Propuesta de implementación de seguridad y protección de datos de pacientes en la telemonitorización de la marcha mediante IoT

David Alexander López Díaz

Universidad Antonio Nariño

Facultad de Ingeniería Mecánica, Electrónica y Biomédica

Bogotá, Colombia

2021

Propuesta de implementación de seguridad y protección de datos de pacientes en la telemonitorización de la marcha mediante IoT

David Alexander López Díaz

Proyecto de grado presentado como requisito parcial para optar al título de:

Ingeniero Biomédico

Director (a):

Ph.D Andres Felipe Ruiz Olaya

Línea de Investigación:

Ingeniería de rehabilitación y telemedicina

Grupo de Investigación:

Bioingeniería

Universidad Antonio Nariño

Facultad de Ingeniería Mecánica, Electrónica y Biomédica

Bogotá, Colombia

2021

A mis padres

Que con apoyo incondicional, amor y confianza me formaron como un gran ser humano y me dieron la oportunidad de lograr una meta más de muchas que tengo en mente.

Agradecimientos

En primer lugar, agradezco a Dios por darme vida y salud, a mis padres Rodrigo López y Carmen Diaz por creer en mi visión y alentarme siempre en los momentos más difíciles que se me presentaron en mi formación como profesional. Estar lejos de mi familia y despegarme de ellos de la noche a la mañana fue un reto muy grande para mí. Me fui con la bendición de Dios y con la mentalidad de que iba a crecer como persona y que iba a hacer sentir orgullosa a mi familia. Y aquí estoy escribiendo los agradecimientos y con una sonrisa que no cabe en mi rostro.

También agradezco a cada uno de mis docentes que hicieron parte de este proceso de formación donde cada uno aportó un granito de arena tanto en mi vida profesional como en mi vida personal. Al ingeniero Andrés Ruiz, por creer en mi visión apoyándome y guiándome en cada una de las letras plasmadas en esta tesis.

A toda mi familia que siempre estuvo ahí, mis abuelos, mi compañera sentimental, mis hermanos, mis tíos y mis primos les doy infinitas gracias.

Resumen

El internet de las cosas (IoT), es una tecnología emergente en donde convergen la capacidad de medición de sensores y la internet existente, con potencial aplicación en el área de la salud y especialmente en la telemonitorización. La telemonitorización es una de las modalidades de la telemedicina, que requiere el registro, almacenamiento y transmisión de información del paciente y de parámetros biomédicos relacionados al servicio de salud. Según la resolución 2654 de 2019, esta modalidad debe asegurar la calidad de los datos a través de plataformas tecnológicas o dispositivos electrónicos, que incluye fortalecer la seguridad y protección de datos del paciente, y garantizar cuatro objetivos: autenticidad, integridad, disponibilidad y fiabilidad, de tal manera que se garantice la integridad de las personas. En este trabajo se presenta el diseño e implementación de un prototipo de sistema IoT que garantice la seguridad de datos con aplicación en la telemonitorización de variables de la marcha. Este sistema consta de una aplicación desarrollada en Matlab e instalada en un dispositivo móvil con Android, el cual es utilizado para la adquisición de la información cinemática mediante el acelerómetro del celular, su procesamiento y el envío de manera segura a la nube en la plataforma ThingSpeak, para poder ser visualizada y analizada de manera remota. La verificación de las mediciones obtenidas fue realizada mediante el software Kinovea obteniendo un error del 5% y se implementó el sistema para garantizar la seguridad para sistemas IoT. Finalmente, se realizó una validación del sistema para monitorizar la variable cadencia de la marcha en un protocolo efectuado durante una semana, verificando que la información pueda ser visualizada y procesada de manera remota en el servidor ThingSpeak.

Palabras clave: Seguridad y protección de datos, IoT, telemonitorización, telemedicina, resolución 2654 de 2019, ThingSpeak.

Abstract

The internet of things (IoT) is an emerging technology where sensor measurement capacity and the existing internet converge, with potential application in the health area and especially in telemonitoring. Telemonitoring is one of the modalities of telemedicine, which requires the registration, storage and transmission of patient information and biomedical parameters related to the health service. According to resolution 2654 of 2019, this modality must ensure the quality of the data through technological platforms or electronic devices, which includes strengthening the security and protection of patient data, and guaranteeing four objectives: authenticity, integrity, availability and reliability, in such a way that the integrity of the people is guaranteed. This work presents the design and implementation of a prototype of an IoT system that guarantees data security with application in the telemonitoring of gait variables. This system consists of an application developed in Matlab and installed on an Android mobile device, which is used for the acquisition of kinematic information through the cell phone's accelerometer, its processing and its safe delivery to the cloud on the ThingSpeak platform, to be able to be viewed and analyzed remotely. The verification of the measurements obtained was carried out using the Kinovea software, obtaining an error of 5% and the system was implemented to guarantee security for IoT systems. Finally, a system validation was carried out to monitor the gait cadence variable in a protocol carried out for a week, verifying that the information can be viewed and processed remotely on the ThingSpeak server.

Keywords: Security and data protection, IoT, telemonitoring, telemedicine, resolution 2654 of 2019, ThingSpeak.

Tabla de contenido

Lista de figuras

Lista de tablas

Pág.

1. Introducción

La telemedicina es un servicio médico, que consiste en la combinación de tecnología informática, tecnología de comunicación y tecnología médica que tiene como objetivo mejorar el diagnóstico, el nivel médico y satisfacer los requisitos de salud de la persona [1].

En Colombia, con la resolución 2654 de 2019, se fijan los parámetros y lineamientos aplicables a la telemedicina. Además, se establecen disposiciones de la telesalud, y entre los requerimientos necesarios en la prestación de servicios de salud en esta modalidad se encuentra garantizar la seguridad e integridad de la información y datos del paciente.

En este contexto, la seguridad se enfoca en garantizar tres objetivos: autenticación, integridad y confidencialidad. La autenticación garantiza que el usuario es quien dice ser. La integridad garantiza que, durante el intercambio de información, ésta no ha sido modificada o eliminada por parte de usuarios malintencionados. Finalmente, la confidencialidad se garantiza cuando sólo los participantes autorizados del sistema pueden acceder a la información protegida, es decir cuando sólo el transmisor y receptor pueden conocer la información médica [2].

La telemonitorización, de acuerdo al artículo 18 de la resolución 2654 de 2019, es la relación entre el personal de la salud y un usuario donde se recopila y se transmite información clínica mediante una infraestructura tecnológica, para que el personal de la salud realice su respectivo análisis clínico y dé información al paciente [3].

La protección y seguridad de datos en el campo de la salud, y específicamente en la telemonitorización, es un factor fundamental para habilitar este tipo de servicios de salud, según la normatividad vigente. Uno de los principales problemas a los que se enfrentan los pacientes es a los ciberdelincuentes o personas que puedan acceder a información sensible del paciente, pues les toman sus datos y los difunden a terceras personas mediante medios de comunicación como teléfonos o correos electrónicos [4]. De ahí la gran necesidad de establecer normas que permitan la máxima protección y garantía de dichos datos para los pacientes en el campo de la telemedicina.

Por otro lado, el Internet de las Cosas (IoT), es una nueva tecnología en donde convergen la capacidad de medición de sensores y la internet existente, con potencial aplicación en el área de la salud [1]. Se conectan todos los elementos a internet mediante la identificación de una radiofrecuencia y la detección de equipos para lograr una identificación existente; es compatible con varios dispositivos de entrada-salida como cámaras, micrófonos, teclados, bluetooth, entre otros [1].

El Internet de las Cosas Médicas (IoMT), es un tipo de tecnología que incorpora sensores inalámbricos en equipos médicos combinados con internet e integrados en hospitales. La ventaja que se puede evidenciar mediante IoMT, es que se presenta una posibilidad de llevar a cabo tareas cotidianas mientras que el paciente está bajo un monitoreo continuo de salud. Además de esto, mediante IoMT, se resuelven algunos problemas en la portabilidad de dispositivos médicos usuales de monitoreo, puesto que se presentan dispositivos de sensores de potencia ultra baja y de rápida comunicación [1], [5].

Actualmente se vislumbran múltiples aplicaciones de la tecnología IoT en el contexto de la telemonitorización. Uno de los campos de salud potencialmente de interés, es el de la rehabilitación física, en la cual puede ser requerido el intercambio de manera remota entre variables físicas del paciente y el personal de la salud, para registro y seguimiento de valoración y evolución de terapias físicas llevadas a cabo desde el hogar del paciente. En

este contexto, se requiere garantizar la seguridad y la protección de datos enviados desde el sistema de registro con el paciente y el lugar de almacenamiento remoto.

De acuerdo a lo anteriormente mencionado, se identificaron las especificaciones técnicas, requerimientos y parámetros establecidos en la resolución 2654 de 2019 para poder ser implementados en un sistema IoT enfocado a la telemonitorización de la marcha incorporando de manera satisfactoria un algoritmo basado en IoT en el método de seguridad y protección de datos contando con el protocolo HTTPS para subir la información a la nube y el cifrado end-to-end para el envío de la información para poder visualizarla de manera segura y síncrona. Además de esto, se hizo un análisis comparativo entre la magnitud real de la cadencia (obtenida mediante análisis del video Kinovea) y la magnitud calculada por el sistema desarrollado obteniendo un error aproximadamente del 5%.

1.1 Planteamiento del problema

La telemedicina tiene potencial aplicación para proporcionar servicios de rehabilitación física remota, en donde es de interés el monitorizar parámetros cinemáticos relacionados con las actividades físicas del paciente. Particularmente, en rehabilitación de la marcha, los parámetros espacio-temporales proveen información que permiten realizar un diagnóstico y evaluar la evolución de una terapia en un proceso terapéutico.

La telemonitorización es una de las modalidades de la telemedicina, que requiere el registro, almacenamiento y transmisión de información del paciente y de parámetros biomédicos relacionados al servicio de salud. En la resolución 2654 de 2019, la cual rige la normatividad para aplicación de la telemedicina en Colombia, se definen las características que deben tener los servicios de telesalud, y se hace especial énfasis en la seguridad y protección de los datos del paciente, puesto que en la actualidad múltiples entidades que han habilitado prestar el servicio de telemedicina, de acuerdo a la resolución 2654 de 2019, no cumplen con los requerimientos establecidos en el artículo 12 de la presente resolución afectando en sí, la integridad y seguridad de datos del paciente.

A partir de una revisión del estado del arte realizada, se han identificado una variedad de plataformas reportadas, las cuales han sido desarrolladas para transmitir los datos adquiridos en la telemonitorización sin tener en cuenta la seguridad e integridad de datos del paciente, haciéndolo mediante el uso de correos electrónicos o aplicaciones móviles sin la debida protección. Teniendo en cuenta la naturaleza sensible de la información del paciente, se requiere seguir los lineamientos de la normatividad y garantizar la autenticación del usuario y proteger los datos registrados de éste.

1.2 Justificación

La seguridad e integridad de los datos es requerida según la normatividad vigente, particularmente la resolución 2654 de 2019. En la actualidad, mediante varios medios, los ciberdelincuentes realizan acciones indebidas tomando fácilmente los datos personales de pacientes y afectan la integridad de estos.

En el marco al desarrollo de este proyecto, se ha desarrollado e implementado una plataforma tecnológica basada en IoT, y se ha propuesto y evaluado un método para la protección de los datos registrados, transmitidos y almacenados, en una aplicación para la monitorización de variables físicas de manera remota con énfasis en rehabilitación física.

Por lo tanto, se ha realizado un sistema de telemonitoreo donde se registra la cadencia y el nivel de la actividad física en el proceso de la marcha utilizando el sensor acelerómetro de un dispositivo móvil. Esta herramienta tiene el potencial de integrarse en procesos de rehabilitación física.

Finalmente, la presente propuesta de trabajo de grado está alineada con el desarrollo del proyecto de investigación “Apoyo a la Valoración y Telerrehabilitación de Personas con Diversidad Funcional Motora Mediante Plataforma de E- Salud”, el cual está siendo actualmente ejecutado por el Grupo Bioingeniería de la Universidad Antonio Nariño.

1.3 Objetivos

1.3.1 Objetivo General

Proponer e implementar un método para la seguridad y protección de datos acorde a la resolución 2654 de 2019, en una aplicación basada en IoT para la telemonitorización de la cadencia de la marcha en sujetos sanos.

1.3.2 Objetivos Específicos

- Identificar las especificaciones técnicas, requerimientos, y los parámetros requeridos para implementar la protección de datos de un sistema basado en IoT, según la resolución 2654 de 2019.
- Implementar el sistema basado en IoT, incorporando el método de seguridad y protección de datos.
- Evaluar el funcionamiento del sistema bajo condiciones controladas para caracterizar su desempeño técnico.
- Implementar un protocolo de medidas con sujetos sanos para verificar la información de telemonitoreo.

1.4 Estado del arte

En la literatura científica, se encuentran varios trabajos relacionados con algoritmos y métodos para la seguridad de los datos de los pacientes, donde se encontraron los siguientes artículos.

Los factores más importantes para la seguridad de los datos en la internet son la integridad, privacidad, autenticidad y disponibilidad. Es por esto, que en el artículo apoyado por la Universidad Tecnológica K.N. Toosi ubicada en Irán y realizado por H Hamidi presenta en [6] una herramienta para la seguridad de las cosas médicas basada en la tecnología biométrica. La tecnología biométrica tiene varias características que se utilizan como identificadores, puesto que no pueden ser prestados, comprados, olvidados y son muy difícil de falsificar o copiar garantizando la seguridad del paciente. De acuerdo a esto se alcanza una forma más segura de acceder a IoT basada en la biometría y el estándar de identidad rápido para ser utilizada en avances significativos para los sistemas de salud inteligentes basados en la IoT.

En el artículo publicado en IEEE y expuesto en Rio de Janerio , los autorem Kapusta, Memmi y Noura establecen en [7] un método para la protección de datos de manera segura dentro de UWSN (Redes de sensores inalámbricos desatendidas). Esto se basa en un esquema de fragmentación que transforma los datos recopilados por un sensor en varios fragmentos seguros de los cuales se puede obtener la recuperación de datos y para la seguridad de los mismos se establece una dinámica que se actualiza cada vez que se ingresa al sistema. Esto permite equilibrar el rendimiento, la protección de datos y la ocupación de memoria.

En el artículo apoyado por el Plan Nacional de Investigación y Desarrollo de China y con afiliación del tercer instituto de investigación de seguridad pública del ministerio de china, los autores Liu, Zhang, Zhou, y Tang proponen en [8] un sistema de cifrado y seguridad para sistemas de recursos informáticos y de almacenamiento limitados mediante una base

de datos cuyo propósito es evitar la fuga de datos confidenciales que no son de confianza y ataques malintencionados. Este esquema se evalúa en un dispositivo de sistema operativo Android con un procesador Qualcomm Snapdragon 625 de 8 núcleos 2,0 GHz, 4 GB de RAM y 64GB de ROM presentando una gran viabilidad y eficacia para ser implementado en trabajos futuros, por las capacidades y características del hardware.

En el artículo publicado en IEEE en una conferencia dictada en Kanpur India a cargo de Sawardekar y Pawar analizan en [9] un servicio de API abierta en la plataforma IoT de Thingspeak. Esta plataforma conlleva a que estos sensores pueden detectar y monitorear la frecuencia cardíaca y los datos de temperatura de los pacientes en la nueve además de transferir los datos a Matlab con la ayuda del ID del canal de ThingSpeak. Para este trabajo, se utiliza los siguientes componentes: la placa de Arduino UNO, el módulo Wifi ESP8266, sensor de pulso y sensor de temperatura. Estos componentes son útiles para procesar y transferir la información que está en la nube ThingSpeak. En Matlab, la seguridad de los datos de los pacientes se realiza mediante un inicio de sesión de GUIDE. Donde el profesional de la salud tiene un ID para poder ver los datos de los usuarios; incluso los mismos pacientes tienen un ID para poder observar sus datos.

De igual manera, se encuentra un artículo publicado en IEEE siendo éste una conferencia dictada en Ghaziabad, India a cargo de Garg y Dave ponen en [10] la disposición de los detalles sobre cómo la API de Representational State Transfer (REST) concede de forma segura en el envío de datos de dispositivos conectados a aplicaciones en la nube y usuarios. La API REST se utiliza para la comunicación y el intercambio de datos. Middleware además de apoyar al desarrollo de IoT y exponer los datos del dispositivo a través de REST, proporciona una interfaz para que el usuario registre sus dispositivos de IoT y pueda acceder de forma segura a los datos tomados por el dispositivo.

En una conferencia realizada en Timisoara, Romania, los autores Aciobanitei, Buhus, y Pura realizan en [11] un algoritmo basado en el código QR, debido a que las contraseñas necesitan dispositivos adicionales que el usuario utiliza y administra. Hoy en día la mayoría de las personas tienen acceso a un teléfono inteligente y uno de sus usos es como

dispositivo de seguridad de acuerdo a su grado de seguridad y facilidad. Además de esto, tiene la ventaja de que el código QR funciona con conexión o sin conexión a Internet. El algoritmo usado para la implementación del sistema se presenta en la figura 1.

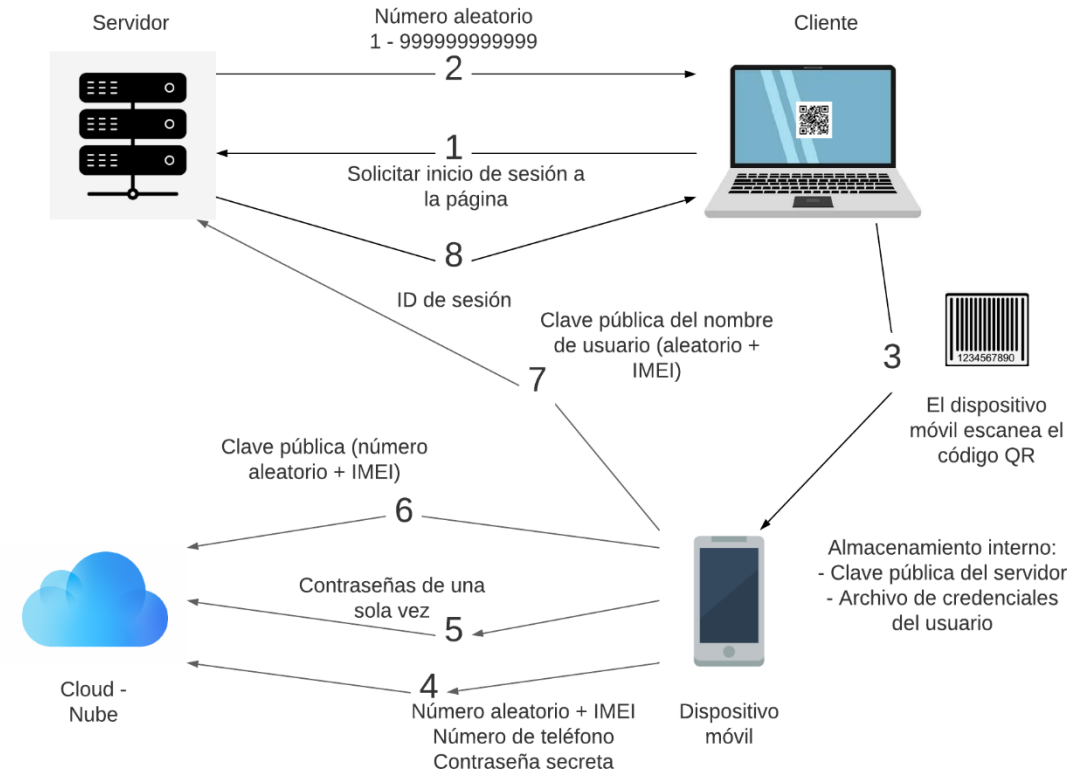


Figura 1: Algoritmo presentado para el diseño del sistema. Adaptado de: [11].

En la figura 1, se puede observar el algoritmo y los pasos que se tuvieron en cuenta para la implementación del sistema. Este algoritmo fue implementado de acuerdo al protocolo de autenticación QPR.

- Paso 1: Mediante el navegador web, el usuario solicita acceso para iniciar sesión en el sistema.

- Paso 2: La respuesta del navegador será un número aleatorio que oscila entre 1 y 999999999. El sistema escoge un número al azar y de acuerdo a esto genera un código QR.
- Paso 3: El usuario inserta el código PIN en el celular para poder acceder a su archivo de credenciales. Posteriormente a esto, se escanea el código QR. Una vez se realice lo anterior, los datos de autenticación se forman de acuerdo al número mostrado en el paso 2 y el IMEI del dispositivo.
- Paso 4: Para una mayor seguridad, la aplicación móvil envía al proveedor de servicios de confianza (TSP) junto con el número de teléfono y una contraseña. Esto sirve para la autenticación del usuario en el TSP.
- Paso 5: En la aplicación del dispositivo móvil, el usuario deberá insertar la Contraseñas de solo una vez (OTP), recibido a través de SMS en el número de teléfono móvil.
- Paso 6: El TSP comprueba la autenticidad del usuario para poder acceder a sus datos.
- Paso 7: El dispositivo móvil envía al servidor el nombre de usuario, datos de autenticación y clave pública, para comprobar su identidad.
- Paso 8: El servidor utiliza la clave del cliente para verificar si hay alguna entrada en la base de datos que contiene los números aleatorios. El servidor lo reemplaza por el IMEI del usuario y posteriormente a esto se le asigna un usuario y envía al explorador del cliente que se ha iniciado un proceso de autenticación.

Además de los anteriores artículos, también se tuvieron en cuenta otros trabajos relacionados con el envío de la información de variables biomecánicas, donde se encontraron los siguientes artículos:

En el artículo publicado en IEEE y expuesto en Atlanta, Estados Unidos, los autores Majumder, Saxena y Ahamed desarrollaron en [12] un modelo biomecánico para mejorar la predicción específica de las caídas en el ciclo de marcha. Por lo tanto, se diseñó y se implementó un zapato inteligente con un módulo de comunicación Wi-Fi para recopilar la información de presión de la plantilla. Finalmente, el sistema propuesto denominado Your

Walk is My Command puede percatar al usuario si la marcha no es la adecuada y así poder advertirle de lesiones futuras.

