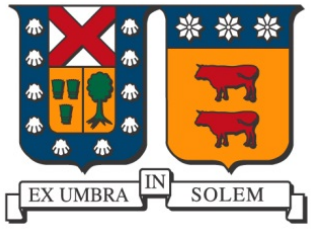
UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
SANTIAGO - CHILE



“DISEÑO DE POLÍTICA DE PRIVACIDAD AJUSTADA A REGULACIONES HIPAA PARA SISTEMA ORIENTADO AL TRATAMIENTO DE PACIENTES EN SECTOR SALUD”

LUIS ARTURO GONZÁLEZ ARISMENDI

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: Oscar Reyes Hevia
Profesor Correferente: Jose Luis Martí Lara

Agosto - 2024

RESUMEN

Resumen— El presente trabajo de título se enfoca en diseñar una política de privacidad para TechneWorks que cumpla con las leyes de privacidad y seguridad de datos en Chile, además de cumplir con la reglamentación HIPAA, con un enfoque centrado en el paciente. Los objetivos incluyen analizar las implicaciones de las leyes nacionales y la regulación HIPAA, asegurar el cumplimiento continuo de las normativas, desarrollar una política de seguridad de datos robusta y proponer un método de verificación periódica del cumplimiento de la política.

Se describe el proceso y análisis realizado para la implementación de una solución que pueda generar efectivamente una política de privacidad apalancando el uso de inteligencia artificial, específicamente *LLMs*. Esta contempla tanto el ambiente y datos que maneja la organización, como las regulaciones que debe cumplir.

Palabras Clave— Privacidad; HIPAA; Seguridad; Datos sensibles;LLM.

ABSTRACT

Abstract— The present thesis focuses on designing a privacy policy for TechneWorks that complies with data privacy and security laws in Chile, as well as with HIPAA regulations, with a patient-centered approach. The objectives include analyzing the implications of national laws and HIPAA regulations, ensuring ongoing compliance with these regulations, developing a robust data security policy, and proposing a method for periodic verification of the policy's compliance.

The process and analysis conducted for the implementation of a solution that can effectively generate a privacy policy leveraging the use of artificial intelligence, specifically LLMs, is described. This considers both the environment and data managed by the organization, as well as the regulations it must comply with.

Keywords— Privacy; HIPAA; Security; Sensitive Data;LLM.

GLOSARIO

HIPAA: La norma de confidencialidad de la Ley de Portabilidad y Responsabilidad de Seguros Médicos, o *Health Insurance Portability and Accountability Act of 1996.* por sus siglas en inglés.

GDPR: General Data Protection Regulation. Regulación Europea sobre el tratamiento de datos personales.

Derechos ARCOP: Derechos sobre los datos personales, específicamente derechos sobre Acceso, Rectificación, Cancelación, Oposición y Portabilidad.

Datos personales: Cualquier información que se relacione a un individuo vivo identificado o identificable. Por ejemplo: Nombre, apellido, dirección, número de identificación. [GDPR, 2022]

Datos sensibles: Datos personales que indiquen: origen étnico o racial, opiniones políticas, religión, participación en sindicatos, datos genéticos, datos biométricos, información relacionada a la salud, información relacionada a la vida sexual del individuo. [GDPR, 2022]

DPO: Delegado de Protección de Datos, o *Data Privacy Officer* por sus siglas en inglés.

AI: Acrónimo de *Artifical Intelligence* o Inteligencia Artificial.

LLM: Acrónimo de *Large Language Model* o Modelo de Lenguaje Grande.

Mapeo de datos: Proceso en el que se toma información de un sistema fuente y se hace coincidir los campos de este repositorio de información con campos de datos de otro sistema objetivo con el fin de tener una visión clara del flujo y la estructura de los datos.

Activo de datos: Recurso tecnológico de valor para una organización o empresa. El valor viene dado generalmente por la información que almacena, la cual puede ser:

- Datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios
- Bases de datos
- Dispositivos de red
- Equipos informáticos como servidores, computadores, tablets, celulares
- Las redes y sistemas que dan soporte a la comunicación de la organización
- Instalaciones donde se almacenan otros activos de información

ÍNDICE DE CONTENIDOS

RESUMEN II

ABSTRACT II

GLOSARIO III

ÍNDICE DE FIGURAS VII

ÍNDICE DE TABLAS VII

CAPÍTULO 1: INTRODUCCIÓN 1

CAPÍTULO 2: DEFINICIÓN DEL PROBLEMA 2
2.1 Contexto 2
2.2 Antecedentes 3
2.3 Identificación del problema 3
2.4 Objetivos 5
2.4.1 Objetivo General 5
2.4.2 Objetivos Específicos 5
2.5 Metodología 6
2.5.1 Fases de la Metodología Propuesta 6

CAPÍTULO 3: MARCO CONCEPTUAL 8
3.1 Definición de Política de Privacidad 8
3.2 Regulaciones Internacionales y Nacionales 9
3.2.1 Regulaciones Internacionales 10
3.2.2 Regulaciones Nacionales 10
3.2.3 Similitudes entre las Regulaciones 11
3.3 Principios de Privacidad de Datos 12
3.4 Desafíos en la Implementación de Políticas de Privacidad 13
3.5 Tecnologías de Protección de Datos 14
3.6 Gestión de Riesgos y Auditoría 15
3.7 Consideraciones Éticas 17
3.8 Definición de Sistema de Gestión de la Privacidad y Seguridad de la Información 18
3.9 Estado del Arte 19
3.10 Uso de Inteligencia Artificial para Manejo de Datos Sensibles 21
3.11 Tipos de datos contemplados por la regulación HIPAA 21
3.12 Entidades designadas para trabajar con datos PHI 22

CAPÍTULO 4: PROPUESTA DE SOLUCIÓN 23
4.1 Alcance de la Solución Propuesta 23

4.2 Desarrollo Mediante Marco de Trabajo con Open Source Intelligence 24
4.3 Delimitación de Datos Personales 26
4.4 Procesos de Recolección y Tratamiento de Datos de Kinteractive 26
4.4.1 Recolección de datos personales del paciente 27
4.4.2 Recolección de datos médicos del paciente 27
4.4.3 Recolección de datos financieros del paciente 27
4.5 Derechos de los Usuarios y Procedimientos de Ejercicio 27
4.6 Uso de Generative AI 31
4.7 Diagrama de flujo 33
4.8 Implementación propuesta 33
4.9 Proceso de análisis de información y datos personales 34
4.9.1 Recolección de datos 36
4.9.2 Mapeo de Datos 36
4.9.3 Enmascaramiento de Datos 36
4.9.4 Análisis de los datos con uso de inteligencia artificial 37
4.9.5 Adaptar Respuesta 38
4.9.6 Monitoreo y Mejora Continua 39
4.10 Flujo de trabajo del sistema de gestión 40
4.10.1 Selección y análisis de las regulaciones 40
4.10.2 Definición y extracción de datos considerados 41
4.10.3 Selección de Repositorios de Datos 42
4.10.4 Descubrimiento de datos sensibles en los repositorios 42
4.10.5 Generar la propuesta de política de privacidad 43
4.11 Ciclo de Vida de los Datos 44
4.11.1 Creación 44
4.11.2 Almacenado 44
4.11.3 Uso 45
4.11.4 Archivado 45
4.11.5 Destrucción 46
4.12 Cultura Organizacional 46

CAPÍTULO 5: VALIDACIÓN DE LA SOLUCIÓN 49
5.1 Política De Privacidad De Techneworks Para El Tratamiento De Datos De Pacientes En El Sector Salud 49
5.2 Revisión de resultados para análisis de datos personales mediante el uso de inteligencia artificial 52
5.3 Revisión de resultados para análisis de puntos claves de las regulaciones . . . 57
5.3.1 Análisis de resultados para regulación HIPAA 58
5.3.2 Análisis de resultados para Ley 19.628 61
5.3.3 Análisis de resultados para Ley 20.584 63
5.3.4 Análisis de resultados para Ley 21.096 65
5.3.5 Resultados generales 67
5.4 Revisión de Sistema de Gestión 69
5.4.1 Proceso de mapeo de datos 72

5.5 Verificación periódica y cumplimiento de política de privacidad 77
5.5.1 Auditorías 78
5.6 Propuesta de mejoras a futuro 81

CAPÍTULO 6: CONCLUSIONES 83

Anexos 85

REFERENCIAS BIBLIOGRÁFICAS 92

ÍNDICE DE FIGURAS

1 Stakeholders map. Elaboración Propia 4

2 Árbol del problema. Elaboración Propia 5

3 Diagrama PPVM de Caso de Uso 5. Extraido de [Ghazinour, Kambiz *et al.*, 2009] 20

4 Componentes del sistema 23

5 Diagrama de bloques metodología OSINT 24

6 Tipos de datos asociados al paciente 27

7 Diagrama de flujo de proceso 34

8 Diagrama de las clases implementadas, sus atributos y relaciones 35

9 Fases del ciclo de vida de los datos [Scope, 2021] 44

10 Categorías de datos sensibles detectadas 56

11 Categorías de datos clasificadas erróneamente 57

12 Categorías de lineamientos e indicaciones generados para regulación HIPAA . . 61

13 Categorías de lineamientos e indicaciones generados para ley 19.628 63

14 Categorías de lineamientos e indicaciones generados para ley 20.584 65

15 Categorías de lineamientos e indicaciones generados para ley 21.096 67

16 Consolidado de las indicaciones generadas para las 4 regulaciones. (HIPAA, Ley 19.628, 20.584 y 21.096) 68

17 Implementación de la clase Tipo de Dato y sus atributos 70

18 Implementación de la clase Categoría de Dato y sus atributos 70

19 Implementación de la clase Activo de Datos y sus atributos 70

21 Implementación de la clase Regulación y sus atributos 71

20 Implementación de la clase Proceso GDPR y sus atributos 71

22 Implementación de la clase Política de Privacidad y sus atributos 71

ÍNDICE DE TABLAS

1 Tipos de datos sensibles detectados según los tres modelos. 53

2 Porcentaje de aciertos obtenidos por tipo de dato y columna por cada modelo. Incluye los resultados de los tres conjuntos de datos. 54

3 Capacidad de manejo de tokens de cada modelo 55

4 Requerimientos generados con modelo GPT-4o para cumplimiento con regulación HIPAA 60

5 Requerimientos generados con modelo GPT-4o para cumplimiento con Ley 19.628 62

6 Requerimientos generados con modelo GPT-4t para cumplimiento con Ley 20.584 64

7 Requerimientos generados con modelo GPT-4o para cumplimiento con Ley 21.096 66

8 Resultados obtenidos para análisis de las 4 regulaciones propuestas 67

9 Extracto de muestra de datos y coincidencias de análisis de datos sensibles con modelo GPT-4 86

10 Extracto de muestra de datos y coincidencias de análisis de datos sensibles con modelo GPT-4o 87

11 Extracto de muestra de datos y coincidencias de análisis de datos sensibles con modelo GPT-4t 88

12 Mapeo de resultados generados con la regulación HIPAA 89

13 Mapeo de resultados generados con la Ley 19.628 90

14 Mapeo de resultados generados con la Ley 20.584 91

CAPÍTULO 1
INTRODUCCIÓN

En el ámbito de la ingeniería civil informática, el tratamiento de datos en el sector de la salud constituye un área de interés crítico debido a la sensibilidad y la confidencialidad de la información médica. En este contexto, la privacidad y la seguridad de los datos se convierten en pilares fundamentales para garantizar la confianza de los pacientes y cumplir con las regulaciones establecidas por las leyes nacionales e internacionales.

La presente investigación se centra en la elaboración de una política de privacidad ajustada a las normativas chilenas y a la regulación HIPAA (Health Insurance Portability and Accountability Act) de Estados Unidos, destinada a TechneWorks, una organización dedicada al desarrollo de sistemas orientados al tratamiento de pacientes en el sector salud.

Se busca confeccionar una guía integral para el diseño, implementación y evaluación de una política de privacidad ajustada a las regulaciones HIPAA y a las leyes de privacidad y seguridad de datos en Chile, con un enfoque centrado en el paciente y orientado a garantizar la confidencialidad y seguridad de la información en el sector de la salud.

Se mostrará en detalle el diseño e implementación de un sistema de gestión que permitirá obtener información del ambiente de datos de la organización y de las regulaciones con las que debe cumplir mediante modelos de inteligencia artificial, *LLMs*. Con dicha información, se generará una serie de lineamientos y prácticas para la organización que permitirá llevar monitoreo continuo sobre los datos sensibles que manejan para garantizar la seguridad y privacidad de la información del paciente.

CAPÍTULO 2
DEFINICIÓN DEL PROBLEMA

2.1. Contexto

Actualmente la privacidad de datos es un factor principal a considerar en sistemas y aplicaciones de carácter médico que almacenan y usan información de sus pacientes. Existen leyes a nivel nacional (Ley 21096 [MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, 2018], Ley 19628 [MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, 2020]) que buscan proteger a los ciudadanos y su privacidad, estas mencionan aspectos fundamentales de la privacidad de datos como lo es: la recolección de los datos, el manejo de estos y solicitar consentimiento, entre otros.

Por otra parte, la regulación HIPAA creada e implementada en Estados Unidos, busca proteger específicamente la información sensible, privada y médica de pacientes que manejan empresas como aseguradores, proveedores de salud, centros médicos y similares [HIPAA Journal, 2022]. Para maximizar la privacidad, esta regulación busca dar al paciente la libertad de elegir que datos pueden ser usados, con que fines, y por qué entidades. Considera la necesidad de políticas robustas para tratamiento de datos, salvaguardar la información almacenada y hace responsables a quienes manejan esta información en caso de alguna fuga de datos.

A pesar de los mecanismos mencionados, las fugas de datos médicos son un problema que ha afectado al menos a 157 millones de usuarios en Estados Unidos entre 2015-2019 y también es un problema que actualmente se ve en mayor proporción en instituciones de carácter médico [Seh, Adil Hussain *et al.*, 2020].

Teniendo en cuenta lo anterior mencionado, la organización para la cual se diseña esta política de privacidad requiere que la información se trate con de manera transparente hacia el paciente y que siga los lineamientos propuestos por las regulaciones nacionales y por la regulación HIPAA. La política de privacidad tomará en cuenta el proyecto Kinteractive de TechneWorks, el cual fue desarrollado como un producto de la 30ma Feria de Software del Departamento de Informática de la Universidad Técnica Federico Santa María.

La organización desarrolló una aplicación orientada a la terapia kinesiológica de manera remota, también conocido como telemedicina, usando reconocimiento de imágenes y video del usuario con el fin de proporcionar un servicio kinesiología de la calidad de un profesional de la salud. Es importante delimitar la política de privacidad de esta organización y de su producto, Kinteractive, para poder asegurar a los potenciales pacientes, instituciones médicas y kinesiólogos el alcance procesos como lo son: obtención de datos, el uso de los datos obtenidos, establecer formas adecuadas y legítimas de obtención de consentimiento. Adicionalmente, se busca realizar una política que sea enfocada y centrada en el paciente, tomando como prioridad la seguridad de su información personal, privada y de carácter

médico.

Cabe destacar que actualmente Techneworks es una organización que no está operativa, por lo que el diseño e implementación en cuestión están enfocadas en un desarrollo inicial del sistema. Sin embargo, la necesidad de soluciones enfocadas a esta materia actualmente en boga hace que sea necesario evaluar a futuro cuales pueden ser los beneficios al extender la solución a un alcance de nivel empresarial.

2.2. Antecedentes

Se busca cuantificar el efecto que tienen los problemas de seguridad con el fin de identificar cuales son los activos que se buscan proteger dentro de la organización, cómo mitigar el robo o mal uso de información privada y que mecanismos implementar para llevar el desarrollo a cabo. Es necesario indagar en el estado actual del área para poder entender cuales son los fallos y cómo proteger el sistema de estos.

La falta de implementación adecuada de mecanismos que mantengan la privacidad de los usuarios afecta negativamente a todos los involucrados/*stakeholders* de organizaciones del área de la salud. La falta de cumplimiento conlleva vulnerabilidades en los sistemas que pueden y generalmente son explotadas por terceros y agentes maliciosos. Artículos escritos por “Compliancy Group” muestran que las infracciones relacionadas a robo de datos con información médica pueden alcanzar cifras en el orden de millones de USD [Compliancy Group, 2022a]; Adicionalmente, estos robos de información afectan a cientos de miles de pacientes [Compliancy Group, 2022b].

Las repercusiones además de afectar directamente a la organización responsable y los pacientes a corto plazo, pueden ser problemáticas para futuros pacientes; las estimaciones y estadísticas recopiladas por D. Georgiev [TechJury, 2022] muestran que hasta el “61 % de los potenciales robos de datos se atribuyen a negligencia de los empleados” y que el “39 % de las organizaciones de salud se enteraron de los incidentes meses después de haber ocurrido”.

2.3. Identificación del problema

TechneWorks, la entidad gestora de Kinteractive, enfrenta una carencia significativa al no contar con una política de privacidad formalmente definida. Esta omisión representa una vulnerabilidad importante, especialmente en el contexto de la sensibilidad y confidencialidad de los datos de los pacientes en el sector de la salud. La ausencia de una política de privacidad adecuada no solo pone en riesgo la protección de la información privada y confidencial de los pacientes, sino que también afecta la reputación de la organización y aumenta las posibilidades de sanciones monetarias u operativas.

La falta de una política de privacidad bien definida afecta directa e indirectamente a todas las partes interesadas (stakeholders) involucradas. Esto incluye a los kinesiólogos, los centros de salud, y, sobre todo, a los pacientes. Aunque las regulaciones como HIPAA están diseñadas para proteger a los pacientes, es responsabilidad de las empresas, como TechneWorks, asegurar la confidencialidad de sus datos. Esta responsabilidad abarca tanto al equipo de desarrollo y operaciones de la organización como a los profesionales de la salud que utilizan la plataforma Kinteractive para recolectar y gestionar la información médica de los pacientes.

Se muestra a continuación la figura 1, la cual denota al paciente como el elemento céntrico ya que en este es que se enfoca la política de privacidad. Adicionalmente, este se relaciona con Dev y Ops que son los equipos de desarrollo y operaciones respectivamente; la relación es tal que el paciente hace uso de los servicios y aplicaciones dispuestos por estos equipos que conforman la organización. Los profesionales de la salud son participantes en este proceso ya que ellos recolectan y hacen uso de información médica provista por los mismos pacientes a través de Kinteractive, además de manejar los datos recopilados de los pacientes y tener un amplio registro de patologías, condiciones, tratamientos, etc. Por último, están las leyes implementadas y la regulación HIPAA, quienes abogan por los derechos y la privacidad del paciente, sin embargo, interactúan y se relacionan directamente con la organización ya que supervisan que esta cumpla con los mandamientos y lineamientos establecidos.

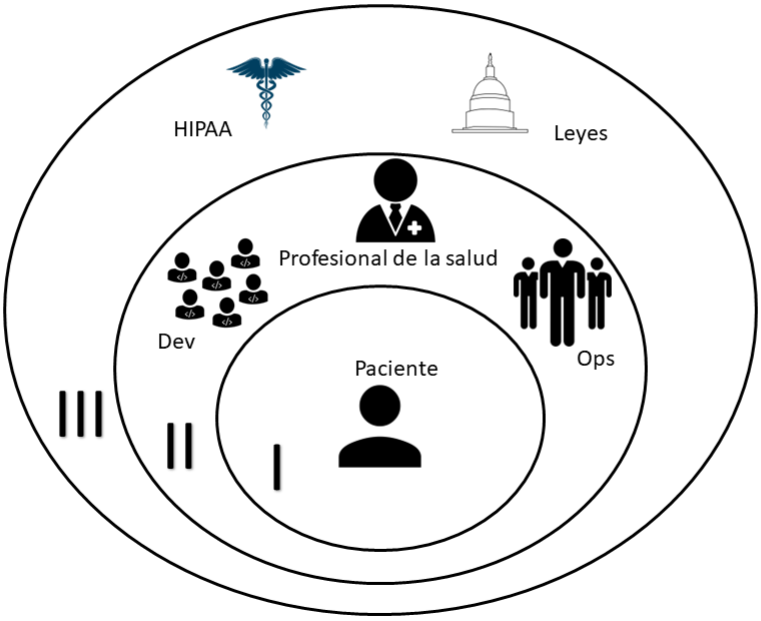


Figura 1: Stakeholders map. Elaboración Propia

De manera general, como se muestra en el árbol del problema en la figura 2, hay una

serie de problemas e inseguridades asociadas a una política de privacidad mal delimitada, con faltas de información, desactualizadas, entre otros. Las causas suelen darse por malas prácticas, falta de una ley que regule adecuada y estrictamente los procedimientos y tratamientos sobre los datos, y en un aspecto más técnico, falta un marco de trabajo formal comprensivo de las regulaciones que se toman en cuenta y que sea centrado en la privacidad. [Al Faresi *et al.*, 2010][Cheng, Vivying SY y Hung, Patrick CK, 2005]

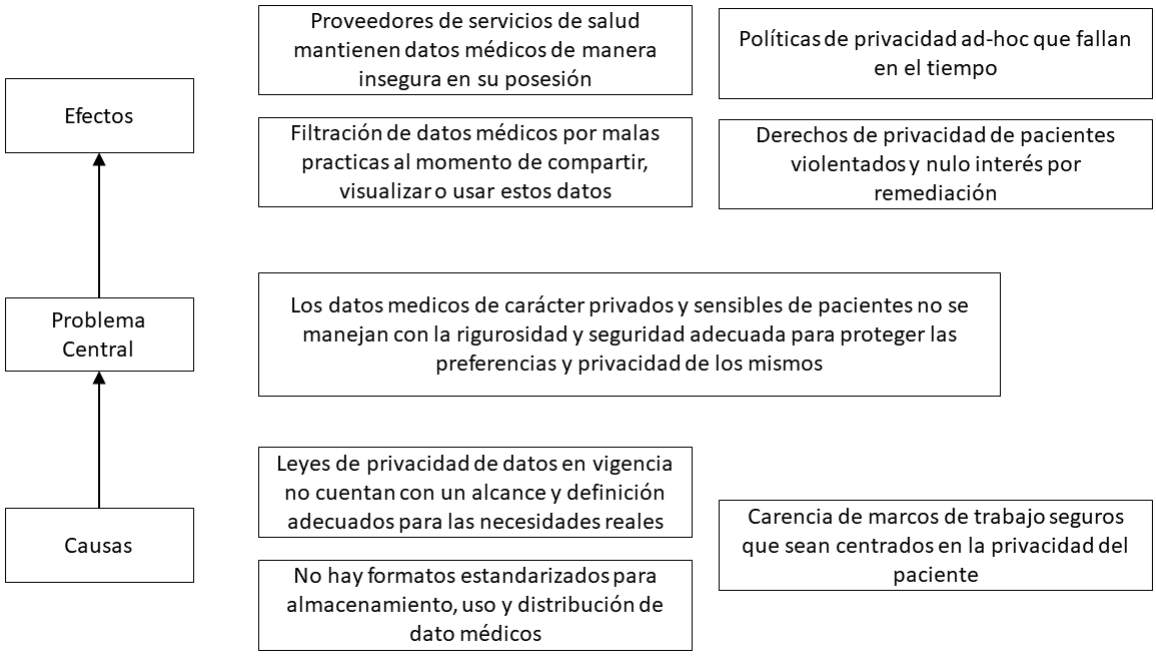


Figura 2: Árbol del problema. Elaboración Propia

2.4. Objetivos

2.4.1. Objetivo General

- Generar una política de privacidad para TechneWorks que cumpla con las leyes de privacidad y seguridad de datos Chilenas y con la reglamentación HIPAA mediante un marco de trabajo cuya principal preocupación sea el paciente.

2.4.2. Objetivos Específicos

- Analizar las implicancias intrínsecas y características de las leyes nacionales y regulación HIPAA para determinar las relaciones entre ellas, con el fin de confeccionar una política comprensiva.

- Asegurar el cumplimiento de las normas vigentes mediante integración continua de los requerimientos a la política de privacidad.
- Generar una política de seguridad de datos autosustentable para la organización.
- Proponer un método de verificación periódica del estado de la política de la empresa y su cumplimiento.
- Realizar un prototipo del sistema que realizará la gestión descrita para la política de privacidad.

2.5. Metodología

En el presente trabajo, se presenta una metodología detallada para el desarrollo de la política de privacidad de TechneWorks, una empresa dedicada a proporcionar servicios en el ámbito de la salud y el bienestar. La elaboración de esta política de privacidad es fundamental para garantizar el cumplimiento de las leyes y regulaciones vigentes en materia de protección de datos, tanto a nivel nacional como internacional, incluyendo las normativas chilenas y la reglamentación HIPAA.

La metodología propuesta se fundamenta en un enfoque iterativo-incremental, que permite abordar de manera efectiva los diversos aspectos relacionados con la privacidad de los datos. Se empieza con la identificación de los procesos clave llevados a cabo por la empresa, como el almacenamiento de información personal y las comunicaciones con los usuarios. A partir de esto, se detallan los tipos de información recopilada, la justificación de su recolección, los procesos utilizados para obtenerla, y los derechos y procedimientos disponibles para los usuarios.

Adicionalmente, se incorpora el uso del marco de trabajo OSINT para abordar la ciberseguridad y comprender mejor los riesgos asociados con la recopilación y tratamiento de datos. Todo ello se lleva a cabo dentro de un alcance definido que busca ofrecer una solución comprensiva y eficiente, capaz de adaptarse a los requerimientos del negocio y a los cambios en la regulación. A continuación, se detalla paso a paso la metodología propuesta para el desarrollo de la política de privacidad de TechneWorks.

2.5.1. Fases de la Metodología Propuesta

La metodología propuesta se divide en varias fases, cada una de las cuales aborda aspectos específicos del desarrollo de la política de privacidad. A continuación, se describen brevemente las principales etapas:

- **Identificación de Procesos Clave:** En esta fase, se identifican los procesos principales llevados a cabo por TechneWorks, incluyendo la recopilación, almacenamiento y uso

de datos personales. Se analizan las interacciones entre la empresa y sus usuarios para comprender mejor cómo se maneja la información.

- **Análisis de Información Recopilada:** Se procede a listar detalladamente la información que se recopila, así como los motivos detrás de su recolección. Se examinan los métodos utilizados para obtener esta información y se identifican las partes autorizadas para acceder a ella.
- **Derechos de los Usuarios y Procedimientos de Ejercicio:** En esta fase, se establecen los derechos que tienen los usuarios sobre sus datos personales y se detallan los procedimientos disponibles para ejercer dichos derechos. Se incluye información sobre cómo contactar a la empresa en caso de dudas o reclamos.
- **Marco de Trabajo OSINT:** Se aplica el marco de trabajo OSINT para evaluar los riesgos asociados con la privacidad de los datos y la ciberseguridad. Se analiza la información disponible públicamente para identificar posibles amenazas y vulnerabilidades.
- **Desarrollo de la Política de Privacidad:** Con base en los resultados obtenidos en las fases anteriores, se procede al desarrollo de la política de privacidad de TechneWorks. Se redacta un documento comprensivo que aborde todos los aspectos relevantes en materia de protección de datos.
- **Verificación y Actualización Periódica:** Finalmente, se establece un método para verificar periódicamente el estado de la política de privacidad y su cumplimiento. Se definen los procedimientos para realizar ajustes y actualizaciones según sea necesario, en respuesta a cambios en la regulación o en las prácticas de la empresa.

La metodología propuesta ofrece un enfoque estructurado y completo para el desarrollo de la política de privacidad de TechneWorks. Al seguir este proceso paso a paso, la empresa puede garantizar el cumplimiento de las leyes y regulaciones vigentes, así como proteger la privacidad y seguridad de los datos de sus usuarios de manera efectiva y continua.

CAPÍTULO 3
MARCO CONCEPTUAL

Actualmente la política de privacidad de una empresa u organización es la cara ante sus usuarios sobre su posición con respecto a la seguridad de los datos que recolectan y almacenan. A pesar de la gran importancia que tiene esta política, es posible que se escapen aspectos relevantes para los desarrolladores, administradores, jefes de seguridad, entre otros que activamente trabajan para mejorar la política de seguridad. Dichos elementos que pueden quedar por fuera al momento de definir formalmente las componentes, funciones y usos, lo cual lleva a una política con fallas fundamentales y que recae en la reputación y estado financiero de la organización.

Para administrar la política de privacidad de la organización Techneworks efectivamente, se implementa un Sistema de Gestión de la Privacidad y Seguridad de la Información. La misión del sistema es permitir administrar de manera global la postura de seguridad ante la información y datos personales de manera continua y comprensiva. Se define como usuario cualquier potencial persona que use software de Techneworks con fines personales o comerciales, cuyos datos provistos por el dispositivo, registro en los sistemas o uso de la aplicación serán los datos, datos personales y datos sensibles a resguardar.

3.1. Definición de Política de Privacidad

Una política de privacidad de la información es el documento legal que detalla como una organización recolecta, maneja, procesa y respeta los datos personales de sus clientes en un sitio o aplicación web. [GDPR, 2016b].

Los principios de privacidad de datos, tanto a nivel internacional como nacional, incluyen la transparencia en el tratamiento de datos, el consentimiento informado de los pacientes para la recolección y uso de sus datos, la limitación del uso y divulgación de datos a lo estrictamente necesario para fines específicos, la seguridad de la información mediante medidas técnicas y organizativas adecuadas, y la responsabilidad en el manejo de datos por parte de los responsables del tratamiento. En el caso que nos ocupa, el consentimiento informado se refiere al del paciente.

La privacidad de los datos en el sector de la salud es un tema de creciente importancia debido a la sensibilidad y confidencialidad de la información médica. La protección de la privacidad de los pacientes se considera fundamental para mantener la confianza en el sistema de salud y garantizar el respeto de los derechos individuales. A medida que avanza la tecnología y se digitalizan los registros médicos, surge la necesidad de establecer normativas y medidas de seguridad adecuadas para proteger la privacidad de los datos de los pacientes. A continuación, se detallan algunos aspectos a considerar. [Uivaru, 2018]

- **Confidencialidad de la información médica:** Los datos médicos, incluyendo historias clínicas, resultados de pruebas, diagnósticos y tratamientos, deben tratarse con la mayor confidencialidad posible para proteger la privacidad de los pacientes. Solo el personal profesional del área de la salud autorizado debe tener acceso a esta información, y se deben implementar medidas de seguridad adecuadas para evitar el acceso no autorizado.
- **Cumplimiento normativo:** En muchos países, existen leyes y regulaciones específicas que rigen la protección de datos en el sector de la salud. Estas leyes, como la HIPAA en Estados Unidos o normativas similares en otros países, establecen estándares y requisitos para la protección de la información médica y la privacidad de los pacientes.
- **Consentimiento informado:** Los pacientes deben otorgar su consentimiento informado para el uso y la divulgación de su información médica. Esto significa que deben comprender completamente cómo se utilizarán sus datos y dar su consentimiento de manera voluntaria y consciente. Además, los pacientes tienen derecho a revocar su consentimiento en cualquier momento.
- **Seguridad de la información:** Se deben implementar medidas de seguridad sólidas para proteger la información médica contra accesos no autorizados, pérdidas o robos. Esto puede incluir el uso de sistemas de cifrado, contraseñas seguras, firewalls y controles de acceso físico y electrónico.
- **Acceso y rectificación de datos:** Los pacientes tienen derecho a acceder a su información médica y solicitar correcciones si encuentran errores o inexactitudes. Las instituciones de salud deben tener procedimientos claros para gestionar estas solicitudes y garantizar la precisión de los datos.
- **Intercambio de datos entre instituciones:** Cuando se comparten datos médicos entre diferentes instituciones de salud, como hospitales, clínicas y consultorios médicos, se deben seguir protocolos y estándares específicos para garantizar la seguridad y la privacidad de la información.
- **Educación y capacitación del personal:** Es fundamental que el personal médico y administrativo esté adecuadamente capacitado en prácticas de privacidad y seguridad de datos. Esto incluye la sensibilización sobre la importancia de proteger la privacidad de los pacientes y la formación en el uso adecuado de sistemas y herramientas tecnológicas.

