador. La aplicación de la ley a todo tratamiento de datos personales realizado en cualquier parte del territorio nacional establece una jurisdicción clara dentro de las fronteras del país. Esto asegura que cualquier entidad, sea nacional o extranjera, que procese datos en Ecuador esté sujeta a las regulaciones ecuatorianas, proporcionando una protección uniforme en todo el territorio nacional.

También el aspecto más innovador de la ley es su aplicación extraterritorial. Al cubrir el tratamiento de datos de residentes ecuatorianos por parte de entidades no establecidas en Ecuador, la ley busca proteger a sus ciudadanos en el contexto global de Internet, donde los datos a menudo son procesados por empresas multinacionales fuera del país de origen del titular de los datos. Así mismo, la inclusión de responsables o encargados no domiciliados en Ecuador dentro del ámbito de la ley es particularmente significativa. Esta disposición refleja la realidad de un mundo interconectado donde los datos fluyen a través de las fronteras nacionales, y busca asegurar que las entidades extranjeras que manejan datos de ecuatorianos cumplan con los estándares de protección establecidos por Ecuador. Conforme a ello, el ámbito de aplicación territorial establece un marco legal ambicioso y de amplio alcance. Al abarcar tanto el procesamiento de datos dentro del país como el manejo de datos de ecuatorianos por entidades extranjeras, la ley busca proporcionar una protección integral en un mundo donde los datos personales fluyen constantemente a través de las fronteras nacionales.

El tratamiento de los datos relativos a la salud en la Ley Orgánica de Protección de Datos Personales 2021

El art. 31 de la Ley Orgánica de Protección de Datos Personales (2021) determina que: “Todo tratamiento de datos relativos a la salud deberá cumplir con los siguientes parámetros mínimos y aquellos que determine la Autoridad de Protección de Datos Personales en la normativa emitida para el efecto”.

Este artículo establece una regulación específica para el tratamiento de los datos relativos a la salud, reconociendo su naturaleza sensible y la necesidad de brindarles una protección reforzada. Al determinar que "todo tratamiento de datos relativos a la salud deberá cumplir con los siguientes parámetros mínimos", la ley está sentando las bases para garantizar el respeto a los derechos fundamentales de los titulares de estos datos y evitar su uso indebido. Además, otorga a la Autoridad de Protección de Datos Personales la facultad de emitir normativa complementaria para establecer parámetros adicionales en el tratamiento de datos de salud. Esto brinda un marco legal flexible que permite adaptar y actualizar los requisitos y garantías en función de los avances tecnológicos, las mejores prácticas internacionales y las necesidades específicas del país.

Objeto del Reglamento General de la Ley Orgánica de Protección de Datos Personales del Ecuador

El art. 1 del presente Reglamento General de la Ley Orgánica de Protección de Datos Personales del Ecuador (2023) establece lo siguiente: “Objeto: El presente Reglamento General tiene por objeto desarrollar la normativa para la aplicación de la Ley Orgánica de Protección de Datos Personales y la protección de los derechos y libertades fundamentales de los titulares de datos personales”.

El reglamento se presenta como un instrumento de desarrollo normativo. Esto significa que su función principal es elaborar y especificar los preceptos generales establecidos en la Ley Orgánica. Esta labor de desarrollo es esencial, ya que transforma los principios y disposiciones amplias de la ley en normas concretas y aplicables, facilitando su interpretación y cumplimiento por parte de todos los actores involucrados. El énfasis en la aplicación de la Ley Orgánica subraya el carácter práctico del reglamento. No se trata simplemente de un documento teórico, sino de

una herramienta diseñada para guiar la implementación real y efectiva de la ley en diversos contextos y situaciones. Este enfoque práctico es crucial para asegurar que la protección de datos personales no quede en meras declaraciones, sino que se traduzca en acciones y medidas concretas.

Además, el reglamento pone un énfasis especial en “la protección de los derechos y libertades fundamentales de los titulares de datos personales". Esta frase es de suma importancia, ya que sitúa al individuo y sus derechos en el centro de la normativa. Reconoce que la protección de datos personales no es un fin en sí mismo, sino un medio para salvaguardar derechos y libertades más amplios, como la privacidad, la dignidad y la autonomía personal. Es así que el artículo 1 del Reglamento General establece un marco sólido y orientado a la acción para la protección de datos personales en Ecuador. Al enfocarse en el desarrollo normativo, la aplicación práctica y la protección de derechos fundamentales, el reglamento se posiciona como un instrumento vital para traducir los principios de la Ley Orgánica en realidades concretas. Este enfoque integral y centrado en el individuo refleja un compromiso serio con la protección de la privacidad y los derechos digitales en la era de la información.

Ámbito de aplicación del Reglamento General de la Ley Orgánica de Protección de Datos Personales del Ecuador

El art. 2 del Reglamento General de la Ley Orgánica de Protección de Datos Personales del Ecuador (2023) determina lo siguiente respecto al ámbito de aplicación:

> Este Reglamento se aplica a todas las personas naturales y jurídicas, nacionales y extranjeras, del sector público y privado, que realicen tratamiento de datos personales, en el contexto de que sus actividades como responsable o encargado de tratamiento de datos personales, tenga lugar en el territorio ecuatoriano o no; también se aplica al tratamiento de datos personales por parte de personas naturales y jurídicas, que actúen como responsables y encargados del tratamiento de datos personales de titulares no residentes en Ecuador, cuando sus actividades de tratamiento sean realizadas en territorio nacional; aplicará para los responsables y encargados del tratamiento de datos personales no establecidos en territorio ecuatoriano a quienes les resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público. Estos deberán designar a un apoderado especial de acuerdo con el artículo 3 de este Reglamento.

El reglamento extiende su aplicación a todas las personas naturales y jurídicas, tanto nacionales como extranjeras, y del sector público como privado. Esto refleja el reconocimiento de que el tratamiento de datos personales es una actividad que trasciende fronteras y sectores. Al no hacer distinción entre entidades nacionales y

extranjeras, el reglamento busca crear un campo de juego nivelado y asegurar que todos los actores que manejan datos de ecuatorianos estén sujetos a las mismas reglas y estándares. Un aspecto relevante del ámbito de aplicación es su alcance extraterritorial. El reglamento se aplica incluso cuando las actividades de tratamiento de datos no tienen lugar en territorio ecuatoriano. Esta disposición es particularmente importante de los servicios digitales globales, donde los datos a menudo se procesan en servidores ubicados en diferentes países. Al extender su jurisdicción más allá de las fronteras nacionales, Ecuador busca proteger los datos de sus ciudadanos dondequiera que estos sean procesados.

Además, el reglamento aborda específicamente el tratamiento de datos de titulares no residentes en Ecuador por parte de entidades que operan en territorio nacional. Esta disposición refleja el papel de Ecuador como un posible centro de procesamiento de datos para la región, y busca asegurar que los estándares de protección de datos se apliquen de manera uniforme, independientemente de la residencia del titular de los datos. Otro aspecto innovador del reglamento es su aplicación a entidades no establecidas en Ecuador, pero que están sujetas a la legislación ecuatoriana en virtud de contratos o regulaciones internacionales. Este amplio ámbito de aplicación plantea desafíos significativos en términos de implementación y cumplimiento, especialmente cuando se trata de entidades extranjeras o actividades que ocurren fuera del territorio nacional. Sin embargo, también demuestra un compromiso firme con la protección integral de los datos personales en un contexto globalizado.

CAPÍTULO III

MÉTODOLOGÍA DE LA INVESTIGACIÓN

La metodología de la investigación según Arias (2012) “incluye el tipo o tipos de investigación, las técnicas y los instrumentos que serán utilizados para llevar a cabo la indagación. Es el “cómo” se realizará el estudio para responder al problema planteado”. Esta descripción detallada de la metodología es fundamental para asegurar la rigurosidad y sistematicidad del proceso de investigación, permitiendo replicar o verificar los resultados obtenidos. La metodología de investigación, permitirá seleccionar los tipos de investigación, técnicas e instrumentos más adecuados para analizar exhaustivamente el marco jurídico ecuatoriano en materia de tratamiento de datos de salud y responder de manera sólida al problema planteado.

Naturaleza de la Investigación:

Tomando en consideración en el presente trabajo, se aborda un paradigma jurídico dogmático, según Núñez (2014) lo define como:

> La actividad realizada por los estudiosos del derecho que tiene como objetivo establecer la calificación deóntica que, en un determinado sistema jurídico, se atribuye a tipos de acciones (casos genéricos) –pero en algunas ocasiones también a conductas concretas (casos individuales)– y al que el sistema jurídico de referencia no reconoce algún valor en ningún procedimiento jurídico. Es decir, la actividad –pero también su método y resultado– que pretende precisar la consecuencia jurídica que un ordenamiento jurídico vigente asocia a un determinado tipo de comportamiento. (pág. 3)

La dogmática jurídica, como actividad de los estudiosos del derecho, permitirá analizar y determinar la calificación deóntica, obligatoriedad, prohibición o permisión que el ordenamiento jurídico ecuatoriano establece sobre el tratamiento de los datos de salud en la Ley Orgánica de Protección de Datos Personales. A través del análisis dogmático de las normas legales ecuatorianas aplicables, se precisará las consecuencias jurídicas que el marco legal vigente asocia a las diferentes conductas o relacionadas con el tratamiento de los datos de salud. Esto implica analizar de manera sistemática la legislación ecuatoriana relevante, normas sobre historias clínicas, regulaciones del sector salud, para identificar cómo califican y regulan el tratamiento de esta información sensible.

Con base a lo anterior el presente trabajo tiene un paradigma interpretativo, para Ricoy (2006) el paradigma interpretativo:

> busca profundizar en la investigación, planteando diseños abiertos y emergentes desde la globalidad y contextualización. Las técnicas de recogida de datos más usuales son la observación participativa, historias de vida, entrevistas, los diarios, cuadernos de campo, los perfiles, el estudio de caso, etc. (pág. 17)

Dicho paradigma interpretativo permitirá analizar el marco jurídico ecuatoriano sobre el tratamiento de datos de salud en su contexto social, cultural e histórico específico. También analizar cómo las leyes y regulaciones se han desarrollado y cómo son interpretadas y aplicadas en la realidad por los diferentes actores involucrados, pacientes, profesionales de la salud, instituciones. También la selección de casos específicos en centros de salud y realizar un análisis detallado de cómo se implementa el tratamiento de datos de salud en esos contextos particulares, explorando las interpretaciones, desafíos y prácticas reales.