Finalmente, en el artículo publicado en IEEE y expuesto el Estambul, Turquía, los autores Ghazal, Alhalabi, Fraiwan, Yaghi y Alkhatib propusieron en [13] un sistema móvil para detectar y clasificar el movimiento de las extremidades y la flexión de las articulaciones. Este sistema incluye sensores que se pueden ubicar en las articulaciones de interés y así poder capturar y registrar los ángulos de las articulaciones durante una sesión de captura. Cuando finaliza esa sesión, los datos se cargan en un servidor para su respectivo análisis. Además de esto, se tiene una aplicación móvil para descargar y utilizar la información para así poder visualizar la calidad del movimiento frente a un patrón estándar. La visualización permite alinear desviaciones encontradas y así poder realizar una corrección para mejorar los movimientos. En conclusión, este sistema ayuda en la evaluación de la calidad del movimiento y así en la fisioterapia se puede comparar las señales capturadas a lo largo de un plan de tratamiento.

2. Marco Teórico

2.1 Telemonitorización y seguridad de la información.

- **Telemonitoreo**

El telemonitoreo es uno de los tipos de telemedicina que consiste en el uso de las tecnologías de información y telecomunicación para evaluar la condición del paciente. Este tipo de telemedicina permite a los profesionales en salud monitorear las variables fisiológicas, resultados de exámenes, imágenes y sonidos provenientes del paciente como la respiración, la presión arterial, la glucosa, oxigeno, pulso, entre otros. Con el fin de decidir qué día y cómo se debe realizar el tratamiento del paciente que por lo general es en los hogares de cada paciente [14].

- **Seguridad de la información**

La seguridad de la información se define como un conjunto de medidas técnicas y legales permitiendo a las organizaciones o personas preservar la confidencialidad, integridad, disponibilidad y autenticidad de la información [2], [15]. Por lo tanto, se puede decir que un sistema es confiable o seguro si garantiza los aspectos observados en la figura 2.

Figura 2: Aspectos importantes en la seguridad de la información los cuales son: Confidencialidad, Integridad, Disponibilidad y Autenticidad. Fuente: Propia.

Los aspectos que se visualizan en la figura 2, se definen a continuación.

- Confidencialidad: La información sólo puede ser utilizada por la persona que tiene autoridad para hacerlo con el objetivo de prevenir la divulgación no autenticada de la información.
- Integridad: Se refiere a la fidelidad de la información, la cual no ha sido borrada, copiada o editada con el objetivo de prevenir modificaciones no autorizadas de la información.
- Disponibilidad: Se refiere a que la información debe estar disponible para su procesamiento o para elementos que tengan acceso con el objetivo de prevenir interrupciones no autorizadas de los medios informáticos.
- Autenticidad: Se refiere a la información legítima, donde se debe verificar la identidad del usuario con el objetivo de que no sea copiada o divulgada.

2.2 Parámetros cinemáticos para seguimiento remoto en rehabilitación física.

2.2.1 Rehabilitación física

La rehabilitación física se enfoca en restaurar las capacidades motrices de una persona que ha padecido una lesión o enfermedad, con la finalidad que de ésta pueda seguir con las actividades de la vida diaria. De acuerdo a lo anterior, la telerehabilitación física consiste en la prestación de servicios de rehabilitación física a través de Internet para personas que se les dificulta el traslado a los centros de salud. Estos servicios de telerehabilitación física se pueden clasificar como evaluación física y fisioterapia. La evaluación física remota consiste en la valoración del cuerpo y sus funciones, mientras que la fisioterapia remota consiste en la asistencia de ejercicios físicos. La telerehabilitación cumple la función de hacer un seguimiento constante de los datos sobre la actividad física de una persona, su estado funcional y la evaluación de los cambios en la condición del paciente [16], [17].

2.2.2 Análisis del ciclo de marcha

El ciclo de marcha se refiere al seguimiento que va desde el contacto del talón con el suelo hasta el siguiente contacto del mismo. Cada ciclo de marcha comprende dos fases, la fase de apoyo que corresponde al 60% del ciclo y la fase de oscilación que corresponde al 40% de este ciclo como se observa en la figura 3. De acuerdo a esto, el paso corresponde a la actividad entre el apoyo del talón y el apoyo sucesivo del talón contralateral [18], [19].

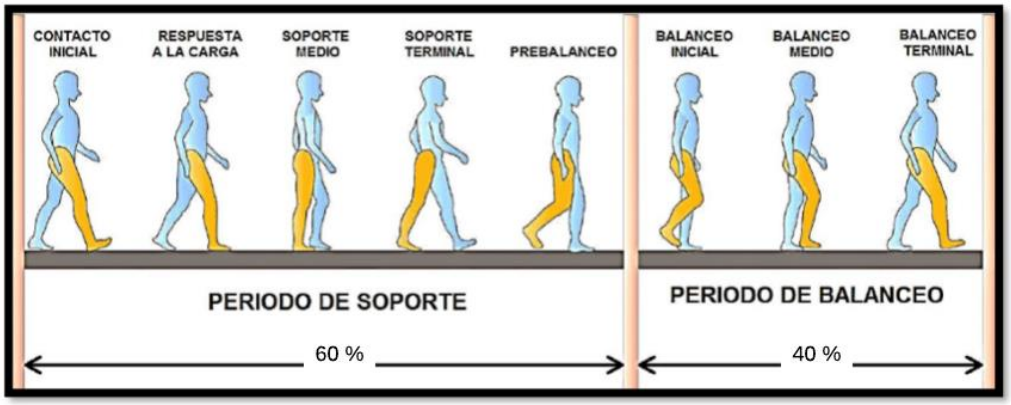


Figura 3: Fases del ciclo de marcha. Fuente: [20].

Una de las aplicaciones de la telerehabilitación física se centra en evaluar de forma remota el ciclo de la marcha de un paciente, lo cual involucra la cuantificación de diversos parámetros espacio-temporales que incluyen: ancho de paso, cadencia, longitud de paso, longitud de zancada, tiempo de apoyo, tiempo de balanceo, velocidad de la marcha, entre otros.

Entre los diferentes parámetros del ciclo de marcha se encuentra la cadencia de la marcha (CAD), que corresponde al número de pasos realizados en la unidad de tiempo [21]. La medición de la cadencia proporciona información objetiva e integral de la función neuromuscular y el rendimiento físico de las extremidades inferiores.

Los valores normales de cadencia según Murray se pueden observar en la tabla 1.

Tabla 1: Cadencia de pasos por rango de edad en hombres. Fuente: [21].

Edad	Cadencia (pasos/min)
20 – 25	115
30 – 35	111
40 – 45	122
50 – 55	118
60 – 65	115

El cálculo de la cadencia de la marcha se realiza mediante la Ec.1

$$CAD = \frac{\#\ de\ pasos\ (pasos)}{tiempo\ (min)} = \frac{pasos}{min} \qquad Ec.1$$

2.2.3 Actividad física

Según la OMS, La actividad física es todo movimiento corporal que es producido por los músculos esqueléticos y que exija gasto de energía [22]. De acuerdo a lo anterior, los

pasos realizados por el sujeto en la rutina terapéutica de la marcha con velocidad moderada en un lapso de tiempo de 10 minutos son de 840 pasos, aproximadamente 84 pasos por minuto.

2.3 Sistemas Basados en IoT (Internet de las Cosas)

El Internet de las Cosas (IoT) es un concepto informático que tiene como objetivo conectar objetos a Internet para comunicarse con varios dispositivos mediante conectividad IP sin interferencia humana. El entorno de IoT contiene varios objetos inteligentes como sensores, teléfonos inteligentes, tablets, entre otros. Además de esto, para intercomunicarse los dispositivos entre sí utilizan la identificación por radiofrecuencia (RFID), código de respuesta rápida (QR), tecnología inalámbrica, etc [23]. El ecosistema de IoT se puede observar en la figura 4.

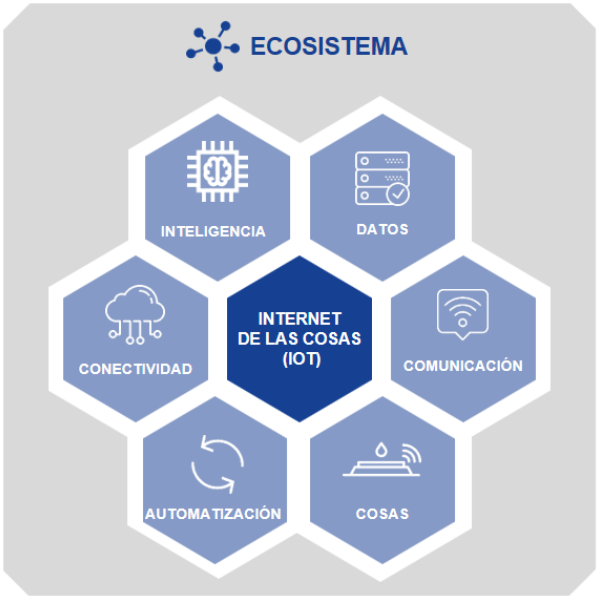


Figura 4: Aspectos relevantes del IoT. Fuente: [24].

De acuerdo a lo anterior, IoT se distingue por tener las siguientes características:

- Facilita la interconexión de personas a un dispositivo y de dispositivo a dispositivo.
- Dispositivos con detección inteligente.

- Ahorro de energía.
- Facilita una mejor comunicación entre humanos y máquinas.
- Brinda seguridad a las personas.

Un campo de aplicación importante del IoT es el entorno de la salud, donde se vislumbra el Internet de las cosas médicas (IoTM), que consiste en un conjunto de dispositivos médicos conectados a Internet para agilizar los procesos y servicios relacionados a la atención médica. Algunas ventajas del IoTM son que mejora la experiencia y la calidad de vida del usuario al optimizar los tiempos de espera y tener un diagnóstico más rápido y eficiente con el fin de prevenir enfermedades que afectan la salud del paciente [25], [26].

2.3.1 Plataformas para implementar sistemas IoT

- **ThingSpeak**

ThingSpeak es una plataforma de análisis de Internet de las cosas, la cual permite agregar, visualizar y analizar flujos de datos en la nube en tiempo real como se observa en la figura 5. Además de esto, ThingSpeak es un servicio de interfaz de programación de aplicaciones (API) que contiene una serie de diferentes sensores, con el objetivo de controlar los datos basados en la nube utilizando datos específicos de Matlab como el ID y la clave API del canal [27], [28].

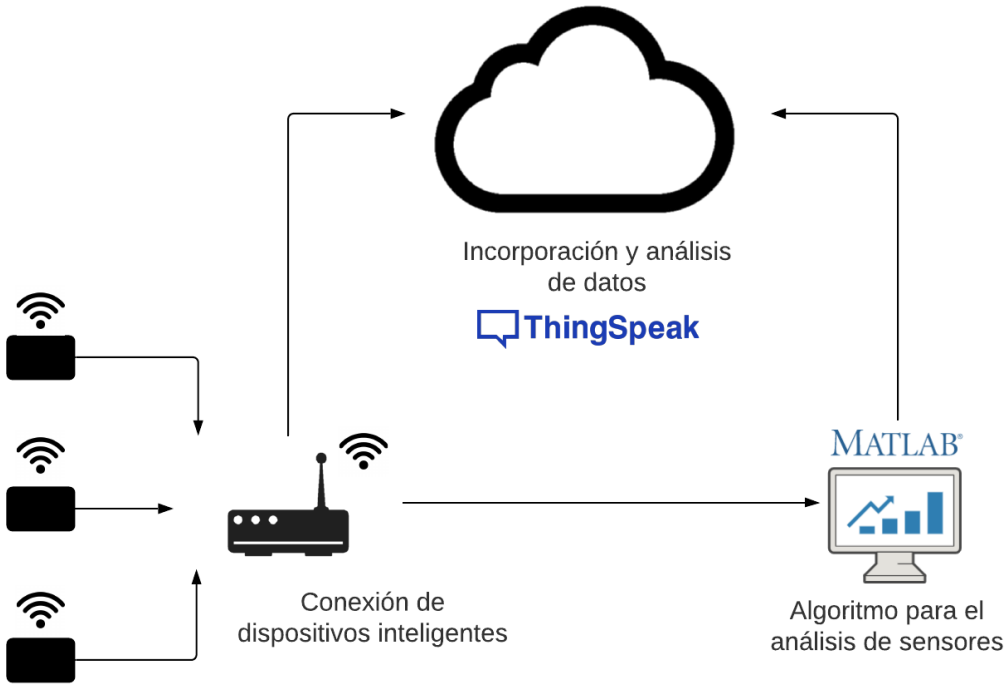


Figura 5: Relación de los elementos de ThingSpeak. Adaptado de: [28].

El canal de ThingSpeak es llamado el corazón de la nube ThingSpeak, puesto que, éste se utiliza para enviar el envío y almacenamiento de datos. Cada canal consta de ocho (8) campos para cualquier tipo de dato, tres (3) campos de ubicación y un campo de estado [27].

- **ThingView APK**

Thingview es una aplicación que está disponible en Play Store para dispositivos con sistema operativo Android y en App Store para dispositivos con sistema operativo IOS de forma gratuita y que permite visualizar los canales de ThingSpeak de forma fácil introduciendo solamente el ID del canal cuando es público y su clave API cuando se trata de un canal privado [29]. Para el ingreso a un canal público se requiere los datos mostrados en la figura 6.

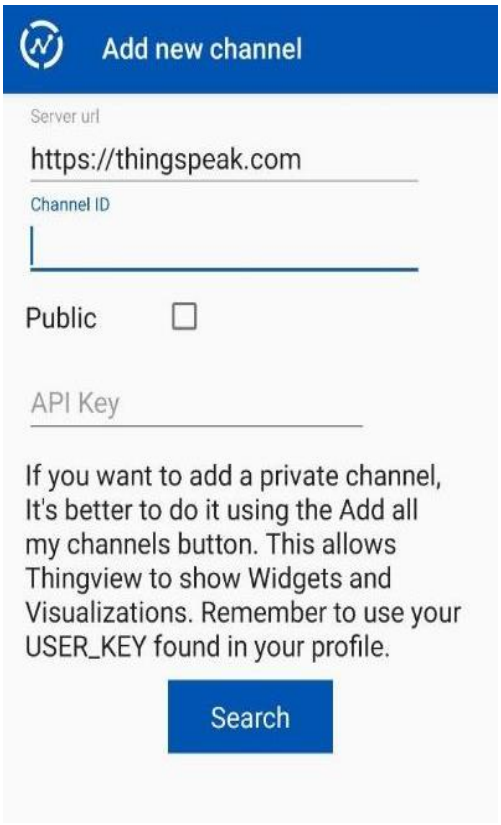


Figura 6: Interfaz principal aplicación Thingview. Fuente: Propia.

- **ThingsBoard**

ThingsBoard consiste en una plataforma IoT de código abierto que se puede utilizar para recopilar, procesar y visualizar los datos, además para la gestión de dispositivos de datos. Para enlazar un dispositivo a la plataforma se debe agregar una cuenta y así generar un token de ingreso. Por lo tanto, estos dispositivos se comunican mediante los siguientes protocolos, el transporte de telemetría de Message Queue Server (MQTT), el protocolo de aplicación restringida (CoAP) y el protocolo de transferencia de hipertexto (HTTP). Una característica importante es que ThingsBoard permite definir alarmas para dispositivos y activos, las cuales se pueden utilizar para enviar notificaciones a los dispositivos cuando se detecta algún problema en la etapa de preprocesamiento o procesamiento de datos [30], [31].

- **Plataforma KAA IoT**

Es una plataforma de IoT de código abierto que permite a los integradores de sistemas de salud establecer conectividad entre dispositivos e implementar funciones inteligentes en dispositivos médicos y productos de software relacionados. Además, proporciona un conjunto de herramientas para el desarrollo de productos con el objetivo de reducir el tiempo, riesgos y costos. Maneja toda la comunicación necesaria a través de objetos conectados y se ocupa de la seguridad de los datos, la interoperabilidad de los dispositivos y proporciona una conectividad a prueba de fallas [32], [33].

2.3.2 Seguridad en sistemas IoT

La mayoría de los dispositivos de IoT utilizan comunicación inalámbrica, por lo que se hace más fácil que los ciberdelincuentes intercepten los datos almacenados en los sistemas que no tienen algún tipo de cifrado correspondiente. Por lo tanto, se presentan algunos métodos o técnicas para implementar seguridad en la capa de aplicación.

- **Protocolo HTTPS**

HTTPS (Protocolo de Transferencia de Hipertexto) es un protocolo que incluye el protocolo de transferencia de hipertexto y el protocolo SSL/TLS para proteger la integridad y la confidencialidad de los datos de los usuarios mediante un canal seguro, donde su puerto es el 443 [34], [35]. Este protocolo garantiza la protección contra usuarios de internet malintencionados puesto que está protegido con la seguridad de la capa de transporte, la cual contiene las siguientes capas [35]:

    - Cifrado: Se cifran los datos intercambiados para que no puedan ser fáciles de interceptarlos ni robarle información.
    - Integridad de los datos: Los datos no pueden modificarse ni destruirse en el periodo de comunicación.

- Autenticación: Demuestra que los usuarios se comunican con el sitio web o sistema de manera segura.

- **MQTT**

MQTT (Message Queue Server Telemetry Transport) es un protocolo de comunicación de OASIS de IoT que se encarga de transmitir datos a través de internet. MQTT es un protocolo liviano con implementaciones de baja complejidad, bajo consumo de energía y poca sobrecarga y espacio. Por lo tanto, es confiable puesto que brinda la posibilidad de utilizar la función de calidad de servicio (QoS), la cual consta de tres niveles de calidad. La primera QoS es sin confirmación, la segunda con confirmación requerida y la última con protocolo de enlace de cuatro pasos. Siendo estas necesarias para que los datos enviados entre el emisor y el receptor sean seguros [36]–[39].

El protocolo se ejecuta sobre TCP / IP (puerto 1883 y puerto 8883 para MQTT sobre TLS/SSL) para la comunicación y el envío de información [39].

- **VPN (Red Privada Virtual)**

Una VPN (Red privada virtual) es una tecnología de red que se usa para la conexión de una o más computadoras a una red privada a través de Internet [40]. Además, es un entorno de comunicaciones en el que el acceso se controla para poder permitir conexiones dentro de un espacio [41].

La estructura lógica de la VPN como la topología, la conectividad, la accesibilidad y el control de acceso se asemeja a una red privada que utiliza instalaciones privadas. También admite varios modos de uso, entre estos las conexiones de cliente de acceso remoto y acceso controlado [42], [43].

De acuerdo a lo anterior, las VPN se establecen en la capa de enlace y la capa de red. Por lo tanto, es importante mencionar los protocolos de cada una de las capas para llegar a la solución de una red privada virtual [42].

- VPN de capa de enlace: Amplían los servicios de acceso remoto a través de Internet. Los protocolos de esta capa son:
    - PPTP: El protocolo de túnel punto a punto canaliza el tráfico PPP dentro de los paquetes IP.
    - L2TP: El protocolo de túnel de capa 2 combina características de PPTP con el protocolo de reenvío de capa 2.

- VPN de capa de red: El protocolo de la capa de red corresponde al IPSec, que está diseñado para brindar seguridad entre dos puertas de enlace o un cliente y una puerta de enlace.

- **Encriptación Liviana**

La encriptación liviana o ligera, consiste en el estudio de algoritmos que pueden ejecutarse en plataformas móviles, conocidas como Smart Device o dispositivos de recursos limitados como IoT, debido a sus propiedades matemáticas. Estos dispositivos ofrecen menor cantidad de recursos como espacio, memoria y energía [44].

2.4 Herramienta *Simulink Support Package for Android Device* de Matlab

Simulink es un entorno gráfico basado en diagrama de bloques para la simulación y diseño de modelos. Admite un diseño a nivel de sistema, simulación, generación automática de código, prueba y verificación continua de sistemas integrados, puede simular sistemas lineales y no lineales y modelos en tiempo continuo y tiempo discreto. Además, es un

entorno gráfico en el cual el modelo a simular se construye arrastrando los diferentes bloques que lo constituyen [45].

El entorno de Simulink incorpora una herramienta denominada Simulink Support Package for Android Devices que permite crear y ejecutar modelos de Simulink en dispositivos compatibles con Android. El soporte incluye una biblioteca de bloques Simulink para: Sensores, Captura y reproducción de audio, entrada de cámara y visualización de video, Widgets de interfaz de usuario y Comunicación mediante ThingSpeak, TCP/IP y UDP [46].

Además de esto, esta herramienta se compone de dos bloques en específico para realizar comunicación mediante IoT en ThingSpeak, en los cuales se deben configurar diferentes parámetros como el ID del canal, la API key, entre otros. Estos bloques son Thingspeak Read, Thingspeak Write.

- **Thingspeak Write:**

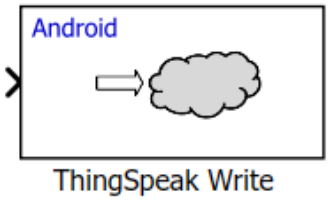


Figura 7: Bloque ThingSpeak Write Simulink. Fuente [47].

Este bloque permite publicar datos desde el host de destino en Internet de las Cosas usando la plataforma Thingspeak [47]. Se compone de los siguientes parámetros:

- Channel ID: ID del canal donde se van a publicar los datos.
- Write API Key: API Key de escritura que se obtiene en la plataforma Thingspeak.
- Number of fields: Número de campos donde se va a enviar la información.
- Intervalo de actualización: Tiempo en segundos de espera para el envío de datos.

Adicionalmente a esto, también se puede enviar la información de la ubicación. Es de gran importancia ya que tiene incorporado el protocolo HTTPS garantizando seguridad en el envío de los datos.