3.2. Regulaciones Internacionales y Nacionales

Las regulaciones internacionales y nacionales en Chile establecen un marco legal integral para la protección de datos personales en el sector de la salud. El cumplimiento de estas regulaciones es fundamental para garantizar la confidencialidad y seguridad de la información médica de los pacientes y mantener la confianza en el sistema de salud.

El marco regulatorio internacional más destacado en materia de privacidad de datos en el sector de la salud es el Health Insurance Portability and Accountability Act (HIPAA) en Estados Unidos. HIPAA establece normas y procedimientos para proteger la privacidad y seguridad de la información médica de los pacientes. En el ámbito nacional, en Chile, la Ley de Protección de Datos Personales y la Ley de Derechos y Deberes de los Pacientes regulan la protección de la privacidad de los datos en el sector de la salud.

3.2.1. Regulaciones Internacionales

Reglamento General de Protección de Datos (GDPR) de la Unión Europea: Aunque no es una regulación específica de Chile, el GDPR establece estándares internacionales muy altos en materia de protección de datos personales. Muchas empresas y organizaciones chilenas que operan en la Unión Europea deben cumplir con los requisitos del GDPR, lo que a menudo influye en las prácticas de protección de datos a nivel nacional. [GDPR, 2016a]

Regla de Privacidad de HIPAA: Esta regla establece estándares para la protección de la privacidad de la información de salud identificable (PHI, por sus siglas en inglés) mantenida por entidades cubiertas, como proveedores de atención médica, compañías de seguros de salud y planes de salud. Establece cómo se puede utilizar y divulgar la PHI y otorga ciertos derechos a los individuos con respecto a su información de salud. [U.S. Department of Health Human Services, 1999b]

Regla de Seguridad de HIPAA: Esta regla establece estándares para la protección de la información de salud electrónica (ePHI, por sus siglas en inglés). Requiere que las entidades cubiertas implementen medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la ePHI. [U.S. Department of Health Human Services, 1998]

Regla de Notificación de Brechas de HIPAA: Esta regla establece requisitos para que las entidades cubiertas notifiquen a los individuos afectados y a la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de EE. UU. sobre ciertas violaciones de seguridad de la PHI. [U.S. Department of Health Human Services, 1999a]

3.2.2. Regulaciones Nacionales

Ley N° 19.628 Protección de la Vida Privada: Esta ley establece los principios generales para la protección de datos personales en Chile. Si bien no se centra específicamente en el sector de la salud, sienta las bases legales para garantizar la privacidad de la información personal en todos los ámbitos, incluido el médico. [MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, 2020]

Ley N° 20.584 Derechos y deberes de las personas en atención de salud: Esta ley regula los derechos y deberes de las personas en relación con la atención de sa-

lud. Establece, entre otras cosas, el derecho de los pacientes a la confidencialidad de su información médica y la obligación de los prestadores de salud de protegerla. [MINISTERIO DE SALUD, SUBSECRETARÍA DE SALUD PÚBLICA, 2023]

Ley N° 21.096 Protección de Datos Personales: Esta ley establece disposiciones destinadas a proteger los derechos fundamentales de las personas en relación con el tratamiento de sus datos personales, garantizando su privacidad y autonomía. Fue promulgada el 23 de mayo de 2018 y publicada en el Diario Oficial el 25 de mayo de 2018. La ley regula el tratamiento de datos personales por parte de los organismos públicos y privados, estableciendo principios, derechos y deberes para las partes involucradas en el manejo de la información personal. [MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, 2018]

El cumplimiento de estas regulaciones implica que las instituciones de salud deben implementar medidas de seguridad y procedimientos adecuados para proteger la privacidad de la información médica de los pacientes. Esto incluye la adopción de tecnologías seguras, la capacitación del personal en prácticas de privacidad y seguridad de datos, y el establecimiento de políticas claras de gestión de datos. [Pablo Recalde, 2023]

3.2.3. Similitudes entre las Regulaciones

Dado el alcance de la regulación HIPAA y el tiempo que esta lleva implementada como estándar en el área de salud, se puede ver que las exigencias que presenta buscan cubrir todas las posibles brechas entre las prácticas que realizan las organizaciones de salud y el riesgo de filtración de información de sus pacientes.

Por el lado de las leyes Chilenas, estas buscan de manera general poder describir las buenas prácticas que deben ser llevadas por las organizaciones a nivel local, no solamente las organizaciones de salud, para el manejo de datos personales y el respeto a la privacidad de estos. En particular las leyes 19.638, 20.584 y 21.096 definen mecanismos a un nivel que no es apto para los estándares modernos, en particular en materia de seguridad de los datos y de la información.

Teniendo en cuenta que estas leyes no mencionan mecanismos específicos sobre datos y registros electrónicos, mecanismos orientados a aplicaciones de carácter digital, ni procedimientos para tratamiento, recolección y uso de los datos, se procede a utilizar estas leyes como un subconjunto de la regulación HIPAA y de los procesos y requerimientos que esta plantea.

Esta brecha entre las tecnologías modernas y las leyes locales se ven cubierta específicamente por la Regla de Seguridad de HIPAA, ya que requiere la implementación de mecanismos de protección adecuados para los procesos administrativos, técnicos y físicos que contengan información personal en formato digital, con el fin de asegurar la integridad, confidencialidad y seguridad de estos datos.

3.3. Principios de Privacidad de Datos

Los principios de privacidad de datos, como los definidos por la Ley de Protección de Datos Personales y HIPAA, incluyen la transparencia en el manejo de datos, el consentimiento informado de los pacientes para el uso de su información, la limitación del uso y divulgación de datos, la seguridad de la información y la responsabilidad en el manejo de datos.

Consentimiento informado: Los individuos deben otorgar su consentimiento informado antes de que su información personal y médica sea recopilada, utilizada o compartida por los proveedores de servicios de salud. Este consentimiento debe ser voluntario, específico, inequívoco y basado en una comprensión clara de cómo se utilizará la información.

Finalidad limitada: La información personal y médica sólo debe recopilarse y utilizarse para fines específicos y legítimos relacionados con la prestación de servicios de salud, la investigación médica o el cumplimiento de obligaciones legales. No debe utilizarse para fines no autorizados o incompatibles con la finalidad original de la recopilación.

Minimización de datos: Se debe recopilar y almacenar la cantidad mínima de datos personales y médicos necesarios para cumplir con la finalidad prevista. Esto implica limitar la recopilación de información a lo que es estrictamente necesario y evitar la recolección de datos innecesarios o excesivos.

Exactitud y actualización de los datos: Los datos personales y médicos deben ser precisos, completos y actualizados. Los proveedores de servicios de salud deben tomar medidas para garantizar la exactitud de la información recopilada y actualizarla regularmente cuando sea necesario para evitar la toma de decisiones erróneas basadas en datos obsoletos o inexactos.

Seguridad de datos: Se deben implementar medidas técnicas y organizativas adecuadas para proteger la seguridad y confidencialidad de la información personal y médica contra accesos no autorizados, divulgaciones indebidas, pérdidas o daños. Esto incluye el uso de sistemas de cifrado, controles de acceso, políticas de seguridad y capacitación del personal.

Transparencia y acceso: Los individuos tienen derecho a conocer cómo se está utilizando su información personal y médica, así como a acceder a sus propios registros de salud y solicitar correcciones si encuentran inexactitudes. Los proveedores de servicios de salud deben ser transparentes sobre sus prácticas de privacidad y proporcionar mecanismos para que los individuos ejerzan sus derechos de acceso y corrección.

Retención y disposición segura: Los datos personales y médicos deben retenerse únicamente durante el tiempo necesario para cumplir con la finalidad prevista y las obligaciones legales aplicables. Después de este período, la información debe ser eliminada de manera segura o anonimizada para proteger la privacidad de los individuos.

[Office of the United Nations High Commissioner for Human Rights, 2022]

3.4. Desafíos en la Implementación de Políticas de Privacidad

La implementación efectiva de políticas de privacidad en el sector de la salud enfrenta una serie de desafíos significativos. Estos desafíos deben ser abordados de manera integral y estratégica para garantizar el cumplimiento normativo y la protección efectiva de los datos de los pacientes.

La complejidad de las regulaciones en constante evolución es uno de los principales obstáculos. Las leyes y regulaciones relacionadas con la privacidad de los datos de salud están en constante cambio y evolución, lo que dificulta mantenerse al día y garantizar el cumplimiento normativo. Mantenerse al día con estos cambios y asegurar el cumplimiento puede ser un desafío para las organizaciones de salud, especialmente cuando las regulaciones varían según la ubicación geográfica y el ámbito de aplicación. Es fundamental contar con un equipo dedicado a monitorear y adaptar las políticas de privacidad en respuesta a los cambios regulatorios.

Además, el rápido avance de la tecnología presenta desafíos adicionales. Nuevas tecnologías como la inteligencia artificial, el análisis de big data y la telemedicina ofrecen oportunidades innovadoras para mejorar la atención médica, pero también plantean riesgos para la seguridad y privacidad de los datos. Las organizaciones deben implementar medidas de seguridad y privacidad que se adapten a estas tecnologías emergentes y garanticen la protección de los datos en todas las etapas del proceso.

La falta de recursos y capacitación en materia de privacidad también es un desafío común. Muchas organizaciones de salud carecen de los recursos y la capacitación necesarios para implementar políticas de privacidad efectivas. La protección de datos requiere inversiones significativas en tecnología, personal y formación. Es crucial que las organizaciones asignen los recursos adecuados para garantizar la seguridad y privacidad de los datos, y que proporcionen capacitación regular a su personal sobre las mejores prácticas de privacidad y seguridad de la información.

Otro desafío importante es encontrar un equilibrio entre la protección de los datos de los pacientes y la accesibilidad de la información. En el sector de la salud, es fundamental garantizar que los datos estén protegidos contra accesos no autorizados, pero también deben permitir un acceso rápido y seguro a la información por parte de los profesionales de la salud cuando sea necesario para el diagnóstico y tratamiento de los pacientes.

Finalmente, establecer una cultura organizacional que valore y priorice la privacidad de los datos puede ser un proceso complejo y a largo plazo. Requiere un cambio profundo en la mentalidad y las prácticas de la organización, desde la alta dirección hasta el personal de nivel operativo. Esto implica educar y sensibilizar a todos los miembros de la organización

sobre la importancia de la privacidad de los datos, así como implementar políticas y procedimientos que promuevan una cultura de privacidad en todas las actividades y decisiones de la organización.

3.5. Tecnologías de Protección de Datos

Las tecnologías de protección de datos son herramientas y medidas diseñadas para garantizar la seguridad y privacidad de los datos personales en entornos de atención médica y otros sectores que manejan información sensible. Sin embargo, es importante destacar que ninguna tecnología es completamente segura, por lo que es necesario implementar un enfoque integral que combine tecnologías de protección con políticas, procesos y controles adecuados para mitigar los riesgos de seguridad de la información. Cada una de estas herramientas contribuye a garantizar la seguridad y privacidad de la información [Ramiro, 2021]. Algunas de las tecnologías que se han implementado se presentan a continuación.

Encriptación de datos: Consiste en convertir la información en un código secreto antes de ser transmitida o almacenada, de modo que solo las personas autorizadas puedan acceder a ella. La encriptación puede aplicarse tanto en reposo (datos almacenados) como en tránsito (datos en movimiento). La encriptación de datos es esencial para proteger la información médica confidencial tanto en reposo como en tránsito. En el caso de los registros médicos electrónicos y la comunicación de datos entre profesionales de la salud, la encriptación garantiza que solo las personas autorizadas puedan acceder y comprender la información, lo que ayuda a prevenir la divulgación no autorizada y el acceso no deseado a datos sensibles. [Salas, 2017]

Firewalls: Son sistemas de seguridad que controlan el tráfico de red y pueden bloquear o permitir el acceso a determinados datos o servicios en función de reglas predefinidas. En resumen ayudan a prevenir accesos no autorizados desde redes externas. Los firewalls y los sistemas de detección de intrusiones son fundamentales para proteger los sistemas de información médica contra accesos no autorizados y ataques cibernéticos. Estas tecnologías ayudan a monitorear el tráfico de red y a detectar y bloquear posibles amenazas, como intentos de acceso no autorizado o malware, antes de que puedan comprometer la seguridad de los datos. [Leyva, 2017]

Sistemas de Gestión de Acceso e Identidad (IAM): Estas soluciones permiten administrar y controlar quién tiene acceso a qué información dentro de una organización. Incluyen funciones como la autenticación de usuarios, autorización de acceso y gestión de credenciales. En entornos de atención médica, donde múltiples profesionales de la salud y personal administrativo acceden a sistemas y datos sensibles, los sistemas de IAM son esenciales para garantizar que solo las personas autorizadas puedan acceder a la información relevante para sus funciones específicas. Estos sistemas ayudan a administrar y controlar el acceso de los usuarios, asegurando que cada usuario tenga los privilegios de acceso adecuados y que se sigan los principios de mínimos privilegios y necesidad de conocer. [González, 2024]

Protección contra Malware y virus: Esta barrera es un a software diseñado para detectar, prevenir y eliminar programas maliciosos que podrían comprometer la seguridad de los datos, como virus, troyanos, ransomware, entre otros. Dado el riesgo constante de ataques de malware y virus en entornos de atención médica, es fundamental contar con soluciones de protección contra estas amenazas. Esto incluye la implementación de software antivirus, antimalware y antiransomware actualizado y la educación continua del personal sobre las mejores prácticas de seguridad cibernética y cómo reconocer posibles amenazas. [Riega Riega, 2015]

Control de acceso físico y lógico: Incluye medidas para restringir el acceso físico a instalaciones donde se almacena o procesa información sensible, así como también controles para limitar el acceso lógico a sistemas y aplicaciones mediante contraseñas, autenticación multifactor, tarjetas de acceso, etc. Además de proteger los sistemas de información médica contra accesos no autorizados desde el exterior, también es importante implementar controles de acceso físico y lógico en las instalaciones médicas para evitar el acceso no autorizado a equipos y sistemas que contienen datos sensibles. Esto puede incluir medidas como sistemas de cerraduras electrónicas, controles de acceso con tarjeta y cámaras de seguridad para monitorear el acceso a áreas sensibles. [Martelo, R. J., 2018]

Anonimización y seudonimización de datos: Procesos para ocultar o modificar ciertos detalles de los datos personales de manera que no sea posible identificar a los individuos a los que pertenecen, mientras se mantienen útiles para su análisis o procesamiento. En ciertos casos, puede ser necesario anonimizar o seudonimizar datos sensibles para proteger la privacidad de los pacientes mientras se permite su uso para fines de investigación y análisis. Estos procesos aseguran que los datos no puedan ser atribuidos a individuos específicos sin el uso de información adicional, lo que ayuda a proteger la privacidad de los pacientes y cumple con las regulaciones de privacidad de datos.

Auditoría y monitoreo de seguridad: Herramientas que permiten supervisar el uso y acceso a los datos, registrar actividades sospechosas y generar informes para análisis y cumplimiento normativo. La implementación de herramientas de auditoría y monitoreo de seguridad permite a las organizaciones de atención médica supervisar de cerca el uso y acceso a los datos sensibles, identificar actividades sospechosas y responder rápidamente a posibles violaciones de seguridad. Estas herramientas permiten a las organizaciones mantener un registro detallado de quién accede a qué datos y cuándo, lo que es fundamental para la detección temprana y la respuesta efectiva a posibles amenazas de seguridad.

3.6. Gestión de Riesgos y Auditoría

La gestión de riesgos en el contexto de la privacidad de datos en el sector de la salud implica identificar, evaluar y mitigar los riesgos asociados con la recopilación, almacenamiento, procesamiento y transmisión de información médica confidencial.

En relación con la identificación de riesgos, implica identificar todas las posibles amenazas y vulnerabilidades que podrían comprometer la seguridad y privacidad de los datos médicos, así como los impactos potenciales de dichas amenazas. Una vez identificados los riesgos, se evalúa su probabilidad de ocurrencia y su impacto potencial en el negocio y en los pacientes. Esto ayuda a priorizar los riesgos y determinar qué medidas de mitigación son más urgentes y efectivas.

Respecto a la evaluación de riesgos, se implementan medidas para mitigar o reducir la probabilidad de ocurrencia de los riesgos identificados, así como para minimizar su impacto en caso de que ocurran. Esto puede incluir la implementación de controles de seguridad adicionales, la mejora de las políticas y procedimientos internos, y la capacitación del personal en prácticas de seguridad de la información.

En general la gestión de riesgos es un proceso continuo que requiere monitoreo constante y revisión periódica para asegurar que las medidas de mitigación implementadas sean efectivas y estén alineadas con los cambios en el entorno operativo y las amenazas emergentes.

Por otra parte la auditoría en el contexto de la privacidad de datos en el sector de la salud implica la evaluación independiente y sistemática de los controles de seguridad y privacidad de datos para garantizar el cumplimiento de las políticas, regulaciones y estándares aplicables.

Durante una auditoría, se evalúan los controles internos implementados por una organización para proteger la seguridad y privacidad de los datos médicos. Esto puede incluir controles de acceso, encriptación de datos, políticas de retención de datos, y procedimientos de respuesta a incidentes, entre otros.

Los auditores realizan pruebas para verificar el cumplimiento de las políticas y procedimientos establecidos. Esto puede implicar revisar registros de auditoría, realizar entrevistas con el personal, y revisar la documentación relacionada con la seguridad y privacidad de los datos.

Durante la auditoría, se identifican posibles deficiencias en los controles de seguridad y privacidad de datos, así como áreas de mejora. Los auditores proporcionan recomendaciones para abordar estas deficiencias y mejorar el cumplimiento normativo y la seguridad de la información.

Al finalizar la auditoría, se emite un informe que resume los hallazgos de la auditoría, incluyendo cualquier deficiencia identificada, recomendaciones para mejorar los controles de seguridad y privacidad, y el nivel de cumplimiento normativo de la organización.

En resumen, la gestión de riesgos y la auditoría son procesos críticos para garantizar la seguridad y privacidad de los datos médicos en el sector de la salud. Al identificar y mitigar

los riesgos asociados con la información médica confidencial y evaluar regularmente los controles de seguridad y privacidad, las organizaciones de atención médica pueden mantener la integridad y confidencialidad de los datos del paciente y cumplir con las regulaciones y estándares aplicables. [Damani, 2004]

3.7. Consideraciones Éticas

Las consideraciones éticas en el ámbito de la privacidad de datos en el sector de la salud son fundamentales para garantizar el respeto y la protección de los derechos de los pacientes, así como para promover la confianza y la transparencia en el manejo de la información médica confidencial. A continuación se presentan algunas consideraciones éticas.

Respeto a la autonomía y la privacidad del paciente: Los profesionales de la salud y las organizaciones deben respetar la autonomía y la privacidad de los pacientes, asegurando que se obtenga el consentimiento informado antes de recopilar, almacenar o compartir su información médica. Esto implica proporcionar a los pacientes información clara y comprensible sobre cómo se utilizarán sus datos y brindarles opciones sobre cómo desean que se maneje su información.

Confidencialidad y seguridad de la información: Los profesionales de la salud tienen la responsabilidad ética de proteger la confidencialidad y seguridad de la información médica de los pacientes. Esto implica implementar medidas de seguridad adecuadas para prevenir el acceso no autorizado, la divulgación o el uso indebido de los datos médicos, así como garantizar que solo el personal autorizado tenga acceso a la información cuando sea necesario para la atención del paciente.

Principio de no maleficencia: Los profesionales de la salud tienen la obligación ética de no causar daño a los pacientes, lo que incluye proteger su privacidad y evitar cualquier uso indebido o malintencionado de su información médica que pueda causarles daño físico, emocional o financiero.

Beneficencia y utilidad de la información: Si bien es importante proteger la privacidad de los pacientes, también es fundamental reconocer el valor potencial de la información médica para mejorar la atención médica y la investigación biomédica. Por lo tanto, las consideraciones éticas deben equilibrar la protección de la privacidad con la necesidad de utilizar la información de manera ética y beneficiosa para el paciente y la sociedad en general.

Transparencia y rendición de cuentas: Las organizaciones de salud deben ser transparentes en sus prácticas de manejo de datos, proporcionando información clara sobre cómo se recopilan, almacenan, utilizan y comparten los datos médicos de los pacientes. Además, deben ser responsables ante los pacientes y la sociedad en general por sus acciones relacionadas con la privacidad de los datos, y estar dispuestas a rendir cuentas en caso de violaciones éticas o legales.

Como se puede evidenciar las consideraciones éticas son fundamentales en el manejo de la privacidad de datos en el sector de la salud, y guían las acciones de los profesionales de la salud y las organizaciones en el manejo responsable y ético de la información médica confidencial. Al respetar la autonomía y la privacidad de los pacientes, proteger la confidencialidad de la información, promover el beneficio y la utilidad de los datos, y ser transparentes y responsables en sus prácticas, las organizaciones de salud pueden garantizar la integridad y la ética en el manejo de la información médica. [Dirección de Investigación Gobierno de México, 2017]

3.8. Definición de Sistema de Gestión de la Privacidad y Seguridad de la Información

La base del control de la información, seguridad y privacidad se debe poder administrar y monitorear desde un gestor que acople todos los sistemas asociados a la organización con el fin de proveer mecanismos de protección para todos los usuarios. Entre los lineamientos que debe seguir el sistema y funciones que debe cumplir, es importante destacar:

- Definir los elementos y componentes sobre los cuales se desarrolla la política de privacidad.
- Verificar que los datos guardados y obtenidos a partir de cualquier proceso, involucren consentimiento explícito.
- Actualizar política y artículos de esta según sea necesario por reglas de negocio o estándares de privacidad y seguridad.
- Asignar y monitorear encargados de procesos para manejo y uso de datos.

Dado el conjunto de procedimientos a realizar por el sistema, es necesario establecer un plan de trabajo para definir formalmente que hará el sistema y el *how to*. Para esto se propone el procedimiento *"Plan-do-check-act"* (PDCA) [ASQ, 2022], el cual consiste de 4 etapas y ayuda a desarrollar procesos desde el inicio, identificar patrones repetitivos y preparar recolección de datos y análisis de estos. Los pasos de este procedimiento se describen de la siguiente forma:

1. "Plan: Reconocer una oportunidad y planear un cambio.
2. Do: Probar el cambio; llevar a cambio estudio a pequeña escala.
3. Check: Revisar la prueba, analizar resultados e identificar aprendizaje.
4. Act: Tomar acción basado en lo aprendido en este paso del estudio."

3.9. Estado del Arte

Un acercamiento para abordar la definición de una política de privacidad, son las herramientas para generar políticas online. En general cuentan con un flujo funcional que permite a través de una interfaz gráfica seleccionar manualmente las opciones que correspondan a como se realiza la recopilación, uso y almacenamiento de los datos personales y sensibles.

Este acercamiento es suficiente para cubrir los casos de uso de una organización cuyo enfoque sea otro rubro y que no necesiten trabajar grandes volúmenes de información sensible y confidencial. La forma de usarlo es bastante directa, seleccionando por interfaz que elementos aplican para el uso de los datos, como se muestra en el anexo **A**.

Es por esto que desde 2003 cuando HIPAA entró en vigencia, ha aumentado el deseo de generar un marco de trabajo que asegure a las empresas y a los usuarios. Para este propósito, se han desarrollado lenguajes como P3P y EPAL que buscaban estandarizar las prácticas de privacidad de sitios web en un formato interpretable por máquina para que el usuario pudiera determinar desde su navegador si la página cumplía con sus expectativas de privacidad [Ghazinour, Kambiz *et al.*, 2009]. Sin embargo, la dificultad para seguir estos lineamientos no oficiales ni reglamentados hicieron que los lenguajes no fueran adoptados como estándares y son usados como complemento o como extensión de otra componente.

Las prácticas y avances actuales buscan la inclusión de un marco de trabajo acoplado al servicio de salud ofrecido o el sistema que almacena los datos. En particular Cheng et al. “sugieren que un meta-lenguaje de privacidad independiente del vocabulario es esencial para arquitecturas de servicios web” [Cheng, Vivying SY y Hung, Patrick CK, 2005], lo cual es validado por el trabajo de Al Faresi et al. [Al Faresi *et al.*, 2010] que busca implementar un marco de trabajo que incluye un lenguaje basado en atributos de la política de privacidad y se codifica bajo el formato xml.

Entre las prácticas que más estancan un proceso limpio de generación de política de privacidad, está vincular los roles y permisos de la organización con los datos de los pacientes y cómo pueden utilizarlos [Al Faresi *et al.*, 2010]. Esto implica acceso a recursos mal administrado, ya que administradores de sistema adquieren acceso a datos confidenciales en base a atributos que no están relacionados.

En un sistema adecuado como el que propone AL Faresi et al. se tiene la lógica de la privacidad de datos separada de la lógica de políticas de control de acceso. Esto quiere decir que las preferencias del usuario para cada uno de sus datos, tienen prioridad sobre el acceso que pudo conseguir alguien de la organización para otros fines, como administrar base de datos, implementación, etc.

Adicionalmente, Ghazinour et al. hace énfasis en las ventajas y beneficios que trae poder mostrar el dominio de las políticas de manera gráfica y visual con el fin de facilitar al usuario qué ocurre con sus datos y como son usados [Ghazinour, Kambiz *et al.*, 2009]. Muestra casos

de uso ajustados a la realidad donde se ilustran interacciones con sistemas que recolectan datos personales, las restricciones que puede haber y como se presentan.

En la figura 3 se puede ver un caso de uso explicado mediante PRIVACY POLICY VISUALIZATION MODEL (PPVM) que indica explícitamente bajo qué condiciones un tercero puede requerir revelar información personal y privada si la ley lo requiere. Hace referencia a los distintos procesos que realiza la organización.

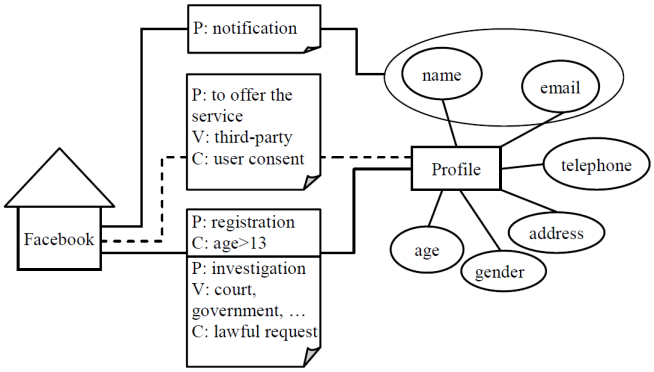


Figura 3: Diagrama PPVM de Caso de Uso 5. Extraido de [Ghazinour, Kambiz *et al.*, 2009]

A pesar de las múltiples posibilidades de usar sistemas y marcos de trabajo que cumplan con las regulaciones vigentes, lo cual se considera la cota inferior para proteger la privacidad del paciente, la mayoría de las organizaciones que necesitan cumplir con estos reglamentos, raramente cumplen total o parcialmente los lineamientos. Según el estudio de Carrión et al. [Carrión, Inmaculada *et al.*, 2011] que indaga sobre el estado actual de servicios web para mantener récords de pacientes (PHR), en una muestra n=20 solo el 25 % de los proveedores cumplían parcial o totalmente con los 6 requerimientos establecidos.

Desde el auge de la computación en la salud la cantidad de fugas de datos que ocurren diariamente ha aumentado aceleradamente en comparación a otras fuentes de información, no hay indicadores de que esta tendencia disminuya, por lo mismo se considera imperativo analizar más al respecto y poder generar herramientas que sean replicables para múltiples casos de uso y que los pacientes puedan contar con la seguridad de su información.

Los trabajos y artículos elegidos consisten de una amplia gama de investigaciones orientadas a diseños de políticas de privacidad, implementación de sistemas y metalenguajes que promueven la seguridad de la privacidad del paciente. Además, se incluyen estadísticas de documentos de carácter histórico que llevan cuenta de eventos como fugas y filtraciones de información personal a gran escala [Seh, Adil Hussain *et al.*, 2020].

3.10. Uso de Inteligencia Artificial para Manejo de Datos Sensibles

El uso de modelos de inteligencia artificial es una tendencia en aumento que permite reducir la brecha entre la necesidad de trabajo de análisis manual y el trabajo automatizado. Actualmente a nivel empresarial se generan grandes cantidades de datos que no cumplen con un esquema o definición rígida, por lo que se dificulta llevar un registro adecuado y conciso de que datos sensibles y personales se están almacenando y donde.

Para que las organizaciones puedan dar cumplimiento a las regulaciones de privacidad de datos es importante saber donde se están generando y recopilando los datos en la cadena de producción, este proceso se denomina “descubrimiento de datos”. El descubrimiento consiste en realizar un análisis a un repositorio de datos para extraer patrones que ayudan a determinar que tipo de información se está guardando en este repositorio.

Este análisis es adecuado para repositorios de datos estructurados, como bases de datos, ya que permite identificar la información guardada a nivel de columnas y definir cual es la relación entra una persona cuyos datos están siendo almacenados y los datos sensibles que se manejan de esta persona.

Los casos donde se propone el uso de soluciones deterministas basadas en reglas para el descubrimiento de datos son cuando el tipo de información almacenada es altamente consistente a lo largo del tiempo, por lo que el descubrimiento puede mantener una alta tasa de efectividad sin la necesidad ajustar los criterios para determinar si es un dato sensible o no. Para ese caso de uso descrito, puede que una solución basada en inteligencia artificial no aporte mayor confianza en la detección. [Jie SHI *et al.*, 2023]

Por otro lado, los sistemas de datos actuales cada vez necesitan una mejor detección de información sensible ya que el desarrollo de aplicaciones y servicios es un área en crecimiento y cada vez más difícil de monitorear en su totalidad, se hace necesario una solución que permita automatizar parte del trabajo, manteniendo la calidad en la identificación.

3.11. Tipos de datos contemplados por la regulación HIPAA

Los tipos de datos que considera la regulación HIPAA se denominan *Protected Health Information* (PHI), los cuales son datos e información asociados a cualquier aspecto de la salud, incluida información genética, de un paciente o de una persona cuyos datos son usados por una organización y que esta se puede compartir o ser almacenada en cualquier tipo de medio, particularmente en registros electrónicos. Estos pueden ser relacionados a la actualidad, eventos pasados o condiciones futuras que puede desarrollar la persona, la cual puede permitir identificar al paciente.

