DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE ADQUISICIÓN DE SEÑALES ELECTROCARDIOGRÁFICAS CON ALMACENAMIENTO REMOTO DE DATOS ENCRIPTADOS

CARLOS EDUARDO MORENO DORIA
JUAN SEBASTIÁN MUNAR ALDANA

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C.
2020

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE ADQUISICIÓN DE SEÑALES ELECTROCARDIOGRÁFICAS CON ALMACENAMIENTO REMOTO DE DATOS ENCRIPTADOS

CARLOS EDUARDO MORENO DORIA
JUAN SEBASTIÁN MUNAR ALDANA

Proyecto de grado presentado como requisito para optar al título de
INGENIERO ELECTRÓNICO

Director:
Jaime Vitola Oyaga MSc.
Codirector:
Oscar Mauricio Gélvez Lizarazo MSc.

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C.
2020

A mi familia, por su amor incondicional desde el inicio, mi madre y su ternura, mi padre y su sacrificio, a mis hermanos, mis abuelos, amigos, A mi compañero de tesis Juan Sebastián Munar por el apoyo y compañía durante este periodo de trabajo juntos y a todos los que han hecho posible que yo siga aquí, siendo ellos el motor que me impulsaba a diario para lograr lo que soy ahora.

Carlos Moreno Doria.

A mi madre Mabel.
Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

***A mi padre Álvaro**.*
Por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor.

A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.
Todo este trabajo ha sido posible gracias a ellos.

***A mi compañero Carlos Moreno**.*
Por su lealtad y constante acompañamiento en este largo y enriquecedor camino, pero más que todo por brindarme su valiosa amistad.

Juan Sebastián Munar Aldana

AGRADECIMIENTOS

A los profesores Jaime Vitola Oyaga y Oscar Mauricio Gélvez por su dirección, constante asesoría y paciencia a lo largo del desarrollo de este trabajo de grado.

CONTENIDO

GLOSARIO

Algoritmo AES: Es un esquema de cifrado por bloques cuyas siglas en español significan “Estándar de Encriptación Avanzada.”

API: Es una interfaz que sirve para comunicar diferentes aplicaciones a partir de un código de programa. Sus siglas significan Interfaz de Aplicación de Programación.

Criptografía: Es una técnica donde se cifra con llaves únicas un texto o mensaje, de tal forma que el documento encriptado solamente sea legible por quien pueda descifrarlo.

DES: “Data Encryption Standard”, es un algoritmo de cifrado de datos de clave única implementado en 1976 en Estados unidos.

ECG: Es la ilustración del movimiento eléctrico del corazón.

IDE: En español, ambientes de desarrollo integrado. Son aplicaciones que permiten el desarrollo, implementación y depuración de código de programa.

IOT (Internet of things): Es un concepto que se refiere a la posibilidad de interconectar diversos dispositivos a través de internet.

Json: Json (JavaScript Object Notation), es un formato de archivos estándar al igual que un formato de intercambio de datos, utilizado principalmente para transmitir datos tipo “data object” los cuales contienen el valor de algún objeto.

Menisco: En física se define como la curvatura de la superficie de un líquido ya que esta superficie no es horizontal. Dependiendo de la interacción entre líquido y recipiente el menisco puede ser cóncavo o convexo.

Microcontrolador: Es un circuito integrado programable, compuesto por un procesador, memoria RAM y memoria ROM, capaz de ejecutar las órdenes grabadas en su memoria.

Python: Es un lenguaje de programación orientado a objetos de sencillo uso por sus librerías. Es más versátil y amigable que lenguajes como C.

Terminal Central de Wilson: Es el punto de referencia que permite medir la diferencia de potenciales en un ECG.

Telemedicina: Es el uso de intercambio de información médica de un sitio a otro, vía comunicación electrónica para mejorar el estado de salud de un paciente. [1]

Zigbee: Es un protocolo de comunicación inalámbrica, alternativa del WIFI o Bluetooth.

RESUMEN

La telemedicina, según la asociación americana de telemedicina, “es el uso de intercambio de información médica de un sitio a otro, vía comunicación electrónica para mejorar el estado de salud de un paciente” [1]. Actualmente, uno de los campos de acción en la comunidad científica hace esfuerzos para mejorar la adquisición, filtrado y transmisión de los datos, lo que permite que exámenes médicos de diferente naturaleza sean enviados desde el lugar dónde se realiza la muestra hasta la ubicación del especialista encargado de llevar a cabo el diagnóstico; sin embargo, los costos para poder acceder a un servicio como este, suelen ser muy elevados y de difícil acceso para las familias y habitantes ubicados en zonas rurales, por tal motivo, es necesario promover el desarrollo de sistemas de buen desempeño y bajo costo, que sean dirigidas a las poblaciones donde los centros de salud no cuenten con los recursos y cuyas necesidades sean evidentes.

Teniendo en cuenta lo anterior, se diseñó e implemento un sistema que captara la señal del corazón con la ayuda del circuito integrado AD8232, específico para señales del corazón. Este es dirigido por el microcontrolador ARM STM32f405, el cual alimenta al dispositivo y mediante un conversor analógico digital recibe los datos y los almacena. Posteriormente, con el mismo microcontrolador se encriptan las señales mediante el algoritmo AES para finalmente enviarlas vía WiFi a una base de datos online, donde se descargan las muestras desde otro dispositivo, para así desencriptar y graficar la señal adquirida. Además, se utiliza una micro SD como respaldo para guardar los datos en caso de fallar la conexión a internet.

INTRODUCCIÓN

Sistemas de salud como el que se presencia en el país, que resultan ineficientes por diferentes motivos, como la falta de infraestructura, representada en personal médico, para atender las necesidades básicas clínicas que se presentan día a día, los largos tiempos de espera para lectura de resultados, y la concentración del personal capacitado para llevar acabo diagnósticos relacionados con exámenes del corazón en las grandes ciudades del país, junto con los altos costos que esto implica. Dificultan entre otras cosas el acceso a servicios médicos por parte de personas de bajos recurso y/o marginadas en regiones rurales del país.

Al ser la salud un derecho fundamental para el ser humano, se deben ofrecer soluciones orientadas a una atención rápida y de calidad. Así mismo se deben evitar largas esperas y lograr la tranquilidad del paciente en cuanto a rapidez de obtención de resultados, aunado a garantizar la seguridad y privacidad de su información con la confidencialidad paciente médico.

Es por esto que se planteó en este proyecto, diseñar e implementar un sistema que capturara la señal del corazón por medio de un dispositivo portátil de bajo costo, integrado con un canal seguro que transfiriera la información vía Wifi, impidiendo que personas inescrupulosas accedan a la información del paciente y permitiendo la obtención de resultados de manera ágil y rápida.

1. PROBLEMA

Entre los problemas que se presentan actualmente en el sector salud se encuentran, en primera instancia la infraestructura disponible, ya que según estudios realizados por el ministerio de salud publicados en el documento “Composición de la oferta de profesionales de medicina en Colombia 2009” [2] en promedio por cada 10.000 habitantes en el país se encuentran aproximadamente 16 médicos, mientras que en Reino Unido, país con mejor sistema de salud del mundo según Health Consumer Powerhouse en su estudio de 2014 titulado “Mirror, Mirror on the Wall - How the Performance of the U.S. Health Care System Compares Internationally” [3], cuenta con 32 médicos aproximadamente. Una investigación realizada por la Organización Mundial de Salud (OMS) indica que los países con menos de 23 profesionales en medicina (incluidos únicamente médicos y enfermeras) por cada 10.000 habitantes, no alcanzan a cubrir adecuadamente las intervenciones clave de atención médica que son prioritarias en el marco de los objetivos de desarrollo del milenio.

En segunda instancia, se encuentra la formación de especialistas en cardiología, puesto que como se expresa en el artículo “ESTUDIO DE DISPONIBILIDAD Y DISTRIBUCIÓN DE LA OFERTA DE MÉDICOS ESPECIALISTAS, EN SERVICIOS DE ALTA Y MEDIANA COMPLEJIDAD EN COLOMBIA” [4] para obtener el título en esta área los aspirantes deben aprobar primero los cursos en la especialidad de medicina interna, lo que dificulta el aumento de número de estos. Según un artículo publicado por El Espectador en el año 2011 en todo el país se contaba con 7.872 especialistas de los cuales solo 2.011 eran médicos internistas. A raíz de lo mencionado anteriormente, y teniendo en cuenta que para ese año la población colombiana era de aproximadamente 46.41 millones y actualmente este número sigue en aumento, los profesionales que están capacitados para interpretar señales electrofisiológicas del corazón son muy pocos y no alcanzan a cubrir la demanda necesaria en el sistema de salud.

Finalmente, un tema importante a tratar es la repercusión en los tiempos de lectura de resultados de un electrocardiograma (ECG), que se da principalmente por la concentración de los pocos especialistas que se encuentran a lo largo del país, en las ciudades principales como: Bogotá, Medellín y Cali. Esto afecta principalmente a la población de las zonas rurales y alejadas que deben desplazarse para acceder a estos servicios médicos. En consecuencia entre 2005 y 2014 la principal causa de muerte en la población general fueron las enfermedades del sistema circulatorio, provocando 306.680 muertes en hombres y 288.608 muertes en mujeres, de las cuales 293.458 muertes fueron causadas por enfermedades del corazón, dando como resultado 78.24 muertes por cada 100.000 habitantes como se expresa en un estudio realizado por el Ministerio de protección social registrado en el documento ”Análisis de situación de salud (ASIS) Colombia, 2016” [5] . Lo cual implica que la atención brindada hacia los pacientes que padecen alguna anomalía de sistema circulatorio sea deficiente.

2. ANTECEDENTES

El electrocardiógrafo, es un dispositivo médico que permite capturar y amplificar la señal eléctrica producida por el corazón. Siendo un dispositivo importante en el ámbito médico, es necesario entender cómo funciona, por tal motivo, a continuación, se relatará un poco la historia de este artefacto que permitirá poner en contexto su funcionamiento. Así mismo, se irá explicando el surgimiento del Internet de las cosas (IOT) como un apoyo a los equipos médicos, dando como origen a lo que se conoce hoy en día como telemedicina.

En el año 1872 el físico francés Gabriel Lippmann hace una primera aproximación a un electrocardiógrafo, basado en las afirmaciones del físico italiano Carlo Matteucci que mostró cómo la corriente eléctrica acompaña a cada latido cardiaco, esta primera aproximación consistía en un tubo fino de vidrio con una columna de mercurio bañada con ácido sulfúrico. El menisco de mercurio se mueve con las variaciones de los potenciales eléctricos y esto es observables a través del microscopio. Veinte años más tarde en la University College de Londres dos fisiólogos británicos perfeccionan el electrómetro capilar de Lippmann esta vez conectando las terminales a la mano derecha y a la piel sobre la zona del latido del ápex y muestra unas variaciones trifásicas acompañando a cada latido del corazón, estas deflexiones fueron llamadas posteriormente Onda P. En 1901 Einthoven publica el primer electrocardiograma adaptado de un galvanómetro de cuerda, creado en años anteriores por un ingeniero eléctrico francés que lo registró como un sistema de amplificación de señales, en este se da la primera perspectiva de las cinco deflexiones principales conocidas como P, Q, R, S y T. [6]

En el año de 1961, fue implementado un sistema de monitoreo pre amplificador para una señal de electrocardiograma, diseñado para su uso principalmente en una sala de operaciones. Este sistema utilizó el acoplamiento de unos transformadores para la reducción de interferencia de 60 cps (ciclos por segundo) y únicamente se construyó una unidad prototipo. Un año después, fue publicado un artículo que hace referencia a la extracción de información médica con ayuda de computadoras a través de formas de onda electrofisiológicas, los datos tomados del ECG quedaron registrados en cintas magnéticas. La señal analógica fue muestreada 625 veces por segundo y los datos fueron convertidos de tal forma que una computadora digital de propósito general pudiese captar las muestras. [7][8]

En el año 1973, se realizó un estudio donde se analizaba la interferencia producida al captar una señal de electrocardiograma a 60 Hz, donde esta perturbación o

zumbido tiene como origen principalmente el potencial de línea o voltaje que está inevitablemente presente en cualquier situación clínica. [9]

Posteriormente en el año 1985, como alternativa a los circuitos analógicos que se utilizaban para el acondicionamiento de las señales de los electrocardiogramas, se implementaron algoritmos en microprocesadores que tenían como tarea el filtrado digital de manera más eficiente, procesos que son difíciles utilizando técnicas analógicas. Se presentó un conjunto de filtros digitales en tiempo real, cada uno implementado como una subrutina que al ser llamados en secuencias apropiadas generan un filtrado deseado en un solo microprocesador. Se incluyen filtros adaptables de interferencia de 60 Hz, filtros de eliminación de desplazamiento de Corriente Continua (CC), Filtros de detección del complejo QRS (presente en la señal eléctrica del corazón), y un algoritmo de reducción de datos, que logran velocidades de tiempo real y al solo requerir aritmética de enteros pudieron ser implementados en bastantes microprocesadores disponibles en el momento.[10]

En 1988 en una conferencia se dio a conocer el diseño de un sistema de adquisición de datos multicanal de tercera generación para el análisis de electrocardiogramas cardiacos. El sistema era capaz de registrar datos de 240 sitios de electrodos, tomando muestras a 2000hz. El diseño requería electrónica de propósito especial para grabaciones intraoperatorias y adquisición de datos de un gran ancho de banda para el análisis de datos en línea. El tiempo requerido para procesar los datos fue reducido drásticamente y proporcionó hardware que puede realizarlos en tiempo real. [11]

En 1990, fue publicado en “Computers in Cardiology 1990, Proceedings” un documento que presentó un sistema de electrocardiografía de alta resolución basado en PC, el cual contaba con una tarjeta complementaria, un computador y una impresora. La tarjeta contenía todos los circuitos análogos y digitales necesarios para la adquisición de datos. Se utilizó una memoria RAM de dos MBytes para la recopilación de datos ininterrumpidos de 2.5 minutos. Una parte del sistema controlada por el operador era seguida por el promedio de la señal, el filtrado pasa alto estaba entre 20 y 250 Hz. Se mostró que la porción terminal del QRS se puede modelar como la suma de sinusoides en descomposición con una frecuencia inferior a 25 Hz. [12]

En 1991 se realiza la aplicación de dos técnicas de reconocimiento de patrones, es decir, análisis conglomerados y redes neurales que tienen como punto de enfoque la investigación de la clasificación diagnóstica de los electrocardiogramas de 12 derivaciones. Para este estudio se empleó una base de datos previamente utilizada

por otros investigadores y establecida en la Universidad de Lovaina. La sensibilidad y la precisión total fueron los índices determinantes para la evaluación de rendimiento de este sistema de clasificación, en donde se presentaron resultados bastante satisfactorios luego de varios experimentos que fueron realizados en grupos de tres, cinco y siete redes neuronales que fueron reportadas en tablas de datos y demostraron una tasa de efectividad bastante alta. [13]

Los dispositivos continuaron evolucionando de gran manera, tanto así que en 1995 se implementó un sistema de monitoreo de ECG multicanal utilizando PC-AT 386 por el laboratorio de WIEECT medical electronics. El monitor utilizó datos modulados por ancho de pulso transmitidos desde la unidad cerca de la cama del paciente y los datos se recuperaban en 8255 (puerto paralelo) en una tarjeta DIO. No se necesitó convertidor analógico digital ya que se descifraba y demultiplexaba la información a través de software únicamente. La sincronización y el restablecimiento del hardware también se realizó mediante software que utilizaba la misma tarjeta DIO. Entonces la confiabilidad del sistema era bastante alta. [14]

Para 2004, los ingenieros en biomédica, Philip de Chazal, M. O'Dwyer, RB Reilly, presentaron un método para el procesamiento automático de un electrocardiograma (ECG) para la clasificación de los latidos del corazón. Las 5 clases de latidos asignadas por el método son las recomendadas por ANSI/AAMI EC57, Latido normal, latido ectópico ventricular (LEV), latido ectópico supra ventricular (LESV), fusión de un normal y un LEV, o tipo de ritmo desconocido. Se comparó el rendimiento de 12 configuraciones de clasificación y se eligió la mejor configuración para una evaluación de rendimiento independiente. Los datos obtenidos se dividieron en 2 conjuntos de datos, cada uno contenía aproximadamente 50000 latidos en 22 grabaciones. El primer conjunto se utilizó como clasificador de configuraciones candidatas. El segundo conjunto de datos fue usado para evaluar el rendimiento independiente a la configuración deseada. La evaluación del rendimiento independiente de esta configuración dio como resultado una sensibilidad del 75.9%, una predicción positiva del 38.5% y FPR (False Positive Rate) del 4.7% para la clase LESV. La sensibilidad del LEV fue 77.7%, la predicción positiva del 81.9% y el FPR del 1.2%. [15]

El uso del internet de las cosas (IOT) como aplicación para material médico, se presenta unos años atrás cuando se empieza a tener presente la telemedicina, la cual surge como un complemento de la medicina tradicional, que busca la comunicación entre médicos y pacientes a través de una red de comunicaciones móviles de alta velocidad, segura y estable que permita cumplir su principal objetivo, la prestación de servicios médicos a distancia.

Con el paso de los años, las nuevas tecnologías implementadas en los dispositivos ECG permiten mejorar la captación de las señales con ayuda de convertidores análogo-digitales para que luego la señal sea procesada y tratada a partir de electrónica digital. [16]

Hay diferentes dispositivos médicos en los cuales se implementa el internet de las cosas, entre ellos se encuentran aquellos que captan las señales electrocardiográficas (ECG), estos son considerados dispositivos médicos esenciales para la detección y prevención de enfermedades cardiovasculares, ya que son artefactos altamente eficaces para obtener información sobre la estructura y funcionamiento del corazón

En el año 2014, fue construida una aplicación móvil basada en la plataforma Android para el dominio de la atención médica la cual utiliza la idea del IOT (Internet Of Things) y almacenamiento virtual en una nube. La aplicación se llamó 'ECG Android App' y proporciona al usuario final la visualización de sus ondas del electrocardiograma (ECG), los datos registrados se pueden cargar en una nube médica específica, la cual mantiene un registro de todos los datos monitoreados por el personal médico. Este proyecto incluyó varias tecnologías tales como microcontroladores, procesamiento de señal para ondas de ECG, protocolos de comunicación y diseño de sistemas para respaldar la transferencia de datos privada y segura, además de DBMS (DataBase Managment System), servicios web y técnicas en la nube para la gran cantidad de almacenamiento de datos y transferencia confiable utilizando patrones de diseño de software comprobados. Por último, Se construyó una infraestructura basada en las tecnologías mencionadas previamente para la monitorización de ondas de un ECG. [17]

Para 2016, fue propuesta una aplicación de IOT como transmisión de datos multimedia para la señal de un electrocardiograma, esta se desarrolló mediante un sistema de monitoreo de ECG al que pueden acceder varios usuarios simultáneamente a través de internet. Se utilizó como Hardware un ECG, un módulo de transmisión basado en ZigBee y un servidor web para almacenar datos. La señal de ECG tomada de los pacientes es adquirida por la máquina de ECG, y luego los datos brutos se envían en serie al servidor de la computadora usando Zigbee. [18]

Para el mismo año en una conferencia 2016 5th International Conference on Modern Circuits and Systems Technologies (MOCAST) se desarrolló un algoritmo para el análisis de una señal ECG y su clasificación a partir de un diagnóstico del ritmo cardiaco implementándolo en una plataforma embebida de IOT. Esto tenía como propósito ser usado en un dispositivo ECG portable y de uso diario que monitoree

el paciente continuamente durante las 24 horas del día. Este algoritmo utiliza la DWT (Discret Wavelet Transform) para el análisis y un clasificador SVM (Support Vector Machine). Diferentes implementaciones del algoritmo en una tarjeta Galileo ayudaron a demostrar que el costo computacional es tanto que el análisis y clasificación ECG puede ser realizado en tiempo real. Así mismo conjuntamente fue propuesto un sistema inalámbrico para el monitoreo electrocardiográfico del corazón basado en dispositivos Android. Las señales cardiacas son grabadas a partir de tres electrodos y posteriormente se almacenó el resultado de la señal en una base de datos que luego fue sincronizada en una Nube a través del uso del internet. La señal final fue mostrada en un sitio Web para ser usada por los usuarios en tiempo real y procesada por algoritmos de procesamiento y análisis profundo usando la transformada de Wavelet. [19] [20]

3. JUSTIFICACION

Al ser la salud un derecho fundamental para el ser humano, se deben ofrecer soluciones orientadas a una atención rápida y de calidad. Sistemas, como el aquí presentado, apuntan a tener un impacto social importante, dado que, al agilizar los procedimientos se puede tener diagnósticos de especialistas en cualquier lugar, reduciendo la posibilidad de errores en la evaluación.

