UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UNA SEGURIDAD BIOMÉTRICA CON COBERTURA DE RED, USANDO MENSAJERÍA PROGRAMADA CON TELEGRAM ASOCIADO CON RASPBERRY PI3 Y ARDUINO PARA LA EMPRESA PHONIX-CELL

Trabajo de titulación previo a la obtención del
Título de Ingeniero electrónico y telecomunicaciones

AUTOR: JOSÉ GEOVANNY FUELA ECHEVERRÍA
TUTOR: MSc. LUIS ANTONIO NEIRA CLEMENTE

GUAYAQUIL - ECUADOR
2022

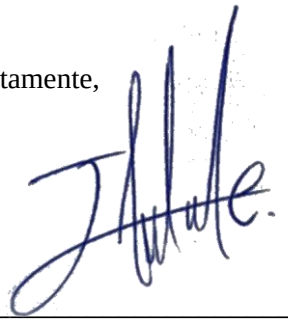
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, José Geovanny Fuela Echeverría con documento de identificación **N°** 0704971001 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 20 de marzo del año 2022

Atentamente,



José Geovanny Fuela Echeverría

0704971001

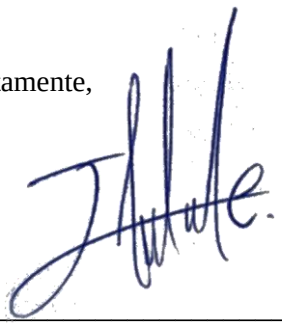
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, José Geovanny Fuela Echeverría con documento de identificación, N° 0704971001, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Proyecto Técnico: "Diseño e implementación de una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram asociado con Raspberry PI 3 y Arduino para la empresa ´´Phonix-Cell" ", el cual ha sido desarrollado para optar por el título de: Ingeniero electrónico y telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 20 de marzo del año 2022

Atentamente,



José Geovanny Fuela Echeverría

0704971001

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Luis Antonio Neira Clemente con documento de identificación N° 0909136582, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DISEÑO E IMPLEMENTACIÓN DE UNA SEGURIDAD BIOMÉTRICA CON COBERTURA DE RED, USANDO MENSAJERÍA PROGRAMADA CON TELEGRAM ASOCIADO CON RASPBERRY PI 3 Y ARDUINO PARA LA EMPRESA ´´PHONIX-CELL´´, realizado por José Geovanny Fuela Echeverría, con documento de identificación N° 0704971001, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 20 de marzo del año 2022

Atentamente,

Luis Antonio Neira Clemente

0909136582

DEDICATORIA

Dedico este proyecto a mi Dios, ya que gracias a sus bendiciones he podido salir adelante, en especial a mi mama Rosa Germania Echeverría Cajamarca quien ha sido, es y será mi más grande admiración, ya que ella es la que ha sacado adelante el hogar con sacrificios trabajando desde la madrugada hasta la noche dibujado planos y haciendo levantamientos de terrenos sin importar el peligro porque para ella no le importaba llegar cansada a la casa, y a pesar que he sido irresponsable, odioso, en muchas ocasiones no le he hecho caso y a pesar de mis errores no me ha dejado solo, por eso quiero dedicarle mis logros ya que sin sus esfuerzos yo no fuera nada, a mi papa (+) (José Benito Fuela Tobar) quien en vida me motivaba a seguir adelante en mis estudios y eso es lo que me ha dado el valor y el coraje de poder llegar hacer un profesional, me hubiera gustado que este conmigo para compartir este logro con el mi amado padre gracias por todo.

AGRADECIMIENTO

Me gustaría agradecer a mi familia por darme el apoyo, a mi tío (+) (Abel Echeverría) quien en vida me recibió en su casa y me trató como a un hijo y pudo compartir sus conocimientos conmigo, los cuales me ayudaron mucho para mi formación académica, también agradezco al señor Oswaldo Clavijo por ser una persona dispuesta a ayudar a colaborar a escuchar y darme consejos en los momentos más cruciales de mi vida el cariño que le tengo es como al de un padre, agradezco a mis profesores los de la escuela, colegio y universidad por haber compartido sus conocimientos los cuales me han ayudado intelectualmente para mi desarrollo profesional, agradezco a mis amigos por sus consejos, su ayuda infinita, por ese apoyo incondicional que a pesar de la distancia sé que puedo contar con ellos y ellos también podrán contar conmigo.

RESUMEN

Año	Alumno	Director del proyecto	Tema de proyecto de titulación
2022	José Geovanny Fuela Echeverría	Ing. Luis Antonio Neira Clemente Msc.	Diseño e implementación de una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram asociado con Raspberry PI3 y Arduino para la empresa Phonix-cell.

La biometría es una tecnología que analiza todas las características del individuo, permitiendo la identificación de manera fiable, usando varias técnicas para el proceso de reconocimiento que se lo realizó mediante la huella dactilar, siendo esta la técnica más utilizada dentro de la industria. En el siguiente trabajo de titulación se diseñó una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram, de esta manera se controlaría la entrada y salida de los empleados. Este trabajo está enfocado en una tecnología avanzada, compuesta por Raspberry PI 3 y Arduino, recordando que éste es un microcontrolador que ejecuta cualquier información que está previamente guardada, es necesario tener conectividad a internet para poder enviar y recibir la información del ingreso y salida del trabajador. Para ello, se utilizará diferentes materiales tales como: Protoboard, led azul y amarillo, resistencia de 1kΩ, lector de huella, Arduino, cable USB, cable UTP y Raspberry Pi. Para saber cómo queda la red se manejaron diferentes programas, entre los cuales tenemos: "Visual Studio Code", en este programa se definen las líneas de código, el programa "Network IP Scanner" se lo usa para identificar la red de la Raspberry Pi, "PuTTY" es el programa donde se ejecutan: Telegram, Flask, cuba y Python, estos generan la interfaz web y el aplicativo Telegram que es donde se recibe el mensaje generado por la Raspberry Pi, indicando que el usuario ha ingresado al almacén. A su vez se elaboró varias simulaciones con su respectivo procedimiento, lo cual puede evidenciar los pasos a seguir para elaborar dicha seguridad biométrica.

La característica del estuche donde se alojarán todos los componentes a utilizar, previamente mencionados se los acopló en un estuche metálico de color negro cuyas dimensiones son: de altura es de 13 cm, de largo 15 cm y de ancho 6 cm. Este proyecto técnico fue diseñado para los interiores de la empresa "Phonix-Cell", y no para los exteriores.

Palabras claves: Biométrico, Telegram, Arduino, Raspberry Pi, huella dactilar.

ABSTRACT

Year	Student	Technical Project Manager	Item of Project of titulation
2022	José Geovanny Fuela Echeverría	Ing. Luis Antonio Neira Clemente Msc.	Design and implementation of biometric security with network coverage, using programmed messaging with Telegram associated with Raspberry PI3 and Arduino for the company Phonix-cell.

Biometrics is a technology that analyzes all the characteristics of the individual, allowing the identification in a reliable way, using various techniques for the recognition process that was carried out by means of the fingerprint, this being the most used technique within the industry. In the following degree work, a biometric security with network coverage was designed, using programmed messaging with Telegram, in this way the entry and exit of employees would be controlled. This work is focused on an advanced technology, composed of Raspberry PI 3 and Arduino, remembering that this is a microcontroller that executes any information that is previously saved, it is necessary to have internet connectivity to be able to send and receive the information of the entry and exit of the worker. For this, different materials will be used such as: breadboard, blue and yellow led, 1kΩ resistor, fingerprint reader, Arduino, USB cable, UTP cable and Raspberry Pi. To know how the network looks, different programs were managed, among which we have: "Visual Studio Code", in this program the lines of code are defined, the "Network IP Scanner" program is used to identify the Raspberry Pi network, "PuTTY" is the program where they are executed: Telegram, Flask, Cuba and Python, these generate the web interface and the Telegram application, which is where the message generated by the Raspberry Pi is received, indicating that the user has entered the store. In turn, several simulations were developed with their respective procedure, which can show the steps to follow to develop said biometric security.

The case feature where shall be stock all the components to utilize above mentioned were compiled into a black color metal case whose dimensions are: 13 centimeters in height 15 centimeters long and 6 centimeters wide. This technic project was designed for the indoors of “Phonix-Cell” company and no for outdoors.

Keywords: Biometric, Telegram, Arduino, Raspberry Pi, fingerprint.

ÍNDICE GENERAL

INTRODUCCIÓN 15

CAPÍTULO I: PROBLEMA 17

1.1 Antecedentes 17

1.2 Importancia y alcance 17

1.3 Delimitación del problema 18

1.4 Explicación del problema 18

1.5 Objetivos 19

1.5.1 Objetivo General 19

1.5.2 Objetivos específicos 19

1.6 Marco metodológico 19

CAPÍTULO II: MARCO TEÓRICO 22

2.1 Seguridad biométrica 22

2.2 Sistemas biométricos más utilizados 23

2.3 Arquitectura de un sistema biométrico 23

2.4 Elementos principales de los dispositivos biométricos 25

2.5 Etapas para la identificación de un sistema biométrico 25

2.6 Técnicas biométricas 28

2.7 Parámetros para la elección de una técnica biométrica 30

2.8 Beneficios del uso del sistema biométrico 31

2.9 Datos biométricos 32

2.10 Legislación latinoamericana en el uso del sistema 32

2.11 Riesgos y retos del sistema 32

2.12 Puntos fuertes y débiles que existen en el sistema biométrico 32

2.13 Hardware para implementar en el sistema biométrico 33

2.13.1 Placas Arduino 33

2.14 Compatibilidad Arduino 36

2.15 Programación Arduino 36

2.15.1 Ardublock 36

2.15.2 Minibloq 37

2.15.3 Modkit 37

2.15.4 Scratch 38

2.15.5 Physical Etoys 38

2.15.6 Ardulab 39

2.16 Lenguaje de programación de Arduino 39
2.17 Fritzing 40
2.18 Raspberry Pi 3 40
CAPITULO III: FUNCIONAMIENTO Y CONFIGURACIÓN DEL SISTEMA BIOMÉTRICO 42
3.1 Diseño del circuito 42
3.2 Diagrama de flujo del funcionamiento del algoritmo del prototipo 42
3.3 Diagrama de bloques del prototipo 43
3.4 Diagrama esquemático del prototipo 44
3.5 Diseño de la caja del biométrico 44
3.6 Configuración del biométrico 45
3.6.1 Distribución y accesos de configuración 45
3.7 Comunicación del biométrico 46
3.7.1 Herramientas del software 46
3.8 Funcionamiento del lector biométrico 46
3.8.1 Ingreso de huella dactilar al sistema biométrico 46
3.9 Materiales utilizados para la realización del sistema biométrico 47
3.9.1 Elementos indispensables para la elaboración del proyecto 47
3.10 Composición del Protoboard 47
3.10.1 Distribución y enlaces del Protoboard 47
3.11 Codificación del sistema 47
3.11.1 Elaboración y programación de hardware en el sistema biométrico 47
CAPITULO IV: RESULTADOS 81
4.1 Características generales del sistema 81
4.2 Características técnicas del sistema biométrico 82
4.2.1 Características técnicas del Arduino nano 82
4.2.2 Características técnicas de la Raspberry Pi 3 82
4.3 Sistema de enlace del biométrico 83
4.3.1 Estructura de enlace 83
4.4 Carga eléctrica del sistema 83
4.4.1 Fuente de voltaje 83
4.5 Resultados de las muestras dactilares 84
4.5.1 Constancia de registro en la plataforma web 84
4.5.2 Respuesta del sistema biométrico 86
4.5.3 Notificación de mensajería del sistema vía Telegram 87