- **Thingspeak Read:**

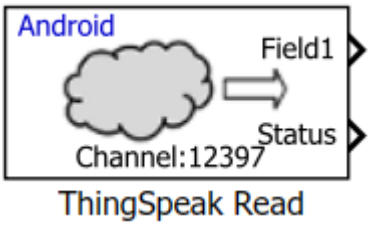


Figura 8: Bloque ThingSpeak Read Simulink. Fuente: [48].

Este bloque permite leer los datos almacenados en un canal de Thingspeak. Los puertos de salida corresponden a Field1 y Status. Donde Field1 corresponde a los datos leídos del campo que se seleccione, en el cual si es 0 significa que los datos son nulos y Status se refiere a la respuesta del servidor ThingSpeak para cada una de las solicitudes de lectura, donde 200 significa que la lectura se completó correctamente y 0 que los datos recibidos son nulos [48].

De acuerdo a lo anterior, los parámetros para este bloque están compuestos por:

- Channel ID: ID del canal donde se van a leer los datos.
- Channel Access, en el cual se puede seleccionar si el canal donde se van a leer los datos es público o privado. En el caso de seleccionar privado aparece un parámetro adicional que es Read API Key, la cual se encuentra en ThingSpeak.
- Field Number: Campo del canal ThingSpeak donde se van a leer los datos.
- Sample Time: Frecuencia de lectura de los datos.

2.5 Herramienta de análisis de video Kinovea

Kinovea es un software gratuito de análisis de videos e imágenes para el estudio del movimiento humano. Esta herramienta proporciona funciones tales como la captura, observación, anotación y medición. Además de esto, permite modificar y gestionar videos de una manera sencilla utilizando un sistema de ventanas y pequeños iconos gráficos como: cálculos de tiempo mediante cronómetros, cálculo de ángulos, medición de distancias, seguimiento de trayectoria, entre otros [49], [50].

En Ecuador en un estudio realizado en la Universidad de las fuerzas Armadas y realizando pruebas con deportistas que entrenan en la pista atlética los Chasquis; los autores, Criollo, Espinoza, Calero, Chávez y Fletiase, utilizan en [51] la herramienta Kinovea para analizar las diferencias biomecánicas entre deportistas principiantes y de alto rendimiento en la marcha deportiva. Para esto, en Kinovea se determinan con exactitud los grados de amplitud de las articulaciones de la rodilla y el codo en las diferentes fases de la marcha. Además, con el correcto estudio en Kinovea se determinaron aspectos como la forma de apoyo del pie en la fase de apoyo simple y apoyo doble, entre otros. Con el objetivo de comparar el rendimiento en los deportistas.

2.6 Normatividad de la telemonitorización en Colombia

2.6.1 Ley 1581 de 2012

La ley 1581 de 2012 es la ley de protección de datos personales reconoce y protege el derecho de toda persona a conocer, actualizar y modificar la información recopilada de bases de datos o archivos que puedan ser tratados por entidades de carácter público o privado [52], [53].

2.6.2 Resolución 2654 de 2019

La resolución 2654 de 2019 establece disposiciones para la telesalud y parámetros para la práctica de la telemedicina en el país. Así mismo establece el correcto uso de los medios

tecnológicos y lo primordial que es la calidad y seguridad en la atención e información de datos [3].

De acuerdo a lo anterior, es de vital importancia hacer hincapié en la seguridad del paciente, donde las actividades de telesalud y telemedicina deberán desarrollarse en el marco de la política nacional de seguridad del paciente implementando las barreras de seguridad para evitar y así mismo eliminar acontecimientos en los eventos adversos o incidentes relacionados en su aplicación. Además de esto, al prestar el servicio de la telemedicina, el profesional de la salud debe cumplir con su autonomía, responsabilidad y presentar ante el usuario un consentimiento informado. Pues este es donde se exponen todos los riesgos, beneficios y el tipo de información se va a manejar de la persona [3], [54].

En el capítulo IV de la resolución, relacionada con la Calidad de los Datos a través de Plataformas Tecnológicas o Dispositivos Electrónicos, se menciona que tales plataformas deben garantizar la Autenticidad, Integridad, Disponibilidad y Fiabilidad de la información.

2.6.3 Resolución 8430 de 1993

La resolución 8430 de 1993 es una de las principales pautas éticas que establece las normas científicas, técnicas y administrativas para la investigación en salud. En esta resolución se estipulan los aspectos éticos a tener en cuenta para realizar investigación en seres humanos para no tener ningún riesgo y poder efectuar una investigación segura donde prevalece la privacidad y seguridad del individuo [55].

2.7 Aplicaciones de Mensajería instantánea

2.7.1 Telegram

Telegram es una aplicación de mensajería instantánea que está diseñada para que los usuarios envíen fácilmente mensajes de texto, audios, imágenes, videos, archivos e incluso compartir ubicación de forma segura. Puesto que, utiliza el protocolo MTProto, que es diseñado a partir de algoritmos probados provocando que la seguridad sea acorde con el envío de mensajes a alta velocidad y la credibilidad en conexiones débiles [56], [57].

Además de esto, esta aplicación cuenta con dos capas de cifrado seguro. La primera capa de cifrado seguro es el cifrado servidor-cliente es utilizado en los chats privados y grupales. El protocolo que maneja este cifrado se subdivide en:

- Componente de alto nivel: Se define el método donde las consultas y respuestas API se convierten en mensajes binarios.
- Capa criptográfica: Se define el método donde se cifran los mensajes y se autorizan para transmitirse en la capa de transporte.
- Componente de transporte: Se define el método para que tanto el cliente como el servidor transmitan mensajes a través de un protocolo de red como HTTP, HTTPS, entre otros.

La segunda capa de cifrado seguro es el cifrado cliente-cliente o también llamado end-to-end, el cual es utilizado por los usuarios en los chats secretos donde solo el emisor y el receptor pueden visualizar los mensajes puesto que son específicos en cada dispositivo y no son parte de la nube de Telegram [57].

3. Metodología y Análisis de resultados

El presente proyecto se realizó mediante las fases metodológicas presentadas en la figura 9.

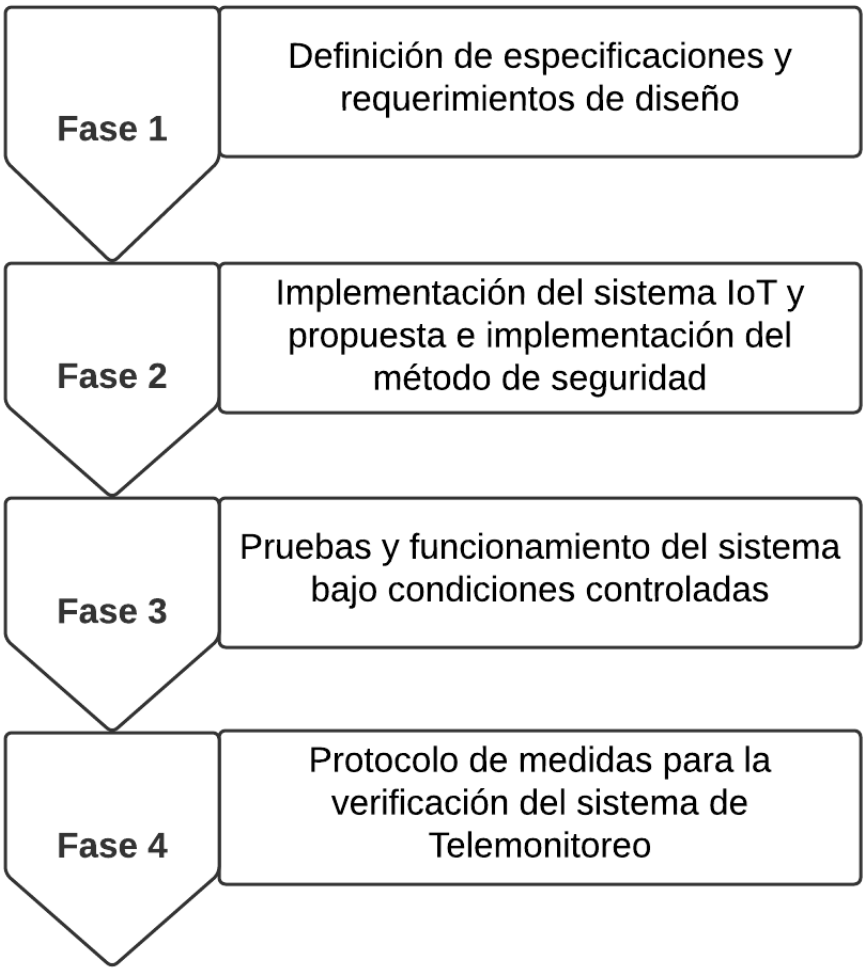


Figura 9: Fases metodológicas para cumplir el objetivo general. Fuente: Propia.

3.1 Definición de especificaciones y requerimientos de diseño

En esta sección se va a describir el funcionamiento del sistema, sus características y especificaciones para la implementación de seguridad. Inicialmente, se tuvo en cuenta los parámetros estipulados en la resolución 2654 de 2019.

Para esto, se han identificado las especificaciones funcionales definidas a continuación:

- Adquisición remota de información cinemática.
- Envío de datos a la nube.
- Almacenamiento de la información en la nube.
- Visualización de la información.
- Procesamiento de la información.
- Seguridad en el manejo de la información.
- Fiabilidad de la información.
- Registro mediante sistema IoT.
- Servidor en la nube gratuito.

Además, el sistema debe incluir los requerimientos técnicos establecidos en la tabla 2.

Tabla 2: Requerimientos técnicos del sistema IoT implementado. Fuente: Propia.

	Requerimiento	Magnitud
1	Variable a medir	Cadencia
2	Rango de medida	Marcha normal
3	Tipo de comunicación	Internet
4	Protocolo para la comunicación	HTTPS Cifrado end-to-end
5	Entorno IoT	ThingSpeak
6	Adquisición de datos	Dispositivo móvil.
7	Sensor	Acelerómetro

A partir del problema planteado y las especificaciones definidas, se propone el diagrama de bloques del sistema mostrado en la figura 10.

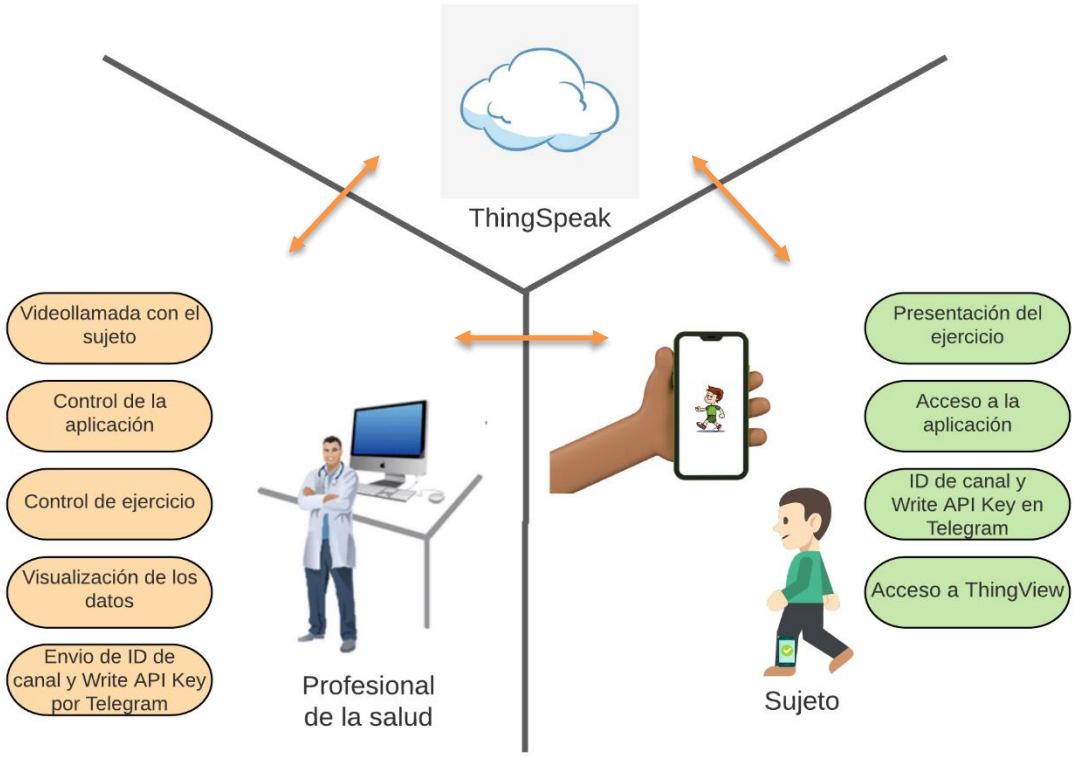


Figura 10: Esquema de funcionamiento del sistema IoT. Fuente: Propia.

Según la normatividad, por medio de un consentimiento informado, el sujeto proporciona la autorización para usar sus datos personales en la realización del proyecto. Con esta información se procede a implementar el sistema que consta de dos partes importantes: Una de registro de la información cinemática y otra del método de seguridad.

3.1.1 Sistema de registro de información cinemática

La acelerometría es una de las técnicas más fiables en el registro del nivel de actividad física que es realizada por una persona en un periodo de tiempo determinado [58]. De acuerdo a lo anterior, el sensor utilizado para el registro de información cinemática y particularmente para el cálculo de la cadencia de la marcha fue el acelerómetro, que

consiste en un elemento que mide la aceleración de una persona cuando realiza un movimiento y que puede ser uniaxial (un eje) o triaxial (tres ejes) [59].

Los parámetros temporales de la marcha que se pueden medir con el acelerómetro son la cadencia, la velocidad de la marcha y la velocidad de zancada. La velocidad de la marcha se define como la distancia recorrida en un intervalo de tiempo; mientras que la velocidad de la zancada mide la distancia recorrida en una zancada en relación a un intervalo de tiempo definido [19]. La cadencia de la marcha mide el número de pasos que una persona realiza en un minuto por lo que con el acelerómetro se facilita realizar la adquisición de los datos.

El sistema implementado de registro de información cinemática está enfocado a registrar la cadencia de la marcha del sujeto que se calculó utilizando el sensor acelerómetro de un dispositivo móvil con sistema operativo ANDROID. Posteriormente, por medio de una aplicación creada mediante Simulink y utilizando la herramienta Simulink Support Package for Android Devices, se registran y procesan los datos para subirlos a la nube ThingSpeak.

- **Dispositivo de registro de datos**

El dispositivo usado para la adquisición de datos es un celular Samsung J2 Prime con sistema operativo Android 6.0.1 Marshmallow, Procesador MediaTek MT6737T a 1.4 GHz, 1.5 GB de RAM y 8GB de almacenamiento interno. Para esto, se instalaron diversas aplicaciones en el computador tales como Android Studio, Android Tools, entre otras. Es requerido que la herramienta de Simulink junto con el dispositivo móvil se sincronicen y funcionen correctamente para poder instalar la aplicación en el dispositivo móvil. El procedimiento está detallado en el anexo A.

3.1.2 Método de seguridad

Tal como se argumentó en la sección anterior, el registro de datos se definió y realizó mediante un dispositivo móvil con Android. Según la sección 2.3.1 “Plataformas para implementar sistemas IoT”, existen diferentes alternativas para la implementación del sistema de telemonitorización. Teniendo en cuenta las especificaciones funcionales de la sección 3.1 y su capacidad para procesado de datos, se identificó la plataforma ThingSpeak y ThingView como herramientas de implementación del sistema IoT. Además, se realizó un análisis y búsqueda sobre el método de seguridad de envío de datos, el cual está basado en HTTPS. Según la sección 2.3.2 “Seguridad en sistemas IoT”, el HTTPS es uno de los métodos para implementar seguridad en la capa de aplicación.

De acuerdo a lo anterior, en el desarrollo del método de seguridad se emplearon Matlab y Simulink para realizar la aplicación en el celular, puesto que además cuenta con bloques de sensores como acelerómetro, giroscopio, entre otros; y de comunicación como TCP/IP y ThingSpeak Write, con el fin de subir los datos recolectados a la nube. ThingSpeak cuenta con conexión a Simulink facilitando el envío de datos y lo más importante de forma segura. Además, dispone de una Write API key de lectura que consta de 16 caracteres, donde descifrarla se tardaría mucho tiempo como se puede evidenciar en la tabla 3. ThingView tiene comunicación con ThingSpeak, en el cual con el ID del canal y la API Key de lectura se pueden visualizar los datos almacenados en el canal de la nube.

Tabla 3: Tiempo para descifrar una contraseña. Fuente: [60].

Caracteres		Tiempo estimado
“abcdefg”	7 caracteres	29 milisegundos
“abcdefgh”	8 caracteres	5 horas
“abcdefghi”	9 caracteres	5 días
“abcdefghij”	10 caracteres	4 meses
“abcdefghijk”	11 caracteres	1 década
“abcdefghijkl”	12 caracteres	2 siglos

En el caso en que el sujeto requiera visualizar los datos registrados, se empleó la aplicación de mensajería instantánea Telegram, para el envío de información de acceso necesaria. Telegram tiene una función incorporada de chat secreto que abarca la

encriptación end-to-end, la cual garantiza que solo el emisor y el receptor pueden visualizar los mensajes puesto que son específicos en cada dispositivo y no son parte de la nube de Telegram. Además, no se pueden tomar pantallazos, ni reenviar mensajes. Así mismo cuenta la autodestrucción del mensaje que se elimina automáticamente después de un determinado tiempo.

Según lo descrito en la sección 2.4, Simulink proporciona la herramienta de Simulink Support Package for Android Devices, la cual incluye varias librerías. Teniendo en cuenta que el sistema debe registrar, calcular y enviar a la nube la información de la variable de la cadencia de la marcha, se utilizaron las siguientes librerías:

- Sensor acelerómetro, para la obtención de los datos.
- Bloque de Matlab Function, para realizar el procesamiento de los datos.
- Bloque de ThingSpeak Write, para subir datos a la nube de manera segura.

3.2 Implementación del sistema IoT y propuesta e implementación del método de seguridad

En esta sección se describe el proceso realizado en la implementación del sistema IoT definido en la sección anterior, desde la protección de la nube ThingSpeak hasta el envío de datos de manera segura. Además de esto, se tiene en cuenta todo lo utilizado para tener un sistema seguro.

3.2.1 Sistema IoT basado en la plataforma ThingSpeak

La implementación del sistema IoT se realizó mediante la plataforma ThingSpeak, facilitando así el desarrollo de la aplicación tal y como se muestra en la figura 11.

Figura 11: Activación de la seguridad de verificación dos pasos en la plataforma ThingSpeak. Fuente: Propia.

En la figura 11, se puede observar el proceso que el especialista debe realizar para ingresar al sistema de manera segura. Por lo tanto, procede hacer lo siguiente:

El especialista médico inicia sesión en Mathworks, después de iniciar sesión se dirige a la pestaña mi cuenta y se hace click en ajustes de seguridad. En ajustes de seguridad se selecciona verificación dos pasos.

La verificación dos pasos de Mathworks ofrece una mayor protección a un dispositivo o navegador de confianza mediante un código de verificación. Puesto que, cada vez que ingrese al sistema el código cambia evitando que usuarios malintencionados puedan usar la licencia e incluso puedan acceder a los datos almacenados [61].

En la verificación dos pasos se puede seleccionar tres métodos diferentes:

- Por medio de mensaje de texto, al número de celular que se coloque en la configuración.

- A través de correo electrónico.
- Por medio de aplicaciones para teléfonos móviles como Google Authenticator.

Al seleccionar uno de los tres métodos, cada vez que se ingresa al sistema se va a enviar un código de verificación accediendo de forma segura. Se describe de manera detallada en el anexo B.

3.2.2 Desarrollo de la aplicación en Simulink

En el entorno de Simulink y utilizando la herramienta Simulink Support Package for Android Devices se realizó la aplicación mostrada en la figura 12.

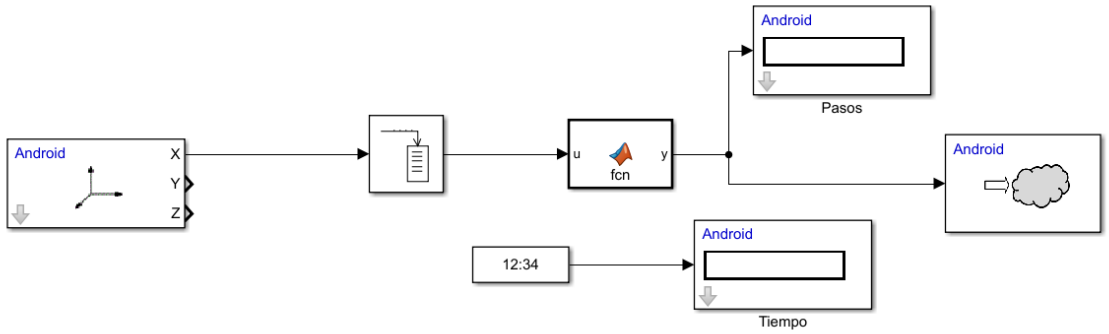


Figura 12: Modelo de la aplicación implementado en Simulink. Fuente: Propia.

En la figura 12, se observan los bloques utilizados para realizar el modelo de la aplicación en Simulink y así mismo poder subir los datos a la nube ThingSpeak de manera segura.

En el modelo implementado en Simulink es de interés resaltar que se va a calcular la variable cinemática cadencia, la cual se obtiene por un periodo de tiempo determinado. De acuerdo a lo anterior, el tiempo escogido fue de 30 segundos debido a que el intervalo de actualización en el bloque ThingSpeak Write para subir los datos a la nube no puede ser inferior a 22 segundos. Pero aún así, según lo reportado en la literatura y en algunos estudios cinemáticos el valor de la frecuencia de medida del sensor acelerómetro es de 100 Hz para el análisis de la marcha [62], [63] . A ese bloque se le conecta un buffer que

acumula los datos por un tiempo de 30 segundos con el fin que los datos almacenados puedan estar sincronizados con el bloque de ThingSpeak Write. A la salida del bloque de buffer se le conecta el bloque de Matlab Function, en la cual se hace el procesamiento de los datos con el fin de seleccionar la información correcta de la señal mostrada por el acelerómetro. Finalmente, a esa salida del bloque Matlab Function se le conecta el bloque de ThingSpeak Write para subir los datos a la nube ThingSpeak de una manera segura, teniendo en cuenta que trabaja con el protocolo HTTPS. En el anexo C, se describe cada uno de los bloques junto a su configuración.