Así mismo se evitan largas esperas y se logra tranquilidad del paciente en cuanto a rapidez de obtención de resultados. Unificado a esto la seguridad y privacidad de su información no se ven comprometidas gracias a la encriptación de los datos que permitió la confidencialidad de la relación paciente médico.

La solución que se planteó a este problema específico, fue el diseño de un sistema que permitiera la toma de señales electrocardiográficas por medio de un dispositivo portátil que integrara el ámbito médico con un sistema computacional. Aprovechando las virtudes del Internet de las cosas (IOT) como lo son: mejora en la eficiencia de los procesos, facilidad al acceso de la información en diferentes lugares, seguridad de la información y la posibilidad de realizar procesamiento adicional para inferir conclusiones y generar alertas oportunas.

Estas bondades dotaron al dispositivo de la capacidad de realizar diagnósticos remotos por parte de personal especializado para la interpretación de resultados acercando al especialista con el paciente. Sin embargo, el hecho que los datos fuesen transportados por canales de comunicaciones públicos, hace que la seguridad de los mismos pueda verse comprometida, lo cual determinó un nuevo reto que es ocultar la información privada de personas inescrupulosas. En tal sentido se utilizó el mecanismo de encriptación de datos desde la fuente hasta el destino evitando este inconveniente.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar e implementar un sistema de adquisición de señales electrocardiográficas, con almacenamiento remoto de datos encriptados.

4.2 OBJETIVOS ESPECÍFICOS

- Diseñar e implementar un sistema que permita la toma de señales electrocardiográficas por medio de un dispositivo portátil.
- Implementar un algoritmo de seguridad para la confidencialidad de la información y poder transmitirla hacia un servidor remoto utilizando un canal inalámbrico.
- Integrar un dispositivo de adquisición de señales electrocardiográficas con un canal seguro para la transmisión de información.
- Realizar las pruebas pertinentes que puedan evidenciar el correcto funcionamiento del prototipo en cuanto a adquisición de la señal electrocardiográfica, transmisión y almacenamiento remoto de la información.

5. MARTO TEÓRICO

La telemedicina se podría definir como la transferencia de información y atención médica a través de redes de telecomunicaciones. Esto incluiría la transmisión de imágenes fijas, videos, monitoreo remoto y demás datos médicos.
Actualmente, la telemedicina es implementada para resolver problemas de falta de especialistas, escasez de recursos, centros rurales con limitaciones, entre otros, permitiendo así proveer servicios de salud sin importar la ubicación geográfica.

El marco teórico que sustenta este proyecto de grado proporcionará al lector una idea más clara de la temática a tratar. Se hallarán los conceptos, básicos, específicos y complementarios.

5.1 CARDIOLOGÍA

La cardiología es una rama de la medicina interna que se encarga del estudio, análisis, diagnóstico y tratamiento de pacientes que padecen enfermedades cardiacas. Dentro de la cardiología, existe un método rápido y sencillo de obtener los pulsos eléctricos que el corazón genera al bombear sangre al cuerpo llamado electrocardiografía, donde se amplifica la señal cardiaca a partir de instrumentos electrónicos obteniendo así un registro que ilustra el comportamiento del corazón. Este registro se conoce como electrocardiograma y se realiza cuando ocurre alguna dolencia de tipo cardiaca o como monitoreo preventivo en personas de edades medianas y edades avanzadas. [21]

5.1.1 FISIOLOGÍA CARDIACA.

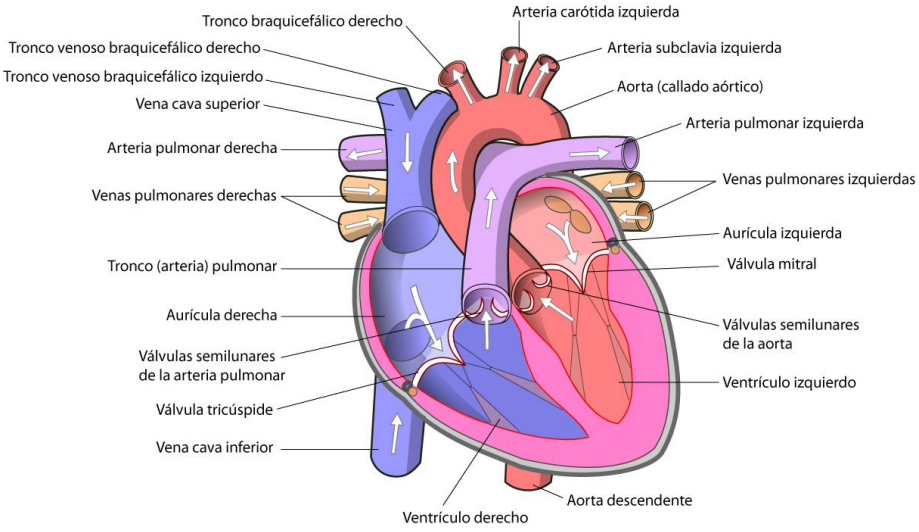
El corazón es el órgano principal del sistema circulatorio. En los seres humanos, es una bomba muscular doble, de un tamaño similar al puño de su portador, compuesto por cuatro cámaras divididas en 2 mitades, donde cada una cuenta con una aurícula y un ventrículo. Las cámaras superiores (arteria derecha e izquierda) son puntos de entrada al corazón, mientras que las cámaras inferiores (ventrículo derecho e izquierdo) son cámaras de contracción que envían sangre constantemente mediante circulación a todo el cuerpo. [22]

La circulación se divide en dos ciclos, en el primero la sangre es expulsada a los pulmones, mediante la arteria pulmonar para ser oxigenada, obtiene oxígeno “O2” y entrega dióxido de carbono “CO2”. A continuación, la sangre ingresa a la aurícula ubicada en la parte izquierda del corazón, donde pasa al ventrículo por la válvula mitral o bicúspide. Finalmente, en el segundo ciclo, la sangre es bombeada al cuerpo a través de la arteria aorta donde el oxígeno es distribuido. [23]

Los movimientos rítmicos descritos en el párrafo anterior son producidos por medio de contracciones y relajaciones musculares que se crean mediante pequeñas descargas eléctricas.

La figura 5.1 muestra a detalle cómo está compuesta la fisiología del corazón

FIGURA 5.1 FISIOLOGIA CARDIACA



FUENTE: L. Perdomo (21 de marzo 2016) Fisiología Cardiaca Recuperado 12 de abril 2020 [Online]. Available: Fiiologiacardiaca.Blogspot.Com/2016/03/Potencial-De-Accion-Funcionalmente-El.Html

5.1.2 SEÑAL ELECTROCARDIGRÁFICA

Una señal electrocardiográfica se compone principalmente por ondas y segmentos. Las ondas son desviaciones de la dirección de la corriente por encima y por debajo de la línea base. Los segmentos son divisiones de la línea de base entre ondas. Las tres ondas principales en una señal de electrocardiografía son las ondas P, Q y T. Existen, además, ondas que complementan la muestra cardiaca siendo estas la S, R, U. Por último, existen una serie de intervalos y complejos que son el resultado de combinaciones entre ondas primarias y complementarias. A continuación, una breve explicación de cada una de las ondas. [22]

Onda P: Se produce por la despolarización o contracción auricular. Dura aproximadamente 0.06 segundos.

Onda Q: Es la primera desviación de la dirección de corriente negativa o deflexión negativa del complejo QRS.

Onda T: Indica la distención de los ventrículos. Esta onda no es simétrica y tiene una forma redonda generalmente.

Onda R: Es la desviación de corriente positiva del complejo QRS, si Q no se puede visibilizar la onda R será la primera desviación de corriente después del intervalo PR

Onda S: Es cualquier onda negativa del complejo QRS siempre que sea precedida por una onda positiva (R).

Onda U: No se conoce bien su significado, pero se cree que es producida por la distención o relajación ventricular.

Intervalo PR: Es la distancia medida entre el comienzo del complejo QRS y la onda P.

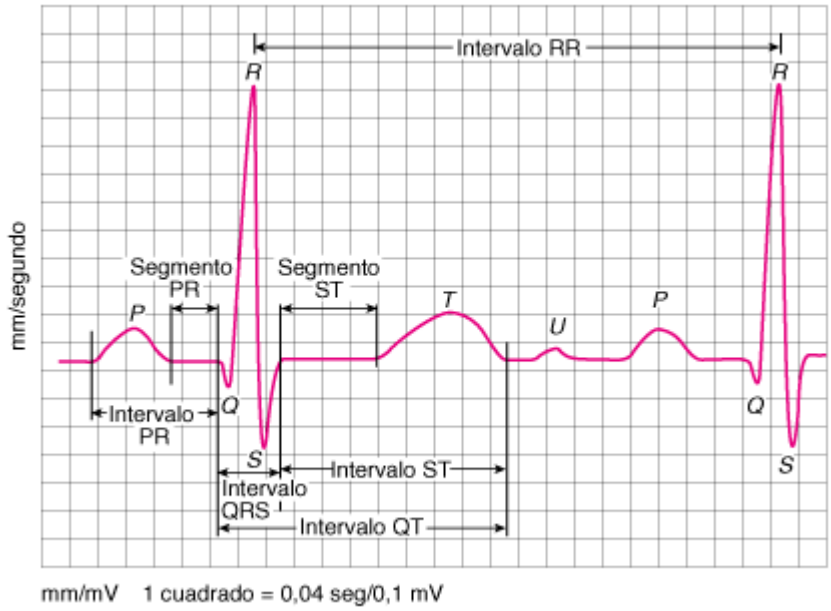
Complejo QRS: Es la sucesión de la contracción ventricular. Su duración varía según la edad de cada persona, pero en promedio es de 0,12[s].

Segmento ST: Es la primera parte de la distención ventricular. Es una línea horizontal sin voltaje que inicia desde el final del complejo QRS y va hasta el comienzo de la onda T.

Intervalo QT: Representa la actividad eléctrica ventricular en su totalidad. Se mide desde el inicio del complejo QRS hasta el final de la onda T.

La figura 5.2 ilustra a detalle cómo es el comportamiento de la señal de electrocardiografía a la hora de tomar una muestra de ECG.

FIGURA 5.2 SEÑAL ELECTROCARDIOGRÁFICA



FUENTE: M. J. Shea, MD, (September 2017) Electrocardiografía Recuperado 12 de abril 2020 [Online]. Available: Https://Www.Msdmanuals.Com/Es/Professional/Trastornos-Cardiovasculares/Pruebas-Y-Procedimientos-Cardiovasculares/Electrocardiograf%C3%Ada

5.1.3 DERIVACIONES CARDIACAS

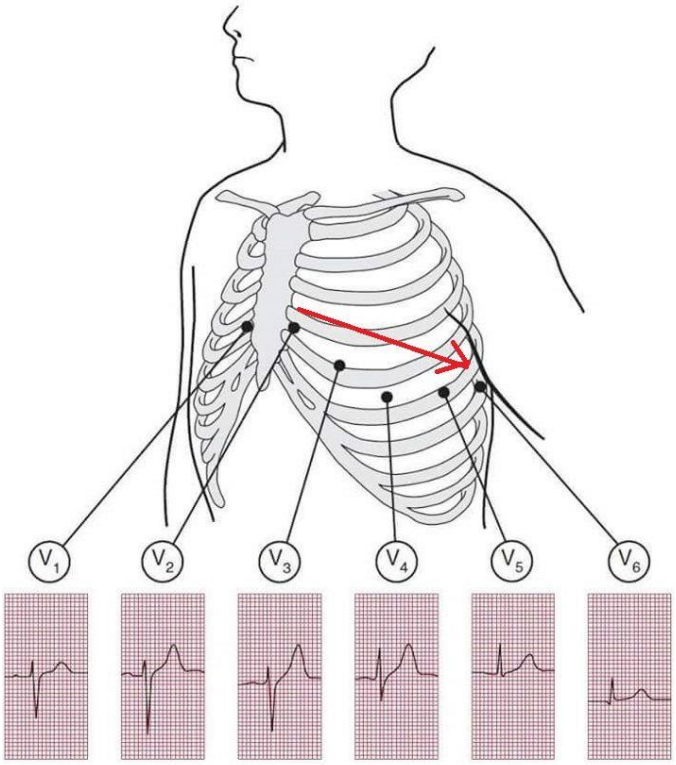
Son la medida del voltaje del corazón mediante electrodos, los cuales son colocados en puntos específicos del paciente para la obtención de las señales ECG. En los hospitales se emplea el ECG de 12 derivaciones para tener mayor precisión a la hora de dictar un diagnóstico.

Existen 3 tipos de derivaciones que conforman las 12 mencionadas previamente.

- **Derivaciones precordiales:** Son seis en total, Se miden por delante y alrededor del tórax. Estas derivaciones registran la dirección de corriente que se genera sobre la parte frontal del pecho, y permiten examinar el voltaje generado por el punto donde es colocado el electrodo con respecto al terminal de Wilson. Se considera que son las que mejor referencia dan de las alteraciones del ventrículo izquierdo.[24]

  A continuación, en la figura 5.3, se visualiza el comportamiento de las derivaciones precordiales.

FIGURA 5.3 DERIVACIONES PRECORDIALES

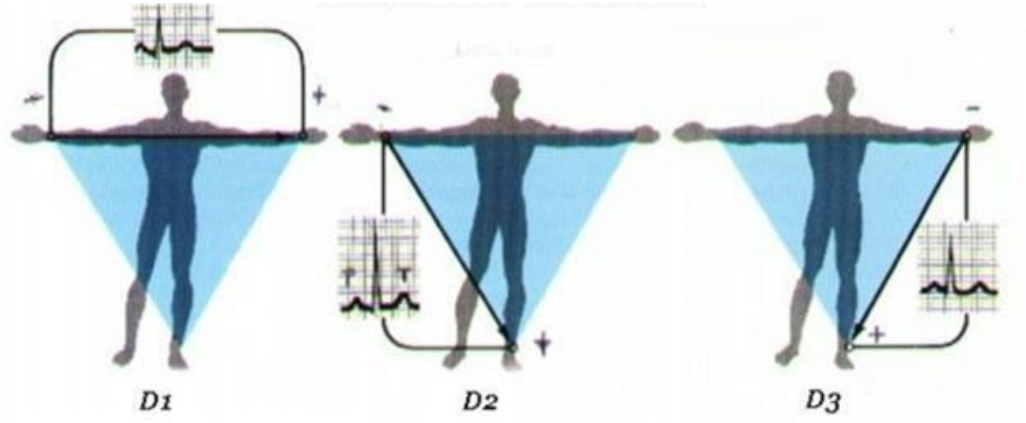


FUENTE: E. Plaza Moreno. Urgencias y emergencias, Las Derivaciones Del Electrocardiograma Recuperado 12 de abril 2020 [Online] Available: Https://Www.Urgenciasyemergen.Com/Las-Derivaciones-Del-Electrocardiograma/

- **Derivaciones bipolares:** Son tres, denominadas por Einthoven (creador del electrocardiograma) como, DI, DII, DIII, las cuales forman un triángulo equilátero entre si llamado triángulo de Einthoven. Las señales de cada derivación se obtienen gracias a tres electrodos conectados sobre los brazos derecho e izquierdo y el pie izquierdo. DI, es la diferencia de potencial que hay entre el brazo derecho y el brazo izquierdo, DII es la diferencia de potencial entre pierna izquierda y brazo derecho y DII se obtiene de la diferencia de potencial entre pierna izquierda y brazo izquierdo.[24]

  La figura 5.4 muestra cómo se obtienen estas derivaciones al colocar los electrodos de forma diferente.

FIGURA 5.4 DERIVACIONES BIPOLARES

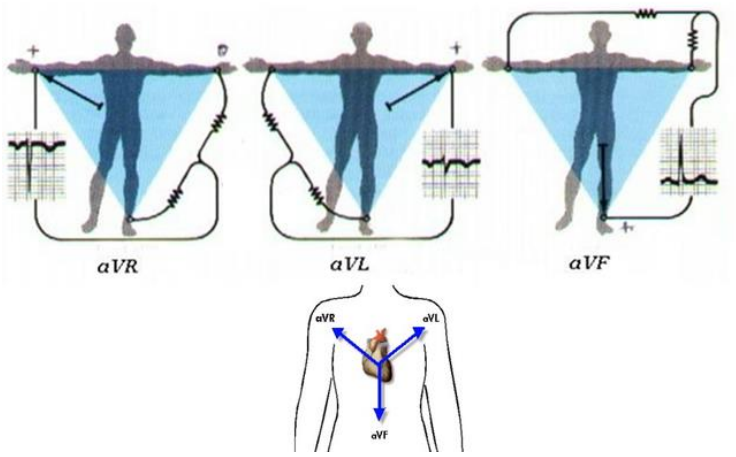


FUENTE: S. Velasco, (marzo 2015). Lectura de Electrocardiograma (ECG) normal (1/2) Recuperado 12 de abril 2020 [Online] Available: https://unascosasdesimon.blogspot.com/2015/03/lectura-de-electrocardiograma-ecg.html

- **Derivaciones unipolares aumentadas o monopolares aumentadas:** Son tres, y determinan el voltaje entre un electrodo positivo y un terminal central que sirve como referencia y se genera a partir de los tres electrodos, a esta referencia se le designa terminal central de Wilson (WCT). [24]
  Estos potenciales de denominan de la siguiente manera:
  Derivación unipolar aumentada brazo derecho aVR: Donde se toma el brazo derecho como referencia positiva mientras que la pierna y brazo izquierdos se toman como referencia negativa.
  Derivación unipolar aumentada brazo izquierdo aVL: La cual se deriva de tomar como referencia positiva el brazo izquierdo y la pierna izquierda y el brazo derecho como referencia negativa.
  Derivación unipolar aumentada de pie izquierdo aVF: Esta se deduce de tomar la pierna izquierda como referencia positiva y los brazos izquierdo y derecho como referencia negativa.

  En la figura 5.5 se muestra cómo detectar las derivaciones unipolares aumentadas.