Teniendo en cuenta la información que debe ser protegida, se lista una serie de ejemplos prácticos de PHI:

- Diagnóstico de una enfermedad realizada por un médico
- Resultados de un perfil bioquímico
- Imágenes de rayos X
- Registro escrito de una sesión de terapia psicológica con un paciente

Para el caso de información estructurada y tabulada, los datos que se deben proteger bajo la regulación HIPAA son:

1. Nombre del paciente
2. Elementos geográficos
3. Fechas relacionadas a la salud o identidad del individuo
4. Números de teléfono
5. Números de fax
6. Direcciones de email
7. Números de identidad como SSN
8. Identificadores de registros médicos
9. Números de beneficiarios del seguro médico
10. Números de cuentas
11. Identificador o número de licencia
12. Identificadores de vehículo
13. Atributos o números de serie de dispositivos
14. Identificadores digitales, como URLs
15. Direcciones IP
16. Elementos biométricos
17. Fotografía del rostro del paciente
18. Otros números o identificadores

3.12. Entidades designadas para trabajar con datos PHI

Las entidades en capacidad de poder hacer uso, transmitir y manejar datos de tipo PHI son denominados *"HIPAA Covered Entities"* o Entidades Reguladas por HIPAA. En particular estas entidades que pueden hacer tratamiento, uso y compartir datos de tipo PHI son organizaciones como las que se mencionan, pero no se limitan a estas:

- Compañías aseguradoras
- Hospitales y Clínicas
- Doctores afiliados a una institución de salud o independientes
- Psicólogos afiliados a una institución de salud o independientes
- Dentistas afiliados a una institución de salud o independientes
- Compañías farmaceúticas
- Terapeutas físicos afiliados a una institución de salud o independientes

CAPÍTULO 4
PROPUESTA DE SOLUCIÓN

El sistema de gestión propuesto tiene como misión ayudar a los oficiales de privacidad a comprender mejor los marcos y regulaciones bajo los cuales tiene que operar. La visión de este proyecto es dar un precedente hacia la automatización del cumplimiento de manera continua, haciendo uso de tecnología emergente, específicamente la inteligencia artificial generativa.

Cabe destacar que esto implica que la solución cumple con documentar y mapear los procesos que realiza Kinteractive y generar la política de privacidad que permita cumplimiento con las leyes Chilenas y la regulación HIPAA sobre la protección de datos.

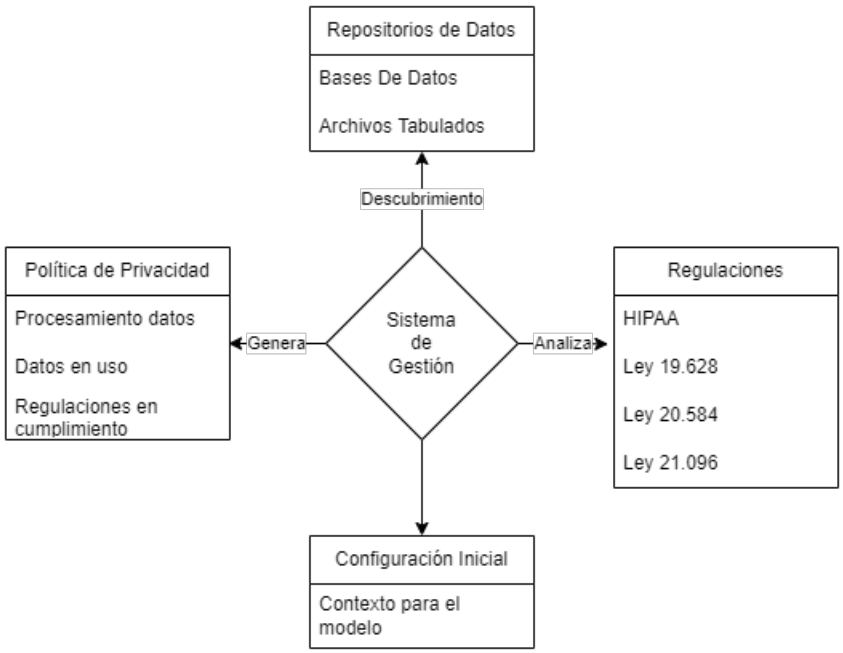


Figura 4: Componentes del sistema

4.1. Alcance de la Solución Propuesta

El proceso de redacción de la política de privacidad se seccionó en etapas tal que se pudieran llevar a cabo las siguientes actividades:

1. Levantamiento de información sobre las regulaciones que se buscan cumplir.

2. Definir puntos clave a implementar para dar cumplimiento con los puntos específicos de la regulación.
3. Analizar datos e información sensible que maneja la organización.
4. Realizar un mapa de los procesos que realiza la organización y los datos sensibles asociados.
5. Redactar la política de privacidad en base a los hallazgos.

4.2. Desarrollo Mediante Marco de Trabajo con Open Source Intelligence

La metodología OSINT (Open Source Intelligence) es un enfoque sistemático para recopilar, procesar y analizar información proveniente de fuentes abiertas y disponibles públicamente. Se usa específicamente esta metodología para seguir un marco de trabajo que permite levantar individualmente las necesidades a cubrir con la solución y trabajarlas en varias etapas, cada una de las cuales desempeña un papel crucial en el proceso de obtención de inteligencia.

OSINT se basa en información de carácter público, lo que contempla a una variedad de fuentes como bases de datos académicas, publicaciones gubernamentales, sitios web de noticias, foros y redes sociales, lo que enriquece el contenido del documento con diferentes perspectivas y datos actualizados. Las fuentes abiertas de información se actualizan constantemente, lo que permite acceder a datos recientes y relevantes que son verificables.

Dado que el aspecto de la privacidad de los datos y sus regulaciones es algo que se actualiza de manera continua, es más viable revisar información de fuentes abiertas. Dado el origen de la información, se tiene que considerar el riesgo de desinformación y por lo mismo, corroborar desde múltiples fuentes.

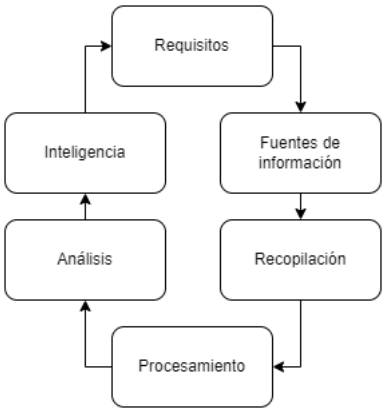


Figura 5: Diagrama de bloques metodología OSINT

Fuentes de Información
En esta fase, se identifican y seleccionan las fuentes de información pertinentes para el análisis. Estas fuentes pueden incluir sitios web públicos, redes sociales, bases de datos gubernamentales, informes de noticias, foros en línea, entre otros. Es fundamental evaluar la credibilidad y la relevancia de cada fuente para garantizar la calidad de la información recopilada.

Recopilación
Una vez identificadas las fuentes de información, se procede a recopilar los datos de manera sistemática y organizada. Esto puede implicar la descarga de documentos, la extracción de datos de sitios web, la recopilación de información de redes sociales, entre otras técnicas. Es importante asegurarse de recopilar toda la información relevante y mantener un registro detallado de las fuentes utilizadas.

Procesamiento
En esta etapa, se lleva a cabo el procesamiento inicial de los datos recopilados. Esto puede implicar la limpieza de datos, la normalización de formatos, la eliminación de duplicados y la estructuración de la información para facilitar su análisis posterior. El procesamiento de datos también puede incluir la aplicación de técnicas de minería de texto o análisis de datos para identificar patrones o tendencias significativas.

Análisis
Una vez procesados los datos, se procede al análisis en profundidad para obtener hallazgos y generar inteligencia significativa. Esto implica la identificación de relaciones, la detección de anomalías, la evaluación de la credibilidad de la información y la identificación de posibles implicaciones o riesgos. El análisis se realiza con el objetivo de generar una comprensión clara y completa de la situación o el tema de interés.

Inteligencia
En esta fase, se transforma la información analizada en inteligencia accionable y relevante para la toma de decisiones. Esto implica la elaboración de informes, generar recomendaciones y la comunicación de hallazgos de manera clara y efectiva a los interesados relevantes. La inteligencia resultante debe ser oportuna, precisa y pertinente para facilitar la toma de decisiones informadas.

Requisitos
Por último, se deben identificar y establecer los requisitos específicos de inteligencia que guiarán todo el proceso de OSINT. Estos requisitos pueden incluir objetivos de análisis, preguntas de investigación, áreas temáticas de interés y criterios de evaluación de la calidad de la información. Es fundamental definir claramente estos requisitos desde el principio para orientar eficazmente el proceso de obtención de inteligencia. [Freire Silva, 2022]

4.3. Delimitación de Datos Personales

Para abordar la protección de datos de manera efectiva, es fundamental comprender exhaustivamente los tipos de información que se deben proteger. En este sentido, se propone una fase inicial que se centra en identificar y englobar de manera comprensiva los datos personales relevantes, conforme a las disposiciones de la Ley 21906, Ley 19628 y la regulación HIPAA.

Estos datos representan un alto riesgo para la privacidad del paciente si son comprometidos o divulgados de manera indebida. La clasificación de datos se estructura en cinco categorías principales, a saber:

- **Información Personal:** Datos básicos de identificación como nombre, dirección, y número de identificación personal (RUT).
- **Información Financiera:** Información relacionada con métodos de pago, dirección de domicilio y registros de transacciones económicas.
- **Información Biométrica:** Datos biológicos únicos, como huellas dactilares, reconocimiento facial o de voz, utilizados para la identificación de usuarios.
- **Información Genética:** Datos relacionados con el perfil genético de un individuo, que pueden incluir información sobre enfermedades hereditarias o predisposiciones genéticas.
- **Información Médica:** Datos relacionados con la salud de un individuo, como historiales clínicos, resultados de pruebas médicas y diagnósticos.

4.4. Procesos de Recolección y Tratamiento de Datos de Kinteractive

Kinteractive cuenta con procesos para obtener información de sus pacientes que son estrictamente manejados para beneficio de los mismos, es decir, todos los procesos que involucran sus datos son realizados con un propósito explícito y que no beneficia directamente a la organización.

Cabe destacar que Kinteractive es una aplicación para atención de manera completamente digital, por lo que se garantiza que no existe recolección de información en formatos físicos como formularios, fichas o similares.

La siguiente fase se enfoca en los procesos de recolección y tratamiento de datos implementados por Kinteractive. Es fundamental entender cómo se recopilan y utilizan los datos de los pacientes para garantizar su privacidad y seguridad.

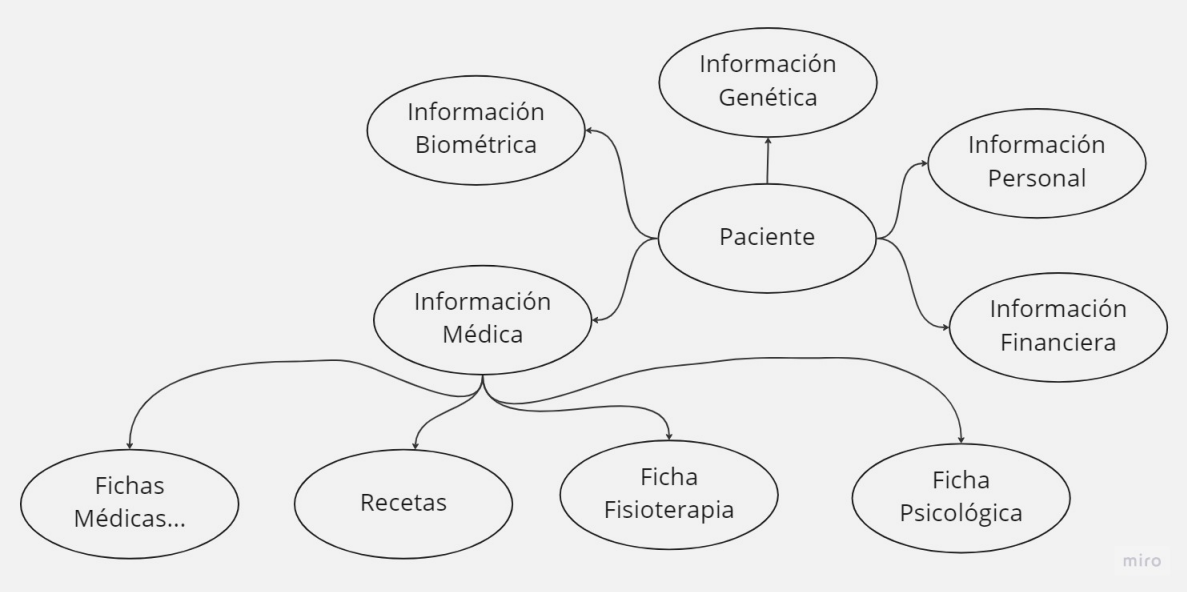


Figura 6: Tipos de datos asociados al paciente

4.4.1. Recolección de datos personales del paciente

Kinteractive recopila datos básicos de identificación, como nombre, apellido y RUT, con el fin de identificar adecuadamente a los pacientes en la plataforma.

4.4.2. Recolección de datos médicos del paciente

Además, se solicita información médica relevante, como edad, peso, estatura y condiciones médicas pertinentes, para facilitar el tratamiento del paciente por parte de los profesionales de la salud.

4.4.3. Recolección de datos financieros del paciente

La plataforma registra información financiera relacionada con el modelo de suscripción de Kinteractive, incluyendo métodos de pago, dirección y registros de transacciones económicas.
Estos procesos se llevan a cabo con un enfoque centrado en el paciente y garantizan el cumplimiento de las regulaciones de privacidad y seguridad de datos.

4.5. Derechos de los Usuarios y Procedimientos de Ejercicio

En esta fase, se abordan aspectos fundamentales relacionados con la protección de los datos personales de los usuarios y los procedimientos disponibles para garantizar el ejercicio efectivo de sus derechos. Se centra en establecer una base sólida para la protección de

la privacidad y la transparencia en el manejo de los datos personales por parte de la empresa.

En primer lugar, se tiene que definir claramente los derechos que tienen los usuarios sobre sus datos personales. Esto incluye derechos reconocidos por la regulación, como el derecho de acceso, rectificación, cancelación, oposición y portabilidad de datos (Ley de Protección de Datos Personales en Europa o GDPR, Derechos ARCOP). Estos derechos garantizan que los usuarios tengan control sobre sus datos personales y puedan tomar decisiones informadas sobre su uso y procesamiento.

Es importante que los usuarios sepan cómo comunicarse con la empresa y que cuenten con canales efectivos para resolver cualquier inquietud o problema relacionado con la privacidad de sus datos personales. A continuación se describen los procedimientos que debe ofrecer la organización para asegurar un correcto tratamiento de datos y así poder tener una política de privacidad que sea sustentable en el tiempo:

Derecho de Acceso

Este derecho otorga a los individuos la facultad de solicitar información sobre los datos personales que una organización tiene sobre ellos. Las personas pueden solicitar conocer qué datos personales se están procesando, con qué propósito se utilizan, y quién más tiene acceso a esa información. Esencialmente, les permite a los individuos confirmar si sus datos están siendo tratados legalmente y de manera transparente por una organización.

Se debe establecer un procedimiento claro mediante el cual los usuarios puedan solicitar acceso a sus datos personales que están siendo procesados por la empresa. Esto puede incluir la creación de un formulario en línea o un mecanismo de solicitud por correo electrónico, donde los usuarios puedan proporcionar la información necesaria para verificar su identidad y especificar qué datos desean acceder.

Los usuarios deben poder realizar el siguiente procedimiento:

1. Completar un formulario de solicitud de acceso a datos personales disponible en el sitio web de la empresa.
2. Proporcionar la información requerida para verificar su identidad, como nombre completo, dirección de correo electrónico y número de identificación.
3. Especificar los datos personales a los que desea acceder.
4. Envíe el formulario completado junto con una copia de su documento de identificación válido por correo electrónico a la dirección designada para solicitudes de datos personales.

Derecho de Rectificación

Este derecho permite a las personas corregir o modificar los datos personales que son inexactos o incompletos. Si un individuo encuentra que la información que la organización tiene sobre ellos es incorrecta, desactualizada o está incompleta, puede solicitar que se rectifiquen esos datos para garantizar que la información sea precisa y esté actualizada.

Para permitir a los usuarios corregir cualquier inexactitud o incompletitud en sus datos personales, se establece el siguiente proceso mediante el cual podrán solicitar la rectificación de sus datos:

1. Complete el formulario de rectificación de datos personales disponible en el sitio web de la empresa.
2. Indique claramente qué información es incorrecta y proporcione los detalles correctos.
3. Proporcione la información necesaria para verificar su identidad.
4. Envíe el formulario completado junto con una copia de su documento de identificación válido por correo electrónico a la dirección designada para solicitudes de rectificación de datos personales.

Derecho de Cancelación (Derecho al Olvido)

El derecho de cancelación, también conocido como derecho al olvido, permite a los individuos solicitar la eliminación de sus datos personales de los sistemas de una organización. Este derecho es especialmente relevante cuando los datos ya no son necesarios para los fines para los cuales fueron recopilados, si se ha revocado el consentimiento para su procesamiento, o si el tratamiento de los datos no cumple con las disposiciones legales.

Se debe establecer un procedimiento claro para que los usuarios puedan solicitar la cancelación de sus datos, que incluya la verificación de su identidad y la evaluación de si existen motivos legales para retener los datos:

1. Envíe una solicitud de cancelación de datos por correo electrónico a la dirección designada para solicitudes de cancelación de datos personales.
2. Proporcione la información necesaria para verificar su identidad, como nombre completo y dirección de correo electrónico asociada con su cuenta.
3. Espere la confirmación de recepción de su solicitud y la verificación de su identidad por parte del equipo de privacidad de la empresa.
4. Una vez verificada su identidad, sus datos personales serán eliminados de manera segura de todos los sistemas de la empresa en los plazos indicados según la regulación.

Derecho de Oposición

El derecho de oposición permite a los individuos oponerse al procesamiento de sus datos personales en determinadas circunstancias, como cuando el procesamiento se lleva a cabo para fines de mercadotecnia directa o cuando el tratamiento de los datos es incompatible con los fines originales para los cuales fueron recopilados.

Se establece el siguiente procedimiento para que los usuarios puedan ejercer este derecho, que incluya la presentación de una solicitud que explique los motivos de la objeción y la verificación de la identidad del usuario:

1. Completar el formulario de objeción al procesamiento de datos personales disponible en el sitio web de la empresa.
2. Especifique claramente los motivos de su objeción al procesamiento de sus datos personales en caso de que aplique.
3. Proporcionar la información necesaria para verificar su identidad.
4. Envíe el formulario completado junto con una copia de su documento de identificación válido por correo electrónico a la dirección designada para objeciones al procesamiento de datos personales.

Derecho a la Portabilidad de Datos

Este derecho otorga a los individuos la capacidad de solicitar y recibir sus datos personales en un formato estructurado, de uso común y legible por máquina, y en algunos casos, transmitir esos datos a otro responsable del tratamiento sin impedimentos por parte del responsable al que se los proporcionaron inicialmente. Este derecho facilita la movilidad de los datos entre diferentes proveedores de servicios y promueve la competencia entre proveedores al otorgar a los individuos un mayor control sobre sus datos.

Se establece el siguiente procedimiento para que los usuarios soliciten la portabilidad de sus datos, que incluya la verificación de su identidad y la provisión de los datos en el formato solicitado.

1. Enviar una solicitud de portabilidad de datos por correo electrónico a la dirección designada para solicitudes de portabilidad de datos personales.
2. Especificar el formato en el que desea recibir sus datos personales y la dirección a la que deben ser enviados.
3. Proporcionar la información necesaria para verificar su identidad, como nombre completo y dirección de correo electrónico asociada con su cuenta.
4. Una vez verificada su identidad, sus datos personales serán proporcionados en el formato solicitado el plazo indicado por la regulación.

Además de establecer estos derechos, es importante detallar los procedimientos disponibles para que los usuarios ejerzan dichos derechos. Esto puede incluir la implementación de un formulario o mecanismo específico para solicitar el acceso, rectificación o eliminación de datos personales, así como los plazos y procesos internos para responder a estas solicitudes. Es fundamental que estos procedimientos sean claros, accesibles y efectivos para garantizar que los usuarios puedan ejercer sus derechos de manera sencilla y sin obstáculos.

Asimismo, se debe proporcionar información sobre cómo contactar a la empresa en caso de dudas o reclamaciones relacionadas con la protección de datos. Esto puede incluir la designación de un encargado de protección de datos o un departamento específico dentro de la empresa responsable de atender las consultas y reclamaciones de los usuarios.

Estos procedimientos deben ser claramente comunicados a los usuarios a través de la política de privacidad de la empresa y otros medios de comunicación apropiados. Además, es importante que la empresa cuente con mecanismos internos para procesar estas solicitudes de manera oportuna y efectiva, asegurando el cumplimiento de los derechos de privacidad de los usuarios en todo momento.

Es fundamental establecer una base sólida de protección de datos y transparencia en el manejo de la información personal. Al definir claramente los derechos de los usuarios y los procedimientos disponibles para ejercer dichos derechos, se garantiza que los usuarios tengan control sobre sus datos personales y puedan confiar en que sus derechos serán respetados por la empresa.

4.6. Uso de Generative AI

La solución cuenta con una serie de componentes que en conjunto cumplen con el objetivo de generar una política de privacidad para la organización. Para poder llevar esto a cabo, se hará uso de inteligencia artificial generativa para el análisis de los datos personales en el ambiente de la organización y para el análisis de las regulaciones con las que tiene que cumplir la misma. Esto permitirá un chequeo continuo por parte de la organización sobre sus políticas de privacidad y de tratamiento de datos, teniendo en cuenta las regulaciones que apliquen.

Se usarán tres modelos de procesamiento de lenguaje desarrollados por Open AI para analizar los conjuntos de datos, estos son GPT-4o, GPT-4 y GPT-4 turbo. Estos *Large Language Models (LLM)* serán la herramienta central para el análisis de datos, ya que estos "están diseñados para entender y completar tareas relacionadas a información personal y geográfica, tales como determinar ubicaciones geográficas relacionadas a un número de teléfono o responder donde se ubica una institución educacional en una respuesta y sin buscar información en internet" [OpenAI *et al.*, 2023].

Adicionalmente, se analizan los casos que describe la documentación del modelo para

entender como usar mejor las capacidades que tiene en la compresión de textos y ajustar como interactúa con otros sistemas, tales como la información que se le enviará. Dichos procesos tienen en cuenta el manejo de información sensible, por lo que este servicios de LLMs tienen procesos seguros por diseño, en los cuales se limitan las tareas que puede realizar, a identificar que tipo de información no puede ser revelada o compartida y rechazar tipos de solicitudes específicas, entre otros lineamientos.

Parte de las consideraciones a tener, es que la solución actuará como un fuerte primer indicador sobre que datos existen en los diferentes repositorios, sin embargo es necesario cierto grado de revisión no automatizable ya que estos modelos de lenguaje pueden producir resultados y salidas con información ficticia o errónea, también conocidos como alucinaciones.

En cuanto a los datos personales que maneja la organización, se tiene un proceso que entrega contexto al LLM y posteriormente se le entrega un conjunto de datos a analizar. Este proceso se lleva a cabo dentro de los activos de datos de la organización. Los activos de datos de la organización son todos los sistemas que cuentan con información de los diferentes tipos de usuarios como pueden ser empleados, clientes, usuarios finales, pacientes, entre otros. Al analizar estos activos de datos, se puede tener una imagen completa de que datos personales maneja la organización y en que sistemas específicamente, esto permite un fácil mapeo de los datos dentro de los procesos que realiza Kinteractive.

Al poder llevar una detallada documentación sobre los procesos que realiza Kinteractive con los datos de los pacientes y tener de manera continua un detalle de la información manejada, se puede dar cumplimiento continuo ante las regulaciones a las que tiene que atender Kinteractive, específicamente las leyes chilenas definidas previamente y la regulación HIPAA.

El uso de inteligencia artificial (IA) en el proceso de análisis de datos proporciona una serie de ventajas significativas en comparación con la definición de reglas estáticas. En primer lugar, la IA permite obtener resultados más precisos y adaptables a los cambios dinámicos en la estructura de los datos. Esto es especialmente relevante en entornos donde la información puede variar en términos de formato, como en bases de datos relacionales o archivos tabulados. [Rouhiainen, 2022]

El flujo de procesamiento de datos propuesto consta de varias etapas clave para garantizar la eficacia y la seguridad del proceso. En primer lugar, la recolección de datos implica la extracción de muestras de información de los repositorios pertinentes, ya sean bases de datos relacionales o archivos tabulados en formato csv. Esta etapa es crucial para garantizar que la muestra de datos sea representativa y adecuada para el análisis.

Una vez recopilados los datos, se procede al mapeo de datos, donde se asigna un contexto a la información para facilitar su procesamiento posterior. Es importante proporcionar al procesador de datos el contexto necesario para comprender el alcance y la naturaleza de la información que se está analizando.

Finalmente, se envía la solicitud al modelo y se adapta la respuesta obtenida del modelo, segmentando los datos identificados según su sensibilidad y categoría. Esto permite tener un proceso automatizado que puede detectar cambios en la estructura de las bases de datos o archivos tabulados y adaptarse en consecuencia.

4.7. Diagrama de flujo

En el ámbito de la gestión y la planificación, la visualización de procesos es fundamental para comprender cómo funciona una serie de actividades relacionadas. El siguiente diagrama de flujo describe el proceso que sigue la solución para poder obtener los tipos de datos personales manejados por la organización, considerando desde el inicio cuando se obtienen datos de un sistema de origen, hasta el final del proceso cuando se analizan los resultados y se realizan cambios basados en los hallazgos, para cumplir con un plan de mejora continua.

El diagrama de la figura 7 describe los pasos a seguir dentro de este proceso para identificar posibles cuellos de botella, puntos donde se realicen tareas redundantes o donde se duplique información. Cabe destacar que para casos más complejos y en producción de una organización, es necesario contar con una serie de mecanismos de emergencia y flujos alternos que puedan recuperar el estado del sistema en el caso de que exista un error en alguno de los procesos.

Adicionalmente, el objetivo de los flujos alternativos es extender el dominio de la solución. Para casos donde sea necesario tomar decisiones en base a los datos encontrados, se analiza la salida del proceso de “Procesamiento de datos IA” y este se pasa a “Adaptar respuesta” o al flujo que corresponda al caso identificado.

4.8. Implementación propuesta

Para implementar una solución a los requerimientos definidos se modeló en base a la política de privacidad de la organización, la cual será la primera herramienta que protege los derechos de datos de los pacientes de Kinteractive. La política de privacidad se genera en bases a las regulaciones que se le dan como entrada y una serie de estructuras que representan el dominio de los datos manejados en cada proceso que realiza la organización con los datos de los pacientes.

Específicamente se tiene un orden jerárquico descrito en la figura 8, donde la política de privacidad tiene mapas de datos de los procesos documentados, los procesos tienen activos de datos asociados a ellos y cada activo de datos tiene un conjunto de diferentes tipos de datos, tanto personales como no personales. Por último, se hace una última clase que es categoría de datos, la cual permite agrupar los diferentes tipos de datos.

El modelo descrito corresponde al sistema de gestión y como se realizará el mapa de los datos para dar cumplimiento con el artículo 30 de la ley de protección de datos europea (GDPR), el

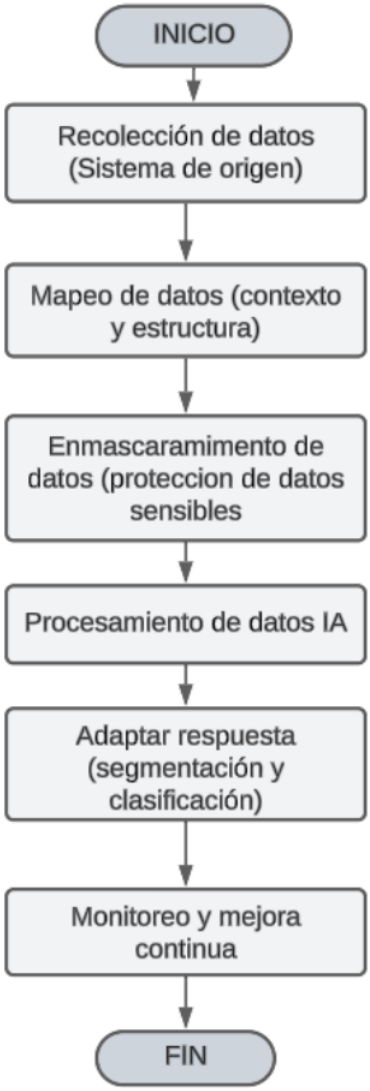


Figura 7: Diagrama de flujo de proceso

estándar para la documentación de procesamiento de datos. En cuanto a los datos sensibles que maneja el sistema y las regulaciones que se deben validar, se muestra a continuación el detalle de la evaluación realizada.

4.9. Proceso de análisis de información y datos personales

Kinteractive realiza procesos de captura de información de pacientes, los cuales son almacenados en bases de datos de la organización. Para llevar a cabo un debido proceso de tratamiento de datos es necesario seguir un plan robusto, este debe especificar las acciones y procesos que se harán con la información de los pacientes, especialmente cuidando aquella definida como sensible.