4.6 Análisis de resultados 87
CONCLUSIONES 88
RECOMENDACIONES 90
REFERENCIAS 91

ÍNDICE DE FIGURAS

Figura 1. 1: Diagrama del sistema biométrico, Fuente: (Autor) ..... **¡Error! Marcador no definido.**

Figura 2. 1: Arquitectura de un sistema biométrico con huella dactilar, Fuente: (Cortes , Jimy, Medina, & Francisco , 2010)..... **¡Error! Marcador no definido.**

Figura 2. 2: Verificación y reclutamiento, Fuente: (Ruiz & Olivares , Una mirada a la biometria, 2009)..... **¡Error! Marcador no definido.**

Figura 2. 3: Reconocimiento y autentificación, Fuente: (Ruiz, Rodriguez, & Olivares , Una mirada a la biometria, 2009) ..... **¡Error! Marcador no definido.**

Figura 2. 4: Ventajas y desventajas de las técnicas biométricas, Fuente: (Ruiz & Olivares, Una mirada a la biometria,2009) ..... **¡Error! Marcador no definido.**

Figura 2. 5: Arduino Nano, Fuente: (Herrero & Allende,2015) **¡Error! Marcador no definido.**

Figura 2. 6: Ventana de Ardublock, Fuente: (Herrero & Allende,2015) ... **¡Error! Marcador no definido.**

Figura 2. 7: Programación Minibloq, Fuente: (Herrero & Allende,2015) . **¡Error! Marcador no definido.**

Figura 2. 8: Configuración Modkit, Fuente: (Herrero & Allende,2015) ... **¡Error! Marcador no definido.**

Figura 2. 9: Configuración Scratch, Fuente: (Herrero & Allende,2015) ... **¡Error! Marcador no definido.**

Figura 2. 10: Configuración Physical, Fuente: (Herrero & Allende,2015) **¡Error! Marcador no definido.**

Figura 2. 11: Configuración Ardulab, Fuente: (Herrero & Allende,2015) **¡Error! Marcador no definido.**

Figura 2. 12: Configuración externa, Fuente: (Santander Frank,2016) .... **¡Error! Marcador no definido.**

Figura 2. 13: Configuración interna, Fuente: (Santander Frank,2016)..... **¡Error! Marcador no definido.**

Figura 2. 14: Raspberry Pi 3, Fuente: (Gabriel Franco,2020) 41

Figura 3. 1: Diagrama de conexiones del circuito en Proteus, Fuente: (Autor) 42

Figura 3. 2: Flujo de funcionamiento del algoritmo, Fuente: (Autor)..... 43

Figura 3. 3: Diagrama de bloques, Fuente: (Autor) 44
Figura 3. 4: Diagrama esquemático, Fuente: (Autor) 44
Figura 3. 5: Diseño final de la caja del biométrico, Fuente: (Autor) 45
Figura 3. 6: Configuración con el protoboard, Fuente: (Autor)..... **¡Error! Marcador no definido.**
Figura 3. 7: Programa Fritzing, Fuente: (Autor)..... 48
Figura 3. 8: Lector Biométrico, Fuente: (Autor)..... 48
Figura 3. 9: Carpeta Arduino, Fuente: (Autor) 49
Figura 3. 10: Comunicación inalámbrica, Fuente: (Autor)..... 50
Figura 3. 11: Comunicación del Raspberry Pi 3, Fuente: (Autor) 53
Figura 3. 12: Diseño de protoboard, Fuente: (Autor)..... 54
Figura 3. 13: Parte posterior del lector de huella, Fuente: (Autor) 55
Figura 3. 14: Conexión del cableado, Fuente: (Autor)..... 55
Figura 3. 15: Conexión de tierra, Fuente: (Autor) 56
Figura 3. 16: Módulo Raspberry Pi 3, Fuente: (Autor)..... 57
Figura 3. 17: Raspberry Pi 3 conectado al módulo, Fuente: (Autor) 57
Figura 3. 18: Carpeta APP, Fuente: (Autor) 58
Figura 3. 19: Archivo Cuba, Fuente: (Autor)..... 59
Figura 3. 20: Comunicación con la base de datos, Fuente: (Autor)..... 62
Figura 3. 21: Registro de acceso, Fuente: (Autor) 62
Figura 3. 22: Código interfaz, Fuente: (Autor) 64
Figura 3. 23: Codificación del programa, Fuente: (Autor) 65
Figura 3. 24: Comunicación con Telegram, Fuente: (Autor)..... 67
Figura 3. 25: Registro, Fuente: (Autor)..... 69
Figura 3. 26: Ícono Network IP Scanner, Fuente: (Autor)..... 71
Figura 3. 27: Menú Principal de la app descargada, Fuente: (Autor) 71
Figura 3. 28: Programa PUTTY, Fuente: (Autor)..... 72
Figura 3. 29: Ingreso al programa PUTTY, Fuente: (Autor) 73
Figura 3. 30: Conexión Raspberry, Fuente: (Autor) ..... **¡Error! Marcador no definido.**

Figura 3. 31: Ventanas con direcciones IP, Fuente: (Autor) 74
Figura 3. 32: Ingreso de plataforma del biométrico, Fuente: (Autor) 75
Figura 3. 33: Plataforma del biométrico, Fuente: (Autor) 75
Figura 3. 34: Mensaje de la aplicación de Telegram, Fuente: (Autor) 76
Figura 3. 35: Registro de los empleados, Fuente: (Autor) 77
Figura 3. 36: Configuraciones de la lista de los empleados, Fuente: (Autor) 78
Figura 3. 37: Explicación de la lista para editar, Fuente: (Autor) 79
Figura 3. 38: Descarga del registro realizado, Fuente: (Autor) 80
Figura 4. 1: Sistema biométrico, Fuente: (Autor) 81
Figura 4. 2: Módulo Raspberry Pi 3 conectado, Fuente: (Autor) 82
Figura 4. 3: Alimentación de energía al dispositivo, Fuente: (Autor) 83
Figura 4. 4: Constancia del registro en el dispositivo, Fuente: (Autor) 83
Figura 4. 5: Usuario no registrado en el dispositivo, Fuente: (Autor) 83
Figura 4. 6: Usuarios registrados en la plataforma web, Fuente: (Autor) 83
Figura 4. 7: Monitoreo de acceso por medio del aplicativo web, Fuente: (Autor) 83
Figura 4. 8: Plataforma de acceso en tiempo real del sistema biometrico, Fuente: (Autor) 83
Figura 4. 9: Notificacion de mensajeria via Telegram, Fuente: (Autor) 83

INTRODUCCIÓN

En la actualidad el sistema de seguridad biométrico ayuda a proteger la información de una empresa y de cada uno de sus usuarios; esta seguridad se encuentra muy presente en cualquier contexto laboral por lo que cumple un papel relevante.

Se decidió elaborar el presente proyecto por la necesidad que hay en la empresa "Phonix-Cell" ubicada en la ciudad de Pasaje, ya que es necesario e importante contar con seguridad biométrica, de esta manera se pretende que el Gerente de la empresa tenga el control de sus empleados referente al cumplimiento de los horarios de entrada y salida.

Este trabajo de titulación consiste en diseñar una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram asociado con Raspberry PI 3 y Arduino para la empresa ´´Phonix-Cell", la cual cuenta con procesos importantes como la captura, extracción, creación de un standard y prueba de evaluación de una seguridad biométrica.

Este proyecto está enfocado en el uso de una tecnología en evolución como es la seguridad biométrica con cobertura de red, compuesta por Raspberry Pi 3 y Arduino. Este sistema se encuentra distribuidos en grandes empresas, hospitales, dispositivos móviles, facilitando la identificación y verificación de identidades. Se elaboró varias simulaciones con su respectivo procedimiento, lo cual puede evidenciar los pasos a seguir para elaborar dicha seguridad biométrica.

En el capítulo I, se identifica el problema existente, de esta manera se plantea los objetivos generales y específicos para diseñar una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram asociado con Raspberry PI3 y Arduino para la empresa "Phonix-Cell".

En el capítulo II, se relata cada uno de los conceptos generales para llegar a comprender como se llevará a cabo el desarrollo del presente proyecto, se explicará de manera detallada y se asociarán los objetivos específicos.

En el capítulo III, se describe la conceptualización más específica para diseñar la seguridad biométrica y la importancia que tiene aplicar esta seguridad en la empresa "Phonix-Cell", además se especifica su estructura.

En el capítulo IV, se describen los resultados obtenidos durante el proceso de elaboración, tomando en cuenta la calidad de los materiales para su manufactura.

.

CAPÍTULO I: PROBLEMA

1.1 Antecedentes

En la actualidad, la empresa "Phonix-Cell" con sede ubicada en el cantón Pasaje y sucursal en Santa Rosa, ya cuenta con una seguridad biométrica que permita al gerente de la empresa, a quien más adelante llamaremos "empresario o empleador", tener el control referente al ingreso y salida de sus empleados en los horarios establecidos. Esto resulta un impedimento poder abrir otra sucursal, surgiendo la necesidad de implementar una seguridad biométrica para que el empresario pueda llevar un registro diario de cada uno de sus empleados a través de su dispositivo móvil.