Para calcular el parámetro de la cadencia, se procesó los datos del acelerómetro de acuerdo al diagrama de flujo que se presenta en la figura 13:

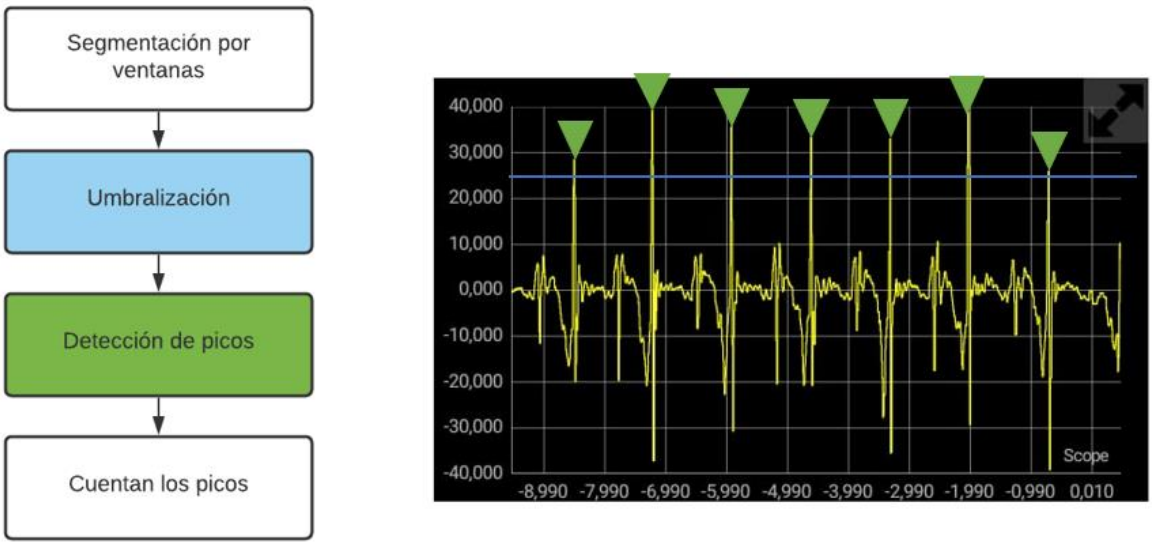


Figura 13. Diagrama de flujo para calcular la cadencia de la marcha. Fuente: Propia.

En la figura 13, se observa el diagrama para el procesamiento de los datos y así poder calcular correctamente la información de la cadencia de la marcha. Por lo tanto, se hizo una segmentación por ventanas en la cual el buffer almacena 3000 datos que son muestreados a 100 Hz, teniendo una ventana de 30 segundos de datos. A esa ventana, se le realizó una umbralización por inspección visual detectando en las señales registradas cual umbral era el más adecuado para detectar los picos más altos que corresponden a un

paso. Finalmente, se obtiene la longitud del vector para contar los picos y así tener la información necesaria.

3.2.3 Visualización de datos por parte del sujeto y el especialista médico

La visualización de los datos obtenidos por parte del sujeto se llevó a cabo mediante la aplicación de mensajería instantánea Telegram y la aplicación ThingView. Además de esto, el especialista médico mediante la herramienta Matlab Visualization ofrecida por Thingspeak puede realizar un mejor análisis de los datos accediendo al servidor en la nube.

A continuación, se muestra el diagrama implementado para la visualización de datos de manera segura.

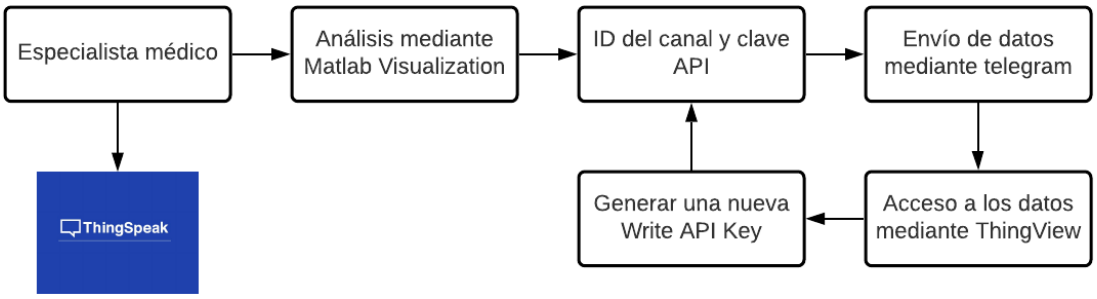


Figura 14: Esquema para el envío y la visualización de la información almacenada en la nube. Fuente: Propia.

En la figura 14, se puede evidenciar el diagrama implementado para la visualización y análisis de datos por parte del sujeto y del especialista médico. Por lo tanto, se va a explicar cada uno de los bloques:

- Los datos son subidos a la nube mediante el bloque ThingSpeak Write tal y como se evidencia en la sección 3.2.2. Una vez se suben, el especialista médico realiza un análisis con herramientas proporcionadas por Matlab Visualization que incluye el diagrama de cajas para evaluar de manera más precisa los datos obtenidos.

- El especialista médico al tener acceso a la nube ThingSpeak, tiene la información completa de los datos necesarios para que el sujeto pueda observar los resultados obtenidos. Para esto, se dirige a la pestaña de API keys donde se mostrará la información que se presenta en la figura 15. Los datos encerrados en el cuadro rojo que corresponde al ID del canal y la Write API Key son los que se va a enviar en el siguiente paso.

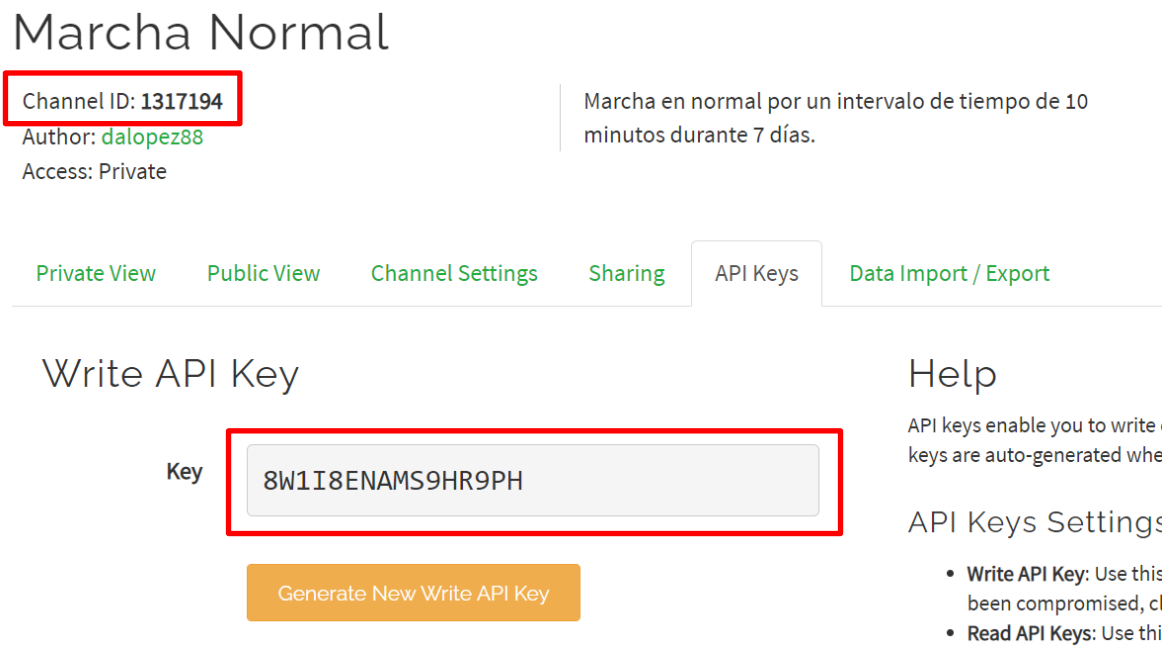


Figura 15: Datos enviados por el especialista médico. Fuente: Propia.

- El ID del canal y la clave API son datos ofrecidos por ThingSpeak, al tener 16 caracteres y como se observa en la tabla 3, que con tan solo 12 caracteres demora en descifrar 2 siglos, con 16 caracteres es muy segura y en algunos casos imposible de descifrar.

- Envío de datos mediante Telegram:

  El envío de datos mediante Telegram se hizo siguiendo los pasos mostrados en la figura 16.

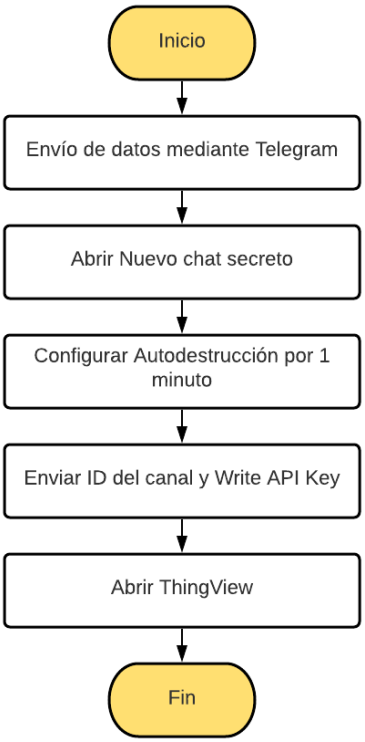


Figura 16: Envío de datos mediante Telegram. Fuente: Propia.

Para el envío de datos mediante Telegram, se utilizó el chat secreto como se explicó anteriormente y que cuenta con cifrado end-to-end, autodestrucción automática de los mensajes y la imposibilidad de reenviar mensajes y tomar capturas de pantalla. Para esto, se crea un nuevo chat secreto mediante el dispositivo móvil del especialista médico, se configura la autodestrucción de mensajes por 1 minuto y se envía el ID del canal y la Write API Key al sujeto. Estas características garantizan la seguridad del sujeto donde solo él puede tener el ID del canal y la Write API Key que le permitirán ingresar a la información de sus datos.

- Acceso a los datos mediante ThingView y Generar nueva Write API Key.

  Para el acceso a los datos mediante ThingView, se siguieron los pasos mostrados en la figura 17.

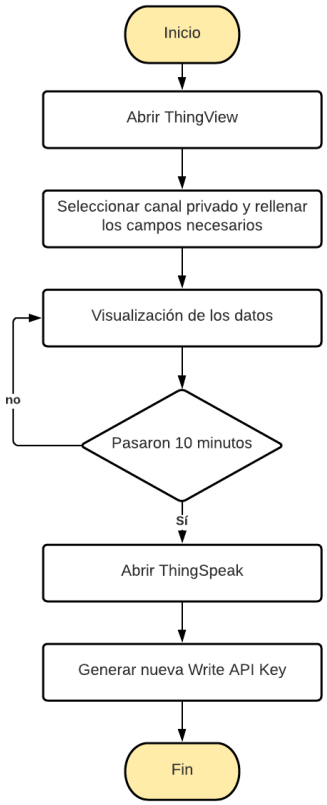


Figura 17: Visualización de datos mediante ThingView. Fuente: Propia

Una vez el sujeto tenga los datos necesarios, abre ThingView y procede a rellenar los campos para ingresar al sistema. Esto se puede observar en la figura 18 y 19.

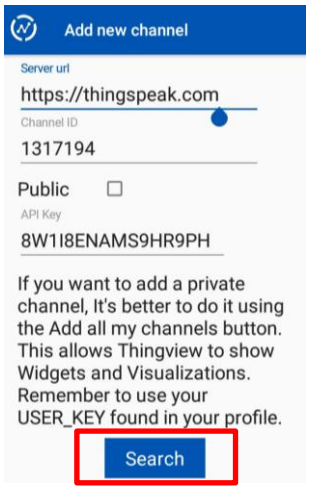


Figura 18: Aplicación ThingView. Fuente: Propia.

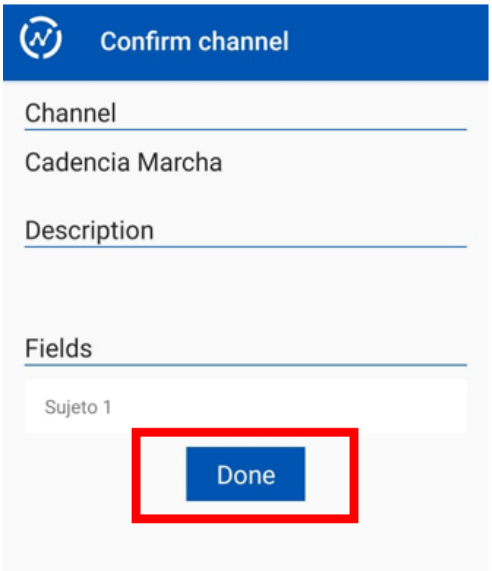


Figura 19: Aplicación ThingView. Fuente: Propia.

Al presionar el botón Done, la aplicación se dirige a lo mostrado en la figura 20, donde se muestra el canal y al presionar puede acceder a la información de los datos adquiridos.

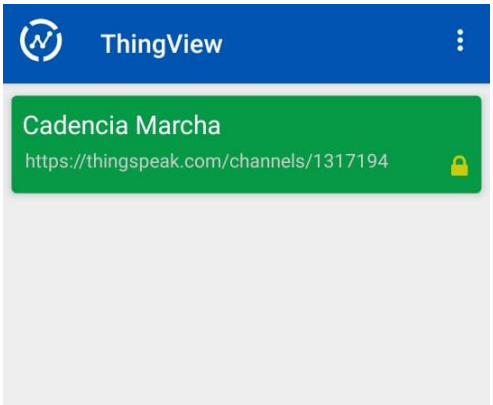


Figura 20: Aplicación ThingView. Fuente: Propia.

Al ver los datos por diez (10) minutos, se autodestruye el mensaje enviado por el especialista que corresponde al ID del canal y la Write API Key, por lo que el especialista médico se redirige nuevamente a ThingSpeak → pestaña API Keys → Generar nueva Write API Key, tal y como se evidencia en la figura 21.

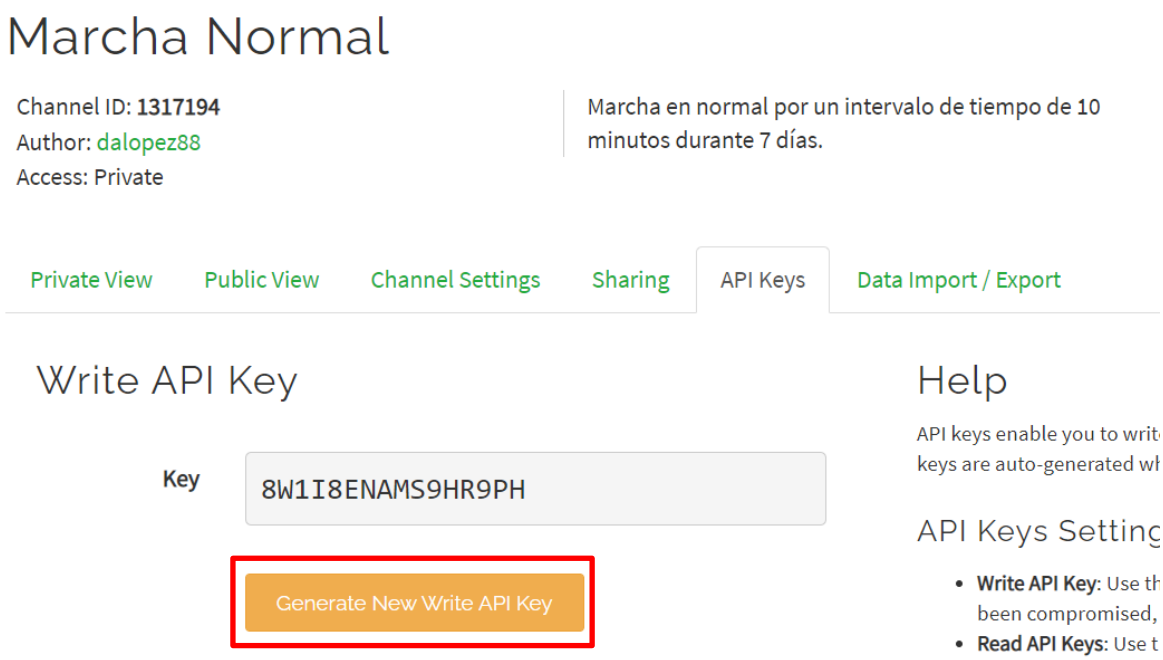


Figura 21: Indicación para generar una nueva Write API Key. Fuente: Propia.

Para volver a ingresar a los datos, el sujeto debe comunicarse con el especialista médico para que le brinde la nueva Write API Key y así pueda acceder nuevamente al sistema. En el caso que no lo haga, no le permitirá acceder a los datos como se muestra en la figura 22.

Figura 22: Error al ingresar a la información. Fuente: Propia.

3.3 Evaluación del funcionamiento del sistema bajo condiciones controladas

En esta sección se describe lo relacionado a las pruebas realizadas para verificación técnica del funcionamiento del sistema. Abarca desde la elección de los parámetros de los bloques de la aplicación en Simulink hasta la visualización y análisis de los datos mediante ThingView y Matlab Visualization respectivamente.

3.3.1 Protocolo de pruebas

Las pruebas se llevaron a cabo siguiendo la normatividad 8030 de 1993 relacionada a investigación y estudios con personas. A los participantes se les proporcionó un consentimiento informado, describiendo el procedimiento experimental. Ver anexo D.

Las pruebas se realizaron en sujetos sanos, teniendo en cuenta que el objetivo es evaluar la funcionalidad técnica de la herramienta desarrollada y no realizar un seguimiento terapéutico con la herramienta. Dentro de las pruebas, tampoco está contemplada la evaluación de la usabilidad, lo cual se considera como un trabajo futuro.

3.3.2 Evaluación de la ubicación para registro de información cinemática

El propósito de la evaluación es identificar la ubicación y orientación adecuada del celular sobre el cuerpo del usuario, para adquirir la información del acelerómetro. Existen múltiples estudios que han propuesto diferentes ubicaciones del celular para registrar información de acelerometría para estimar parámetros de la marcha [64]. Sin embargo, no hay una ubicación única.

Se realizaron las pruebas experimentales utilizando la orientación del acelerómetro tanto del eje X como del eje Y del dispositivo y ubicados en la cintura y en los segmentos de la cadena cinemática del miembro inferior.

En la figura 23, se observa el dispositivo ubicado a nivel de la cintura entre el ombligo y la pelvis, cuando el usuario realiza marcha a una velocidad normal.

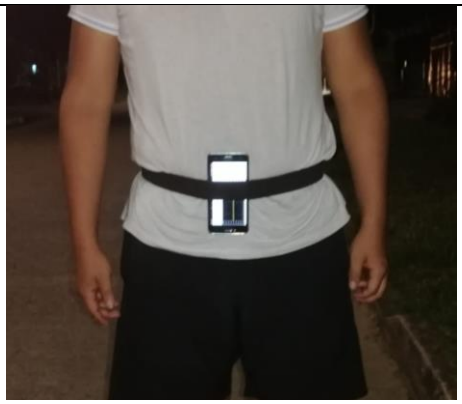
Cintura – Eje X	Cintura – Eje Y
	
Figura 23 A: Dispositivo instrumentado en la cintura con orientación en el eje X. Fuente: Propia.	Figura 23 B: Dispositivo móvil en la cintura con orientación en el eje Y. Fuente: Propia.

Figura 23: Dispositivo móvil en la cintura con orientación en el eje X y Y. Fuente: Propia.

Antes de iniciar con las pruebas, se debe tener en cuenta realizar un buen procesamiento de los datos para que los datos adquiridos sean lo correcto. Por lo tanto, se hizo el siguiente procesamiento en Simulink con el dispositivo móvil ubicado en la cintura:

MATLAB Function*

```
1   function y = fcn(u)
2   umb = [15 -15]; %Se escogen umbrales de acuerdo
3                   %a la gráfica obtenida por el acelerometro
4   u(and(u<umb(1),u>umb(2)))=0; % Se hace la condición para poner
5                                % los valores en 0.
6   a = findpeaks(u); % Se detectan los picos de la señal
7   y = length(a);
8   %y = 2*length(a); % Se cuentan los picos detectados y se
9                     % multiplican por 2.
10  end
```

Figura 24: Procesamiento de la señal en Simulink. Fuente: Propia.

Una vez el procesamiento de los datos sea el correcto, se procede a realizar las pruebas utilizando el eje X y Y del sensor acelerómetro con una frecuencia de 100 Hz y al ubicar el dispositivo en la cintura se obtuvieron las siguientes gráficas:

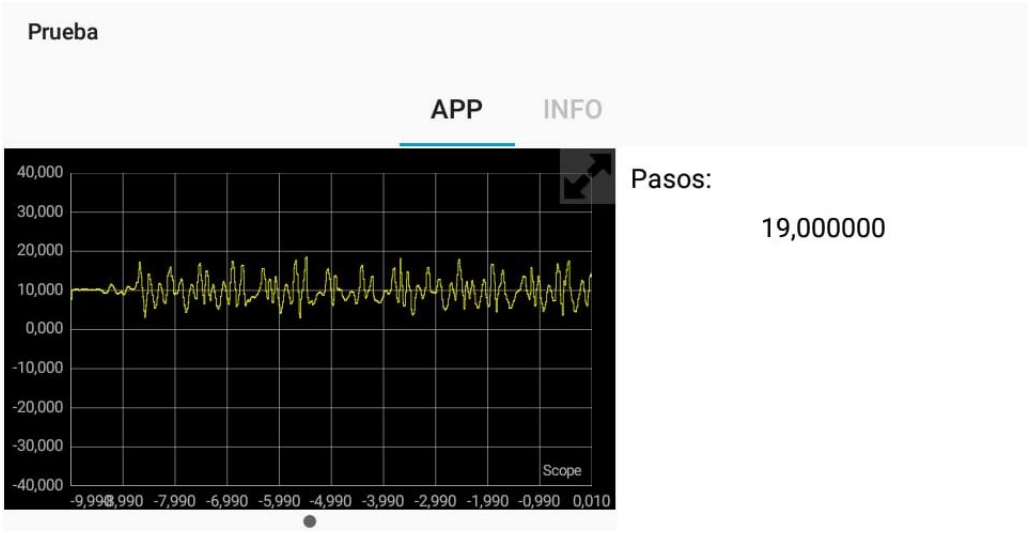


Figura 25: Gráfica con dispositivo móvil en la cintura utilizando el eje X del acelerómetro y frecuencia de 100 Hz. Fuente: Propia.