FIGURA 5.5 DERIVACIONES UNIPOLARES AUMENTADAS



FUENTE: (Marzo 2018) Aprendamos a leer un ECG Electrocardiografía Básica [PARTE 1 - DERIVACIONES]. Recuperado 12 de abril 2020 [Online] Available: Https://Steemit.Com/Stem-Espanol/@Hipocrates/Aprendamos-A-Leer-Un-Ecg-Electrocardiografia-Basica-Parte-1-Derivaciones

5.2 CRIPTOGRAFÍA

La palabra criptografía proviene del griego “kriptos” cuyo significado es oculto y “graphia” que significa escritura. La criptografía es un conjunto de técnicas o métodos matemáticos que surge con el objetivo de encriptar textos y hacerlos ininteligibles para aquellos que no deben saber su contenido.
El primer sistema de criptografía que se caracterizó por ocultar el significado real de un mensaje se da en Esparta hacia el año 400 a.C. “La Escitala” era el nombre que se le atribuida a este artefacto de cifrado. A lo largo de la historia fueron apareciendo instrumentos más modernos y robustos para encriptar mensajes
Actualmente en la era digital, existen diferentes técnicas de cifrado clasificadas en sistemas de cifrado simétrico y asimétrico, los cuales se explicarán a continuación. [25]

5.2.1 CRIPTOGRAFÍA SIMÉTRICA:

Es un sistema de cifrado donde se utiliza una sola clave tanto para encriptar como para des encriptar, por lo que es indispensable que solamente el emisor y el receptor del mensaje sean los poseedores y conocedores de la clave.

La criptografía simétrica es la que más se conoce y más se utiliza actualmente, siendo usada para las aplicaciones de telefonía móvil, encriptación de datos en aplicativos que manejan bases de datos, cifrado de archivos de oficina, entre otras. Este método de codificación es capaz de cifrar cantidades grandes de datos en poco tiempo debido a su facilidad matemática, por esto mismo, son implementados en hardware de manera sencilla. Entre los algoritmos de encriptación que emplean este método se encuentran:

DES (Data Encryption Standard): Es el más utilizado en la criptografía simétrica, está basado en la operación lógica XOR, la cual usa dos veces además de operaciones de sustitución y permutación. [26]

Triple DES o TDES: Consiste en emplear tres veces el algoritmo DES, lo que genera 3 claves diferentes y resulta difícil descifrar. [26]

AES: cuyas siglas significan “Advanced Encryption Standard”, es un sistema de cifrado por bloques que aplica, gracias a su diseño, longitudes de bloque y claves cambiantes. AES es el algoritmo de criptografía más utilizado en la actualidad, no solo por su nivel de seguridad, sino por su rapidez de ejecución tanto en software como en hardware. Algunas de las aplicaciones que este cifrado tiene son en el campo de las transferencias bancarias Online, las comunicaciones inalámbricas como Redes WIFI, o la protección de datos de discos duros de computadores. [27] Se explicará este algoritmo con mayor detalle más adelante en este mismo capítulo en la sección 5.2.3.

5.2.2 CRIPTOGRAFÍA ASIMÉTRICA:

A diferencia del método de cifrado simétrico, esta modalidad de encriptación utiliza dos claves, una pública con la que se cifra el mensaje y poseen tanto emisor como receptor o cualquier usuario y una privada que es con la que se des encripta el documento y solo dispone de esta el dueño de la clave, en este caso el receptor únicamente. Esto con el fin de suplir la necesidad que presenta la criptografía simétrica de transferir las claves.

Este método se basa en operaciones matemáticas complejas, por lo que resulta ser mucho más lento en ejecución (entre 100 y 1000 veces más lento que los algoritmos simétricos), pero asimismo mucho más robusto y seguro. Normalmente, el texto encriptado con esta modalidad de cifrado suele ser más grande que el original. Sus principales aplicaciones son la firma digital para autenticar documentos y la clave privada [28]. Algunos de los algoritmos de criptografía asimétrica más usados son:

RSA: Sus siglas tienen por significado “Rivest Shamir Adleman”, Es quizá el algoritmo más utilizado y predominante en la actualidad y está basado en la

multiplicación de dos números primos de gran tamaño ya que la factorización de ese producto resulta imposible computacionalmente, de aquí se derivan ambas claves. [28][29]

DEFFIE-HELLMAN: También conocido como “El cambio de clave de Deffie-Hellman”, es un algoritmo en el cual los usuarios acuerdan una clave secreta y la intercambian por un medio inseguro. [28][29]

5.2.3 CIFRADO POR BLOQUES AES:

Nace en 1997, en el Instituto Nacional De Estándares Y Tecnología De Los Estados Unidos (NIST) como reemplazo del DES y su sucesor 3-DES con el fin de proteger la información del gobierno en el siglo que se avecinaba (XXI). Este algoritmo hace uso de funciones matemáticas invertibles, lo cual quiere decir, que cada vez que se ejecuta una operación, se tendrá una operación inversa definida, por lo tanto, los cálculos son bidireccionales, permitiendo así el cifrado y descifrado de los mensajes. [29]

Para codificar un mensaje, se ingresa al algoritmo el texto original y una llave, estos dos elementos se pasan por un determinado número de iteraciones o rondas de transformación para obtener el mensaje cifrado. El número de iteraciones depende del tamaño de la clave.

AES es un algoritmo que se ejecuta sobre bloques de datos de 128 bits y su clave puede emplear valores de 128 bits, lo que implicaría un número de rondas igual a 10, 192 bits que significarían 12 rondas de transformación y 256 bits que involucran 14 iteraciones. [29] Cada ronda es conformada por cinco matrices, en donde la primera hace alusión a la entrada (clave y mensaje) y los 4 restantes son funciones de trasformación definidas, como se muestra a continuación:

1. Matriz de Entrada: En esta matriz, se almacena el mensaje original ya que cada una de las iteraciones necesitan realizar cálculos con el texto de entrada.

2. Matriz SubBytes: Sustituye cada uno de los bytes por otro de acuerdo a una tabla fija de manera no lineal.

3. Matriz ShiftRows: Desplaza cada byte de cada fila hacia la izquierda circularmente de forma periódica.

4. Matriz MixColum: Esta operación Combina cada columna de la matriz, es decir permite mezclar los bytes que conforman cada columna. Este

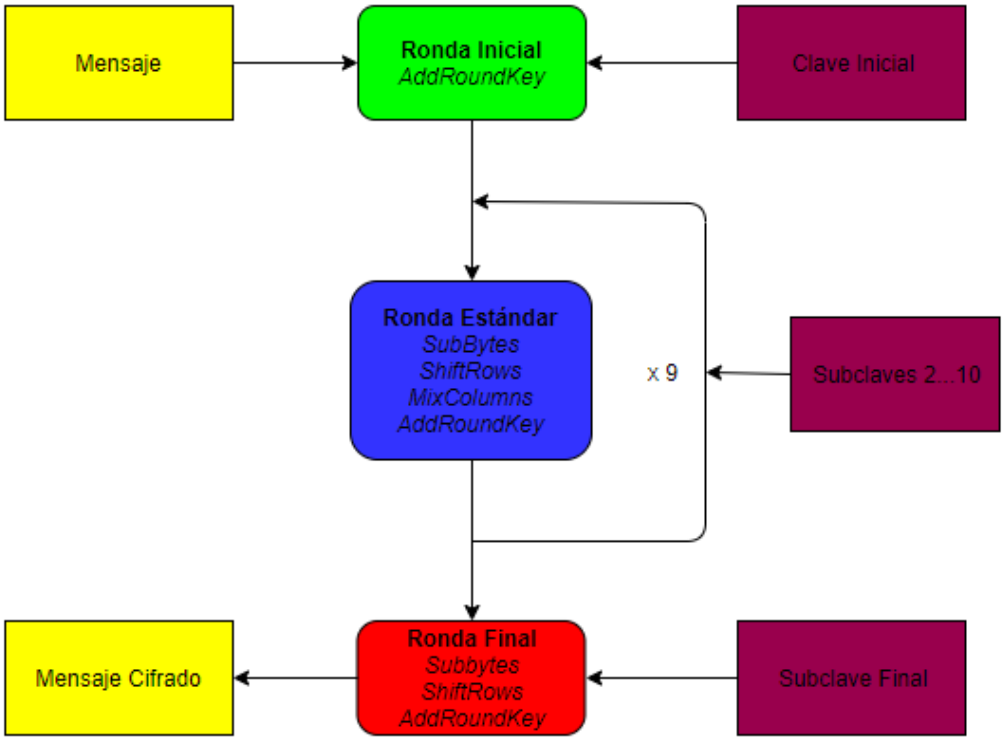
proceso se logra multiplicando la columna a mezclar por una matriz fija.

5. Matriz Round Key: Esta transformación modifica el estado de la clave realizando una operación XOR byte a byte y sumando el resultado a cada bit de la subclave de la ronda correspondiente.

6. En la última iteración se omite el cálculo de la matriz MixColum.

   A continuación, la figura 5.6 ilustra la representación del algoritmo en diagrama de bloques.

FIGURA 5.6 DIGRAMA DE BLOQUES CIFRADO AES



FUENTE: AUTORES

Para decodificar el mensaje, se utiliza el texto cifrado y la clave como entrada al algoritmo, a diferencia de la codificación, estos componentes se pasan por operaciones de transformación inversas. Por ejemplo, si en la codificación hubo desplazamiento hacia la izquierda en la matriz ShiftRows, en la decodificación el desplazamiento se hará hacia la derecha en una matriz que se llame InvShiftRows, para así poder obtener el mensaje original de la siguiente manera:

1. Matriz DataEncriptada: Esta matriz tiene almacenado el mensaje cifrado, para cada una de las rondas es necesario calcularla de la siguiente manera: Ronda 1: Cripto Original ⊕ RoundKey.
   Ronda 2 a Ronda n: InvMixColumns (InvSubBytes ⊕ RoundKey).

2. Matriz InvShiftRows (ISR): Desplaza cada byte de cada fila hacia la derecha circularmente de forma periódica.

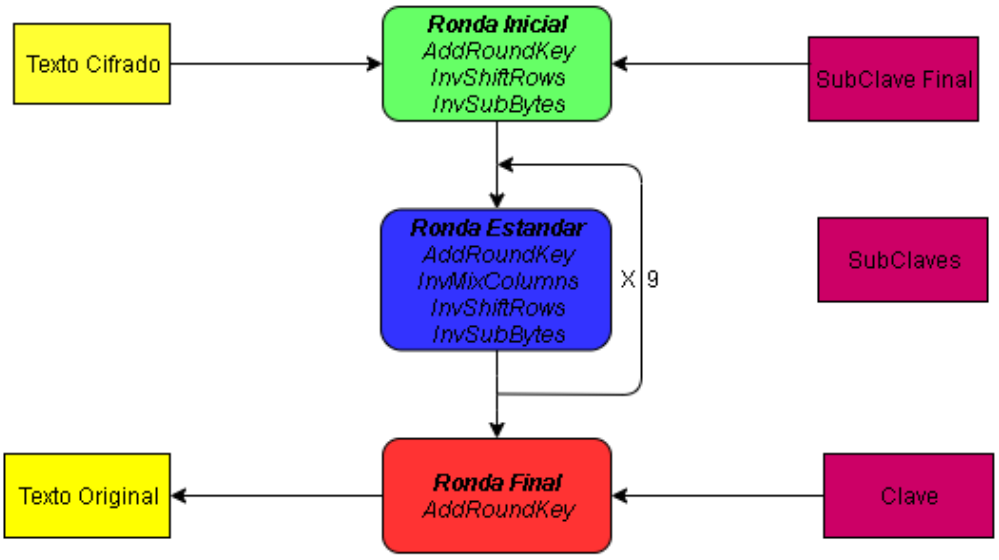
3. Matriz InvSubByte (ISB): Se implementa del mismo modo que en el cifrado, pero se emplea la tabla S-box.

4. Matriz RoundKey(RK): Se invierte la transformación restando el resultado de la operación XOR a cada bit de la subclave de la ronda correspondiente.

5. Matriz ISB ⊕ RK: El mensaje descifrado se obtiene del resultado de la operación ISB ⊕ RK (ISB xor RK) en la última iteración.

La figura 5.7 muestra el diagrama de bloques de Descifrado por AES.

FIGURA 5.7 DIAGRAMA DE BLOQUES DESCIFRADO AES



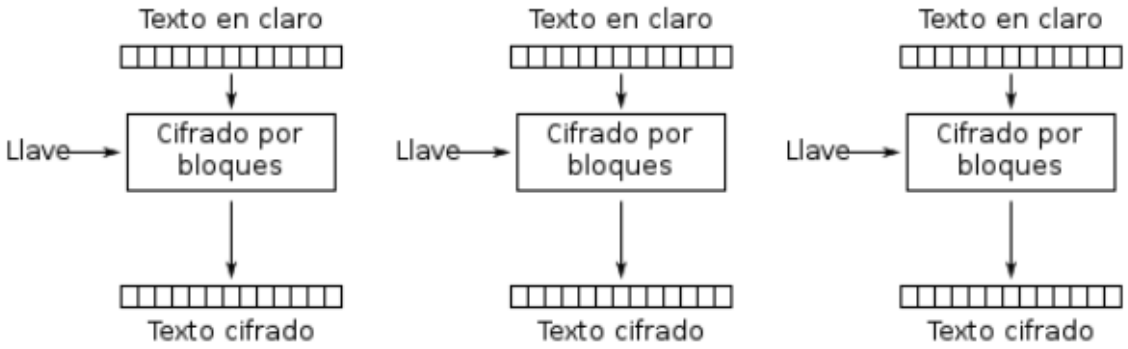
FUENTE: AUTORES

Según expertos que trabajaban en investigación para Microsoft hacia el año 2011, el cifrado AES es un algoritmo difícil de vulnerar, debido a que para descifrar un mensaje que haya sido encriptado con esta técnica se debe tener la clave. Esta llave esta expresada como $2^{Longitud\ de\ \ la\ clave}$, entonces, si se tiene una contraseña de 128 bits se tendrían en realidad $2^{128} = 3.40x10^{34}$ claves posibles, lo que hace que para un computador sea imposible dar con el resultado original, incluso si se colocaran a trabajar un billón de ordenadores que probasen cada uno mil millones de claves por segundo, tardarían alrededor de 2000 millones de años en dar con una llave del sistema AES de 128 bits. Ahora, si se emplea una clave de 192 o 256 bits, el tiempo será mucho más extenso, pero hay que resaltar que las máquinas actuales solo pueden probar en promedio 10 millones de claves por segundo, lo que dificulta aún más hallar la contraseña.[32]

AES es creado para reemplazar a DES, pero emplea los modos de cifrado y descifrado que el segundo maneja, siendo ECB, CBC, CFB algunos de los modos usados por AES. A continuación, una corta explicación de cada uno de estos modos.

ECB: Sus siglas significan Electronic Code Block, en este modo el texto se divide en bloques de 16 bytes y cada uno de los bloques se cifra independientemente utilizando la misma clave. Este modo es el más débil de todos porque no usa medidas de seguridad adicionales además del algoritmo básico de AES, sin embargos, es el más rápido y fácil de implementar. [30]

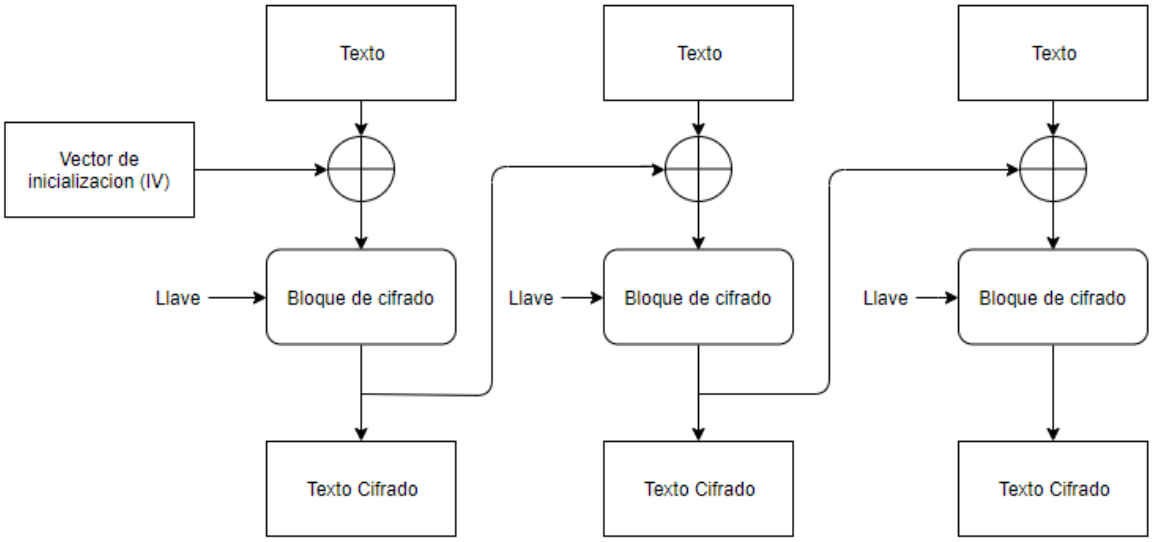
FIGURA 5.8.a CIFRADO POR BLOQUES ECB



FUENTE: Fig 5.8 a) Diagrama Bloques ECB, Modos De Cifrado Aes Recuperado 12 de abril 2020 [Online] Available:Es.Wikipedia.Org/Wiki/Modos_De_Operaci%C3%B3n_De_Una_Unidad_De_Cifrado_Por_Bloques.

CBC: Cuyas siglas son por Cipher Block Chaining, es quizá el más utilizado de los AES y funciona aplicándole a cada bloque de texto una operación XOR con el bloque cifrado inmediatamente anterior, así cada bloque de texto cifrado depende de todo el texto en claro. Para hacer cada bloque del mensaje único se utiliza un vector de inicialización abreviado a IV, el cual se combina con el texto sin formato. Además, como el primer bloque de cifrado no tiene texto cifrado anterior, el primer bloque encriptado se da como resultado de IV XOR primer bloque a cifrar. Este modo es más seguro que ECB porque tiene la operación XOR como medida de seguridad adicional [30].

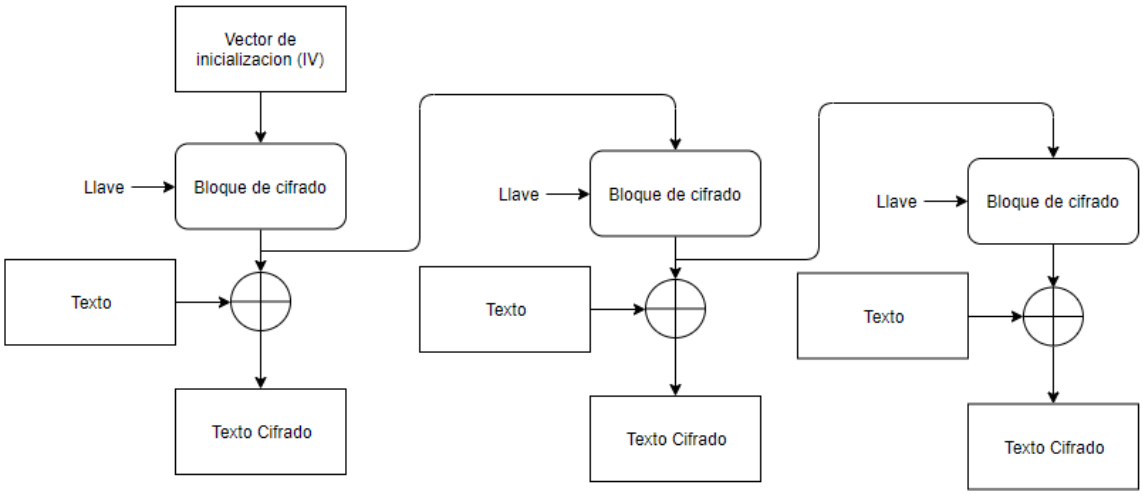
FIGURA 5.8.b CIFRADO POR BLOQUES CBC



FUENTE: AUTORES, ADAPTADO DE Diagrama Bloques CBC, Modos De Cifrado Aes Recuperado 12 de abril 2020 [Online] Available:Es.Wikipedia.Org/Wiki/Modos_De_Operaci%C3%B3n_De_Una_Unidad_De_Cifrado_Por_Bloques.