El presente trabajo tiene un enfoque cualitativo, para lo cual Aranzamendi (2008) dice que esta investigación:

> está orientada principalmente hacia la descripción y la comprensión de una situación o fenómeno (caso del Derecho) a diferencia de la cuantitativa que se centra en la cuantificación, predicción y control (…) el conocimiento se construye, no se descubre. Con regularidad se tiende a observar, a describir e interpretar lo que se encuentra en los datos (documentales o no), y solo tiene sentido para esa situación o contexto determinado. (pág. 148)

De este modo, a través del enfoque cualitativo se describe con profundidad cómo se aplica e interpreta el marco jurídico ecuatoriano en relación al tratamiento de datos de salud en la práctica real. A su vez, se construye un conocimiento a partir de la, análisis de documentos legales, y otras fuentes de datos, interpretando cómo se manifiesta este marco jurídico en contextos específicos, para el tratamiento de los datos de salud.

El diseño de investigación que se utiliza se adapta y alinea con la naturaleza, estructura y propósitos específicos de este estudio en particular, es el hermenéutico. Es por ello que Quintana (2019) define a la hermenéutica de la siguiente manera:

> La hermenéutica es un paradigma que se aplica a todas aquellas investigaciones que están centradas en la interpretación de texto ello implica que el investigador debe realizar un proceso dialéctico a los efectos de analizar todas las partes del documento estudiado para de esta forma poder comprenderlo y efectuar un análisis y vincularlo al tema que está investigando. (pág. 163)

A través de este diseño se va a interpretar de manera profunda la normativa legal, la doctrina jurídica y los casos prácticos relacionados con el tema. En primer lugar, se

realizará una lectura minuciosa y detallada de los textos legales, las teorías y los precedentes judiciales relevantes, con el objetivo de captar su complejidad y desentrañar los múltiples significados implícitos. Aplicando el proceso dialéctico propio de la hermenéutica, se analizarán todas las partes y elementos que conforman el marco jurídico ecuatoriano en torno al tratamiento de datos de salud, considerando cómo se vinculan e interrelacionan entre sí dentro de un todo coherente. Esta interpretación rigurosa y contextualizada permitirá explicar a fondo las diversas aristas del tema, apreciando sus matices y posibles contradicciones.

Unidad de Análisis

Con respecto a la unidad de análisis en investigación, Hurtado (2010) afirma que: “Una unidad de análisis es una cadena textual que se distingue del resto del documento por abordar un tema específico”. En otros casos, se fundamenta únicamente en criterios espaciales y sintácticos. La unidad de análisis principal serán los textos legales, doctrinarios, relacionados con el tratamiento de datos de salud según el marco normativo ecuatoriano. Mediante una lectura minuciosa y un examen dialéctico, se analizarán detalladamente las secciones y componentes de las leyes, reglamentos, tratados y otros instrumentos jurídicos vinculados al tema.

Consecuentemente se seleccionaron los siguientes documentos:

- Constitución de la República del Ecuador (2008)
- Ley Orgánica de Protección de Datos Personales (2021)
- Reglamento de la Ley Orgánica de Protección de Datos Personales (2023)
- Libros y artículos

Técnica de recolección de información

La técnica de recolección de información dentro de la investigación según Hernández Fernández, y Baptista (2018) significa: a) elegir uno o más métodos o herramientas, adaptarlos o crearlos según el enfoque del estudio y el planteamiento del problema; b) usar las herramientas seleccionadas, y c) organizar los datos obtenidos para un análisis adecuado”. Para llevar a cabo un análisis efectivo, se puede emplear esta técnica para reunir la documentación necesaria para la investigación.

De igual manera, en lo que respecta a la técnica de recolección de información se selecciona la revisión documental, Hurtado (2010) indica que: “La revisión documental implica localizar, reunir, seleccionar, revisar, analizar, extraer y registrar información de documentos.” La técnica de revisión de documentos puede servir para varios propósitos.

Se muestra que en esta investigación la norma será una base crucial para sustentar el análisis y para identificar los aspectos importantes del objeto de estudio del presente trabajo de titulación, debido a que se examina de manera exhaustiva todas aquellas normativas, textos obtenidos. Para dar cumplimiento a lo expuesto se utiliza el siguiente instrumento, la ficha de registro para la sistematización de la información.

Ficha de registro

Documento	Análisis

Técnica de análisis de datos

Para entender lo que es la técnica de análisis de datos Arias (2012) manifiesta que: “se describen las distintas operaciones a las que serán sometidos los datos que se obtengan: clasificación, registro, tabulación y codificación si fuere el caso”

La técnica de análisis de datos involucra una serie de pasos y procedimientos que permiten organizar, estructurar y preparar los datos para su posterior análisis e interpretación, de manera que se pueda extraer información valiosa y conclusiones relevantes para el presente trabajo. Para resolver el problema de investigación propuesto, es necesario examinar detenidamente todos los datos relevantes y organizar de manera adecuada la documentación que se requiera.

Un aspecto fundamental de este capítulo es examinar a profundidad los temas centrales de la investigación del caso de estudio, conjuntamente con los artículos, la doctrina, que sean pertinentes. uno de los temas centrales a analizar es el tratamiento

de los datos de salud y cómo este se rige según la legislación ecuatoriana vigente. Para abordar este tema de manera exhaustiva, será necesario examinar detenidamente los artículos, la doctrina relacionados con la protección de datos personales, particularmente en el ámbito de la salud.

Una forma efectiva de organizar y presentar esta información podría ser mediante la elaboración de tablas, donde se recopilen y clasifiquen los diferentes aspectos legales y normativos que regulan el tratamiento de los datos de salud en Ecuador. Estas tablas podrían incluir, por ejemplo, los artículos específicos de la Ley Orgánica de Protección de Datos Personales, los fundamentos de la Constitución ecuatoriana, la normativa del Ministerio de Salud Pública, entre otros sustentos legales relevantes.

De esta manera, al tener toda la información organizada y sistematizada en tablas, facilitará el análisis exhaustivo de cada uno de los aspectos legales involucrados, permitiéndote realizar un examen riguroso y fundamentado del marco jurídico que rige el tratamiento de los datos de salud en Ecuador.

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

En el presente capítulo, resulta fundamental realizar un exhaustivo análisis documental de diversas fuentes de información, tales como la doctrina jurídica, relevante y la legislación vigente, todas ellas relacionadas con el tratamiento de los datos de salud en el contexto del marco legal ecuatoriano.

Políticas Internas para el tratamiento de datos de salud aplicadas en los centros de salud del Ecuador

La protección de datos personales ha dejado de ser un concepto teórico y se ha convertido en una obligación legal. Por lo tanto, todas las entidades relacionadas con el sector de la salud, incluyendo consultorios médicos, hospitales, clínicas y otras instituciones pertenecientes al sistema nacional de salud, implementan normativas internas claras que demuestren su cumplimiento estricto de las regulaciones vigentes en materia de protección de datos personales. Las Políticas internas para el tratamiento de datos de salud emanadas por el Ministerio de Salud Pública constituyen el marco normativo interno que rige la forma en que la organización recopila, utiliza, almacena, transfiere y elimina los datos personales, garantizando el respeto a los derechos de los titulares de los datos y cumpliendo con los requisitos impuestos por las leyes y reglamentos aplicables en materia de privacidad y protección de datos.

De este modo, Angarita (2019) señala que:

> "las políticas internas suelen incluir aspectos como la definición de roles y responsabilidades, los procedimientos para la obtención del consentimiento, los controles de acceso y medidas de seguridad, la gestión de incidentes de seguridad, los plazos de conservación de datos, los mecanismos para atender los derechos de los titulares, y la realización de evaluaciones de impacto en la protección de datos, entre otros elementos".

Es importante resaltar que, si bien esta política garantiza el acceso público a la información recolectada por el Ministerio de Salud Pública, también establece medidas de seguridad y privacidad para proteger los datos personales sensibles de los ciudadanos, como información médica, historiales clínicos. En este sentido, la política contempla procedimientos para el manejo, almacenamiento y difusión de datos personales sensibles

El Ministerio de Salud Pública protege la seguridad de los datos personales conforme a los principios de seguridad de la información (confidencialidad, integridad y disponibilidad) y al cumplimiento del Esquema Gubernamental de Seguridad de la Información (EGSI). Este marco normativo y técnico establece directrices para el sector público en materia de tratamiento de datos, abarcando diversos aspectos críticos de políticas internas de la seguridad informática. Estas medidas, diseñadas para adaptarse a las necesidades particulares del sector de la salud, se detallan a continuación:

El Equipamiento de Seguridad Perimétrica

Para Hubbard (2022) la seguridad perimetral informática "es el conjunto de mecanismos y sistemas relativos al control del acceso no autorizado". Es decir que dicho sistema trata de proteger los datos que sean accesibles por medio de la red y que existe la posibilidad de que sean modificados, robados o mal usados. En el ámbito sanitario enfrentan dificultades para mantenerse al día con la rápida evolución de las amenazas cibernéticas. Razza (2021) manifiesta que "Los centros de salud luchan por implementar y mantener medidas de protección efectivas debido a restricciones presupuestarias y falta de personal especializado". En este sentido, la falta de recursos financieros adecuados impide que muchas instituciones sanitarias inviertan en tecnologías de seguridad de vanguardia

.

El Equipamiento de Seguridad Perimétrica como política interna para el tratamiento de los datos de salud, es una medida superficial e insuficiente, que ignora la complejidad y diversidad de las amenazas cibernéticas modernas, como es el caso del virus troyano, que para Hubbard (2022) "es una amenaza muy dañina que puede llevar a cabo varias acciones maliciosas en el sistema de la víctima. Suele infiltrarse a través de correos electrónicos, con el objetivo de robar datos confidenciales y compartirlos con los piratas informático". En el contexto del tratamiento de datos de salud, el impacto de un ataque de virus troyano tiene consecuencias catastróficas que, ya que compromete la integridad de los datos de salud, ya que la exposición de historiales médicos, representa una violación grave de la confidencialidad médico-paciente, un principio fundamental en la ética médica.