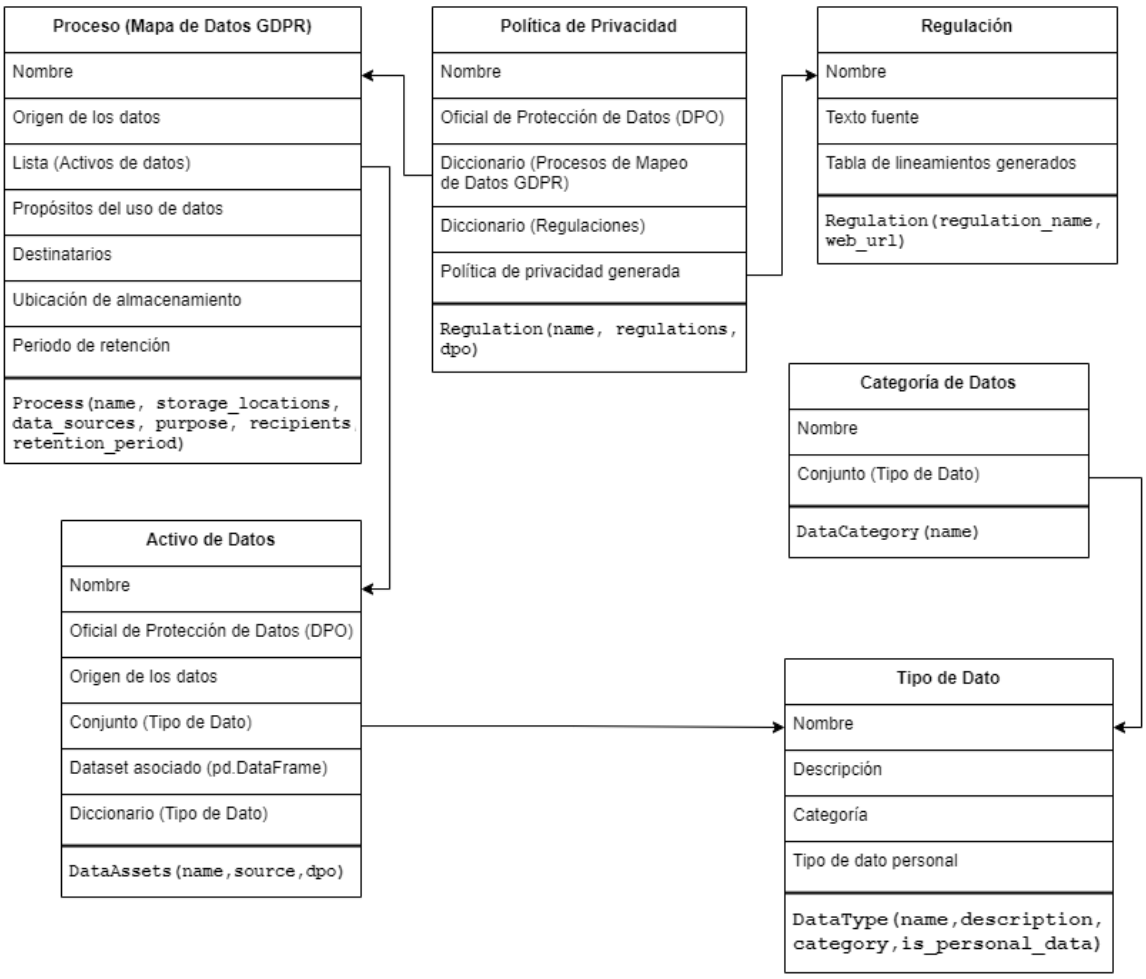


Figura 8: Diagrama de las clases implementadas, sus atributos y relaciones

Para categorizar la información se realiza el siguiente procedimiento, que incluye desde la etapa inicial de recolección de datos, pasando por el uso de *LLMs* para análisis, y terminando en la entrega de la respuesta.

4.9.1. Recolección de datos

En esta etapa, se recopilan datos desde el sistema de origen. La mayoría de los activos de datos son sistemas como bases de datos relacionales, archivos tabulados y otras fuentes de datos estructurados. La recolección puede realizarse mediante consultas a bases de datos, extracción de archivos CSV, o cualquier otro método de acceso a los datos disponibles. Los datos recopilados pueden incluir información como nombres, fechas, números de identificación y otros datos relevantes para el análisis.

Se recomienda utilizar métodos seguros para la extracción de datos y asegurarse de asignar los permisos adecuados para manejar el acceso a la información. Adicionalmente, es necesario verificar la legalidad y ética de la recolección de datos, evitando la obtención de información sin consentimiento o en violación de las regulaciones de privacidad que apliquen.

Se deja propuesta una extensión de este desarrollo, ya que este principio es aplicable para otros sistemas de datos, como bases de datos relacionales y tecnologías usadas a nivel empresarial. En general se pueden desarrollar conexiones a dichos sistemas u orquestar la exportación y envío de esta información a sistemas que funcionen como repositorio de datos y posteriormente usar la solución sobre este repositorio consolidado.

4.9.2. Mapeo de Datos

Después de la recolección, los datos se someten a un proceso de mapeo donde se asigna un contexto y una estructura a los datos recopilados. Esto implica comprender la naturaleza de los datos y cómo se relacionan entre sí. Por ejemplo, en una base de datos de pacientes, los datos pueden incluir información médica, como diagnósticos, tratamientos y resultados de exámenes, así como información demográfica como edad, género y ubicación.

Se debe realizar un proceso de documentación de los detalles del proceso de mapeo, incluyendo la estructura de los datos y cualquier transformación realizada. El proceso debe asegurarse de mantener la integridad y confidencialidad de los datos durante el proceso de mapeo, evitando la pérdida o divulgación no autorizada de información sensible.

4.9.3. Enmascaramiento de Datos

Dependiendo de la forma en la que opera la organización (*B2B*, *B2C*, *etc*), la cantidad de datos personales que maneja y que tipo de información sensible contiene, se debe

considerar una componente dentro del sistema que funcione como capa adicional de seguridad para mantener la privacidad de los datos.

Para aplicar un enmascaramiento de datos es necesario tener conocimiento previo de que tipo de dato se desea ocultar y donde se ubican dentro del ambiente de datos. Una vez determinado esto, se puede aplicar un algoritmo para realizar la tarea, por ejemplo, cambiar el tipo de dato personal “Apellido” por otro Apellido. Cabe destacar que el proceso de enmascaramiento sería necesario cuando se envía información sensible vinculada a una identidad.

Dependiendo del uso de los datos se puede considerar un procesos de enmascaramiento reversible o irreversible.

- Para procesos internos se puede manejar información enmascarada de manera reversible, ya que permite obtener información verídica al momento de tener que mostrar cumplimiento con regulaciones, que sea necesario corroborar la información para una auditoría general o por un caso específico.
- Para procesos de traspaso de información fuera de la organización, se recomienda que el enmascaramiento de datos sea irreversible para garantizar la seguridad de la información.

Dado que Kinteractive hará uso de los datos de manera aislada, es decir, se enviarán subconjuntos de los datos de manera que solo sean un tipo de dato y no información personal vinculada a una identidad, no sería necesario aplicar un proceso de enmascaramiento en el estado actual del sistema.

4.9.4. Análisis de los datos con uso de inteligencia artificial

El uso de inteligencia artificial permite un proceso que identifica la información sensible en el ambiente de datos de la organización y toma en cuenta los diferentes contextos en los que la organización obtiene y recolecta datos. Para un mejor uso de la tecnología, se trabajó específicamente con LLMs y se implementaron medidas para aumentar la tasa de efectividad con la que detecta la información sensible que se le programa para identificar. En particular estos modelos funcionan mejor cuando es posible establecer un contexto de manera previa [Jain, Shrey *et al.*, 2023] , para esto la solución implementa una componente donde se establece dicho contexto para cada una de los diferentes procesos en los que se le pide completar una tarea al modelo.

El proceso a realizar en la solución consta de 2 partes:

1. Establecer contexto: se define un conjunto de indicaciones o “prompts” que describan la tarea que debe realizar, bajo que especificaciones hacer el análisis y que tipo de formato se espera como respuesta. Dado que estos modelos se encuentran en constante mejora, se propone una serie de lineamientos a indicar como contexto, que pueden

ser modificados en forma y fondo para ajustarse mejor a la tarea que se desea realizar y en el ámbito específico que se desea analizar, adicionalmente, se pueden segmentar estas indicaciones en subtareas más específicas y comparar el rendimiento y resultados. Los lineamientos y contexto propuestos para dar al LLM son:

a) Su tarea es analizar un conjunto de datos y responder a las preguntas específicas que se hagan sobre estos datos.

b) El conjunto de datos se entrega mediante un *string* que contiene palabras separadas por ; (punto y coma).

c) Use este conjunto de datos para determinar que tipo de información personal contiene.

d) Considere el ámbito específico a la regulación indicada y el tipo de información personal que cubre.

e) Retorne la respuesta en un formato específico. Solo retorne el nombre del tipo de dato determinado

2. Obtener respuesta: Una vez indicado el contexto, se envía el conjunto de datos según el formato indicado y se obtiene la respuesta para el caso específico consultado.

Este proceso es realizado sobre los activos de datos que maneja la organización, para este trabajo se usa información almacenada en formato .csv. El alcance de la información a analizar consta de datos personales almacenados en un formato tabulado que permita ajustar la entrada que se da al modelo.

Se asume que cada activo de datos dentro de este ambiente será un archivo con información potencialmente sensible, para cada tabla se analiza los datos de cada columna. Por ejemplo, para una columna con el tipo de dato “Apellido”, se envía al LLM un string del tipo “Apellido1;Apellido2;...”. Los datos preparados son analizados por el LLM según el contexto indicado y retorna el tipo de dato que detectó.

4.9.5. Adaptar Respuesta

Finalmente, se segmentan y clasifican los datos identificados según su sensibilidad y categoría. Esto permite una respuesta adaptada a los datos procesados, lo que facilita su uso posterior según las necesidades específicas del proyecto o aplicación. Por ejemplo, los datos sensibles pueden ser clasificados como información médica confidencial y tratados con medidas de seguridad adicionales, mientras que los datos no sensibles pueden utilizarse de manera más abierta para análisis y visualización.

Entre los lineamientos a seguir para generar la respuesta están:

- Definir criterios claros para la segmentación y clasificación de datos.

- Mantener actualizados los procedimientos mediantes los que se establece el contexto del LLM.
- Realizar un monitoreo continuo sobre los cambios en la sensibilidad de los datos y ajustar los criterios de segmentación en consecuencia para mantener la precisión de la respuesta.

4.9.6. Monitoreo y Mejora Continua

Se establecen mecanismos de monitoreo para seguir de cerca el rendimiento del sistema y detectar posibles problemas o áreas de mejora. Se realizan ajustes y actualizaciones periódicas para garantizar que el sistema siga cumpliendo con los objetivos y requisitos de la organización.

Se propone un proceso adicional para futuras implementaciones, donde se aplica la mejora continua sobre la seguridad de los datos personales. Se sugiere realizar un programa de protección de datos transversal en los ambientes de desarrollo, pruebas, control de calidad (QC) y producción. Además del ambiente de producción que mantienen las organizaciones, es usual tener múltiples ambientes replicados para diferentes propósitos, como los mencionados anteriormente.

Los ambientes de la organización como Desarrollo y QA, son en algunos casos más vulnerables que los sistemas de producción, por lo mismo es una vía de entrada para ataques maliciosos. [Agencia Española de Protección de Datos, 2022] Esto se da en algunas organizaciones porque al ser ambientes que no deberían estar expuestos a redes externas, o que son ambientes locales controlados, entre otras razones, se dejan sin procedimientos de seguridad adecuados, como todos los mecanismos que tendrían en producción para acceder a la información sensible.

El programa debe seguir, describir y promover lineamientos tal que:

1. Se usen datos anonimizados en el caso de representar conjuntos de información identificable. Para datos personales de carácter sensible, como lo puede ser un resultado médico, se tiene que eliminar, tokenizar o enmascarar la identidad del sujeto de datos representado en ese activo de datos.
   Para conjuntos de datos que por si solos no tienen o muestran un vínculo a un sujeto de datos, como el nombre o número de cédula de identidad, no es necesario realizar este proceso.

   Es necesario tener un mapa de los datos de carácter personal y que identifiquen al sujeto de datos para poder tener visión de donde es necesario realizar este proceso y sobre que datos exactamente, ya que una vez se altera o remueve la identidad, los datos personales sensibles pasan a ser solo datos, no vinculantes con ningún sujeto de datos.

2. Incorporar proceso de eliminación de datos que sean robustos tanto en producción, como en los demás ambientes. Esto permite garantizar a los sujetos de datos que su información personal será eliminada de todos los ambientes de la organización y no solo el de producción.
   Ya que estos ambientes pueden ser replicados múltiples veces y usados para diferentes propósitos tales como marketing, procesos de entrega de productos, venta y similares, pueden existir múltiples instancias donde existe información personal como correos electrónicos y números de teléfonos. Para esto es necesario poder buscar dicha información y eliminarla cuando los usuarios ejerzan sus derechos de eliminación sobre los datos, garantizando que no quedaron almacenados en ningún repositorio de la organización.

Se recomienda además establecer métricas de desempeño y realizar auditorías periódicas para evaluar la eficacia y eficiencia del proceso. Esto permite estar preparado para realizar ajustes y mejoras en el flujo de datos según sea necesario para adaptarse a cambios en los requisitos del proyecto o las condiciones del entorno.

4.10. Flujo de trabajo del sistema de gestión

La solución propuesta mediante el Sistema de Gestión es fundamental para asegurar el cumplimiento de las regulaciones de privacidad de datos y garantizar la protección de la información personal y privada de los pacientes. Este sistema no solo se encarga de generar un documento de Política de Privacidad, sino que también despliega un conjunto de procesos y prácticas que aseguran la integridad y confidencialidad de los datos sensibles.

El Sistema de Gestión es una plataforma integral que abarca desde la recopilación inicial de datos hasta su almacenamiento, uso y procesamiento, proporcionando una visión completa y detallada de cómo se manejan los datos en toda la organización. Además de documentar los procedimientos, la Política de Privacidad establece pautas claras sobre el acceso a la información, los controles de seguridad implementados y los protocolos de respuesta ante posibles incidentes de seguridad.

En este sentido, la Política de Privacidad no solo es un documento estático, sino que representa un compromiso continuo con la protección de la privacidad de los pacientes. Se actualiza y adapta de manera regular para reflejar los cambios en las regulaciones y en el entorno operativo de la organización. Esto asegura que Kinteractive esté siempre alineado con las mejores prácticas en materia de privacidad de datos y que sus procesos cumplan con los más altos estándares de seguridad y confidencialidad.

4.10.1. Selección y análisis de las regulaciones

La selección y análisis de las regulaciones es un paso crítico en el diseño del Sistema de Gestión de Privacidad de Datos de Kinteractive, especialmente considerando su ámbito

de telemedicina a través de una aplicación móvil. En este contexto, se han identificado varias regulaciones relevantes que deben ser consideradas para garantizar el cumplimiento adecuado y la protección de los datos sensibles de los pacientes.

En primer lugar, se han tomado en cuenta las leyes chilenas pertinentes, específicamente la Ley 21096 y la Ley 19628. Estas leyes establecen normativas clave relacionadas con la privacidad de datos y la protección de la información personal en el ámbito de la salud. Al incorporar estas regulaciones en el análisis inicial, Kinteractive demuestra su compromiso con el cumplimiento legal en el contexto nacional.

Además de las leyes chilenas, se ha reconocido la importancia de adherirse a estándares internacionales de privacidad de datos, en particular la regulación estadounidense conocida como HIPAA (Ley de Portabilidad y Responsabilidad del Seguro de Salud). Al adoptar HIPAA como un lineamiento principal, Kinteractive se posiciona para cumplir con los estándares más rigurosos en cuanto a la protección de datos de salud, asegurando así el derecho a la privacidad de cada paciente cuya información se maneja en sus sistemas.

Cumplir con la regulación HIPAA implica más que simplemente implementar políticas y procedimientos. También implica garantizar que los pacientes estén plenamente informados sobre cómo se utilizarán sus datos personales y sensibles. En este sentido, generar una Política de Privacidad detallada y accesible se convierte en un componente fundamental del Sistema de Gestión, ya que proporciona transparencia y claridad sobre el manejo de datos, fortaleciendo así la confianza y la protección de la privacidad de los pacientes.

4.10.2. Definición y extracción de datos considerados

La definición y extracción de datos considerados implica un análisis exhaustivo de los tipos de datos que se manejan en el contexto de las regulaciones mencionadas. Dado que estas regulaciones no proporcionan una lista exhaustiva de los tipos de datos sensibles que deben protegerse, es fundamental desarrollar un proceso para identificar y categorizar adecuadamente las características que cumple un dato para ser considerado sensible.

Para abordar esta tarea, se propone un enfoque híbrido que combina la capacidad de análisis de la inteligencia artificial con la validación humana. En este sentido, se hará uso de modelos de inteligencia artificial para realizar un análisis inicial de las regulaciones y generar lineamientos específicos que la organización debe seguir para estar en cumplimiento con dichas regulaciones.

Dado que el ambiente en el que se maneja la información sensible, los datos personales y los bienes digitales en general, es necesario poder adaptar estos procesos a un mapa de la organización donde se tenga claro e tipo de información que se maneja, su propósito, políticas de retención, entre otras características. Adicionalmente, para validar que se cumplen las necesidades específicas de la organización, se requerirá la validación por parte del usuario del sistema. Este proceso de validación permitirá ajustar y refinar la definición

de datos sensibles de acuerdo con las particularidades del caso de uso de la organización.

En resumen, la definición y extracción de datos considerados implica un enfoque colaborativo entre la inteligencia artificial y el conocimiento humano, asegurando así una identificación precisa y completa de los datos sensibles que deben protegerse según las regulaciones pertinentes. Este enfoque híbrido garantiza que requerimientos son levantados de manera adecuada y que se adapten a las necesidades específicas de Kinteractive.

4.10.3. Selección de Repositorios de Datos

La selección de los repositorios de datos ayuda a que se analicen únicamente aquellos que contienen información relevante para el cumplimiento de las regulaciones de privacidad de datos, en este caso, los datos personales de los pacientes. Dado que una organización como Kinteractive maneja una amplia variedad de datos que van más allá de los datos de los pacientes, es fundamental delimitar el alcance del análisis y centrarse en los repositorios que contienen información sensible.

Kinteractive ha adoptado una estrategia de segmentación de la información, lo que significa que ha organizado sus datos de manera que puede distinguir claramente dónde se encuentran los datos relacionados con los pacientes y dónde están los datos no relacionados con ellos, como los datos internos referentes a proyectos, empleados, infraestructura, comerciales, entre otros.

Esta segmentación permite a Kinteractive tener un mayor control sobre qué repositorios de datos deben ser analizados en el contexto de la privacidad de datos. Al separar los datos de los pacientes de otros tipos de datos, la organización puede identificar con precisión los repositorios que representan un riesgo potencial de fuga de información personal y, por lo tanto, deben ser objeto de análisis detallado.

4.10.4. Descubrimiento de datos sensibles en los repositorios

El descubrimiento de datos sensibles en los repositorios permite identificar y proteger adecuadamente la información que requiere un tratamiento especial en términos de privacidad y seguridad. Para llevar a cabo esta tarea de manera efectiva, se hará uso de modelos de inteligencia artificial.

El uso de los LLMs y *generativa AI* permite tomar una muestra representativa de los repositorios de datos y analizar el contenido de estos para determinar qué tipo de datos se está manejando. Esto incluye identificar datos personales como nombres, direcciones, números de identificación, información médica, entre otros, que están sujetos a regulaciones específicas de privacidad y protección de datos.

En el proceso definido en la sección 4.4, se establece cómo se obtienen y procesan los datos manejados por Kinteractive, lo que proporciona la base para identificar los datos

sensibles en los repositorios de datos. Esta metodología garantiza que se aborden de manera exhaustiva todos los aspectos relevantes para la protección de la privacidad de los datos.

Es importante destacar que, para validar la certeza de los resultados obtenidos por Open AI, se propone realizar una comparación con datos previamente clasificados. Esta validación cruzada asegura la precisión y la fiabilidad del proceso de determinación de datos sensibles, lo que permite a Kinteractive tomar medidas adecuadas para proteger la información y cumplir con las regulaciones de privacidad de datos de manera efectiva.

4.10.5. Generar la propuesta de política de privacidad

Generar un borrador de política de privacidad es un paso crucial para garantizar que Kinteractive cumpla con las regulaciones de privacidad de datos y proteja adecuadamente la información sensible de sus usuarios. Para llevar a cabo este proceso de manera efectiva, se han establecido directrices claras que permiten adaptar la política de privacidad a las actividades y procesos específicos de la organización.

En primer lugar, se reconoce que Kinteractive realiza actividades estándar de manera continua como parte de sus operaciones comerciales. Estas actividades, que involucran la recopilación, el uso y el procesamiento de datos personales, son esenciales para el funcionamiento del negocio. Por lo tanto, se pueden definir de manera estática en la política de privacidad, lo que garantiza que se aborden de manera adecuada y consistente en todos los casos.

Además, se reconoce que Kinteractive está en constante evolución como negocio, lo que puede implicar la incorporación de nuevas actividades y procesos, así como la eliminación de aquellos que ya no son relevantes. Por lo tanto, la política de privacidad debe ser lo suficientemente flexible para adaptarse a estos cambios y garantizar que la información crucial y relevante se aborde de manera efectiva en todo momento.

Estas directrices permiten mantener una política de privacidad precisa y acotada, evitando la inclusión de actividades innecesarias que podrían llevar a una política exhaustiva y poco práctica. Además, fomentan una revisión continua de los procesos de la organización para garantizar que la política de privacidad esté siempre actualizada y en cumplimiento con las regulaciones aplicables.

En general, el proceso para generar un borrador de política de privacidad en Kinteractive se basa en la identificación de actividades estándar y en la flexibilidad para adaptarse a los cambios en el negocio, lo que garantiza una protección efectiva de la privacidad de los datos de los usuarios y el cumplimiento con las regulaciones pertinentes.

4.11. Ciclo de Vida de los Datos

El ciclo de vida de los datos representa la serie de procesos por los cuales pasa la información obtenida de una persona a través de un sistema digital y los lineamientos seguidos para realizar estos procesos. En general se espera que el manejo del ciclo de vida del dato sea un mecanismo bajo el cual se cumplen reglamentos específicos en la recolección, almacenado, uso y destrucción de estos.

La administración de este ciclo de vida permite a las organizaciones entender los puntos críticos de los procesos y como afectan a sus usuarios y clientes. Para esto, se tomará el modelo en [Scope, 2021] que describe las fases del ciclo de vida (ver figura 9) y en qué consisten.



Figura 9: Fases del ciclo de vida de los datos [Scope, 2021]

4.11.1. Creación

Es la etapa en los procesos de la organización donde se da origen a nuevos datos de usuarios que serán almacenados y trabajados en los sistemas digitales. Gracias a las características de la información a almacenar, es necesario que desde esta etapa del ciclo se consideren los lineamientos de las regulaciones.

En particular, Techneworks realiza un proceso de creación de datos a través de la aplicación Kinteractive durante el proceso denominado como “Registro de paciente”, donde se enrola por primera vez a un paciente en el sistema y sus datos, específicamente:

- Nombres
- Apellidos
- Estatura
- Peso
- Email
- R.U.T

4.11.2. Almacenado

Una vez obtenidos los datos desde el proceso de creación, estos necesitan ser almacenados en una base de datos que cumpla con características de seguridad y políticas tales que:

- Se pueda ver con detalle a quien pertenece la información y vincularla a cualquier otra instancia de información existente de esta persona. Es decir si se cuenta con información de la misma persona en múltiples sistemas, es necesario que esta persona

comparta un identificador universal entre los múltiples sistemas para poder vincular toda la información que se encuentra distribuida.

- Se pueda definir exactamente que usuarios pueden acceder a esta información sea por un proceso basado en roles o en usuarios. Se necesita para esto dejar claramente establecido los usuarios con acceso a datos y que nivel de acceso tienen, en particular se busca segmentar la información a la que pueden acceder según las funciones que cumplen dentro de la organización.

  Cabe destacar que este proceso de almacenado necesita consentimiento inicialmente por parte del paciente, y solo es válido por el periodo de retención necesario para resguardar información personal, sensible y médica según HIPAA.

- Se pueda definir en qué contexto se puede acceder a la información, como por ejemplo, ver información financiera al momento de registrar un pago o ver información del paciente durante una consulta, pero no permitir que esta información sea accesible sin un motivo que lo justifique para cumplir con la regulación.

Al contar con estas tres características sobre un conjunto de datos, se pueden establecer políticas que modelan el comportamiento del mundo real y que permitan actuar con seguridad sobre la información, manteniendo la integridad y privacidad del paciente.

4.11.3. Uso

El uso de los datos queda definido por las políticas de la organización y debe ser seguido por los sistemas que trabajan la información, entre los procesos que realiza Kinteractive con la información que maneja están:

- Almacenado de datos al momento de registrar un paciente.
- Visualización de información del paciente cuando un kinesiólogo necesita ver su perfil.
- Modificación de datos almacenados por solicitud del paciente o kinesiólogo.

4.11.4. Archivado

El archivado consiste en almacenar información y datos que ya no son usados de manera activa en otro repositorio específico para datos de estas características, específicamente enfocado en la retención de los datos a largo plazo. Es necesario mantener esta información histórica ya que el paciente puede solicitar a la organización un reporte de la información que esta maneja de el, sin importar el propósito del paciente.

Adicionalmente, la regulación HIPAA establece que es necesario mantener los registros del paciente, comunicación e información relevante por un periodo de al menos 6 años. Por

lo mismo, es necesario un mecanismo bajo el cual paciente que es dado de alta, suspende su tratamiento, o abruptamente decide retirarse de la organización, igual mantenga su información dentro del sistema para propósitos de cumplimiento.

4.11.5. Destrucción

La información que cumpla con las condiciones adecuadas tras su periodo de archivado, serán eliminados siguiendo los lineamientos de HIPAA que cubren la información de salud protegida (PHI) electrónica. HIPAA requiere por cumplimiento que los datos sean destruidos adecuadamente, lo que implica borrar el disco utilizando productos de software o hardware para sobrescribir los medios con datos no sensibles; depurar, desmagnetizar o exponer los medios a un campo magnético fuerte para interrumpir los dominios magnéticos grabados; o destruir los medios mediante desintegración, pulverización, fundición, incineración o trituración.

4.12. Cultura Organizacional

La cultura organizacional es el conjunto de los valores, creencias, normas y prácticas compartidas que moldean el comportamiento y la mentalidad de los miembros de una organización. Esta influye en cómo interactúan los miembros entre ellos y con las partes interesadas externas, suele ser implícita, desarrollada a lo largo del tiempo, y puede reflejarse en la misión, visión, políticas y operaciones diarias de la organización.

Para poder definir mejor esta cultura, es necesario identificar como afecta el trabajo realizado por los empleados:

Valores y Prioridades: Los valores y prioridades fundamentales de una organización moldean su enfoque hacia la privacidad de datos. Si una organización prioriza la transparencia, la ética y la confianza del cliente, estos valores se impregnarán en sus prácticas e influirán en cómo se maneja la información.

Comportamiento de los Empleados: Una cultura organizacional sólida establece expectativas para el comportamiento de los empleados. En una organización con una cultura de privacidad robusta, los empleados tienen mayor atención con respecto a la protección de datos, adhiriéndose a las mejores prácticas y protocolos para asegurar el cumplimiento.

Comunicación y Capacitación: La cultura organizacional influye en cómo se llevan a cabo la comunicación y la capacitación. Una cultura que valora la mejora continua y el aprendizaje invertirá en programas de capacitación regular para mantener a los empleados actualizados sobre las últimas regulaciones y prácticas de privacidad de datos.

Toma de Decisiones: El proceso de toma de decisiones dentro de una organización está

profundamente influenciado por su cultura. Una cultura adecuada fomenta la de toma de decisiones ética considerando las implicaciones de privacidad en sus acciones, asegurando que la privacidad de los datos sea una parte fundamental de sus decisiones estratégicas y operativas.

Cultura Organizacional y Cumplimiento de HIPAA
La Ley de Portabilidad y Responsabilidad de Seguro de Salud (HIPAA) establece el estándar para proteger la información sensible del paciente. Las organizaciones que manejan información de salud protegida (PHI) deben asegurarse de que todas las medidas de seguridad físicas, de red y de procesos requeridas estén en su lugar y se sigan.

Dado el gran dominio que es necesario abarcar, es fundamental que dentro de la organización se vea el manejo de la privacidad como un pilar, y no como requisito adicional que hay que cumplir. Para cumplir con esta visión, se propone que la organización defina un código de ética y conducta que considere al menos:

Compromiso con la Privacidad: Valorar altamente la privacidad de los pacientes, de manera que la organización busque alinearse naturalmente con los requisitos de HIPAA. Esta cultura asegura que todos los empleados comprendan la importancia de proteger la PHI y estén comprometidos con mantener el cumplimiento.

Políticas y Procedimientos: Es necesario documentar los procesos que realiza la organización de manera clara y concisa, esto da paso a políticas que indiquen como hacer tratamiento de dichos datos adecuadamente. Las organizaciones con una cultura sólida de cumplimiento tienen políticas definidas para manejar la PHI y serán actualizadas regularmente para reflejar cambios en las regulaciones y mejores prácticas.

Capacitación y Concientización de los Empleados: Los programas continuos de capacitación y concientización son esenciales para el cumplimiento de HIPAA. Una cultura organizacional que enfatiza la importancia de la privacidad de datos asegurará que todos los empleados, desde los altos ejecutivos hasta los trabajadores de primera línea, estén bien capacitados y conscientes de sus responsabilidades bajo HIPAA.

Respuesta a Incidentes: Una cultura organizacional proactiva tendrá planes de respuesta a incidentes robustos. En caso de una violación de datos o cualquier otro incidente que involucre PHI, la organización estará preparada para responder rápida y efectivamente, minimizando el daño potencial y asegurando el cumplimiento con los requisitos de notificación de violaciones de HIPAA.

En general, la cultura organizacional juega un papel crucial en cómo se aborda y maneja la privacidad de datos dentro de una organización. Fomentando una lineamientos que valoren la privacidad del usuario, la ética y el cumplimiento, las organizaciones pueden crear un entorno donde los empleados estén motivados y equipados para proteger datos sensibles, asegurando la adhesión a regulaciones como HIPAA. Esto no solo ayuda a mantener

el cumplimiento, sino que también construye confianza con clientes y partes interesadas, contribuyendo en última instancia al éxito de la organización.

CAPÍTULO 5
VALIDACIÓN DE LA SOLUCIÓN

La solución planteada está compuesta múltiples elementos que buscan cubrir de manera comprensiva los requerimientos de la organización Kinteractive en su ambiente de datos específicos, este incluye datos de pacientes de tipo sensible, personal, financiero y médico. Adicionalmente, se busca estar en cumplimiento con las regulaciones establecidas anteriormente, que corresponden a la regulación HIPAA y las leyes Chilenas 19.628, 20.584, 21.096.

Se implementó un proceso de análisis de datos con LLMs que determina el tipo de dato sensible que representa una muestra de datos. Esto permite determinar los ambientes de datos más sensibles y que uso de información necesita ser monitoreada según el origen y sensibilidad de esta, cuyo proceso se detalla en 4.9.4.

Teniendo en cuenta las regulaciones mencionadas, se hizo un análisis de los lineamientos que plantean y se redactó una política de privacidad en 5.1 que cumple con describir los principios y prácticas de Kinteractive y que se centra en los derechos de privacidad del paciente, describiendo procesos para resguardarla y mecanismos para empoderar a los pacientes y usuarios sobre sus datos personales.

Por último, se implementó un proceso de documentación de procesos que hace referencia a los lineamientos planteados por la ley de protección de datos europea (GDPR) en el artículo 30. Se detalla la implementación de este modelo generado en 4.8 y el proceso de validación en 5.4.

El objetivo de la solución es obtener los requerimientos para estar en cumplimiento, permitiendo generar hallazgos sobre brechas de seguridad, y completando documentación de manera automatizada para generar la política de privacidad de Kinteractive.

5.1. Política De Privacidad De Techneworks Para El Tratamiento De Datos De Pacientes En El Sector Salud

Introducción

En el contexto del tratamiento de datos en el sector de la salud, TechneWorks reconoce la importancia crítica de la privacidad y la seguridad de la información médica de los pacientes. Esta política de privacidad se establece con el objetivo de garantizar el cumplimiento de las regulaciones nacionales e internacionales, así como de proporcionar una guía integral para el diseño, implementación y evaluación de prácticas de privacidad efectivas. Esta política se aplica a todos los datos relacionados con la salud de los pacientes procesados, almacenados o transmitidos por TechneWorks y sus plataformas, incluyendo, pero no

limitado a, Kinteractive.

