**FACULTAD DE POSTGRADOS**

**MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN**

**TÍTULO DE LA INVESTIGACIÓN**

# Políticas de protección de datos personales de una empresa que desarrolla aplicaciones de telesalud en la ciudad de Quito


**Profesor**

Lorena Naranjo Godoy

**Autores**

María Elisa Soto Laso

Santiago Martín Acurio Del Pino


**2023**

**Resumen**

Actualmente, dado el contexto de post pandemia en el que nos encontramos, el diagnóstico clínico y las prestaciones sanitarias mediante aplicaciones de E-HEALTH y Telesalud se han vuelto comunes y necesarias. La atención médica online es el nuevo paradigma al que se ve abocado el Sistema Nacional de Salud Pública. Esto conlleva, obligatoriamente, contemplar la necesidad de proteger los datos personales de los usuarios.

Esta investigación recoge un estudio de campo sobre el tratamiento de la data de esta empresa con sede en Ecuador para la creación de una política de protección de datos personales alineada a la normativa y estándares internacionales.

**Abstract**

Due to current events aligned to the post pandemic world, there has been an increasing need to have tools to facilitate clinical diagnosis and health benefits through E-HEALTH and Telehealth applications. Therefore, this is the new paradigm to which the National Public Health System is focused, which leads to the need for the implementation of personal data protection.

This work includes a field study on the processing of personal data of this company with headquarters in Ecuador for the creation of a personal data protection policy aligned with international regulations and standards regarding the subject.

**Dedicatoria**

Este trabajo está dedicado a las personas que nos apoyan y ayudan e inspiran en el ámbito de nuestra vida personal: nuestra familia.

A la Dra. Laura Nahabetián Brunet por su cátedra de protección de datos personales, porque nos ayudó a entender muchos conceptos dentro de la materia.

**Tabla de Contenido**

Resumen .....2

Abstract.....3

Dedicatoria.....4

Tabla de Contenido.....5

Índice de Tablas.....7

Índice de Ilustraciones .....7

Introducción .....8

1. Marco Conceptual y Revisión de la Literatura .....11

1.1 Desde el derecho a la Salud, pasando por la Cibersalud hasta el *mHealth* ..... 11

1.1.1 Derecho a la Salud..... 11

1.1.2 La Cibersalud ..... 12

1.1.3 Telemedicina y Telesalud..... 13

1.1.4 Salud Móvil o mHealth..... 13

1.2 Datos personales, datos sensibles y datos de salud..... 14

1.3 Uso de teléfonos inteligentes y Apps en la prestación sanitaria... 17

1.4 Gobernanza del Dato y la Política de la empresa que desarrolla aplicaciones de Telesalud..... 18

1.4.1 Alcance de la Política empresarial..... 19

1.5 Antecedentes teóricos del problema..... 19

2. Identificación del problema.....21

3. Pregunta General de Investigación .....22

3.1 Efectos del problema..... 22

3.2 Causas del Problema ..... 23

3.3 Escenarios..... 24

4. Objetivo General .....24

5. Objetivos Específicos .....24

6. Justificación y aplicación de la metodología .....25

7.- Establecer el Alcance y los Objetivos de la Política de protección de datos personales .....29

7.1 Análisis de los factores contractuales ..... 30

7.2 Análisis de factores legales y regulatorios ..... 31

7.3 Análisis de acuerdo con el modelo de negocio ..... 32

7.4 Análisis de acuerdo con la realidad tecnológica actual ..... 33

7.5 Resultados del análisis de los puntos anteriores ..... 33

8. Describir las Funciones y Obligaciones de los responsables y los encargados del tratamiento .....34

8.1 Definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional para la aplicación de la política ..... 34

8.1.1 Sobre el Titular de los Datos Personales..... 34

8.1.1.1 Rendición de cuentas del Titular de los datos ..... 34

8.1.2 Sobre el Responsable del Tratamiento..... 35

8.1.2.1 Rendición de cuentas del Responsable del Tratamiento. ... 35

8.1.3 Sobre el Encargado del Tratamiento ..... 36

8.1.3.1 Rendición de cuentas del Encargado del Tratamiento..... 36

8.1.4 Sobre el Delegado de Protección de Datos Personales ..... 36

8.1.4.1 Rendición de cuentas del Delegado de Protección de Datos Personales ..... 37

9. Elaborar un inventario de los datos personales.....37

9.1 Definir el ciclo de vida de los Datos Personales ..... 37

10. Realizar un Análisis de Riesgo de Datos Personales .....40

10.1 Definir las características del riesgo de acuerdo con el impacto que puede tener en la empresa ..... 41

10.2 Definir los criterios de impacto con relación al daño y al perjuicio al Titular de los Datos Personales ..... 43

10.3 Definir los criterios de aceptación con relación al daño a la empresa ..... 43

11. Estudio de Campo y Propuesta de solución al problema.....44

12. Conclusiones y recomendaciones.....47

12.1 Conclusiones..... 47

12.2 Recomendaciones. ..... 51

Bibliografía.....52

Referencias.....58

**Índice de Tablas**

Tabla 1: Objetivos Específicos..... 25

Tabla 2: Fases del Proyecto – Metodología SCRUM..... 27

Tabla 3: Objetivos específicos y actividades..... 29

Tabla 4: Actividades de Tratamiento..... 50

**Índice de Ilustraciones**

Ilustración 1: Ciclo de Vida del Dato Personal ..... 37

## Introducción

La información sobre la empresa que desarrolla aplicaciones de Telesalud fue entregada a través de un convenio de confidencialidad firmado entre la compañía y los investigadores. Toda la información detallada en el presente texto corresponde a un documento interno facilitado por la compañía para la investigación.

La Empresa es de origen vasco fundada en 2018 con una sucursal en el Ecuador. Su visión radica en la digitalización de los procesos médicos con el fin de mejorar la calidad de la atención y la eficiencia operativa. Se ha enfocado exclusivamente en el desarrollo de herramientas de salud digital, siendo pionera en este mercado, y desarrollando productos *eHealth*. Durante los últimos años ha adquirido los conocimientos técnicos necesarios para la digitalización de los procesos sanitarios.

Su misión es servir de órgano consultor y revisor de las funcionalidades y especificaciones de los desarrollos y productos generados. Su composición es variable pero fundamentalmente participan profesionales de la sanidad de reconocido prestigio y dilatada experiencia tanto a nivel clínico como docente.

La visión de la empresa está enmarcada en la búsqueda y el desarrollo de soluciones digitales que permiten agilizar los procesos administrativos. De esta forma, ayuda a optimizar los tiempos, reducir costos e incrementar la interacción y la calidad de atención con el paciente.

Entre los servicios que presta la empresa están el llamado consentimiento inteligente o *SMART CONSENT*. También se encuentra la firma inteligente o *SMART SIGN*, el servicio denominado alerta de pastillas o *PILL ALARM*. Además, la empresa cuenta con un canal de comunicación que une el emprendimiento y la innovación en un solo espacio, denominado ENNOVATION. De esta manera, mantienen al tanto a los clientes de los productos y servicios que ofrece la empresa.

La empresa tiene como actividad central el desarrollo de servicios de aplicaciones; así como otros tipos de consultoría técnica de telecomunicaciones

y capacitación en informática dentro del campo de la investigación y desarrollo en ciencias médicas, ingeniería y tecnología.

La estrategia empresarial se asienta tanto en la comercialización de soluciones tecnológicas para el sector sanitario, como en la prestación de servicios integrales de asesoría en el diseño, simulación y desarrollo de las principales novedades que existen en tecnología aplicada a salud. Se entiende que el negocio debe sustentarse en los principios de innovación, de mejora continua e integridad, y en la profesionalidad y experiencia del equipo para mejorar así la experiencia de los usuarios. La compañía ofrece un excelente servicio para asegurar, en todo momento, la provisión de asistencia sanitaria de calidad. La empresa realiza una apuesta por el desarrollo de tecnologías y soluciones propias basadas en la experiencia asistencial de su equipo fundador, lo cual le aporta el valor diferencial y le permite competir.

La principal competidora de la organización, desde nuestra experiencia, es TICBIOMED[1], una asociación empresarial que impulsa la salud digital a nivel de España y Europa. Tiene un profundo conocimiento y experiencia en el ecosistema de Salud Digital, dentro de las mismas áreas que la empresa ofrece sus servicios y productos. De igual forma, apoya el proceso de innovación en salud digital para toda clase de empresas y centros hospitalarios.

Dentro del entorno económico, desde el 2020, el Ecuador se ha visto afectado por la pandemia y la emergencia sanitaria causada por el COVID-19. De acuerdo con el Banco Mundial, la crisis puso en evidencia algunas debilidades estructurales tales como la carencia de amortiguadores macroeconómicos, la elevada informalidad, un sistema de salud poco preparado y las grandes brechas en el acceso a servicios públicos (Banco Mundial, 2022). Aunque el gobierno, a partir de mediados del 2021, logró vacunar al 85 % de la población consiguiendo, con esto, salir de la recesión y reducir secuelas frente a la crisis (Agencia EFE, 2021) aún se debe buscar una mejora sistemática del ambiente de inversiones que permita retomar una senda de crecimiento menos

[1] Para más información ver https://ticbiomed.org/

dependiente del petróleo, el cual, en el mediano plazo, podría verse desplazado por energías renovables.

Al analizar el entorno sociocultural, se puede citar a la Comisión Económica para América Latina (Cepal), que dice lo siguiente: “Si la inflación supera en dos puntos a la proyección inicial de 2,8% para Ecuador; es decir, si se llega a por lo menos 4,8% hasta finales de 2022, un número importante de ecuatorianos no tendrán ni para cubrir lo básico en alimentación” (LA HORA, 2022, párrafo. 4). En resumen, los índices de pobreza siguen creciendo. La clase media tiene cada día más dificultad en acceder a la canasta básica, reduciendo cantidades y calidad de productos.

Tras la pandemia, se ha podido presenciar notablemente un incremento en la inseguridad, el narcotráfico y el crimen organizado. Otro de los grandes indicadores es el desempleo: “El Instituto Nacional de Estadística y Censos (INEC) publicó las cifras mensuales que establecen que la tasa de desempleo se ubicó en abril de 2022 en un 4,7 %. Ese porcentaje indica que son casi 399.500 personas las que no encuentran trabajo, y es menor al 5,1 % reportado en abril del 2021” (Redacción Eluniverso.com, 2022).

En el contexto tecnológico, se puede señalar que:

> Ecuador ha logrado incrementar en un 12% la cantidad de conexiones generadas de parte de usuarios en Google, que cuentan con un promedio de 2 dispositivos para acceder a plataformas y servicios digitales, captando un 20% de crecimiento promedio transaccionado en canales digitales (comercio telemático). (Del Alcázar, 2022)

Evidentemente, la pandemia logró acelerar los procesos de transformación digital en los usuarios.

En cuanto al entorno ambiental, el Gobierno Nacional se definió en sus propuestas electorales como un gobierno de transición ecológica, para que los modelos tanto de producción como de consumo fueran económicamente

sostenibles y sustentables. Sin embargo, en la actualidad el Gobierno ha cambiado su postura por una mayor explotación minera, así como el aumento de la deforestación. Aunque es un proceso que lleva tiempo y no se logrará por completo durante el actual Gobierno, los expertos opinan que la transición se contradice con la política extractivista que se está implementando (Loaiza, 2021).