Por esta razón, si un atacante que logra acceder a una parte del sistema podría potencialmente moverse lateralmente y acceder a bases de datos completas de historiales médicos, comprometiendo la privacidad de múltiples pacientes simultáneamente, sino que también puede exponer información delicada sobre condiciones médicas, tratamientos o diagnósticos que los pacientes preferirían mantener en estricta confidencialidad. También, Angarita (2019) dice que:

> La ausencia de protocolos de respuesta a incidentes bien definidos agrava aún más la situación. Cuando ocurre una brecha de seguridad, la falta de procedimientos claros puede llevar a respuestas caóticas y poco efectivas. Esto puede resultar en un tiempo de exposición prolongado de los datos comprometidos, aumentando la probabilidad de que la información privada de los pacientes sea explotada por actores malintencionados. (pág. 79)

Por lo que, esta visión limitada ignora las amenazas internas, que pueden ser igual de peligrosas que las externas. Sin políticas y controles adecuados para el acceso y manejo de datos por parte del personal interno, existe el riesgo de que empleados malintencionados o descuidados accedan, modifiquen o filtren información confidencial de los pacientes sin ser detectados. En definitiva, esta política inadecuada minimiza la confianza que los pacientes depositan en el sistema de salud. La percepción de que sus datos más íntimos no están adecuadamente protegidos puede llevar a los pacientes a ocultar información importante a sus proveedores de atención médica, comprometiendo potencialmente la calidad de su tratamiento y, por extensión, su salud.

Además, el art. 38 de la Ley Orgánica de Protección de Datos del Ecuador, determina lo siguiente respecto de las medidas de seguridad:

> El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

Se establece un mandato integral para la protección de datos personales, abarcando una amplia gama de riesgos y amenazas. Sin embargo, este enfoque pone de manifiesto las limitaciones de depender exclusivamente del equipamiento de seguridad perimetral como medida de protección. Sin embargo, la seguridad perimetral, resulta insuficiente frente a la complejidad de las amenazas modernas y los requisitos establecidos en el artículo. Este enfoque, aunque importante, no aborda adecuadamente todos los aspectos mencionados en la ley, especialmente en lo que respecta a pérdidas, alteraciones, destrucción o comunicación accidental o ilícita de los datos.

En primer lugar, la seguridad perimetral no puede proteger eficazmente contra amenazas internas o accesos no autorizados que se originan dentro del perímetro establecido. Los incidentes de seguridad causados por empleados descuidados o malintencionados, que ya tienen acceso legítimo a los sistemas, no son mitigados por firewalls o mejor conocido como sistema de seguridad de red de las computadoras, el cual se encarga de prevenir de manera nula la actividad maliciosa para el robo de datos.

En este sentido, mientras que la seguridad perimetral sigue siendo un componente importante de una estrategia de seguridad integral, su ineficacia para abordar completamente los requisitos del artículo 38 LOPDP, subraya la necesidad de un enfoque más amplio y en capas para la protección de datos personales. Las organizaciones deben implementar una combinación de medidas técnicas, organizativas y procedimentales para cumplir verdaderamente con el espíritu y la letra de la ley.

Equipamiento de Seguridad de Red

Para López (2022) el equipamiento de seguridad de la red “es toda aquella actividad, proceso, tecnología o política que busca proteger los recursos digitales de un individuo u organización de amenazas a su confidencialidad y disponibilidad”. En el contexto del tratamiento de datos de salud, esta política interna para el tratamiento de datos de salud también enfrenta vulnerabilidades ante las amenazas cibernéticas. Entre las amenazas más significativas se encuentra el phishing, una técnica de engaño sofisticada que para Hubbard (2022) :

> es un conjunto de técnicas que se basa en el engaño, para ganar la confianza de la persona, haciéndose pasar por una empresa o servicio, es decir que suplanta la identidad, con el propósito de conseguir información personal o hacer el clic en un enlace. (pág. 20)

Los atacantes pueden hacerse pasar por autoridades sanitarias, proveedores de servicios médicos, compañías de seguros o incluso pacientes, para engañar al personal médico y administrativo. El objetivo es obtener acceso a sistemas de información médica, credenciales de acceso o datos sensibles de pacientes. Por ende, el equipamiento de seguridad de red, queda invariablemente un paso atrás de esta técnica utilizada para robar la información. En este sentido, esta política de seguridad es un parche temporal en el sistema vulnerable del tratamiento de los datos de salud, por lo cual contraviene al art. 37 de la normativa vigente que determina lo siguiente:

> El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales

Dentro de este escenario, el responsable del tratamiento de DP debe crear un proceso de verificación, evaluación y revisión constante de la efectividad de las medidas técnicas del equipamiento de seguridad de red. En cuanto a las medidas técnicas, Hubbard (2022) argumenta que “estas se centran principalmente en los computadores y sistemas de red de los centros de salud. Esto incluye la instalación y actualización regular de software antivirus”. Esto se debe a que los datos de salud pueden ser accedidos y procesados desde diversos puntos, y cada uno de estos puntos representa un potencial vector de ataque. Al asegurar que todos los dispositivos cumplan con los estándares de seguridad establecidos, se crea un entorno de tratamiento de datos más uniforme y seguro. La exigencia legal de un proceso continuo y permanente subraya la insuficiencia de esta política de seguridad ya que es vulnerable a la amenaza cibernética denominada phishing, ya que no se ha determinado el número de incidentes detectados y resueltos, ni tampoco el tiempo de respuesta ante amenazas, y el nivel de cumplimiento de esta política.

El equipamiento de seguridad de red, si bien es una política importante para el tratamiento de datos de salud, presenta limitaciones significativas en el contexto actual de ciberseguridad. También se debe considerar que la protección efectiva de los datos de salud requiere un enfoque integral que va más allá de la simple implementación de equipamiento de seguridad de red, ya que se pone en consideración que es sumamente necesario un proceso continuo de verificación, evaluación y valoración, acompañado de una documentación rigurosa, para garantizar la confidencialidad y disponibilidad de los datos de salud.

Canal de Comunicaciones

Para López (2022) un canal de comunicación “es el medio físico a través del cual se lleva a cabo un acto comunicativo, es decir, que sirve para el intercambio de información entre un emisor y uno o varios receptores”. Los canales de comunicación en el ámbito de la salud han evolucionado significativamente, siendo la telemedicina uno de los más prominentes en la actualidad. Esta modalidad de

atención médica utiliza las tecnologías de la información para llevar a cabo servicios de salud como el diagnóstico y tratamiento sin la necesidad de estar en contacto físico entre el personal médico y el paciente. Se debe recalcar que este canal de comunicación, a pesar de que brinde un servicio a través de medios tecnológicos como video llamadas, o plataformas especializadas en atención medicas supuestamente diseñados para proteger la información médica confidencial, en realidad representan un grave riesgo para la privacidad y seguridad de los datos de salud. Baena (2015) afirma que: "la modalidad de telemedicina ignora los peligros inherentes, que a menudo son blanco de ciberataques sofisticados. Dentro de estos ataques se encuentra el malware o secuestro de datos, que para (López, 2022), "es un sistema creado para acceder al sistema de un usuario y bloquear el acceso a su propia información y archivos personales, con el objetivo de exigir el pago de un rescate para liberar la información". El impacto en el tratamiento de los datos de salud va más allá del bloqueo temporal. Existe el riesgo de pérdida permanente de datos si los sistemas de respaldo no están adecuadamente protegidos. Aunque el objetivo principal del atacante sea obtener un rescate, no hay garantía de que los datos no hayan sido copiados o comprometidos durante el ataque.

Esto deja expuesta la información sensible de los pacientes. La limitación del acceso a la información es a menudo ineficaz, ya que los atacantes internos o los errores humanos pueden comprometer fácilmente estos sistemas. Estos ataques no solo ponen en riesgo la confidencialidad de la información médica, sino que también pueden comprometer la integridad de los datos, lo cual podría tener consecuencias graves para el diagnóstico y tratamiento de los pacientes.

Es así que esta política de canales de información, lejos de ser una solución integral para la protección de datos de salud, se ha convertido en un problema respecto de la seguridad médica, exponiendo a millones de pacientes a riesgos de privacidad, seguridad. Los canales de comunicación, al no estar correctamente protegidos, exponen la información médica sensible a partes no autorizadas. Esto incluye diagnósticos, historiales médicos, resultados de pruebas y tratamientos, todos ellos datos que los pacientes esperan que se mantengan en estricta confidencialidad, tal cual lo establece el art. 30 de la Ley Orgánica de Protección de Datos personales, en el que se estipula lo siguiente:

> “Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad, de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas organizativas apropiadas. Esta obligación será complementaria del secreto profesional de conformidad con cada caso”

El deber de confidencialidad impuesto por esta ley se extiende a todos los actores involucrados en el tratamiento de datos personales, desde los responsables y encargados hasta cualquier persona que intervenga en cualquier fase del proceso. Esto crea una red de responsabilidad compartida que busca garantizar la protección integral de la información sensible de los pacientes. La ley no solo exige la confidencialidad, sino que también demanda una seguridad adecuada de los datos personales. Esto implica que las instituciones de salud deben implementar medidas adecuadas para prevenir el tratamiento no autorizado o ilícito de los datos, así como su pérdida, destrucción o daño accidental.

Todas las estaciones de trabajo y computadoras de usuario final deben tener instalado software de protección contra virus

Para López (2022) el programa antivirus es “un sistema de seguridad informática diseñado para proteger a las computadoras de posibles ataques maliciosos”. Si bien los programas antivirus son generalmente considerados como una herramienta esencial para la seguridad informática, en el contexto del tratamiento y protección de datos de salud, su implementación y confianza excesiva en ellos, ya que muchos administradores de sistemas y personal médico creen erróneamente que la mera presencia de un antivirus garantiza la protección total de los datos sensibles de los pacientes.

Como consecuencia de una incorrecta implementación, los ciberdelincuentes están constantemente desarrollando programas maliciosos que evaden la detección de los antivirus tradicionales. Esto significa que los datos de salud están expuestos a riesgos incluso con el antivirus instalado dando como resultado que centros de salud pueden caer en la trampa de pensar que el antivirus es suficiente, ignorando aspectos críticos como la capacitación del personal en seguridad informática.

Esta visión limitada de la ciberseguridad deja numerosos puntos vulnerables sin abordar. López (2022) manifiesta que “El software antivirus también tiene un impacto

negativo en el rendimiento de los sistemas, especialmente en equipos médicos especializados o en computadoras más antiguas.” Esto puede resultar en retrasos en el acceso a información crítica del paciente o incluso en interrupciones del servicio, comprometiendo la calidad de la atención médica y potencialmente poniendo en riesgo la vida de los pacientes. Por lo cual, los virus alteran o corrompen la información sin ser detectados.