Objetivos

- Cumplir con las leyes de privacidad y seguridad de datos chilenas y la reglamentación HIPAA de Estados Unidos.
- Proteger la privacidad y confidencialidad de la información médica de los pacientes.
- Establecer prácticas de privacidad transparentes y responsables.
- Promover una cultura organizacional centrada en la privacidad y la seguridad de los datos.

Alcance

Esta política se aplica a todas las actividades relacionadas con el tratamiento de datos de pacientes realizadas por TechneWorks, incluyendo la recopilación, almacenamiento, procesamiento, uso y divulgación de datos médicos.

Principios de Privacidad de Datos

- Consentimiento informado: Se obtendrá el consentimiento informado de los pacientes antes de recopilar, procesar o compartir su información médica, y se respetará su derecho a revocar el consentimiento en cualquier momento.
- Finalidad limitada: Los datos médicos se utilizarán únicamente para fines específicos relacionados con la atención médica, la investigación o el cumplimiento de obligaciones legales, y no se utilizarán para fines no autorizados.
- Minimización de datos: Se recopilará y almacenará la cantidad mínima de datos necesarios para cumplir con la finalidad prevista, y se evitará la recopilación de datos innecesarios o excesivos.
- Exactitud y actualización de datos: Se garantizará la precisión y actualización de la información médica, y se proporcionarán mecanismos para que los pacientes accedan y corrijan sus datos cuando sea necesario.
- Seguridad de datos: Se implementarán medidas técnicas y organizativas adecuadas para proteger la seguridad y confidencialidad de la información médica contra accesos no autorizados, pérdidas o robos.
- Transparencia y acceso: Se proporcionará información clara y transparente sobre las prácticas de privacidad de TechneWorks, y se facilitará a los pacientes el acceso a sus propios datos médicos.

Cumplimiento Normativo
TechneWorks se compromete a cumplir con todas las leyes y regulaciones aplicables en materia de privacidad y seguridad de datos, incluyendo la Ley de Protección de Datos Personales y la Ley de Derechos y Deberes de los Pacientes en Chile, así como la reglamentación HIPAA en Estados Unidos.

Responsabilidades y Capacitación del Personal
Todo el personal de TechneWorks que tenga acceso a datos de pacientes recibirá capacitación regular sobre prácticas de privacidad y seguridad de datos, y será responsable de cumplir con las políticas y procedimientos establecidos en esta política.

Monitoreo y Auditoría
TechneWorks realizará auditorías periódicas para evaluar el cumplimiento de esta política y tomará medidas correctivas en caso de identificar deficiencias o incumplimientos.

Mejora Continua
Esta política se revisará y actualizará regularmente para garantizar su eficacia y cumplimiento continuo con las regulaciones y mejores prácticas en materia de privacidad y seguridad de datos.

Recopilación de Datos
TechneWorks recopilará datos de pacientes únicamente con el consentimiento informado de los mismos y para fines específicos relacionados con la atención médica.

Uso de los Datos
Los datos de pacientes recopilados por TechneWorks se utilizarán únicamente para los fines previstos y no se compartirán con terceros sin el consentimiento expreso del paciente, excepto cuando sea requerido por ley.

Protección de Datos
TechneWorks implementará medidas de seguridad sólidas para proteger la confidencialidad e integridad de los datos de pacientes, incluyendo el uso de cifrado, contraseñas seguras y controles de acceso.

Compartir Datos
Los datos de pacientes solo se compartirán con terceros autorizados y bajo acuerdos de confidencialidad que garanticen la protección de la información médica.

Derechos ARCOP de los Usuarios
Los pacientes tendrán derecho a acceder, corregir y eliminar sus datos médicos, así como a revocar su consentimiento para el tratamiento de los mismos en cualquier momento.

Para poder realizar una solicitud sobre sus datos, Kinteractive dispondrá de una página web debidamente identificada por la organización, donde existirá un formulario disponible para

todos los usuarios que visiten la página y desde este podrán enviar su solicitud mediante una verificación de identidad.

Para realizar una adecuada validación de la identidad se pide la información de contacto del paciente:

- Nombre
- Apellido
- Correo electrónico
- Foto o escaneo de la cédula de identidad

Una vez realizada la validación de identidad, se procede a llevar a cabo la solicitud siguiendo los pasos definidos para cada caso: acceso, rectificación, cancelación, oposición y portabilidad de los datos, descritos en la sección 4.5.

Estos derechos permiten al usuario tener dominio sobre diferentes aspectos de como el paciente tiene acceso y control a su información y datos personales y garantizan que Kinteractive cumplirá con lineamientos específicos para el tratamiento de los datos.

Cambios en la Política
TechneWorks se reserva el derecho de modificar esta política en cualquier momento, y cualquier cambio se comunicará a los pacientes de manera oportuna y transparente.

Contacto
Para consultas o preocupaciones relacionadas con esta política de privacidad, los pacientes pueden ponerse en contacto con el equipo de privacidad de TechneWorks a través de los canales de comunicación designados.

En caso de requerir comunicarse con el delegado de protección de datos o DPO, es posible ponerse en contacto mediante los correos electrónicos dispuestos en la página web informando su solicitud y el detalle.

Vigencia
Esta política de privacidad entra en vigencia a partir de su publicación y se mantendrá en vigor hasta su modificación o anulación por parte de TechneWorks.

5.2. Revisión de resultados para análisis de datos personales mediante el uso de inteligencia artificial

Se validará el caso de uso planteado en 4.9.4, el cual representa parte de los procesos de tratamiento de datos que realiza Kinteractive. Se hace un análisis sobre los datos personales mediante un modelo de inteligencia artificial, específicamente LLM, con el cual

se busca determinar los tipos de datos sensibles que se encuentran en un conjunto de datos específico.

Para este proceso se tienen 3 conjuntos de datos con información previamente clasificada, con los cuales se probará la solución y posteriormente se realizará un análisis para validar el porcentaje de coincidencias que se obtienen entre la información detectada y la información real.

Estos conjuntos de datos usados representan bases de datos tradicionales de organizaciones que llevan registro de sus clientes, proveedores, transacciones, entre otros. Parte de las complejidades a considerar, es el análisis de datos numéricos tales como números de ID internos, números de tarjeta de crédito, números de cédula o identificadores de gobierno, entre otros.

Los conjuntos de datos a usar son:

- Dataset DS1: Contiene 16 campos de datos sensibles etiquetados y una muestra de 12 sujetos de datos.
- Dataset DS2: Contiene 15 campos de datos sensibles no etiquetados y una muestra de 68 sujetos de datos.
- Dataset DS3: Contiene 53 campos de datos sensibles etiquetados y una muestra de 100 sujetos de datos.

Dataset	Tipos de Datos Sensibles	Modelo LLM	Datos sensibles detectados por valores	Datos sensibles detectados por columna
DS1	16	4	15,5	15
		4o	12,5	16
		4t	13,5	16
DS2	15	4	14,5	N/A
		4o	12	N/A
		4t	12,5	N/A
DS3	53	4	50	52,5
		4o	49	53
		4t	50	53

Tabla 1: Tipos de datos sensibles detectados según los tres modelos.

El proceso de prueba consistió en realizar 27 ejecuciones del análisis de datos sensibles. Específicamente se realizaron 3 ejecuciones por cada conjunto de datos (DS1, DS2, DS3)

Modelo LLM	Dataset	% Tipos de datos sensibles detectados	% Columnas detectadas
4	DS1+DS2+DS3	95,2%	97,8%
4o	DS1+DS2+DS3	88,1%	100%
4t	DS1+DS2+DS3	90,5%	100%

Tabla 2: Porcentaje de aciertos obtenidos por tipo de dato y columna por cada modelo. Incluye los resultados de los tres conjuntos de datos.

por cada modelo (4, 4o, 4t), de esta manera se tienen 3 muestras de resultados para cada caso específico; para los resultados mostrados se excluyeron la mejor y peor ejecución según los resultados obtenidos, dejando solo los datos de lo que se considera el caso promedio.

En la tabla 1 se muestran los aciertos obtenidos en cada dataset (conjunto de datos), separados por modelo del LLM. La variación entre los resultados obtenidos por cada dataset no es muy indicativa del rendimiento general, por lo que se agrupan los resultados de los 3 conjuntos de datos en la tabla 2 y se puede ver en mayor detalle el rendimiento de cada modelo. En el anexo B se deja detalle de los tipos de datos que fueron puestos a prueba, los resultados obtenidos del análisis del modelo y un resultado de verificar manualmente si corresponde el tipo de dato detectado por cada uno de los modelos. Los puntajes se hicieron de manera que:

- Acertar con el tipo de dato o nombre de columna corresponde a +1 punto.
- Indicar erróneamente el tipo de dato o nombre de columna corresponde a -1 punto.
- Indicar un tipo de dato parcialmente correcto o relacionado más no completamente preciso, corresponde a +0,5 puntos.
- Existen casos que no aplican, específicamente la detección de nombre de columna para los nombres de columna que no están etiquetados (col1, col2, col3,..., etc)

El principal hallazgo es la efectividad que muestra para poder categorizar etiquetas de datos sensibles en base a muestras de un solo elemento, como lo es el caso para la detección de columnas. Los modelos que ofrece Open AI que fueron usados tienen diferentes características y rendimiento. Según la documentación actual, existe una serie de *tradeoffs* que se tienen que considerar, como el costo de uso del LLM y la capacidad de análisis del modelo seleccionado.

La capacidad de análisis es un conjunto de parámetros tales como: conjunto de datos de entrenamiento, algoritmos implementados, cantidad de tokens que acepta para contexto, y cantidad de tokens que puede utilizar para la salida de texto. Para este caso se hará uso de los tokens que acepta cada modelo para contexto y que tantos tokens puede utilizar para

Modelo	Máxima cantidad de tokens de contexto	Máxima cantidad de tokens de salida
4	8.192	8.192
4t	128.000	4.096
4o	128.000	4.096

Tabla 3: Capacidad de manejo de tokens de cada modelo

generar la salida, como se muestra en la tabla 3.

A pesar de las mayores ventanas de contexto que ofrecen los modelos GPT-4t y GPT-4o, el mejor resultado general se obtuvo con el modelo GPT-4. Actualmente la documentación de los modelos indica que el modelo 4o es el doble de eficiente con un costo del 50 %, adicionalmente se tiene que el costo del modelo 4 es mayor al de 4o y menor que el de 4t.

Dadas las condiciones mencionadas anteriormente, es recomendable trabajar actualmente con el modelo GPT-4 que ofrece el mejor rendimiento a un costo moderado. También es necesario considerar que los costos mayores del uso de este modelo se ven compensados con los gastos que puede representar la detección errónea de información sensible dentro de la organización en forma de multas por incumplimiento.

A continuación se muestran las categorías a las que se asignaron los datos clasificados (el detalle de estos datos se pueden ver en la tabla 9):

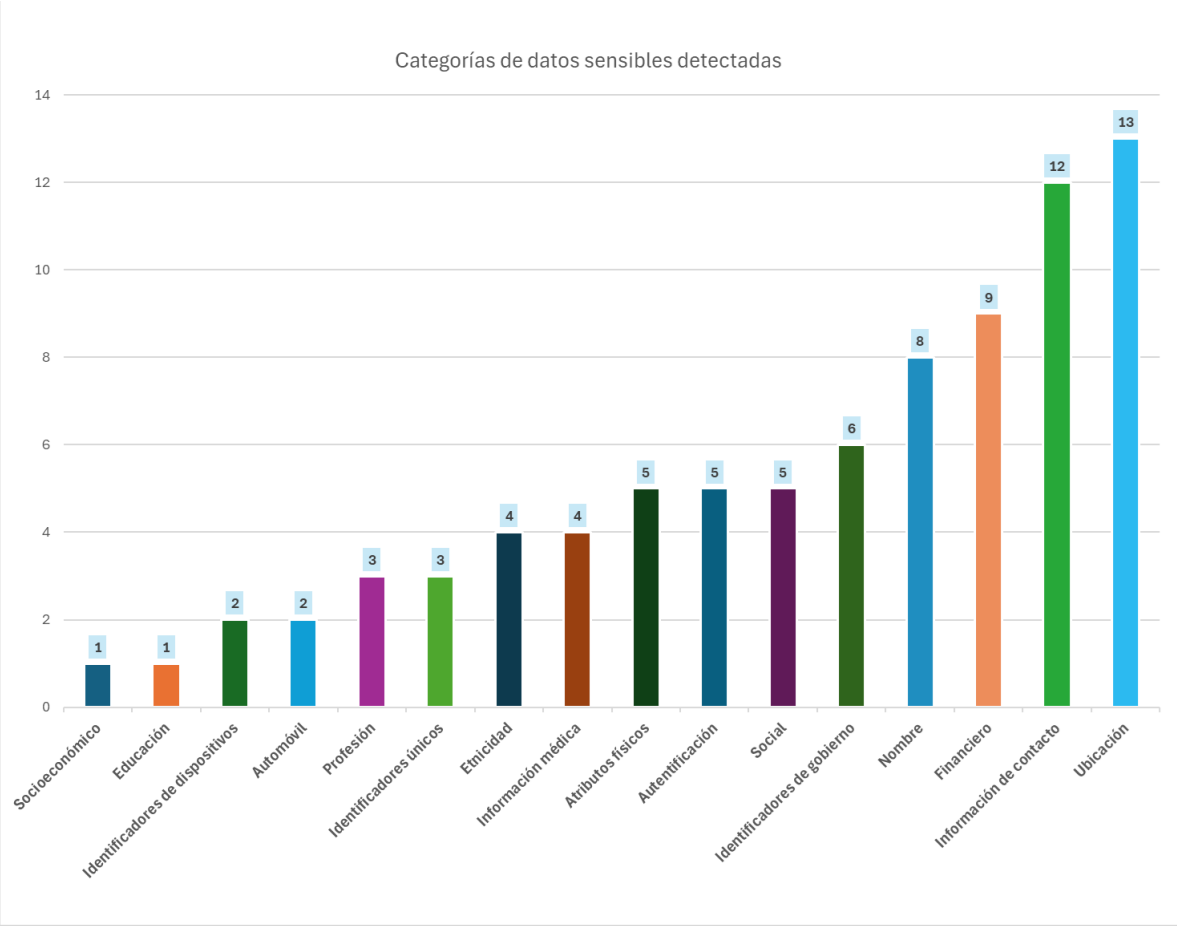


Figura 10: Categorías de datos sensibles detectadas

Al agrupar en categorías los datos sensibles detectados, se puede ver una imagen más completa del ambiente de datos que se maneja. En particular se incluyeron tipos de datos relevantes que representan a los usuarios de Kinteractive, tales como datos asociados a procesos de autentificación de pacientes, registro de usuarios y llenado de información adicional como datos sobre la etnia o sociales.

Considerando que se detectaron correctamente los datos de carácter más sensible, tales como la información médica, identificadores de gobierno y datos financieros, esto representa una herramienta de mucho valor para organizaciones de gran tamaño y con múltiples ambientes de datos que no necesariamente están documentados o cuyo proceso para documentar es mucho mayor que al proceso propuesto.

Por el lado de los tipos de datos que no fueron detectados correctamente, cabe destacar que estos fueron clasificados como parcialmente correctos, es decir, siempre se relacionaba al menos el ámbito o categoría del tipo de dato. Para estos casos se tiene la siguiente distribución:
Por último, se pudo obtener resultados certeros para identificar los datos previamente

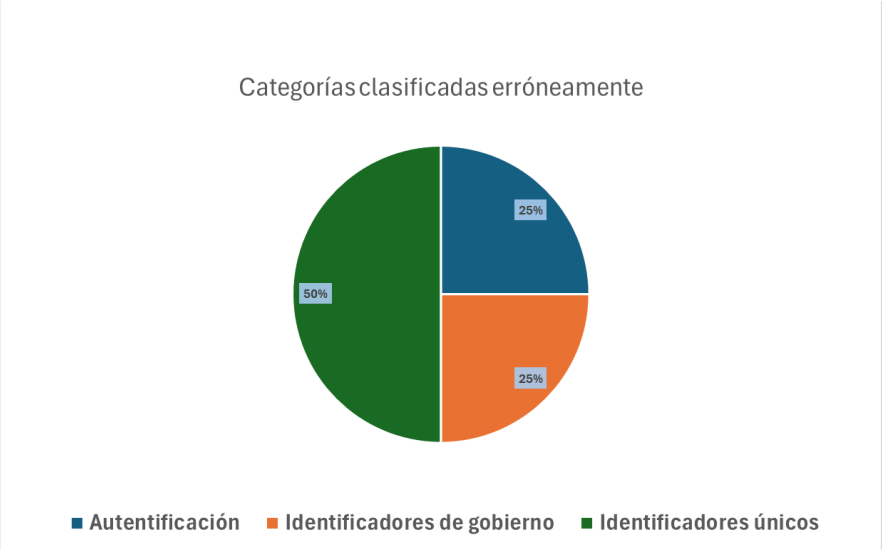


Figura 11: Categorías de datos clasificadas erróneamente

destacados como casos complejos. En particular se nota la capacidad de identificar y diferenciar los siguientes tipos de datos que fueron incluidos en el análisis:

- Número de seguro social (SSN)
- Número de registro de contribuyente Brasileño (CPF)
- Códigos postales
- Números de tarjeta de crédito
- Números de cuenta bancaria
- Número de código de banco

La muestra de datos contenía datos en general representativos de un caso de uso real y que representa ambientes de organizaciones que trabajan con información de este tipo. Dadas las condiciones establecidas y los resultados obtenidos a partir de la componente de la solución implementada, se considera exitoso el cumplimiento del requerimiento para mantener un ambiente de datos documentado y con las debidas identificaciones de los datos sensibles que se manejan.

5.3. Revisión de resultados para análisis de puntos claves de las regulaciones

Se realizó una serie de pruebas para validar la componente de la solución que específicamente analiza las regulaciones indicadas. El objetivo es que a partir de la fuente de información de la regulación, pueda obtener los aspectos más importantes y generar indicaciones para estar en cumplimiento con cada uno de estos puntos.

Se usaron 3 modelos LLM para llevar a cabo la experimentación, cada uno de estos tiene diferentes características que son relevantes para el caso de uso en aspectos regulatorios.

Se busca determinar los puntos clave que indican las regulaciones con las que se busca cumplir y describir a alto nivel qué mecanismos implementar para estar en cumplimiento. Para el caso de Kinteractive se consideran la regulación HIPAA y la regulación chilena que comprende las leyes 19.628, 20.584 y 21.096.

Se analizarán los resultados obtenidos a partir del LLM, al que se le da la tarea de generar una serie de normas y mecanismos a seguir o implementar con el fin de estar en cumplimiento con las regulaciones mencionadas anteriormente. Dada una serie de lineamientos a seguir que serán definidos según estas regulaciones, se hará un análisis cualitativo que determine cuantos puntos claves de cada regulación son descritos por la respuesta del modelo.

Para el análisis de resultados se realizaron 3 ejecuciones de cada regulación por cada modelo, de los cuales se eligió y se muestra el mejor resultado para cada regulación incluyendo todos los modelos, siendo el mejor resultado aquel que describiera la mayor cantidad de puntos claves de la regulación y tiene menos puntos erróneos o que no corresponden a la regulación; de esta manera se tiene en cuenta la posibilidad de que se generen alucinaciones por parte del LLM.

5.3.1. Análisis de resultados para regulación HIPAA

La regulación descrita por HIPAA consiste de múltiples documentos para procedimientos administrativos, de seguridad física y digital, programas de privacidad, entre otros. Para este caso se hace análisis específicamente de la "*HIPAA Privacy Rule*" [U.S. Department of Health Human Services, 1999b] o Regla de Privacidad, que describe procedimientos a implementar dentro de la organización cuando se hace manejo de información en registros electrónicos de los pacientes. El documento de esta regla consiste de 115 páginas y abarca múltiples aspectos técnicos y administrativos. Específicamente se cubre la sección *"PART 164—SECURITY AND PRIVACY"* que describe los estándares, requerimientos y especificaciones de implementación.

La implementación de la solución obtuvo el mejor resultado con el modelo GPT-4o, el cual generó 33 lineamientos y descripciones a seguir. Viendo en detalle los puntos generados, estos corresponden al documento correcto y la sección específica mencionada anteriormente, ya que todos los resultados generados pueden ser indicados dentro de la regulación, esto además significa que no hubo casos de alucinaciones para este resultado.

Por último, el resultado obtenido hace mención de reglas definidas en las siguientes secciones del documento:

- SUBPART A—GENERAL PROVISIONS
- SUBPART C—SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

- SUBPART D—NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION
- SUBPART E—PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

Estos corresponde a todas las secciones dentro de la parte 164 de seguridad y privacidad de la regulación. Las indicaciones generadas no corresponden a la totalidad de las centenas de indicaciones, sin embargo es una lista acotada que permite implementar mecanismos que posteriormente pueden dar cobertura a la totalidad de los puntos en la ley. El detalle de como se relacionaron los puntos de la regulación con el resultado obtenido se puede ver en el anexo C.

	Puntos clave	Descripción	Requisitos de cumplimiento
1	Confidencialidad	Protección de la información de salud del paciente (PHI) contra el acceso no autorizado	Implementar medidas de seguridad administrativas, físicas y técnicas para garantizar la confidencialidad de la PHI.
2	Integridad	Garantizar que la PHI no se altere ni se destruya de manera no autorizada	Implemente medidas como el cifrado y las copias de seguridad seguras de los datos para mantener la integridad de los datos.
3	Disponibilidad	Garantizar que la PHI sea accesible cuando sea necesario para los usos autorizados	Establezca planes de contingencia, procesos de recuperación de datos y sistemas de respaldo para garantizar la disponibilidad de la PHI.
4	Controles de acceso	Limitar el acceso a la PHI solo al personal autorizado	Utilice ID de usuario únicos, procedimientos de acceso de emergencia y mecanismos de cierre de sesión automático para controlar el acceso.
5	Controles de auditoría	Implementar hardware, software y/o mecanismos de procedimiento que registren y examinen la actividad en los sistemas de información que contienen o utilizan PHI.	Mantenga registros de auditoría y revíselos periódicamente para detectar y responder a los incidentes de seguridad.
6	Seguridad en la transmisión de datos	Proteja la PHI transmitida a través de redes electrónicas	Cifre los datos durante la transmisión y utilice canales de comunicación seguros, como las VPN.
7	Capacitación de empleados	Capacitar a los miembros de la fuerza laboral sobre sus responsabilidades con respecto a la protección de la PHI	Llevar a cabo sesiones periódicas de capacitación y repasos sobre las políticas y procedimientos de HIPAA.
8	Respuesta a incidentes	Procedimientos para responder a brechas e incidentes de seguridad	Adopte un plan de respuesta a incidentes, pruébelo regularmente y documente e informe cada incidente según sea necesario.
9	Norma Mínima Necesaria	Divulgar solo la cantidad mínima de PHI necesaria para lograr el propósito previsto	Implemente políticas y controles de acceso basados en roles para garantizar el cumplimiento de la regla mínima necesaria.
10	Acuerdos de Socios Comerciales (BAAs)	Asegúrese de que los socios comerciales que manejan PHI también cumplan con la HIPAA	Ejecutar acuerdos de acuerdo con todos los socios comerciales y exigirles que implementen las salvaguardas adecuadas.
11	Derechos del paciente	Informar a los pacientes sobre sus derechos a acceder, modificar y restringir la PHI	Proporcionar políticas claras a los pacientes e implementar procedimientos para facilitar el ejercicio de estos derechos.
12	Derechos de acceso a los datos	Derechos de los pacientes a acceder a su propia PHI	Garantizar respuestas oportunas y precisas a las solicitudes de los pacientes de sus registros de salud.
13	Modificación de la PHI	Derechos de los pacientes a solicitar enmiendas a su PHI	Desarrollar y seguir procedimientos para evaluar y hacer enmiendas, y documentar las respuestas.
14	Restricciones sobre el uso de PHI	Derechos de los pacientes a solicitar restricciones sobre ciertos usos y divulgaciones de su PHI	Cree y aplique políticas para administrar y cumplir con las solicitudes de restricción de pacientes.
15	Comunicaciones confidenciales	Derecho de los pacientes a recibir comunicaciones a través de medios alternativos o en lugares alternativos	Habilitar mecanismos para las comunicaciones confidenciales según lo soliciten los pacientes.
16	Aviso de Prácticas de Privacidad	Informar a los pacientes sobre cómo se usará y divulgará su PHI.	Crear, difundir y exhibir de manera destacada un Aviso de Prácticas de Privacidad.
17	Notificación de violación de datos	Requisitos para notificar a las personas y a las autoridades sobre violaciones de PHI no asegurada	Implemente una política de notificación de infracciones que cumpla con los requisitos de HIPAA, incluidos los plazos y la documentación.
18	Acceso basado en roles	Limitar el acceso a la PHI en función de la función del usuario dentro de la organización	Defina claramente las funciones y responsabilidades y limite el acceso a la PHI en consecuencia.
19	Salvaguardas físicas	Medidas para proteger el acceso físico a los sistemas que contienen PHI	Aplique medidas de seguridad física, como instalaciones cerradas, requisitos de identificación y vigilancia.
20	Salvaguardas técnicas	Tecnologías y políticas para proteger la PHI electrónica	Implemente firewalls, software antivirus y evaluaciones periódicas de vulnerabilidades.
21	Auditorías de cumplimiento	Revisiones periódicas para garantizar el cumplimiento de las regulaciones de HIPAA	Programar auditorías y revisiones periódicas de políticas, procedimientos y prácticas.
22	Análisis del riesgo	Evaluar los riesgos y vulnerabilidades potenciales para la confidencialidad, integridad y disponibilidad de la PHI	Realizar una evaluación de riesgos exhaustiva y actualizarla periódicamente como parte del plan de gestión de riesgos de la organización.
23	Desidentificación de la PHI	Procedimientos para anonimizar la PHI para su uso en investigación u otros fines, garantizando el anonimato del paciente	Aplicar técnicas de desidentificación y verificar que cumplan con los estándares de HIPAA.
24	Política de sanciones	Aplicación de sanciones para los miembros de la fuerza laboral que no cumplan con las políticas de HIPAA	Desarrollar una política de sanciones por escrito y asegurarse de que se comunique a todos los empleados.
25	Planes de contingencia	Preparación para emergencias u otros eventos que amenacen la seguridad de la PHI	Desarrolle, implemente y pruebe periódicamente planes de contingencia y recuperación ante desastres.
26	Controles de dispositivos y medios	Pautas para la recepción, eliminación y eliminación de hardware y medios electrónicos que contienen PHI	Adoptar procedimientos para la eliminación segura y la reutilización de dispositivos para prevenir violaciones de PHI.
27	Tiempo de espera de la sesión	Terminación automática de sesiones electrónicas después de un período de inactividad	Configure los sistemas para que se desconecten automáticamente después de un período predefinido de inactividad.
28	Copia de seguridad y almacenamiento de datos	Garantizar copias de seguridad periódicas de los datos y el almacenamiento seguro de la PHI	Implemente programas de copia de seguridad regulares y soluciones de almacenamiento seguro para toda la PHI.
29	Encriptación	Uso del cifrado para proteger la PHI tanto en reposo como en tránsito	Adopte estándares y tecnologías de encriptación para una protección integral de la PHI.
30	Seguridad de la estación de trabajo	Protección de las estaciones de trabajo que acceden a la PHI	Implemente políticas para el uso adecuado de la estación de trabajo, la seguridad física y los controles de acceso de los usuarios.
31	Recuperación ante desastres	Planes para recuperar y mantener la PHI en caso de un desastre	Establezca y pruebe periódicamente un plan de recuperación ante desastres para garantizar la disponibilidad de la PHI.
32	Documentación de la póliza	Documentar todas las políticas y procedimientos relacionados con HIPAA	Mantenga la documentación actualizada y asegúrese de que esté disponible para la capacitación y las auditorías.
33	Información de contacto del Oficial de Privacidad	Proporcionar los datos de contacto del responsable de privacidad de la organización	Asegúrese de que la información de contacto del oficial de privacidad sea fácilmente accesible para los empleados y pacientes.

Tabla 4: Requerimientos generados con modelo GPT-4o para cumplimiento con regulación HIPAA

Adicionalmente, se agruparon los lineamientos e indicaciones generadas según el tipo de

requerimiento que exige. En el gráfico a continuación se muestra como una gran parte de los lineamientos están enfocados al cumplimiento de normativas y a los derechos del paciente.

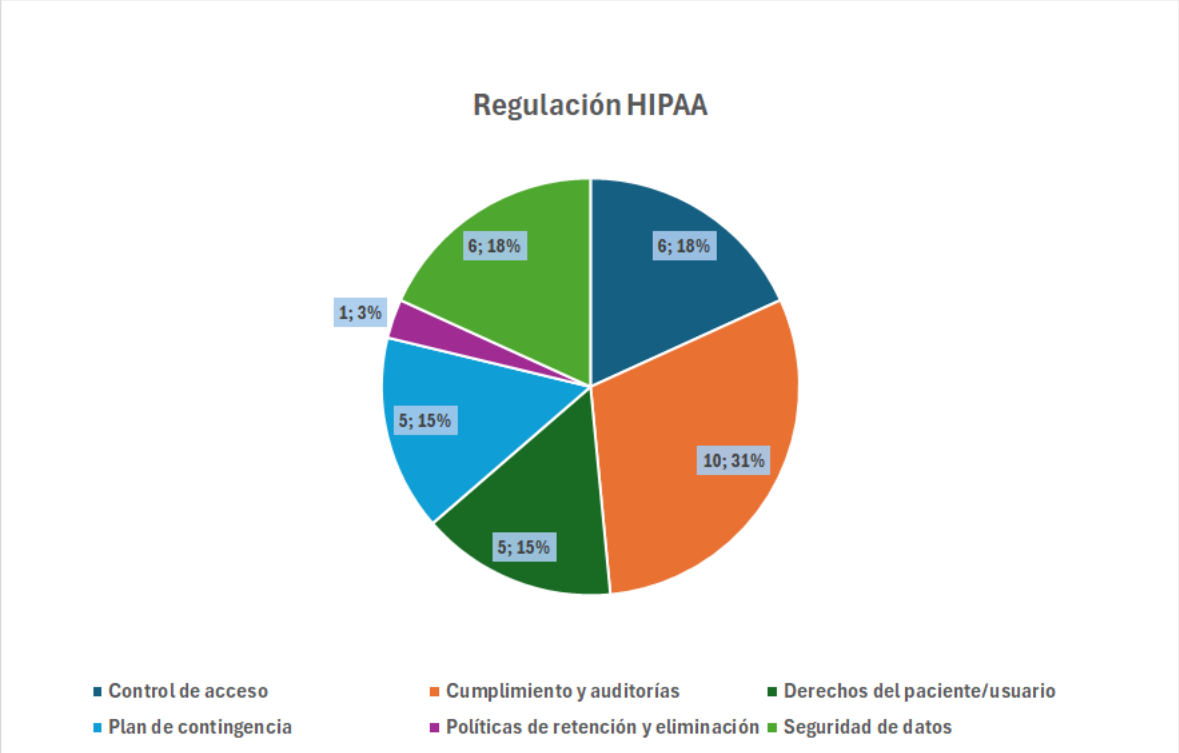


Figura 12: Categorías de lineamientos e indicaciones generados para regulación HIPAA

5.3.2. Análisis de resultados para Ley 19.628

La ley 19.628 describe como se deben proteger los datos asociados a personas y su vida privada. Consiste de cinco títulos que abarcan aspectos como disposiciones generales, a quien aplica, y en su mayor parte, como hacer uso de los datos de carácter sensible o privado de las personas de quien se tiene registros de información.