1.2 Importancia y alcance

Hoy en día la seguridad biométrica ayuda a proteger la información de la empresa y sus usuarios, esto cada vez se encuentra presente en nuestras vidas, por lo que cumple un papel importante, porque de alguna manera ayuda a mejorar la seguridad de los establecimientos, tomando en cuenta que cada facción y característica del individuo es única.

La biometría es un sistema de seguridad que identifica a la persona y tiene un elevado nivel de confiabilidad al momento de identificar a cada uno de los individuos, tiene como base el reconocimiento de las características físicas, que son únicas e inimitables y no se pueden transferir de una persona. a otra. Por ejemplo: el reconocimiento facial, huella digital, patrón del iris, entre otros.

El sistema biométrico tiene una tecnología que permite computarizar el reconocimiento del ser humano, llevando esta seguridad al siguiente nivel de modo integrado; este sistema maneja el mismo proceso que el de un ser humano, identificándose quién es y quién no. En fin, cuando se habla de biometría, se refiere a una tecnología científica que permite la identificación de cada ser humano, mediante los rasgos fisiológicos, lo que permite una identificación total y precisa.

Este trabajo de titulación está enfocado en el uso de una tecnológica avanzada en evolución, como es la seguridad biométrica, compuesta por cobertura de red,

Raspberry PI3 y Arduino. Este sistema se encuentra funcionando en empresas, hospitales, dispositivos móviles, que va a permitir la identificación y verificación de identidades.

Se decidió elaborar el presente proyecto por la necesidad que hay dentro de la empresa "Phonix-Cell", ya que es necesario e importante contar con esta seguridad biométrica, y de esta manera el empresario tenga control de sus empleados referente al cumplimiento de los horarios de entrada y salida.

1.3 Delimitación del problema

Este trabajo de titulación está enfocado en la implantación de una seguridad biométrica, para la empresa "Phonix-Cell". Dicha implementación se realizó en el cantón Pasaje provincia de El Oro, permitiendo de esta manera que el empresario tenga control de cada uno de sus empleados cuando ingresen y salgan de su lugar de trabajo.

1.4 Explicación del problema

Generalmente en la empresa "Phonix-Cell" las actividades de ventas y logística no son organizadas de manera eficiente, de esta forma se torna una tarea complicada llevar un control adecuado sobre la organización de su personal, teniendo como resultado la dificultad de conocer las jornadas laborales que cumplen los empleados en el transcurso del día, generando posibles pérdidas económicas al no cumplir las horas reglamentarias de trabajo.

En la empresa perteneciente al sector tecnológico comercial, se presentaban problemas al momento que el personal laboral no cumplía los horarios establecidos de ingreso y salida, cuando el gerente no se encontraba en el establecimiento, pues en las cámaras se observaba el incumplimiento de la jornada, lo cual genera insatisfacción en los clientes al momento de visitar el almacén y encontrar éste cerrado, ante esto se propone la implementación de un dispositivo biométrico que permita el control de los horarios de ingreso y salida para así poder corregir dichos inconvenientes y controlar la organización de los empleados.

1.5 Objetivos

1.5.1 Objetivo General

Diseñar e implementar una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram asociado con Raspberry Pi3 y Arduino para la empresa “Phonix-Cell”

1.5.2 Objetivos específicos

- Realizar una codificación en el cual exista una comunicación entre el biométrico y la aplicación Telegram.

- Diseñar una interfaz única en la cual se pueda registrar las veces que sea necesario a los empleados existentes y nuevos de dicha empresa.

- Desarrollar el diseño del circuito de la seguridad biométrica.

1.6 Marco metodológico

1.6.1 Método sintético

Es el encargado de volver a reconstruir un acontecimiento ya que siempre se apoya en la información más precisa, en este caso se revisará el estado del arte sobre los sistemas biométricos usados en la historia, mediante investigación bibliográfica, para definir los fundamentos teóricos de gran aporte para el presente trabajo.

1.6.2 Método experimental

Es un método en el cual se caracteriza por ver, dirigir y registrar las distintas variables que afectan a un determinado fenómeno u objeto de estudio, permitiéndonos de este modo realizar el proceso de diseño, armado e implementación de una seguridad

biométrica, aplicando los conocimientos profesionales adquiridos en el transcurso de la carrera universitaria, para el correcto funcionamiento de sus distintos elementos.

1.6.3 Método inductivo

Es el encargado de llegar a las conclusiones, pero comenzando desde una hipótesis y utilizando siempre el razonamiento, para lo cual se analizará los resultados, mediante pruebas de funcionamiento y escenarios de trabajo, para la determinación de su correcto desempeño en el uso diario.

1.6.4 Conectividad e interfaz web

Para el módulo del biométrico, el conjunto de materiales a utilizar fueron: un lector de huellas, el cual escanea el dedo del usuario, y la imagen obtenida la convierte a un código digital, el cual se almacena en la base de datos, el Arduino es un microcontrolador que ejecuta cualquier información previamente guardada, es muy útil porque no es necesario ejecutar la misma línea de código al encender el módulo, la Raspberry Pi 3 es un microprocesador el cual funciona como un CPU, y se complementa con una conectividad inalámbrica a internet lo cual es necesario para enviar y recibir información del ingreso o salida del trabajador.

Para definir la interfaz web se usó: Visual Studio Code, en este programa definimos las líneas de código, el programa Network IP Scanner, se lo usa para identificar la red de la Raspberry, PuTTY es el programa donde se ejecuta: Telegram, Flask, cuba y Python estos generan la interfaz web, y el aplicativo Telegram que es donde se recibe el mensaje generado por la Raspberry Pi 3 indicando que el usuario a ingresado al almacén.

Figura 1. 1: Diagrama del sistema biométrico

Fuente: (Autor)

CAPÍTULO II: MARCO TEÓRICO

2.1 Seguridad biométrica

El sistema biométrico no es una creación reciente, por lo que ha estado en vigencia desde el año 1858, entre los sistemas biométricos más comunes están, el reconocimiento: facial, del iris y dactilar (Diaz, 2013).

El termino biometría se origina del latín bio que es vida y metría que son medidas, es por ellos que los datos biométricos generan información de las medidas y las características fisiológicas, como también morfológicas de los seres humanos mediante técnicas automatizadas y manuales (Diaz, 2013).

Desde el comienzo del siglo XXL, el sistema de seguridad biométrico ha sido un medio eficaz y eficiente en el reconocimiento del individuo, destacando el reconocimiento facial, reconocimiento de la voz, reconocimiento de la huella dactilar, análisis de la forma de la mano y análisis del patrón del iris, entre otros (Diaz, 2013).

La biometría radica en medir los rasgos únicos del ser humano, en la cual permite identificarse de un individuo a otro, por consiguiente, se debe elegir una característica fuerte del individuo, para el funcionamiento del sistema biométrico se necesita de un hardware, esto incluye sensores que llevan a cabo las mediciones, en cambio, otra parte del software compara los datos ya registrados previamente.

El sistema que se utiliza con más frecuencia dentro del campo en diversas situaciones es el de reconocimiento de huellas dactilares o digitales, tomando en cuenta que puede haber un margen de error, aunque esto no conlleva a un problema mayoritario. Para que el sistema biométrico entre en funcionamiento, se podría decir que es necesario una parte física que es el hardware, ya que en su mayoría se compone de muchos sensores que permiten llevar a cabo la medición y a la vez se ejecuta las comparaciones entre datos que están ya previamente registrados en la plataforma (Cortez, Medina, & Muriel, 2010).

Un sistema biométrico es un sistema que realiza trabajo de biometría, es decir que realiza reconocimiento a través de características personales, que puede ser verificada de manera automatizada.

La biometría es un sistema de seguridad que identifica a la persona, y tiene un elevado nivel de confiabilidad al momento de identificar individuos, tiene como base el reconocimiento de las características físicas que son únicas e inimitables y no se pueden transferir de una persona a otra como, por ejemplo: el reconocimiento facial, huella digital, patrón del iris.

2.2 Sistemas biométricos más utilizados

a) **Reconocimiento facial:** miden la distancia entre los ojos, la apariencia de la nariz, el contorno de la boca o la forma de la mandíbula.

b) **Reconocimiento de la voz:** funciona mediante la digitalización de diferentes palabras entonadas por una persona.

c) **Retina del ojo:** este sistema mide el patrón de las venas del ojo, se alcanza a través de la luz infrarroja de la pupila.

d) **Reconocimiento de la huella dactilar:** Esta técnica es la más usada en todo el mundo, afirmando que la huella dactilar es única y no van a cambiar a lo largo de su vida, se identifican principalmente en la dirección y ubicación de las crestas, valles, bifurcaciones.

2.3 Arquitectura de un sistema biométrico

En la siguiente figura se representa la arquitectura de un sistema biométrico.

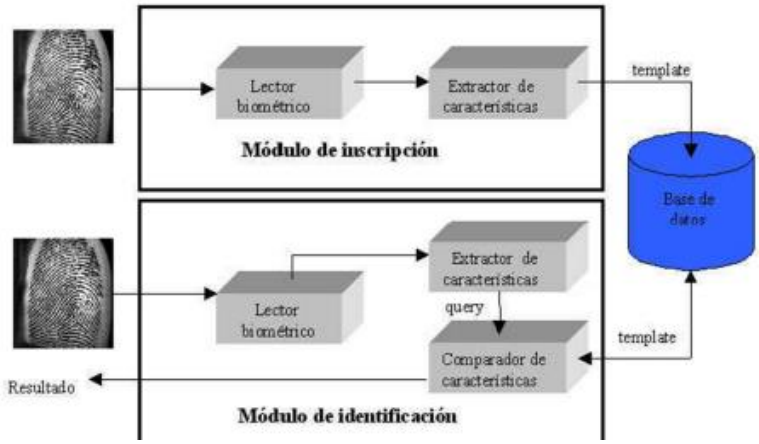


Figura 2. 1: Arquitectura de un sistema biométrico con huella dactilar

Fuente: (Cortes , Jimy, Medina, & Francisco , 2010)

La arquitectura de un sistema biométrico se concibe por medio de dos módulos:

Módulo de inscripción: es el que se encarga de adquirir y almacenar las señales que provienen del biométrico, con la finalidad de comprobar que la señal obtenida proporciona directamente del sistema, esto es posible gracias al lector biométrico del extractor de características.