Así mismo, la toma de decisiones clínicas basada en datos alterados o incorrectos puede llevar a errores de diagnóstico o tratamiento con graves repercusiones para la salud de los pacientes. En lo que respecta en a términos de privacidad, la ausencia de protección antivirus deja los datos de los pacientes extremadamente vulnerables a accesos no autorizados. Sin esta barrera básica, la información médica confidencial queda expuesta a ser interceptada, copiada o robada por actores malintencionados. Esto puede incluir detalles sensibles como diagnósticos, tratamientos, medicaciones e incluso información personal identificable.

El rol del superintendente de protección de datos personales en el tratamiento de datos de la salud

La autoridad encargada de la protección de datos personales es el Superintendente de Protección de Datos Personales. De acuerdo con Reigada (2021) el Superintendente es la máxima autoridad en materia de protección de datos personales, encargado de velar por el cumplimiento efectivo de la normativa, fiscalizar a los responsables, resolver reclamos, administrar el registro nacional y promover la cultura de protección de datos en la sociedad. La Ley Orgánica de Protección de Datos Personales y el respectivo Reglamento le otorga facultades específicas a esta autoridad para desempeñar sus funciones en esta materia.

La Ley Orgánica de Protección de Datos Personales (2021) y su respectivo Reglamento otorgan facultades específicas a esta autoridad para el desempeño de sus funciones. En particular, el artículo 76 de dicha Ley establece un amplio conjunto de atribuciones y facultades del Superintendente. Si bien este artículo enumera

diversas responsabilidades, es importante destacar las más relevantes para comprender el alcance de su autoridad:

Ejercer la supervisión, control y evaluación de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales

Esta atribución otorga al Superintendente la facultad de vigilar y monitorear las acciones de quienes manejan datos personales. Implica una responsabilidad significativa para asegurar que los procesos de tratamiento de datos se realicen de manera ética y legal. Por lo cual, Zarza (2021) sostiene que "el Superintendente debe establecer mecanismos efectivos de supervisión y evaluación para garantizar el cumplimiento de las normativas de protección de datos". La atribución del Superintendente de ejercer supervisión, control y evaluación sobre el tratamiento de datos personales adquiere una relevancia especial cuando se trata de datos de salud.

En este contexto, el rol del Superintendente es crucial para garantizar el tratamiento de información altamente sensible y personal tal cual lo argumenta Reigada (2021). Por lo cual, en el ámbito de la salud, los datos personales son particularmente delicados y requieren un nivel de protección más elevado dado que el superintendente al tener esta atribución debe asegurar que los responsables y encargados del tratamiento de estos datos implementen medidas de seguridad y cumplan estrictamente con las normativas de protección de datos. Esto implica una vigilancia más estrecha de hospitales, clínicas, laboratorios y otras entidades del sector salud. El superintendente también puede establecer protocolos específicos para la supervisión de datos de salud, que incluyan auditorías más frecuentes, requisitos de seguridad más estrictos y evaluaciones de impacto en la privacidad obligatorias para sistemas que manejan datos médicos.

Además, puede prestar especial atención a la forma en que se obtiene el consentimiento para el tratamiento de estos datos, asegurando que sea explícito e informado. Esta atribución otorgada le permite al superintendente desarrollar en implementar varias técnicas para poder controlar las actividades desarrolladas por el responsable y el encargado del tratamiento de los datos de salud. El Superintendente puede acceder a las nuevas tecnologías en el sector salud, como la telemedicina o las aplicaciones de salud móvil, que presentan nuevos desafíos en términos de

protección de datos, evaluando constantemente cómo estas innovaciones afectan la privacidad de los pacientes y adaptar sus mecanismos de supervisión en consecuencia

Además, debe coordinar sus esfuerzos con entidades como el Ministerio de Salud para asegurar que las regulaciones de protección de datos se alineen con las necesidades específicas del sector sanitario, sin comprometer la calidad de la atención médica.

Ejercer la potestad sancionadora respecto de responsables, delegados, encargados y terceros, conforme a lo establecido en la presente Ley

Razza (2021) sostiene que "es una herramienta crucial para hacer cumplir la normativa y disuadir violaciones." Por lo que a través de esta atribución el Superintendente debe ejercer esta facultad de manera justa y proporcional, estableciendo un sistema claro de sanciones y procedimientos para su aplicación. Es importante reconocer la sensibilidad y el carácter especial de los datos de salud. Estos datos requieren un nivel de protección más elevado debido a su naturaleza íntima y al potencial impacto que su mal uso podría tener en la vida de las personas. La capacidad del Superintendente para sancionar a quienes manejan inadecuadamente estos datos es crucial para garantizar su protección efectiva.

Además, Barahona (2020) sostiene que "el sector de la salud tiene características únicas y complejas en cuanto al manejo de datos". Las sanciones administrativas que el Superintendente puede imponer en casos de violaciones a la protección de datos de salud pueden variar en severidad. Estas podrían incluir desde amonestaciones y multas económicas hasta la suspensión temporal o permanente de actividades relacionadas con el tratamiento de datos. La gradualidad de estas sanciones permite al Superintendente responder de manera proporcional a la gravedad de las infracciones.

La existencia de sanciones significativas puede motivar a los responsables del tratamiento de datos de salud a implementar medidas de seguridad amplias y a adherirse estrictamente a las normativas de protección de datos. Esto puede resultar en una mejora general en las prácticas de manejo de información sanitaria en todo el

sistema de salud. Además, González (2020) dice que “es importante considerar los desafíos que enfrenta el Superintendente en la aplicación de estas sanciones”. Debe equilibrar la necesidad de proteger los datos de los pacientes con la de no obstaculizar indebidamente la prestación de servicios de salud. Además, la determinación de la gravedad de las infracciones y la proporcionalidad de las sanciones requiere un análisis cuidadoso y un profundo conocimiento de la legislación de protección de datos.

Así mismo se considera un aspecto crítico de esta facultad es la necesidad de un debido proceso. El Superintendente debe garantizar que los presuntos infractores tengan la oportunidad de defenderse y presentar evidencias antes de que se impongan sanciones. Esto no solo es un requisito legal, sino que también ayuda a asegurar la justicia y la legitimidad de las decisiones sancionadora

Atender consultas en materia de protección de datos personales

De manera general esta facultad posiciona al Superintendente como un recurso central de conocimiento y orientación en el complejo ámbito de la protección de datos personales. Así mismo, Luño (2020) dice que: “Al atender consultas, el Superintendente puede proporcionar claridad sobre la interpretación y aplicación de la normativa”. De esta manera, ayudando así a prevenir infracciones y promover buenas prácticas en el tratamiento de datos personales.

Esta atribución también refleja un enfoque proactivo en la protección de datos, ya que el superintendente podría guiar a las organizaciones y ciudadanos hacia el cumplimiento, fomentando una cultura de respeto a la privacidad. Sin embargo, esto plantea el desafío de mantenerse actualizado en un campo que evoluciona rápidamente debido a los avances tecnológicos y las cambiantes prácticas de recopilación y uso de datos.

Al acercarnos al ámbito específico de los datos de salud, la importancia de esta atribución se intensifica. Como se ha mencionado anteriormente, los datos de salud son altamente sensibles por lo que el superintendente, al atender consultas en este campo podrían abarcar temas como el manejo adecuado de historias clínicas

electrónicas, los requisitos de consentimiento para el uso de datos en investigación médica, o las medidas de seguridad necesarias para proteger la información genética. El Superintendente debe estar preparado para proporcionar orientación clara y práctica sobre estos temas complejos.

De igual manera , Cano (2015) señala que “se debe considerar las necesidades legítimas de acceso e intercambio de información para una atención médica eficaz y para el avance de la investigación científica”. Esto proporciona una orientación que equilibre estos intereses requiere un profundo conocimiento tanto de la legislación de protección de datos como del funcionamiento del sector sanitario. En sí, la atribución de atender consultas, especialmente en el ámbito de los datos de salud, es una herramienta poderosa para promover el cumplimiento y la comprensión de la normativa de protección de datos. Sin embargo, su efectividad depende de la capacidad del Superintendente para proporcionar orientación clara, equilibrada y actualizada en un campo complejo y en constante evolución.

Ejercer la representación internacional en materia, de protección de datos personales

Esta atribución posiciona al Superintendente como la voz oficial del Ecuador en el escenario internacional en lo que respecta a la protección de datos personales. Esto es crucial en un mundo cada vez más interconectado, donde los flujos de datos traspasan fronteras constantemente. La capacidad de representar al país en foros internacionales permite al Superintendente participar en discusiones globales, compartir perspectivas nacionales y aprender de las mejores prácticas internacionales.

Sin embargo, esta facultad conlleva una gran responsabilidad. Barahona (2020) señala que: “el superintendente debe estar altamente capacitado no solo en la legislación nacional, sino también en las tendencias y normativas internacionales de protección de datos”. Por lo que, debe estar en una actualización constante y un entendimiento profundo de cómo las diferentes jurisdicciones abordan los desafíos de la protección de datos personales.

Además, esta facultad implica colaborar en acuerdos internacionales que afecten la protección de datos de los ciudadanos ecuatorianos. Esto podría incluir acuerdos de

transferencia de datos transfronterizos, estándares de protección de datos en comercio internacional, o colaboración en la lucha contra el cibercrimen. De esta manera la atribución de ejercer la representación internacional en materia de protección de datos personales es una facultad que ofrece grandes oportunidades para posicionar a Ecuador en el escenario global de la protección de datos. Sin embargo, su ejercicio efectivo requiere un alto nivel de experticia, recursos adecuados, y la capacidad de equilibrar los intereses nacionales con la colaboración internacional. El éxito en esta función puede contribuir significativamente a fortalecer la posición de Ecuador en el ámbito de la protección de datos a nivel mundial.

Normativa jurídica de protección de datos personales en Ecuador, España y Argentina

Aspecto	Ecuador	España	Argentina
Base Normativa	Constitución de la República del Ecuador, 2008, art.66, núm.19	Constitución Española, art.18, núm.4	Constitución de la Nación Argentina, art.43.
Ley Principal	Ley Orgánica de Protección de Datos Personales 2021	Ley Orgánica 3/18 de Protección de Datos Personales y Garantía de los Derechos Digitales	Ley 25.326 de Protección de Datos Personales 2000
Autoridad de Control	Superintendente de Protección de Datos Personales	Agencia Española de Protección de Datos	Agencia de Acceso a la Información Pública
Consentimiento	Libre, específico, informado e inequívoco	Libre, específico, informado e inequívoco. Consentimiento explícito para datos sensibles	Libre, expreso e informado
Derechos del titular	Acceso, rectificación, cancelación, oposición, portabilidad, limitación del tratamiento	Acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad, no ser objeto de decisiones individuales.	Acceso, rectificación, actualización, supresión, confidencialidad.