Como último indicador, se debe mencionar al sector de la salud. Aunque la Constitución del Ecuador señala que se deberá destinar como presupuesto un valor equivalente y no menor al 4 % del PIB a la salud, esto no se cumple. “La asignación en 2019 para el sector de salud fue del 2,78% del Producto Interno Bruto (PIB) por lo que, pese al leve incremento con respecto del año anterior, aún es insuficiente” (COMERCIO, 2019. Párrafo 16). Estos cortes presupuestarios resultaron en que la mitad de la población no cuente con un seguro de salud, y que 1 de cada 4 ecuatorianos no tenga acceso a ningún servicio de salud (Agencia EFE, 2021). Es así como Ecuador encabeza la lista de los países que peor manejaron la pandemia del Covid19 a nivel mundial. (Castillo, 2021)

# 1. Marco Conceptual y Revisión de la Literatura

## 1.1 Desde el derecho a la Salud, pasando por la Cibersalud hasta el *mHealth*

### *1.1.1 Derecho a la Salud*

La Constitución de la República, en su Artículo 32, dispone que la salud es un derecho garantizado por el Estado, cuya realización se vincula al ejercicio de otros derechos mediante políticas económicas, sociales, culturales, educativas y ambientales; y, el acceso permanente, oportuno y sin exclusión a programas, acciones y servicios de promoción y atención integral de salud (Asamblea Constituyente del Ecuador, 2008).

El Artículo 361 de la Constitución de la República prevé que el Estado ejercerá la rectoría del Sistema Nacional de Salud a través de la Autoridad Sanitaria Nacional (Asamblea Constituyente del Ecuador, 2008). De acuerdo con

la Ley Orgánica de Salud[2], esta autoridad es el Ministerio de Salud, el cual es responsable de formular la política nacional de salud y de normar, regular y controlar todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector (Asamblea Nacional del Ecuador, 2006).

### *1.1.2 La Cibersalud*

En mayo de 2005, los ministros y ministras de Salud de los 192 países miembros de la Organización de las Naciones Unidas reunidos en Ginebra con motivo de la 58ª Asamblea de la Organización Mundial de la Salud (OMS) aprobaron la resolución sobre la Cibersalud. Por primera vez, la OMS reconoció la aportación que para la salud y la gestión de los sistemas de salud supone la incorporación de las TICs, entendiéndose a estas como una oportunidad única para el desarrollo de la salud pública en la que se puede, al fin, cumplir el principio de universalidad de la atención sanitaria. Esto se convirtió en una opción práctica para reducir la brecha en el acceso a la salud por razones geográficas.

El desarrollo de la Cibersalud contempla el uso eficiente, efectivo y seguro de las tecnologías de la información y comunicación en los servicios de atención sanitaria, vigilancia de la salud, literatura y educación, conocimiento e investigación. En ese sentido, el fortalecimiento de los sistemas de salud a través de la Cibersalud "refuerza los derechos humanos fundamentales aumentando y mejorando la equidad, la solidaridad, la calidad de vida y la calidad en la atención" (Organización Mundial de la Salud, 2004).

En estos últimos años, se ha dado un efecto de transformación digital forzado por la pandemia del COVID-19, lo que ha impulsado el campo de la Cibersalud. La inversión privada en el sector de salud ha incluido el desarrollo

[2] "La autoridad sanitaria nacional es el Ministerio de Salud Pública, entidad a la que corresponde el ejercicio de las funciones de rectoría en salud; así como la responsabilidad de la aplicación, control y vigilancia del cumplimiento de esta Ley; y, las normas que dicte para su plena vigencia serán obligatorias." Art. 4 Ley Orgánica de Salud del Ecuador (Asamblea Nacional del Ecuador, 2006).

de aplicaciones de mHealth como las de que desarrolla aplicaciones de Telesalud.

### *1.1.3 Telemedicina y Telesalud*

La Telemedicina/Telesalud representa una herramienta valiosa para vencer las barreras de acceso a los servicios de salud de calidad. En especial, funciona en zonas rurales o con limitada capacidad resolutiva porque permite la promoción, prevención, educación y rehabilitación (Organización Panamericana de la Salud, 2016).

Existen muchas ventajas en la aplicación de la telemedicina. La primera es la accesibilidad, ya que no importa el lugar en el que se encuentra el paciente, ya que gracias a la tecnología mínima puede enlazarse a un teleconsultorio. La segunda ventaja es la eficiencia, lograda a través de una reingeniería de la atención sanitaria en la que se reducen las listas de espera. La tercera, es el mejoramiento de la calidad del servicio mediante la precisión diagnóstica, más la posibilidad de obtener una segunda opinión. Y la cuarta ventaja está relacionada a la equidad, ya que esta metodología brinda la posibilidad de universalizar el servicio sanitario, eliminando la marcada desigualdad en la disponibilidad y calidad de la asistencia médica en poblaciones rurales y urbano marginales (Ferrer, 2001).

### *1.1.4 Salud Móvil o mHealth*

De acuerdo con Erazo (2022), una aplicación o APP móvil es un tipo de *software*[3] diseñada para ejecutarse en un dispositivo móvil, que puede ser un teléfono inteligente o una tableta. Incluso si las aplicaciones suelen ser pequeñas unidades de *software* con funciones limitadas, se las arreglan para proporcionar a los usuarios servicios y experiencias de calidad.

[3] A pesar de que algunas personas dicen que en el caso de las aplicaciones tienen un sentido diferente a los programas de computadora, siguen siendo un código objeto y un código fuente que, según la definición común de *software*, en ese sentido para nosotros son exactamente iguales.

El *mHealth*[4] es, según definición de la OMS, es: “La práctica de la medicina y la salud pública soportada por dispositivos móviles como teléfonos, dispositivos de monitorización de pacientes, asistentes digitales y otros dispositivos inalámbricos” (Organización Mundial de la Salud, 2022). Todo ello incluye aplicaciones sobre el estilo de vida y bienestar que conectan a las personas con dispositivos médicos o sensores (“Internet de las cosas”), recordatorios de medicación e información de salud a través de mensajes de texto y servicios de telemedicina.

Algunas de las características del *mHealth* son:

- La capacidad para prestar los servicios de medicina a distancia a través de los dispositivos móviles, en los que se incluye el diagnóstico, el tratamiento y el seguimiento de pacientes a distancia.
- La prevención de enfermedades y formación médica.
- La optimización de los servicios de atención en salud, insistiendo en la eficacia, calidad y disponibilidad.

### 1.2 Datos personales, datos sensibles y datos de salud

Nelson Remolina sobre la protección de los datos personales destaca la importancia de fomentar el respeto a la privacidad y garantizar la seguridad de los datos personales (Molina Angarita, 2017). Parafraseando a Colaner (2022), los datos son *recorded facts* (hechos guardados/registrados); entonces, el dato es la unidad de información más pequeña que representa un hecho que se encuentra registrado, ya sea en medios analógicos como el papel, o en medios digitales como las bases de datos, los mismos que han sido tratados desde muchos años atrás para construir información valiosa.

Desde la perspectiva de la Constitución, en aplicación del principio de convencionalidad dispuesta en el pacto de San José de Costa Rica, es notable el esfuerzo que realiza el Comité Jurídico Interamericano para difundir y expandir

[4] El termino fue acuñado por Robert S. H. Istepanian, profesor invitado en la Facultad de Medicina, Instituto de Innovación en Salud Global, Imperial College, Londres.

los conceptos relacionados a la protección de datos personales. En nuestra opinión, esta es la definición de datos personales más precisa y completa:

> (…) abarca la información que identifica o puede usarse de manera razonable para identificar a una persona física de forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea o a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. Incluye información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo. La frase no abarca la información que no identifica a una persona en particular (o no puede usarse de manera razonable para identificarla). (Comité Jurídico Interamericano, 2021)

En este mismo sentido, el Comité Jurídico Interamericano definió el concepto de datos sensibles como:

> […] una categoría más estrecha, que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria. (Comité Jurídico Interamericano, 2021)

En ese contexto, los datos relativos a la salud son parte de los datos sensibles, por lo que merecen una protección reforzada y solo se podrán almacenar, transmitir o revelar, entre otras formas de tratamiento, bajo ciertas condiciones y con determinadas garantías (Agencia Española de Protección de Datos Personales, 2022). En ese sentido el trabajo de Karina Ingrid Medinaceli sobre el tratamiento de los datos sanitarios en la historia clínica electrónica: caso boliviano, detalla cómo la protección de los datos personales es una preocupación crítica para garantizar la privacidad y seguridad de los pacientes (Medinaceli, 2017).

Los datos sensibles se definen en el Art. 4 de la Ley Orgánica de Protección de Datos Personales (LOPDP) como: “Los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud” (Asamblea Nacional del Ecuador, 2021).

También son datos de salud los datos genéticos (Art. 4 de LOPDP), que son “aquellos datos personales únicos relativos a las características genéticas heredadas o adquiridas de una persona natural, que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona” (Asamblea Nacional del Ecuador, 2021). Por tanto, los datos personales existentes en bases de datos sanitarias son de dos tipos: los de tipo estándar, que identifican a la persona, tales como nombre y apellidos, dirección, teléfono, cédula de identidad, número de seguro social, etc.; y los especiales, que son toda la información acerca de su estado de salud, tales como pruebas diagnósticas, cirugías, medicamentos, antecedentes familiares, etc. (Agencia Española de Protección de Datos Personales, 2019).

En definitiva, “son datos de salud cualquier información que ofrezca una visión sobre su situación médica o estado de salud (presente, pasada o futura), incluida la prestación de servicios de atención sanitaria” (Agencia Española de Protección de Datos Personales, 2022).

### 1.3 Uso de teléfonos inteligentes y Apps en la prestación sanitaria

En el estudio del 2021 sobre marketing digital de la empresa *We are Social*, citado por Clay Alvino, sobre el estado general del uso de móviles, internet y redes sociales en el Ecuador, se señala que el número de dispositivos móviles conectados en el país es de 13.82 millones, lo que constituye un 77,8% de la población; también se explica que hay 10.17 millones de usuarios de internet y 14 millones de perfiles de redes sociales, número que representa el 78,8% de los 17.77 millones de habitantes del país (Alvino, 2022).

En nuestro país, como en otros países del mundo, la relación entre el paciente y el sistema sanitario es incongruente y no funciona correctamente. El paciente tiene mucha información médica que puede ser registrada mediante cuestionarios validados, en todo momento debemos mantener la privacidad de esta información entendiendo esta como una limitación del acceso y uso de la información clínica del individuo para preservar su dignidad, integridad y autonomía (Ferrer-Márquez & Pardo, 2017). El profesional médico se somete a condiciones no apropiadas en el tiempo para recopilar esta información o completar estos cuestionarios en la clínica ambulatoria. Durante la consulta, el profesional médico tiene que recopilar la información y transcribirla en su sistema informático; diferentes estudios han demostrado que existe entre un 10 y 20% de error al transcribir la información. Toda la información recabada es fundamental, tanto para el seguimiento del paciente como para la valoración del profesional médico.

Desde que comenzó la pandemia de COVID19, los servicios de salud de rutina fueron reorganizados o interrumpidos y muchos dejaron de brindar atención a las personas en tratamiento contra enfermedades como el cáncer, enfermedades cardiovasculares y diabetes. De igual manera, se retrasaron 3 millones de operaciones en la primera ola, hubo 1 millón de retrasos en la segunda ola y se espera que los retrasos sigan aumentando. Toda esta situación conlleva que las prioridades y el tiempo de las consultas se haya reducido a su mínima expresión (Organización Panamericana de la Salud, 2020).