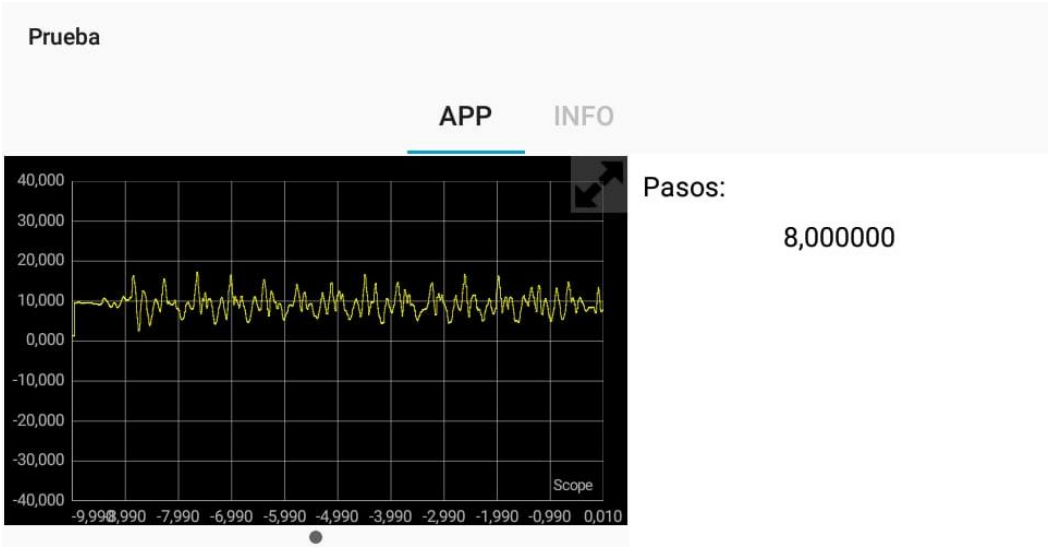


Figura 26: Gráfica con dispositivo móvil en la cintura utilizando el eje Y del acelerómetro y frecuencia de 100 Hz. Fuente: Propia.

Como se puede observar en las figuras 25 y 26, las señales registradas con el dispositivo ubicado en la cintura aparecen mucho ruido por lo que es difícil identificar los picos e incluso tienen un error bastante significativo respecto al valor verdadero. Se contaron los pasos en un tiempo de 10 segundos y posteriormente a esto, se los comparó con los reales donde se obtuvo lo siguiente:

Tabla 4: Error de las señales obtenidas con el dispositivo ubicado en la cintura. Fuente: Propia.

	Eje X	Eje Y
Valor real (pasos)	14	14
Valor experimental (pasos)	19	8
Error obtenido	35.71 %	42.85 %

Posteriormente, se realizaron mediciones en los miembros inferiores, específicamente con el dispositivo ubicado al interior del tobillo como se observan en la figura 27.

Tobillo – Eje X	Tobillo – Eje Y
	
Figura 27 A: Dispositivo móvil en el tobillo con orientación en el eje X. Fuente: Propia.	Figura 27 B: Dispositivo móvil en el tobillo con orientación en el eje Y. Fuente: Propia.

Figura 27: Dispositivo móvil ubicado en el tobillo con orientación en el eje X y Y. Fuente: Propia.

Nuevamente, antes de iniciar con las pruebas se debe tener en cuenta realizar el correcto procesamiento de los datos. Por lo tanto, se hizo el siguiente procesamiento en Simulink con el dispositivo móvil ubicado en el tobillo:

Editor - Block: Prueba/MATLAB Function*

MATLAB Function*

```
function y = fcn(u)
umb = [25 -25]; %Se escogen umbrales de acuerdo
                %a la gráfica obtenida por el acelerometro
u(and(u<umb(1),u>umb(2)))=0; % Se hace la condición para poner
                             % los valores en 0.
a = findpeaks(u); % Se detectan los picos de la señal
y = 2*length(a); % Se cuentan los picos detectados y se
                 % multiplican por 2.
end
```

Figura 28: Procesamiento de la señal en Simulink. Fuente: Propia.

Una vez el procesamiento de los datos sea el correcto, se procede a realizar las pruebas utilizando el eje X y Y del sensor acelerómetro con una frecuencia de 100 Hz y al ubicar el dispositivo al interior del tobillo se obtuvieron las siguientes gráficas:

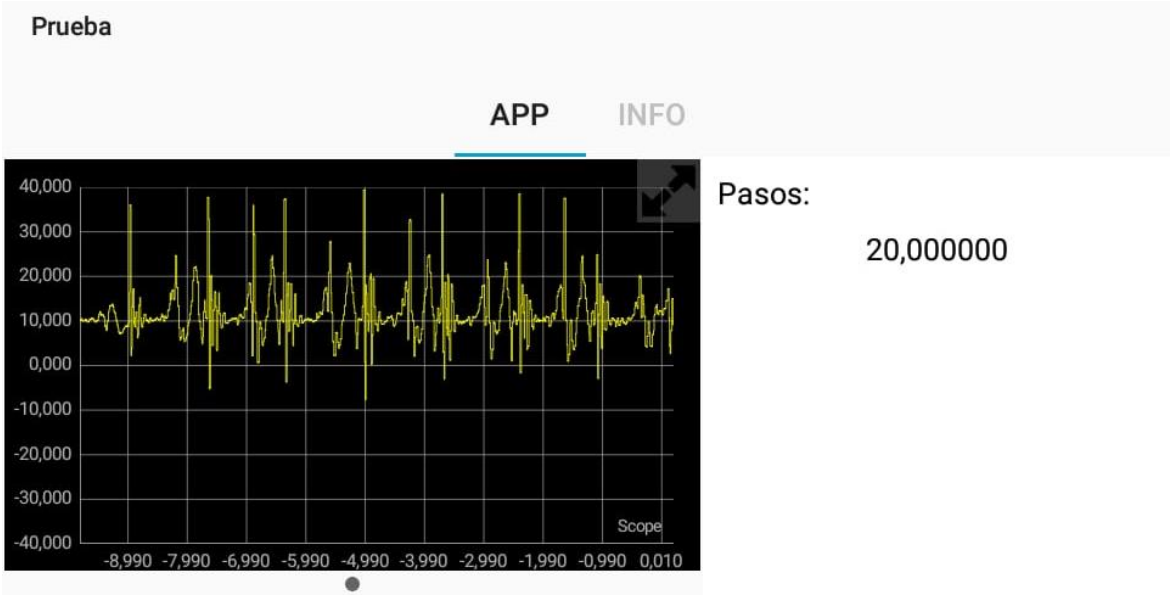


Figura 29: Gráfica con dispositivo móvil en el tobillo utilizando el eje X del acelerómetro y frecuencia de 100 Hz. Fuente: Propia.

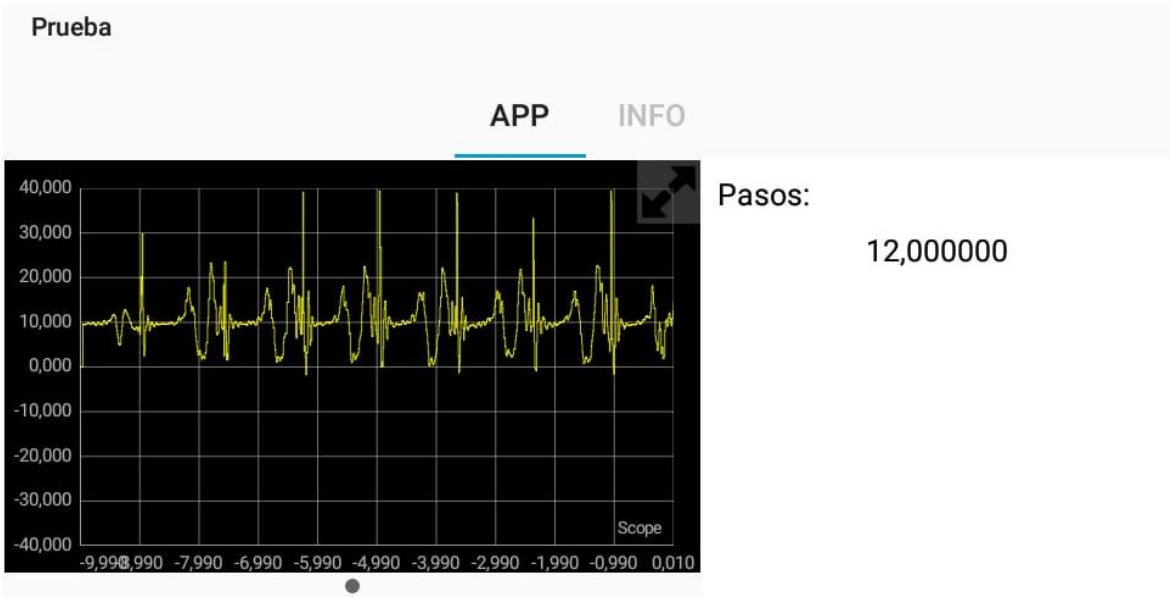


Figura 30: Gráfica con dispositivo móvil en el tobillo utilizando el eje Y del acelerómetro y frecuencia de 100 Hz. Fuente: Propia.

Como se puede observar en las figuras 29 y 30, las señales registradas con el dispositivo ubicado en el tobillo tienen picos más definidos, pero aún así se presenta un error respecto al valor real.

Tabla 5: Error de las señales obtenidas con el dispositivo ubicado en el tobillo. Fuente: Propia.

	Eje X	Eje Y
Valor real (pasos)	14	13
Valor experimental (pasos)	20	12
Error obtenido	42.85 %	7.69 %

En la tabla 4 y 5, se compararon los valores obtenidos en la aplicación y los valores reales con el dispositivo ubicado en la cintura y el tobillo donde se obtuvieron errores muy altos con la imposibilidad de hacer dicha implementación para la realización de las pruebas.

Finalmente, al ubicar el dispositivo como se observa en la figura 27 B utilizando el eje X del acelerómetro y una frecuencia de 100 Hz, se obtuvo una señal tal y como se contempla en la figura 31, donde se pueden identificar de forma más adecuada los picos para realizar el procesamiento de los datos. Cabe destacar que los picos detectados se multiplican por dos. Puesto que, la señal se obtiene de solo un miembro inferior.

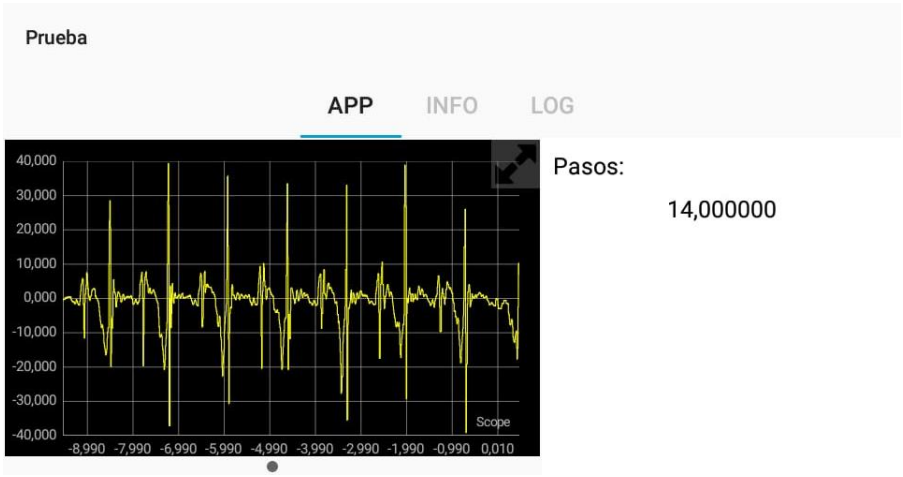


Figura 31: Gráfica con dispositivo ubicado en el tobillo eje Y, utilizando el eje X del acelerómetro y frecuencia de 100 Hz. Fuente: Propia.

3.3.3 Evaluación del envío de la información a la nube

Según la configuración del bloque ThingSpeak Write tal y como se describe en el anexo C, el intervalo de actualización mínimo es de 15 segundos si es un canal público. En este caso se trata de un canal privado que al configurarlo con 15 segundos los datos no se subirán correctamente mostrando un error como se observa en la figura 32. Por lo tanto, cuando se selecciona un intervalo de actualización de 15 segundos ocurre un inconveniente al subir los datos a la nube, donde aparece un mensaje “incremente el intervalo de actualización”. Es por esto que el intervalo de actualización se estableció en 30 segundos en el cual los datos se suben correctamente apareciendo el mensaje “Datos publicados en el servidor ThingSpeak”, lo cual se verificó en el servidor web de ThingSpeak.

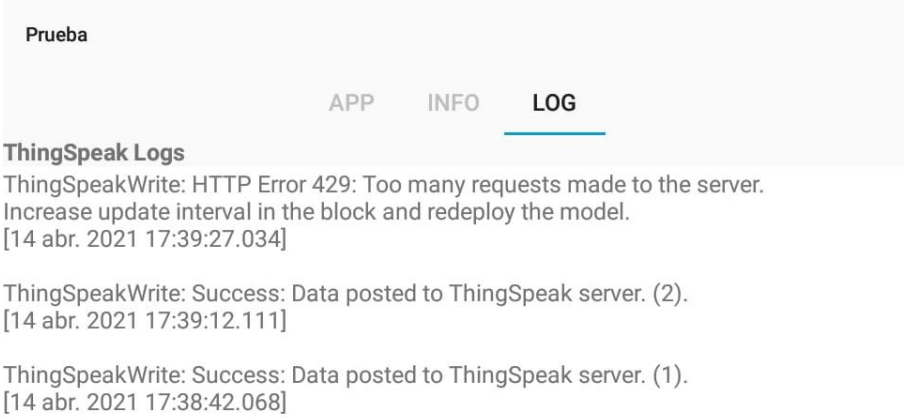


Figura 32: Información de los datos subidos a ThingSpeak. Fuente: Propia.

3.3.4 Evaluación de los parámetros cinemáticos calculados

Con el objetivo de evaluar la fiabilidad de la información adquirida y calculada por la aplicación correspondiente a la cadencia de la marcha, se realizó un conjunto de pruebas que permite cuantificar la similitud entre la información proporcionada por la aplicación y la información real. De acuerdo a lo anterior, se ubicó el dispositivo en el tobillo tal y como se explicaba en la sección 3.3.2 “Evaluación de la ubicación para registro de información cinemática”. Antes de iniciar la marcha se abre la aplicación y se espera durante 30 segundos con el objetivo de adquirir los datos correctamente. Además de esto, al no contar con un espacio adecuado para el estudio de variables cinemáticas, las pruebas se hicieron en una pista donde no se presentaban obstáculos teniendo en cuenta las siguientes condiciones experimentales: La frecuencia de adquisición del video se realizó a 29,42 frames por segundo con una resolución de 1080 x 1920 pixeles. El registro se realizó a una distancia desde el sujeto hasta la cámara de 1.5 metros, con condiciones de iluminación moderada.

Para esto se hizo un análisis comparativo entre la magnitud real de la cadencia (obtenida mediante análisis del video) y la magnitud calculada por el sistema desarrollado. Esto se llevó a cabo mediante tres repeticiones donde el sujeto ejecutaba la marcha durante cinco

minutos, a una velocidad normal. Este tiempo se estableció de acuerdo a lo reportado en la literatura en la cual en un artículo publicado en IEEE en la conferencia Internacional sobre e-Salud y Bioingeniería establecen en [65] que realizan pruebas con un sujeto sano con 5 repeticiones cada una de 60 segundos para el análisis de marcha. Además se hizo búsqueda de otro artículo donde comparan las actividades del tronco y de los miembros inferiores durante la marcha humana en un tiempo de 2 minutos [66]. De acuerdo a lo anterior, se debe tener en cuenta que las pruebas se hacen en un entorno libre sin una velocidad constante donde en muy poco tiempo se adquieren menos datos lo que no nos lleva a tener una información fiable.

Para el análisis en Kinovea se colocó un marcador a la altura del tobillo tal y como se observa en la figura 33.

Figura 33: Marcador para el análisis en Kinovea. Fuente: Propia.

Posteriormente a esto, el sujeto comenzaba la marcha donde se obtuvieron los siguientes resultados.

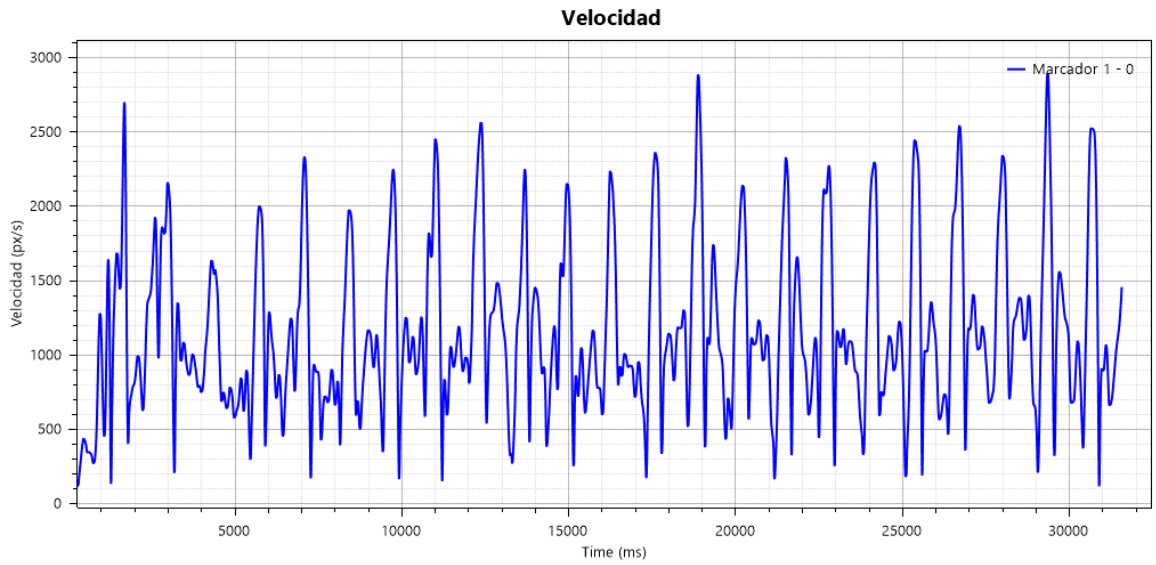


Figura 34: Análisis en Kinovea 30 segundos de la primera prueba. Fuente: Propia.

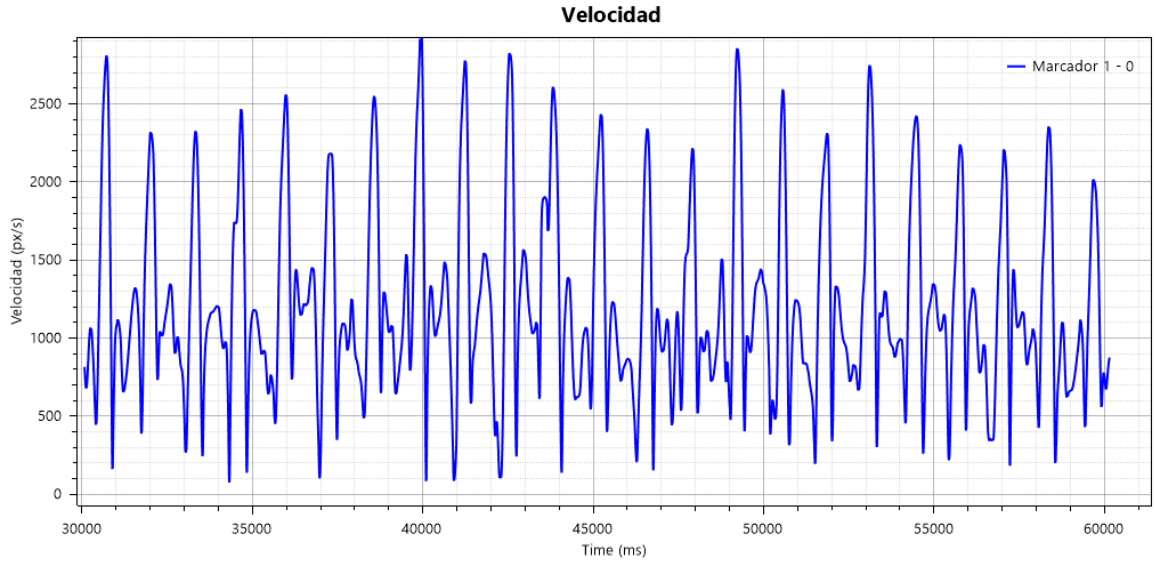


Figura 35: Análisis en Kinovea de los 30 siguientes segundos de la primera prueba. Fuente: Propia.

La figura 34 y 35 muestra la gráfica de los 30 y 60 segundos respectivamente de la primera prueba, donde cada pico corresponde a dos pasos que da el sujeto. De acuerdo a lo anterior, se hizo una tabla comparativa en la cual se muestran el cálculo de pasos mediante la herramienta Kinovea y la nube ThingSpeak.

Tabla 6: Primera prueba de la comparación de la cadencia de la marcha durante cinco minutos mediante el análisis en Kinovea y la nube ThingSpeak. Fuente: Propia.