Tabla 1 Cuadro comparativo de la normativa de protección de datos personales

La protección de datos personales ha cobrado gran relevancia en el ámbito jurídico internacional, y los países de habla hispana no son la excepción. En este sentido, Ecuador, España y Argentina han desarrollado marcos normativos específicos para salvaguardar la privacidad y el manejo adecuado de la información personal de sus ciudadanos. Ecuador ha implementado la Ley Orgánica de Protección de Datos Personales en 2021, Mientras que España se rige por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, complementado por la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales. Así mismo, Argentina cuenta con la Ley 25.326 de Protección de Datos Personales, recientemente actualizada para alinearse con estándares internacionales.

Normativa de Ecuador respecto a la protección de datos personales

La Constitución de la República del Ecuador, tras la reforma de 2008, incorporó en su artículo 66, numeral 19, una importante innovación en materia de derechos fundamentales. Este artículo reconoce explícitamente el derecho a la protección de datos personales como un derecho independiente y autónomo. Para Araujo (2021) “este derecho abarca diversos aspectos ya que por un lado, garantiza a los individuos el acceso a su información personal”. Además, les otorga la facultad de tomar decisiones sobre estos datos. Además, establece la obligación de proteger adecuadamente dicha información. La norma constitucional es clara al establecer condiciones para el manejo de datos personales. Específicamente, indica que cualquier actividad relacionada con estos datos, ya sea su recolección, almacenamiento, procesamiento, distribución o difusión, debe cumplir con uno de dos requisitos: contar con la autorización expresa del titular de los datos, o estar amparada por un mandato legal. Esta disposición constitucional representa un avance significativo en el reconocimiento y protección de los derechos digitales en Ecuador, alineándose con tendencias internacionales en la materia.

El 26 de mayo de 2021, Ecuador dio un paso significativo en la protección de datos personales con la publicación de la Ley Orgánica de Protección de Datos Personales en el Registro Oficial Suplemento 459. Esta ley tiene como propósito principal asegurar el ejercicio del derecho fundamental a la protección de datos personales, incluyendo el acceso, la toma de decisiones sobre dicha información y su adecuada

protección. Para lograr este objetivo, la ley establece un marco integral que incluye principios, derechos, obligaciones y mecanismos de tutela. Barahona (2020) sostiene que: “estas disposiciones son de obligatorio cumplimiento tanto para entidades públicas como privadas, lo que garantiza una amplia cobertura en su aplicación”. Un aspecto destacable de esta ley es su alcance territorial porque se extiende más allá de las fronteras ecuatorianas, asegurando la protección de los datos de los ciudadanos ecuatorianos incluso cuando estos son procesados en otros países.

La ley pone un énfasis especial en el consentimiento del titular de los datos. Araujo (2021) dice que: “Este consentimiento debe cumplir con cuatro características fundamentales: ser libre, específico, informado e inequívoco”. Esto empodera a los ciudadanos, otorgándoles la capacidad de decidir sobre el tratamiento de su información personal basándose en un análisis completo de quién, cómo, cuándo y para qué se procesarán sus datos. Además, la normativa establece que todo procesamiento de datos personales debe tener fines legítimos, los cuales están sujetos a revisión por parte de la Autoridad de Protección de Datos Personales. Esta disposición añade una capa adicional de supervisión y control. Dada la importancia central de este concepto en la ley, se hace necesario examinar con detenimiento la definición jurídica que se le atribuye al término dato personal, como:

> aquel dato que identifica o hace identificable a una persona natural, directa o indirectamente”. De manera que, la unidad mínima objeto de tutela puede ser de diverso contenido y naturaleza y, puede estar disponible en cualquier formato; ya que, la condición esencial es que permita identificar a su titular, con o sin la ejecución de procedimientos informáticos Ley Orgánica de Protección de Datos Personales. (2021).

El concepto de dato personal, como objeto de protección legal, abarca una amplia gama de información de diversa índole y naturaleza. Esta información puede existir en cualquier formato, ya sea físico o digital. Lo crucial es que dicha información tenga el potencial de identificar a una persona específica, ya sea de manera directa o mediante la aplicación de procesos informáticos.

De igual manera, la ley reconoce una serie de derechos que deben garantizar la protección de los datos de salud de los pacientes. Entre estos derechos destaca el derecho a la utilidad, para Razza (2021) “permite a los pacientes solicitar que sus datos de salud sean utilizados de manera efectiva y beneficiosa”. Por ejemplo, Por ejemplo, los datos podrían utilizarse para personalizar tratamientos, o contribuir a la

investigación médica, siempre con el consentimiento informado del paciente. Otro derecho que se ha incorporado es el derecho al olvido, de igual manera para Reigada (2021) este derecho " permite a los pacientes solicitar la eliminación de sus datos personales de salud cuando ya no sean necesarios para los fines para los que fueron recogidos, o cuando el paciente retire su consentimiento". Se deben establecer protocolos para la supresión segura de datos cuando se ejerza el derecho al olvido, garantizando que la eliminación sea completa y que no afecte a otros registros o investigaciones en curso.

Además, Razza (2021) sostiene que: "la confidencialidad y la privacidad son cruciales para mantener la confianza entre el paciente y los profesionales de la salud". En este sentido las instituciones sanitarias deben implementar sistemas para garantizar que puedan responder a estas solicitudes de los pacientes en el plazo establecido de 15 días, manteniendo al mismo tiempo la integridad y seguridad de los registros médicos. Es así que la Ley Orgánica de Protección de Datos Personales de Ecuador, publicada en 2021, ha tenido un impacto significativo en el manejo de los datos de salud en el país. Esta normativa considera los datos de salud como información sensible, lo que implica un nivel más alto de protección y cuidado en su tratamiento.

Uno de los cambios más notables ha sido la necesidad de obtener el consentimiento expreso e informado de los pacientes para la recolección y tratamiento de sus datos de salud. Esto ha llevado a que las instituciones de salud, tanto públicas como privadas, deban revisar y actualizar sus procesos de admisión y registro de pacientes para asegurar que se cumpla con este requisito legal. Además, la ley también ha impulsado la implementación de medidas de seguridad en los centros de salud. Esto incluye la adopción de sistemas informáticos para el almacenamiento de historias clínicas electrónicas, así como protocolos más estrictos para el acceso a la información médica de los pacientes. En cuanto a la confidencialidad, la normativa ha reforzado la obligación de mantener el secreto médico. Ahora, no solo los profesionales de la salud están obligados a mantener la confidencialidad, sino también todo el personal administrativo que pueda tener acceso a datos de salud en el desempeño de sus funciones.

La ley promueve transparencia en el manejo de los datos de salud. Las instituciones sanitarias deben informar claramente a los pacientes sobre cómo se utilizarán sus datos, quiénes tendrán acceso a ellos y por cuánto tiempo se conservarán. Esto ha llevado a la creación de políticas de privacidad para los pacientes. En el ámbito de la investigación médica, la normativa ha influido en la forma en que se utilizan los datos de salud. Se han establecido protocolos más rigurosos para la anonimización de datos y se requiere una justificación más exhaustiva para el uso de información personal en estudios científicos. La ley también ha impulsado lo referente a la transferencia internacional de datos de salud. Las instituciones ecuatorianas deben asegurarse de que cualquier transferencia de datos médicos a otros países cumpla con los estándares de protección establecidos en la ley, lo que ha llevado a una revisión de los acuerdos internacionales en materia de salud. Consecuentemente, la normativa ha impulsado la creación de roles específicos en las organizaciones de salud, como la Autoridad de Protección de Datos, encargado de supervisar el cumplimiento de la ley y actuar como punto de contacto para los pacientes y las autoridades en materia de protección de datos personales en el ámbito de la salud.

Normativa de España respecto a la protección de datos personales

En el contexto español, la protección de datos personales se establece como un derecho fundamental, cuyas bases se encuentran en la Constitución Española de 1978. Específicamente, el artículo 18.4 de esta carta magna anticipó los posibles riesgos asociados con el avance de la tecnología informática. Inicialmente, este derecho se conocía bajo el término "habeas data", pero con el tiempo evolucionó hacia una denominación más precisa: el derecho a la protección de datos. Luño (2020) sostiene que “esta previsión constitucional demuestra la temprana conciencia del legislador español sobre la importancia de salvaguardar la información personal en la era digital”. El primer antecedente significativo en la legislación española sobre protección de datos se produjo en 1992. En ese año, se promulgó la Ley Orgánica 5/1992, de 29 de octubre, conocida como LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal). Esta ley pionera materializó el mandato constitucional establecido en el artículo 18.4.

Su objetivo principal, según Luño (2020) “se desprende de su artículo 1, era establecer límites al uso de la informática y otras tecnologías de procesamiento automático de datos personales”. La finalidad última de estas restricciones era salvaguardar el honor, la privacidad personal y familiar de los individuos, así como garantizar el pleno ejercicio de sus derechos fundamentales. La LORTAD de 1992 marcó un punto de inflexión en la protección de datos personales en España, siendo una de las primeras leyes de su tipo en Europa. Esta ley no solo respondió a la necesidad constitucional, sino que también anticipó muchos de los principios que más tarde se convertirían en estándares internacionales en la materia. Además, estableció la Agencia de Protección de Datos como autoridad de control independiente, sentando las bases para una supervisión efectiva. También introdujo conceptos clave como el consentimiento informado y la calidad de los datos, que siguen siendo fundamentales en la legislación actual.

Para Fraguío (2018) “esta ley sirvió como base para el desarrollo posterior de la normativa de protección de datos en España, evolucionando hacia la Ley Orgánica 15/1999 (LOPD)” y, finalmente, adaptándose al Reglamento General de Protección de Datos (RGPD) de la Unión Europea con la actual Ley Orgánica 3/2018. España tuvo que adaptar su legislación nacional. Esto se materializó en la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales. Esta ley no solo adapta la normativa española al RGPD, sino que también introduce nuevos derechos digitales como el derecho al olvido, a la portabilidad de datos, y a la desconexión digital en el ámbito laboral.