El componente central de este proyecto tecnológico radica en el bienestar del paciente y la mejoría de los centros de salud, tanto en ámbito público o privado. Se busca brindar, a través de una plataforma digital, todo el contenido e información necesarios para el diagnóstico.

La tecnología que ha llevado al “Internet de las cosas” también nos ha dotado de capacidades de aprendizaje profundo e inteligencia aplicada artificialmente al mejoramiento del estilo de vida de los pacientes, pudiendo así cumplir con la disposición constitucional de universalizar el servicio de salud.

Uno de estos factores que está apuntalando actualmente a un escenario tecnológico de digitalización, es la disposición del cliente por mejorar, mediante el uso de la tecnología aplicada, su nivel de salud y, consecuentemente, su estilo de vida. Este aspecto es referenciado como *mHealth* o salud móvil, haciendo referencia al uso de teléfonos inteligentes.

## 1.4 Gobernanza del Dato y la Política de la empresa que desarrolla aplicaciones de Telesalud

De acuerdo con la Agencia Española de Datos Personales, el gobierno o la gobernanza de datos es: “El proceso por el que se implementan políticas y procedimientos para garantizar una gestión efectiva y eficiente de la información en la entidad” (Agencia Española de Protección de Datos Personales, 2021). Por ello, para una gestión efectiva y eficiente dentro de la empresa que desarrolla aplicaciones de Telesalud, se requiere de políticas de protección de datos como un medio para la reducción del riesgo en el tratamiento de los datos personales de salud.

Comenzaremos por explicar que una política es una declaración de alto nivel, que describe la posición de la entidad sobre un tema específico. En este caso, para la empresa es la protección de datos personales. En virtud del principio de responsabilidad proactiva y demostrada, recogido en el Art. 10 literal k de la Ley de Protección de Datos Personales, las políticas han de ser “compromisos establecidos a nivel de la dirección de la organización” (Agencia

Española de Protección de Datos Personales, 2021). La política se basa en la declaración explícita de intenciones frente al tratamiento de datos personales en el diseño y desarrollo de aplicaciones de salud móvil, y pasa a ser la "línea de actuación" convenida por todas las personas interesadas (Organización Panamericana de la Salud, 2018).

### *1.4.1 Alcance de la Política empresarial*

Esta es una empresa *eHealth* creada por profesionales de la sanidad para aportar, a través de la digitalización de los procesos médicos, soluciones eficaces para el paciente el sistema sanitario. El alcance del proyecto será la creación de un marco normativo alineado a la Ley Orgánica de Protección de Datos Personales del Ecuador, que define un modo de actuar efectivo, práctico y ejecutivo, que permita establecer los procesos y mecanismos de tratamiento para la protección de datos personales a lo largo de su ciclo de vida dentro de los productos y servicios que brinda la compañía, garantizando los derechos y libertades de los titulares (Agencia Española de Protección de Datos Personales, 2021).

## 1.5 Antecedentes teóricos del problema

Con la aprobación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo del 2021, el país cuenta por fin con el desarrollo normativo de un derecho humano de cuarta generación (González Álvarez, 2011) contemplado en la norma suprema desde el 2008. A partir de esa resolución, la protección de datos personales no solo es un derecho constitucional, sino también una obligación legal.

Para que funcionen las aplicaciones de telesalud y mHealth es necesario poseer un teléfono inteligente, de acuerdo con Fernández (2022): "El número de usuarios de teléfonos inteligentes a nivel mundial supera los 3.000 millones y se prevé que siga creciendo de forma paulatina durante los próximos años".

La llegada de la LOPDP también se vio impulsada por la transformación digital forzada por el COVID-19, que contribuyó al uso constante de las aplicaciones *mHealth,* que tratan datos personales de salud. Así lo corrobora Bastidas (2020) cuando señala que: “El desarrollo de aplicaciones de salud para dispositivos móviles ha tenido un crecimiento exponencial con la aparición de SARS-CoV-2”. Las aplicaciones se han constituido en herramientas que han servido para el control de la pandemia, pero no se conoce cuántas de ellas cumplen con los principios de protección de los datos personales.

En Europa, a partir de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, se creó el Grupo de Trabajo en materia de protección de Datos Personales y Privacidad de la Comisión Europea. Una de sus tareas era el suministrar a la Comisión dictámenes sobre la protección de datos personales que facilitaran el cumplimiento de la Directiva antes señalada. Es así que, en el año 2013, se emite el Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes (Grupo de Trabajo…, 2013). Ese sería el primer antecedente teórico que aborda la problemática jurídica planteada en el problema de investigación.

Posteriormente, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogó la Directiva 95/46/CE, creándose el Reglamento General de Protección de Datos Personales que entró en plena vigencia en Europa en mayo del 2018. Es este instrumento europeo el que sirvió de base para construir la Ley Orgánica de Protección de Datos Personales vigente en Ecuador.

Por tanto, el problema ha sido abordado principalmente desde el aspecto jurídico, generando directrices por parte de los organismos creados para la Protección de Datos Personales y dando instrucciones que se establecen o se tienen en cuenta al proyectar la protección de datos personales sobre los dispositivos inteligentes.

Es así como este grupo asesor o grupo de expertos, por medio de debates internos, procede a realizar, desde un enfoque cualitativo, el análisis jurídico de la normativa europea sobre protección de datos personales, sumado al análisis los riesgos “significativos para la vida privada y la reputación de los usuarios de dispositivos inteligentes” (Grupo de Trabajo en materia de protección de datos y privacidad, 2013). Así también, reseñando y aclarando el marco jurídico aplicable al tratamiento de los datos personales en el desarrollo, la distribución y el uso de aplicaciones *mHealth* que deben diseñarse de tal manera que la privacidad de los usuarios finales esté protegida de manera óptima (protección por defecto y desde el diseño), colocando como ejes rectores de la directriz el requisito del consentimiento informado, los principios de limitación de la finalidad y de minimización de los datos, la necesidad de adoptar medidas de seguridad adecuadas y finalmente periodos de conservación de datos razonables (Grupo de Trabajo en materia de protección de datos y privacidad, 2013).

## 2. Identificación del problema

Las aplicaciones móviles de *mHealth* deben manejar una gran cantidad de datos personales de salud y estos deben estar en concordancia con las disposiciones de la Ley Orgánica de Protección de Datos Personales. Por tanto, la problemática radica en que la empresa que desarrolla aplicaciones de Telesalud, que opera en el Ecuador, no posee una política de protección de datos personales enfocada a su trabajo como diseñador y desarrollador de aplicaciones y programas de *mHealth*, lo cual luego de expedición de ley es una obligación legal.

Karina Medinaceli recomienda que, para asegurar un alto nivel de seguridad de los datos personales sanitarios, se necesitan leyes eficaces, mecanismos de recopilación seguros, planes de respuesta a incidentes y capacitación adecuada para todos los profesionales involucrados (Medinaceli, 2017).

Por ello es necesario estudiar el caso de los países de Europa[5], cuyas autoridades de protección de datos (Comité Europeo de Protección de Datos) han generado varias directrices destinadas a promover el respeto y garantía del derecho fundamental a la protección de datos personales en el entorno de la *mHealth* (Bastidas, 2020).

Es necesario definir una política de protección de datos personales para la empresa, para, así, determinar los requisitos que deben cumplir las aplicaciones de *software*, como también el proceso de recolección de datos y de información, con el fin de adecuarse a la normativa de protección de datos personales vigente en el país desde el 2021.

La presente investigación tiene como objeto central el estudiar las políticas de protección de datos personales de la empresa que desarrolla aplicaciones de Telesalud, con sede en la ciudad de Quito. El periodo temporal que abarcará la investigación corresponde al año 2022.

## 3. Pregunta General de Investigación

¿Cómo crear las políticas de protección de datos personales de la empresa que desarrolla aplicaciones de telesalud en el 2022?

### 3.1 Efectos del problema

La falta de una línea de actuación alineada a la protección de datos personales por parte de las empresas limita su desempeño dentro de la economía digital, ya que esta se sostiene por los datos, que deben tener una base de legitimación; de lo contrario, son un riesgo a la privacidad, a la seguridad[6] y libertad de las personas, afectando la confianza en los entornos

[5] A este respecto hay que revisar el trabajo de Concepción Conde Ruiz quien investiga la forma en que los países europeos han abordado el uso, almacenamiento y recopilación de datos, donde se concluye que la legislación europea de protección de datos personales está fuertemente influenciada por instituciones como el Comité Europeo de Protección de Datos.

[6] "La compañía de seguridad informática vpnMentor aseguró en un informe que dos de sus expertos detectaron a inicios de septiembre que un servidor utilizado por una empresa de análisis

digitales. El Embajador Charles-Michel Geurts, representante de la Unión Europea en nuestro país, indica que:

> […] la conectividad digital y la promoción de estándares convergentes, también en protección de datos pueden sin duda, ayudar a promover la economía digital como motor de un crecimiento sostenible que también contribuya a cerrar la brecha digital favoreciendo la igualdad de acceso a los servicios de la sociedad de la información, para evitar de esta forma la exclusión social y maximizar el potencial de crecimiento de nuestras economías. Todo ello sin olvidar la importancia de obtener la confianza de los ciudadanos en tanto que usuarios y titulares de derechos; sin esa confianza todos estos esfuerzos no prosperarán. Y una normativa de protección de datos robusta y eficiente es un elemento fundamental para obtener y mantener dicha confianza. (Geurts, 2021)

### 3.2 Causas del Problema

El desarrollo de las tecnologías disruptivas como la inteligencia artificial y el Big Data ha posibilitado el tratamiento masivo de datos personales a través de los dispositivos inteligentes, incluidos los datos personales de salud debido a la pandemia de COVID-19. No obstante, la falta de una política interna sobre tratamiento de datos personales dentro de las empresas ha provocado que no exista una protección por diseño y por defecto de las aplicaciones para dispositivos inteligentes, dejándolas vulnerables a accesos no autorizados y a la utilización ilícita de sus datos.

---

de datos y que contenía información personal sobre millones de ecuatorianos no contaba con los protocolos de protección necesarios" (Redacción BBC News Mundo, 2019).

### 3.3 Escenarios

El principal beneficio de contar con las políticas de protección de datos personales de la empresa es garantizar y proteger los derechos de las personas físicas que tengan relación con el desarrollo de las aplicaciones de Telesalud, de acuerdo con los principios establecidos en la LOPDP. Con esto, se busca evitar cualquier contienda legal a futuro, además de minimizar el riesgo en el tratamiento de datos personales.

## 4. Objetivo General

Crear la política de protección de datos personales de la empresa que desarrolla aplicaciones de Telesalud con sede en la ciudad de Quito, 2022.