Prueba 1	Comparación análisis de marcha		
	Kinovea / Pasos	ThingSpeak / Pasos	Error
30 seg	45	46	2%
60 seg	45	42	7%
90 seg	44	44	0%
120 seg	45	44	2%
150 seg	45	44	2%
180 seg	45	46	2%
210 seg	45	42	7%
240 seg	44	40	9%
270 seg	45	44	2%
300 seg	45	44	2%
Total de pasos	448	436	4%

Tabla 7: Segunda prueba de la comparación de la cadencia de la marcha durante cinco minutos mediante el análisis en Kinovea y la nube ThingSpeak. Fuente: Propia.

Prueba 2	Comparación análisis de marcha		
	Kinovea / Pasos	ThingSpeak / Pasos	Error
30 seg	44	48	9%
60 seg	43	42	2%
90 seg	43	40	7%
120 seg	43	42	2%
150 seg	43	42	2%
180 seg	42	38	10%
210 seg	43	44	2%
240 seg	42	44	5%
270 seg	41	38	7%
300 seg	41	42	2%
Total de pasos	425	420	5%

Tabla 8: Tercera prueba de la comparación de la cadencia de la marcha durante cinco minutos mediante el análisis en Kinovea y la nube ThingSpeak. Fuente: Propia.

Prueba 2	Comparación análisis de marcha		
	Kinovea / Pasos	ThingSpeak / Pasos	Error
30 seg	43	40	7%
60 seg	42	44	5%

90 seg	42	42	0%
120 seg	42	40	5%
150 seg	42	40	5%
180 seg	42	38	10%
210 seg	42	40	5%
240 seg	41	42	2%
270 seg	41	40	2%
300 seg	41	40	2%
Total de pasos	418	406	4%

De acuerdo a lo mostrado en la tabla 6, 7 y 8 los resultados obtenidos mediante el análisis en Kinovea no fueron muy distintos a los subidos a la nube, obteniendo un error promedio de la aplicación del 5%.

3.4 Validación del sistema de Telemonitoreo

Se realizaron pruebas de validación del sistema completo con el objetivo de evaluar lo siguiente:

- Registro de información cinemática, en un período de 7 días.
- Envío adecuado a la nube de la información registrada.
- Verificación de la integridad de los datos en el servidor en la nube.
- Análisis de los datos registrados en el servidor.
- Seguimiento de forma remota de la actividad física.

Teniendo en cuenta que se trata de un análisis donde se evalúa la condición física del sujeto, se definieron los siguientes parámetros de inclusión.

Sujetos mayores de 18 años, sin limitaciones en sus miembros inferiores.

En la figura 36, se presentan los pasos a seguir para la adquisición de los datos, donde se describen cada una de las acciones realizadas.

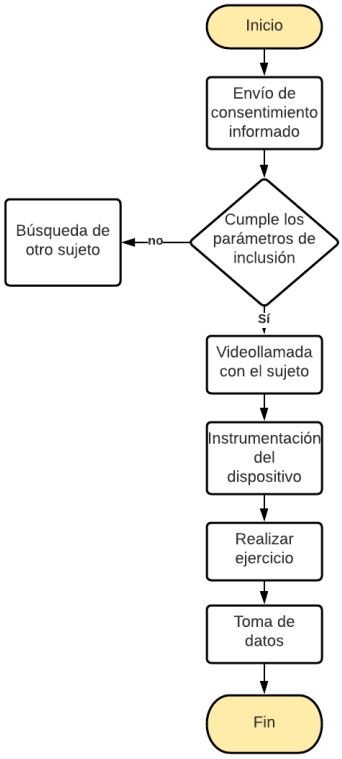


Figura 36: Diagrama para la obtención de los datos: Fuente: Propia.

- Envío de consentimiento informado: Se envió al sujeto un consentimiento informado, donde éste puede autorizarlo o no para continuar el procedimiento propuesto.
- El sujeto cumple los parámetros de inclusión: Una vez lo autorice, se verifica si cumple con los parámetros de inclusión; si no cumple se le comunica al sujeto su no participación en el proyecto. De forma contraria, si cumple con los parámetros de inclusión, el sujeto está listo para el proceso de obtención y verificación de los datos.
- Videollamada con el sujeto: El especialista médico por medio de una videollamada se comunica con el sujeto para explicarle sobre los pasos a seguir en la instrumentación del dispositivo y el ejercicio a realizar.
- Instrumentación del dispositivo y ejercicio a realizar:

- El sujeto debe estar en una parte donde pueda caminar durante un tiempo estimado de forma continua para no tener inconvenientes en el resultado final.
- Para la ubicación del dispositivo al interior del tobillo, se tiene en cuenta el plano sagital y que el celular esté de forma vertical (eje Y) sin presentar ninguna inclinación ni a la derecha ni a la izquierda, tal y como se observa en la figura 37.

Figura 37: Dispositivo ubicado en el tobillo. Fuente: Propia.

- Se abre la aplicación y se espera durante 30 segundos para iniciar el cálculo de la cadencia.
- Al pasar el tiempo estimado, se cierra la aplicación y se repite el proceso cada vez que se vayan a tomar los datos.

La prueba consiste en ejecutar la actividad de la marcha normal durante 7 días con una duración de 10 minutos. Esto se debe a que las pruebas del análisis de la marcha según lo reportado en la literatura son de aproximadamente 2 minutos o más, con esto se quiere evidenciar si el sujeto a medida que pasa el tiempo su marcha va disminuyendo. Adicionalmente a esto, se hizo durante 7 días para verificar que la información obtenida se mantenga en un rango no variable. Para la realización de la prueba se tiene que estar en un espacio el cual este plano y sin ningún obstáculo que afecte el cálculo de los pasos. Además de esto, el dispositivo de adquisición de datos debe tener una buena cobertura a Internet. Si se ejecuta por medio de los datos celulares, se recomienda tener una conexión

de datos en la red 3G o 4G. En el caso de realizarse con conexión a WiFi no estar tan alejado del router o del dispositivo master. Esto con el fin de no tener problemas al momento de subir los datos a la nube.

Al estar los datos en la nube, el especialista médico mediante la herramienta Matlab Visualization y utilizando el diagrama de cajas y bigotes; ver anexo E, se puede hacer un análisis más preciso de la prueba y comunicarle al sujeto cuál es la condición física. Los datos obtenidos en ThingSpeak y el diagrama de cajas y bigotes son mostrados en la figura 38 y 39 respectivamente.

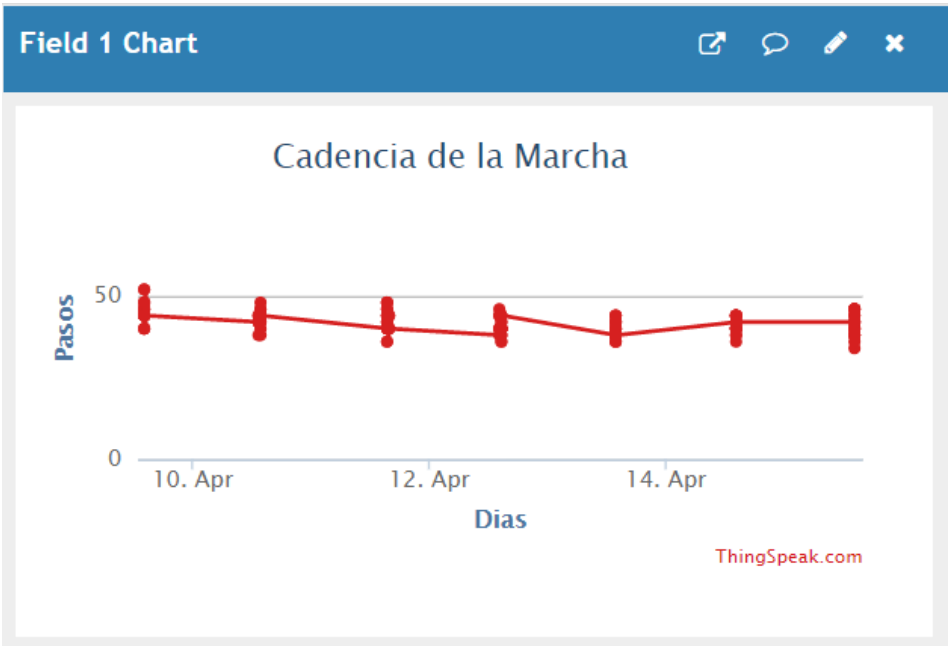


Figura 38: Datos obtenidos en la nube ThingSpeak en una sesión de 10 minutos durante 7 días correspondiente a marcha normal donde cada pico de la señal obtenida corresponde a 2 pasos. Fuente: Propia.

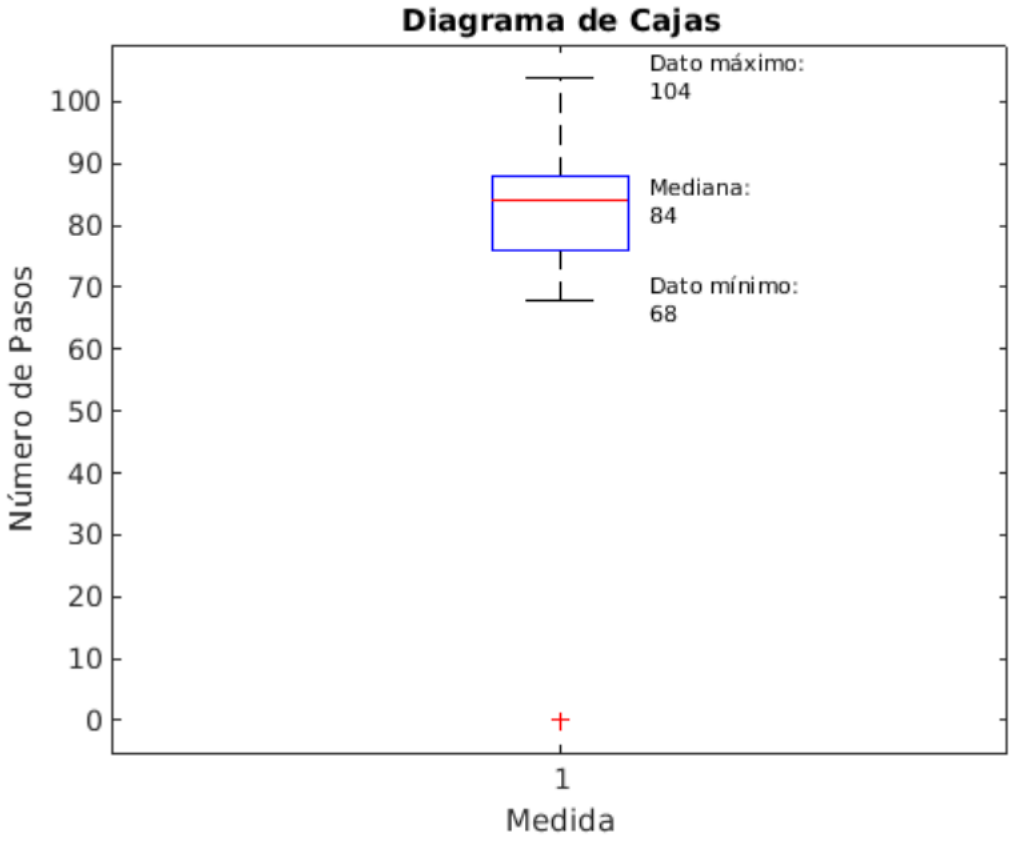


Figura 39: Análisis de Matlab Visualization mediante el diagrama de cajas y bigotes.
Fuente: Propia.

De acuerdo a los datos obtenidos en la nube y al hacer un análisis por medio del diagrama de cajas como se observa en la figura 39, el sujeto tuvo una mediana de 84 pasos. Además, el sujeto realizó 68 pasos que corresponde al menor número de pasos y 104 pasos que corresponde al mayor número de pasos en la sesión ejecutada.

Una vez los datos ya están tabulados y se pueda estimar los pasos del sujeto de manera correcta, se envía el ID del canal y la Write API Key mediante chat secreto en Telegram y se procede a realizar la visualización de la información mediante la aplicación ThingView. El chat secreto de la aplicación de Telegram no permite tomar pantallazos, reenviar mensajes ni grabar la pantalla del dispositivo móvil. Además de esto, se puede configurar una autodestrucción de los mensajes. Ver anexo F. Sin embargo, para mostrar el proceso

que se realizó se tomó una fotografía a un dispositivo externo donde se le envía al sujeto el ID del canal y la Write API Key como se observa en la figura 40.

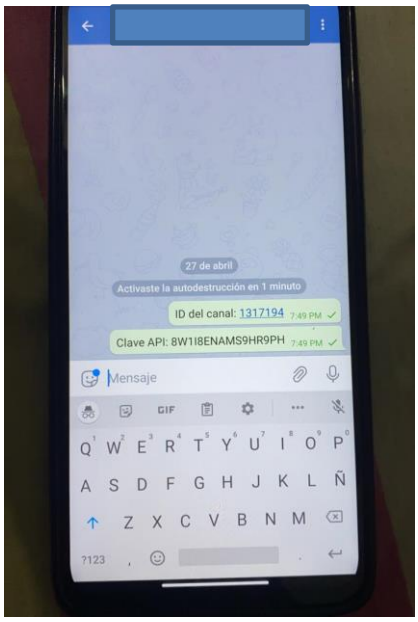


Figura 40: Fotografía tomada de un dispositivo externo al chat secreto de Telegram. Fuente: Propia.

Finalmente, el sujeto al tener los datos de los campos requeridos en el chat secreto de Telegram, procede a colocarlos en la aplicación ThingView y posteriormente a esto, visualizarlos como se muestra en la figura 41.

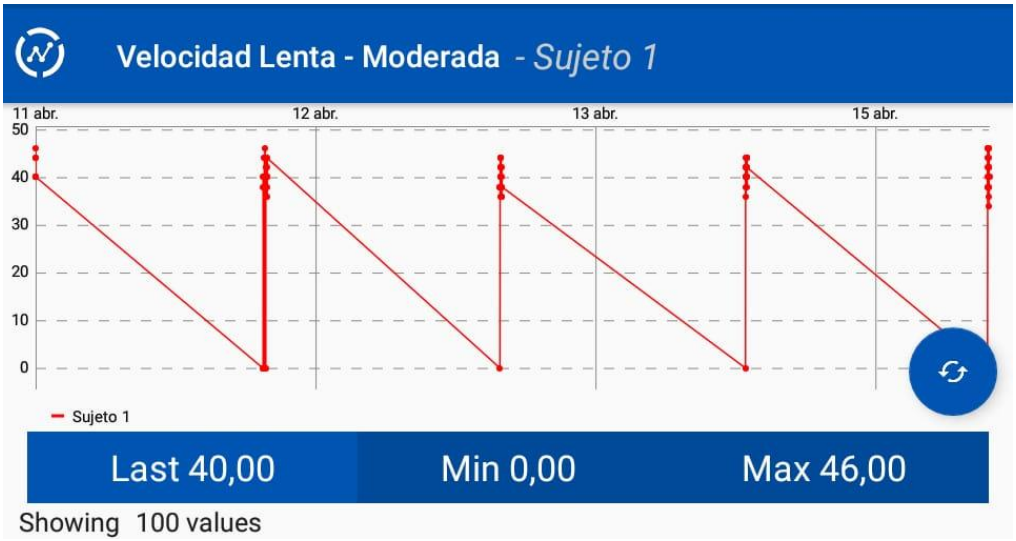


Figura 41: Visualización de los datos en la Aplicación ThingView Free. Fuente: Propia.

En la figura 41, se puede evidenciar que la aplicación solo muestra los 100 últimos valores subidos a la nube. Por lo tanto, cada vez que termine la rutina le informa al especialista médico para el envío de los datos requeridos, entra a la aplicación y verifica la información.

Al evidenciar que los datos son adquiridos, procesados, enviados, almacenados y visualizados en el servidor en la nube, se comprueba la funcionalidad del sistema IoT implementado. Además de esto, se demuestra que el sistema es seguro. Puesto que se verifica y se cumple de manera correcta los cuatro aspectos de la resolución 2654 de 2019 que son la fiabilidad, disponibilidad, integridad y autenticidad. A continuación, se muestra el diagrama de verificación de los 4 aspectos mencionados y se describe como se cumplen estos aspectos.

Figura 42: Aspectos de la seguridad de la información. Fuente: [67].

- La autenticidad se cumple verificando el acceso privado a través de API Key.
- La integridad se cumple mediante el protocolo de seguridad HTTPS para el envío de información a la nube y el cifrando end to end para el envío de los datos necesarios para la visualización mediante la aplicación ThingView.
- La disponibilidad y confidencialidad se cumple puesto que solamente el usuario autorizado (El especialista) puede acceder a la información y adicionalmente está información se encuentra disponible en un servidor de la nube (De forma protegida).
- La fiabilidad se cumple ya que la información obtenida en la nube es la correcta de acuerdo a las pruebas de verificación realizadas anteriormente.

3.5 Potenciales aplicaciones del sistema implementado

El sistema IoT implementado abarca desde el registro de la información mediante el sensor acelerómetro de un dispositivo móvil hasta la visualización y análisis de los datos obtenidos en la nube. Este sistema puede ser utilizado para la telemonitorización en tiempo real de variables cinemáticas como la velocidad de la marcha, la velocidad de la zancada, incluso la cadencia de la marcha que fue la elegida para esta investigación, puesto que con la información que se obtiene mediante el acelerómetro y haciendo un procesamiento de la señal, se pueden obtener los valores precisos para ser subidos a la nube de manera correcta. Esto se comprobó haciendo el análisis con la información almacenada en la nube y la información real mediante el software Kinovea en una ventana de 30 segundos, en la cual si existen alteraciones de la velocidad de la marcha se podrán detectar durante el registro de datos. Solo basta con instalar la aplicación en el dispositivo móvil y empezar a realizar el ejercicio correspondiente al análisis.

De otro lado, el sistema implementado es una herramienta para ser utilizada como plataforma a nivel de laboratorio para evaluar:

- Nuevos métodos para registrar y cuantificar variables espacio-temporales de la marcha.
- Aplicaciones para proporcionar realimentación al usuario, con enfoque a entrenadores virtuales.
- Aplicaciones relacionadas al reconocimiento de actividades físicas.
- Registro de software.

4. Conclusiones, recomendaciones y trabajos futuros

4.1 Conclusiones

Se implementó un sistema IoT seguro de la telemonitorización de la cadencia de la marcha de acuerdo a los parámetros establecidos en la resolución 2654 de 2019. El cual incorpora un método de seguridad de datos protegiendo la información y la integridad del sujeto.

A partir de las diferentes pruebas y evaluaciones, la ubicación correcta del dispositivo y el eje utilizado no se realizó a prueba y error, ni de manera visual con las señales obtenidas; sino que se evaluó diferentes situaciones con el fin de que el valor estimado por el algoritmo tenga un mínimo error.

Se evaluó el funcionamiento del sistema bajo condiciones controladas, donde se validó que los datos se suben de manera correcta a la nube y por medio de la herramienta de análisis de video Kinovea y la información obtenida en la nube se cuantificó el porcentaje de error en el registro y cálculo de la variable cadencia, obteniendo un 5%.

Se implementó un protocolo de medidas para la telemonitorización en los sujetos sanos, de acuerdo al cumplimiento de la normatividad. Además, se comprobó la información correcta de telemonitoreo en la cadencia de la marcha del sujeto con una mediana de 84 pasos por minuto en una rutina terapéutica de 10 minutos.

4.2 Productos Generados

Se verificó el potencial de la aplicación basada en una App para Android con el propósito de evaluar diferentes métodos para implementar sistemas de tele-rehabilitación física, al ser una plataforma abierta basada en Matlab y ThingSpeak. Por lo tanto, se está tramitando un registro de software ante la oficina de transferencia y tecnología (OTT) de la Universidad Antonio Nariño.

4.3 Recomendaciones y Limitaciones

Es importante considerar el correcto funcionamiento de la aplicación y la información adecuada subida a la nube. Para ello, se debe tener en cuenta que el dispositivo móvil donde se realiza la adquisición de los datos tenga una memoria RAM mayor a 1.5 GB y además tenga una buena conexión a internet.

Por otro lado, se debe tener contemplar la ubicación correcta del dispositivo. Puesto que al ubicarlo en un lugar incorrecto o colocarlo en una orientación que no es la adecuada los datos que se obtienen no van a ser los ideales.

Entre las limitaciones encontradas en el sistema IoT implementado se encuentran en la aplicación realizada en Simulink, puesto que esta solo puede ser instalada en el dispositivo que se sincronice con el computador y además no puede ser compartida ni por ningún medio de transmisión como bluetooth o NFC, ni por aplicaciones de mensajería instantánea. Además de esto, se evidencia otra limitación en la plataforma ThingSpeak ya que permite subir datos cada 30 segundos.

Otra limitación encontrada es en relación a la aplicación ThingView, la cual solo muestra las 100 últimas entradas que se suben a la nube en el caso de que sea un canal privado y las 60 últimas entradas si es un canal público.

4.4 Trabajos Futuros

- Realizar pruebas de evaluación de la usabilidad, según la norma ISO 9241-11, para cuantificar la efectividad, eficacia y satisfacción del usuario en la interacción con la App.
- Realizar pruebas de repetibilidad para obtener un registro de información de la App más confiable.
- Realizar pruebas piloto con un grupo significativo de usuarios, para evaluar el desempeño bajo un protocolo de medidas común.
- Calcular otros parámetros espacio-temporales de la marcha, para ser usados en actividades de tele-monitorización física.
- Incorporar información de realimentación al usuario respecto a la ejecución de la actividad física.

5. Anexos

5.1 Anexo A: Configuración Simulink Support Package for Android Devices.

1. Instalación y configuración de la herramienta Simulink Support Package for Android Devices.

   1.1 Desde Matlab y estando en la pestaña de HOME → Enviroment → Add-Ons → Simulink Support Package for Android Device, se puede instalar fácilmente esta herramienta.

   1.2 Una vez se instala la herramienta se dispone a realizar la configuración para poderla conectar con el dispositivo Android como se observa en la figura 1.