Módulo de identificación: es el que se encarga del reconocimiento del individuo, este proceso se da cuando el lector biométrico ya captura dichas características del ser humano, de esta manera pasa a ser verificado y posteriormente las convierte en un formato digital llamado TEMPLATES.

En resumidas palabras, se puede decir que el sistema biométrico tiene un lector que se encarga de obtener datos que son relativos y a su vez entregar un formato de forma digital, este extractor toma particulares representativos a partir de la salida de dicho lector, en la cual será almacenado en la base de datos que se conoce como template que son usados en la identificación en el punto de acceso (Cortes , Jimy, Medina, & Francisco , 2010).

Estos sistemas tienen dos objetivos clave, el primero es identificar al individuo utilizando los datos y comparándolos con las bases de datos, el segundo objetivo es verificar la identidad del ser humano basándose en la utilización de los datos y comparándolo con el mismo (Ruiz, Rodriguez, & Olivares , 2009).

2.4 Elementos principales de los dispositivos biométricos

- Uno de los elementos principales se refiere a la adquisición digital del indicador biométrico de la persona.

- El segundo elemento es la compresión, almacenamiento, procesamiento y comparación de los datos almacenados.

- En el tercer elemento se da un interfaz con aplicaciones que se ubican en el sistema.

2.5 Etapas para la identificación de un sistema biométrico

Para la identificación de las técnicas biométricas, existen muchas variables porque cualquier patrón de una persona es utilizable de manera significativa como un componente de identificación biométrica. En la siguiente figura se muestra gráficamente la identificación biométrica (Ruiz & Olivares , 2009).

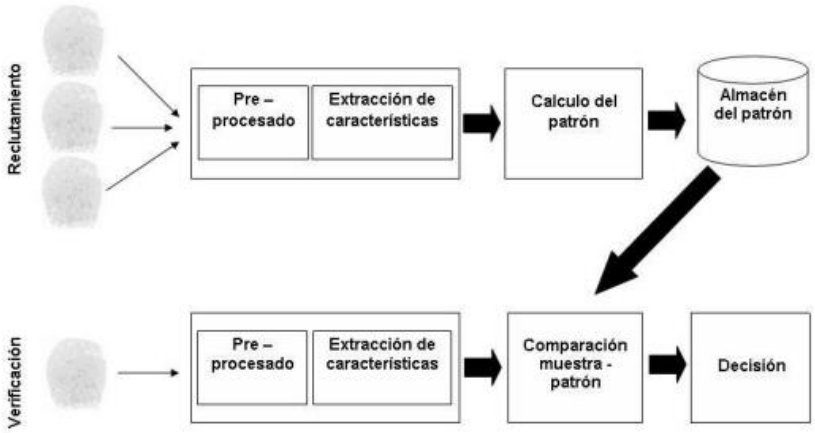


Figura 2. 2: Verificación y reclutamiento

Fuente: (Ruiz & Olivares , Una mirada a la biometria, 2009)

a) **Reclutamiento**: En esta etapa se procede a tomar numerosas muestras del usuario para procesarla y a su vez extraer el patrón deseado, el cual se almacenará, de esta forma se podrá caracterizar al usuario, es por ello que es importante tomar algunas muestras para que las características obtenidas sean más precisas, todo este proceso se tiene que realizar de manera supervisada, es decir tiene que estar presente una persona que será la encarga de llevar un control al momento de la captura de datos, de esta manera también se asegura la identidad de la persona o trabajador.

b) **Utilización:** Luego de haber obtenido los datos se tiene almacenado el patrón del trabajador, ya se puede utilizar el procedimiento con normalidad comparando sus características del usuario, de esta manera de determina el éxito o el fracaso.

Las fases de las características biológicas o de comportamiento son:

a) **Captura:** En esta fase se toman datos bio- físicos, es decir el comportamiento del ser humano, esto depende de la técnica que se empleó, esta fase llega a ser muy importante porque existe una conexión entre hombre y máquina.

b) **Preprocesado:** en esta fase los datos que son capturados van a facilitar el siguiente paso, se realizan tareas como reconocer la primera fase y de esta manera realizar una extracción de la imagen dada.

c) **Extracción de características**: esta fase se considera lo más significativo de dicha técnica, considerando que esta etapa los datos dados son procesados y las características de alguna manera forman una plantilla, que serán almacenadas en la base de datos para su uso.

d) **Comparación:** una vez que se tiene las características de las capturas, se comparan con las que están previamente guardadas, tomando en cuenta que al hablar de comparación no se trata de una comparación que es binaria o de

igualdad, sino más bien, se trata de las variaciones de las muestras, por lo tanto, para determinar si se obtuvo éxito o fracaso en la comparación, se tendrá que determinar N de tolerancia a la probabilidad.

1) Reconocimiento y autenticación: Este proceso está basado en los esquemas del funcionamiento del sistema de seguridad biométrico, el reconocimiento se basa en la identificación del usuario en comparación con los demás usuarios que se encuentran registrados en una base de datos.

La autenticación, también conocida como verificación, responde una pregunta sencilla pero importante: ¿este usuario es la persona?, este bosquejo permite al usuario a quién se le tomaron las características pertinentes comunique su identidad, es decir dicho sistema está encargado de realizar una comparación de las características que fueron extraídas con el usuario que introduce el patrón, si dicho usuario supera una determinada similitud es considerado el usuario indicado, de esta forma se rechaza la comparación con otros usuarios. En la siguiente figura se muestra el proceso de reconocimiento y autenticación que debe llevar a cabo un sistema de reconocimiento biométrico.

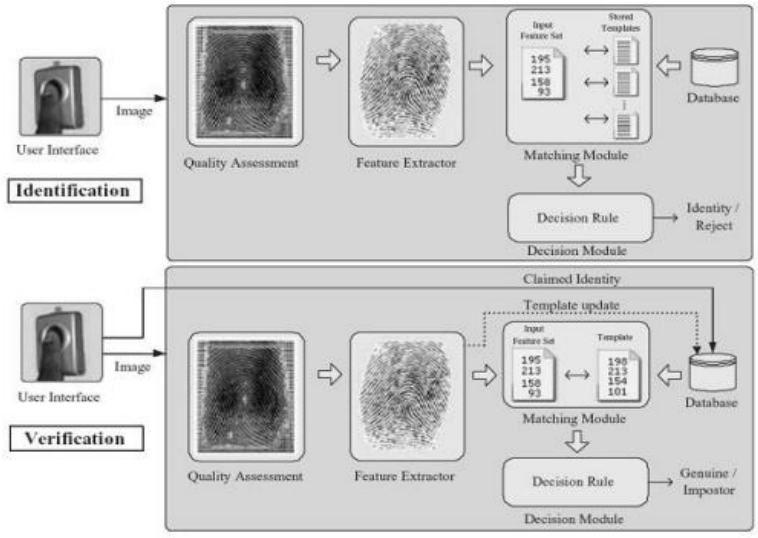


Figura 2. 3: Reconocimiento y autentificación

Fuente: (Ruiz, Rodriguez, & Olivares , Una mirada a la biometria, 2009)

2) Medición del rendimiento: Este punto es muy importante ya que se trata del rendimiento del funcionamiento del sistema biométrico, esto hace referencia a la tasa de error igual, es decir Equal Error Rate (ERR) y el valor dprima es decir Dprime Value,

cuando existe un rendimiento bueno el sistema bota un valor bajo en el (ERR), lo que hace el valor dprima es medir la separación de las medias de la probabilidad del impositor y el genuino (Ruiz, Rodriguez, & Olivares , Una mirada a la biometria, 2009).

2.6 Técnicas biométricas

La biometría radica en medir los rasgos únicos del ser humano en la cual permite identificarse de un individuo a otro, por consiguiente, se debe elegir una característica fuerte del individuo, para el funcionamiento del sistema biométrico se necesita de un hardware que esto incluye sensores que llevan a cabo las mediciones, en cambio otra parte del software compara los datos ya registrados previamente (Pérez, 2018).

Existen varias técnicas para la identificación del ser humano en el sistema biométrico, entre los más comunes están:

a) **Técnica de reconocimiento facial:** Actualmente el reconocimiento facial ha generado menos probabilidad de confiabilidad ya que los sistemas que se basan en reconocimiento facial intentan medir algunos puntos del rostro, es decir miden la distancia entre los ojos, la apariencia de la nariz, el contorno de la boca o la forma de la mandíbula, en dicho análisis el sistema elimina algunos inconvenientes que se pueden generar al momento del reconocimiento como son: la sombra, pose de la cara o expresiones inusuales del rostro, hoy en día existen muchos códigos que permiten un estudio de manera más simple como en la red social Facebook.

b) **Técnica de reconocimiento de la voz**: Este sistema fue utilizado a inicios de los años 60, considerándose este sistema como el más eficaz, funcionando de esta manera mediante la digitalización de diferentes palabras entonadas por una persona, obteniendo segmentos de 3 a 4 tonos dominantes capturados de forma digital, donde se guarda en la plantilla de la voz.

c) **Técnica de retina del ojo:** Este sistema mide el patrón de las venas del ojo, se alcanza a través de la luz infrarroja de la pupila, este sistema no es muy confiable ya que se puede producir irritaciones oculares.

d) **Técnica de reconocimiento de la huella dactilar:** Esta técnica es la más usada en todo el mundo, afirmando que la huella dactilar es única y no van a cambiar a lo largo de su vida, por lo general la huella digital se conforma por series de líneas y series de espacios que se representan los valles. Las huellas dactilares se identifican principalmente en la dirección y ubicación de las crestas, valles, bifurcaciones (Madrigal, Ramirez, & Hoyos, 2007).

Se puede decir que las características del comportamiento de las personas son reconocidas como biometría dinámica, en cambio la medición de dichas características corporales es reconocida como biometría estática (Mendoza & Mendoza, 2016).