## 5. Objetivos Específicos

| Objetivo General | Preguntas específicas | Objetivos específicos |
|---|---|---|
| Crear la política de protección de datos personales de la empresa que desarrolla aplicaciones de Telesalud con sede en la ciudad de Quito, 2022. | ¿Cuál es el alcance y los objetivos de la Política de protección de datos personales? | Establecer el Alcance y los Objetivos de la Política de protección de datos personales |
| | ¿Cuáles son las funciones y obligaciones de los responsables y encargados del tratamiento? | Describir las Funciones y Obligaciones de los responsables y los Encargados del tratamiento |
| | ¿Cómo elaborar un inventario de datos personales? | Elaborar un Inventario de Datos Personales |
| | ¿Cómo realizar un análisis de riesgo de datos personales? | Realizar un Análisis de Riesgo de Datos Personales |
| | ¿Cómo identificar las medidas de seguridad y | Identificar las medidas de seguridad y realizar un Análisis de Brecha |

| Objetivo General | Preguntas específicas | Objetivos específicos |
|---|---|---|
| | realizar un análisis de brecha? | |

*Tabla 1: Objetivos Específicos*

## 6. Justificación y aplicación de la metodología

El presente trabajo de investigación realizará un estudió exploratorio de las políticas de protección de datos personales, motivado por el limitado estudio teórico y práctico del problema de investigación dentro del país, dada la falta del marco normativo apropiado. El estudio también será descriptivo, en la medida que permita especificar los principios y derechos relacionados con la protección de datos personales de salud en dispositivos inteligentes.

Las modalidades de investigación serán de campo y documental. La investigación se realizará en las instalaciones de la empresa que desarrolla aplicaciones de Telesalud, con sede en la ciudad de Quito, ya que es necesario observar cómo se realiza el tratamiento de los datos personales dentro de la misma. También se revisará la documentación digital e impresa sobre protección de datos personales, principalmente la proveniente de fuentes europeas.

Se utilizará, además, el método inductivo-deductivo, en la medida que la deducción permite establecer un vínculo entre la teoría sobre la protección de datos personales y la observación de los procesos de tratamiento de datos en la empresa. Por otro lado, la inducción conlleva analizar la posición particular de la empresa como desarrolladora de aplicaciones de telesalud y telemedicina, y su adecuación a la LOPDP. También manejaremos el método analítico-sintético, ya que basaremos nuestra investigación en el análisis del derecho a la autodeterminación informativa, y su aplicación progresiva a las políticas de protección de datos personales.

Al ser una investigación de tipo cualitativo, no es necesario hacer el cálculo de población, ni muestra.

Los instrumentos de investigación que se utilizarán son: las entrevistas a los personeros y trabajadores de la empresa que desarrolla aplicaciones de

Telesalud, la observación directa del modelo de negocio y el análisis de los documentos relacionados con el desarrollo de las aplicaciones de eHealth y telesalud de la empresa.

Todos los datos recabados durante la investigación servirán para elaborar la política de protección de datos personales de acuerdo con la metodología SCRUM que es un marco de trabajo liviano que ayuda a las personas, a los equipos y a las organizaciones a generar valor a través de soluciones adaptativas para problemas complejos. Para Mariño y Alfonzo (2014), siguiendo a Diaz y Del Dago, el SCRUM es una colección de procesos para la gestión de proyectos que permite centrarse en la entrega de valor para el cliente y la potenciación del equipo para lograr la máxima eficiencia, dentro de un esquema de mejora continua:

> SCRUM es un marco de trabajo iterativo e incremental para el desarrollo de proyectos y se estructura en ciclos de trabajo llamados SPRINTS. Estos son iteraciones de 1 a 4 semanas, y se suceden una detrás de otra. Al comienzo de cada Sprint, el equipo multifuncional selecciona los elementos (requisitos del cliente) de una lista priorizada. Se comprometen a terminar los elementos al final del Sprint. Durante el Sprint no se pueden cambiar los elementos elegidos. Al final del Sprint, el equipo lo revisa con los interesados en el proyecto, y les enseña lo que han construido. (Mariño; Alfonzo, 2014)

El proyecto consta de cuatro fases:

- Inicio
- Planificación
- Desarrollo
- Entrega

Durante la fase de inicio, se realizará la encuesta de situación de cumplimiento de LOPDP; luego, en la fase de planificación se llevarán a cabo los objetivos específicos y se describirán las actividades a realizar; esta planeación nos permite generar los *sprints* con cada objetivo específico en la fase de

planeación y por cada actividad en las fases de desarrollo y entrega, las cuales tendrán una duración promedio de 1 a 3 semanas, lo que permitirá señalar las fechas de duración de las fases y de todo el proyecto.

| **Fases** | **Objetivos específicos** |
|---|---|
| Inicio | Realizar encuesta de situación del cumplimiento de LOPDP |
| Planificación | Establecer el Alcance y los Objetivos de la Política |
| | Describir las Funciones y Obligaciones de los responsables y los encargados del tratamiento |
| | Elaborar un Inventario de Datos Personales |
| | Realizar un Análisis de Riesgo de Datos Personales |
| | Identificar las medidas de seguridad y Análisis de Brecha |
| Desarrollo | **Actividades** |
| | Elaboración de la Política de Protección de Datos Personales |
| | Revisión de la Política |
| Entrega | Revisión Final |
| | Entrega Final |

*Tabla 2: Fases del Proyecto – Metodología SCRUM*

| **Objetivos específicos** | **Actividades** |
|---|---|
| Establecer el Alcance y los Objetivos de la Política de protección de datos personales | 1. Realizar el análisis de los factores contractuales<br>2. Realizar el análisis de los factores legales y regulatorios<br>3. Realizar el análisis de acuerdo con el modelo del negocio<br>4. Realizar el análisis de acuerdo con la realidad |

| Objetivos específicos | Actividades |
|---|---|
| | tecnológica actual<br>5. Definir el alcance de la política y los objetivos de esta, con base en los análisis anteriores |
| Describir las Funciones y Obligaciones de los responsables y los encargados del tratamiento | 1. Definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional para la aplicación de la política<br>2. Definir el marco sancionatorio por incumplimiento de la política |
| Elaborar un Inventario de Datos Personales | 1. Definir el Ciclo de vida del Dato Personal<br>2. Crear el catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales<br>3. Determinar las finalidades de cada tratamiento de datos personales<br>4. Crear el catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no<br>5. Crear el catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales<br>6. Crear la lista de responsables y encargados del tratamiento y el instrumento jurídico por el cual se legitima el tratamiento |
| Realizar un Análisis de Riesgo de Datos Personales | 1. Definir las características del riesgo de acuerdo con el impacto que puede tener en la empresa<br>2. Definir los criterios de impacto con relación al daño y al perjuicio al titular de los datos |

| Objetivos específicos | Actividades |
|---|---|
| | personales<br>3. Definir los criterios de aceptación con relación al daño a la empresa |
| Identificar las medidas de seguridad y realizar un Análisis de Brecha | 1. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable |

*Tabla 3: Objetivos específicos y actividades*

## 7.- Establecer el Alcance y los Objetivos de la Política de protección de datos personales

Lo que se busca con el presente trabajo investigativo aplicado es desarrollar una guía práctica para crear una política de protección de datos personales para la empresa que desarrolla aplicaciones de Telesalud, para lo cual se toma en cuenta su contexto actual en relación con los procesos, procedimientos y la información que esta posee, para luego garantizar la eficacia en la protección de datos personales, y que esta no se limite a una pura declaración formal en un documento desvinculado de la realidad de los procesos, información y procedimientos de la entidad (Agencia Española de Protección de Datos Personales, 2021).

Para ello se ha realizado las siguientes actividades:

1. Una encuesta sobre protección de datos personales a la empresa para verificar su estado de situación,
2. Un inventario de datos personales
3. Verificar la necesidad una EIPD y el análisis del riesgo inherente
4. Un consentimiento informado de tratamiento de datos personales
5. Una Política de Protección de Datos Personales de las aplicaciones

## 7.1 Análisis de los factores contractuales

Generalmente, es necesario realizar un examen de los acuerdos existentes entre los diferentes integrantes del sistema de protección de datos personales, con la finalidad de determinar sus derechos y obligaciones a la luz de los contratos válidamente celebrados.

Dentro del diseño de una política de protección de datos personales, el análisis de los contratos válidamente celebrados se realiza por la exigencia de legitimar la actuación de la empresa al momento de obrar como un tercero de confianza y recibir los datos personales de salud que provienen de los prestadores de servicios de salud, tanto públicos como privados.

> La relación con los responsables del tratamiento se debe realizar mediante un contrato que ha de constar por escrito, (incluso en formato digital, aplicando el principio de equivalencia funcional de la Ley de Comercio Electrónico), debiendo constar en su contenido algunos requisitos que se encuentran en la LOPDP. Así, es necesario identificar de forma clara y concreta cuáles son los datos y las instrucciones para el tratamiento de estos que realizará ese encargado del tratamiento y establecer la forma en que asegura el cumplimiento de las obligaciones de responsabilidad proactiva. Como, por ejemplo, la existencia de políticas de protección de datos, la gestión del riesgo para los derechos y libertades, la aplicación de medidas de protección de datos desde el diseño y por defecto, la aplicación de medidas de seguridad orientadas a la protección de datos con relación a la confidencialidad, integridad, disponibilidad y resiliencia, la existencia de procedimientos para gestionar correctamente las brechas de datos personales, si se ha nombrado un delegado de protección de datos, la adecuación a los requisitos de transferencias internacionales de datos, etc. (Agencia Española de Protección de Datos Personales, 2022)

### 7.2 Análisis de factores legales y regulatorios

La revisión de los factores legales y regulatorios abarca leyes nacionales y locales o acuerdos internacionales, así como en la regulación secundaria (INAI, 2015). Por ejemplo, dentro de que desarrolla aplicaciones de Telesalud el giro de negocio está enfocado en crear soluciones tecnológicas para el sector sanitario. Sin embargo, es obligatorio ajustar el accionar de la empresa con la Ley de protección de datos personales. Debido a esto, hacemos referencia a Valpuesta y Hernández (2021), quienes indican que existen tres principios medulares: licitud, lealtad y transparencia, mismos que concuerdan con el Artículo 7 de la Ley Orgánica de Protección de Datos Personales.

Es necesario manifestar que, en cuanto al establecimiento de una política de protección de datos personales dentro de una organización, de acuerdo con la Ley Orgánica de Protección de Datos, son los responsables del tratamiento quienes tienen como obligación legal implementar esta clase de políticas (Asamblea Nacional del Ecuador, 2021).

En ese sentido, el tratamiento sería lícito si la finalidad de este es la prestación de la asistencia sanitaria y se refiere únicamente a datos personales que el interesado haya aportado, o que se utilicen dentro de esa relación, por ejemplo, el número de teléfono (Agencia Española de Protección de Datos Personales, 2022).

La Ley Orgánica de Protección de Datos Personales regula como derechos de los titulares el obtener confirmación de si los datos están siendo o no objeto de tratamiento (Art. 12 inciso final LOPDP) y, en caso afirmativo, el acceder a ellos. Asimismo, regula los derechos de rectificación, supresión, oposición, limitación del tratamiento, portabilidad y el derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles (Asamblea Nacional del Ecuador, 2021).

Sin embargo, en el ámbito sanitario, estos derechos se concretan en relación con la historia clínica[7], que consta como un derecho en la Ley Orgánica de Salud (Art.7 literal F) (Asamblea Nacional del Ecuador, 2006), además del derecho a la confidencialidad y la información de la Ley de Derechos y Amparo al Paciente (Arts. 4 y 5), y que, por tanto, pueden ser objeto de algunas limitaciones (como la posibilidad de rectificar o suprimir datos de la historia clínica); y otros tendrán escasa aplicación (como el derecho de oposición[8]) (Agencia Española de Protección de Datos Personales, 2022).