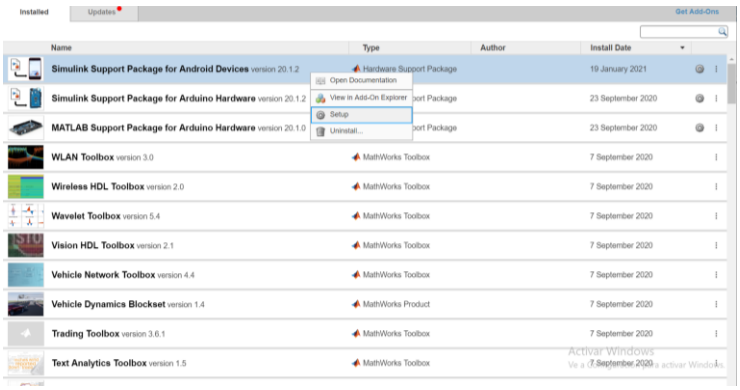


Figura 1: Interfaz principal herramientas de Matlab. Fuente: Propia.

   1.3 En la configuración, se pide descargar una aplicación desde cualquier navegador web llamada Android Studio para poder continuar como se evidencia en la figura 2. Se recomienda descargar una versión no tan actualizada. Posteriormente a esto, se pide instalar Android SDK Platform

Packages and Tools para continuar la instalación tal y como se observa en la figura 3.

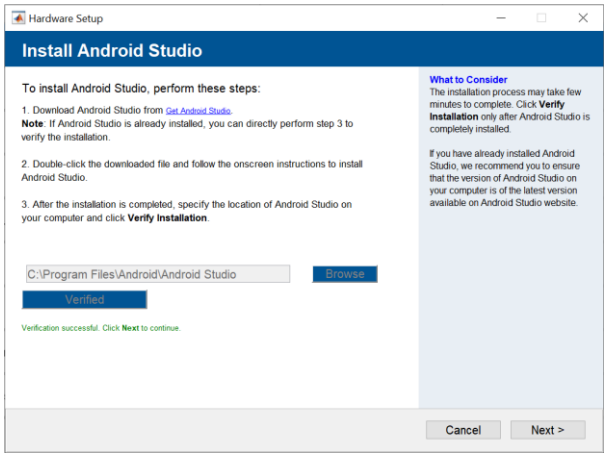


Figura 2: Verificación de la instalación de Android Studio. Fuente: Propia.

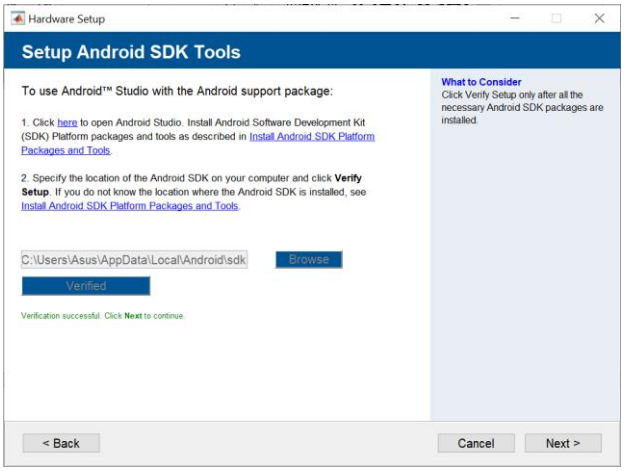


Figura 3: Verificación de la instalación de Android SDK Tools. Fuente: Propia.

1.4 Una vez se haya completado el paso anterior, se procede a configurar el dispositivo móvil que se vaya a emparejar. Para esto, utilizamos la siguiente secuencia: ajustes → acerca del teléfono. En esa pestaña buscamos el número de compilación y presionamos siete veces hasta que aparezca un mensaje “El modo desarrollador ha sido activado”.

1.5 Al tener el modo desarrollador activado, se sigue la siguiente secuencia: ajustes → modo desarrollador → depuración USB. Se activa depuración USB, como se observa en la figura 4.

Figura 4: Activación modo depuración USB en el dispositivo móvil. Fuente: Propia.

1.6 Ahora viene algo fundamental para que el dispositivo se pueda configurar correctamente. Si se tiene un dispositivo móvil de marca Samsung, tal como es el del proyecto; Esta herramienta tiene por defecto este driver y lo único que se hace es presionar en instalar driver y así se puede continuar con la configuración como se observa en la figura 5. En el caso de no contar con un dispositivo de marca Samsung, se selecciona dispositivo diferente y en ese caso aparecerá un link que los redirecciona a los drivers de algunos dispositivos.

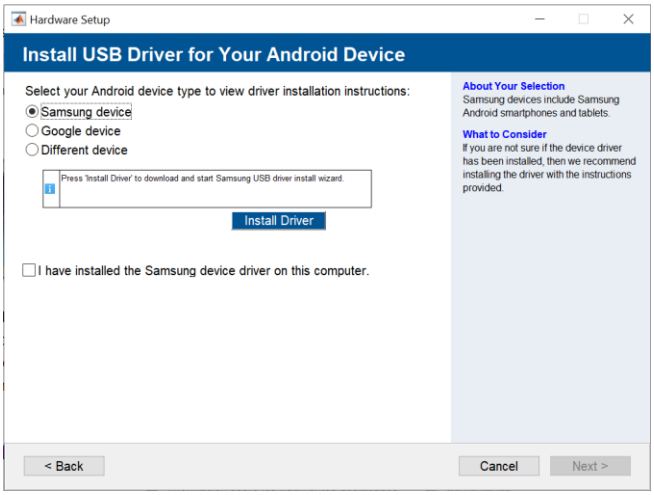


Figura 5: Seleccionar el driver del dispositivo utilizado. Fuente: Propia.

1.7 Al ya tener el driver instalado, se conecta el dispositivo móvil mediante un cable USB al computador, donde aparecerá un mensaje de “Permitir la depuración de USB”; le damos Aceptar. Esto se evidencia en la figura 6.

Figura 6: Permitir depuración USB desde el dispositivo móvil. Fuente: Propia.

1.8 En pantalla aparece el dispositivo que se tiene conectado mediante USB como se evidencia en la figura 7. Se selecciona siguiente.

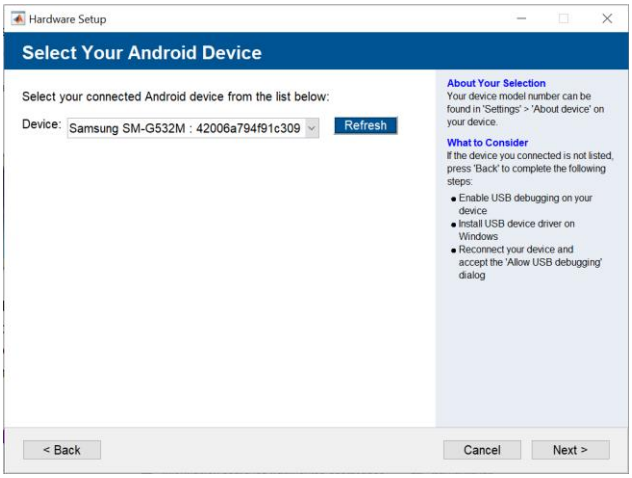


Figura 7: Seleccionar el dispositivo que se va a sincronizar. Fuente: Propia.

1.9 Ahora sí llega la parte final, donde se verifican todas las condiciones y la correcta configuración de la herramienta con el dispositivo móvil como se observa en la figura 8.

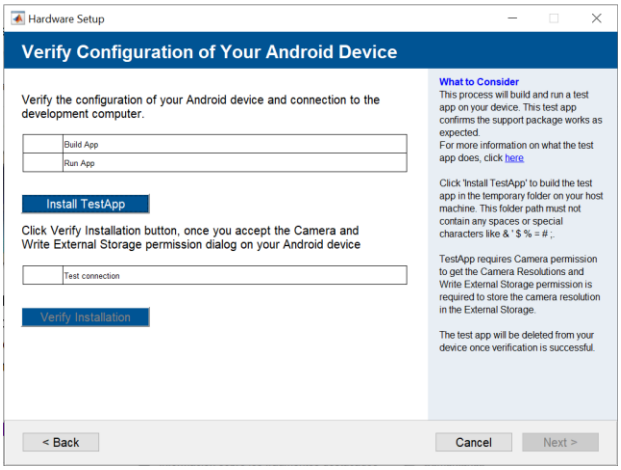


Figura 8: Verificación final de la configuración del dispositivo Android. Fuente: Propia.

2. Al ya tener configurada la herramienta Simulink Support Package for Android Devices y emparejada con el dispositivo móvil que se va a utilizar, se procede a realizar la programación. Para esto, se abre Simulink y se siguen los siguientes pasos.

2.1 Se selecciona la pestaña Modeling y en la ventana de setup, se presiona model setting.

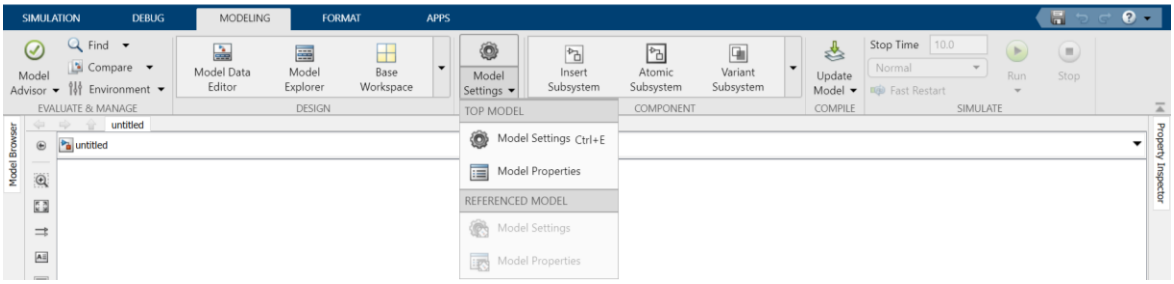


Figura 9: Pestaña Modeling Simulink. Fuente: Propia.

2.2 Aparecerá otra ventana donde se debe seleccionar “hardware implementation” y en hardware board se escoge Android Device y se le da

Ok. Esto con el objetivo de que Simulink se sincronice con el dispositivo Android.

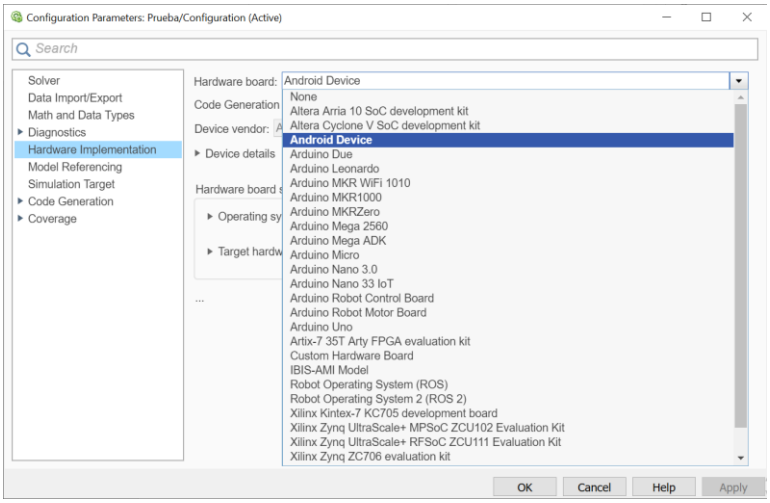


Figura 10: Configuración de parámetros del hardware. Fuente: Propia.

2.3 Se hizo una configuración exitosa y se procede a realizar la programación requerida.

3. Completando el paso 1 y 2, aparece en Simulink una pestaña llamada hardware donde se escoge el dispositivo y con el botón de Build, Deploy & Start se instala la aplicación que se programe.

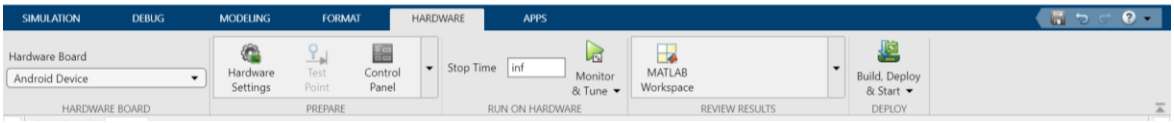
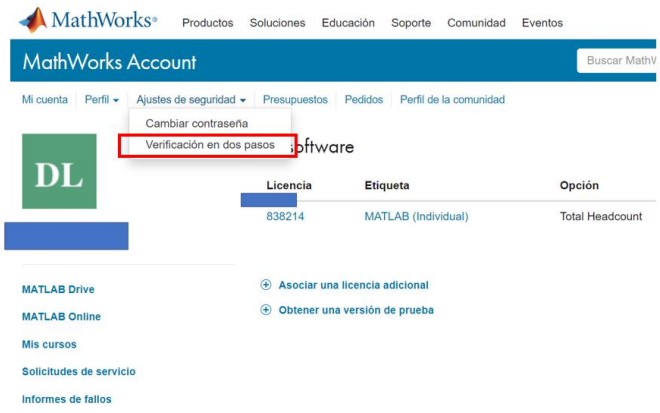


Figura 11: Pestaña Hardware Simulink. Fuente: Propia.

5.2 Anexo B: Verificación dos pasos MathWorks

Ingresar a MathWorks y seleccionar en la pestaña ajuste de seguridad la opción de verificación en dos pasos.



Aparece una segunda pestaña, en la cual se presiona el botón de activar para poder seguir con la configuración.

Aparece una tercera pestaña, donde se debe seleccionar el método para recibir códigos de verificación. Se puede seleccionar por medio de App autenticadora, mensaje de texto o por medio de correo electrónico.

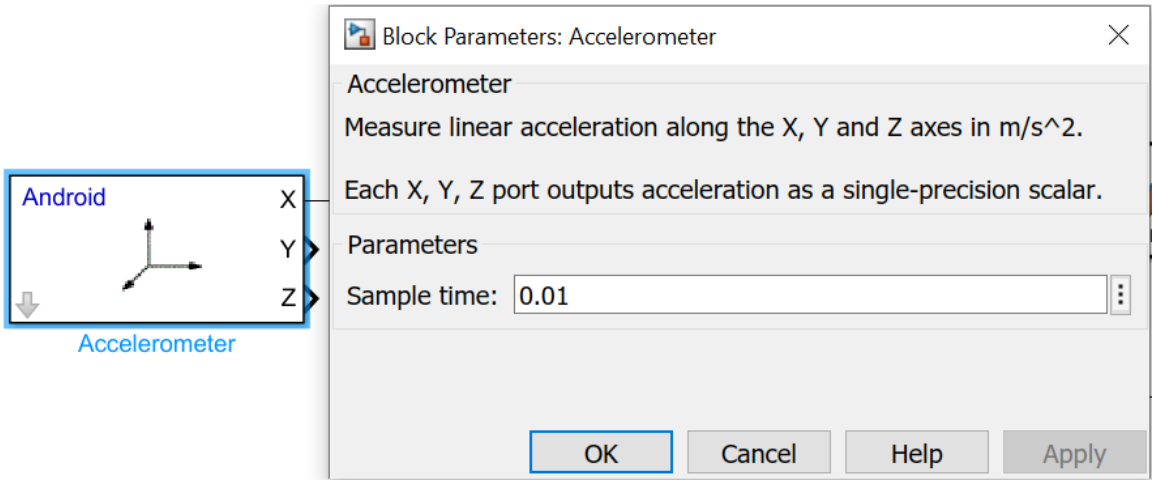
Aparece una cuarta pestaña, en la cual el método seleccionado para recibir los códigos de verificación es App autenticadora. Puesto que es una aplicación que aparece un código de seguridad y se va actualizando cada 30 segundos garantizando seguridad en la información de los datos. En este método se tiene que instalar una aplicación llamada Autenticador de Google y una vez instalada, se procede a escanear el código QR y a colocar el código de verificación que aparece en pantalla del dispositivo móvil.

Al presionar verificar y que el código de verificación sea el correcto, aparece una quinta pestaña informando que la verificación dos pasos ha sido activada correctamente.

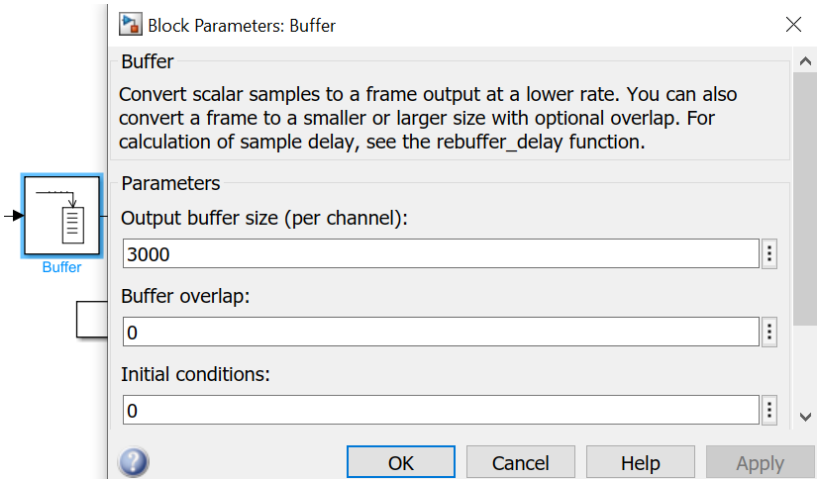
Finalmente, se vuelve a iniciar sesión y al colocar el correo electrónico y la contraseña aparece una sexta pestaña donde pregunta el código de verificación. Para esto, se abre la aplicación instalada en el dispositivo móvil y se coloca el código que aparece en pantalla. Posteriormente a esto, presionamos verificar y ya se ingresa nuevamente a la cuenta MathWorks y a todos sus servicios.

5.3 Anexo C: Bloques Aplicación en Simulink.

- Bloque Acelerómetro.



- Bloque Buffer.

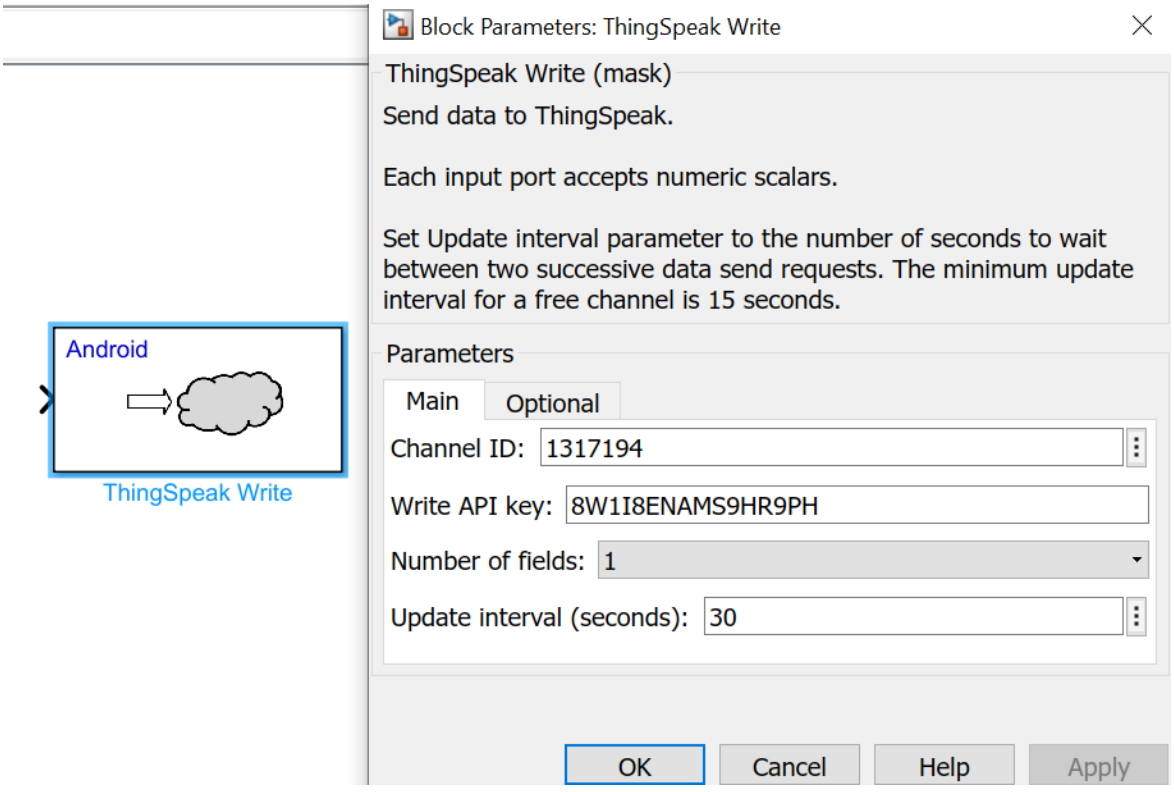


- Bloque Matlab Function

MATLAB Function*

```
function y = fcn(u)
umb = [25 -25]; %Se escogen umbrales de acuerdo
                %a la gráfica obtenida por el acelerometro
u(and(u<umb(1),u>umb(2)))=0; % Se hace la condición para poner
                             % los valores en 0.
a = findpeaks(u); % Se detectan los picos de la señal
y = 2*length(a); % Se cuentan los picos detectados y se
                 % multiplican por 2.
end
```

- Bloque ThingSpeak Write



5.4 Anexo E: Consentimiento Informado

DOCUMENTO DE CONSENTIMIENTO INFORMADO

Nombre del Investigador: David Alexander López Díaz

Objetivo
Documento de Consentimiento Informado para el registro de datos cinemáticos de la marcha para poder ser subidos, visualizados y analizados en la nube ThingSpeak. Este formulario de consentimiento informado se dirige a personas que estudian y/o trabajan en la Universidad Antonio Nariño y que se les invita a participar en la investigación que se lleva a cabo en la facultad de Ingeniería Biomédica, Electrónica y Mecatrónica de la UAN.

Tipo de Intervención de Investigación:
Esta investigación abarca una sesión durante siete días, donde se instrumenta un dispositivo móvil al interior del tobillo y realiza una marcha normal.