CFB (Cipher FeedBack): Es un modo de cifrado que emplea una clave para crear un bloque pseudoaleatorio, entonces se realiza una operación XOR entre este bloque aleatorio y cada uno de los bloques a cifrar para así generar el texto cifrado [30]. De la siguiente manera

FIGURA 5.8.c CIFRADO POR BLOQUES CFB



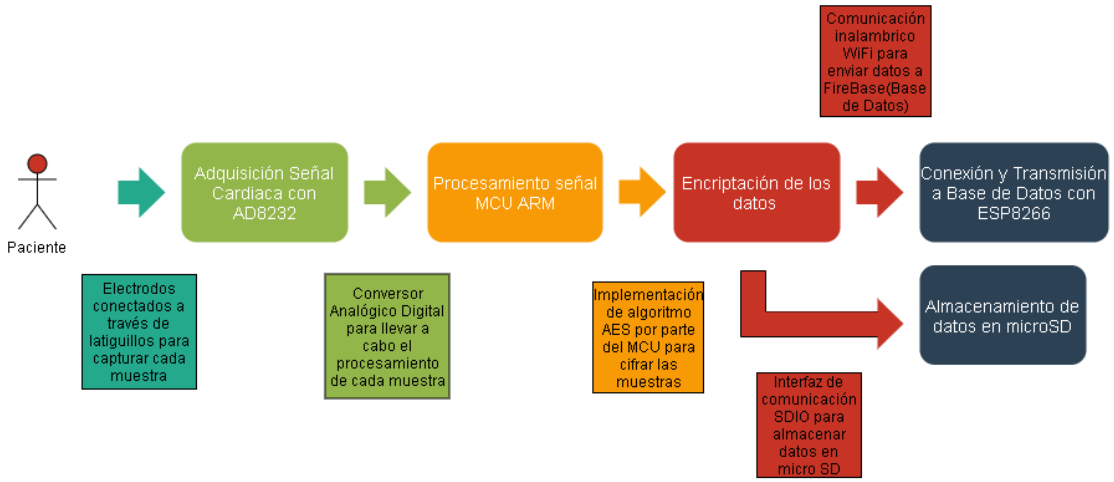
FUENTE: AUTORES, ADAPTADO DE Diagrama Bloques CFB, Modos De Cifrado Aes Recuperado 12 de abril 2020 [Online] Available:Es.Wikipedia.Org/Wiki/Modos_De_Operaci%C3%B3n_De_Una_Unidad_De_Cifrado_Por_Bloques.

6. DISEÑO METODOLÓGICO

En este capítulo, se especificará la metodología que se empleó para la elaboración del presente proyecto de grado, aquí se describirán los elementos necesarios para el diseño e implementación de un sistema de adquisición de señales electrocardiográficas con almacenamiento remoto de datos encriptados.

6.1 HARDWARE

FIGURA 6.1 DIAGRAMA DE BLOQUES FUNCIONAMIENTO HARDWARE



FUENTE: AUTORES

Como se puede apreciar en el esquema anterior, cada una de las unidades que conforman este sistema juegan un papel específico para garantizar el funcionamiento de este.

El dispositivo que se encarga de llevar a cabo la tarea de captar la señal trabaja de tal forma que solo se deba alimentar y el empieza a adquirir los datos correspondientes a las muestras a través de los electrodos conectados al paciente.

Posteriormente se digitalizan cada una de las muestras con ayuda de uno de los conversores analógico digitales (CAD) presentes en el microcontrolador, estos conversores tienen una capacidad de resolución de 12 bits por lo que cada muestra es un dato digital de 0 a 4096.

Cada una de las unidades siguientes presentes en el proyecto, el cifrado, la transmisión y el almacenamiento en micro SD de los datos, trabajan con valores de 0 a 255, por lo tanto, cada muestra se divide en dos datos de 8 bits y se almacenan en un arreglo para poder realizar cada uno de los procesos siguientes y obtener el resultado esperado.

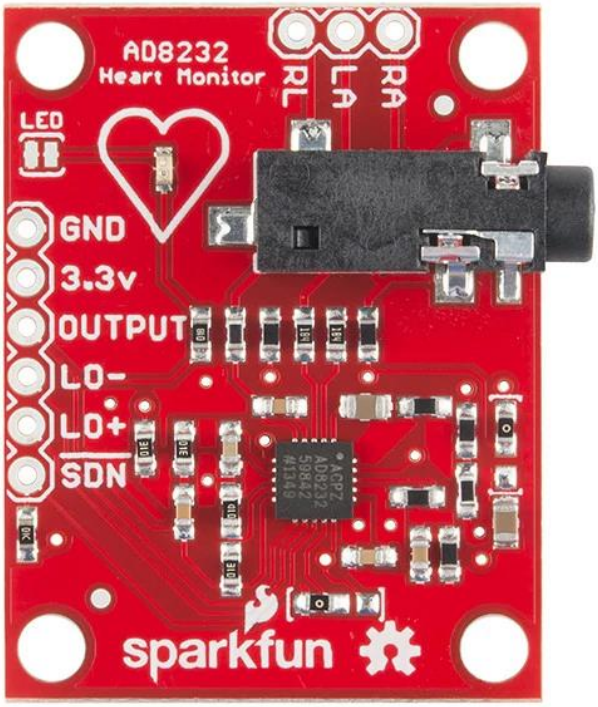
El algoritmo de cifrado implementado en el microcontrolador es el AES y este se encarga de brindar seguridad a cada una de las muestras adquiridas del sistema.

La unidad de almacenamiento en base de datos, se da por la transmisión realizada por el módulo WiFi, mientras la microSD guarda las muestras por medio de interfaz SDIO.

6.1.1 AQUISICIÓN SEÑAL ELECTROCARDIOGRÁFICA

Para adquirir la señal del corazón se emplea el dispositivo AD8232, el cual es un instrumento que se usa para llevar a cabo la medición de la actividad eléctrica del corazón. Este dispositivo es de fácil uso, ya que no requiere de soladuras o conectores adicionales puesto que este tiene amplificadores y filtros conectados en él. Contiene 3 electrodos que corresponden a RA (Brazo Derecho), LA (Brazo Izquierdo) y RL (Pierna Derecha) los cuales son conectados al cuerpo respectivamente.

FIGURA 6.2 AD8232



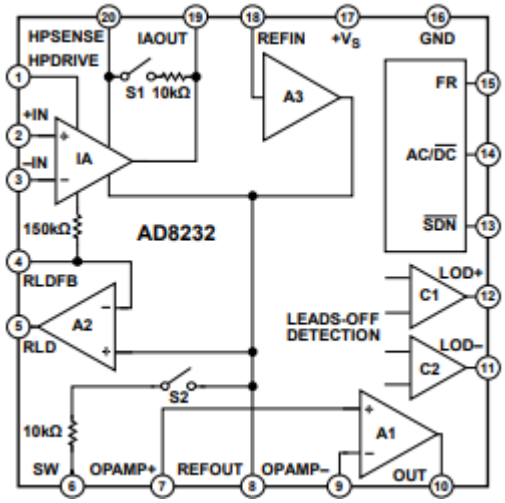
FUENTE: 330ohms Ad8232, recuperado el día 12 de marzo de 2020 [Online] Available: https://www.330ohms.com/products/monitor-de-ritmo-cardiaco-ad8232

El AD8232 está diseñado para extraer amplificar y filtrar pequeñas señales lo que permite que cualquier microcontrolador pueda interactuar fácilmente. Adicionalmente, este artefacto permite realizar el monitoreo de ritmo del corazón de manera portátil, siendo así muy útil para lo que se pretende desarrollar en este proyecto, además de su bajo costo, y fácil alimentación.

A continuación, se detalla la distribución de los pines que integran este dispositivo:

- GND: Este corresponde a la tierra de AD8232, se debe conectar a la tierra del microcontrolador.
- 3.3v: Es el pin de alimentación del dispositivo, se conecta al VCC del sistema embebido.
- OUTPUT: Mediante este pin salen los datos correspondientes a la señal amplificada a monitorear, es este pin al que se le debe realizar lectura mediante el conversor analógico digital (ADC) del microcontrolador en este caso el pin PA5.
- LO -: Detecta voltajes negativos. No se conecta
- LO+: Detecta voltajes positivos. No se conecta
- SDN: Controla el encendido del dispositivo. No se conecta
- PLUG: Es donde se conectan los electrodos para tomar la señal.

FIGURA 6.3 DIAGRAMA DE BLOQUES FUNCIONAMIENTO INTERNO AD8232



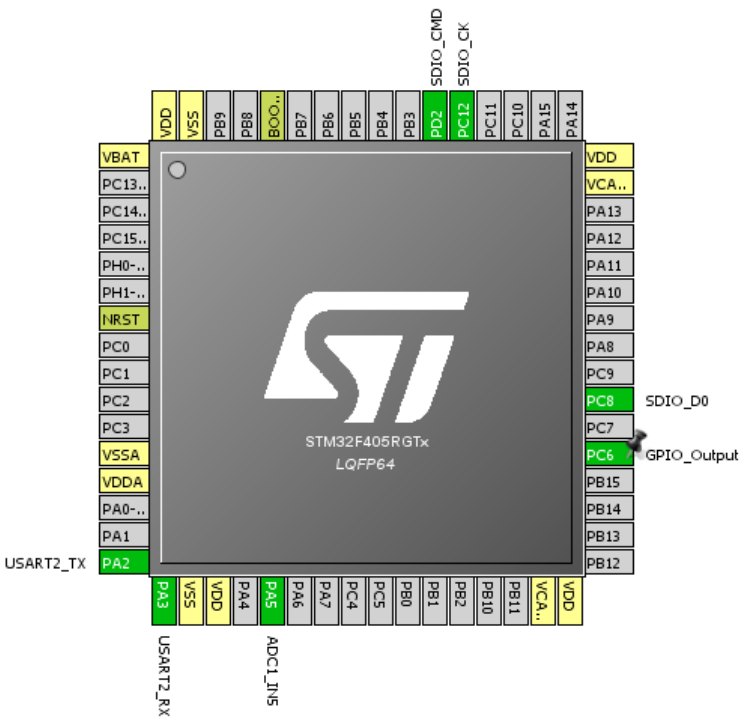
FUENTE: Functional Block Diagram AD8232. Recuperado el día 12 de abril de 2020 [Online] Available: https://www.analog.com/media/en/technical-documentation/data-sheets/AD8232.pdf

6.1.2 MICROCONTROLADOR STM32F405RG

ARM (Advanced RISC Machine) es, como su nombre lo indica, una arquitectura RISC (Reduced Instruction Set Computer) de 32 bits desarrollada por ARM Holdings, es decir son procesadores que permiten llevar a cabo un conjunto sencillo y reducido de instrucciones a un bajo nivel de consumo de energía.

El microcontrolador seleccionado para ejecutar las funciones de este proyecto es el STM32f405rg, el cual está basado en el alto rendimiento del procesador ARM Cortex M4 de 32 bits cuyo núcleo opera a una frecuencia máxima de 168MHz. Los dispositivos de esta familia tienen incorporados memorias embebidas de alta velocidad siendo estas, una memoria flash de 1Mbyte, una SRAM de 192Kbytes y un respaldo de 4Kbytes de SRAM. Adicionalmente, cuenta con un extenso rango de periféricos mejorados conectados a dos APB (Advance Peripheral Bus), tres AHB (AMBA High-performance Bus).

FIGURA 6.4 MICROCONTROLADOR STM32F405RG



FUENTE: AUTORES.

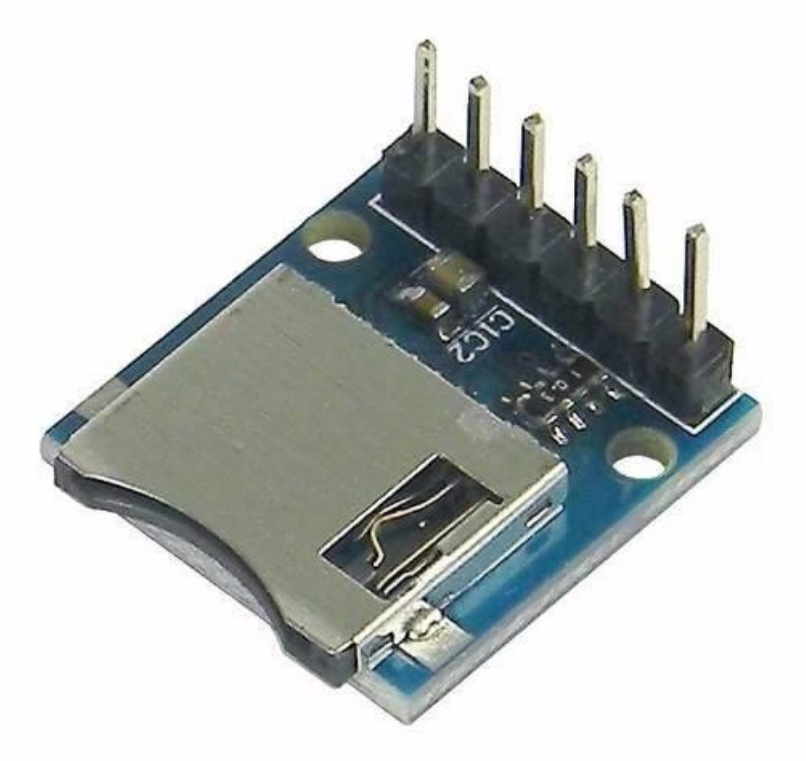
Este dispositivo ofrece 3 conversores analógico digital (ADC) de 12 bits cada uno, 2 conversores digital análogo (DAC), un reloj en tiempo real (RTC) de bajo consumo, 12 timers de propósito general de 16 bits incluyendo 2 timers de PWM para controlar motores, además de incluir más de 15 interfaces de comunicación estándar, entre ellas USART/UART e interfaz SDIO, los cuales fueron utilizados para el desarrollo de este proyecto de grado.

6.1.3 ALMACENAMIENTO DE DATOS LOCAL

Para el almacenamiento de los datos localmente se utilizó una micro SD, esto con la finalidad de que en caso de fallo en la red WiFi queden los datos aquí, siendo un respaldo del sistema.
Esta microSD se conectó al microcontrolador a través de interfaz de comunicación SDIO, la cual permite una fácil interacción entre dispositivos. Se utilizó un adaptador o módulo microSD que cuenta con los siguientes pines:

- GND: Se conecta a GND del microcontrolador
- 3.3v: Se conecta a la alimentación
- MISO/DAT0: Conector de datos se conecta al pin PC8 del microcontrolador.
- MOSI/CMD: Es la línea de comandos y se conecta al pin PD2 del Stm32f405
- CLK/SCLK: Corresponde al reloj y se conecta al pin PC12 de la tarjeta.
- CS: Chip Select, no se conecta ya que no se trabaja mediante protocolo SPI

FIGURA 6.5 MODULO MICROSD



FUENTE: Modulo Micro Sd Card 3v3 Arduino Pic Monarca Mona. Recuperado el día 12 de abril de 2020 [Online] Available: Https://Monarcaelectronica.Com.Ar/Productos/Modulo-Micro-Sd-Card-3v3-Arduino-Pic-Monarca-Mona/

6.1.4 MÓDULO WiFi ESP01

Es un dispositivo que trasmite y recibe señales WiFi, permitiendo conectar diversos artefactos a internet. Integra un potente procesador con arquitectura de 32 bits y está basado en el SoC (System on Chip) ESP8266. Este módulo viene cargado con el firmware AT y se puede trabajar bajo el entorno de desarrollo Arduino, permitiendo así el uso de diversas librerías que se pueden encontrar en internet, debido a que la comunidad de este medio es muy activa se da soporte a plataformas como ESP8266.

Algunas características que integran este dispositivo incluyen:

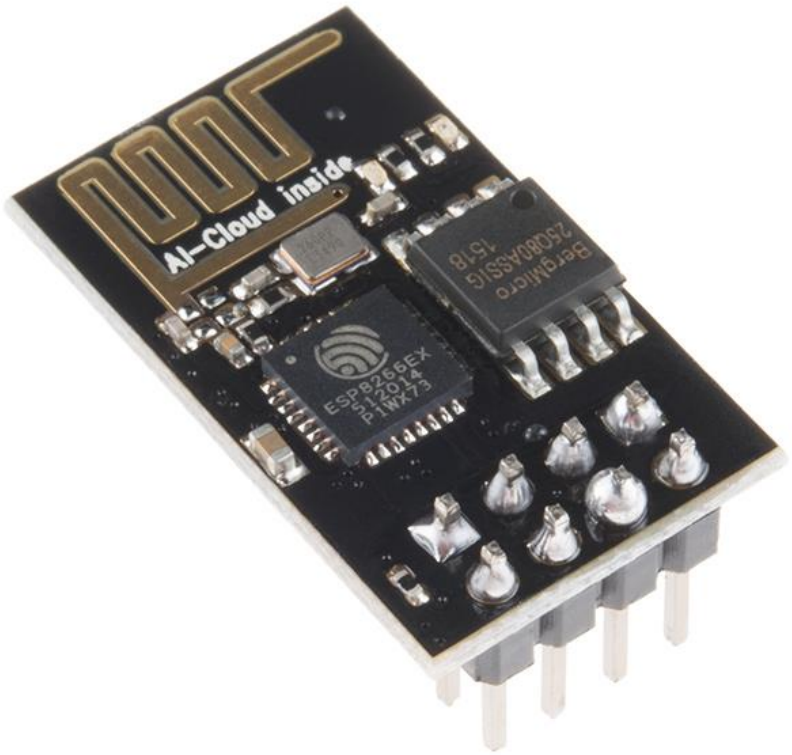
- Alimentación 3.3v
- Tipos de interfaces de comunicación integradas: Serial y UART.

- Wifi Directa punto a punto (P2P), Access Point.
- Stack TCP/IP integrado.

Los pines de este módulo se distribuyen de la siguiente manera:

- GND: Es la tierra del módulo y se conecta a tierra del circuito.
- GPIO2: Por default esta siempre en alto (3.3v). No se conecta.
- GPIO0: En Modo Operación Está en alto (3.3v, En modo Programación debe ir a tierra. No se conecta.
- Rx: Se conecta al pin PA2 del microcontrolador que corresponde a Tx.
- Tx: Se conecta al pin PA3 del microcontrolador, es decir, Rx.
- CH_PD: Este pin debe estar en alto para que el módulo opere, por lo tanto, se conecta a la alimentación (VCC) del circuito.
- Vcc: Es el pin de alimentación del dispositivo, por lo que se conecta a los 3.3v que se suministran al microcontrolador.