1) **Dinámica del teclado:** esta técnica está basada en reconocer la forma en la que el usuario escribe, manteniendo la hipótesis de que es una técnica basada en el comportamiento, aunque también existen limitaciones al no poder ser utilizada con frecuencia, entre usuarios que no mantienen una facilidad al momento de escribir en máquina.

2) **DNA:** es una técnica que es idónea a la hora de identificar de manera unívocamente a un usuario, además siendo esta técnica capaz de utilizar el sudor como muestra para la máquina.

3) **Firma:** esta técnica es la más antigua dentro del campo, aunque tiene la posibilidad de que existan falsificaciones porque está basada en las características que tiene el ser humano en su comportamiento además de tomar en cuenta el acto de firmar, de esta manera se muestra una tabla grafica como parámetros de velocidad o posición del polígrafo.

4) **Olor:** esta técnica es muy reciente dentro del campo, tratando de reconocer a un individuo mediante el olor corporal, teniendo así una gran incógnita del rendimiento de dicha técnica, frente a colonia u olores que existen en el entorno ambiental.

5) **Geometría del mano o del dedo:** En esta técnica se estudian diversos estándares morfológicos de la mano o del dedo del individuo como, por ejemplo, la altura o la anchura.

En la siguiente figura se describen las diferentes técnicas de reconocimiento biométrico existentes, las ventajas y las limitaciones que presenta cada una de ellas.

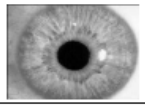
TECNICA	VENTAJAS	INCONVENIENTES
 VOZ	-Muy bajo costo -En algunas aplicaciones puede resultar inapropiables para el usuario(por ejemplo servicios telefónicos)	-Rendimiento bajo. -Se está estudiando el aumentar la unicidad y la estabilidad
 HUELLAS	-Muy estudiado/desarrollado -Unicidad, estabilidad y rendimientos altos. -Reconocimiento legal. -Medio coste	-connotaciones "policiales" para el usuario -Detención de dedo vivo, depende de pruebas colaterales a la captura
 IRIS	-Unicidad mayor que huella -Gran estabilidad por protección de la cornea. -FAR prácticamente nula. - Fácil detención de ojo vivo	-Alto coste. -Inicialmente incomodo para el usuario
 MANO	-Fácil uso y gran aceptación por el usuario. -Medio coste. -Bajo coste computacional. -Sin connotación "policial"	-unicidad y estabilidad no probadas en grandes poblaciones. -Detención de mano viva, depende de pruebas colaterales
 ROSTRO	-Cómodo, e incluso inapreciable para el usuario. -Medio coste	-Sensible a cambios del sujeto (barbas, gafas, pelos….). Todavía en investigación y desarrollo

Figura 2. 4: Ventajas y desventajas de las técnicas biométricas

Fuente: (Ruiz & Olivares , Una mirada a la biometria, 2009)

2.7 Parámetros para la elección de una técnica biométrica

1. **Universalidad:** es decir que las características de ser humano pueden ser extraída de cualquier usuario.

2. **Estabilidad:** dichas características extraída tienen que permanecer en relación con diferentes parámetros, por ejemplo, la edad, el tiempo y las enfermedades.

3. **Unicidad:** la probabilidad es nula que dos sujetos tengas las mismas o igual características.

4. **Rendimiento:** se tiene que tomar en cuenta el acierto y el margen de error.

5. **Facilidad de captura**: deben de existir formas sencillas de poder capturas los datos de comportamiento del individuo.

6. **Aceptación:** esta fase es de gran importancia para poder tener colaboración.

7. **Coste**: este es un requisito para la seguridad del usuario y de la identificación.

8. **Robustez:** si la técnica seleccionada puede capturar de manera inmediata fotos o dedos de látex, se tendría que anular dicha técnica.

2.8 Beneficios del uso del sistema biométrico

La utilización de las tecnologías biométricas trae un conjunto de ventajas tanto para el sector público como privados, a pesar de que estas medidas están relacionadas específicamente con a la ciberseguridad, algunos de los beneficios que brindan a los usuarios como (Perez, 2016):

1. Reducción en mantenimiento del sistema
2. Control diario del horario
3. Mejoría de la imagen de la corporación

Las ventajas del sistema biométrico son:

1. Comodidad, porque queda almacenado la información
2. Resiste al fraude
3. Se asocia o se enfoca en un usuario en concreto

2.9 Datos biométricos

Los datos biométricos son aquella información que es manual o computarizada, se recolecta por medio de alguna persona u organización ya sea pública o privada, dichos datos deben ser bajo consentimiento del usuario (Zurita, 2004).

2.10 Legislación latinoamericana en el uso del sistema

En América latina este sistema es utilizado con mucha frecuencia y es más evidente en los sectores públicos que en los privados, pero esto tiene un marco jurídico, es decir dentro el sector público los cuidados comunes no tiene acceso a dichos datos (Gonzalez & Perez, 2012).

2.11 Riesgos y retos del sistema

El uso del internet ha ocasionado un gran riesgo en la seguridad y privacidad, los riesgos que se tienen son diversos pero, entre lo más primordiales es el robo y el fraude, pues si solo se tiene un identificador que se conecta con la base de datos y este es robado pues no se tendrá acceso a los datos (Quintanilla , 2020).

2.12 Puntos fuertes y débiles que existen en el sistema biométrico

- **Confidencialidad**, la contraseña la pueden copiar otros usuarios, pero la ventaja es que el único que tiene unas medidas determinadas es el usuario.

- **Mantenimiento económico**, una vez que se instala el sistema quedan grabados los datos biométricos.

Cada uno de los sistemas biométricos utiliza cierta clase de interfaz, en la cual recopilan la información de la persona que quiere acceder, dicho software especializado comienza a procesar la información de los datos comparándolo con otros usuarios que se introdujeron previamente al sistema, si dicho usuario se encuentra en la fase MATCHING, se confirma la identidad del usuario y se procesa al acceso de registro (BALDEÓN, 2016).

2.13 Hardware para implementar en el sistema biométrico

2.13.1 Placas Arduino

Existen más de 30 modelos de Arduino con sus respectivas características, entre ellos varían los tamaños, lo que da gran amplitud a diferentes proyectos complejos y sencillos, aun así, cada vez van saliendo más modelos de Arduino que permiten abordar todos los campos.

La placa Arduino se define como un microcontrolador que facilitará los procesos involucrados en la medición y almacenamiento de los datos, es un hardware que posee un código abierto, perfecto para la elaboración de los dispositivos que van a permitir la interacción física con el medio ambiente (Vega & Rivas, 2014). Arduino es una plataforma electrónica con código abierto a la que se le puede dar diferente tipo de utilidad.

El Arduino es un componente que se conecta de manera fácil a otra red, permitiendo que servidores con protocolos de nivel alto se conecten, tiene capacidad de procesamiento, memoria, programación de lenguajes y puertos físicos. Existen diferentes tipos de Arduino entre ellos, los siguientes:

- **Arduino Ethernet Shield**

Se basa en el chip Wiznet W5100, promoviendo una pila de red IP, que soporta cuatro conexiones de manera simultánea, usando librería Ethernet para poder escribir programas, además dispone conectores que van a permitir conectarse con más placas Arduino, esta placa tiene un conector estándar RJ45.

- **Arduino Mega 2560**

Esta placa está basada en ATmega 2560, en la cual tiene 54 pines de entrada y salida que son digitales, 16 entradas y salidas analógicas, cuatro puertos seriales, conexión vía USB, un oscilador 16 MHz de cristal y un botón para reinicio. Esta placa es compatible con un gran número de protectores que son diseñados para el Arduino Diecimila.

El Arduino está conformado por una placa, apoyada en un microcontrolador ATMEL, estos microcontroladores son circuitos integrados, que pueden grabar instrucciones, dichas instrucciones interactúan con los diferentes circuitos de placa (Herrero & Sanchez, 2015).

El Arduino tiene un microcontrolador, llamada interfaz de entrada, en la que se puede conectar diferentes tipos de periféricos, se encargara de procesar los datos que lleguen a través de ellos (Vargas, Castillo, & Sandoval , 2015).

Además, estos tipos de Arduino también cuentan con una interfaz de salida encargada de llevar la información procesada, existen diferentes tipos de placas, cambiando su forma, tamaño y colores dependiendo del proyecto en lo que se vaya a utilizar.

- **Arduino UNO**

La más representativa entre los usuarios Arduino es ésta por su sencillez al momento de usarla y su bajo costo, hacen que esta plataforma sea la más adecuada como una opción final dentro de todos los proyectos que se implementan. Este sistema está compuesto por un microcontrolador de 8 bits, que incluye un conversor digital y analógico, su placa posee un LED conectándose al pin 13, es decir que utiliza como un dispositivo de verificación y depuración (Lopez & Gustavo , 2013).

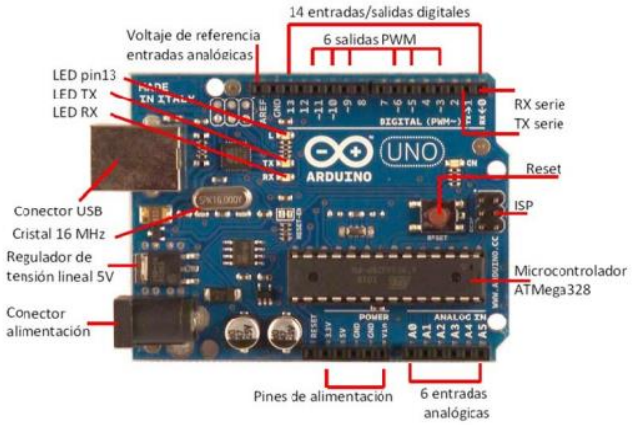


Figura 2. 5: Arduino Uno

Fuente: (Herrero & Allende,2015)

- **Arduino Tre**

Está basado en un procesador Sitara, incluye 1 puerto Ether, 1 puerto USB 2.0 y 4 puertos USB host, es decir son dos sistemas en uno, que permite editar, compilar y a la vez ejecutar los sketches.

- **Arduino Robot**

Este es un sistema que es super completo y tiene la forma de un robot, ya que posee dos placas Arduino, una que viene a ser de control y otra de motores.

- **Arduino Fio**

Este Arduino tiene 14 pines de entrada y salida que son digitales, entre ellas 6 son de salida y 8 de entrada, está fabricada para aplicaciones inalámbricas montada en un módulo Xbee.