Posteriormente, en diciembre de 1999, las Cortes Generales aprobaron la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD). Esta ley, al igual que su predecesora LORTAD, se fundamentaba directamente en el artículo 18.4 de la Constitución Española, hecho que posteriormente fue ratificado por el Tribunal Constitucional en su Sentencia 292/2000. Arenas (2018) afirma que: “La LOPD se centró en dos objetivos principales, establecer una regulación para el tratamiento de datos personales y los ficheros que los contenían”, independientemente del formato en que se procesaran y detallar los derechos de las personas físicas y las obligaciones de quienes creaban ficheros y procesaban datos, ya fueran responsables o encargados del tratamiento.

La Ley Orgánica 15/1999 (LOPD) y su posterior Reglamento de desarrollo (RLOPD) marcaron un antes y un después en la protección de datos personales en España. Estos instrumentos legales introdujeron varios conceptos y prácticas innovadoras que tuvieron un impacto significativo. Esta normativa no solo elevó los estándares de protección de datos en España, sino que también preparó el terreno para la futura adaptación al Reglamento General de Protección de Datos (RGPD) de la Unión Europea, facilitando la transición hacia un marco de protección de datos más robusto y armonizado a nivel europeo. Es por ello que, La Unión Europea, en su empeño por unificar y armonizar la legislación sobre protección de datos en todos sus estados miembros, promulgó el Reglamento General de Protección de Datos (RGPD) en 2016. Este reglamento, oficialmente denominado Reglamento (UE) 2016/679, fue aprobado por el Parlamento Europeo y el Consejo el 27 de abril de 2016. Su objetivo principal es salvaguardar los derechos de las personas físicas en relación con el tratamiento de sus datos personales, al tiempo que facilita la libre circulación de estos datos dentro de la Unión. Esta nueva normativa sustituyó a la anterior Directiva 95/46/CE. Como resultado directo de la implementación del RGPD, España se vio en la necesidad de actualizar su marco legal nacional. Esto llevó a la aprobación de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que entró en vigor el 6 de diciembre de 2018. Esta nueva ley no solo alinea la legislación española con el RGPD, sino que también deroga en gran medida la anterior Ley Orgánica de Protección de Datos (LOPD), adaptando así el marco normativo español a las exigencias europeas en materia de protección de datos.

En este sentido Arenas (2018) manifiesta que: “con la promulgación de la normativa española de protección de datos personales ha tenido un impacto significativo en el ámbito de la protección de los datos de salud”. Se ha dado un reconocimiento de la sensibilidad de los datos de salud, desde la LORTAD de 1992, pasando por la LOPD de 1999, hasta la actual LOPDGDD de 2018, la legislación española ha reconocido consistentemente los datos de salud como una categoría especial de datos personales que requieren un nivel superior de protección. Así mismo Araujo (2021) dice que: “este reconocimiento ha llevado a la implementación de medidas de seguridad más estrictas y a un mayor control sobre el tratamiento de esta información en el sector sanitario”.

La evolución de la normativa ha reforzado el requisito del consentimiento explícito del titular para el tratamiento de datos de salud. Sin embargo, también ha definido excepciones importantes, como el tratamiento necesario por razones de interés público en el ámbito de la salud pública, o para garantizar elevados niveles de calidad y seguridad de la asistencia sanitaria. Esto ha permitido un equilibrio entre la protección de la privacidad y la necesidad de utilizar estos datos para fines médicos y de investigación. La legislación ha evolucionado para exigir medidas de seguridad cada vez más robustas en el tratamiento de datos de salud

El Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) estableció medidas de seguridad de nivel alto para estos datos, incluyendo el cifrado en su transmisión y almacenamiento. La LOPDGDD y el RGPD han continuado esta tendencia, exigiendo la implementación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Además, la normativa ha fortalecido progresivamente los derechos de los pacientes sobre sus datos de salud. Así mismo de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) ya contemplados en legislaciones anteriores, la LOPDGDD ha introducido nuevos derechos como el de portabilidad de datos, que permite a los pacientes obtener y transferir sus historiales médicos de manera más fácil y segura.

En este sentido, dicha normativa ha buscado un equilibrio entre la protección de la privacidad y la necesidad de utilizar datos de salud para la investigación y la salud pública. La LOPDGDD, en línea con el RGPD, establece condiciones específicas para el tratamiento de datos con fines de investigación en salud, permitiendo, por ejemplo, un consentimiento amplio para proyectos de investigación, siempre que se cumplan las garantías apropiadas. Introduciendo, el principio de responsabilidad proactiva (accountability) en el RGPD y la LOPDGDD, que ha tenido un impacto significativo en el sector sanitario. Las organizaciones que tratan datos de salud deben ahora demostrar activamente su cumplimiento con la normativa, lo que ha llevado a la implementación de políticas de privacidad más robustas, evaluaciones de impacto en la protección de datos, y la designación de Delegados de Protección de Datos en muchas instituciones sanitarias.

Normativa de Argentina respecto a la protección de datos personales

En Argentina, la protección de datos personales adquirió rango constitucional a partir de la reforma de 1994. La salvaguarda de la privacidad y la seguridad de la información personal se consolidó con la promulgación de la Ley 25.326 en el año 2000. Bianchi (2018) sostiene que “Esta legislación estableció un marco regulatorio integral, definiendo los principios fundamentales, los derechos de los titulares de los datos y las obligaciones de quienes los manejan, con el fin de asegurar un tratamiento adecuado de la información personal”. Por lo cual, la Ley 25.326 se destacó como una iniciativa pionera en América Latina, sentando un precedente importante en la región. Su objetivo principal fue proporcionar a los ciudadanos las herramientas necesarias para ejercer control sobre sus datos personales, independientemente de si estos se encontraban en repositorios de carácter público o privado. Esta normativa no solo marcó un hito en la protección de la privacidad en Argentina, sino que también sirvió como referente para el desarrollo de legislaciones similares en otros países latinoamericanos.

La vigente Ley de Protección de Datos Personales en Argentina establece una serie de principios y derechos cruciales para salvaguardar la privacidad y seguridad de la información personal. Un aspecto fundamental de esta normativa es el requisito de que los datos procesados sean verídicos, apropiados, relevantes y no excesivos en relación con el propósito y el contexto para el cual fueron recolectados. Además, la ley establece que una vez que se ha cumplido el propósito para el cual se recolectaron los datos y ha transcurrido el período de conservación legalmente establecido, esta información debe ser eliminada de manera segura.

La legislación argentina establece que para que el procesamiento de datos personales sea considerado legal, la entidad o individuo responsable del tratamiento debe cumplir con un requisito fundamental: registrarse ante la Agencia de Acceso a la Información Pública (AAIP) y declarar oficialmente todas las bases de datos que estén bajo su control. Este proceso de registro tiene un propósito crucial: proporcionar transparencia y accesibilidad a la información para los titulares de los datos. Para facilitar el acceso a esta información, se ha implementado una herramienta en línea: el buscador web del Registro Nacional de Bases de Datos Personales. Esta plataforma permite a los

ciudadanos consultar de manera sencilla y directa la información relativa a las bases de datos registradas y sus responsables.

En lo que respecta a la protección de los datos de salud, regulada por la Ley 25.326 de Protección de Datos Personales, promulgada en el año 2000, ha tenido un impacto significativo en la forma en que se manejan los datos de salud en el país. La ley establece que los datos de salud son considerados datos sensibles, lo que implica un nivel más alto de protección. Esto ha llevado a que las instituciones de salud, tanto públicas como privadas, deban implementar medidas de seguridad más estrictas para el almacenamiento y tratamiento de estos datos. Una de las principales influencias de esta normativa ha sido la necesidad de obtener el consentimiento expreso del paciente para la recolección y tratamiento de sus datos de salud. Esto ha promovido una mayor transparencia en la relación médico-paciente y ha empoderado a los ciudadanos en el control de su información personal.

La ley también ha impulsado la implementación de políticas de confidencialidad más robustas en los centros de salud. Esto incluye la restricción del acceso a los datos de salud solo al personal autorizado y la implementación de sistemas de auditoría para monitorear quién accede a la información y con qué propósito. En cuanto al tratamiento de los datos, la normativa ha influido en la adopción de prácticas de anonimización y disociación de datos para investigaciones médicas. Esto permite el uso de información valiosa para el avance de la ciencia médica, mientras se protege la identidad de los pacientes. Además, la implementación de la Historia Clínica Electrónica en Argentina también se ha visto influenciada por esta normativa. Se han establecido estándares de seguridad y protocolos de acceso para garantizar la confidencialidad y la integridad de los datos de salud en formato digital.

Así mismo, la ley ha promovido la creación de roles específicos en las organizaciones de salud, como el de Delegado de Protección de Datos, encargado de supervisar el cumplimiento de la normativa y actuar como punto de contacto con las autoridades de control. La figura del Delegado de Protección de Datos (DPD), aunque no está explícitamente mencionada en la Ley 25.326, ha ganado relevancia en Argentina siguiendo las tendencias internacionales en materia de protección de datos,

especialmente tras la implementación del Reglamento General de Protección de Datos (GDPR) en Europa.

Diferencias

Una diferencia significativa se encuentra en la evolución del marco regulatorio ya que Ecuador presenta un marco regulatorio emergente, con la Ley Orgánica de Protección de Datos Personales promulgada en 2021. Esta novedad implica que el país está en las primeras etapas de implementación y adaptación, lo que puede conllevar desafíos en términos de interpretación legal, creación de jurisprudencia y desarrollo de una cultura de protección de datos en la sociedad y las organizaciones. Mientras que España el marco regulatorio más maduro y evolucionado de los tres países. Su trayectoria en protección de datos se remonta a la Constitución de 1978, con una serie de leyes que han ido adaptándose a lo largo de las décadas. Esta evolución refleja una comprensión profunda y dinámica de los desafíos en protección de datos, desde la LORTAD de 1992 hasta la actual LOPDGDD de 2018. Esta madurez se traduce en una normativa más robusta y probada, con jurisprudencia establecida y una cultura de protección de datos más arraigada en la sociedad y las instituciones. Por otro lado, Argentina ocupa una posición intermedia ya que su Ley de Protección de Datos de 2000 le otorga una experiencia considerable, pero no tan extensa como la española. Esto sugiere un marco regulatorio establecido, pero menos adaptado a los rápidos cambios tecnológicos recientes en comparación con la legislación española actualizada en 2018.