En general, estas limitaciones son consecuencia de la Ley Orgánica de Salud y la Ley de Derechos y Amparo al Paciente, que obliga a conservar toda la información necesaria para conocer el estado de salud del paciente con el fin de garantizar la asistencia sanitaria. Lo que implica que dichos derechos pueden limitarse o modularse conforme a los criterios de los profesionales sanitarios que permitan garantizar la finalidad de ser necesarios para una adecuada asistencia sanitaria a los pacientes.

### 7.3 Análisis de acuerdo con el modelo de negocio

Es necesario definir las características específicas de la estrategia de negocio, las cuales varían de una organización a otra (INAI, 2015) y se encuentran, por ejemplo, en guías, códigos de conducta o mejores prácticas de un sector como el de salud. A lo largo de nuestra vida, todos somos usuarios del sistema sanitario; es decir, nuestros datos más sensibles van a ser tratados por médicos, personal sanitario, centros de salud, hospitales o terceros de confianza, como en el caso de la empresa que desarrolla soluciones tecnológicas para el sector sanitario (Agencia Española de Protección de Datos Personales, 2019).

---

[7] Tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida y a que se le entregue su epicrisis (Asamblea Nacional del Ecuador, 2006).

[8] El derecho de oposición está pensado fundamentalmente para defenderse de las comunicaciones comerciales, de acuerdo con el Art. 16 de la LOPDP (Asamblea Nacional del Ecuador, 2021).

### 7.4 Análisis de acuerdo con la realidad tecnológica actual

Se requiere, además, el entendimiento de la organización entre las tecnologías que se utilizan, y su tratamiento de datos personales (INAI, 2015). En el caso de la empresa, la utilización de tecnologías disruptivas es parte del modelo de negocio, sobre todo en lo que tiene que ver con capacidades de aprendizaje profundo e inteligencia aplicada artificialmente al mejoramiento del estilo de vida de los pacientes, a través de modelos de pronóstico generados mediante el tratamiento de una gran cantidad de datos (Fernández, 2022).

### 7.5 Resultados del análisis de los puntos anteriores

Luego del análisis de los puntos anteriores de esta sección podemos definir el alcance y el objetivo de la política de protección de datos personales para la aplicaciones de telesalud que desarrolla la empresa estudiada.

El alcance de la política será la creación de un marco normativo alineado con la Ley Orgánica de Protección de Datos Personales del Ecuador, que defina un modo de actuar, efectivo, práctico y ejecutivo, que permita establecer los procesos y mecanismos de tratamiento para la protección de datos personales a lo largo de todo su ciclo de vida dentro de los productos y servicios que brinda la compañía, especialmente en aplicaciones de salud móvil, garantizando los derechos y libertades de los titulares (Agencia Española de Protección de Datos Personales, 2021).

El objetivo de la política es cumplir con los derechos ARCO-PLUS[9] en el tratamiento de datos personales de salud.

[9] Derechos, de Información, Acceso, Rectificación, Actualización, Eliminación, Oposición, Portabilidad, Limitación, Suspensión, y a no ser objeto de decisiones automatizadas. (Asamblea Nacional del Ecuador, 2021)

## 8. Describir las Funciones y Obligaciones de los responsables y los encargados del tratamiento

### 8.1 Definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional para la aplicación de la política

De acuerdo con la Ley Orgánica de Protección de Datos Personales, en su Artículo 5 se mencionan a los integrantes del sistema de protección de datos personales, cada uno de los cuales tiene un rol particular dentro del modelo de negocio de que desarrolla aplicaciones de Telesalud.

En primer lugar, hablaremos del rol de encargado del tratamiento, ya que la compañía funge como tercero con el que se contrata la prestación de un servicio que conlleva tratamiento de datos personales. Por eso se denomina “encargado del tratamiento”, y tiene la obligación de ser diligente en seleccionar un encargado que ofrezca las condiciones necesarias para las garantías de cumplimiento (Agencia Española de Protección de Datos Personales, 2022).

El criterio relevante para determinar quién es responsable o corresponsable del tratamiento es el de identificar quién toma las decisiones sobre los fines y los medios de este (Agencia Española de Protección de Datos Personales, 2022).

A continuación, desglosamos los diferentes roles dentro del ecosistema de protección de datos personales con sus respectivas responsabilidades y su cadena de rendición de cuentas:

#### *8.1.1 Sobre el Titular de los Datos Personales*

El Titular es la persona natural cuyos datos son objetos del tratamiento; por tanto, cuenta con derechos y libertades como Titular frente al banco de datos, al responsable y al encargado del tratamiento.

##### *8.1.1.1 Rendición de cuentas del Titular de los datos*

El titular no debe rendir cuentas. Por el contrario, este tiene la potestad de exigir los derechos de acceso, información, rectificación, cancelación y oposición.

Dentro de la realidad de la empresa que desarrolla aplicaciones de Telesalud, los datos personales se reciben por medio del responsable de su tratamiento, y su recogida debe tener fines determinados, explícitos y legítimos.

### *8.1.2 Sobre el Responsable del Tratamiento*

Es la persona natural o jurídica que determina los fines y medios del tratamiento del dato; por tanto, es quien ejerce control sobre las decisiones, incluyendo las de delegarlas a un encargado. No obstante, el responsable del tratamiento no se libra de su obligación frente al titular por el hecho de delegar el tratamiento a un encargado.

Este puede ser tanto una entidad pública (hospital o centro de salud público) como privada (hospital/clínica), o un profesional a título individual.

El facultativo de la salud, cuando realiza su actividad asistencial, no necesita pedir el consentimiento del paciente para tratar sus datos personales. Es así porque, aunque la regla general que establece la LOPDP es que está prohibido, entre otros, el tratamiento de datos personales de salud, de datos genéticos y de datos biométricos, se establece como excepción el caso de la asistencia sanitaria, como dispone el Art. 31 numeral 1 de la LOPDP (Abellán-García; García, 2020).

Las personas físicas responsables del tratamiento deben ser profesionales de la salud sujetos a la obligación de secreto profesional. Se deberá pedir el consentimiento, por ejemplo, en el caso de que el odontólogo o el fisioterapeuta requieran enviar publicidad.

Por ello, el Responsable del Tratamiento de datos será el encargado de suministrar instrucciones a sus empleados sobre cómo debe actuar en relación con la historia clínica, la cumplimentación de esta, la determinación de las medidas de seguridad a seguir o qué hacer si los pacientes solicitan el ejercicio de uno de los derechos ARCO-PLUS, entre otras cuestiones.

#### *8.1.2.1 Rendición de cuentas del Responsable del Tratamiento.*

En el sector sanitario público y privado, se reciben los datos del paciente y se debe cumplir con la responsabilidad de garantizar al Titular, en todo

momento, el pleno y efectivo ejercicio de sus derechos ARCO-PLUS, así como las libertades consagradas en la Ley.

Como parte de la rendición de cuentas, es imprescindible determinar las obligaciones de los Responsables del Tratamiento, de acuerdo con el marco legal expuesto en la LOPDP. En este caso, el Responsable debe rendir cuentas a la Autoridad de Datos Personales.

### *8.1.3 Sobre el Encargado del Tratamiento*

Es la persona natural o jurídica la que se encarga de tratar el dato por cuenta del responsable del Dato. La empresa que desarrolla aplicaciones de Telesalud actúa en este ecosistema como un tercero de confianza.

La dicha empresa a su vez también es la encargada de un responsable (hospitales, centros médicos) con relación a los tratamientos en la sanidad pública o privada, cuando ha sido contratada para llevar a cabo dichas obligaciones de forma específica.

#### *8.1.3.1 Rendición de cuentas del Encargado del Tratamiento*

El encargado debe responderle al responsable del tratamiento, al titular de los datos y a la Autoridad de Datos Personales.

### *8.1.4 Sobre el Delegado de Protección de Datos Personales*

La designación de un Delegado de Protección de Datos Personales (DPD) es obligatoria cuando el tratamiento de los datos lo lleve a cabo una autoridad u organismo público, de acuerdo con el Art. 48 de la LOPDP en concordancia con el Art. 225 de la Constitución.

El DPO será una persona que cuente con la experticia en las áreas jurídicas, de gestión y técnico/científicos necesarios para explicar, ilustrar y supervisar al responsable en el cumplimiento de la normativa de protección de datos de salud y de los tratamientos concretos que se lleven a cabo (Agencia Española de Protección de Datos Personales, 2022).

El DPO ha de estar dotado con los recursos necesarios para ejecutar con eficacia sus funciones.

#### *8.1.4.1 Rendición de cuentas del Delegado de Protección de Datos Personales*

Los Responsables de los centros sanitarios públicos respaldarán al DPD en el desempeño de las funciones que tiene asignada, facilitarán los recursos necesarios para ejercer sin problemas su competencia, de igual forma se facilitará el acceso a los datos personales y a las operaciones de tratamiento, y garantizarán que informe al más alto nivel de la organización y la formación necesaria para el mantenimiento de sus conocimientos especializados (Agencia Española de Protección de Datos Personales, 2022).

El Responsable deberá velar y adoptar las medidas adecuadas para que el DPD ejerza sus funciones en ausencia de conflictos de intereses y con total independencia.

El Responsable no podrá despedir ni sancionar al DPD por el ejercicio de sus funciones.

## 9. Elaborar un inventario de los datos personales

### 9.1 Definir el ciclo de vida de los Datos Personales


*Ilustración 1: Ciclo de Vida del Dato Personal*

Los datos de salud siempre han sido una valiosa fuente de conocimientos en el ámbito de la asistencia sanitaria. Por ello, es importante conocer el flujo de los datos personales e identificarlo, definirlo y documentarlo a través de los

diferentes procesos de la empresa que desarrolla aplicaciones de Telesalud, la cual permite conocer cómo se realiza el tratamiento al que son sometidos. Se conoce como el ciclo de vida del dato al siguiente proceso:

- **Obtención o captura:** La obtención de los datos implica toda actividad de captura de datos personales que tiene como fin actividades de tratamiento. Esa captura de información puede provenir del propio Titular de los datos, o de terceros que realicen cesiones o comunicaciones (Agencia de Acceso a la Información Pública, 2020).
- **Almacenamiento y Categorización:** El almacenamiento de datos personales consiste en la conservación de información empleando una tecnología que permita garantizar la seguridad y confidencialidad de estos, para que se encuentren accesibles siempre que sean necesarios. Por otro lado, la categorización implica toda actividad de clasificación de la información, incorporándose en distintas categorías (especiales o estándar) definidas por el tipo de dato y su finalidad. También refiere a la determinación de los potenciales vínculos de los datos capturados con otros datos, preexistentes o no, a efectos de obtener inferencias, por ello es necesario realizar una lista que describa lo siguiente: (Agencia de Acceso a la Información Pública, 2020).
    a. Uso y explotación de los datos:
        i. Acceso
        ii. Manejo
        iii. Aprovechamiento
        iv. Monitoreo
        v. Procesamiento (incluidos los sistemas físicos y/o electrónicos que se utilizan para este fin)
- **Divulgación**: La divulgación comprende remisiones, cesiones y transferencias. La remisión de los datos personales puede suceder, por ejemplo, del Responsable al Encargado del Tratamiento. Por otro lado, la cesión se refiere a toda revelación o envío de datos personales a personas distintas del Titular, en el marco del tratamiento legítimo de los

datos personales. Por su parte, la transferencia internacional es aquella cesión o comunicación que tiene como destinatario un responsable de tratamiento ubicado en el extranjero.