FIGURA 6.6 MODULO ESP01



FUENTE: ESP8266 – ESP-01 – Módulo Transceptor WiFi Serial. Recuperado el día 12 de abril de 2020 [Online] Available: Https://Electronilab.Co/Tienda/Esp8266-Modulo-Wifi-Serial-Transceptor/

El módulo puede trabajar en 2 modos: como estación Wifi (Wifi Station), donde se conecta a una red WiFi predeterminada, se asigna SSID y contraseña solo trabajara bajo dicha red o como Punto de Acceso (Access Point), el cual se usa si quiere crear una red propia en el chip y así conectarse directamente a la red más cercana o a la que se pueda tener acceso en ese momento.

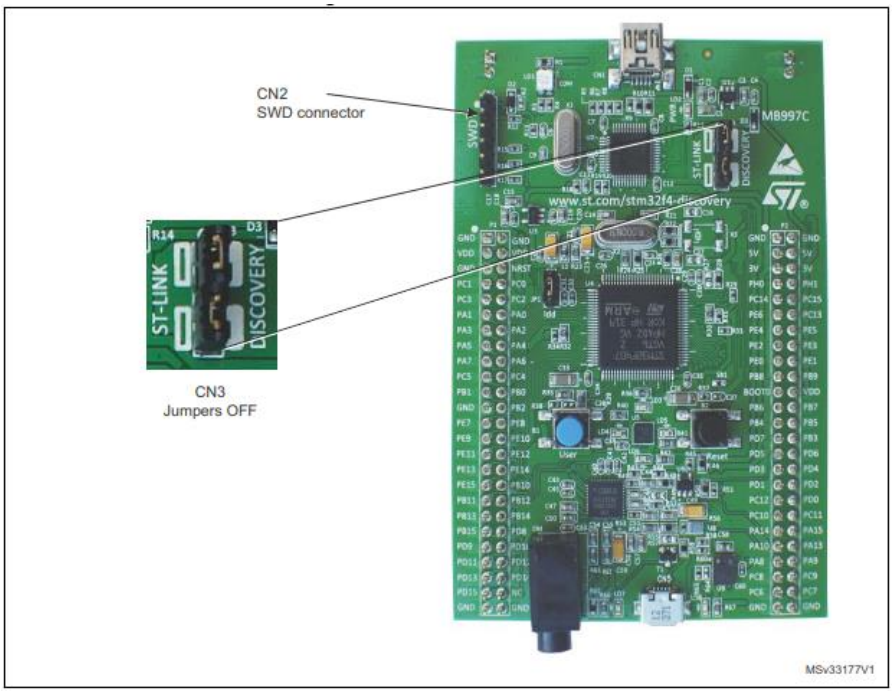
6.1.5 TARJETA DISCOVERY STM32F407 COMO PROGRAMADOR

Esta tarjeta de desarrollo está basada en la familia de microcontroladores STM32F4xx el cual cuenta con procesadores ARM M4-Cortex y cuenta con las mismas características del microcontrolador Stm32f405, pero al ser una tarjeta de desarrollo o un kit de demostración la empresa STM integra ciertos componentes que permiten aprovechar al 100% la capacidad de este microcontrolador. Dentro de estos componentes integrados se encuentra un programador SWD, el cual se utiliza en este proyecto para transferir programas desde el ambiente de desarrollo integrado Keil uVision.
Para poder acceder al programador se debe realizar la conexión mediante un conector integrado que lleva por nombre CN2 connector en la tarjeta y cuyos pines se distribuyen como sigue:

- VDD: Es el VDD de la tarjeta, por lo que se debe conectar al VCC del microcontrolador
- SWDCLK: Es la señal de reloj y se conecta al pin PA14 del microcontrolador
- GND: Es la tierra del programador y va a la tierra del sistema.
- SWDIO: Es el pin que proporciona entrada y salida de datos entre programador y microcontrolador, se conecta al pin PA13 del microcontrolador.
- NRST: Corresponde al Reset del microcontrolador, por lo cual se conecta al pin NRST.
- SWO: Este pin es reservado, por lo tanto, no se conecta.

Por último, se debe retirar los jumpers que se encuentran conectados en la tarjeta de desarrollo en el conector CN3, ya que estos son los encargados de comunicar el programador con el microcontrolador integrado en la tarjeta. Es decir, conectados los jumpers se programa el microcontrolador integrado en la discovery, retirados los jumpers se programa un microcontrolador externo, como se muestra en la figura 6.7.

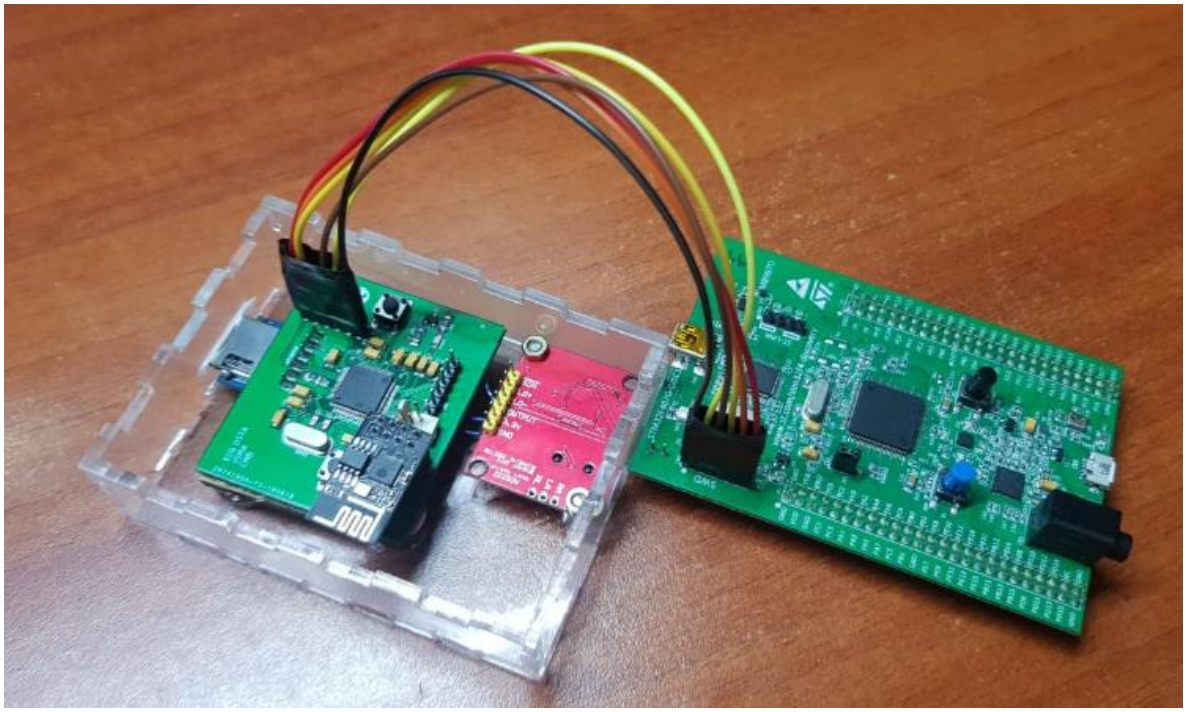
FIGURA 6.7 STM32F407VG COMO PROGRAMADOR



FUENTE: STMicrocontrollers. Discovery Kit with Stm32f407vg Mcu Um1472 User Manual. Recuperado el día 12 de abril de 2020 [Online] Available: https://www.st.com/resource/en/user_manual/dm00039084-discovery-kit-with-stm32f407vg-mcu-stmicroelectronics.pdf

A continuación, se presenta la figura 6.8 donde se evidencia la conexión entre el microcontrolador diseñado y la tarjeta Discovery STM32F407VG como programador

FIGURA 6.8 STM32F407VG COMO PROGRAMADOR CONECTADO AL MICROCONTROLADOR DISEÑADO

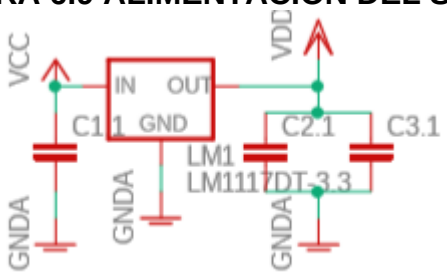


FUENTE: AUTORES

6.1.6 ALIMENTACIÓN DEL SISTEMA

Para generar el voltaje de 3.3v necesario para alimentar cada uno de los componentes que integran este proyecto, se utiliza el regulador de voltaje LM1117. Este tiene la capacidad de entregar 800mA. Debido al consumo que requieren dispositivos como el microcontrolador o el módulo WiFi, se opta por este regulador para no tener inconvenientes por falta de corriente.
Para obtener el voltaje de 3.3v deseado, se configura de la siguiente forma:

FIGURA 6.9 ALIMENTACIÓN DEL SISTEMA



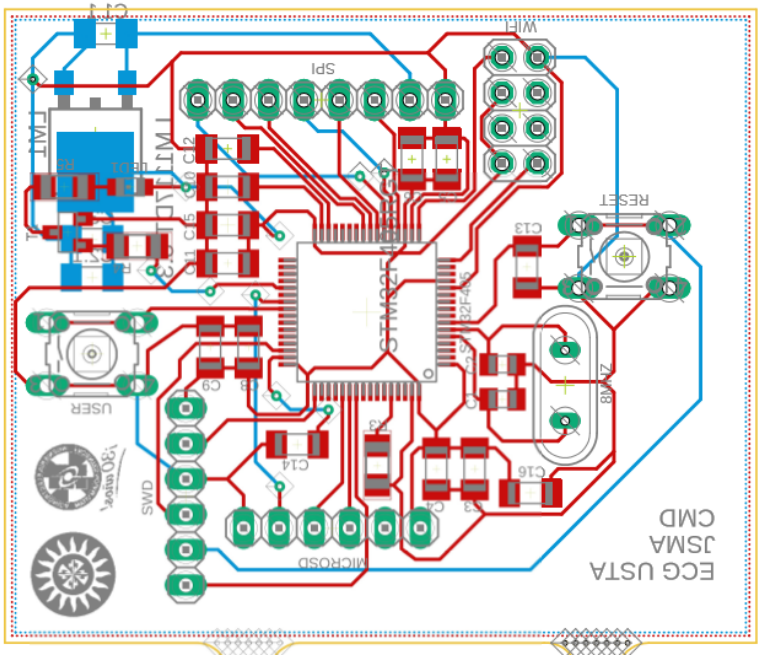
FUENTE: AUTORES

Donde:
C1 = 100nf
C2= 10uf
C3=100nf.
VCC= Voltaje de entrada de 5 a 15 voltios.
VDD= Voltaje de salida 3.3v.

6.1.7 DISEÑO PCB

A continuación, la figura 6.10 muestra el diseño final de la placa donde se integran el regulador 1117, el microcontrolador, la micro SD, el módulo WiFi y los pines donde se conectará el AD8232.

FIGURA 6.10 PCB FINAL



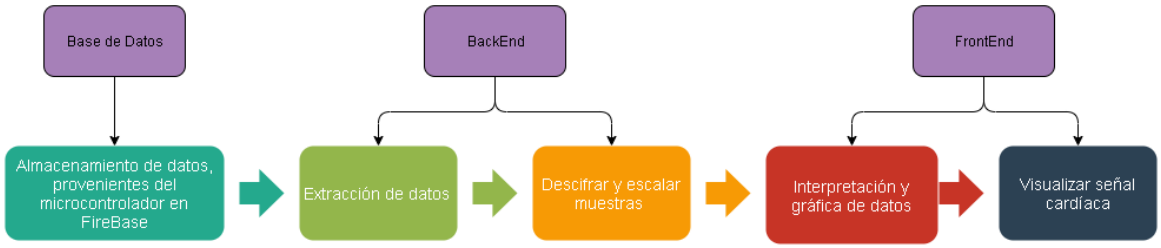
FUENTE: AUTORES

El diseño anterior se llevó a cabo siguiendo la guía de usuario "*Getting started with STM32F4xxxx MCU hardware development*" que proporciona STM para todos aquellos que desean realizar sus diseños propios manejando sus microcontroladores, se siguen las indicaciones de la sección POWER SUPPLY SCHEMES para la correcta inicialización del microcontrolador.

Después de cumplir con los requerimientos básicos de inicialización del microcontrolador, se realizan las conexiones de los diferentes elementos que conforman el circuito impreso.

6.2 SOFTWARE

FIGURA 6.11 DIAGRAMA DE BLOQUES FUNCIONAMIENTO SOFTWARE



FUENTE: AUTORES

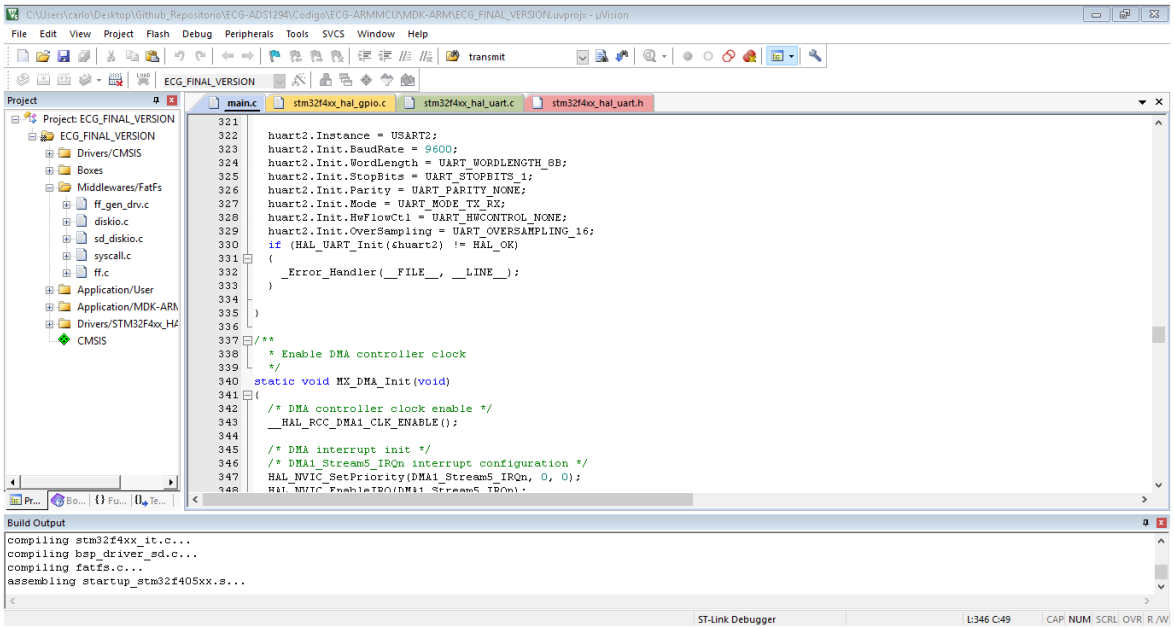
La imagen anterior representa el funcionamiento de software del sistema. Primero el almacenamiento de las muestras remotamente, pasando por la extracción desde la base de datos, el descifrado e interpretación de los datos para llevar a acabo su posterior visualización en la interfaz.

6.2.1 KEIL uVISION

Keil uVision es un ambiente de desarrollo integrado (IDE) gratuito, desarrollado por la empresa alemana Keil Elektronik GmbH, actualmente propiedad de ARM. Este software combina manejo de proyectos, edición de códigos fuente, ejecución de programas y más, en un solo ambiente.

El editor de código integrado de Keil uVision, incluye todas las características modernas de un editor de código fuente, como subrayar errores de sintaxis, sangría en texto, entre otros. A continuación, una muestra del editor en la figura 6.12.

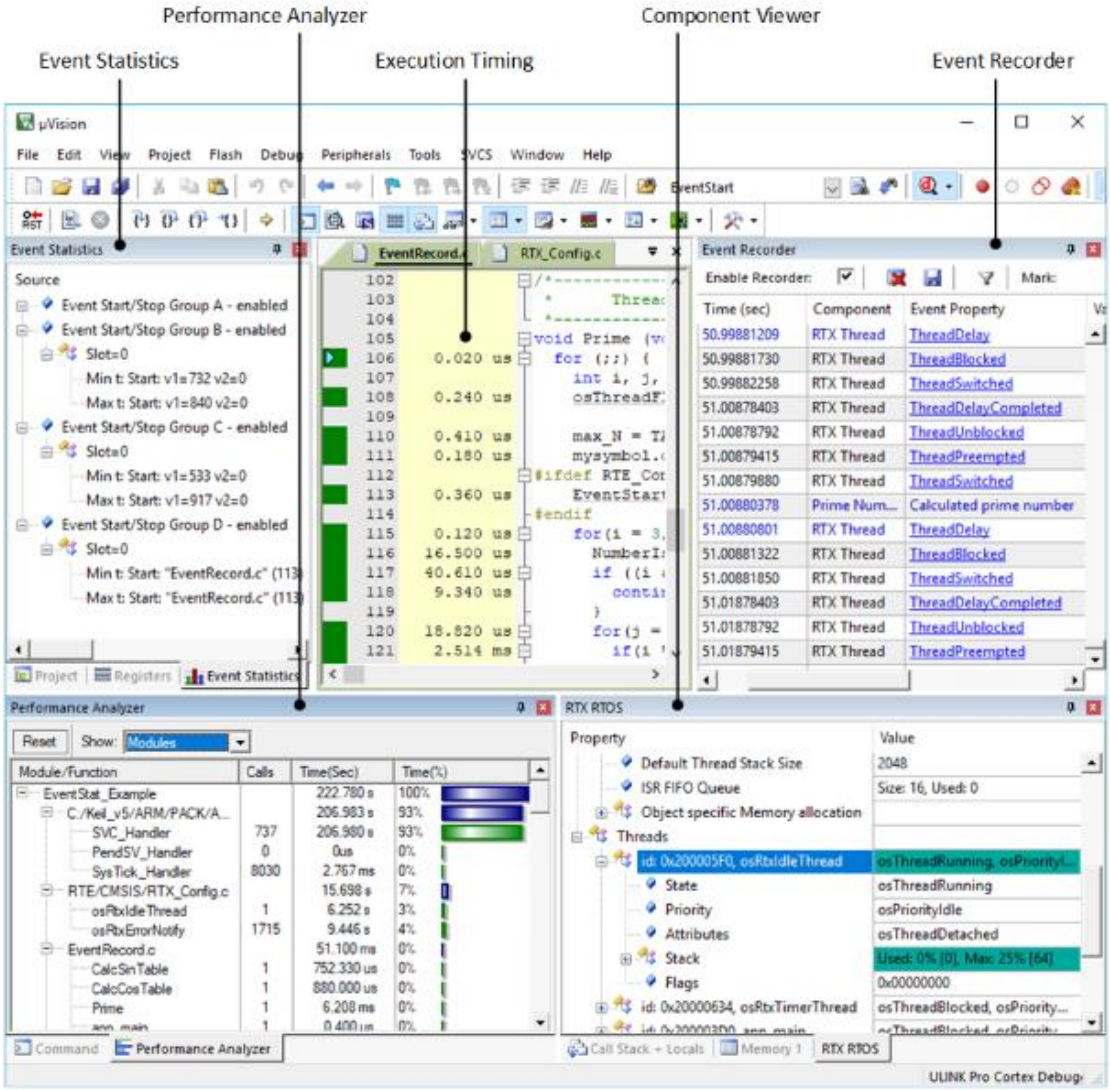
FIGURA 6.12 KEIL UVISION EDITOR DE CODIGO



FUENTE: AUTORES

Keil uVision, contiene un “debugger” en el cual se puede probar, verificar y optimizar el código de usuario, esto se logra gracias a que dicho “debugger” cuenta con características tradicionales de ejecución como breakpoint, ejecuciones paso a paso, ventana de monitoreo de variables y una completa visibilidad de los dispositivos conectados a los periféricos, como se puede apreciar a continuación.