El alcance de la solución se enfoca en los capítulos I y II que corresponden a “La utilización de datos personales” y “Derechos de los titulares de datos”, de estos se consideran 12 de los 16 artículos que contiene, ya que los artículos 2, 8, 15 y 16 no aplican para el proceso de implementar mecanismos de privacidad, sino definiciones. A continuación se muestra la tabla con los puntos generados para cubrir con los diferentes artículos.

	Puntos clave	Descripción	Requisitos de cumplimiento
1	Finalidad del Tratamiento de Datos	Los datos deben ser usados exclusivamente para el propósito con el cual fueron recolectados.	Establecer y documentar claramente las finalidades para las cuales se recogen los datos y asegurar que no se utilicen para fines distintos.
2	Consentimiento del Titular	El tratamiento de datos personales requiere el consentimiento expreso del titular, salvo excepciones establecidas por la ley.	Obtener y registrar el consentimiento explícito de los titulares antes de procesar sus datos, a menos que una excepción legal sea aplicable.
3	Derecho de Acceso	Las personas tienen derecho a solicitar información sobre los datos personales que se han recopilado sobre ellas.	Implementar procedimientos para responder a las solicitudes de acceso a datos personales de manera oportuna y precisa.
4	Derecho de Rectificación	Los titulares tienen derecho a solicitar la corrección de datos incorrectos, imprecisos, desactualizados o incompletos.	Establecer mecanismos para que los titulares puedan solicitar y obtener la rectificación de sus datos personales de manera eficiente.
5	Derecho de Cancelación	Las personas tienen derecho a solicitar la eliminación de sus datos personales cuando ya no sean necesarios para el propósito para el cual fueron recogidos o tratados.	Implementar procesos para la pronta eliminación de datos personales cuando se haga una solicitud de cancelación válida.
6	Derecho de Oposición	Los titulares pueden oponerse al tratamiento de sus datos personales por motivos justificados.	Asegurar que se respeten las solicitudes de oposición debidamente fundamentadas y cesar el tratamiento de los datos en cuestión.
7	Seguridad de los Datos	Es obligatorio implementar medidas de seguridad adecuadas para proteger los datos personales contra el acceso no autorizado, pérdida o destrucción.	Desarrollar y mantener políticas de seguridad que incluyan controles técnicos y administrativos apropiados para la protección de datos personales.
8	Confidencialidad	Las entidades que tratan datos personales deben garantizar la confidencialidad de estos datos.	Establecer y hacer cumplir acuerdos de confidencialidad para todos los empleados y contratistas que tengan acceso a datos personales.
9	Transferencia de Datos	La transferencia de datos personales a terceros solo se permite si se garantiza un nivel de protección adecuado.	Evaluar las políticas de privacidad de terceros y asegurarse de que cumplan con los estándares de protección de datos antes de transferir datos personales.
10	Reclamos y Denuncias	Las personas tienen el derecho de presentar reclamos si consideran que sus derechos han sido infringidos.	Disponer de un canal formal para la recepción, análisis y resolución de reclamos sobre el tratamiento de datos personales.
11	Actualización de Datos	Es responsabilidad de la entidad mantener actualizados los datos personales.	Establecer procedimientos para la verificación y actualización periódica de los datos personales recolectados.

Tabla 5: Requerimientos generados con modelo GPT-4o para cumplimiento con Ley 19.628

Los resultados obtenidos muestran que el modelo generó 11 puntos para cubrir los requerimientos de la regulación, el análisis y mapeo de los puntos clave con los artículos de la ley se pueden ver en el anexo C. De estos 11 puntos cubiertos, se puede representar una

relación con cada uno de los 12 artículos cubiertos en la ley.

Al igual que en la experimentación con la regulación anterior, se puede ver una capacidad adecuada para separar los propósitos de los textos dentro de las regulaciones, ya que no ha producido alucinaciones donde se indiquen requerimientos que no existen o de manera errónea. Específicamente, se considera bastante provechoso que la solución pueda efectivamente diferenciar a que corresponde cada título de la ley y enfocarse, generar lineamientos y requerimientos, específicamente sobre los artículos relacionados a los titulares de datos y sus derechos.

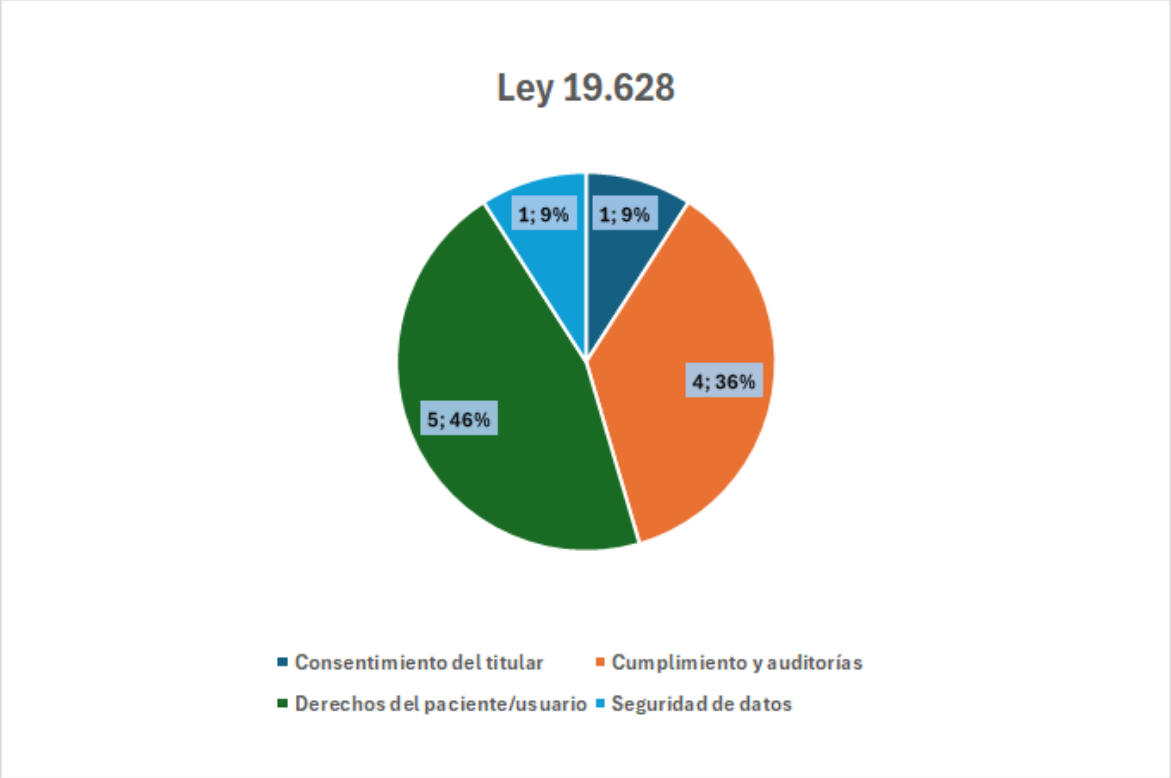


Figura 13: Categorías de lineamientos e indicaciones generados para ley 19.628

De manera similar al caso anterior, la mayoría de los lineamientos se enfocan en el cumplimiento normativo y los derechos del paciente. Este resultado está alineado con el objetivo del proyecto, el cual era buscar cumplimiento regulatorio y generar una política de privacidad cuyo enfoque sea el paciente, en este caso, sus derechos.

5.3.3. Análisis de resultados para Ley 20.584

La ley 20.584 se enfoca en los derechos y deberes de las personas en cuanto a la atención en salud, por lo que el dominio del documento no es principalmente técnico o tecnológico. Sin embargo, se hace referencia en pocos artículos a los mecanismos que se deben proveer a los pacientes. En general los requerimientos mencionados hacen referencia a derechos

similares a los derechos ARCOP.

En la siguiente tabla se muestran los lineamientos generados para esta ley, considerando que es una ley con cinco títulos y más de 40 artículos distintos.

	Puntos clave	Descripción	Requisitos de cumplimiento
1	Consentimiento informado	Los pacientes tienen derecho a otorgar o rechazar su consentimiento luego de recibir toda la información necesaria respecto a los procedimientos médicos a los que serán sometidos.	Los profesionales de la salud deben documentar el consentimiento informado de los pacientes antes de proceder con cualquier tratamiento o procedimiento invasivo.
2	Confidencialidad de la Información	La información del paciente debe ser tratada de manera confidencial, solo compartida con el personal médico directamente involucrado en el tratamiento del paciente.	Las instituciones de salud deben implementar políticas asegurando que la información de los pacientes se maneje de manera confidencial y limitada a el personal autorizado.
3	Acceso a la ficha clínica	Los pacientes tienen derecho a acceder a su propia ficha clínica, la cual contiene todos los registros sobre su diagnóstico, tratamiento y datos personales.	Las instituciones de salud deben proporcionar acceso fácil y oportuno a los pacientes a sus fichas clínicas, cumpliendo con los procedimientos establecidos para tal efecto.
4	Rectificación de la información	Los pacientes tienen derecho a solicitar la corrección de cualquier dato incorrecto en sus fichas clínicas.	Las instituciones de salud deben establecer procedimientos para que los pacientes pueden solicitar correcciones y asegurarse de que estos cambios sean realizados de manera adecuada.
5	Retención de la ficha clínica	La ficha clínica debe ser conservada por un mínimo de 15 años desde la fecha del último registro.	Las instituciones de salud deben asegurarse de mantener las fichas clínicas en condiciones adecuadas y seguras por el plazo establecido.
6	Salvaguarda de la Información	Las instituciones de salud deben tomar medidas apropiadas para proteger la información de salud contra el acceso no autorizado, la pérdida o la alteración.	Implementación de tecnologías de la información y políticas de seguridad que garanticen la protección de los datos.

Tabla 6: Requerimientos generados con modelo GPT-4t para cumplimiento con Ley 20.584

Al analizar en detalle la regulación, se extraen cuatro artículos que hace referencia al manejo de información digital, los cuales son cubiertos en las seis indicaciones generadas. El detalle de estos artículos y su relación se puede ver en el anexo C. Sin embargo en esta instancia se generó la indicación 4 que hace referencia a la rectificación de información. Para esta ley no existen puntos específicos a la actualización de información, por lo que se considera que este punto es erróneo para el alcance de esta ley.

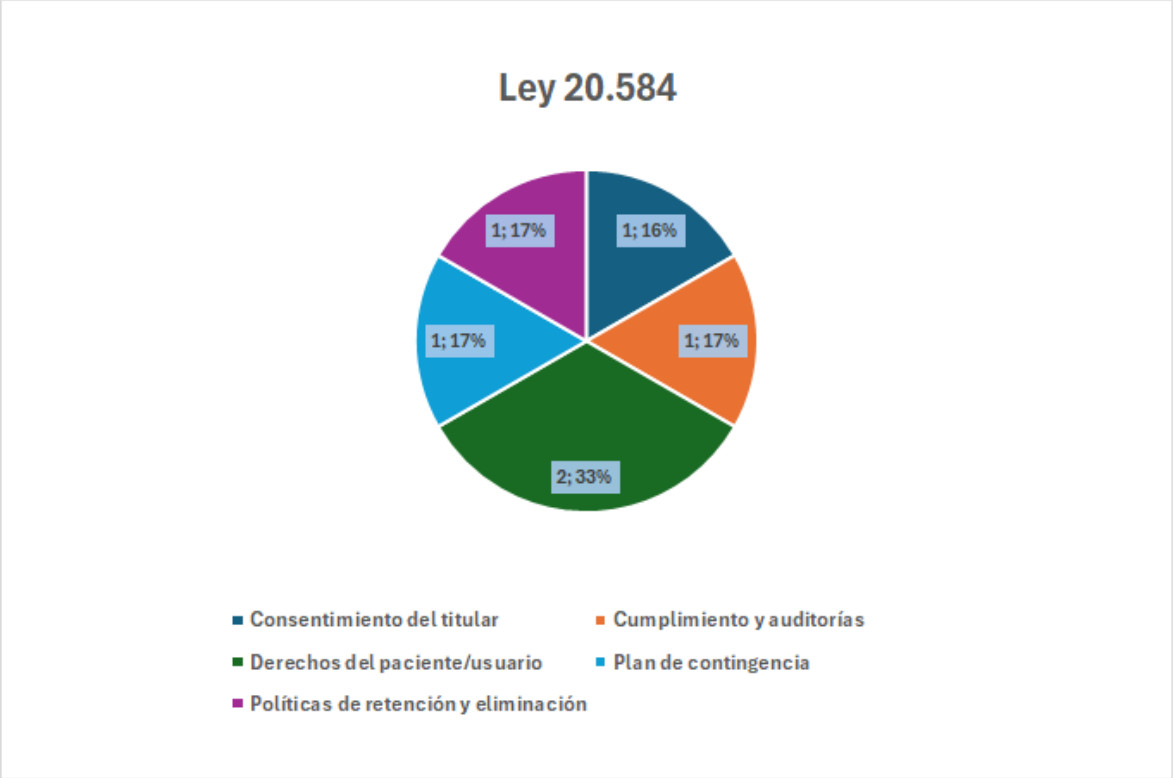


Figura 14: Categorías de lineamientos e indicaciones generados para ley 20.584

La ley en cuestión se enfoca en un ámbito más amplio, es decir, no se mantiene exclusivamente dentro del dominio de la tecnología y la información en registros electrónicos. Por lo que la variedad y cantidad de lineamientos generados no son tantos como en los otros casos. Sin embargo, se puede ver que abarca las diferentes áreas que plantea la ley, haciendo énfasis en los derechos del paciente.

5.3.4. Análisis de resultados para Ley 21.096

La ley 21.096 indica una reforma de un artículo de la constitución previamente establecido, donde se indica que se agrega la protección de los datos sensibles e información personal como parte del dominio de la protección de la vida privada. De igual manera, indica que este tipo de información deberá ser resguardada bajo la ley Chilena, sin indicar de forma explícita mecanismos o procedimientos a establecer.

Teniendo lo anterior en cuenta, se hizo un análisis de los resultados generados por el LLM y estos son tales que: no se hace referencia directamente a información descrita en la ley 21.096, la respuesta generada hace referencia a artículos de otras leyes que si se encargan de describir los mecanismos de protección necesarios. En particular la respuesta generada tenía:

- 11 Indicaciones en total, de las cuales:

- 8 pertenecen a requerimientos de la ley 19.628
- 3 pertenecen a requerimientos de la ley 20.584

En la tabla a continuación describen los puntos generados, que son similares a los generados con respecto a las últimas dos leyes.

	Puntos clave	Descripción	Requisitos de cumplimiento	Artículo y Ley correspondiente
1	Finalidad de los Datos	Los datos personales deben ser recolectados para cumplir con una finalidad específica y legítima.	Definir y comunicar claramente la finalidad del uso de los datos al titular.	Artículo 4. Ley 19.628
2	Principio de Proporcionalidad	Solo se deben tratar los datos estrictamente necesarios para el cumplimiento de la finalidad.	Limitar la recolección y tratamiento de datos a lo estrictamente necesario.	Artículo 9. Ley 19.628
3	Derecho de Acceso	El titular de los datos tiene derecho a acceder a sus datos personales tratados.	Establecer mecanismos para solicitar y proporcionar acceso a los datos.	Artículo 12. Ley 19.628
4	Rectificación de Datos	El titular tiene derecho a corregir sus datos en caso de ser inexactos.	Implementar procedimientos para la actualización y rectificación de datos.	Artículo 12. Ley 19.628
5	Derecho de Cancelación	El titular puede solicitar la eliminación de sus datos personales.	Incluir procesos para la eliminación de datos cuando sea solicitado o necesario.	Artículo 12. Ley 19.628
6	Oposición al Tratamiento	El titular puede oponerse al tratamiento de sus datos personales.	Garantizar mecanismos para que los titulares puedan ejercer su derecho a oposición.	Artículo 12. Ley 19.628
7	Seguridad de los Datos	Implementar medidas de seguridad adecuadas para proteger los datos personales.	Adopción de medidas técnicas y organizativas para la protección de datos.	Artículo 1. Ley 19.628
8	Deber de Confidencialidad	Quienes traten datos personales deben mantener la confidencialidad de los mismos.	Implementar políticas claras de confidencialidad y capacitación para el personal.	Artículo 1 y Artículo 7. Ley 19.628
9	Transparencia en el Tratamiento	Comunicar de manera clara y accesible la información sobre el tratamiento de datos.	Establecer políticas de privacidad y asegurarse de que sean comprensibles y accesibles.	Artículo 10 bis. Ley 20.584
10	Conservación de Datos	Los datos personales no deben conservarse más tiempo del necesario para la finalidad.	Crear políticas claras sobre el período de retención de datos.	Artículo 13. Ley 20.584
11	Responsable del Tratamiento	Designar un responsable de asegurar el cumplimiento de la normativa de protección de datos.	Designación formal de un encargado de la protección de datos y definir sus responsabilidades.	Artículo 3. Ley 20.584

Tabla 7: Requerimientos generados con modelo GPT-4o para cumplimiento con Ley 21.096

Los resultados obtenidos para la ley 21.096 se pueden asignar “uno a uno” con las leyes 19.628 y 20.584, donde la mayoría de los lineamientos generados hacen referencia a los derechos de los pacientes y cumplimiento normativo. Esto es consistente con los resultados obtenidos para las otras dos regulaciones, ya que se mantiene la alta proporción de lineamientos enfocados en el paciente y sus derechos.

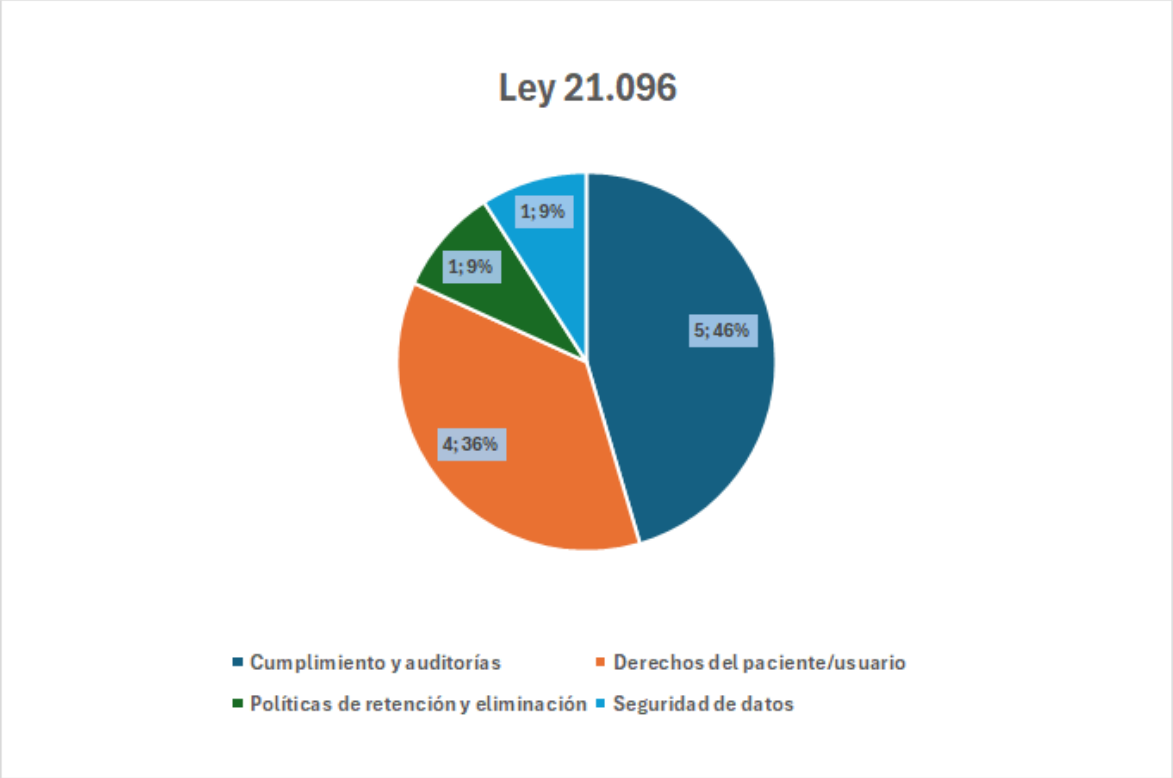


Figura 15: Categorías de lineamientos e indicaciones generados para ley 21.096

5.3.5. Resultados generales

Los resultados obtenidos se consideran buenos en general ya que estos permitieron describir de manera comprensiva los lineamientos necesarios para estar en cumplimiento con las regulaciones y leyes propuestas, todo esto en base a información muy acotada como lo fue el contexto configurado inicialmente para el LLM.

Regulación	Indicaciones Generadas	Artículos cubiertos	Artículos faltantes por cubrir	Indicaciones generadas erróneamente
HIPAA	33	31	N/A	0
Ley 19.628	11	12	0	0
Ley 20.584	6	4	0	1
Ley 21.096	11	8	N/A	0

Tabla 8: Resultados obtenidos para análisis de las 4 regulaciones propuestas

Teniendo en cuenta que se hizo uso de información de carácter público, se plantea como una posible mejora adaptar las entradas del modelo para que acepten la regulación en un formato más fácil de analizar y/o clasificar. Esto puede llevar a ahorros de tiempo,

complejidad y costos.

Sin embargo, al poder asegurar de manera cuantitativa una cobertura tan alta, que considera la totalidad de los artículos de las leyes nacionales, podemos decir que la solución propuesta es un buen punto de partida para el análisis de regulaciones mediante automatización con LLMs. De igual manera, sigue siendo prioritario que esta información generada pueda ser validad por un equipo legal o de cumplimiento para asegurar una cobertura adecuada y poder refinar el modelo y sus resultados para futuras implementaciones o iteraciones.

Por último, al hacer un análisis de los lineamientos generados tomando en cuenta las cuatro regulaciones, se puede observar que se tiene una distribución de los lineamientos enfocados, y en su mayoría generados, para el manejo de derechos del paciente sobre sus datos.

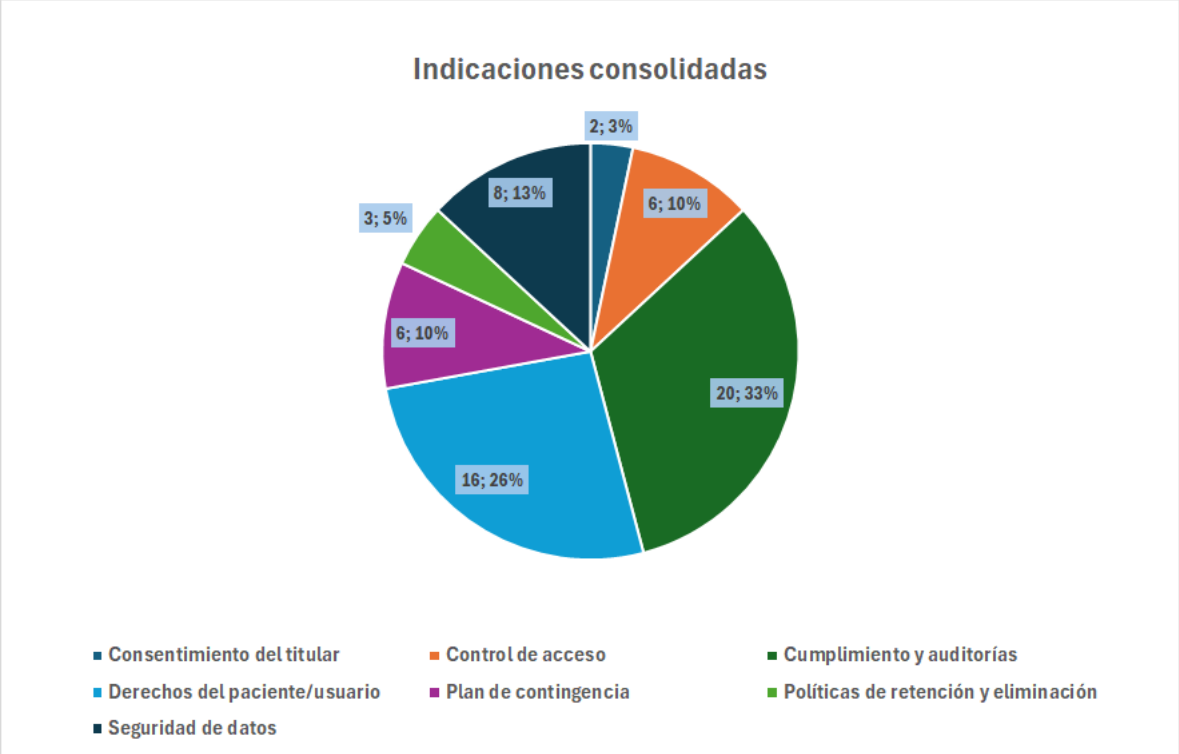


Figura 16: Consolidado de las indicaciones generadas para las 4 regulaciones. (HIPAA, Ley 19.628, 20.584 y 21.096)

El hallazgo principal a rescatar, podría decirse que es el hecho de que el enfoque sobre el paciente y cumplimiento normativo viene dado por el contexto que se le entrega al LLM antes de generar la respuesta. Ya que como se menciona anteriormente, el contexto provisto permite acotar los resultados que se generan, dando así mayor precisión al contenido.

De igual manera, esto podría ser parametrizado para otros casos de uso donde el enfoque no

necesariamente sea el usuario, dando así una gran cantidad de posibilidades sobre el contenido e información de la organización. Tomando en cuenta que el trabajo se realizó a partir de los datos crudos de Techneworks, este trabajo puede verse apalancado en ambientes de grado empresarial ya que en general tienden a tener conjuntos de datos previamente etiquetados con los que se podría validar automáticamente los resultados, y llevar una revisión continua con mínimo esfuerzo de mantenimiento.

5.4. Revisión de Sistema de Gestión

Se busca validar la solución planteada como sistema de gestión para las políticas de privacidad. Para este caso se propone un sistema que ayuda específicamente a mapear los procesos que realiza Kinteractive para dar cumplimiento según el artículo 30 de la regulación GDPR.

Se modeló el proceso de documentación que establece la regulación, también denominado *mapeo de datos*, incluyendo atributos sobre los datos personales recolectados y tratados. Para documentar los procesos que realiza Kinteractive es necesario hacer un listado de los procesos de tratamiento de datos que realizan, garantizar que la información obtenida sea con consentimiento explícito y debe documentar la siguiente información con cada proceso que Kinteractive realiza con los datos personales:

- Identidad y datos de contacto del responsable y DPO de los datos.
- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Los destinatarios o las categorías de destinatarios de los datos personales.
- Plazos de retención de los datos.

El sistema de gestión está diseñado con el objetivo de generar la política de privacidad, considerando los procesos según el mapeo de datos. Esto necesario como evidencia para la regulación de privacidad GDPR y considera como enfoque principal la privacidad del paciente o usuario del sistema.

Para cada proceso a documentar, se tiene registro de los activos de datos asociados a este y el detalle de estos activos de datos. En general, para cada activo de datos se debe recopilar y documentar la siguiente información del mismo:

- Nombre.
- DPO.
- Fuente de la información.
- Tipos de datos que maneja.

- Base de datos o conjunto de datos manejados.

Adicionalmente, la solución lleva registro de los tipos de datos que se han detectado en los conjuntos de datos de cada activo y genera indicaciones y lineamientos a seguir para estar en cumplimiento según las regulaciones que se le indiquen; este proceso mencionado está descrito y validado en 5.2 y 5.3 respectivamente. La componente de análisis de datos permite diferenciar y hacer un análisis sobre la información que se espera que maneje la organización y la que realmente se está usando, mientras que la componente de análisis de las regulaciones genera indicaciones que permiten cerrar brechas entre las regulaciones y la operación de la organización.
La implementación propuesta mencionada en 4.8 se detalle en las siguientes figuras:

```
class DataType

# @title class DataType
class DataType:
  def __init__(self, name:str, description:str,\
               category:str, is_personal_data:bool):
    self.name = name
    self.description = description
    self.category = category
    self.is_personal_data = is_personal_data
```

Figura 17: Implementación de la clase Tipo de Dato y sus atributos

```
class DataCategory

# @title class DataCategory
class DataCategory:
  def __init__(self, name:str):
    self.name = name
    self.data_types:set[DataType] = set()
```

Figura 18: Implementación de la clase Categoría de Dato y sus atributos

```
class DataAsset

# @title class DataAsset
class DataAsset:
  def __init__(self, name:str, source:str, dpo:str):
    self.name = name
    self.dpo = dpo
    self.source = source
    self.data_types:set[DataType] = set()
    self.df_data:pd.DataFrame = None
    self.detected_data_types:dict[str] = {}
```

Figura 19: Implementación de la clase Activo de Datos y sus atributos

```
class Regulation
[ ]  1 # @title class Regulation
     2 class Regulation:
     3   def __init__(self,regulation=None,data_str=None):
     4     self.name:str = regulation
     5     if regulation:
     6       self.data_str = data_str
     7       self.df_cumplimiento:pd.DataFrame = self.set_cumplimiento()
```

Figura 21: Implementación de la clase Regulación y sus atributos

```
class Process (GDPR Mapping)
     1 # @title class Process (GDPR Mapping)
     2 class Process:
     3   def __init__(self, name:str, data_sources:list[str],\
     4                purpose:list[str], recipients:list[str],\
     5                storage_location:list[str],\
     6                retention_period\:list[str]):
     7     self.name = name
     8     self.data_sources = data_sources
     9     self.data_assets:list[DataAsset] = []
    10     self.purpose = purpose
    11     self.recipients = recipients
    12     self.storage_location = storage_location
    13     self.retention_period = retention_period
```

Figura 20: Implementación de la clase Proceso GDPR y sus atributos

```
class PrivacyPolicy
     1 # @title class PrivacyPolicy
     2 class PrivacyPolicy:
     3     def __init__(self):
     4         self.dpo = dpo = ''
     5         self.gdpr_mapping:dict[Process] = {}
     6         self.regulations:dict[Regulation] = {}
     7         self.privacy_policy_string:str = ''
```

Figura 22: Implementación de la clase Política de Privacidad y sus atributos

El control estricto implementado permite mantener consistencia entre la información levantada inicialmente por la organización y la que se genera a lo largo del tiempo conforme a la organización adquiere más pacientes y realiza más tratamiento de datos.

Para el caso de Kinteractive se tienen 3 procesos registrados que corresponden a:

- Reclutamiento de empleados
- Incorporación de socios
- Incorporación de clientes

Estos consisten de diferentes atributos definidos según el artículo 30 de la GDPR, donde se hace uso del sistema de gestión para levantar dichos procesos, y se usa la componente de análisis de tipos de datos para determinar la información sensible que se maneja en los activos de datos asociados a cada uno de estos procesos.