- **Bloqueo**: Se trata de no permitir el acceso al Dato Personal por orden de la autoridad competente, o por el Responsable del Tratamiento en caso de que pudiese ocasionar un daño al Titular. Por ejemplo, el médico siquiatra sobre el diagnóstico de su paciente.
- **Cancelación, eliminación o destrucción:** El hecho de que se conserve la información no significa que esta deba permanecer en poder del Responsable o Encargado de forma indefinida. Salvo excepciones, una vez cumplida la finalidad para la que se obtuvo la información, corresponde proceder a su eliminación (Art. 15 LOPD). Asimismo, no se considera válida aquella finalidad que justifica la conservación de datos personales a perpetuidad o por lapsos desproporcionados de tiempo. Por esta razón, el responsable debe eliminar la información de manera periódica, en plazos cuya razonabilidad ha de determinarse conforme a la naturaleza de los datos y la finalidad del tratamiento (Agencia de Acceso a la Información Pública, 2020).

Es importante documentar el ciclo de vida de los datos personales por parte del responsable del tratamiento, sobre todo la trazabilidad de los datos personales, lo que puede definirse como el proceso mediante el cual se permite conocer todas las etapas, ubicaciones o cambios por los que han pasado estos en el contexto de una actividad de tratamiento (PRIDATEC S.L., 2019). El ciclo tiene dos funciones. La primera es una función práctica, que consiste en informar a la organización de las categorías de datos personales que trata, para obtener una gestión más eficiente y adecuada de estas categorías. Seguidamente, esa información constará como parte de lo que se conoce en la legislación nacional como Registro Nacional de Datos Personales (Art. 51 LOPDP) y a nivel del RGPD como Registro de Actividades de Tratamiento o RAT (Art. 30), donde se hará constar el origen de los datos, la finalidad para la que se recaban, el nombre del Responsable, del Encargado, dónde se almacenan, qué terceros acceden a

la información y finalmente, cómo se procede con la destrucción de la información.

Un inventario de datos personales debe contener:[10]

1. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen o capturan los datos personales.
2. Las finalidades de cada tratamiento de datos personales.
3. El catálogo de los tipos de datos personales que se tratan, indicando si son estándar o de categorías especiales, como los datos sensibles, datos de salud, datos de niñas, niños y adolescentes, datos de personas con discapacidad y de sus sustitutos (Art. 25 LOPDP).
4. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.
5. La lista de los responsables y encargados que tienen acceso a los sistemas de tratamiento.
6. El nombre completo, denominación o razón social del responsable y del encargado del tratamiento.
7. El instrumento jurídico que formaliza la prestación de los servicios que brinda el encargado al responsable.
8. Los destinatarios o terceros receptores de las transferencias o remisiones que se efectúen, así como las finalidades que justifican las mismas.

## 10. Realizar un Análisis de Riesgo de Datos Personales

Para realizar este trabajo de investigación se realizó el análisis de los riesgos de las aplicaciones que desarrolla la empresa, ya que son los usuarios

[10] Lista creada a partir de la guía para la implementación de un sistema de protección de datos personales propuesto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, 2015).

de estas quienes se ven expuestos al riesgo de sus derechos y libertades. Las aplicaciones son:

1. SMC 2.0
2. Firma Digital
3. PROMS

Todas las operaciones de tratamiento de datos personales implican un riesgo para las personas cuyos datos son tratados. En particular si son datos sensibles como los de salud, ya que el obtener una marca negativa por afectación a la confidencialidad, integridad y disponibilidad de esta categoría especial de datos, puede resultar en un mayor impacto contra los derechos y libertades de los titulares, y no puede ser tolerada o aceptada por la organización ya que no es un riesgo menor (Agencia Española de Protección de Datos Personales, 2021).

Como parte de la analítica para el procesamiento sobre la gestión de riesgos, la política de que desarrolla aplicaciones de Telesalud se basará en la normativa ISO 31000 que se ha plasmado dentro de la metodología MAGERIT. Esta metodología establece un marco de trabajo para que las empresas tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

### 10.1 Definir las características del riesgo de acuerdo con el impacto que puede tener en la empresa

No existe manera de proteger los datos al cien por ciento, tanto los datos automatizados como los no automatizados. Por ello, el análisis y gestión de riesgos se constituye como un parámetro necesario para una mejora constante en el tratamiento de datos.

Para esto, se debe tener en cuenta la naturaleza, el alcance, el contexto y los fines con que se realiza el tratamiento de los datos (Agencia Española de Protección de Datos Personales, 2022).

Dentro del ámbito de la salud, no existe un mínimo de tolerancia. Los impactos que pueden surgir en cuanto a una brecha de seguridad o a los riesgos en su tratamiento dependen de la tipología, y pueden clasificarse, de acuerdo con los parámetros de la Agencia Española de Protección de Datos Personales (2021), según su nivel de compromiso con la:

1) Confidencialidad
2) Disponibilidad
3) Integridad

Cuando hablamos de riesgo o compromiso de la confidencialidad nos referimos casos como la suplantación de identidad de un Titular de datos personales, que permite acceder ilícitamente a los mismos y generar alteraciones afectando su integridad, o impidiendo que el Titular legítimo pueda acceder a los datos, afectando así a la disponibilidad. Para la empresa que desarrolla aplicaciones de Telesalud, este riesgo se considera alto debido a que los datos personales de salud se catalogan como datos sensibles, y si su información sufre cualquier tipo de alteración, puede afectar gravemente al paciente. Por ello, es necesario realizar una evaluación de impacto en este caso.

Con respecto a la disponibilidad, es necesario mencionar la accesibilidad y usabilidad sobre la propiedad de un activo. Dentro de este campo, es inminente determinar si la empresa cuenta con el procedimiento adecuado para realizar copias de seguridad y gestionar las mismas. Esta copia de seguridad será parte del plan de contingencia que la empresa establece para la información o datos personales que se encuentran en tratamiento, en caso de la generación de un riesgo de disponibilidad. De igual forma, con el fin de minimizar los riesgos, que desarrolla aplicaciones de Telesalud necesita adoptar en los tratamientos y en su implementación las medidas y garantías que sean necesarias y proporcionales a dichos riesgos, descritos brevemente en los acápites anteriores. En particular, debe implementar políticas de protección de datos como la que estamos proponiendo, así como medidas organizativas, de protección de datos desde el diseño y por defecto, así como también medidas

de seguridad de la información (Agencia Española de Protección de Datos Personales, 2022).

### 10.2 Definir los criterios de impacto con relación al daño y al perjuicio al Titular de los Datos Personales

La empresa que desarrolla aplicaciones de Telesalud tiene como fin conseguir que el tratamiento cumpla los requisitos de la LOPDP, garantizando y pudiendo demostrar la protección de los derechos de los interesados. Por lo que la empresa, en su afán de alinearse, desarrolla una política de protección que incluya la gestión del riesgo y evaluación de impacto en tratamientos de datos personales.

El que la empresa decida no contar con medidas de seguridad óptimas en sus sistemas de tratamiento de datos sensibles, sería considerado por la ley como una infracción grave para el Encargado de la Protección de Datos Personales, ya que estaría causando un daño inmediato para los Titulares, y afectaría sus derechos y libertades, garantizadas en la Ley (Art.70.4 LOPDP).

### 10.3 Definir los criterios de aceptación con relación al daño a la empresa

A nivel operativo, es esencial que la organización incluya en su modelo de gestión a un responsable sobre la elaboración, celebración y ejecución de los Avisos de Privacidad, para detectar si el concepto de brecha sucede por la falta de cumplimiento y regulación de los protocolos.

Los criterios de aceptación de brechas de seguridad en la protección de datos personales deben cumplir con los estándares de calidad establecidos por la Ley Orgánica de Protección de Datos Personales. Esto significa que dicha aceptación debe basarse en el uso de procesos, protocolos y herramientas diseñadas para detectar, analizar y corregir problemas de seguridad (Jones & Kosa, 2019). Estos criterios deben ser establecidos de forma clara y transparente para garantizar que se limiten al máximo las posibles brechas de seguridad.

Además, estos deben ser revisados periódicamente para asegurar que se adecuen al cambiante entorno tecnológico (Wood et al., 2017).

## 11. Estudio de Campo y Propuesta de solución al problema

Una vez que se han definido los conceptos básicos para la creación de la Política de Protección de Datos de la empresa, procedemos a describir el estado de situación de esta en cuanto al manejo y tratamiento de los datos personales que se utilizan como parte del giro de negocio.

Durante nuestro estudio de campo, nuestro objetivo fue recolectar la información fidedigna de los responsables y encargados del tratamiento de la información. Es por esto por lo que como parte de los procesos para el levantamiento de información contamos con:

a. **Encuesta para el cumplimiento de la Ley de Protección de Datos Personales Anexo 1**: Se utilizó una serie de tablas basadas en la LOPDP, que pueden ser manejadas como un método básico que nos permitió identificar los requisitos de cumplimiento de la LOPDP, en este caso, para mostrarnos la situación de la empresa que desarrolla aplicaciones de Telesalud con el objeto de poder valorar los aspectos sobre el consentimiento, la base legitimadora, los derechos ARCO-PLUS y las libertades. Además, estas se deben tener en cuenta durante los procesos de análisis de riesgos y evaluación de impacto, de forma que se puedan implantar los controles necesarios a fin de garantizar la proactividad que la LOPDP exige a los antes mencionados Responsables y Encargados del Tratamiento (Agencia Española de Protección de Datos Personales, 2019).
b. **Inventario de datos personales dentro del ecosistema que maneja la empresa Anexo 2**.
c. **Necesidad de una Evaluación de Impacto y el análisis del riesgo inherente Anexo 3**.
d. **Consentimiento Informado del tratamiento de datos personales Anexo 4**.

e. **Política de Protección de Datos Personales Anexo 5**.

Al recabar la información descrita anteriormente, obtuvimos los insumos necesarios para construir la propuesta de solución. En este caso, la redacción de la política correspondiente a la medida de las necesidades regulatorias actuales, así como los estándares internacionales en protección de datos personales y seguridad de la información.

En nuestro estudio de campo pudimos observar que la empresa realiza el análisis y la validación de las aplicaciones para garantizar la calidad y el rendimiento de estas (SMC 2.0, Firma Digital, PROMS), luego se realizan pruebas con herramientas automatizadas para detectar vulnerabilidades y errores de código, en la empresa se hace esto por más de siete años de acuerdo con el gerente general.

Las herramientas automatizadas de análisis de código fuente (ACFA) son herramientas de detección de vulnerabilidades que pueden escanear y analizar el código fuente para detectar errores potenciales. Estas herramientas suelen usar técnicas como el análisis estático para identificar posibles fallos en la arquitectura y el diseño de la aplicación, además de errores de lógica y programación (Netz & Schäppi, 2020). Estas herramientas automatizadas proporcionan al equipo de programadores de la empresa información precisa y oportuna sobre las vulnerabilidades en el código para que puedan mitigarlo antes de que se produzcan incidentes, tomando en consideración la seguridad por defecto y por diseño, al igual que la privacidad de los usuarios.