FIGURA 6.13 KEIL UVISION DEBUGGER



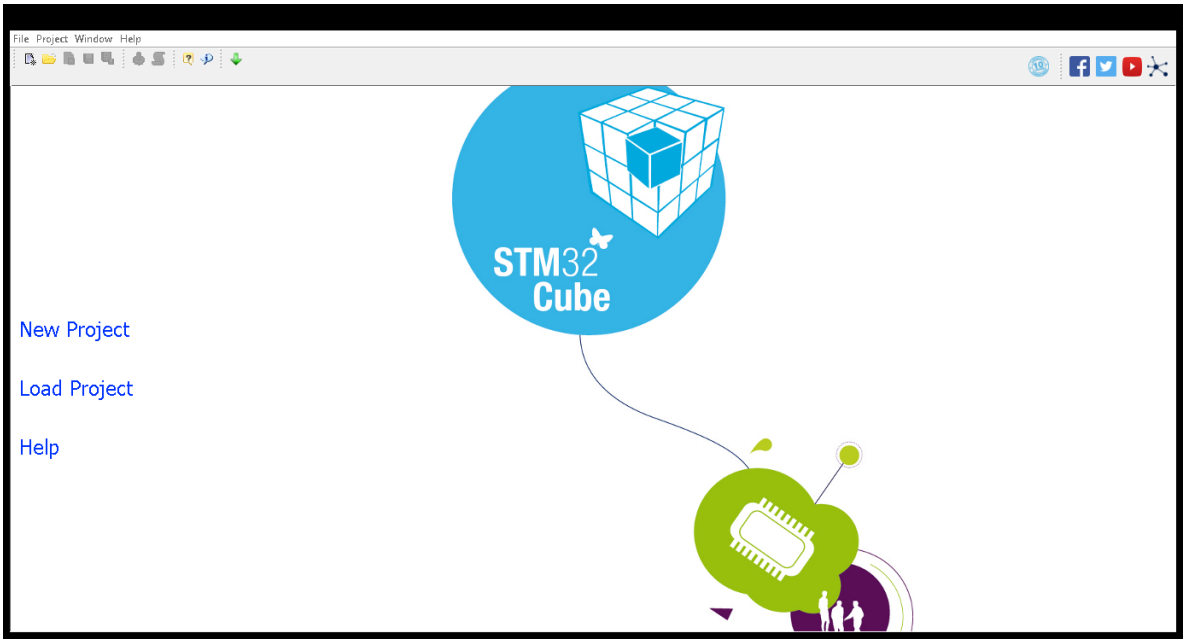
FUENTE: ARM KEIL, ARM LIMITED, µVision® Debugger**.** Recuperado el día 12 de abril de 2020 [Online] Available: http://www2.keil.com/mdk5/Debug/

Esta herramienta además de todas las facilidades descritas previamente permite programar todos los microcontroladores que estén basados en procesadores ARM, es por esta razón que se designa este software para transferir el código fuente al microcontrolador STM32F405RG.

6.2.2 STM32CubeMX

STM32CubeMX, es un software de la empresa ST que proporciona las herramientas necesarias para generar el código fuente en el ambiente de desarrollo (IDE) donde se va a realizar el proyecto, en este caso Keil.
Esta plataforma se utiliza únicamente para generar el proyecto, es decir, se emplea para la inclusión de las librerías necesarias, asignación de los roles que tendrán cada uno de los pines del dispositivo, configuración de los relojes y demás parámetros de relevancia del microcontrolador para garantizar su buen funcionamiento según lo requiera el proyecto.

FIGURA 6.14 STM32CUBEMX



FUENTE: AUTORES

6.2.3 ARDUINO IDE

Arduino IDE es el entorno de desarrollo en el que se lleva a cabo la programación de las placas o tarjetas de desarrollo de Arduino. En este proyecto se utiliza este software como medio de programación del módulo WiFi ESP01, ya que como se explica en la sección 6.1.4 al ser esta comunidad muy activa se puede acceder a muchas librerías y ejemplos que permiten brindarles soporte a las plataformas de ESP8266, que es el dispositivo sobre el cual está basado el módulo ESP01.

6.2.4 ALMACENAMIENTO REMOTO CON FIREBASE

Firebase es una plataforma que ofrece un conjunto de herramientas orientadas a la creación de aplicaciones de alta calidad, este proyecto se centra en probablemente una de sus mejores herramientas ofrecidas por este software, la base de datos Realtime. En ella se pueden guardar todos los datos que requiere el aplicativo.
Al ser una base de datos no relacional los datos son almacenados en formato Json y pueden ser actualizados en tiempo real a partir de APIs diseñadas específicamente para la herramienta. Como se explica en la sección anterior 6.2.3, el IDE de desarrollo para el módulo ESP8266 es Arduino, por lo tanto, para la conexión con la plataforma de firebase se usó la librería firebase-arduino que permite generar request o peticiones desde el módulo wifi para el almacenamiento de los datos capturados.

6.2.5 INTERFAZ GRÁFICA DE USUARIO

Con el objetivo del procesamiento, desencriptación y visualización de los datos capturados por el dispositivo, se desarrolló una aplicación que consta de dos capas esenciales en la construcción de un sitio web. La capa de datos desarrollada en un Framework de Python llamado Flask y la capa de presentación desarrollada en un Framework de HTML llamado Angular.

6.2.6 PYTHON COMO BACKEND DE PROCESAMIENTO DE DATOS

Python es un lenguaje de programación interpretado, por lo que funciona en cualquier tipo de sistema que integre su interpretador a parte es multiplataforma y multiparadigma perfecto para el desarrollo de la aplicación web, cuenta con una gran ventaja y es su extenso número de librerías y frameworks que pueden facilitarle la vida a un desarrollador. En esta ocasión se hará uso de un framework y dos librerías principalmente para el desarrollo de la plataforma:

Flask:
Flask es un microframework escrito en Python, es catalogado como microframework debido a que no requiere herramientas o bibliotecas particulares para su uso. No posee capa de abstracción de base de datos, validación de formularios ni ningún otro componente que hagan complejo su manejo, esto permitirá que el código funcione como una API web para el procesamiento de los datos del dispositivo.

Pyrebase
La librería Pyrebase es un contenedor sencillo escrito en Python que proporcionará métodos para la conexión con la base de datos Firebase. Esta es compatible con múltiples servicios, entre ellos Realtime Database, donde se alojan todos los datos capturados por el dispositivo.

PyCryptodome
Al ser el microcontrolador Stm32f405 directamente el encargado de encriptar los datos después de capturarlos vía AD8232, se opta por realizar el método de descifrado por medio de una plataforma cuya simplicidad, versatilidad y rapidez de desarrollo de código, permitan realizar este proceso sin mayor inconveniente. Para esta tarea se usó la librería PyCryptodome, un paquete de módulos autónomos que es compatible con la mayoría de los métodos criptográficos de bajo nivel, esta herramienta servirá para desencriptar los datos almacenados en la base de datos para su posterior procesamiento y visualización.
Implementar el código de descifrado por medio de esta librería resulta realmente sencillo, ya que, gracias a la extensa documentación y soporte por medio de foros, bastaran un par de líneas de comando para que se haga efectivo el cifrado o descifrado de datos.

El uso de las herramientas anteriormente listadas permite el desarrollo de un aplicativo que se acomoda a las necesidades del proyecto, por medio de ellas se logró la implementación de un BackEnd capaz de conectarse a la base de datos, obtener los datos allí almacenados, desencriptarlos y posteriormente enviárselos al FrontEnd para la visualización de estos.

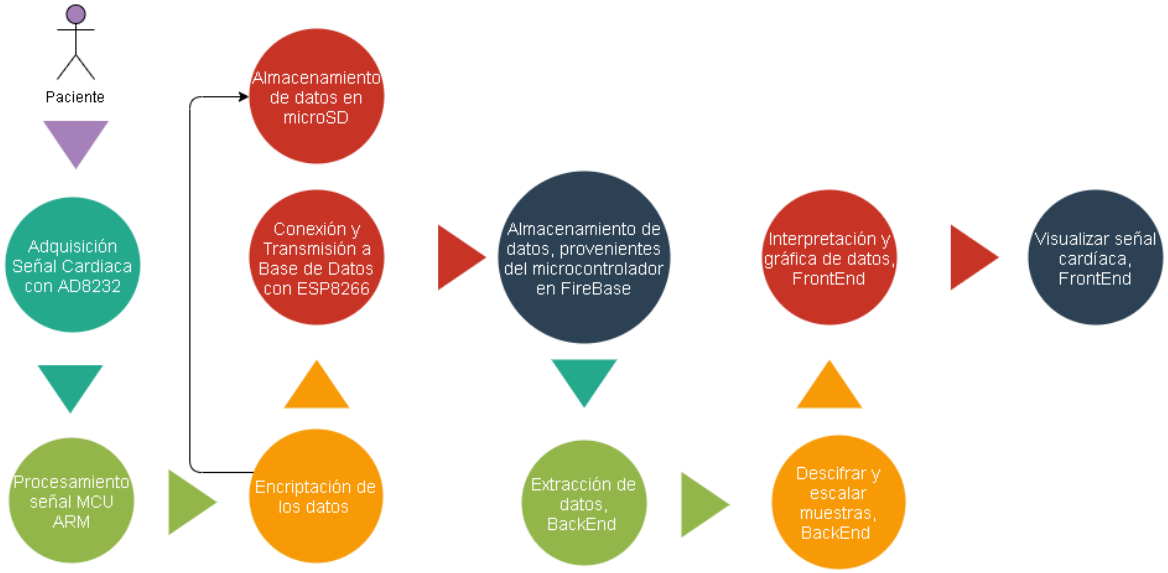
6.2.7 ANGULAR COMO FRONTEND DE VISUALIZACION DE DATOS

Angular es un framework para aplicaciones web desarrollado en Typescript un lenguaje de código abierto que tiene soporte directo de Google, su objetivo principal es aumentar las aplicaciones basadas en modelo vista controlador (MVC) para hacer el desarrollo y testing de una manera más sencilla. Angular se basa en clases tipo componentes, las cuales poseen propiedades y métodos de manera convencional.
Para la visualización de datos capturados por el dispositivo se usó una librería llamada Highcharts, Esta librería es una biblioteca de gráficos basada en Javascript con propiedades configurables a partir de formatos JSON. Admite una amplia gama de tipos de gráficos de forma predeterminada, en esta ocasión se utilizó un gráfico de tipo línea para la visualización de la señal ECG anteriormente desencriptada y procesada por el BackEnd.

7. RESULTADOS

Culminado el diseño e implementación del sistema, se procede a realizar las pruebas pertinentes que puedan evidenciar el correcto funcionamiento del prototipo en cuanto a adquisición de la señal electrocardiográfica, cifrado, transmisión, almacenamiento remoto, descifrado y posterior visualización de los datos mediante la interfaz de usuario.

FIGURA 7.1 DIAGRAMA DE BLOQUES SISTEMA INTEGRADO



FUENTE: AUTORES

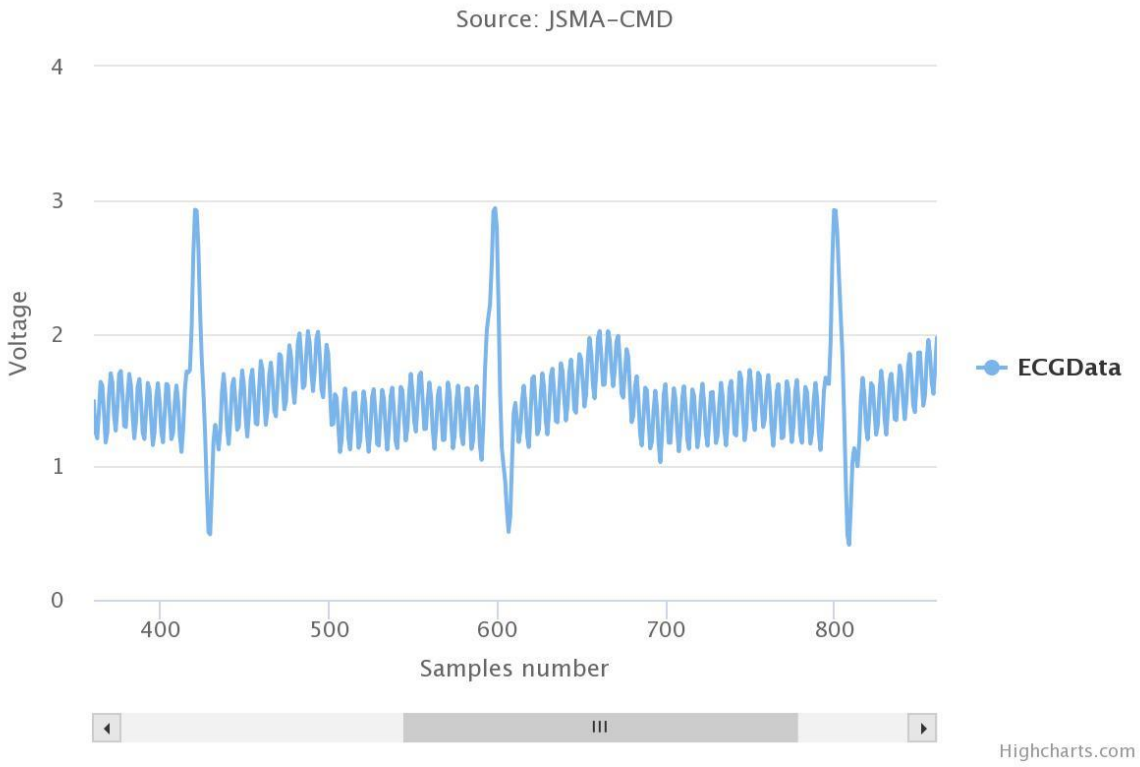
7.1 PRUEBAS DE FUNCIONAMIENTO

A continuación, se presentarán los resultados obtenidos de las pruebas realizadas en: cifrado de datos, transmisión a base de datos, almacenamiento en microSD y adquisición de muestras.

PRUEBAS DE ADQUISICIÓN:

Para esta prueba se llevó a cabo la conexión del integrado AD8232 a un pin del microcontrolador configurado como conversor analógico digital, se almacenaron los datos en un arreglo y se realizó la conversión de las muestras entrantes de 12 bits (0 a 4096) a valores de voltaje entre 0 y 3 voltios. posteriormente, se grafican los datos almacenados en el arreglo y se obtiene el siguiente resultado.

FIGURA 7.2 PRUEBA ADQUISICIÓN DE DATOS



FUENTE: AUTORES

Como se puede apreciar, la imagen anterior muestra el comportamiento del corazón captado con el integrado AD8232. La frecuencia de muestreo que se utiliza para examinar la señal cardiaca, es la recomendada por la Asociación americana del corazón, la cual es de 500 SPS (Samples per second).

PRUEBAS DE TRASMISIÓN:

Con el fin de comprobar que los datos quedaran almacenados en base de datos de manera correcta, se desarrollaron las siguientes pruebas para corroborar el buen funcionamiento del sistema en cuanto a trasmisión de datos.
La primera prueba consistió en elaborar un ciclo for de 0 a 255 donde se concatenó en un arreglo el valor de la iteración correspondiente y en cada iteración se trasmitió este vector, obteniendo así el siguiente resultado:

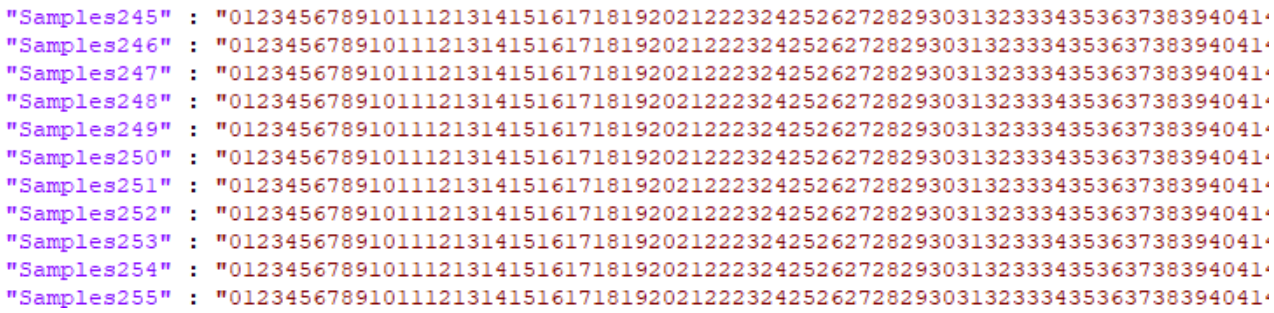
FIGURA 7.3 PRUEBA 1 DE TRASMISIÓN


```
"Samples1" : "",
"Samples2" : "01",
"Samples3" : "012",
"Samples4" : "0123",
"Samples5" : "01234",
"Samples6" : "012345",
"Samples7" : "0123456",
"Samples8" : "01234567",
"Samples9" : "012345678",
"Samples10" : "0123456789",
"Samples11" : "012345678910",
"Samples12" : "01234567891011",
"Samples13" : "0123456789101112",
"Samples14" : "012345678910111213",
"Samples15" : "01234567891011121314",
"Samples16" : "0123456789101112131415",
"Samples17" : "012345678910111213141516",
"Samples18" : "01234567891011121314151617",
"Samples19" : "0123456789101112131415161718",
"Samples20" : "012345678910111213141516171819",
"Samples21" : "01234567891011121314151617181920",
"Samples22" : "0123456789101112131415161718192021",
"Samples23" : "012345678910111213141516171819202122",
"Samples24" : "01234567891011121314151617181920212223",
"Samples25" : "0123456789101112131415161718192021222324",
"Samples26" : "012345678910111213141516171819202122232425",
"Samples27" : "",
"Samples28" : "01234567891011121314151617181920212223242526 27",
"Samples29" : "012345678910111213141516171819202122232425262728",
"Samples30" : "0123456789101112131415161718192021222324252627 2829",
"Samples31" : "012345678910111213141516171819202122232425262728293 30",
"Samples32" : "01234567891011121314151617181920212223242526272829303 1",
"Samples33" : "012345678910111213141516171819202122232425262728293031 32",
"Samples34" : "0123456789101112131415161718192021222324252627282930313233",
"Samples35" : "01234567891011121314151617181920212223242526272829303132333 4",
"Samples36" : "012345678910111213141516171819202122232425262728293031323334 35",
```


FUENTE: AUTORES

Los datos mostrados en la imagen anterior corresponden a los valores almacenados remotamente en la base de datos durante esta prueba, como se puede ver el arreglo aumenta dinámicamente hasta alcanzar el valor de 255.
En total se realizaron 255 trasmisiones de las cuales hubo fallas en la muestra 27 como se evidencia en la ilustración. Este rechazo se debió a que los datos en dicha muestra no respetaban las condiciones necesarias para llevar a cabo el descifrado, es decir, los datos estaban corruptos y el algoritmo los rechazó no almacenándolos en base de datos. A continuación, una muestra más amplia de las trasmisiones realizadas.