Otra diferencia es que Ecuador, al ser un país más pequeño y no pertenecer a un bloque económico con normativas de protección de datos tan desarrolladas como la UE, ha tenido que desarrollar su marco regulatorio de manera más autónoma. Sin embargo, su ley reciente parece inspirarse en estándares internacionales. Mientras que, la normativa española está profundamente integrada con el marco legal de la Unión Europea, específicamente con el RGPD. Como indica Luño, esta integración va más allá de una simple adopción de estándares; implica una participación activa en la formación y evolución de la política de protección de datos a nivel europeo. En Argentina, se encuentra en una posición intermedia. Aunque no está sujeta a un marco supranacional tan desarrollado como el RGPD, su normativa ha sido reconocida por

la UE como ofreciendo un nivel adecuado de protección, lo que indica un esfuerzo por alinearse con estándares internacionales mientras mantiene su autonomía regulatoria.

La normativa ecuatoriana, siendo más reciente, incorpora conceptos modernos de protección de datos, pero no parece abordar de manera tan explícita los nuevos derechos digitales. Esto podría reflejar un enfoque más centrado en establecer primero una base sólida de protección de datos. Mientras que la legislación española, a través de la LOPDGDD, aborda explícitamente nuevos desafíos tecnológicos y derechos digitales emergentes, como el derecho al olvido, la portabilidad de datos y la desconexión digital en el ámbito laboral. Arenas destaca la importancia de estos nuevos derechos en el contexto digital actual. Por otro lado, Argentina, con una ley del año 2000, enfrenta desafíos para abordar adecuadamente las nuevas realidades tecnológicas sin una actualización sustancial. Bianchi sugiere que la ley argentina, aunque pionera en su momento, podría requerir actualizaciones para abordar los desafíos tecnológicos actuales.

Semejanzas

Los tres países han elevado la protección de datos personales al rango de derecho constitucional, aunque en diferentes momentos históricos. Ecuador lo hizo en su reforma de 2008, España lo anticipó en su Constitución de 1978, y Argentina lo incorporó en su reforma constitucional de 1994. Este reconocimiento constitucional en los tres países refleja una comprensión profunda de la importancia de la protección de datos en la era digital y proporciona una base sólida para el desarrollo de legislación específica. Como señala Luño para el caso español, se puede extender a los otros dos países, esta previsión constitucional demuestra "la temprana conciencia del legislador sobre la importancia de salvaguardar la información personal en la era digital".

Los tres países otorgan una protección especial a los datos sensibles, particularmente a los datos de salud. En Ecuador, la Ley Orgánica de Protección de Datos Personales de 2021 considera los datos de salud como información sensible. En España, desde la LORTAD de 1992 hasta la actual LOPDGDD, se ha mantenido esta consideración. Argentina, en su Ley 25.326, también clasifica los datos de salud como sensibles. Esta

similitud refleja una comprensión común de la necesidad de proteger de manera más rigurosa ciertos tipos de información personal. Como sostiene Razza en el contexto ecuatoriano, pero aplicable a los tres países, "la confidencialidad y la privacidad son cruciales para mantener la confianza entre el paciente y los profesionales de la salud".

Los tres países han establecido autoridades de control independientes para supervisar el cumplimiento de las normativas de protección de datos. En España, se creó la Agencia de Protección de Datos; en Argentina, la Agencia de Acceso a la Información Pública (AAIP); y en Ecuador, la Autoridad de Protección de Datos Personales. Aunque estas autoridades pueden tener diferentes niveles de madurez y capacidades, su existencia en los tres países refleja un compromiso común con la supervisión y el control efectivo de la protección de datos. Esto se alinea con lo que Arenas señala para España, pero que es aplicable a los tres casos: la necesidad de "establecer una regulación para el tratamiento de datos personales y los ficheros que los contenían".

Los tres países han incorporado el principio de consentimiento informado como un elemento central de sus normativas de protección de datos. En Ecuador, Araujo destaca que el consentimiento debe ser "libre, específico, informado e inequívoco". En España, este principio ha sido fundamental desde la LORTAD de 1992 y se ha reforzado con el RGPD. En Argentina, la Ley 25.326 también enfatiza la importancia del consentimiento del titular de los datos. Esta similitud refleja un enfoque común centrado en el empoderamiento del individuo y su derecho a controlar sus datos personales.

CAPÍTULO V

REFLEXIONES FINALES

En este capítulo del trabajo de investigación se presentan los hallazgos y reflexiones que da cumplimiento al objetivo general planteado que es analizar la protección de datos de salud en el ámbito legal. Esto ha sido derivado de un análisis de la normativa vigente y su aplicación práctica, que ha permitido obtener una visión más amplia del estado actual de la protección y tratamiento de los datos de salud.

Hallazgos

Los hallazgos obtenidos a lo largo de esta investigación revelan diversos aspectos del tratamiento de los datos de salud en el contexto ecuatoriano. A continuación, se detallan estos hallazgos según cada objetivo específico planteado.

En lo que concierne al primer objetivo específico se resalta que las políticas internas de protección de datos personales en los centros de salud del Ecuador presentan deficiencias significativas, particularmente en el contexto del Art. 38 de la normativa de protección de datos, dicho artículo determina que se debe incluir medidas para hacer frente a riesgos, amenazas, vulnerabilidades y accesos no autorizados en el tratamiento de datos personales. Además, se ha determinado una dependencia en el equipamiento de seguridad perimetral, lo cual contradice el enfoque requerido por la ley. Esta aproximación respecto a la ciberseguridad no solo genera una falsa protección, sino que también incumple con el principio de seguridad de datos personales estipulado en la normativa. Como consecuencia, existe un riesgo elevado de que un atacante pueda acceder a bases de datos completas de historiales médicos, comprometiendo la privacidad de múltiples pacientes. Además, la falta de directrices para la actualización continua del equipamiento y las estrategias de seguridad contraviene lo establecido en art. 38, que busca proteger contra riesgos existentes. Esta omisión deja a las instituciones sanitarias expuestas a un panorama de ciberseguridad en constante evolución, aumentando el riesgo de seguridad y exposición no autorizada de datos de salud.

Lo que corresponde al segundo objetivo específico se evidencia que la potestad sancionadora del Superintendente es un desafío particular. Esta facultad, otorgada

por la ley, permite al Superintendente imponer sanciones a responsables, delegados, encargados y terceros que incumplan las normativas de protección de datos personales. Sin embargo, en el contexto de los datos de salud, esta atribución adquiere una complejidad particular debido a la naturaleza sensible de la información y la importancia crítica de los servicios de salud. la necesidad de imponer sanciones significativas en casos de violaciones de datos de salud es indiscutible. Los datos médicos son extremadamente sensibles y su mal uso o divulgación no autorizada pueden tener consecuencias graves para los individuos, desde discriminación laboral hasta impactos en relaciones personales. Por lo tanto, las sanciones deben ser lo suficientemente severas para disuadir efectivamente a los potenciales infractores y promover una cultura de cumplimiento riguroso en el manejo de datos de salud.

En cuanto al tercer objetivo específico, se destaca que los datos de salud son considerados una categoría especial que necesita mayor protección, siendo un aspecto común en las leyes de Ecuador, España y Argentina. Aunque las tres normativas reconocen la necesidad de una protección especial para los datos de salud, la implementación práctica varía significativamente. España, beneficiándose de su larga experiencia y de la influencia del riguroso marco europeo, presenta un nivel de implementación más avanzado. Ecuador y Argentina, aunque han establecido bases sólidas en sus legislaciones, se encuentran en un proceso de desarrollo y maduración en la aplicación práctica de estas protecciones, enfrentando desafíos en términos de recursos, infraestructura y cambio cultural necesarios para alcanzar niveles comparables a los europeos. Aunque Argentina cuenta con una ley de protección de datos desde el año 2000, y Ecuador desde 2021, la implementación práctica de medidas de protección para los datos de salud en estos países aún está en proceso de maduración. Esto se refleja en una menor estandarización de los procesos de manejo de datos de salud, una menor integración de las consideraciones de privacidad en el diseño de sistemas de información sanitaria, y en algunos casos, una menor concienciación entre el personal sanitario sobre la importancia de la protección de datos.

Reflexiones

La población ecuatoriana es la principal beneficiaria y sujeto de protección en el tratamiento de datos de salud. Esta información abarca desde historiales clínicos y resultados de pruebas diagnósticas hasta datos genéticos y hábitos de vida, todos ellos componentes esenciales de la identidad y la intimidad personal. La protección de estos datos se materializa a través de un tratamiento complejo de medidas y acciones. Mediante la implementación de políticas públicas integrales que aborden todos los aspectos del ciclo de vida de los datos de salud, desde su recolección hasta su eliminación. Estas políticas deben estar respaldadas por marcos regulatorios sólidos y actualizados que contemplen las particularidades del contexto ecuatoriano y se alineen con los estándares internacionales de protección de datos. Estas acciones pueden salvaguardar los derechos fundamentales de los ciudadanos ecuatorianos, particularmente el derecho a la privacidad y a la autodeterminación informativa en el ámbito de la salud, ya que, al proteger la confidencialidad de los datos médicos, se preserva la dignidad individual y se fortalece la relación de confianza entre el paciente y el sistema de salud, elemento crucial para una atención médica efectiva.

La Universidad Iberoamericana del Ecuador juega un papel crucial en la formación de profesionales conscientes del marco jurídico que regula el tratamiento de datos de salud. La universidad podría incorporar asignaturas específicas en sus planes de estudio, especialmente en la carrera de derecho ya que estas asignaturas no solo abordan los aspectos legales del tratamiento de datos de salud, sino también las implicaciones éticas y las mejores prácticas internacionales en la materia. Estas iniciativas que se podrían incluir en la carrera de Derecho de la Universidad Iberoamericana del Ecuador ayudaría a formar a una nueva generación de abogados especializados en el manejo ético y legal de los datos de salud. En un contexto donde la digitalización de la información médica avanza rápidamente, es crucial contar con profesionales del derecho que comprendan las complejidades de este campo de protección de datos personales.