En la siguiente sección se deja el ejemplo generado por la solución, donde se hace uso de los conjuntos de datos descritos en 5.2 y se indica cada uno de los tipos de datos identificados por activo de datos, y la información asociada a estos. En particular la información asociada será denominada como “metadadata” la cual corresponde a la ubicación dentro de la base de datos, es decir el nombre de la columna.

Cabe destacar que los hallazgos presentados a continuación fueron validados previamente y representan la información que maneja la organización para cada proceso y como se lleva registro de este con el sistema de gestión. Esto permite mantener actualizado el registro de los datos que se están moviendo dentro del ambiente de Kinteractive dinámicamente, permite obtener documentación que cumpla con las regulaciones para ser mostradas en auditorías y por último, cumple con los requisitos de GDPR para tener en cada proceso y mantener el cumplimiento con las diferentes reglas que propone.

5.4.1. Proceso de mapeo de datos

Política de Privacidad de Datos
Esta política describe nuestro compromiso con la protección de datos personales y el cumplimiento de las regulaciones de privacidad de datos.

Información de Contacto:
Si tiene alguna pregunta sobre esta política, por favor contáctenos en contacto@techne-works.cl.

Revisión y Actualizaciones de la Política:
Podemos actualizar esta política de vez en cuando para reflejar cambios en nuestras prácticas o requisitos legales. Por favor, revise periódicamente para ver las actualizaciones.

Tipos de Datos Cubiertos
Nombre: Dirección de Correo Electrónico
Descripción: Una dirección de correo electrónico utilizada para enviar y recibir correos electrónicos.
Categoría: Información de Contacto
Datos personales: Sí

Nombre: Historial de Compras
Descripción: Un registro de los productos y servicios comprados por un cliente.
Categoría: Datos de Transacción
Datos personales: No

Nombre: Datos de Geolocalización
Descripción: Información que puede ser utilizada para identificar la ubicación física de un dispositivo.
Categoría: Información de Ubicación
Datos personales: No

Nombre: Expedientes Médicos
Descripción: Documentación del historial médico y atención de un paciente.
Categoría: Información de Salud
Datos personales: Sí

========== Mapeo de Procesos de Datos - GDPR ==========
1. Proceso: Reclutamiento de Empleados Activo de datos: Base de Datos de Clientes Elementos/tipos de datos detectados ([metadata])

- Número de identificación ([id], [identification number])
- Correo electrónico ([email_address, personal_email, Email Address])
- Número de teléfono: ([home_phone, fax_number, business_phone, phone number, contact information])
- Ciudad ([city, Location])
- Apellido ([last_name, Surname])
- Nombre ([first_name, Given name])
- Título de empleo ([job_title,Employment Information])
- País ([country_region, location])
- Habilidad lenguaje: ([notes, miscellaneous information])
- Dirección ([address], [home location])
- Región ([state_province, Location])
- Código Postal ([zip_postal_code, Address])

Fuentes de datos: Portales de empleo en línea, Referencias de empleados, Agencias de reclutamiento.
Finalidades: Contratación de nuevos empleados, Construcción de una reserva de talentos.
Destinatarios: Departamento de RRHH, Gerentes de contratación, Agencias de reclutamiento.
Ubicación de almacenamiento: Sistema de seguimiento de candidatos, Base de datos de RRHH.

Período de retención: 3 años, Hasta la retirada del candidato.

————————————————

2. Proceso: Incorporación de Socios Activo de datos: Análisis de Sitio Web Elementos/tipos de datos detectados:

- Número de identificación ([id], [identification number])
- Correo electrónico ([email_address, personal_email, Email Address])
- Número de teléfono: ([home_phone, fax_number, business_phone, phone number, contact information])
- Ciudad ([city, Location])
- Apellido ([last_name, Surname])
- Nombre ([first_name, Given name])
- Título de empleo ([job_title,Employment Information])
- País ([country_region, location])
- Habilidad lenguaje: ([notes, miscellaneous information])
- Dirección ([address], [home location])
- Región ([state_province, Location])
- Código Postal ([zip_postal_code, Address])
- Número de CPF
- Número de tarjeta de crédito: ([FINANCIAL_BANK_ACCOUNT (Financial accounts), FINANCIAL_CC_ACCOUNT (Credit card account number), Bank account details, Financial Information])
- Código de banco: ([FINANCIAL_BANK_BIC (persons BIC), Bank Identifier Code])
- Número de cuenta IBAN: ([FINANCIAL_BANK_IBAN (persons IBAN), Bank Account Information])
- Número de ruta bancaria: ([FINANCIAL_BANK_ROUTING (Bank routing number), Bank account details])
- Código swift: ([FINANCIAL_BANK_SWIFT (SWIFT number), Bank account information])
- Ingresos: ([DEMOGRAPHIC_INCOME (Income)], [Income])
- Identificador de gobierno: ([ID_DRIVER_ID (US drivers license ID number), Drivers license number])

- ID de empleado: ([ID_EMPLOYEE_ID (Employee ID), Employment Information])
- Número de licencia de vehículo ([ID_VEHICLE_LICENSE (Vehicle license plate number)], [Vehicle Information])
- Número de identificación de vehículo ([ID_VEHICLE_VIN (Vehicle identification number)], [Vehicle Information])

Fuentes de datos: Formulario de registro en línea, formulario en sede.
Finalidades: Prestación de servicios, ejecución de un contrato.
Destinatarios: Equipo de ventas interno, CRM de terceros, Recursos humanos.
Ubicación de almacenamiento: Base de datos en la nube.
Período de retención: 3 años.

————————————————

3. Proceso: Incorporación de Clientes Activo de datos: Registros de Clientes Elementos/tipos de datos detectados:

- Número de ifentificación ([id], [identification number])
- Primer nombre ([NAME_FIRST (persons first name)], [First Name])
- Apellido ([NAME_LAST (persons last name)], [Surname])
- Sufijo ([NAME_SUFFIX (persons name suffix)], [Name Suffix])
- Título honorario: ([NAME_HONORIFIC (Honorific for a persons name)], [Title])
- Nombre ([Full Name], [Full Name])
- Dirección ([GEO_STREET_NAME (Street name)1], [Address])
- Ciudad ([GEO_CITY_NAME (City name)], [Location])
- Estado ([GEO_PROVINCE (Province/state name)], [Location])
- Código postal ([GEO_POSTAL_CODE (Postal code)], [Location])
- País ([GEO_COUNTRY (Country name)], [Country])
- Coordenadas ([GEO_COORDINATES (Geographical coordinates)], [Location])
- Número de teléfono ([CONTACT_PHONE (Phone number), CONTACT_PHONE:HOME (Home phone), CONTACT_PHONE:MOBILE (Mobile phone), CONTACT_PHONE:WORK (Work phone)], [Phone number, Phone Number, Phone Number, Work Contact Information])
- Correo electrónico ([CONTACT_EMAIL (Email)], [Email address])
- Número de seguridad social (SSN) ([ID_SSN (persons SSN)], [Social Security Number])

- Número de registro médico ([ID_MRN (Medical records number)], [Health information])
- Nombre de usuario ([AUTH_USERNAME Username], [Username])
- Fechas de acceso ([AUTH_ACCESS_DATE (Access time)], [Date of Access])
- Información encriptada ([AUTH_PASSWORD_HASH (Hashed password)], [Password])
- Pregunta de seguridad ([AUTH_RECOVERY (Recovery question answers)], [Security information])
- Perfil red social ([BIOGRAPHIC_SOCIAL_MEDIA (URL to persons social media account)], [Social Media Information])
- Edad ([DEMOGRAPHIC_AGE (Age)], [Age])
- Fecha de nacimiento ([DEMOGRAPHIC_DOB (Date of birth)], [Age])
- Idioma ([DEMOGRAPHIC_LANGUAGE (Persons language)], [Language])
- Nacionalidad ([DEMOGRAPHIC_NATIONALITY (Persons nationality)], [Nationality])
- Etnicidad ([DEMOGRAPHIC_RACE (Persons race)], [Race])
- Género ([DEMOGRAPHIC_SEX_OR_GENDER (Persons sex)], [Gender])
- Orientación sexual ([DEMOGRAPHIC_SEXUAL_PREFERENCE (Persons sexual preference)], [Sexual Orientation])
- Número de CPF
- Número de tarjeta de crédito: ([FINANCIAL_BANK_ACCOUNT (Financial accounts), FINANCIAL_CC_ACCOUNT (Credit card account number), Bank account details, Financial Information])
- Código de banco: ([FINANCIAL_BANK_BIC (persons BIC), Bank Identifier Code])
- Número de cuenta IBAN: ([FINANCIAL_BANK_IBAN (persons IBAN), Bank Account Information])
- Número de ruta bancaria: ([FINANCIAL_BANK_ROUTING (Bank routing number), Bank account details])
- Código swift: ([FINANCIAL_BANK_SWIFT (SWIFT number), Bank account information])
- Ingresos: ([DEMOGRAPHIC_INCOME (Income)], [Income])
- Identificador de gobierno: ([ID_DRIVER_ID (US drivers license ID number), Drivers license number])

- ID de empleado: ([ID_EMPLOYEE_ID (Employee ID), Employment Information])
- medical test result: ([MEDICAL_BLOOD_ (Persons blood)], [Medical Information])
- health condition: ([MEDICAL_DISABILITY (persons medical disabilities)], [Health Information])
- medication: ([MEDICAL_PRESCRIPTION (Medications)], [Health information])
- ip address: ([NETWORK_IP (IPv4 and IPv6 addresses)], [IP address])
- mac address: ([NETWORK_MAC (Unique ID for a network card)], [MAC Address])
- interest: ([PERSONAL_PREFERENCES (Non-specific sensetive preferences)], [Sensitive Personal Information])
- eye color: ([PHYSICAL_EYE_COLOR (persons eye color)], [Physical Traits])
- hair color: ([PHYSICAL_HAIR_COLOR (persons hair color)], [Physical Characteristics])
- physical measurement: ([PHYSICAL_MEASUREMENTS (persons measurements)], [Physical characteristics])

Fuentes de datos: Formulario de registro en línea, Sistema CRM
Finalidades: Prestación de servicios, Comunicaciones de marketing
Destinatarios: Equipo de ventas interno, CRM de terceros, Departamento de marketing
Ubicación de almacenamiento: Base de datos en la nube, Sistema CRM
Período de retención: 5 años, Hasta que el cliente se dé de baja

5.5. Verificación periódica y cumplimiento de política de privacidad

El método de verificación periódica del estado de la política de privacidad y su cumplimiento es una parte importante de la estrategia de TechneWorks para garantizar la protección efectiva de los datos de los pacientes. Este proceso se lleva a cabo de manera sistemática y regular para evaluar la conformidad de la empresa con sus propias políticas y con las regulaciones de privacidad y seguridad de datos aplicables.

Durante la verificación periódica, se es necesario realizar una serie de acciones diseñadas para evaluar la efectividad de las medidas de seguridad implementadas, así como el grado de cumplimiento de la política de privacidad. Esto incluye auditorías internas exhaustivas, pruebas de seguridad, evaluaciones de procedimientos, revisiones externas por parte de auditores independientes y evaluaciones del nivel de capacitación del personal en materia de privacidad y seguridad de datos.

Los resultados de estas verificaciones se utilizan para identificar posibles brechas o debilidades en el sistema de protección de datos y para tomar medidas correctivas y preventivas

adecuadas. Además, se generan informes detallados sobre los hallazgos y las acciones correctivas tomadas, y se implementan medidas de mejora continua para fortalecer aún más el programa de privacidad de datos de la empresa.

5.5.1. Auditorías

La periodicidad de las auditorías puede variar según las necesidades y el riesgo de la empresa, pero se recomienda realizarlas al menos una vez al año. Esto permite una evaluación exhaustiva y regular del cumplimiento de la política de privacidad y la identificación oportuna de cualquier área que requiera mejoras.

Lista de chequeo para la auditoría de cumplimiento de la política de privacidad:

A continuación, se estructura una lista de chequeo para la auditoría de cumplimiento de la política de privacidad la cual proporciona una guía para evaluar el grado en que la empresa cumple con sus compromisos y obligaciones en materia de privacidad de datos. Esta herramienta exhaustiva abarca diversos aspectos clave, desde la documentación y la gestión de consentimientos hasta las medidas de seguridad implementadas y la capacitación del personal. Al seguir esta lista de verificación detallada, la empresa puede identificar áreas de mejora, fortalezas y posibles riesgos en su cumplimiento de la política de privacidad, garantizando así la protección adecuada de los datos personales y el cumplimiento de las regulaciones aplicables.

- Revisión de la documentación de la política de privacidad y sus actualizaciones.
- Verificación del registro de consentimiento de los usuarios para el procesamiento de datos.
- Evaluación de los procedimientos de recopilación, almacenamiento y procesamiento de datos personales.
- Revisión de las medidas de seguridad implementadas para proteger los datos.
- Evaluación de los procedimientos para responder a solicitudes de acceso, rectificación y eliminación de datos.
- Verificación de la capacitación del personal en materia de privacidad de datos.
- Revisión de los acuerdos con terceros proveedores que puedan acceder a datos personales.
- Pruebas de seguridad de los sistemas informáticos y redes de la empresa.
- Evaluación de la respuesta a incidentes de seguridad de datos reportados.

- Verificación del cumplimiento de las regulaciones de privacidad y seguridad de datos aplicables.

Indicadores de cumplimiento

La medición de indicadores clave es fundamental para evaluar de manera efectiva el cumplimiento de la política de privacidad de una empresa. Estos indicadores proporcionan una visión cuantitativa y cualitativa del desempeño de la organización en términos de protección de datos y cumplimiento normativo.

Al tomar medidas regulares y sistemáticas de estos indicadores, la empresa puede monitorear de cerca su nivel de conformidad, identificar posibles áreas de riesgo o incumplimiento, y tomar medidas correctivas de manera oportuna. Además, la medición de indicadores permite a la empresa demostrar de manera objetiva su compromiso con la privacidad de los datos ante sus partes interesadas, incluidos clientes, socios comerciales y reguladores.

Esto contribuye a fortalecer la confianza del público en la empresa y a mitigar el riesgo de posibles sanciones legales o pérdida de reputación debido a incumplimientos de privacidad. A continuación, se proporcionan indicadores para medir el cumplimiento de la política.

- Porcentaje de cumplimiento de la política de privacidad: Este indicador mide el grado en que la empresa cumple con los requisitos establecidos en su política de privacidad. Se calcula dividiendo el número de medidas de cumplimiento implementadas entre el total de medidas requeridas y multiplicando por 100.
- Número de incidentes de seguridad reportados: Este indicador cuenta el número de incidentes de seguridad de datos que se han reportado durante un período determinado. Un aumento en el número de incidentes puede indicar debilidades en el cumplimiento de la política de privacidad o la necesidad de mejorar las medidas de seguridad.
- Tiempo medio de respuesta a solicitudes de acceso a datos: Mide la rapidez con la que la empresa responde a las solicitudes de acceso a datos personales por parte de los usuarios. Un tiempo de respuesta más corto indica una mayor eficiencia en la gestión de solicitudes y un mejor cumplimiento de los derechos de los usuarios.
- Número de capacitaciones realizadas sobre privacidad de datos: Este indicador registra el número de sesiones de capacitación realizadas sobre privacidad de datos para el personal de la empresa. Un aumento en el número de sesiones puede indicar un mayor compromiso con la formación y concienciación sobre privacidad de datos.
- Resultados de las pruebas de seguridad: Se refiere a los resultados de las pruebas de penetración y evaluaciones de seguridad realizadas en los sistemas de la empresa. Un bajo número de vulnerabilidades identificadas y una alta puntuación en las pruebas de seguridad indican un buen nivel de cumplimiento de las medidas de seguridad.

Capacitación del personal en materia de privacidad y seguridad de datos

La propuesta de capacitación del personal en materia de privacidad y seguridad de datos es fundamental para garantizar un adecuado cumplimiento de las políticas establecidas y para fortalecer la cultura organizacional en torno a la protección de datos. Para llevar a cabo esta propuesta de manera efectiva, se deben realizar una serie de acciones concretas.

En primer lugar, es necesario diseñar un programa de capacitación integral que aborde los aspectos clave de la privacidad y seguridad de datos, adaptado a las necesidades y roles específicos de cada miembro del personal. Este programa debe incluir sesiones de formación presenciales o virtuales, materiales educativos, casos de estudio y evaluaciones para medir el nivel de comprensión y retención de los conceptos impartidos.

La capacitación debe ser impartida por expertos en privacidad y seguridad de datos, ya sea internos o externos a la organización, y debe estar actualizada en función de las regulaciones vigentes y las mejores prácticas de la industria. Se debe establecer un calendario de capacitación periódica para garantizar que todo el personal reciba formación regularmente y se mantenga al tanto de los cambios en las políticas y procedimientos.

La frecuencia de las sesiones de capacitación puede variar según las necesidades específicas de la organización, pero se recomienda realizar al menos una sesión anual de actualización y revisión de políticas, así como sesiones adicionales para nuevos empleados o en caso de cambios significativos en las regulaciones o procesos internos.

En cuanto al porcentaje de adherencia óptimo, se busca alcanzar una tasa cercana al 100 %. Sin embargo, se debe tener en cuenta que el éxito de la capacitación no solo se mide en términos de participación, sino también en términos de comprensión y aplicación de los conceptos aprendidos en el trabajo diario. Por lo tanto, es importante evaluar regularmente la efectividad de la capacitación mediante encuestas de satisfacción, pruebas de conocimientos y evaluaciones de desempeño.

Para optimizar la capacitación del personal, es recomendable utilizar una variedad de métodos educativos, como presentaciones interactivas, estudios de casos, simulaciones y ejercicios prácticos. Además, se pueden ofrecer recursos adicionales, como manuales de referencia, documentos de políticas y procedimientos, y sesiones de tutoría individualizada para abordar preguntas o inquietudes específicas.

En resumen, la capacitación del personal en materia de privacidad y seguridad de datos es un proceso continuo y multidimensional que requiere un enfoque estratégico y sistemático. Al invertir en la formación y el desarrollo de su personal, las organizaciones pueden fortalecer su postura en materia de privacidad y seguridad, mitigar riesgos y cumplir con las regulaciones aplicables de manera efectiva.

5.6. Propuesta de mejoras a futuro

La solución inicialmente abarca la creación de una política de privacidad para la organización Kinteractive, la cual se redacta en base a las necesidades de los usuarios, los clientes y sus derechos sobre sus datos personales. Dado el diseño de la solución y su enfoque, se puede decir que esta busca definir las necesidades de la organización para estar en cumplimiento con las regulaciones necesarias, esto quiere decir que el mismo trabajo puede ser extendido a otro dominio de datos o a otras regulaciones según los requerimientos de la organización o el negocio.

Las mejoras propuestas son en diferentes dimensiones y aspectos de los problemas que se pueden encontrar al trabajar con privacidad de datos. Las principales mejoras que fueron discutidas y evaluadas durante la elaboración del sistema son:

- Hacer uso de modelos de inteligencia artificial en conjunto con algoritmos de detección para tipos de datos específicos. En el caso de datos como tarjetas de crédito, estas son secuencias de números basadas en un algoritmo que se puede comprobar, por esta razón se recomendaría validar los hallazgos del modelo con un algoritmo específico. De manera que cada vez que se obtenga un tipo de dato con un algoritmo de validación asociado, se realice este proceso.
- Crear flujos de procesos alternativos elevaría el alcance de la solución al poder funcionar como un orquestador de eventos, de manera que cada vez que se realicen detecciones de datos sensibles o se completen ciertos eventos, se desencadenen flujos adicionales a los descritos en este trabajo y así tener más capacidades de integración con otros sistemas de la organización.
- Considerando que se está trabajando con un LLM de Open AI de acceso público, estos resultados pueden mejorarse al conseguir infraestructura dedicada al caso de uso que se requiera. Es decir, es posible obtener los modelos que ofrecen las diferentes compañías proveedoras de servicios de LLMs y entrenarlos con datos específicos de la organización y del negocio al que será orientada la solución, esto permitiría obtener mejores tasas de detección con muestras de datos más reducidas.
- Al tener múltiples tipos de datos que se repiten en las diferentes muestras y ambientes que son analizados, se puede crear un diccionario de datos que permita recolectar información sobre tipos de datos encontrados recurrentemente, por ejemplo, a medida que se encuentran múltiples columnas que corresponden a correo electrónico, se registra información de que el tipo de dato “Email” puede ser visto con la etiqueta “E-mail”, “Correo electrónico”, “web mail”, entre otros, ahorrando el análisis de las filas de datos. Se puede armar un diccionario que tenga estos términos previamente guardados y hacer búsquedas más eficientes en base a los nombre de las columnas.
- Revisar el proceso propuesto y los resultados obtenidos, es decir, analizar en detalle el proceso bajo el que se generan los requerimientos y contextos para el LLM y las políticas generadas con la ayuda de un profesional o abogado en el área de cumplimiento.

Esto permite desplazar parte de la carga de trabajo dentro de la organización del área legal y de cumplimiento a procesos automatizados.

CAPÍTULO 6
CONCLUSIONES

La elaboración de una política de privacidad adaptada a las regulaciones HIPAA y a las leyes chilenas es un componente crucial para asegurar la protección de los datos de los pacientes en el ámbito de la salud. Esta política no solo garantiza el cumplimiento legal, sino que también fortalece la confianza de los pacientes en la organización. Es esencial reconocer que la privacidad y seguridad de los datos son aspectos críticos en el tratamiento de la información médica, y su adecuado cumplimiento es necesario para cumplir con los estándares y expectativas tanto nacionales como internacionales.

Las regulaciones internacionales y nacionales establecen directrices específicas que las organizaciones deben seguir para proteger la privacidad de los datos. En este sentido, es fundamental que TechneWorks se mantenga al día con estos requisitos y los integre de manera efectiva en su política de privacidad. La complejidad de estas regulaciones y su constante evolución implican que la organización debe establecer mecanismos para monitorear y adaptar su política de manera continua.

Para enfrentar los desafíos en la implementación de políticas de privacidad, TechneWorks debe establecer un enfoque proactivo y estratégico. Esto incluye la asignación de recursos adecuados para abordar las necesidades de capacitación del personal, la implementación de tecnologías seguras y la realización de evaluaciones periódicas de riesgos y auditorías de cumplimiento. Además, es esencial que la organización promueva una cultura de privacidad y seguridad de datos en todos los niveles, desde la alta dirección hasta el personal operativo.

En cuanto a la capacitación del personal, se recomienda que TechneWorks desarrolle un programa integral que incluya sesiones regulares de formación y actualización, así como recursos educativos accesibles para todos los empleados. Estas iniciativas no solo fortalecerán el conocimiento y la conciencia del personal en materia de privacidad y seguridad de datos, sino que también fomentarán una cultura organizacional comprometida con la protección de la información confidencial de los pacientes.

El uso de tecnologías relacionadas a la inteligencia artificial, como los LLMs, fueron un punto crucial en el desarrollo de este trabajo, ya que se hizo mucho énfasis en lo dinámico y cambiantes que son los ambientes de datos como el de Kinteractive, pero manteniendo la necesidad de mantener una cierta estructura para los procesos que realiza. Al contar con soluciones que apalancan estas capacidades de analizar datos con procesamiento de lenguaje natural se abren múltiples posibilidades a procesos que sean igual o más confiables que la revisión o humana, y con un grado de automatización que permitiría crecer exponencialmente el ambiente de datos manteniendo los costos y esfuerzos de analizar grandes cantidades de datos al mínimo.

El mayor aprendizaje obtenido es el cambio de paradigma que debe ser acogido por las

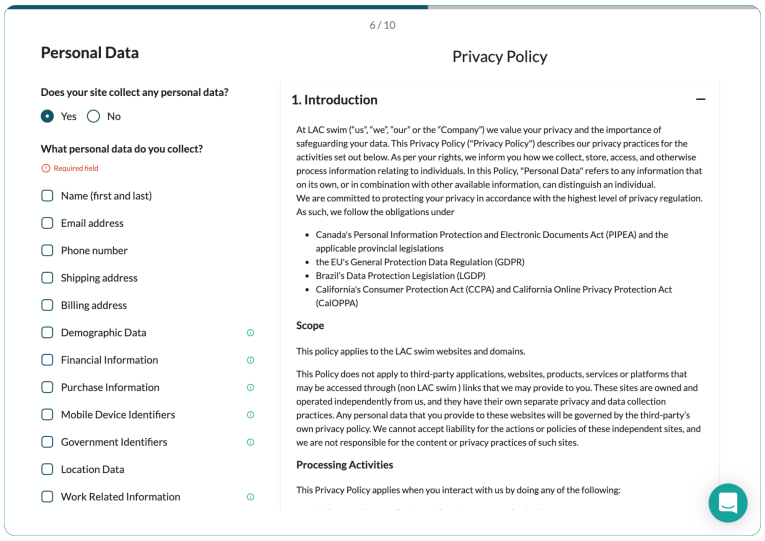
áreas de organizaciones que se enfoquen en cumplimiento y área legal; quedó evidenciado en el estudio previo que el manejo convencional de políticas de manera estática o que requieren ser generadas y validadas manualmente es un enfoque que no es posible escalar y consume muchos recursos especializados. La solución propuesta se define como un primer paso en el ámbito legal administrado con inteligencia artificial, sirve como precursor y antecedente a futuras iteraciones que buscarán optimizar los recursos utilizados y explotar de mejor manera los recursos existentes como lo son las fuentes públicas de información y conjuntos de datos especializados durante el entrenamiento.

Adicionalmente, se espera que este proyecto pueda ser continuado considerando las propuestas de mejora, ya que estas agregan no solo una capa de flexibilidad a la solución dentro de diferentes ámbitos de datos, también agrega funcionalidades que pueden llevar más allá el proceso de automatización ya que reduciría considerablemente las excepciones y casos de borde que pueden requerir revisión manual.

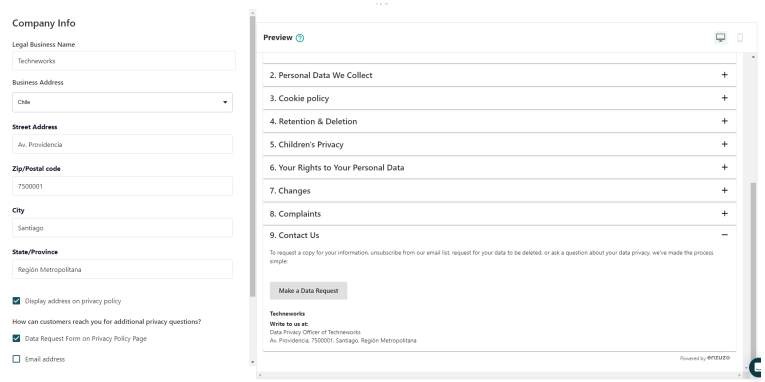
En definitiva, se espera que este proyecto sea solo el comienzo de una larga serie de sistemas futuros e iteraciones que puedan ampliar las capacidades de automatización dentro del área de la salud, siempre teniendo en consideración que esto se hace en beneficio y para los pacientes de la organización, cuya privacidad es el foco de este sistema y de esta solución en general.