- **Arduino Pro**

Este Arduino posee 14 pines, entre ellas de entrada y salida, se distribuyen de la siguiente manera 6 tiene la función de salida, en su mayoría se utiliza para realizar instalaciones semipermanentes.

- **Arduino LilyPad Usb**

Este Arduino tiene 9 pines, entre ellas de entrada y de salida que son digitales, poseen una memoria de 32 Gb., este dispositivo está diseñado para utilizarlo electrónicamente en ropa de vestir, para lo cual se puede coser a la ropa con hilos especializados.

2.14 Compatibilidad Arduino

Arduino posee una plataforma abierta, es decir puede modificarse en cualquier segundo, aunque es necesario limitar varias prestaciones para mantener una buena compatibilidad. Algunas empresas comercializan plataformas que son similares a un Arduino pero que incorporan la conectividad vía bluetooth.

2.15 Programación Arduino

Existen muchos softwares que permiten utilizar la plataforma Arduino, la mayoría son gráficas, generando códigos para que el Arduino funcione de manera autónoma.

A continuación, señalamos aplicaciones entorno a la programación y aplicaciones que interactúan directamente con la plataforma:

2.15.1 Ardublock

Es similar a la aplicación java, dicha programación da encajando las instrucciones del lenguaje Arduino, configurando parámetros, de esta manera de genera códigos.

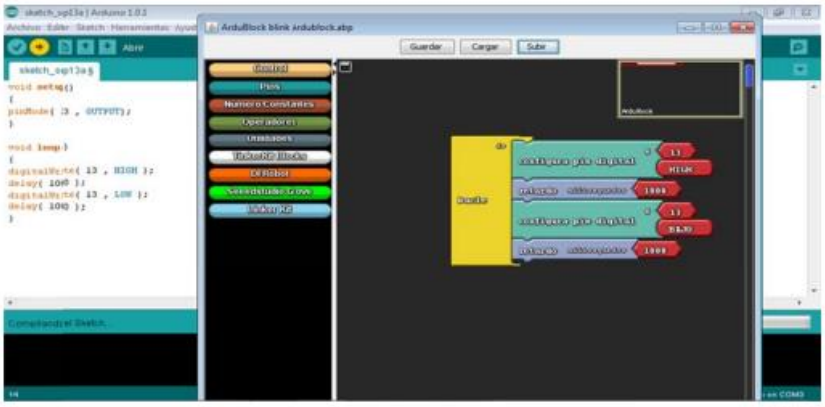


Figura 2. 6: Ventana de Ardublock

Fuente: (Herrero & Allende,2015)

2.15.2 Minibloq

Esta aplicación permite programar distintas plataformas de Arduino, a través de sencillos códigos que se van configurando, dependiendo de sus parámetros, este programa en general recopila datos para posteriormente enviar el código al Arduino, es software libre.

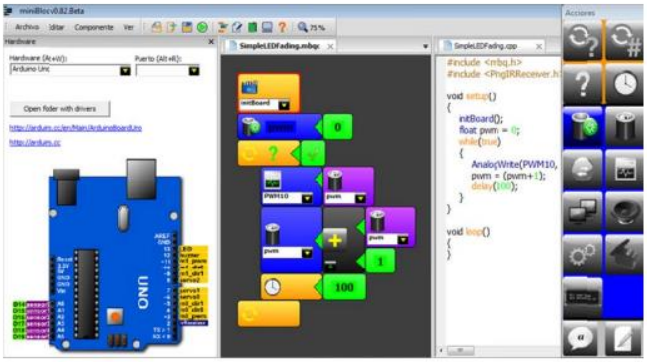


Figura 2. 7: Programación Minibloq

Fuente: (Herrero & Allende,2015)

2.15.3 Modkit

Este software permite programar diferentes plataformas entre ellos está Arduino, se configuran mediante valores, generando de esta manera el lenguaje apropiado para los códigos, se realiza mediante una aplicación WEB abierta desde el navegador.

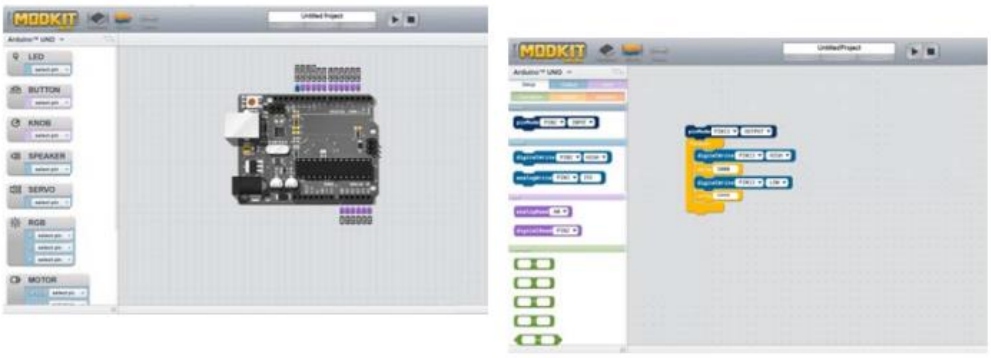


Figura 2. 8: Configuración Modkit

Fuente: (Herrero & Allende,2015)

2.15.4 Scratch

Este programa es enfocado para niños con edad promedio de 10 años, es fácil de manejar ya que el bloque se divide para formar el programa, de esta manera crea animaciones, músicas y juegos interactivos.

Figura 2. 9: Configuración Scratch

Fuente: (Herrero & Allende,2015)

2.15.5 Physical Etoys

Este programa se utiliza con fines didácticos, ya que está orientado en la educación de los niños al ser un programa visual, permitiendo así escribir datos para posteriormente ser leídos.

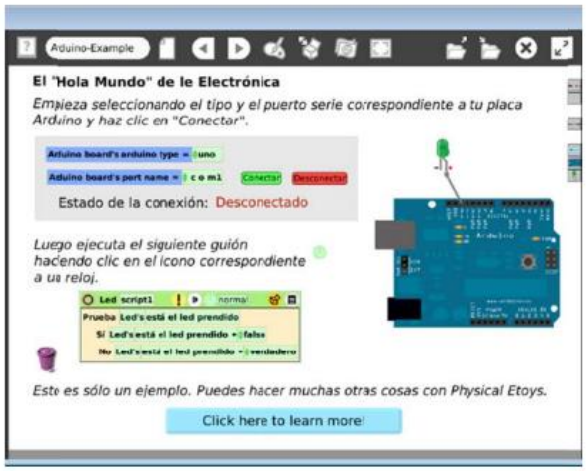


Figura 2. 10: Configuración Physical

Fuente: (Herrero & Allende,2015)

2.15.6 Ardulab

Este programa permite crear un laboratorio de manera virtual, que experimente con conectores y sensores sin la necesidad de alguna otra aplicación, este programa está relacionado con electrónica y robótica, para poseer dicho programa se debe tener licencia.

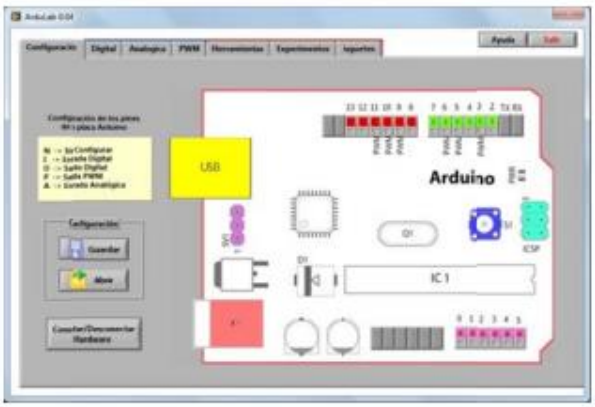


Figura 2. 11: Configuración Ardulab

Fuente: (Herrero & Allende,2015)

2.16 Lenguaje de programación de Arduino

El lenguaje que se utiliza para escribir en los programas es parecido a C++, teniendo la función setup, siendo así la primera función en ejecutarse y hacerlo una sola vez, en cambio la función loop se ejecuta cíclicamente, lo que da la activación de salidas y lectura de entrada, con sus respectivas comprobaciones.

2.17 Fritzing

Fritzing siempre será una herramienta necesaria para poder diseñar Arduino u otras en general, permite montar y documentar prototipos, de esta manera se realiza un montaje del diseño que se va a utilizar interna y externamente.

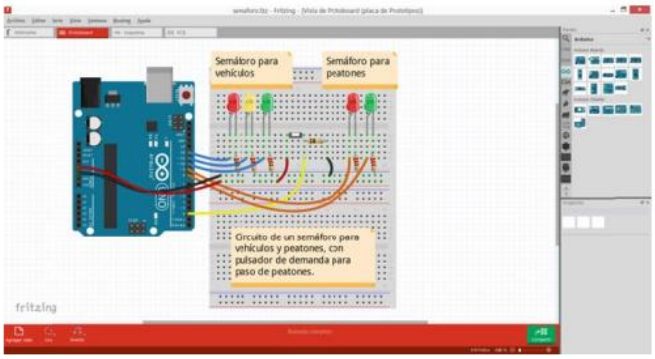


Figura 2. 12: Configuración externa

Fuente: (Santander Frank,2016)

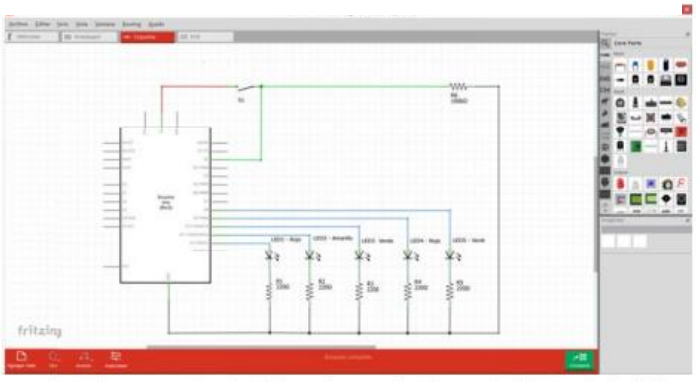


Figura 2. 13: Configuración interna

Fuente: (Santander Frank,2016)

2.18 Raspberry Pi 3

La Raspberry Pi 3, conlleva series de pequeños de miniordenadores, constituida por una placa simple con un bajo costo, tiene como objetivo impulsar en el aprendizaje de los niños y el manejo de la programación, hoy en día este modelo es muy popular en el sistema de internet.