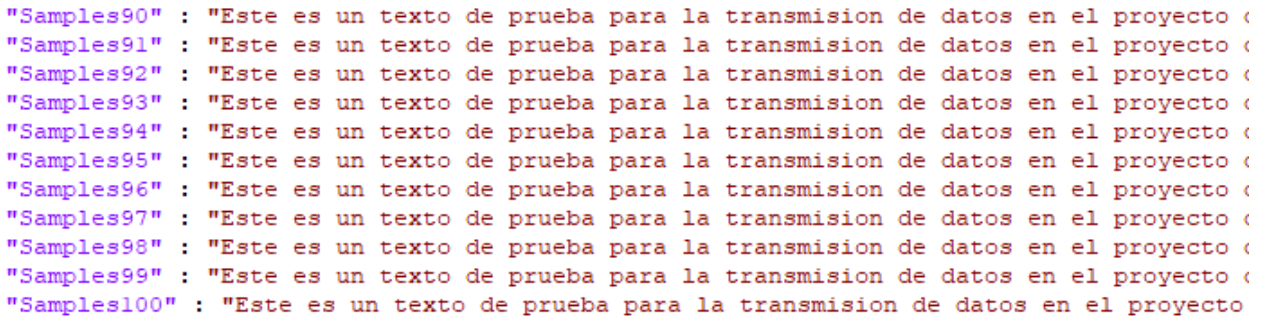
FIGURA 7.4 PRUEBA 1 DE TRASMISIÓN



FUENTE: AUTORES

La segunda prueba consistió en la trasmisión de la cadena de caracteres "Este es un texto de prueba para la transmisión de datos en el proyecto de grado Diseño e implementación de un sistema de adquisición de señales electrocardiográficas con almacenamiento remoto de datos encriptados desarrollado por Juan Sebastián Munar Aldana y Carlos Eduardo Moreno Doria de la facultad de Ingeniería Electrónica de la universidad Santo Tomas en Bogotá, Colombia. Asesorada por Jaime Vitola" un número determinado de veces, obteniendo el siguiente resultado:

FIGURA 7.5 PRUEBA 2 DE TRASMISIÓN



FUENTE: AUTORES

Esta cadena se trasmitió un total de 100 veces de las cuales llegaron correctamente 98 y se presentó falló en las trasmisiones 1 y 46, el texto llegó incompleto en estas iteraciones.

PRUEBAS DE CIFRADO:

Para estas pruebas se configuró un arreglo con la cadena de caracteres “Este es un texto de prueba para la encripcion de datos con algoritmo AES del proyecto de grado Diseño e implementación de un sistema de adquisición de señales

electrocardiográficas con almacenamiento remoto de datos encriptados desarrollado por Juan Sebastián Munar Aldana y Carlos Eduardo Moreno Doria de la facultad de Ingeniería Electrónica de la universidad Santo Tomas en Bogotá, Colombia. Asesorada por Jaime Vitola" y se pasó por el algoritmo de cifrado AES implementado en el microcontrolador. Posteriormente, se comparó el resultado con la herramienta de encriptación online "aes.online-domain-tools" para determinar si el algoritmo realmente funcionó como se esperaba, obteniendo lo siguiente:

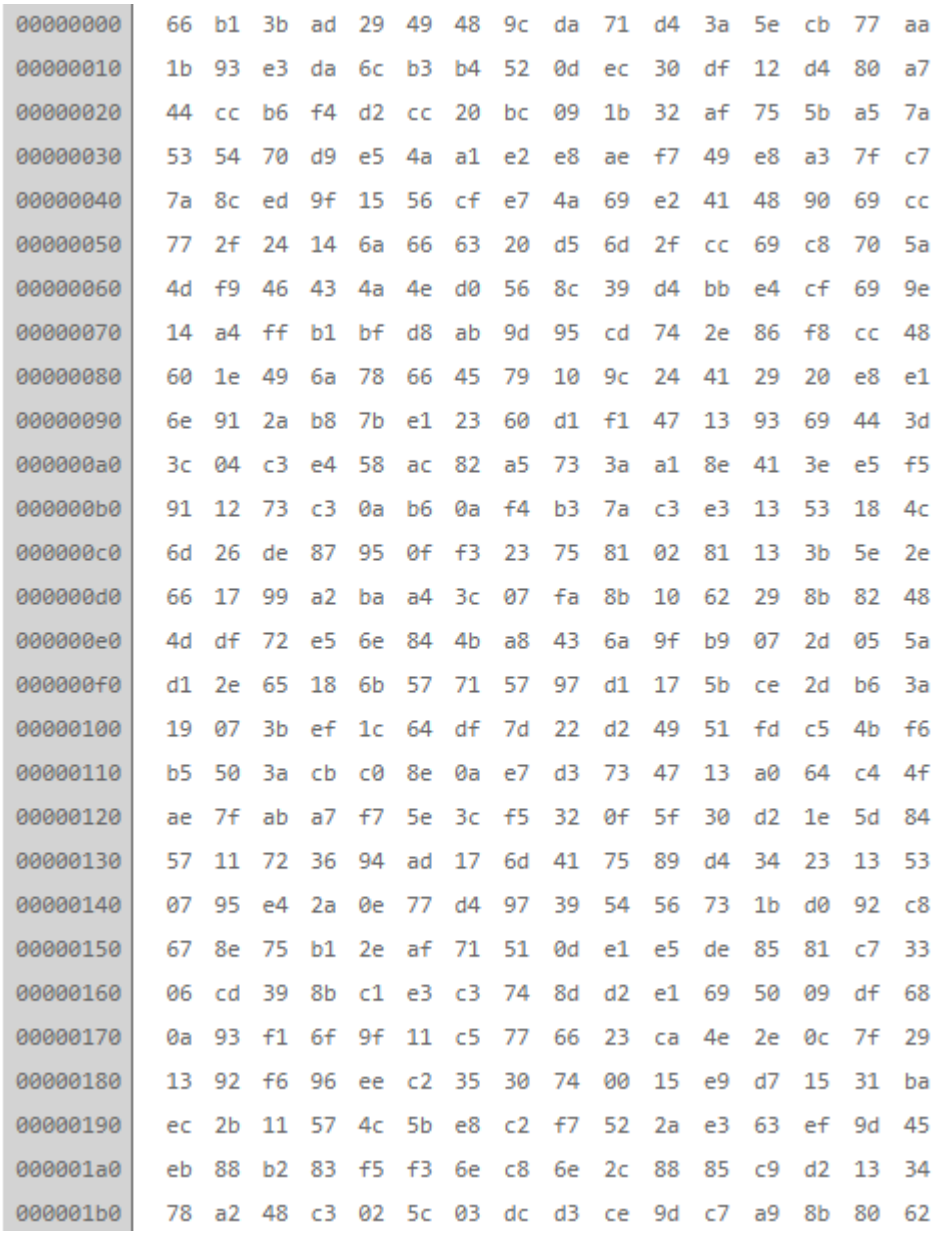
FIGURA 7.6 PRUEBA DE CIFRADO CON ALGORITMO AES EN MICROCONTROLADOR

```
66B13BAD2949489CDA71D43A5ECB77AA
1B93E3DA6CB3B4520DEC30DF12D480A7
44CCB6F4D2CC20BC091B32AF755BA57A
535470D9E54AA1E2E8AEF749E8A37FC7
7A8CED9F1556CFE74A69E241489069CC
772F24146A666320D56D2FCC69C8705A
4DF946434A4ED0568C39D4BBE4CF699E
14A4FFB1BFD8AB9D95CD742E86F8CC48
601E496A78664579109C24412920E8E1
6E912AB87BE12360D1F147139369443D
3C04C3E458AC82A5733AA18E413EE5F5
911273C30AB60AF4B37AC3E31353184C
6D26DE87950FF32375810281133B5E2E
661799A2BAA43C07FA8B1062298B8248
4DDF72E56E844BA8436A9FB9072D055A
D12E65186B57715797D1175BCE2DB63A
19073BEF1C64DF7D22D24951FDC54BF6
B5503ACBC08E0AE7D3734713A064C44F
AE7FABA7F75E3CF5320F5F30D21E5D84
5711723694AD176D417589D434231353
0795E42A0E77D497395456731BD092C8
678E75B12EAF71510DE1E5DE8581C733
06CD398BC1E3C3748DD2E1695009DF68
0A93F16F9F11C5776623CA4E2E0C7F29
1392F696EEC23530740015E9D71531BA
EC2B11574C5BE8C2F7522AE363EF9D45
EB88B283F5F36EC86E2C8885C9D21334
78A248C3025C03DCD3CE9DC7A98B8062
```

FUENTE: AUTORES

La imagen anterior ilustra los datos cifrados en hexadecimal de la cadena definida previamente con el algoritmo AES implementado en el microcontrolador

FIGURA 7.7 PRUEBA DE CIFRADO CON ALGORITMO AES DE LA HERRAMIENTA ONLINE AES.ONLINE-DOMAIN-TOOLS



00000000	66	b1	3b	ad	29	49	48	9c	da	71	d4	3a	5e	cb	77	aa
00000010	1b	93	e3	da	6c	b3	b4	52	0d	ec	30	df	12	d4	80	a7
00000020	44	cc	b6	f4	d2	cc	20	bc	09	1b	32	af	75	5b	a5	7a
00000030	53	54	70	d9	e5	4a	a1	e2	e8	ae	f7	49	e8	a3	7f	c7
00000040	7a	8c	ed	9f	15	56	cf	e7	4a	69	e2	41	48	90	69	cc
00000050	77	2f	24	14	6a	66	63	20	d5	6d	2f	cc	69	c8	70	5a
00000060	4d	f9	46	43	4a	4e	d0	56	8c	39	d4	bb	e4	cf	69	9e
00000070	14	a4	ff	b1	bf	d8	ab	9d	95	cd	74	2e	86	f8	cc	48
00000080	60	1e	49	6a	78	66	45	79	10	9c	24	41	29	20	e8	e1
00000090	6e	91	2a	b8	7b	e1	23	60	d1	f1	47	13	93	69	44	3d
000000a0	3c	04	c3	e4	58	ac	82	a5	73	3a	a1	8e	41	3e	e5	f5
000000b0	91	12	73	c3	0a	b6	0a	f4	b3	7a	c3	e3	13	53	18	4c
000000c0	6d	26	de	87	95	0f	f3	23	75	81	02	81	13	3b	5e	2e
000000d0	66	17	99	a2	ba	a4	3c	07	fa	8b	10	62	29	8b	82	48
000000e0	4d	df	72	e5	6e	84	4b	a8	43	6a	9f	b9	07	2d	05	5a
000000f0	d1	2e	65	18	6b	57	71	57	97	d1	17	5b	ce	2d	b6	3a
00000100	19	07	3b	ef	1c	64	df	7d	22	d2	49	51	fd	c5	4b	f6
00000110	b5	50	3a	cb	c0	8e	0a	e7	d3	73	47	13	a0	64	c4	4f
00000120	ae	7f	ab	a7	f7	5e	3c	f5	32	0f	5f	30	d2	1e	5d	84
00000130	57	11	72	36	94	ad	17	6d	41	75	89	d4	34	23	13	53
00000140	07	95	e4	2a	0e	77	d4	97	39	54	56	73	1b	d0	92	c8
00000150	67	8e	75	b1	2e	af	71	51	0d	e1	e5	de	85	81	c7	33
00000160	06	cd	39	8b	c1	e3	c3	74	8d	d2	e1	69	50	09	df	68
00000170	0a	93	f1	6f	9f	11	c5	77	66	23	ca	4e	2e	0c	7f	29
00000180	13	92	f6	96	ee	c2	35	30	74	00	15	e9	d7	15	31	ba
00000190	ec	2b	11	57	4c	5b	e8	c2	f7	52	2a	e3	63	ef	9d	45
000001a0	eb	88	b2	83	f5	f3	6e	c8	6e	2c	88	85	c9	d2	13	34
000001b0	78	a2	48	c3	02	5c	03	dc	d3	ce	9d	c7	a9	8b	80	62

FUENTE: AUTORES

La imagen anterior representa los datos cifrados de la cadena definida previamente con el algoritmo AES implementado en la utilidad online “aes.online-domain-tools”.

Para ambas pruebas, tanto la del algoritmo diseñado en el microcontrolador como en la herramienta online, se toman la misma cantidad de datos y se procede a comparar los resultados obtenidos línea por línea para validar si el diseño del algoritmo implementado es correcto.
Como se evidencia en las figuras 7.6 y 7.7 las muestras encriptadas coinciden en cada una de las líneas registradas, obteniendo así el resultado esperado para poder realizar encriptación de datos desde el microcontrolador.

PRUEBAS DE ALMACENAMIENTO EN MICROSD:

Esta prueba se realizó almacenando en la microSD la cadena de caracteres “Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño e implementación de un sistema de adquisición de señales electrocardiográficas con almacenamiento remoto de datos encriptados desarrollado por Juan Sebastián Munar Aldana y Carlos Eduardo Moreno Doria de la facultad de Ingeniería Electrónica de la universidad Santo Tomas en Bogotá, Colombia. Asesorada por Jaime Vitola” 100 veces en 3 archivos diferentes, obteniendo así los siguientes resultados.

Archivo 1:

FIGURA 7.8 PRUEBA DE ALMACENAMIENTO MICROSD ARCHIVO 1

```
 90  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 91  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 92  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 93  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 94  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 95  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 96  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 97  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 98  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 99  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
100  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
```

FUENTE: AUTORES

En este primer archivo, de 100 veces que se quiso almacenar el string en microSD desde el microcontrolador, se almacenaron correctamente 100 cadenas de caracteres.

Archivo 2:

FIGURA 7.9 PRUEBA DE ALMACENAMIENTO MICROSD ARCHIVO 2

```
 90  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 91  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 92  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 93  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 94  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 95  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 96  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 97  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 98  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
 99  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
100  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
```

FUENTE: AUTORES

En este segundo archivo, de 100 veces que se requería almacenar el texto en microSD, fueron correctamente almacenadas 100 cadenas de caracteres.

Archivo 3:

FIGURA 7.10 PRUEBA DE ALMACENAMIENTO MICROSD ARCHIVO 3

```
80  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
81  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
82  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
83  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
84  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
85  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
86  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
87  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
88  Este es un texto de prueba para el almacenamiento de datos en microSD del proyecto de grado Diseño
```

FUENTE: AUTORES

En este tercer archivo, de 100 veces que se ordenó almacenar el mensaje en microSD desde el microcontrolador, se almacenaron correctamente 88 cadenas de caracteres.

Dando así por finalizadas las pruebas, abriendo paso a la integración completa del sistema.

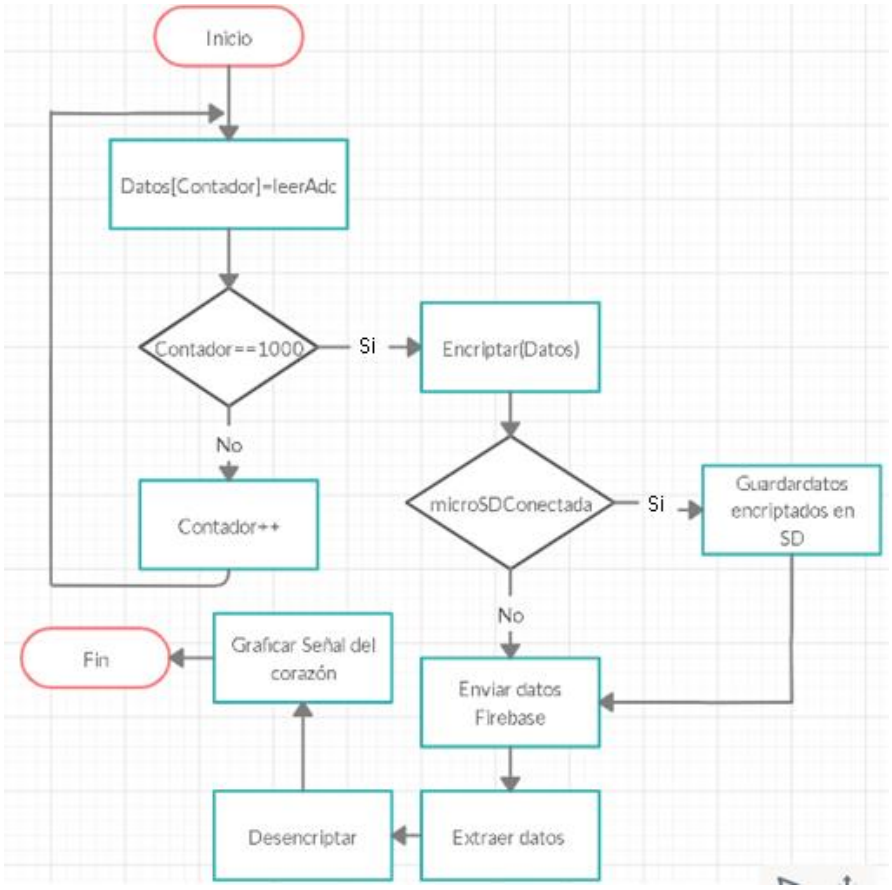
7.1.1 MANEJO DEL SISTEMA

Se conectan al paciente los latiguillos que se enchufan al plug presente en el AD8232, cada latiguillo se enlaza a un electrodo especifico colocado en una de las extremidades que generan el triángulo de Einthoven, en este caso, RA (Brazo

Derecho) se conecta al latiguillo rojo, LA (Brazo Izquierdo) al latiguillo amarillo, y finalmente RL (Pierna Izquierda) al latiguillo verde.

Después de conectado, se verá parpadear el led presente en el AD8232 indicando que este está tomando muestras y espera que se le haga lectura por el pin OUTPUT, es aquí donde se enchufa la salida del dispositivo al pin designado como ADC del microcontrolador.
Una vez enlazado microcontrolador y AD8232, se procede a almacenar los datos recibidos del ADC en un arreglo o vector. Cuando dicho arreglo se llena con el número de muestras captadas, se envían a una función creada para encriptar los datos. Una vez cifrados, se guardan en la microSD y se envían vía UART al módulo Wifi para que este se conecte con la base de datos online Firebase y queden almacenados remotamente. Posteriormente, la interfaz extrae los datos para descifrarlos y graficar obteniendo así la señal del corazón.
A continuación, un diagrama de flujo que explica el proceso.

FIGURA 7.11 DIAGRAMA DE FLUJO DEL SISTEMA



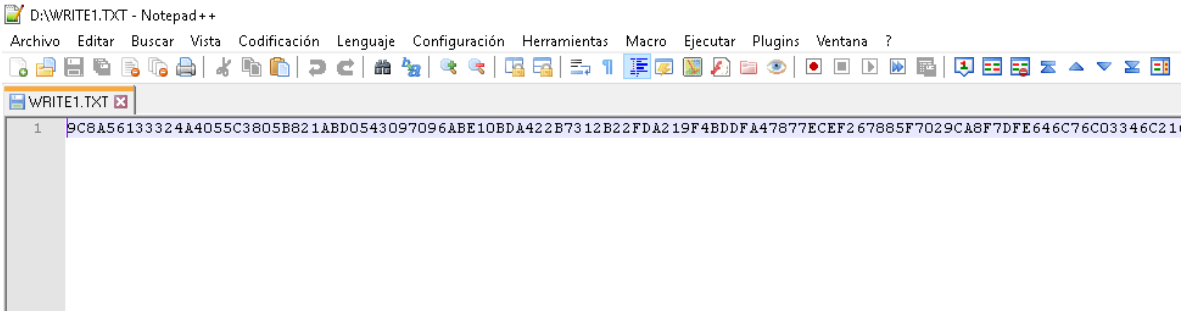
FUENTE: AUTORES

El diagrama anterior muestra, el proceso completo que sigue el sistema desde la captación de los datos por el microcontrolador, hasta representar gráficamente la señal descifrada por medio de la interfaz gráfica de usuario.