Anexos

Anexo A



(a) Vista 1 herramienta Enzuzo



(b) Vista 2 herramienta Enzuzo

Anexo B

	Nombre de columna	Dato detectado	Columna detectada	Coincidencia dato detectado	Coincidencia columna detectada
1	id	numerical datum	Identification Number	0,5	1
2	email_address	email address	Email Address	1	1
3	personal_email	email	Email Address	1	1
4	home_phone	phone number	Contact Information	1	1
5	fax_number	phone number	Contact Information	1	1
6	city	city	Residential Location	1	1
7	last_name	last name	Surname	1	1
8	first_name	first name	Personal Identification	1	0,5
9	job_title	job title	Employment Information	1	1
10	business_phone	phone number	Contact Information	1	1
11	country_region	country	Residential Location	1	1
12	notes	employment history and language proficiency	Personal Commentary	1	0,5
13	company	company name	Employment Information	1	1
14	address	address	Location	1	1
15	state_province	location	Location	1	1
16	zip_postal_code	zip code	Residential Address	1	1
17	col1	numeric datum	Unknown	1	0
18	col2	full name	Unknown	1	0
19	col3	credit card number	Unknown	1	0
20	col4	brazilian social security numbers (cpf)	Unknown	1	0
21	col5	brazilian taxpayer registry number (cpf)	Unknown	1	0
22	col6	email address	Unknown	1	0
23	col7	credit card number	Unknown	1	0
24	col8	phone number	Unknown	1	0
25	col9	birthdate	Unknown	1	0
26	col10	city	Unknown	1	0
27	col11	state code	Unknown	1	0
28	col12	financial information	Unknown	1	0
29	col13	nationality	Unknown	1	0
30	col14	product code	Unknown	0,5	0
31	col15	brazilian company registration number	Unknown	1	0
32	name)	first name	First Name	1	1
33	NAME_LAST (persons last name)	last name	Last Name	1	1
34	NAME_SUFFIX (persons name suffix)	suffix	Name Suffix	1	1
35	NAME_HONORIFIC (Honorific for a persons name)	title	Title	1	1
36	Full Name	name	Identity	1	1
37	GEO_STREET_NAME (Street name)1	address	Street Address	1	1
38	GEO_CITY_NAME (City name)	city name	City	1	1
39	GEO_PROVINCE (Province/state name)	state abbreviation	Geographical Location	1	1
40	GEO_POSTAL_CODE (Postal code)	zip code	Location	1	1
41	GEO_COUNTRY (Country name)	country name	Country of Residence	1	1
42	GEO_COORDINATES (Geographical coordinates)	geolocation coordinate	Location	1	1
43	CONTACT_PHONE (Phone number)	phone number	Phone Number	1	1
44	CONTACT_PHONE:HOME (Home phone #)	phone number	Phone Number	1	1
45	CONTACT_PHONE:MOBILE (Mobile phone #)	phone number	Phone Number	1	1
46	CONTACT_PHONE:WORK (Work phone #)	phone number	Phone Number	1	1
47	CONTACT_EMAIL (Email)	email address	Email address	1	1
48	ID_SSN (persons SSN)	social security number	Social Security Number	1	1
49	ID_MRN (Medical records number)	medical record number	Medical Information	1	1
50	AUTH_USERNAME Username	twitter username	Authentication Username	1	1
51	AUTH_ACCESS_DATE (Access time)	timestamp	Date/Time of Authentication Access	1	1
52	AUTH_PASSWORD (Unhashed password)	username	Sensitive Personal Data	0,5	0,5
53	AUTH_PASSWORD_HASH (Hashed password)	hashed identifier	Password	1	1
			Total	80	67,5

Tabla 9: Extracto de muestra de datos y coincidencias de análisis de datos sensibles con modelo GPT-4

	Nombre de columna	Dato detectado	Columna detectada	Coincidencia dato detectado	Coincidencia columna detectada
1	id	unknown	Identifier	0,5	1
2	email_address	email address	Contact Information	1	1
3	personal_email	email address	Email Address	1	1
4	home_phone	phone number	Phone Number	1	1
5	fax_number	phone number	Contact Information	1	1
6	city	city name	Location Information	1	1
7	last_name	name	Name	0,5	1
8	first_name	name	Name	0,5	1
9	job_title	occupation	Employment Information	1	1
10	business_phone	phone number	Contact Information	1	1
11	country_region	country	Geographic Information	1	1
12	notes	employment history	Other	1	1
13	company	travel history	Organizational Information	-1	1
14	address	address	Location Information	1	1
15	state_province	state or region	Location Information	1	1
16	zip_postal_code	zip code	Location Data	1	1
17	col1	numerical sequence	Unknown	1	0
18	col2	name	Unknown	1	0
19	col3	credit card number	Unknown	1	0
20	col4	cpf number	Unknown	1	0
21	col5	identification number	Unknown	1	0
22	col6	email address	Unknown	1	0
23	col7	credit card number	Unclear	-1	0
24	col8	phone number	Unknown	1	0
25	col9	dates of birth	Unknown	1	0
26	col10	city	Unknown	1	0
27	col11	brazilian state	Unknown	1	0
28	col12	salary	Unknown	1	0
29	col13	nationality	Unknown	1	0
30	col14	license plate number	Unknown	0	0
31	col15	cnpj	Unknown	1	0
32	NAME_FIRST (persons first name)	name	First Name	0,5	1
33	NAME_LAST (persons last name)	name	Name	0,5	1
34	NAME_SUFFIX (persons name suffix)	suffix	Identity Information	1	1
35	NAME_HONORIFIC (Honorific for a persons name)	title	Personal Information	1	1
36	Full Name	name	Name	1	1
37	GEO_STREET_NAME (Street name)1	address	Address Information	1	1
38	GEO_CITY_NAME (City name)	city	Location Information	1	1
39	GEO_PROVINCE (Province/state name)	state	Geographic Information	1	1
40	GEO_POSTAL_CODE (Postal code)	zip code	Location Information	1	1
41	GEO_COUNTRY (Country name)	country name	Geographic Information	1	1
42	GEO_COORDINATES (Geographical coordinates)	geographical coordinate	Geolocation Data	1	1
43	CONTACT_PHONE (Phone number)	phone number	Contact Information	1	1
44	CONTACT_PHONE:HOME (Home phone #)	phone number	Phone Number	1	1
45	CONTACT_PHONE:MOBILE (Mobile phone #)	phone number	Contact Information	1	1
46	CONTACT_PHONE:WORK (Work phone #)	phone number	Phone Number	1	1
47	CONTACT_EMAIL (Email)	email address	Email Address	1	1
48	ID_SSN (persons SSN)	social security number (ssn)	Identification Number	1	1
49	ID_MRN (Medical records number)	medical record numbers (mrn)	Medical Information	1	1
50	AUTH_USERNAME Username	username	Credential Information	1	1
51	AUTH_ACCESS_DATE (Access time)	datetime	Temporal Information	1	1
52	AUTH_PASSWORD (Unhashed password)	Mix of alphanumeric strings that could represent various forms of personal identifiers	Password	1	1
53	AUTH_PASSWORD_HASH (Hashed password)	hash	Authentication information	1	1
			Total	74	69

Tabla 10: Extracto de muestra de datos y coincidencias de análisis de datos sensibles con modelo GPT-4o

	Nombre de columna	Dato detectado	Columna detectada	Coincidencia dato detectado	Coincidencia columna detectada
1	id	unknown	Identifier	0,5	1
2	email_address	email address	Contact Information	1	1
3	personal_email	email address	Email Address	1	1
4	home_phone	phone number	Phone Number	1	1
5	fax_number	phone number	Contact Information	1	1
6	city	city name	Location Information	1	1
7	last_name	name	Name	0,5	1
8	first_name	name	Name	0,5	1
9	job_title	occupation	Employment Information	1	1
10	business_phone	phone number	Contact Information	1	1
11	country_region	country	Geographic Information	1	1
12	notes	employment history	Other	1	1
13	company	travel history	Organizational Information	-1	1
14	address	address	Location Information	1	1
15	state_province	state or region	Location Information	1	1
16	zip_postal_code	zip code	Location Data	1	1
17	col1	numerical sequence	Unknown	1	0
18	col2	name	Unknown	1	0
19	col3	credit card number	Unknown	1	0
20	col4	cpf number	Unknown	1	0
21	col5	identification number	Unknown	1	0
22	col6	email address	Unknown	1	0
23	col7	credit card number	Unclear	-1	0
24	col8	phone number	Unknown	1	0
25	col9	dates of birth	Unknown	1	0
26	col10	city	Unknown	1	0
27	col11	brazilian state	Unknown	1	0
28	col12	salary	Unknown	1	0
29	col13	nationality	Unknown	1	0
30	col14	license plate number	Unknown	0	0
31	col15	cnpj	Unknown	1	0
32	NAME_FIRST (persons first name)	name	First Name	0,5	1
33	NAME_LAST (persons last name)	name	Name	0,5	1
34	NAME_SUFFIX (persons name suffix)	suffix	Identity Information	1	1
35	NAME_HONORIFIC (Honorific for a persons name)	title	Personal Information	1	1
36	Full Name	name	Name	1	1
37	GEO_STREET_NAME (Street name)1	address	Address Information	1	1
38	GEO_CITY_NAME (City name)	city	Location Information	1	1
39	GEO_PROVINCE (Province/state name)	state	Geographic Information	1	1
40	GEO_POSTAL_CODE (Postal code)	zip code	Location Information	1	1
41	GEO_COUNTRY (Country name)	country name	Geographic Information	1	1
42	GEO_COORDINATES (Geographical coordinates)	geographical coordinate	Geolocation Data	1	1
43	CONTACT_PHONE (Phone number)	phone number	Contact Information	1	1
44	CONTACT_PHONE:HOME (Home phone #)	phone number	Phone Number	1	1
45	CONTACT_PHONE:MOBILE (Mobile phone #)	phone number	Contact Information	1	1
46	CONTACT_PHONE:WORK (Work phone #)	phone number	Phone Number	1	1
47	CONTACT_EMAIL (Email)	email address	Email Address	1	1
48	ID_SSN (persons SSN)	social security number (ssn)	Identification Number	1	1
49	ID_MRN (Medical records number)	medical record numbers (mrn)	Medical Information	1	1
50	AUTH_USERNAME Username	username	Credential Information	1	1
51	AUTH_ACCESS_DATE (Access time)	datetime	Temporal Information	1	1
52	AUTH_PASSWORD (Unhashed password)	Mix of alphanumeric strings that could represent various forms of personal identifiers	Password	1	1
84	PHYSICAL_MEASUREMENTS (persons measurements)	height and weight	Biometric Information	1	1
			Total	73,5	69

Tabla 11: Extracto de muestra de datos y coincidencias de análisis de datos sensibles con modelo GPT-4t

Anexo C

	Puntos clave	Descripción	Requisitos de cumplimiento	Indicación según HIPAA Privacy Rule
1	Confidencialidad	Protección de la información de salud del paciente (PHI) contra el acceso no autorizado	Implementar medidas de seguridad administrativas, físicas y técnicas para garantizar la confidencialidad de la PHI.	Access and Uses. For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.
2	Integridad	Garantizar que la PHI no se altere ni se destruya de manera no autorizada	Implemente medidas como el cifrado y las copias de seguridad seguras de los datos para mantener la integridad de los datos.	§ 164.306 Security standards: General rules. (a) General requirements. Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
3	Disponibilidad	Garantizar que la PHI sea accesible cuando sea necesario para los usos autorizados	Establezca planes de contingencia, procesos de recuperación de datos y sistemas de respaldo para garantizar la disponibilidad de la PHI.	(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
4	Controles de acceso	Limitar el acceso a la PHI solo al personal autorizado	Utilice ID de usuario únicos, procedimientos de acceso de emergencia y mecanismos de cierre de sesión automático para controlar el acceso.	(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.
5	Controles de auditoría	software y/o mecanismos de procedimiento que registren y examinen la actividad en los sistemas de	Mantenga registros de auditoría y revíselos periódicamente para detectar y responder a los incidentes de seguridad.	(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
6	Seguridad en la transmisión de datos	Proteja la PHI transmitida a través de redes electrónicas	Cifre los datos durante la transmisión y utilice canales de comunicación seguros, como las VPN.	(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
7	Capacitación de empleados	miembros de la fuerza laboral sobre sus responsabilidades con respecto a la protección de la PHI	Llevar a cabo sesiones periódicas de capacitación y repasos sobre las políticas y procedimientos de HIPAA.	(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.
8	Respuesta a incidentes	Procedimientos para responder a brechas e incidentes de seguridad	Adopte un plan de respuesta a incidentes, pruébelo regularmente y documente e informe cada incidente según sea necesario.	§ 164.404 Notification to individuals. (a) Standard —(1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.
9	Norma Mínima Necesaria	Divulgar solo la cantidad mínima de PHI necesaria para lograr el propósito previsto	Implemente políticas y controles de acceso basados en roles para garantizar el cumplimiento de la regla mínima necesaria.	(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
10	Acuerdos de Socios Comerciales (BAAs)	Asegúrese de que los socios comerciales que manejan PHI también cumplan con la HIPAA	Ejecutar acuerdos de acuerdo con todos los socios comerciales y exigirles que implementen las salvaguardas adecuadas.	(e)(1) Standard: Disclosures to business associates. (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
11	Derechos del paciente	Informar a los pacientes sobre sus derechos a acceder, modificar y restringir la PHI	Proporcionar políticas claras a los pacientes e implementar procedimientos para facilitar el ejercicio de estos derechos.	(1) Providing the access requested. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.
12	Derechos de acceso a los datos	Derechos de los pacientes a acceder a su propia PHI	Garantizar respuestas oportunas y precisas a las solicitudes de los pacientes de sus registros de salud.	(i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.
13	Modificación de la PHI	Derechos de los pacientes a solicitar enmiendas a su PHI	Desarrollar y seguir procedimientos para evaluar y hacer enmiendas, y documentar las respuestas.	§ 164.526 Amendment of protected health information. (a) Standard: Right to amend. (1) Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.
14	Restricciones sobre el uso de PHI	Derechos de los pacientes a solicitar restricciones sobre ciertos usos y divulgaciones de su PHI	Cree y aplique políticas para administrar y cumplir con las solicitudes de restricción de pacientes.	(2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.
15	Comunicaciones confidenciales	pacientes a recibir comunicaciones a través de medios alternativos o en lugares alternativos	Habilitar mecanismos para las comunicaciones confidenciales según lo soliciten los pacientes.	(i) A covered health care provider must permit individuals to request [65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013] and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.
16	Aviso de Prácticas de Privacidad	Informar a los pacientes sobre cómo se usará y divulgará su PHI.	Crear, difundir y exhibir de manera destacada un Aviso de Prácticas de Privacidad.	§ 164.520 Notice of privacy practices for protected health information. (a) Standard: notice of privacy practices, (1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.
17	Notificación de violación de datos	Requisitos para notificar a las personas y a las autoridades sobre violaciones de PHI no asegurada	Implemente una política de notificación de infracciones que cumpla con los requisitos de HIPAA, incluidos los plazos y la documentación.	Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted. § 164.400 Applicability. The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

Tabla 12: Mapeo de resultados generados con la regulación HIPAA

	Puntos clave	Descripción	Requisitos de cumplimiento	Indicación según Ley 19.628
1	Finalidad del Tratamiento de Datos	Los datos deben ser usados exclusivamente para el propósito con el cual fueron recolectados.	Establecer y documentar claramente las finalidades para las cuales se recogen los datos y asegurar que no se utilicen para fines distintos.	Artículo 4°.- El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello...
2	Consentimiento del Titular	El tratamiento de datos personales requiere el consentimiento expreso del titular, salvo excepciones establecidas por la ley.	Obtener y registrar el consentimiento explícito de los titulares antes de procesar sus datos, a menos que una excepción legal sea aplicable.	Artículo 3°.- En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. Artículo 4°.- ...La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. Artículo 10.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice o exista consentimiento del titular
3	Derecho de Acceso	Las personas tienen derecho a solicitar información sobre los datos personales que se han recopilado sobre ellas.	Implementar procedimientos para responder a las solicitudes de acceso a datos personales de manera oportuna y precisa.	Artículo 12.- Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. Artículo 14.- Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos
4	Derecho de Rectificación	Los titulares tienen derecho a solicitar la corrección de datos incorrectos, imprecisos, desactualizados o incompletos.	Establecer mecanismos para que los titulares puedan solicitar y obtener la rectificación de sus datos personales de manera eficiente.	Artículo 6°.- Los datos personales han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. Artículo 12.- En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.
5	Derecho de Cancelación	Las personas tienen derecho a solicitar la eliminación de sus datos personales cuando ya no sean necesarios para el propósito para el cual fueron recogidos o tratados.	Implementar procesos para la pronta eliminación de datos personales cuando se haga una solicitud de cancelación válida.	Artículo 6°.- Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Artículo 12.- Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. Artículo 13.- El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.
6	Derecho de Oposición	Los titulares pueden oponerse al tratamiento de sus datos personales por motivos justificados.	Asegurar que se respeten las solicitudes de oposición debidamente fundamentadas y cesar el tratamiento de los datos en cuestión.	Artículo 12.- Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.
7	Seguridad de los Datos	Es obligatorio implementar medidas de seguridad adecuadas para proteger los datos personales contra el acceso no autorizado, pérdida o destrucción.	Desarrollar y mantener políticas de seguridad que incluyan controles técnicos y administrativos apropiados para la protección de datos personales.	Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, Nº 12, de la Constitución Política. Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.
8	Confidencialidad	Las entidades que tratan datos personales deben garantizar la confidencialidad de estos datos.	Establecer y hacer cumplir acuerdos de confidencialidad para todos los empleados y contratistas que tengan acceso a datos personales.	Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, Nº 12, de la Constitución Política. Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce. Artículo 7°.- Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo. Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.
9	Transferencia de Datos	La transferencia de datos personales a terceros solo se permite si se garantiza un nivel de protección adecuado.	Evaluar las políticas de privacidad de terceros y asegurarse de que cumplan con los estándares de protección de datos antes de transferir datos personales.	Artículo 5º.- El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes. Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de: a) La individualización del requirente; b) El motivo y el propósito del requerimiento, y c) El tipo de datos que se transmiten. La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga. El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión. No se aplicará este artículo cuando se trate de datos personales accesibles al público en general. Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.
10	Reclamos y Denuncias	Las personas tienen el derecho de presentar reclamos si consideran que sus derechos han sido infringidos.	Disponer de un canal formal para la recepción, análisis y resolución de reclamos sobre el tratamiento de datos personales.	Artículo 5º.- El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes. Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de: a) La individualización del requirente; b) El motivo y el propósito del requerimiento, y c) El tipo de datos que se transmiten. La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga. El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión. No se aplicará este artículo cuando se trate de datos personales accesibles al público en general. Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.
11	Actualización de Datos	Es responsabilidad de la entidad mantener actualizados los datos personales.	Establecer procedimientos para la verificación y actualización periódica de los datos personales recolectados.	Artículo 9°.- Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

Tabla 13: Mapeo de resultados generados con la Ley 19.628

	Puntos clave	Descripción	Requisitos de cumplimiento	Indicación según Ley 20.584
1	Consentimiento informado	Los pacientes tienen derecho a otorgar o rechazar su consentimiento luego de recibir toda la información necesaria respecto a los procedimientos médicos a los que serán sometidos.	Los profesionales de la salud deben documentar el consentimiento informado de los pacientes antes de proceder con cualquier tratamiento o procedimiento invasivo.	Artículo 14.- Toda persona tiene derecho a otorgar o denegar su voluntad para someterse a cualquier procedimiento o tratamiento vinculado a su atención de salud, con las limitaciones establecidas en el artículo 16. Este derecho debe ser ejercido en forma libre, voluntaria, expresa e informada, para lo cual será necesario que el profesional tratante entregue información adecuada, suficiente y comprensible, según lo establecido en el artículo 10.
2	Confidencialidad de la Información	La información del paciente debe ser tratada de manera confidencial, solo compartida con el personal médico directamente involucrado en el tratamiento del paciente.	Las instituciones de salud deben implementar políticas asegurando que la información de los pacientes se maneje de manera confidencial y limitada a el personal autorizado.	Artículo 10 .- Los prestadores deberán adoptar las medidas necesarias para asegurar la adecuada confidencialidad durante la entrega de esta información, así como la existencia de lugares apropiados para ello.
3	Acceso a la ficha clínica	Los pacientes tienen derecho a acceder a su propia ficha clínica, la cual contiene todos los registros sobre su diagnóstico, tratamiento y datos personales.	Las instituciones de salud deben proporcionar acceso fácil y oportuno a los pacientes a sus fichas clínicas, cumpliendo con los procedimientos establecidos para tal efecto.	Artículo 13 .- Título II Las personas individualizadas en las letras a) y b) precedentes podrán requerir, de conformidad con la ley N° 19.628, la entrega gratuita y sin dilaciones indebidas de una copia íntegra de la información contenida en la ficha clínica, en un formato estructurado, de uso común y lectura legible, que sea susceptible de ser portado a otro sistema de ficha clínica o transmitirlos a otro prestador que se indique en la solicitud, según lo dispuesto en la resolución que apruebe la norma técnica dictada para tales efectos por el Ministerio de Salud.
4	Rectificación de la información	Los pacientes tienen derecho a solicitar la corrección de cualquier dato incorrecto en sus fichas clínicas.	Las instituciones de salud deben establecer procedimientos para que los pacientes pueden solicitar correcciones y asegurarse de que estos cambios sean realizados de manera adecuada.	
5	Retención de la ficha clínica	La ficha clínica debe ser conservada por un mínimo de 15 años desde la fecha del último registro.	Las instituciones de salud deben asegurarse de mantener las fichas clínicas en condiciones adecuadas y seguras por el plazo establecido.	Artículo 13.- Los prestadores deberán conservar la ficha clínica por un período de al menos quince años. Asimismo, serán responsables del cumplimiento de lo dispuesto en la ley N° 19.628, sobre protección de la vida privada, de adoptar las medidas que permitan su interoperabilidad con otros prestadores de salud, y del acceso oportuno a la información contenida en la ficha que sea necesaria para garantizar la continuidad del cuidado del paciente, cuando ésta sea requerida por un profesional de la salud que participe directamente en la atención del titular de los datos contenidos en ella. Un reglamento expedido a través del Ministerio de Salud establecerá la forma y las condiciones bajo las cuales los prestadores almacenarán las fichas, así como las normas necesarias para su administración, adecuada protección, eliminación e interoperabilidad.
6	Salvaguarda de la Información	Las instituciones de salud deben tomar medidas apropiadas para proteger la información de salud contra el acceso no autorizado, la pérdida o la alteración.	Implementación de tecnologías de la información y políticas de seguridad que garanticen la protección de los datos.	Artículo 3.- Será responsabilidad de los prestadores institucionales e individuales de salud que otorguen acciones de salud digital, utilizar medios técnicos que cumplan los estándares de seguridad que establezca el Ministerio de Salud en todas las etapas del tratamiento de datos, siendo responsables de todo daño que ocasionare el incumplimiento a dicho deber.

Tabla 14: Mapeo de resultados generados con la Ley 20.584

REFERENCIAS BIBLIOGRÁFICAS

[Agencia Española de Protección de Datos, 2022] Agencia Española de Protección de Datos (2022). Personal data breaches: Development and pre-production environments.

[Al Faresi *et al.*, 2010] Al Faresi, A., Wijesekera, D., y Moidu, K. (2010). A comprehensive privacy-aware authorization framework founded on hipaa privacy rules. En *Proceedings of the 1st ACM International Health Informatics Symposium*, pp. 637–646.

[ASQ, 2022] ASQ (2022). PDCA Cycle - What is the Plan-Do-Check-Act Cycle? | ASQ.

[Carrión, Inmaculada *et al.*, 2011] Carrión, Inmaculada, Alemán, José Luis Fernández, y Toval, Ambrosio (2011). Assessing the hipaa standard in practice: Phr privacy policies. En *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2380–2383. IEEE.

[Cheng, Vivying SY y Hung, Patrick CK, 2005] Cheng, Vivying SY y Hung, Patrick CK (2005). Towards an integrated privacy framework for hipaa-compliant web services. En *Seventh IEEE International Conference on E-Commerce Technology (CEC'05)*, pp. 480–483. IEEE.

[Compliancy Group, 2022a] Compliancy Group (2022a). Accellion Settles Healthcare Data Breach Suit for $8.1 Mil.

[Compliancy Group, 2022b] Compliancy Group (2022b). Data Breach Lawsuit Filed After Theft of Nearly 320k Records.

[Damani, 2004] Damani, N. (2004). Gestión de riesgos. Londres-Reino Unido. Editorial Theific.

[Dirección de Investigación Gobierno de México, 2017] Dirección de Investigación Gobierno de México (2017). Comité de Ética para la atención médica. Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán.

[Freire Silva, 2022] Freire Silva, J. E. (2022). Metodología para mitigar vulnerabilidades de almacenamiento mediante inteligencia de fuentes abiertas (osint) en la eeasa. Master's thesis, Pontificia Universidad Católica del Ecuador.

[GDPR, 2016a] GDPR (2016a). Protección de datos - unión europea. `https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es`.

[GDPR, 2016b] GDPR (2016b). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), art. 13.

[Ghazinour, Kambiz *et al.*, 2009] Ghazinour, Kambiz, Majedi, Maryam, y Barker, Ken (2009). A model for privacy policy visualization. En *2009 33rd Annual IEEE International Computer Software and Applications Conference*, volumen 2, pp. 335–340. IEEE.

[González, 2024] González, S. M. (2024). Gestión de identidad y acceso (iam) en la nube: Mecanismos y desafíos. Universitat Politècnica de València.

[HIPAA Journal, 2022] HIPAA Journal (2022). What is the purpose of HIPAA? Update 2022.

[Jain, Shrey *et al.*, 2023] Jain, Shrey, Hitzig, Zoë, y Mishkin, Pamela (2023). Contextual confidence and generative AI.

[Jie SHI *et al.*, 2023] Jie SHI, ShuFang Cui, Fei Chen, y ChengTao Wang (2023). Sensitive data discovery technology based on artificial intelligence. EAI.

[Leyva, 2017] Leyva, M. R. P. (2017). Implementación de una solución de seguridad perimetral administrada utilizando un firewall fortigate 1500d para la protección de la red lan de la universidad nacional de trujillo. UNIVERSIDAD POLITÉCNICA DE SINALOA PROGRAMA ACADÉMICO DE INGENIERÍA EN INFORMÁTICA.

[Martelo, R. J., 2018] Martelo, R. J., Tovar, L. C., . M. (2018). Modelo básico de seguridad lógica. caso de estudio: El laboratorio de redes de la universidad de cartagena en colombia. Centro de Información Tecnológica.

[MINISTERIO DE SALUD, SUBSECRETARÍA DE SALUD PÚBLICA, 2023] MINISTERIO DE SALUD, SUBSECRETARÍA DE SALUD PÚBLICA (2023). LEY 20584 SOBRE LOS DERECHOS Y DEBERES QUE TIENEN LAS PERSONAS EN RELACIÓN CON ACCIONES VINCULADAS A SU ATENCIÓN EN SALUD. `https://www.bcn.cl/leychile/navegar?idNorma=1039348`.

[MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, 2018] MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA (2018). Ley 21096 consagra el derecho a protecciÓn de los datos personales. `https://bcn.cl/2c9xg`. Online; visitado 2 Octubre 2022.

[MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, 2020] MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA (2020). LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. `https://www.bcn.cl/leychile/navegar?idNorma=141599`. Online; visitado 2 Octubre 2022.

[Office of the United Nations High Commissioner for Human Rights, 2022] Office of the United Nations High Commissioner for Human Rights (2022). Principios que sustentan la privacidad y la protección de datos personales. `https://www.ohchr.org/es/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data#:~:text=Analizaremos%20en%20particular%20los%20siguientes,y%20protecci%C3%B3n%20de%20datos%20personales`.

[OpenAI *et al.*, 2023] OpenAI, Achiam, J., Adler, S., Agarwal, S., Ahmad, L., Akkaya, I., Aleman, F. L., Almeida, D., Altenschmidt, J., Altman, S., Anadkat, S., Avila, R., Babuschkin, I., Balaji, S., Balcom, V., Baltescu, P., Bao, H., Bavarian, M., Belgum, J., Bello, I., Berdine, J., Bernadett-Shapiro, G., Berner, C., Bogdonoff, L., Boiko, O., Boyd, M., Brakman, A.-L., Brockman, G., Brooks, T., Brundage, M., Button, K., Cai, T., Campbell, R., Cann, A., Carey, B., Carlson, C., Carmichael, R., Chan, B., Chang, C., Chantzis, F., Chen, D., Chen, S., Chen, R., Chen, J., Chen, M., Chess, B., Cho, C., Chu, C., Chung, H. W., Cummings, D., Currier, J., Dai, Y., Decareaux, C., Degry, T., Deutsch, N., Deville, D., Dhar, A., Dohan, D., Dowling, S., Dunning, S., Ecoffet, A., Eleti, A., Eloundou, T., Farhi, D., Fedus, L., Felix, N., Fishman, S. P., Forte, J., Fulford, I., Gao, L., Georges, E., Gibson, C., Goel, V., Gogineni, T., Goh, G., Gontijo-Lopes, R., Gordon, J., Grafstein, M., Gray, S., Greene, R., Gross, J., Gu, S. S., Guo, Y., Hallacy, C., Han, J., Harris, J., He, Y., Heaton, M., Heidecke, J., Hesse, C., Hickey, A., Hickey, W., Hoeschele, P., Houghton, B., Hsu, K., Hu, S., Hu, X., Huizinga, J., Jain, S., Jain, S., Jang, J., Jiang, A., Jiang, R., Jin, H., Jin, D., Jomoto, S., Jonn, B., Jun, H., Kaftan, T., Kaiser, □ Kamali, A., Kanitscheider, I., Keskar, N. S., Khan, T., Kilpatrick, L., Kim, J. W., Kim, C., Kim, Y., Kirchner, J. H., Kiros, J., Knight, M., Kokotajlo, D., Kondraciuk, □ Kondrich, A., Konstantinidis, A., Kosic, K., Krueger, G., Kuo, V., Lampe, M., Lan, I., Lee, T., Leike, J., Leung, J., Levy, D., Li, C. M., Lim, R., Lin, M., Lin, S., Litwin, M., Lopez, T., Lowe, R., Lue, P., Makanju, A., Malfacini, K., Manning, S., Markov, T., Markovski, Y., Martin, B., Mayer, K., Mayne, A., McGrew, B., McKinney, S. M., McLeavey, C., McMillan, P., McNeil, J., Medina, D., Mehta, A., Menick, J., Metz, L., Mishchenko, A., Mishkin, P., Monaco, V., Morikawa, E., Mossing, D., Mu, T., Murati, M., Murk, O., Mély, D., Nair, A., Nakano, R., Nayak, R., Neelakantan, A., Ngo, R., Noh, H., Ouyang, L., O'Keefe, C., Pachocki, J., Paino, A., Palermo, J., Pantuliano, A., Parascandolo, G., Parish, J., Parparita, E., Passos, A., Pavlov, M., Peng, A., Perelman, A., Peres, F. d. A. B., Petrov, M., Pinto, H. P. d. O., Michael, Pokorny, Pokrass, M., Pong, V. H., Powell, T., Power, A., Power, B., Proehl, E., Puri, R., Radford, A., Rae, J., Ramesh, A., Raymond, C., Real, F., Rimbach, K., Ross, C., Rotsted, B., Roussez, H., Ryder, N., Saltarelli, M., Sanders, T., Santurkar, S., Sastry, G., Schmidt, H., Schnurr, D., Schulman, J., Selsam, D., Sheppard, K., Sherbakov, T., Shieh, J., Shoker, S., Shyam, P., Sidor, S., Sigler, E., Simens, M., Sitkin, J., Slama, K., Sohl, I., Sokolowsky, B., Song, Y., Staudacher, N., Such, F. P., Summers, N., Sutskever, I., Tang, J., Tezak, N., Thompson, M. B., Tillet, P., Tootoonchian, A., Tseng, E., Tuggle, P., Turley, N., Tworek, J., Uribe, J. F. C., Vallone, A., Vijayvergiya, A., Voss, C., Wainwright, C., Wang, J. J., Wang, A., Wang, B., Ward, J., Wei, J., Weinmann, C., Welihinda, A., Welinder, P., Weng, J., Weng, L., Wiethoff, M., Willner, D., Winter, C., Wolrich, S., Wong, H., Workman, L., Wu, S., Wu, J., Wu, M., Xiao, K., Xu, T., Yoo, S., Yu, K., Yuan, Q., Zaremba, W., Zellers, R., Zhang, C., Zhang, M., Zhao, S., Zheng, T., Zhuang, J., Zhuk, W., y Zoph, B. (2023). Gpt-4 technical report.

[Pablo Recalde, 2023] Pablo Recalde, S. (2023). Gestión de riesgos de datos sensibles de la dirección general de aviación civil lineados al cumplimiento de la ley orgánica de protección de datos personales. Quito, Ecuador: Universidad Tecnológica Israel.

[Ramiro, 2021] Ramiro, A. M. (2021). Nuevas tecnologías y retos para la protección de datos personales en europa: el rastreo de contactos durante la pandemia por covid-19. *Confluências| Revista Interdisciplinar de Sociologia e Direito*, 23(2):99–17.

[Riega Riega, 2015] Riega Riega, L. E. A. (2015). Implementación de protección perimetral contra amenazas de malware desconocidas que o están basadas en firmas en essalud a nivel nacional. Universidad Señor de Sipán.

[Rouhiainen, 2022] Rouhiainen, L. (2022). Inteligencia artificial. Madrid: Alienta Editorial.

[Salas, 2017] Salas, J. R. (2017). Encriptado de datos para proteger información de las empresas. UNIVERSIDAD POLITÉCNICA DE SINALOA PROGRAMA ACADÉMICO DE INGENIERÍA EN INFORMÁTICA.

[Scope, 2021] Scope, Rasin, H. L. W. (2021). The sixth international conference on cyber-technologies and cyber-systems - cyber 2021. pp. 51–57.

[Seh, Adil Hussain *et al.*, 2020] Seh, Adil Hussain, Zarour, Mohammad, Alenezi, Mamdouh, Sarkar, Amal Krishna, Agrawal, Alka, Kumar, Rajeev, y Ahmad Khan, Raees (2020). Healthcare data breaches: insights and implications. En *Healthcare*, volumen 8, p. 133. Multidisciplinary Digital Publishing Institute.

[TechJury, 2022] TechJury (2022). 25+ Alarming Healthcare Data Breaches Statistics for 2022.

[Uivaru, 2018] Uivaru, L. C. (2018). *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud. La protección de datos de carácter sensible*. J. M. Bosch.

[U.S. Department of Health Human Services, 1998] U.S. Department of Health Human Services (1998). Health information security. `https://www.hhs.gov/hipaa/for-professionals/security/index.html`.

[U.S. Department of Health Human Services, 1999a] U.S. Department of Health Human Services (1999a). Breachnotification rule. `https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html`.

[U.S. Department of Health Human Services, 1999b] U.S. Department of Health Human Services (1999b). Health information privacy. `https://www.hhs.gov/hipaa/for-professionals/privacy/index.html`.