La política comienza definiendo los alcances de esta y su objetivo principal. Después de esto, se hace alusión a las definiciones que utiliza la LOPDP en el Art. 4. Posteriormente, se hace una referencia a los principios de protección de datos personales descritos en el Art. 10 de la LOPDP, dentro de los cuales destacan los que tienen relación directa con el giro de negocio de que desarrolla aplicaciones de Telesalud.

Los principios a los que se hace referencia tienen relación directa con las aplicaciones *eHealth* que la empresa desarrolla; en especial, la protección por

diseño y por defecto que menciona la LOPDP. También se hace énfasis en el consentimiento libre, específico, informado e inequívoco que debe ser recabado de los Titulares previo a cualquier tratamiento de datos personales.

En este mismo orden de ideas, se hace referencia a las otras bases legitimadoras como son el cumplimiento de los contratos, las obligaciones legales, el interés vital y el interés legítimo.

Se debe recalcar que la empresa que desarrolla aplicaciones de Telesalud trata los datos personales de forma lícita, leal y transparente, principio que es desarrollado íntegramente en la Política. Subsiguientemente, se determina las finalidades de forma explícita de cada una de las herramientas desarrolladas por la empresa, SMC 2.0, la herramienta de firma digital y la herramienta PROMS.

En consecuencia, a estas finalidades, se requiere de los interesados la exactitud de sus datos personales, en específico, los que tienen relación con la documentación clínica que describa la situación real de salud del paciente. También se hace énfasis en la minimización de datos personales que se adecuen a la necesidad y sean relevantes con las finalidades previstas en las bases legitimadoras.

Otro de los puntos de la política hace referencia a la integridad y confidencialidad de los datos personales, así como a las medidas de seguridad por posibles violaciones, accesos no autorizados, accesos ilícitos y toda comunicación que no cuente con el consentimiento informado del interesado, reconociendo así el principio de responsabilidad proactiva o rendición de cuentas dentro de la política. Por lo tanto, la empresa debe ser capaz de demostrarlo cuando sea requerido por la autoridad competente.

En el apartado 4 de la Política se especifican los derechos del Titular de los datos, como, por ejemplo, el derecho a ser informado. También es parte de la política el ejercicio de los derechos ARCOPLUS.

Finalmente, se determina el contenido del Aviso de Privacidad que se desplegará en las aplicaciones de telesalud desarrolladas por la empresa, luego

cuales son las partes interesadas, el Delegado de Protección de Datos Personales y la vigencia del instrumento.

El contenido detallado de la política se encuentra en el **Anexo 5**.

## 12. Conclusiones y recomendaciones

Una vez que se ha planteado a detalle el contenido y el proceso para la creación de la Política, es necesario establecer como parte de las conclusiones y recomendaciones de la empresa que es responsable de planear el proceso de implementación de la misma, el cual incluye la adopción de medidas de seguridad aplicables a los datos personales, la fase de monitoreo y revisión de la Política —en donde se debe plantear una evaluación y auditoría continua con respecto al registro pormenorizado de actividades del tratamiento de datos personales— y, por último, el planteamiento de mejoras a la política, en donde se realiza un planteamiento de mejora continua y capacitación a los involucrados en el manejo del ecosistema de datos de la empresa.

### 12.1 Conclusiones

La intimidad es el derecho a la privacidad individual, el derecho a estar solo. Esto implica que una persona tiene el derecho a gozar de su vida privada sin ser interferida por otros. La privacidad, por otro lado, es la capacidad de un individuo de mantener sus pensamientos, sentimientos y acciones dentro su entorno personal o profesional de manera confidencial, es por tanto una limitación del acceso y uso de la información del individuo. Y la protección de datos personales se refiere al derecho de autodeterminación informativa relativo a como nuestros datos se recopilan, procesan, almacenan y se comparten a partir de una base legitimadora que determina su finalidad con relación a su conservación y limitación de uso, que impone deberes y responsabilidades tanto a encargados, terceros como a los responsables del tratamiento.

La ciberseguridad debe ser entendida como la capacidad de la empresa para protegerse a sí mismas, a otras personas, a sus bienes, a sus activos de

información y demás servicios esenciales de su ciberentorno ante riesgos y amenazas que se identifican en el ciberespacio, y así propender a una cultura de paz y de seguridad humana integral, como menciona el Art. 393 de la Constitución del Ecuador

En nuestro estudio de campo pudimos verificar no obstante que, en una de las preguntas de la encuesta para evaluar el cumplimiento de la LOPDP, se contestó por parte de la empresa que desarrolla aplicaciones de Telesalud *a priori* que no mantiene la trazabilidad de los fines del tratamiento. Este tema quedó más claro al realizar el inventario de los datos personales tratados por la empresa, donde el poder de la trazabilidad la tienen las aplicaciones (SMC 2.0, Firma Digital y PROMS), junto con los Responsables y Encargados del tratamiento. Esta consiste en tener un control exhaustivo del proceso de tratamiento de los datos personales, controlando qué datos son tratados (descrito en el **Anexo 2**), quién interviene en el proceso de tratamiento de datos, qué terceros tienen acceso (**Anexo 5**) y qué sistemas están implicados (**Anexo 2**).

En relación con el retiro del consentimiento, pudimos constatar que no se trata de un caso frecuente, y es muy improbable que ocurra, tomando en cuenta que son consentimientos que pueden tener otra base legitimadora como el interés vital. Por otro lado, los interesados siempre estarán ávidos en recibir una atención sanitaria de calidad, y para ello se necesita su consentimiento para almacenar y tratar su información personal para construir su historia clínica para futuros diagnósticos.

En cuanto a la supresión de datos y el tiempo de conservación (plazo precautorio), se debe mencionar que el “Manual de Normas de Conservación de las Historias Clínicas y aplicación del Tarjetero Índice Automatizado", aprobado mediante Acuerdo Ministerial 00457 de 12 de diciembre de 2006, publicado en el Registro Oficial 436 de 12 de enero del 2007 dispone que las historias médicas se mantengan por un plazo de cinco años desde su ultima consulta, superado aquel plazo deberán ser trasladas al archivo pasivo de la institución sanitaria.

En cuanto a la portabilidad de datos personales, actualmente se está trabajando en una opción mediante un base de datos con seguridad criptográfica (*blockchain*), a través de monederos para almacenar claves criptográficas, y así poder obtener acceso ubicuo a la historia clínica de los interesados.

De acuerdo con el inventario de datos personales, los datos tratados por la empresa que desarrolla aplicaciones de Telesalud son de tres clases: Datos Personales Estándar (DPE), Datos Personales de Salud (DPS), y Datos Personales Financieros (DPF).

Todos los datos personales tratados por la empresa que desarrolla aplicaciones de Telesalud son almacenados en formato digital en medios de almacenamiento permanentes, como en servidores y discos duros, al igual que almacenamiento en la nube.

Dentro del Inventario de Datos Personales, se determinó la existencia de once actividades de tratamiento, que se describen a continuación:

| No. | Actividades de tratamiento | Aplicación |
|---|---|---|
| **1.** | Actividades de tratamiento con los usuarios del sistema SMC 2.0 | **Sistema SMC 2.0** |
| **2.** | Actividades de tratamiento con los pacientes SMC 2.0 | |
| **3.** | Historia clínica SMC 2.0 | |
| **4.** | Consentimiento informado SMC 2.0 | |
| **5.** | Estructuras SMC 2.0 | |
| **6.** | Formularios para el consentimiento informado SMC 2.0 | |
| **7.** | Tratamiento de la Firma Digital de los clientes | **Firma Digital** |
| **8.** | Tratamiento de los documentos con la firma digital de los clientes | |

| No. | Actividades de tratamiento | Aplicación |
|---|---|---|
| **9.** | Tratamiento del Agendamiento de los pacientes SMC 2.0 | **Sistema SMC 2.0** |
| **10.** | Tratamiento de los usuarios de PROMS | **PROMS** |
| **11.** | Tratamiento de los formularios de PROMS | |

*Tabla 4: Actividades de Tratamiento*

Una vez realizado el análisis de riesgos, se demuestra que existe un riesgo inherente medio en las actividades de tratamiento descritas en la tabla anterior, el cual debe ser tratado, para luego de realizar su mitigación y obtener un riesgo residual en las actividades de tratamiento de la empresa.

La gestión del riesgo en la protección de datos personales debe ser un proceso continuo que se basa en identificar y evaluar los riesgos asociados al tratamiento de datos, para luego implementar planes de acción para minimizarlos. Esta gestión debería incluir un análisis de riesgo inicial para identificar los peligros para cada actividad en el caso de la empresa, tiene que tomar en cuenta que los datos que trata son datos sensibles de salud, posteriormente debe realizar una evaluación periódica para mantenerse al día con el entorno cambiante. Una adecuada gestión del riesgo debe incluir la formación de todos los empleados de la empresa que estén directamente implicados en el tratamiento de datos, así como la evaluación y revisión de los protocolos existentes para asegurar que cumplen con la normativa de protección de datos personales.

Se verifica la existencia de un Sistema de Gestión de la Información en base a la normativa 27001:2012.

Como se puede apreciar en la Tabla 2, cada una de las fases fue cumplida realizando las diferentes actividades descritas, logrando, al final, entregar la Política de Protección de Datos personales de la empresa, que consta en el **Anexo 5** del presente trabajo de titulación.

La política de protección de datos personales realizada se aplica a todos los usuarios de la aplicaciones de Telesalud desarrolladas por la empresa. Esta

política establece los principios básicos para garantizar que los datos personales de los pacientes sean tratados de manera segura y confidencial. Esta política establece los siguientes principios: 1) Solo los trabajadores autorizados y profesionales de la salud tendrán acceso a los datos personales; 2) Los datos personales no se compartirán con terceros sin el consentimiento previo del titular; 3) Los datos personales no se procesarán por períodos más largos de lo necesario; 4) Se tomarán medidas adecuadas para garantizar la seguridad de los datos; 5) Los usuarios tienen derecho a solicitar una copia de sus datos personales; 6) Los usuarios tienen derecho a solicitar que se corrijan o eliminen sus datos personales de las aplicaciones.

**12.2 Recomendaciones.**

Recomendamos que la empresa que desarrolla aplicaciones de Telesalud realice una Evaluación de Impacto en tres categorías:

1. Historia clínica SMC 2.0
2. Consentimiento informado SMC 2.0
3. Formularios para el consentimiento informado SMC 2.0

Aconsejamos que la empresa tiene que revisar continuamente la Política de acuerdo con los nuevos desarrollos tecnológicos en los que incursione o en que se desenvuelva.

Se recomienda también actualizar los controles de la ISO 27001:2022 y la implementación complementaria de los controles de la ISO 27002 y la ISO 27701.

Recomendamos que esta política de protección de datos personales de las aplicaciones de telesalud debe ir acompañada de una fase de implementación, así como una fase de mejora continua, la cual incluye como ya lo mencionamos antes una etapa de capacitación, con el fin de que todos los usuarios dentro del organigrama corporativo, así como los clientes tengan un vasto cocimiento sobre el alcance y tratamiento de los datos personales de salud que se tratan mediante las aplicaciones de eHealth que desarrolla la empresa.

**Bibliografía**

Abellán-García, F.; García, A. (2020). *Protección de Datos Personales de Salud en el plano asistencial e investigación.* Madrid: Fundación Merck Salud. https://www.fundacionmercksalud.com/wp-content/uploads/2020/03/1.5.-PROTECCION-DE-DATOS-DE-SALUD.-Fernando-Abellan-Ana-Garcia.pdf

Agencia de Acceso a la Información Pública, Unidad Reguladora y de control de datos personales (2020). *Guía de Evaluación de Impacto de Datos Personales.* Montevideo: Publicaciones conjuntas URCDP y la AAIP.