Raspberry Pi 3 es una placa simple, compuesta por: un CPU, memoria RAM, puertos de entrada y de salida, SoC, conectividad de red, entre otros (Salcedo & Cendros, 2016).

Raspberry Pi 3 fue elaborada en el 2018 con una mejoría en su conectividad y el procesador, con una banda 2,4 GHz y 5 GHz además cuenta con un bluetooth 4.2.

La Raspberry Pi 3 utiliza un micro USB 5.1, todo depende de lo que se vaya a hacer, teniendo en consideración que esta necesita más corriente que los demás procesadores (Chaglia, Miranda , & Vasquez, 2011).

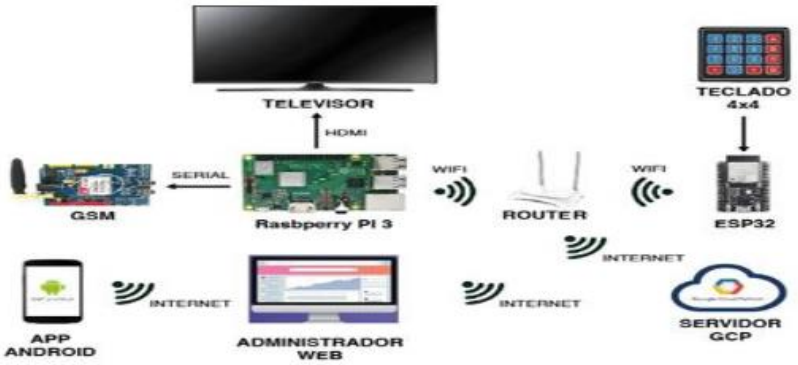


Figura 2.14: Raspberry Pi 3

Fuente: (Gabriel Franco,2020)

CAPITULO III: FUNCIONAMIENTO Y CONFIGURACIÓN DEL SISTEMA BIOMÉTRICO

3.1 Diseño del circuito

En el diseño del circuito fue necesario utilizar el software llamado Proteus 8 Profesional, el mismo que permite la simulación de circuitos eléctricos y electrónicos para comprobar las conexiones y el correcto funcionamiento en tiempo real de cualquier sistema electrónico siendo este el caso de un sistema biométrico.

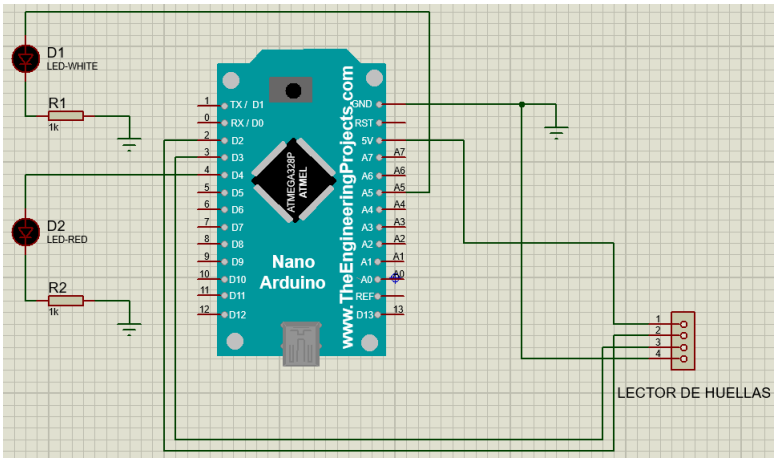


Figura 3. 1: Diagrama de conexiones del circuito en Proteus

Fuente: (Autor)

3.2 Diagrama de flujo del funcionamiento del algoritmo del prototipo

El funcionamiento del sistema biométrico inicia desde que el mismo es conectado a la corriente, desde allí el biométrico está a la espera de que el usuario coloque su dedo en el lector de huellas para que el patrón dactilar sea escaneado, procedente dentro de la codificación ocurre el proceso de validación de la huella para reconocer si el usuario está o no registrado en la base de datos.

Una vez realizado el proceso de validación, el sistema debe reconocer si el ID de la huella pertenece a la base de datos previamente ingresada, de no ser así se encenderá una luz led de color amarillo como advertencia de que el usuario no consta en la base de datos, como respuesta no se genera ningún mensaje al dispositivo móvil.

En caso de que en el proceso de validación de la huella se encuentre existente el ID en la base de datos, se encenderán dos luces led una de color azul y otra de amarillo, inmediatamente se generará un mensaje de texto hacia el dispositivo móvil del gerente indicando la hora y fecha en la que el usuario ha ingresado.

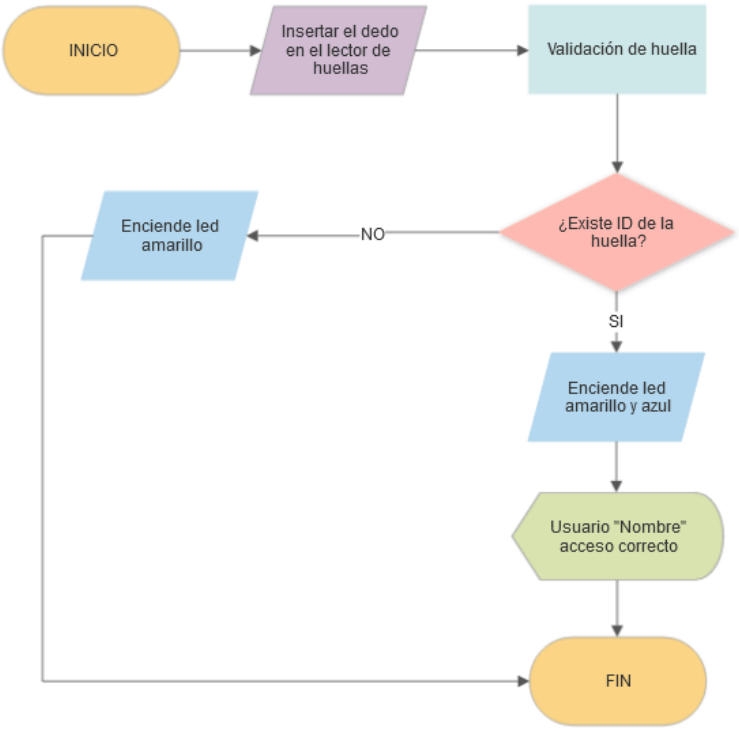


Figura 3. 2: Flujo de funcionamiento del algoritmo

Fuente: (Autor)

3.3 Diagrama de bloques del prototipo

En el diagrama de bloques se muestra la comunicación entre los módulos que permiten el funcionamiento del sistema biométrico, para identificar al usuario en el sistema biométrico inicia desde un sensor de huellas, el cual se comunica con el Arduino y este a su vez se enlaza por un cable USB a la Raspberry Pi 3 donde se tiene la programación del aplicativo web, su memoria de registro y su enlace hacia Telegram, el mismo que es necesario para conectar la mensajería hacia el celular del gerente, al recibir esta notificación se asegura que el usuario ha ingresado.

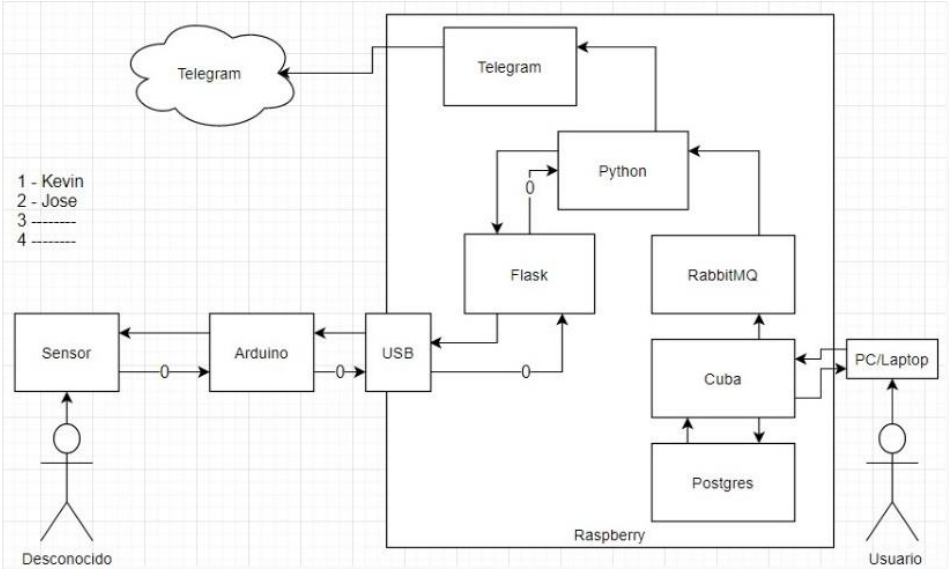


Figura 3. 3: Diagrama de bloques

Fuente: (Autor)

3.4 Diagrama esquemático del prototipo

Para el diseño del esquema se utilizó el software Fritzing, el mismo que permite generar un diagrama de conexiones mediante códigos de colores para el cableado que comunica a todos los componentes del sistema biométrico.

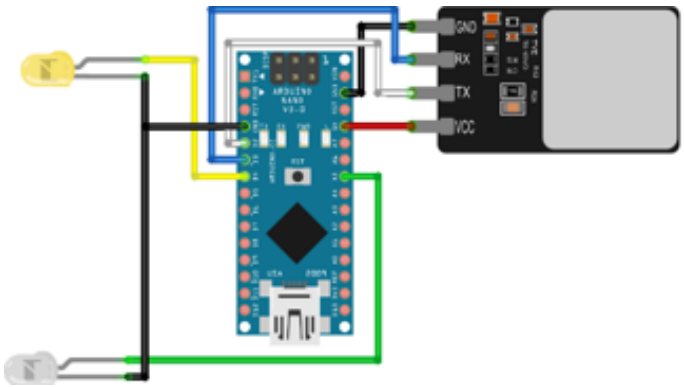


Figura 3. 4: Diagrama esquemático

Fuente: (Autor)

3.5 Diseño de la caja del biométrico

Como material de fabricación, se decidió elaborarlo de metal ya que con las pruebas realizadas de durabilidad sometiéndolo a caídas de 1,26 m de altura, dicho material no presento grietas ni anomalías en su estructura. Por ende, el material elaborado de fibra al aplicarle la misma prueba presentó una abolladura en una de sus esquinas, haciéndolo inseguro para los elementos que van dentro del armazón.