El Ministerio de Salud del Ecuador, como máxima autoridad sanitaria del país, es el principal responsable de establecer, implementar y supervisar el cumplimiento del marco jurídico para el tratamiento de datos de salud. El Ministerio es responsable de

desarrollar e implementar políticas públicas integrales que guíen el tratamiento ético y seguro de la información médica. Esto incluye la elaboración de protocolos detallados para la recolección, almacenamiento, uso y transferencia de datos de salud en todas las instituciones sanitarias del país. Estas acciones son fundamentales para proteger los derechos de los ciudadanos ecuatorianos, especialmente su derecho a la privacidad en el ámbito de la salud. Al establecer un marco amplio para el manejo de datos médicos, se busca garantizar que la información sensible de los pacientes sea tratada con el máximo respeto y seguridad, ya que un manejo adecuado de los datos de salud no solo protege a los individuos, sino que también permite una mejor planificación y asignación de recursos sanitarios, facilita la investigación médica ética, y sienta las bases para políticas de salud pública más efectivas y basadas en evidencia.

Las futuras investigaciones en el ámbito del tratamiento de datos de salud en Ecuador deben abordar los desafíos actuales y los problemas que surgen con el avance tecnológico. La complejidad de estos temas demanda un enfoque en ciertas áreas como, derecho, ética, tecnología de la información, medicina y salud pública. Además, es importante que estas investigaciones incorporen un análisis comparativo, en el cual se evidencien las experiencias y mejores prácticas de otros países en el manejo de datos de salud. A través de estas investigaciones se podría identificar áreas de mejora en el marco jurídico y regulatorio actual que rige el tratamiento de datos de salud en Ecuador, ya que al anticipar los desafíos futuros y evaluar críticamente las políticas existentes, estos estudios pueden proporcionar una base sólida para la actualización y fortalecimiento de las leyes y regulaciones pertinentes.

Los futuros investigadores en el campo del tratamiento de datos de salud deben desarrollar una visión amplia que les permita entender las interconexiones entre la protección de datos, la innovación tecnológica en salud, las políticas públicas y los derechos individuales de las personas. La preparación de estos futuros investigadores requiere de un enfoque en distintas áreas como el derecho con énfasis en la protección de datos personales y derecho digital, salud pública y tecnología de la información. Con la formación de investigadores se contribuye significativamente al avance del conocimiento en el campo de protección de datos de salud en Ecuador, ya que su trabajo será fundamental para desarrollar un cuerpo de investigación

contextualizado que pueda informar y guiar la formulación de políticas públicas y la actualización de marcos normativos.

La protección de datos personales y derecho digital surge como la ciencia específica crucial en el tratamiento de datos de salud dentro del marco jurídico ecuatoriano. Esta disciplina combina principios del derecho con conocimientos de tecnología de la información, enfocándose en la intersección entre las normas legales y los sistemas informáticos que manejan datos sensibles de salud. Esta ciencia el contexto del tratamiento de datos de salud opera a través de varios mecanismos clave ya que se encarga de la interpretación y aplicación de las leyes y regulaciones existentes a los casos específicos que surgen en el manejo digital de información médica, incluyendo la elaboración de dictámenes jurídicos sobre la legalidad de nuevas tecnologías o prácticas en el sector de salud. Esta disciplina juega un papel importante en este contexto que es garantizar que el tratamiento de datos de salud en Ecuador se realice de manera legal, ética y segura, buscando crear un equilibrio entre la necesidad de innovación y eficiencia en el sector salud y la protección de los derechos fundamentales de los pacientes, especialmente su derecho a la privacidad.

Bibliografía

(s.f.).

Angarita, N. R. (2019). Tratamiento de datos personales. Aproximación constitucional de los datos personales . Legis Editores S.A.

Aranzamendi, L. (2008). Epistemología y la Investigación Cualitativa y Cuantitativa en el Derecho. Lima, Peru: ADRUS.

Arias, F. (2012). El Proyecto de Investigación. Caracas-Venezuela: Episteme.

Barahona, V. C. (2020). Antecedentes y fundamentos del Derecho a la protección de datos. Barcelona-España: Bosch, S.L.

Cano, J. J. (2015). Aproximación a la reforma de la protección de datos personales en Colombia . Colombia.

Carlino, P. (2021). Antecedentes y marco teórico en los proyectos de investigación: aportes para construir este apartado. Argentina.

Constitución de la República del Ecuador. (2008). Pub. L. No. Registro Oficial No. 449.

Cristea Uivaru, L. (2017). La Protección de Datos de Carácter Sensible en el ámbito europeo. Historia Clínica Digital y Big Data en Salud.

Cueva, P. L. (2008). el derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática.

Gómez, C. (2009). Disociación/ Anonimización de los Datos de Salud .

Gónzalez, R. P. (2020). Manual Práctico de protección de datos . Atelier.

Hernández, F. y. (2010). Metodología de la investigación. México: Mc.Graw-Hill.

Hernández, R. F. (2018). Metodología de la Investigación. México: Panamericana Formas e Impresos S.A.

Herrero, J. C. (2021). Protección de datos personales: Manual Práctico.

Hurtado, J. (2010). Metodología de la investigación: Guía para la comprensión holística de la ciencia . Caracas.

Jara, J. N. (2022). Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano. Quito.

León, B. (2000). La definición de salud de la Organización Mundial de la Salud y la interdisciplinariedad.

Ley Orgánica de Protección de Datos Personales. (2021).

Lombarte, A. R. (2019). El derecho fundamental a la protección de datos personales. España.

Puceiro, E. Z. (2015). Paradigma dogmático y evolución científica. Madrid.

Quintana, L. (2019). La hermenéutica como método de interpretación de textos en la investigación. Mar de Plata- Argentina.

Reglamento General de la Ley Orgánica de Protección de Datos Personales. (2023).

Ricoy, C. (2006). Contribución sobre los paradigmas de investigación. En C. Ricoy, Contribución sobre los paradigmas de investigación (págs. 11-22). Brasil: 0101-9031.

Salud, L. O. (2018). La Organización Mundial de la Salud. 4.

Uivaru, C. (2017). La Protección de Datos de Carácter Sensible en el ámbito europeo.

Uivaru, C. (2017). La Protección de Datos de Carácter Sensible en el ámbito europeo. .

Uivaru, C. (2017). La Protección de Datos de Carácter Sensible en el ámbito europeo. Historia Clínica Digital y Big Data en Salud.

Valle, P. C. (2022). La protección de los datos personales relativos a la salud. La historia clínica como eje vertebrador. Sevilla.

Vaquero, Á. N. (2014). Dogmática Jurídica . Chile.

Villafranca, D. (2018). Metodología de la Investigación. Venezuela.

Villamil, S. C. (2021). Metodología de la Investigación.

Vivar, M. B. (2022). Las buenas prácticas para el tratamiento del dato de salud . Revista Ruptura de la Asociación Escuela de Derecho PUCE, 219-243.

Ycaza, J. N. (s.f.). Protección de datos personales en la historia clínica electrónica bajo el marco .

ANEXOS

Documento	Análisis
Constitución de la República del Ecuador 2008	Art. 66, núm.19.- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.
Ley Orgánica de Protección de Datos Personales	Art. 4, núm.7.- Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente. Art.30.- Datos relativos a la salud.- Las instituciones que conforman el Sistema Nacional de Salud y los profesionales de la salud pueden recolectar y tratar los datos relativos a la salud de sus pacientes que estén o hubiesen estado bajo tratamiento de aquellos, de acuerdo a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de

	Datos Personales en coordinación con la autoridad sanitaria nacional. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad, de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas organizativas apropiadas. Esta obligación será complementaria del secreto profesional de conformidad con cada caso. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento, No se requerirá el consentimiento del titular para el tratamiento de datos de salud cuando ello sea necesario por razones de interés público esencial en el ámbito de la salud, el que en todo caso deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección

	de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular; Asimismo, tampoco se requerirá el consentimiento del titular cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como en el caso de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, siempre y cuando se establezcan medidas adecuadas y específicas para proteger los derechos y libertades del titular y, en particular, el secreto profesional. Art.31.- Tratamiento de datos relativos a la salud.-Todo tratamiento de datos relativos a la salud deberá cumplir con los siguientes parámetros mínimos y aquellos que determine la Autoridad de Protección de Datos Personales en la normativa emitida para el efecto: 1. Los datos relativos a la salud generados en establecimientos de salud públicos o privados, serán tratados cumpliendo los principios de

	confidencialidad y secreto profesional. El titular de la información deberá brindar su consentimiento previo conforme lo determina esta Ley, salvo en los casos en que el tratamiento sea necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria, y social, sobre la base de la legislación especializada sobre la materia o en virtud de un contrato con un profesional sanitario. En este último caso el tratamiento sólo podrá ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con la legislación especializada sobre la materia o con las demás normas que al respecto pueda establecer la Autoridad. 2. Los datos relativos a la salud que se traten, siempre que sea posible, deberán ser previamente

	anonimizados o seudonimizados, evitando la posibilidad de identificar a los titulares de los mismos. 3. Todo tratamiento de datos de salud anonimizados deberá ser autorizado previamente por la Autoridad de Protección de Datos Personales. Para obtener la autorización mencionada, el interesado deberá presentar un protocolo técnico que contenga los parámetros necesarios que garanticen la protección de dichos datos y el informe previo favorable emitido por la Autoridad Sanitaria.
Reglamento General de la Ley Orgánica de Protección de Datos Personales	Art 4, núm. 2.-. Datos relativos a la salud: La definición de datos de salud establecida en la Ley comprende la información relativa a todos los aspectos de salud, tanto físicos como psíquicos, de la persona. Se incluyen todos los datos relativos al estado de salud del titular que dan información sobre su estado de salud física o mental pasado, presente o futuro. Así también contiene la información sobre la persona natural recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia; todo número, símbolo o

	dato asignado a una persona natural que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del titular, independientemente de su fuente
Doctrina	León, B. (2000). La definición de salud de la Organización Mundial de la Salud y la interdisciplinariedad. “la salud es una síntesis; es la síntesis de una multiplicidad de procesos, de lo que acontece con la biología del cuerpo, con el ambiente que nos rodea, con las relaciones sociales, con la política y la economía internacional”. (pág. 60) Cristea Uivaru, L. (2017). La Protección de Datos de Carácter Sensible en el ámbito europeo. Historia Clínica Digital y Big Data en Salud.

	“Los datos de carácter personal, son la referencia que nos hace individualizables. Es decir, consiste en toda aquella información relevante concerniente a una persona que nos hace identificables” (pág.18). El tratamiento de datos debe entenderse como el conjunto de operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias” (pág. 68)