Agencia EFE (2021, 12 de febrero). Ecuador se fija meta de alcanzar el 85% de población vacunada para fin de año. *Expreso*. https://www.expreso.ec/actualidad/ecuador-fija-meta-alcanzar-85-poblacion-vacunada-ano-116754.html

Agencia Española de Protección de Datos Personales (2018). *Decálogo para adaptación del RGPD a las políticas de privacidad de internet.* Madrid: Publicaciones AEPD.

Agencia Española de Protección de Datos Personales (2019). *Guía para pacientes y usuarios de la sanidad.* Madrid: Publicaciones AEPD.

Agencia Española de Protección de Datos Personales (2019). *Listado de Cumplimiento Normativo.* Madrid: AEPD. https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf

Agencia Española de Protección de Datos Personales (2021). *Gestión del riesgo y evaluación de impacto en tratamiento de datos personales.* Madrid: Publicaciones AEPD.

Agencia Española de Protección de Datos Personales (2022). *Guía de Profesionales del Sector Sanitario.* Madrid: Publicaciones AEPD.

Alvino, C. (2022, 18 de octubre). Estadísticas de la situación digital de Ecuador en el 2020-2021. *Branch.com*. https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/

Asamblea Constituyente del Ecuador. (2008). *Constitución del Ecuador.* Montecristi: Registro Oficial.

Asamblea Nacional del Ecuador. (2006). *Ley Orgánica de Salud.* Quito: Registro Oficial.

Asamblea Nacional del Ecuador (2021). *Ley Orgánica de Protección de Datos Personales.* Quito: Corporación de Estudios y Publicaciones.

Banco Mundial (2022, 28 de septiembre) Ecuador, panorama general. https://www.bancomundial.org/es/country/ecuador/overview#1

Bastidas, Y. (2020). Pandemia, Apps Móviles de Salud y Protección de Datos Personales. *Revista Iberoamericana de Derecho Informático (Segunda Época).* 93-106.

Castillo, J. (2021). *Diagnóstico del Sistema de Salud en el Ecuador.* Quito: Grupo Faro. Obtenido de https://grupofaro.org/wp-content/uploads/2022/11/Diagnostico-El-sistema-de-salud-en-Ecuador_compressed.pdf

Colaner, N. (2022, 13 de junio). The age of Big Data. *Linkedin.* https://www.linkedin.com/learning/ethics-and-law-in-data-analytics/the-age-of-big-data?trk=share_ios_video_learning&shareId=Kej6I+hITW2Zw7O9hwGl9w==

Comisión Económica para América Latina (CEPAL). (2020). *Agenda Digital para América Latina y el Caribe (eLAC2022).* Washington: CEPAL.

Comité Jurídico Interamericano (CJI). (2021). *Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones.* Washington: Organización de los Estados Americanos.

Del Alcázar, J. (16 de 04 de 2022). Aquí está tu informe: "Estado Digital Ecuador Abril 2022". *Mentinno.* https://www.mentinno.com/gracias-aqui-esta-tu-informe-estado-digital-ecuador-abril-2022/

Erazo, L (2022, 14 de junio). ¿Qué es una aplicación móvil? *An Incubator*. https://anincubator.com/que-es-una-aplicacion-movil/

European Union Agency for Fundamental Rights and Council of Europe (2018). *Handbook on European data protection law.* Luxembourg: Publications Office of the European Union. https://data.europa.eu/doi/10.2811/343461

Fernández, R. (2022). Inteligencia artificial y protección de la salud. En A. Madrid Parra, & L. Alvarado Herrera, *Derecho Digital y Nuevas Tecnologías* (pág. 1033). Pamplona: Aranzadi, S.A.U.

Fernández, R. (2022, 14 de febrero). Número de suscripciones de smartphones a nivel mundial desde 2016 hasta 2027 (en millones). *es.statista.com*. https://es.statista.com/estadisticas/636569/usuarios-de-telefonos-inteligentes-a-nivel-mundial/

Ferrer-Márquez, M., & Pardo, T. (2017). *La regulación de la privacidad en el derecho digital.* Madrid: Dykinson.

Ferrer, O. (2001). *Telemedicina.* Madrid: Editorial Médica Panamericana.

Geurts, C. (2021, 1 de octubre). Seminario internacional de protección de datos personales sobre la "Ley Orgánica de Protección de Datos: de la teoría a la práctica". *Delegation of the European Union to Ecuador.* https://www.eeas.europa.eu/delegations/ecuador/seminario-internacional-de-protecci%C3%B3n-de-datos-personales-sobre-la-%C2%ABley_en?s=161

González Álvarez, R. (2011). *Aproximaciones a los derechos humanos de cuarta generación.* México: SOPECJ. Obtenido de https://www.tendencias21.es/derecho/attachment/113651/#:~:text=Es%20conocido%20que%20para%20algunos,los%20pueblos%3B%20lo%20que%20en

Grupo de Trabajo en materia de protección de datos y privacidad. (2013). *Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes.* Bruselas: Comisión Europea - Dirección General de Justicia.

Jones, J. & Kosa, M. (2019). The role of IT in security analysis and incident response planning. International Journal of Computer Science and Information Security, 17(7), 141-145.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2015). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.* México: INAI.

Mariño, S.; Alfonzo, P. (2014). Implementación de SCRUM en el diseño del proyecto del Trabajo Final de Aplicación. *Scientia Et Technica*, 413 - 418.

Medinaceli, K. I. (2017). *El tratamiento de datos personales sanitarios en la historia clínica electrónica: caso boliviano.* Madrid: Agencia Española de protección de Datos y Agencia Estatal Boletín Oficial del Estado.

Molina Angarita, N. (2017). *Tratamiento de los datos personales según el reglamento (UE) 2016/679: El modelo colombiano.* (Vol. 18). Bogotá: Revista Digital Universitaria.

Netz, S., & Schäppi, B. (2020). Análisis de código fuente automatizado como herramienta de detección de vulnerabilidades. Skemantics, 1-11.

Organización Mundial de la Salud (2004). *Informe de la Secretaría sobre eHealth.* Washington: OMS. https://apps.who.int/iris/bitstream/handle/10665/20235/B115_39-en.pdf?sequence=1&isAllowed=y

Organización Mundial de la Salud (2011, 14 de Junio). *mHealth, New horizons for health through mobile technologies.* Ginebra: Organización Mundial de la Salud. https://apps.who.int/iris/bitstream/handle/10665/44607/9789241564250_eng.pdf?sequence=1&isAllowed=y

Organización Mundial de la Salud (2022, 6 de abril). Determinantes Sociales de la Salud en la Región de Las Américas. https://www.paho.org/salud-en-las-americas-2017/?post_t_es=determinantes-sociales-de-la-salud&lang=es#:~:text=La%20Organizaci%C3%B3n%20Mundial%20de%20la,la%20vida%20cotidiana%20(%201%20).

Organización Panamericana de la Salud (2016). *Marco de Implementación de un Servicio de Telemedicina.* Washington: OPS.

Organización Panamericana de la Salud (2018). *Manual para la elaboración de políticas y estrategias nacionales de calidad.* Washington: Organización Panamericana de la Salud. https://iris.paho.org/bitstream/handle/10665.2/49549/9789241565561_spa.pdf?sequence=1&isAllowed=y

Organización Panamericana de la Salud (2020, 17 de junio). La COVID-19 afectó el funcionamiento de los servicios de salud para enfermedades no transmisibles en las Américas. *Paho.org.* https://www.paho.org: https://www.paho.org/es/noticias/17-6-2020-covid-19-afecto-funcionamiento-servicios-salud-para-enfermedades-no#:~:text=Desde%20que%20comenz%C3%B3%20la%20pandemia,c%C3%A1ncer%2C%20enfermedades%20cardiovasculares%20y%20diabetes.

PRIDATEC S.L. (2019). *La Trazabilidad de los Datos Personales.* Madrid: PRIDATEC. www.pridatect.com

Redacción BBC News Mundo (2019, 19 de septiembre). Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano. *BBC*. https://www.bbc.com/mundo/noticias-america-latina-49721456

Redacción El Comercio (2019) Presupuesto de Salud en el Ecuador. Recuperado de https://www.elcomercio.com/tendencias/sociedad/presupuesto-salud-prevencion-ecuador-servicios.html

Redacción El universo com. (2022, 25 de mayo). Desempleo de Ecuador llegó al 4,7 % en abril del 2022, una reducción 'no significativa', reporta el INEC. *El Universo*. https://www.eluniverso.com/noticias/economia/desempleo-de-ecuador-llego-a-47-en-abril-del-2022-una-reduccion-no-significativa-reporta-el-inec-nota/

Redacción LA HORA. (09 de 06 de 2022). https://www.lahora.com.ec/. Obtenido de https://www.lahora.com.ec/pais/pobres-incremento-inflacion-impacto-economia-ecuador/#:~:text=Hasta%20189.000%20ecuatorianos%20pueden%20caer%20en%20la%20pobreza,consecuencia%20de%20la%20alta%20inflaci%C3%B3n%20junio%209%2C%202022

Valpuesta, E.; Hernández, J. (2021). *Principios Generales del Tratamiento de Datos. Tratado de Derecho Digital*. Madrid: Wolters Kluwer Legal & Regulatory España S.A.

Wood, D., Meiklejohn, S., Driscoll, K., & Malan, D. (2017). Toward a better understanding of breach detection criteria. IEEE Security and Privacy, 15(3), 8-11.

**Referencias**


- Acurio, S. (2019). *Derecho Penal Informático, Segunda Edición.* Quito, Pichincha: Editorial Española.
- Agencia Española de Protección de Datos. Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf
- Centre for Information Policy Leadership (2016). Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, CIPL GDPR Interpretation and Implementation Project, 21 December 2016. Disponible en: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf
- Conde Ruiz, C. (2020). Regulación de los datos personales en las legislaciones europeas: Desafíos y oportunidades. Revista Digital Universitaria, 21(1).
- Consejo de Europa. - Digital solutions to fight Covid 19. Disponible en: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c
- Grupo de Trabajo del Artículo 29 (2014). Statement on the role of a risk-based approaching data protection legal frameworks, WP 218, adoptado el 30 de mayo de 2014. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf
- Instituto Nacional de Ciberseguridad. Gestión de riesgos, Una guía de aproximación para el empresario. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf
- López-Pulles, R. (2010). Programa Nacional de Telemedicina y Telesalud del Ecuador. *Latin American Telehealth*, 286-301.
- Nahabetián Brunet, Laura: "Derechos Fundamentales para el gobierno de la información: protección de datos personales, acceso a la información

pública y seguridad de la información" Materiales del curso de Protección de Datos Personales dentro de la Maestría de Derecho Digital de la Universidad de las Américas.

- Nahabetián Brunet, Laura: Presentaciones y Clases magistrales, Materiales del curso de Protección de Datos Personales dentro de la Maestría de Derecho Digital de la Universidad de las Américas.
- Saigí-Rubió, F., Torrent-Sellens, J., Robles, N., Pérez Palaci, J. E., & Baena, M. I. (2021). *Estudio sobre telemedicina internacional en América Latina: motivaciones.* Washington: Banco Interamericano de Desarrollo BID.