7.1.1.1 ALMACENAMIENTO DE DATOS EN MEDIO EXTERNO.

La siguiente imagen es una ilustración de como quedan almacenados los datos de la señal del corazón en la microSD.

FIGURA 7.12 ALMACENAMIENTO EN SD



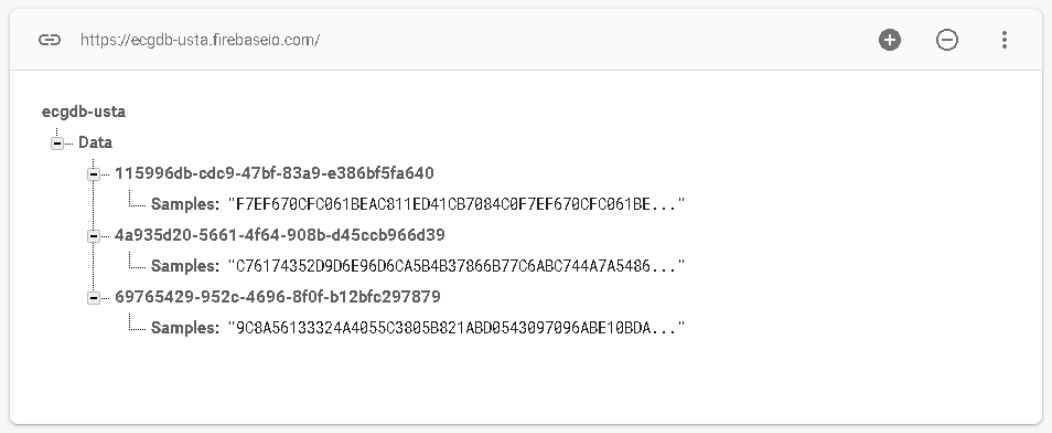
FEUNTE: AUTORES

Se configuran los datos, después de encriptados, en formato hexadecimal desde el microcontrolador, para así facilitar su manejo tanto en la base de datos como a la hora de descifrar los mismos.

7.1.1.2 ALMACENAMIENTO DE DATOS REMOTOS.

A continuación, se presentan algunas muestras almacenadas en la base de datos online Firebase.

FIGURA 7.13 ALMACENAMIENTO REMOTO



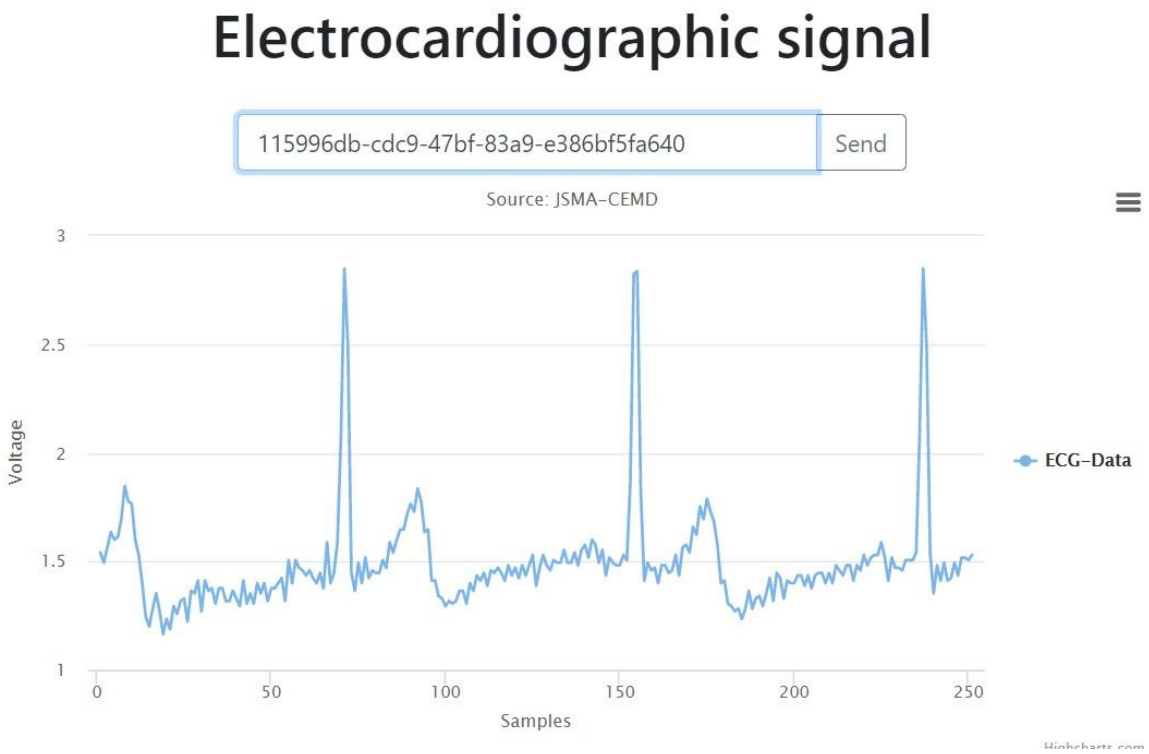
FUENTE: AUTORES

Cómo se puede ver en la ilustración anterior, la última muestra almacenada en la base de datos coincide con los datos guardados en la microSD, lo que confirma el funcionamiento adecuado del sistema para almacenamiento y transferencia de datos, tanto en la base de datos como en el dispositivo que servirá de respaldo.

7.1.1.3 ILUSTRACIÓN DATOS FINALES EN INTERFAZ GRÁFICA.

Se procede a descifrar y graficar los datos almacenados en la base de datos, obteniendo los siguientes resultados:

FIGURA 7.14 SEÑAL CARDIACA DESCIFRADA



FUENTE: AUTORES

Como se puede apreciar en la imagen previa, se relaciona voltaje y muestras para así tener una mejor precisión de la representación del monitoreo del corazón del paciente.
Las muestras tomadas se representan en el eje “x”, por otra parte, el voltaje figura en el eje “y” de la gráfica.

Se comprueba así, que el desarrollo del descifrado y la ilustración gráfica de los datos, se comportan como era de esperarse después de extraer la señal almacenada remotamente.

8. CONCLUSIONES Y TRABAJO FUTURO

Para finalizar, se puede concluir con este proyecto que a partir de un diseño adecuado se puede obtener:

- Un sistema de captación de señales electrocardiográficas portátil, de fácil transporte, de bajo consumo gracias a su tamaño y peso, permitiendo tomar muestras en cualquier parte.
- La facilidad de adquisición del producto por su bajo costo en implementación, esto permite que las poblaciones marginadas tengan acceso rápido a los procedimientos necesarios para obtener un diagnóstico acertado.
- Reducción en tiempos de espera y lectura de resultados, ya que se acerca el paciente con el especialista, reduciendo así la posibilidad de errores en evaluaciones.
- Un canal seguro de transmisión de datos, garantizando la confidencialidad de la relación paciente médico, evitando el acceso de la información a personas inescrupulosas.
- Captación sencilla de señales analógicas del cuerpo similares a las cardiacas para su eventual encriptación y trasmisión segura para un posterior monitoreo.

Trabajo Futuro:

- Considerando la posibilidad de mejorar la seguridad de los datos, se puede implementar un algoritmo de encriptación de clave asimétrica o uno de clave simétrica más robusto puesto que el implementado en este proyecto es el más básico de los AES.
- A partir de este proyecto, se pueden llevar a cabo trabajos de electrocardiografía con más de una derivación utilizando dispositivos que permitan la captación de hasta 12 derivaciones del corazón.
- Teniendo en cuenta la limitación de memoria que presenta el microcontrolador, se puede implementar un diseño donde se incluya una expansión de esta para reducir así limitaciones de memoria flash en el dispositivo.
- Además, utilizar un microcontrolador con mejores especificaciones que incluya módulo de criptografía para que el algoritmo no se limite únicamente a un solo modo de cifrado.

REFERENCIAS BIBLIOGRÁFICAS

1. N. Lacktman L. Vernaglia (11, Nov 2014) Foley And Lardner Llp. Telemedicine Survey. Executive Summary. [Online]. Available: Https://Www.Foley.Com/En/Insights/Publications/2014/11/2014-Telemedicine-Survey-Executive-Summary

2. Ministerio De Protección Social (Ago. 2008), “Composición De La Oferta De Profesionales De Medicina En Colombia 2009”. [Online] Available: Https://Www.Minsalud.Gov.Co/Salud/Documents/Observatorio%20talento%20humano%20en%20salud/Composici%C3%93n%20oferta%20de%20profesionales%20en%20colombia.Pdf

3. K. Davis, K. Stremikis, D. Squires, And C. Schoen (Jun 2014) Mirror, Mirror On The Wall How The Performance Of The U.S. Health Care System Compares Internationally. [Online] Available: Http://Www.Resbr.Net.Br/Wp-Content/Uploads/Historico/Espelhoespelhomeu.Pdf

4. J. L. Amaya Lara, A. Beltrán Villegas, D. Chavarro, G. Romero Silva, M. A. Matallana Gómez, S. Puerto García, F. Ruiz Gómez, M.E Vásquez Candia (Septiembre De 2013), “Estudio De Disponibilidad Y Distribución De La Oferta De Médicos Especialistas, En Servicios De Alta Y Mediana Complejidad En Colombia, 2013”. [Online] Available: Https://Www.Minsalud.Gov.Co/Salud/Documents/Observatorio%20talento%20humano%20en%20salud/Disponibilidaddistribuci%C3%B3nmdespecialistascendex.Pdf

5. C. M. Moreno Segura (Noviembre De 2016) “Analisis De Situacion De Salud (Asis) Colombia, 2016”. [Online] Available: Https://Www.Minsalud.Gov.Co/Sites/Rid/Lists/Bibliotecadigital/Ride/Vs/Ed/Psp/Asis-Colombia-2016.Pdf

6. J. I. Valle Racero, (1er Cuatrimestre 2001) A Brief History Of Electrocardiography. (Online) Available: Https://Www.Enfermeriaencardiologia.Com/Wp-Content/Uploads/22histelectro.Pdf

7. J. B. Tommerdahl, "A Preamplifer for an Electrocardiograph Monitoring System," in *IRE Transactions on Bio-Medical Electronics*, vol. 8, no. 1, pp. 55-58, Jan. 1961.

8. C. A. Steinberg, S. Abraham and C. A. Caceres, "Pattern Recognition in the Clinical Electrocardiogram," in IRE Transactions on Bio-Medical Electronics, vol. 9, no. 1, pp. 23-30, Jan. 1962.

9. J. C. Huhta and J. G. Webster, "60-Hz Interference in Electrocardiography," in IEEE Transactions on Biomedical Engineering, vol. BME-20, no. 2, pp. 91-101, March 1973.

10. M. L. Ahlstrom and W. J. Tompkins, "Digital Filters for Real-Time ECG Signal Processing Using Microprocessors," in IEEE Transactions on Biomedical Engineering, vol. BME-32, no. 9, pp. 708-713, Sept. 1985.

11. K. Laurita, C. W. Thomas, M. Kavuru, H. Vesselle and J. Liebman, "Data acquisition system for cardiac mapping," Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, New Orleans, LA, USA, 1988, pp. 104-105 vol.1

12. Y. Z. Ider and A. Oto, "PC based high resolution ECG system," [1990] Proceedings Computers in Cardiology, Chicago, IL, USA, 1990, pp. 665-668.

13. G. Bortolan, R. Degani and J. L. Willems, "ECG classification with neural networks and cluster analysis," [1991] Proceedings Computers in Cardiology, Venice, Italy, 1991, pp. 177-180.

14. S. D. Joshi, "A low cost multichannel central ECG monitoring system," Proceedings of the First Regional Conference, IEEE Engineering in Medicine and Biology Society and 14th Conference of the Biomedical Engineering Society of India. An International Meet, New Delhi, India, 1995, pp. SPC11-SPC12.

15. Philip de Chazal, M. O'Dwyer and R. B. Reilly, "Automatic classification of heartbeats using ECG morphology and heartbeat interval features," in IEEE Transactions on Biomedical Engineering, vol. 51, no. 7, pp. 1196-1206, July 2004.

16. A. M. Khairuddin, K. N. F. Ku Azir and P. E. Kan, "Limitations and future of electrocardiography devices: A review and the perspective from the Internet

of Things," 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, 2017, pp. 1-7.

17. J. Mohammed, C. Lung, A. Ocneanu, A. Thakral, C. Jones and A. Adler, "Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing," 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), Taipei, 2014, pp. 256-263.

18. M. R. F. Nurdin, S. Hadiyoso and A. Rizal, "A low-cost Internet of Things (IoT) system for multi-patient ECG's monitoring," 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, 2016, pp. 7-11.

19. D. Azariadi, V. Tsoutsouras, S. Xydis and D. Soudris, "ECG signal analysis and arrhythmia detection on IoT wearable medical devices," 2016 5th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, 2016, pp. 1-4.

20. M. F. Amri, M. I. Rizqyawan and A. Turnip, "ECG signal processing using offline-wavelet transform method based on ECG-IoT device," 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2016, pp. 1-6.

21. M. J. Shea (Oct. 2017) Electrocardiografía [Online] Available: Https://Www.Msdmanuals.Com/Es-Co/Hogar/Trastornos-Del-Coraz%C3%B3n-Y-Los-Vasos-Sangu%C3%Adneos/Diagn%C3%B3stico-De-Las-Enfermedades-Cardiovasculares/Electrocardiograf%C3%Ada.

22. O. M. Gelvez Lizarazo, “Diseño Y Construcción De Un Modelo Funcional De Electrocardiografía Utilizando Circuitos Integrados De Propósito Especifico”. Proyecto De Grado, Escuela De Ingenierías Eléctrica, Electrónica Y Telecomunicaciones, Facultad De Ingenierías Físico-Mecánicas, Universidad Industrial De Santander B/Manga, Col, 2013.

23. L. M. Rincon, Development Of An Acquisition Circuit Of Multiple Biological Signals For Integration Into A Wearable Bracelet, M.S. Thesis. Escola Tècnica D'enginyeria De Telecomunicació De Barcelona, Universitat Politècnica De Catalunya, Bar, Esp. 2017

24. A. Barea Cañizares, “Diseño, Desarrollo Y Test De Un Prototipo De Pulsera Para Adquirir El Electrocardiograma Y La Onda De Pulso”, Proyecto Final De Carrera, Escola Tècnica D'enginyeria De Telecomunicació De Barcelona, Universitat Politècnica De Catalunya, Bar, Esp. 2016

25. Introducción A La Criptografía, [Online] Available: Http://Www.Dma.Fi.Upm.Es/Recursos/Aplicaciones/Matematica_Discreta/Web/Aritmetica_Modular/Criptografia.Html#1

26. H. A. Chaves Jiménez, Diseño E Implementación De Un Software Multimedia Para El Aprendizaje De La Criptografía, Proyecto De Grado, Facultad De Ingeniería, Universidad San Buenaventura, Bogotá, 2008.

27. A. R. Madrid (17 Ago 2011), El Algoritmo De Encriptación Aes, Más Vulnerable De Lo Que Se Creía, [Online] Available: Https://Elpais.Com/Sociedad/2011/08/17/Actualidad/1313532009_850215.Html

28. D. I. González Sánchez, Seguridad En Redes Y Criptografía, M.S. Tesis, Instituto Tecnológico Y De Estudios Superiores De Monterrey. 2004.

29. L. E. Martínez Bohórquez, Algoritmo Para La Encriptación Y Desencriptación Entre Archivos Digitales De Audio E Imagen, Tesis para optar el Título profesional, Facultad de Ingeniería, Universidad de San Buenaventura, Bogotá. 2017

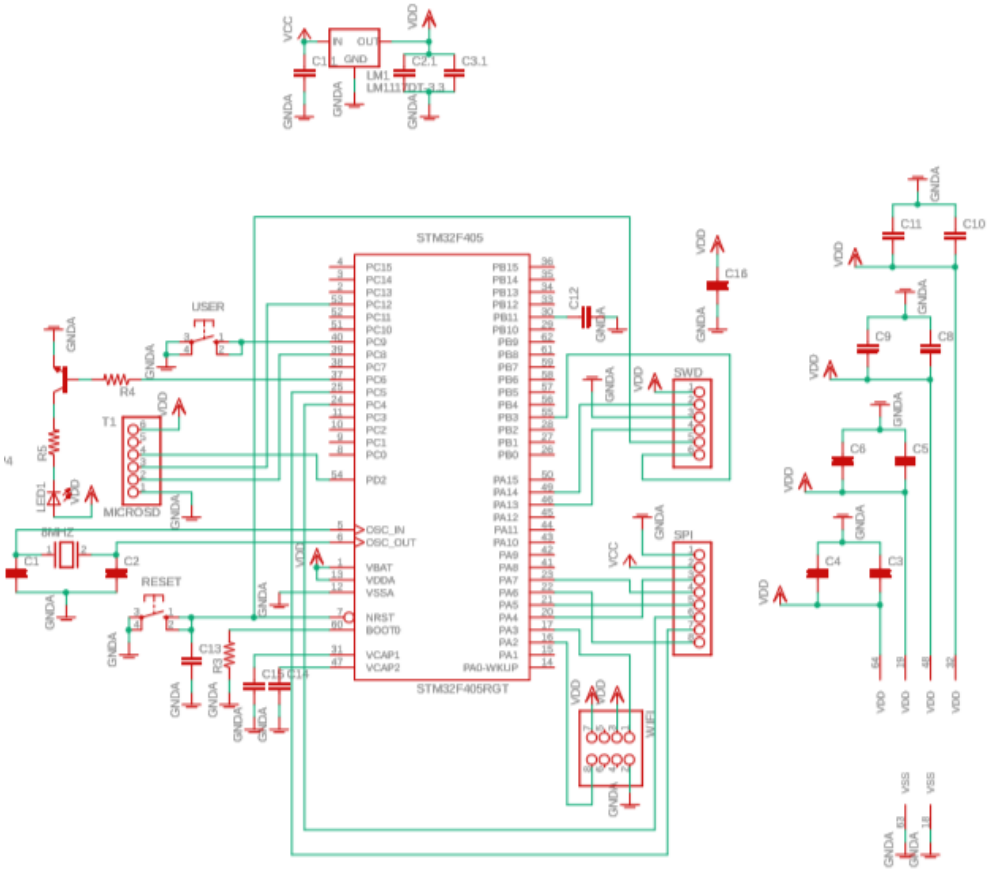
30. Y. T. Medina Vargas, H. A. Miranda Méndez, (Jun 2015). Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES. Edición N° 9. [Online] Avaiable: https://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/download/55/97/0

ANEXOS

DISPOSITIVO EN CAJA DE PRESENTACIÓN

FUENTE: AUTORES

PLANO ELECTRONICO TOTAL DEL SISTEMA



FUENTE: AUTORES