Selección de participantes:
Estudiantes, docentes y administrativos de la UAN que participen de forma voluntaria en la toma de datos. Estos datos se tomarán a personas sanas que no presenten ninguna patología en los miembros inferiores.

Participación Voluntaria:
Su participación en esta investigación es totalmente voluntaria. Usted puede elegir participar o no hacerlo. Usted puede cambiar de idea más tarde y dejar de participar aun cuando haya aceptado antes. No se proporcionará remuneración económica.

Procedimientos y Protocolo:
Se instalan tres aplicaciones en el dispositivo móvil del sujeto (Aplicación de Simulink, ThingView y Telegram) que no contienen virus y no afectan el funcionamiento del dispositivo. Posteriormente a esto, se realiza una videollamada con el sujeto. En la cual

se le explica dónde debe colocar el dispositivo móvil y en qué orientación. Además de esto, se le indica el ejercicio a realizar.

Duración:
Como se maneja de manera remota, la duración de la videollamada tardaría entre 5 a 10 minutos y de ahí la prueba que se realiza es de 10 minutos. En total la prueba tiene una duración de 20 minutos aproximadamente.

La toma de datos no trae implícitos efectos secundarios, ni riesgo alguno para el participante.

Confidencialidad:
La información que recojamos por este proyecto de investigación se mantendrá confidencial. La información acerca de usted que se recogerá durante la investigación será puesta fuera de alcance y nadie sino los investigadores tendrán acceso a verla. Cualquier información acerca de usted tendrá un número en vez de su nombre. Solo los investigadores sabrán cuál es su número.

A Quién Contactar:
Si tiene cualquier pregunta puede hacerlas ahora o más tarde, incluso después de haberse iniciado la toma de datos. Si desea hacer preguntas más tarde, puede contactar a David Alexander López.

FORMULARIO DE CONSENTIMIENTO

He sido invitado a participar en la toma de variables cinemáticas de la marcha para ser monitorizadas a través de la nube ThingSpeak. Entiendo que van a instalar aplicaciones en mi dispositivo móvil que no tiene ningún virus y que me voy a comunicar mediante videollamada con una persona encargada que me indicará el proceso que debo seguir. He sido informado de que los riesgos son mínimos. Sé que puede que no haya beneficios para mi persona y que no se me recompensará con dinero. Se me ha proporcionado el nombre de un investigador que puede ser fácilmente contactado usando el nombre y la dirección de correo electrónico que me fue entregada.

He leído la información proporcionada o me ha sido leída. He tenido la oportunidad de preguntar sobre ella y se me ha contestado satisfactoriamente las preguntas que he realizado. Consiento voluntariamente participar en esta investigación como participante y entiendo que tengo el derecho de retirarme de la investigación en cualquier momento sin que me afecte de ninguna manera.

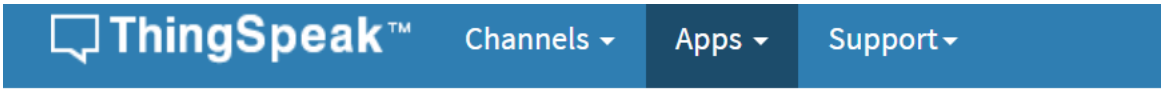
Nombre del Participante_____

Firma del Participante _____
Fecha _____

Nombre del Investigador_____

Firma del Investigador _____
Fecha _____

5.5 Anexo E: Código de diagrama de cajas en Matlab Visualization



Apps / MATLAB Visualizations / Diagrama de Cajas / Edit

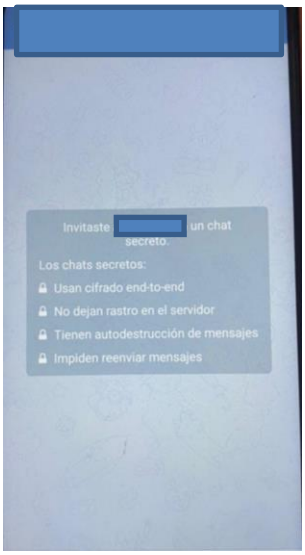
Name

Diagrama de Cajas

MATLAB Code

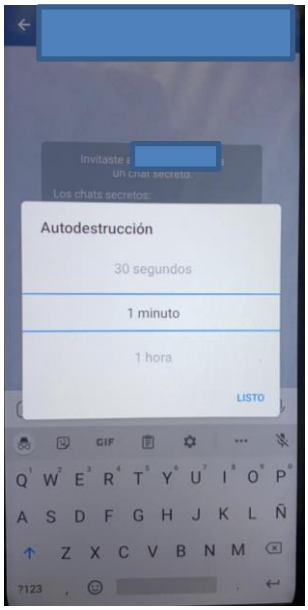
```
readChannelID = 1317194; % Canal de lectura
CadenciaFieldID = 1;  %Campo de lectura de los datos
readAPIKey = '0HMFHPRCAQ14TWJR'; % API Key de lectura
Cadencia = thingSpeakRead(readChannelID,'Fields',CadenciaFieldID,...
'NumPoints', 158,  'ReadKey',readAPIKey);
boxplot(Cadencia*2);
xlabel('Medida');
ylabel('Número de Pasos');
title('Diagrama de Cajas');
Mediana = median(Cadencia)*2;
txt = {'Mediana: ', Mediana};
text(1.1,(Mediana),txt,'FontSize',8)
D_Mayor = max(Cadencia)*2;
txt = {'Dato máximo: ',D_Mayor};
text(1.1,(D_Mayor),txt,'FontSize',8)
D_Minimo = min (Cadencia (Cadencia> 0))*2
txt = {'Dato mínimo: ',D_Minimo};
text(1.1,(D_Minimo),txt,'FontSize',8)
```

5.6 Anexo F: Chat secreto Telegram



Interfaz principal chat secreto Telegram

Captura de pantalla al chat secreto de Telegram



Configuración autodestrucción de mensajes

6. Bibliografía

[1] F. Hu, D. Xie, and S. Shen, “On the application of the internet of things in the field of medical and health care,” *Proc. - 2013 IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCom 2013*, pp. 2053–2058, 2013, doi: 10.1109/GreenCom-iThings-CPSCom.2013.384.

[2] P. Carlos Humberto, “Seguridad informática y seguridad de la información en el mundo , como factor de enseñanza en Colombia,” p. 7, 2018, [Online]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2856/Trabajo de grado.pdf?sequence=1&isAllowed=y.

[3] Ministerio de Salud y Protección Social, “Resolución No. 2654 del 2019.” p. 10, 2019, [Online]. Available: https://www.minsalud.gov.co/Normatividad_Nuevo/Resolución No. 2654 del 2019.pdf.

[4] N. Remolina-Angarita, “Does Colombia Have an Adequate Level of Personal Data Protection in Light of the European Standards?,” *Int. Law*, no. 16, pp. 489–523, 2010.

[5] S. Vishnu, S. R. Jino Ramson, and R. Jegan, “Internet of Medical Things (IoMT)-An overview,” *ICDCS 2020 - 2020 5th Int. Conf. Devices, Circuits Syst.*, pp. 101–104, 2020, doi: 10.1109/ICDCS48716.2020.243558.

[6] H. Hamidi, “An approach to develop the smart health using Internet of Things and authentication based on biometric technology,” *Futur. Gener. Comput. Syst.*, vol. 91, pp. 434–449, 2019, doi: 10.1016/j.future.2018.09.024.

[7] K. Kapusta, G. Memmi, and H. Noura, “Secure and Resilient Scheme for Data Protection in Unattended Wireless Sensor Networks,” vol. 1570391545, pp. 1–8.

[8] J. Liu, Y. Zhang, Z. Zhou, and H. Tang, *A New Lightweight Database Encryption and Security Scheme for Internet-of-Things*, vol. 2. Springer Singapore, 2020.

[9] S. Sawardekar and R. Pawar, “Data Security Approach in IoT Environment,” *2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019*, 2019, doi: 10.1109/ICCCNT45670.2019.8944831.

[10] H. Garg and M. Dave, “Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware,” *Proc. - 2019 4th Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2019*, pp. 0–5, 2019, doi: 10.1109/IoT-SIU.2019.8777334.

[11] I. Aciobanitei, I. C. Buhus, and M. L. Pura, “Using cryptography in the cloud for lightweight authentication protocols based on QR Codes,” *SACI 2018 - IEEE 12th Int. Symp. Appl. Comput. Intell. Informatics, Proc.*, pp. 539–542, 2018, doi: 10.1109/SACI.2018.8440949.

[12] A. K. M. J. A. Majumder, P. Saxena, and S. I. Ahamed, “Your Walk is My Command: Gait Detection on Unconstrained Smartphone Using IoT System,” *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 1, pp. 798–806, 2016, doi: 10.1109/COMPSAC.2016.221.

[13] M. Ghazal, M. Alhalabi, L. Fraiwan, M. Yaghi, and L. Alkhatib, “Assessment of motion quality using an iot-based wearable and mobile joint flexion sensors,” *Proc. - 2019 Int. Conf. Futur. Internet Things Cloud Work. FiCloudW 2019*, pp. 44–48, 2019, doi: 10.1109/FiCloudW.2019.00021.

[14] C. R. Ib, N. Z. D. E. Cadena, and T. Zea, “TELEMEDICINA: Introducción, aplicación y principios de desarrollo,” pp. 77–93, 2007.

[15] A. L. Lorena, “Seguridad informática y seguridad de la información,” p. 7, 2015.

[16] M. Caporuscio, D. Weyns, J. Andersson, C. Axelsson, and G. Petersson, “IoT-enabled physical telerehabilitation platform,” *Proc. - 2017 IEEE Int. Conf. Softw. Archit. Work. ICSAW 2017 Side Track Proc.*, pp. 112–119, 2017, doi: 10.1109/ICSAW.2017.43.

[17] A. A. Orlov, K. V. Makarov, and E. S. Tarantova, “Features selection for human activity recognition in telerehabilitation,” *2019 Int. Sci. Technol. Conf. “EastConf”, EastConf 2019*, 2019, doi: 10.1109/Eastonf.2019.8725408.

[18] C. Sanz, “Cinesiologia de la marcha humana normal,” *Univ. Zaragoza*, pp. 1–14, 2011.

[19] J. C. Arellano-González, H. I. Medellín-Castillo, and J. J. Cervantes-Sánchez, “Identificación y análisis de los parámetros biomecánicos utilizados para la evaluación de la marcha humana normal y patológica,” *Memorias del XXV Congr. Int. Anu. la SOMIM*, pp. 1–9, 2019, [Online]. Available: http://somim.org.mx/memorias/memorias2019/mecteo.html.

[20] L. J. Vargas Escobar, “Sistema para la Medición de Parámetros de Tiempo de la Marcha Humana,” no. February 2020, pp. 1–123, 2017.

[21] J. Cámara Tobalina, “Gait analysis: phases and spatio-temporal variables,” *Entramado*, vol. 7, no. 1, pp. 160–173, 2011, [Online]. Available:

http://dialnet.unirioja.es/servlet/articulo?codigo=3819708&info=resumen&idioma=ENG.

[22] “OMS | Actividad física,” *World Health Organization*. 2000, [Online]. Available: http://www.who.int/dietphysicalactivity/pa/es/.

[23] S. Singh and N. Singh, “Business Opportunities & Reference Architecture for E-commerce,” *Ieee*, pp. 1577–1581, 2015.

[24] “Internet of Things - Definitionen und Anwendungen _ FOSTEC & Company.” [Online]. Available: https://www.fostec.com/es/competencias/estrategia-de-digitalizacion/internet-of-things-iot/.

[25] H. Yi and Z. Nie, “On the security of MQ cryptographic systems for constructing secure Internet of medical things,” *Pers. Ubiquitous Comput.*, vol. 22, no. 5–6, pp. 1075–1081, 2018, doi: 10.1007/s00779-018-1149-y.

[26] M. Cascajo Sastre, “¿Qué es Internet de las Cosas Médicas y qué beneficios tiene?” 2020, [Online]. Available: https://empresas.blogthinkbig.com/que-es-internet-de-las-cosas-medicas-y-que-beneficios-tiene/.

[27] J. R. K. K. Dabbakuti and B. Ch, “Ionospheric monitoring system based on the Internet of Things with ThingSpeak,” *Astrophys. Space Sci.*, vol. 364, no. 8, pp. 1–7, 2019, doi: 10.1007/s10509-019-3630-0.

[28] MathWorks, “IoT Analytics - ThingSpeak Internet of Things.” 2019, [Online]. Available: https://thingspeak.com/.

[29] “ThingView - ThingSpeak viewer - Apps on Google Play.” [Online]. Available: https://play.google.com/store/apps/details?id=com.cinetica_tech.thingview&hl=en.

[30] L. T. De Paolis, V. De Luca, and R. Paiano, “Sensor data collection and analytics with thingsboard and spark streaming,” *EESMS 2018 - Environ. Energy, Struct. Monit. Syst. Proc.*, pp. 1–6, 2018, doi: 10.1109/EESMS.2018.8405822.

[31] M. Henschke, X. Wei, and X. Zhang, “Data Visualization for Wireless Sensor Networks Using ThingsBoard,” *2020 29th Wirel. Opt. Commun. Conf. WOCC 2020*, pp. 2–7, 2020, doi: 10.1109/WOCC48579.2020.9114929.

[32] A. Mijuskovic, I. Ullah, R. Bemthuis, N. Meratnia, and P. Havinga, “Comparing Apples and Oranges in IoT Context: A Deep Dive into Methods for Comparing IoT Platforms,” *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1797–1816, 2021, doi: 10.1109/JIOT.2020.3016921.

[33] K. J. Madukwe, I. J. F. Ezika, and O. N. Iloanusi, “Leveraging Edge Analysis for

Internet of Things Based Healthcare Solutions," pp. 720–725, 2017.

[34] I. Buitrón-Dámaso and G. Morales-Luna, "HTTPS connections over Android," *CCE 2011 - 2011 8th Int. Conf. Electr. Eng. Comput. Sci. Autom. Control. Progr. Abstr. B.*, pp. 1–4, 2011, doi: 10.1109/ICEEE.2011.6106698.

[35] "Proteger sitios web con el protocolo HTTPS." [Online]. Available: https://developers.google.com/search/docs/advanced/security/https?hl=es.

[36] D. Eridani, K. T. Martono, and A. A. Hanifah, "MQTT performance as a message protocol in an IoT based chili crops greenhouse prototyping," *2019 4th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2019*, vol. 6, pp. 184–189, 2019, doi: 10.1109/ICITISEE48480.2019.9003975.

[37] A. Oak and R. D. Daruwala, "Assessment of Message Queue Telemetry and Transport (MQTT) protocol with Symmetric Encryption," *ICSCCC 2018 - 1st Int. Conf. Secur. Cyber Comput. Commun.*, pp. 5–8, 2018, doi: 10.1109/ICSCCC.2018.8703314.

[38] D. Eridani and E. D. Widianto, "Performance of sensors monitoring system using raspberry Pi through MQTT protocol," *2018 Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2018*, pp. 587–590, 2018, doi: 10.1109/ISRITI.2018.8864473.

[39] O. Sadio, I. Ngom, and C. Lishou, "Lightweight Security Scheme for MQTT/MQTT-SN Protocol," *2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019*, pp. 119–123, 2019, doi: 10.1109/IOTSMS48152.2019.8939177.

[40] André Goujon, "¿Qué es una VPN y cómo funciona para la privacidad de la información? | WeLiveSecurity," *Conoce qué es una VPN, cómo funciona, los usos que se le dan y los protocolos de cifrado disponibles para proteger tu información.* 2012, [Online]. Available: https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/.

[41] D. Álvarez Delgado, C. Jorquera Cáceres, G. Sepúlveda Jorquera, and C. Zamora Esquivel, "Redes Privadas Virtuales (VPN)," p. 9, 2014, [Online]. Available: http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes Privadas Virtuales %28VPN%29.pdf.

[42] Z. Zhang, Y. Q. Zhang, X. Chu, and B. Li, "An overview of virtual private network (VPN): IP VPN and optical VPN," *Photonic Netw. Commun.*, vol. 7, no. 3, pp. 213–225, 2004, doi: 10.1023/B:PNET.0000026887.35638.ce.

[43] P. B. Gentry, "What is a VPN?," *Inf. Secur. Tech. Rep.*, vol. 6, no. 1, pp. 15–22, 2001,

doi: 10.1016/s1363-4127(01)00103-0.

[44] M. J. Eterovic and E. M. Cipriano, “Criptografía Liviana para aplicar en dispositivos IoT,” pp. 1008–1010, 2018, [Online]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/68316/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y.

[45] TheMathworks, “Simulink - Simulation and Model-Based Design - MATLAB & Simulink.” 2020, [Online]. Available: https://www.mathworks.com/products/simulink.html.

[46] “Simulink Support Package for Android Devices Documentation.” [Online]. Available: https://www.mathworks.com/help/supportpkg/android/index.html?s_tid=CRUX_lftnav.

[47] MathWorks, “Publish data to the Internet of Things using ThingSpeak - Simulink.” [Online]. Available: https://la.mathworks.com/help/supportpkg/android/ref/thingspeakwrite.html.

[48] “Read data stored in ThingSpeak channel - MATLAB thingSpeakRead.” 2017, [Online]. Available: https://www.mathworks.com/help/thingspeak/thingspeakread.html.

[49] J. Lluch Fruns, “Análisis de imágenes: aplicación de Kinovea en podología,” *El Peu - Rev. Podol.*, vol. 33, no. 2, pp. 30–33, 2012, [Online]. Available: http://www.kinovea.org.

[50] S. Pooli, “KINOVEA- Software para realizar video análisis - International Endurance Work Group.” 2018, [Online]. Available: https://g-se.com/kinovea-software-para-realizar-video-analisis-bp-q5a4e419037dfa.

[51] K. Paúl *et al.*, “Análisis biomecánico en la marcha deportiva entre deportistas de iniciación y alto rendimiento,” *Rev. Cuba. Investig. Biomédicas*, vol. 37, no. 2, pp. 9–17, 2018.

[52] SIC, “Sobre la protección de datos personales | Superintendencia de Industria y Comercio,” *Superintendencia de Industria y comercio* . 2019, [Online]. Available: http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales.

[53] “Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012],” *Diario Oficial No. 48.587 de 18 de octubre de 2012*. 2012, [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

[54] P. Velásquez, “Parámetros Para La Telemedicina En Colombia – Resolución 2654 De 2019,” *Consultorsalud*. 2019, [Online]. Available: https://consultorsalud.com/parametros-para-la-telemedicina-en-colombia-resolucion-2654-de-2019/.

[55] J. C. Mateus *et al.*, “¿Responde la Resolución 8430 de 1993 a las necesidades actuales de la ética de la investigación en salud con seres humanos en Colombia?,” *Biomedica*, vol. 39, no. 3, pp. 448–463, 2019, doi: 10.7705/biomedica.4333.

[56] A. Dargahi Nobari, M. H. K. M. Sarraf, M. Neshati, and F. Erfanian Daneshvar, “Characteristics of viral messages on Telegram; The world’s largest hybrid public and private messenger,” *Expert Syst. Appl.*, vol. 168, no. October 2020, p. 114303, 2021, doi: 10.1016/j.eswa.2020.114303.

[57] Telegram, “Telegram Messenger,” *Https://Telegram.Org*. 2020.

[58] M. J. Aguilar Cordero, A. M. Sánchez López, R. Guisado Barrilao, R. Rodriguez Blanque, J. Noack Segovia, and M. D. Pozo Cano, “Descripción del acelerómetro como método para valorar la actividad física en los diferentes periodos de la vida; revisión sistemática,” *Nutr. Hosp.*, vol. 29, no. 6, pp. 1250–1261, 2014, doi: 10.3305/nh.2014.29.6.7410.

[59] E. Roldán, D. Rendón, and J. Escobar, “Alternativas para la medición del nivel de actividad física,” *EFDeportes.com, Revista Digital.*, no. August 2013. pp. 1–20, 2013, [Online]. Available: http://www.efdeportes.com/efd183/la-medicion-del-nivel-de-actividad-fisica.htm.

[60] J. M. Casanueva, “Seguridad y Privacidad en Internet,” vol. 1, p. 67, 2011.

[61] MathWorks, “Cuenta de MathWorks_ preguntas frecuentes sobre la verificación en dos pasos - MathWorks América Latina.” [Online]. Available: https://la.mathworks.com/mw_account/two_step_verification/frequently-asked-questions.html.

[62] S. Yañez, “Estudio Comparativo de Sistemas de Análisis de Marcha Basados en Sensores Inerciales y Cámaras Infrarrojas,” pp. 1–72, 2018, [Online]. Available: http://repositorio.udec.cl/bitstream/11594/359/1/Tesis_estudio_comparativo_de_sistemas.Image.Marked.pdf.

[63] D. Fernando and S. Lozano, “Sistema para el Análisis de la Marcha Humana Usando Sensores Inerciales,” pp. 1–17, 2019.

[64] W. Tao, T. Liu, R. Zheng, and H. Feng, “Gait analysis using wearable sensors,”

Sensors, vol. 12, no. 2, pp. 2255–2283, 2012, doi: 10.3390/s120202255.

[65] U. Tripathi, S. Sangani, L. L. Y. Liu, and A. Lamontagne, “Auditread: Towards a low-cost wireless auditory feedback and gait analysis system,” *2020 8th E-Health Bioeng. Conf. EHB 2020*, pp. 31–34, 2020, doi: 10.1109/EHB50910.2020.09280251.

[66] S. Monisa Alves Borges *et al.*, “Electromyographic Analysis of Muscle Activation of the Trunk and Lower Limbs During Human Gait and Hippotherapy Using Different Ride Mount Materials,” *J. Bodyw. Mov. Ther.*, 2021, doi: 10.1016/j.jbmt.2021.02.013.

[67] Ministerio de Salud y de la Proteccion Social, “Telesalud / Telemedicina y COVID-19,” 2020, [Online]. Available: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/OT/nuevo-marco-reglamentario-para-la-telesalud-en-colombia-18122019.pdf.