Se decidió hacerlo de forma cuadrada para evitar doblar mucho el material, ya que sus elementos deben tener una base firme y plana para ajustarse al mismo, y de paso esta forma permite una fácil instalación sobre superficies como una pared de cemento, madera o cerámica.

Figura 3. 5: Diseño final de la caja del biométrico

Fuente: (Autor)

3.6 Configuración del biométrico

3.6.1 Distribución y accesos de configuración

Para la configuración del biométrico, se utilizó el programa Visual Studio Code, este programa es muy versátil y accesible para elaborar los códigos y el mismo permite visualizar las imágenes, gracias a esto se pudo ejecutar los comandos más esenciales para elaborar el módulo de la Raspberry Pi 3 y el Arduino. Además, se debe tomar en cuenta los siguientes programas: Network IP Scanner, es el que se encarga de buscar la dirección IP de la Raspberry Pi 3, y Telegram que es un medio de mensajería muy utilizada en las redes sociales y que ahora se lo puede utilizar como una herramienta de trabajo.

3.7 Comunicación del biométrico

3.7.1 Herramientas del software

Para acceder al sistema biométrico, el teléfono del empresario debe tener acceso a internet y contar con el aplicativo Telegram, este vínculo entre ambos dispositivos necesita un programa llamado Network IP Scanner, este permite escanear la dirección IP de la Raspberry Pi 3, el cual se ingresará a la dirección del programa PuTTY.

Automáticamente se genera una página web, con el explorador de preferencia se puede acceder digitando la dirección IP de la Raspberry Pi 3 previamente encontrada, al abrir la página web se debe ingresar con un usuario y contraseña, esta seguridad es esencial para evitar el plagio de información de los trabajadores hacia al empresario gerente del almacén.

3.8 Funcionamiento del lector biométrico

3.8.1 Ingreso de huella dactilar al sistema biométrico

Se configura el lector biométrico con el Arduino, lo que ayudará a almacenar los datos que permiten interactuar con el contexto exterior y el Protoboard, de esta manera se enciende la luz azul, lo cual indica que ya está apto para que el empleador ingrese su huella y de esta manera sean tomados sus datos, (observar figura número 3.1), cuando el led se ponga de color amarillo indicará que el empleador ya puede quitar su huella dactilar porque sus datos ya están siendo procesados.

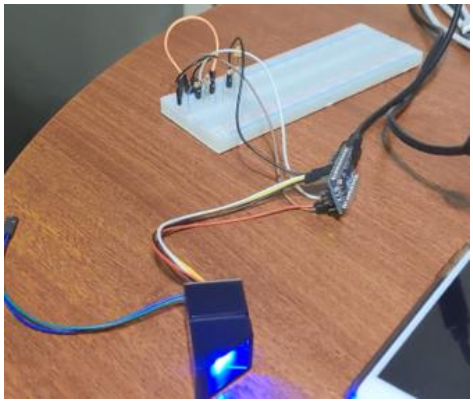


Figura 3. 6: Configuración con el Protoboard

Fuente: (Autor)

3.9 Materiales utilizados para la realización del sistema biométrico

3.9.1 Elementos indispensables para la elaboración del proyecto

Para la elaboración del sistema biométrico se usaron materiales como: lector de huella, Arduino nano, Raspberry Pi 3, Cable USB, cable UTP, Protoboard, un led azul y un led amarillo, resistencia de 1 kilo Ohm y cables jumper.

3.10 Composición del Protoboard

3.10.1 Distribución y enlaces del Protoboard

El Protoboard está compuesto por una resistencia de 1 kΩ, una fuente de voltaje de 5 v con entrada USB y cables jumper, estos cables se van a conectar con las resistencias y los leds, después se enlaza con el módulo de Arduino el cual procesa la información que el lector biométrico sustraerá a partir de la huella dactilar.

De forma inmediata la información le llega al empresario a su dispositivo móvil, es importante destacar que su teléfono móvil tenga que contar con datos móviles ya que la Raspberry Pi 3 se conecta vía internet, si es un usuario de la empresa "Phonix-Cell" se permitirá el acceso, caso contrario será retirado de las instalaciones.

3.11 Codificación del sistema

3.11.1 Elaboración y programación de hardware en el sistema biométrico

Se usó el programa Fritzing para identificar los componentes que se van a manejar mediante este software, permite simular el esquema de conexión del presente proyecto como se puede observar en la siguiente figura.

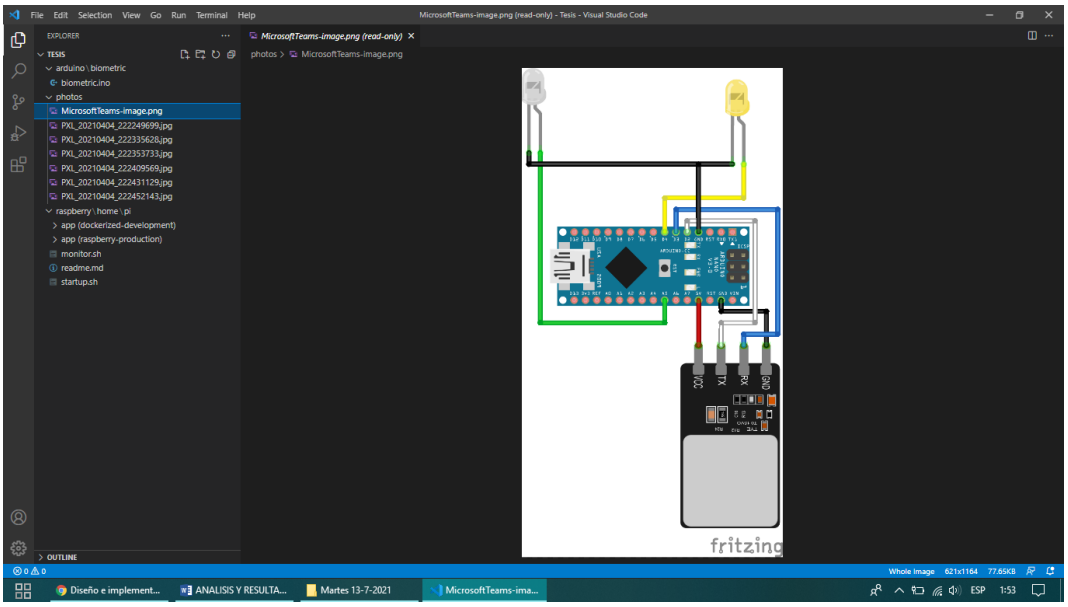


Figura 3. 7: Programa Fritzing

Fuente: (Autor)

Se conecta dos módulos mediante la simulación de Fritzing, se usó el módulo Arduino y el módulo Raspberry Pi 3, un led azul y un led amarillo; cuando se enciende el led azul significa poner el dedo, y al encender el led amarillo es para retirar el dedo del biométrico.

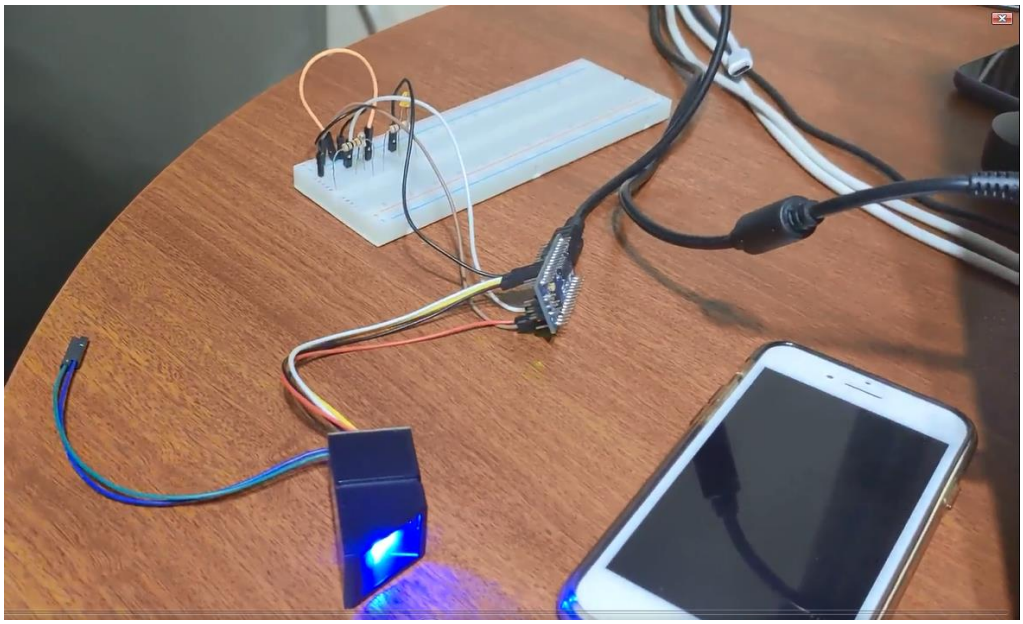


Figura 3. 8: Lector Biométrico

Fuente: (Autor)

El lector biométrico es configurado en el Arduino, y este a su vez es conectado a un Protoboard, donde se encuentran los leds de aviso azul y amarillo, los cuales indican que hay que poner el dedo y sacar el dedo del trabajador.

Para llevar el proyecto: diseño e implementación de una seguridad biométrica con cobertura de red, usando mensajería programada con Telegram asociado con Raspberry Pi 3 y Arduino para la empresa Phonix-Cell, partimos desde un Protoboard el cual tiene en sus elementos, un led azul y un led amarillo además dos resistencias de 1 kΩ, una fuente de voltaje de 5 v con entrada USB y cables jumper, estos cables se van a conectar con las resistencias y los leds, después se enlaza con el módulo de Arduino, el cual procesa la información que el lector biométrico le exporte después que se haya escaneado el dedo (de su elección) de los trabajadores.

En Visual Studio Code se encuentran tres carpetas importantes, las cuales serán: Arduino, fotos y Raspberry Pi 3.

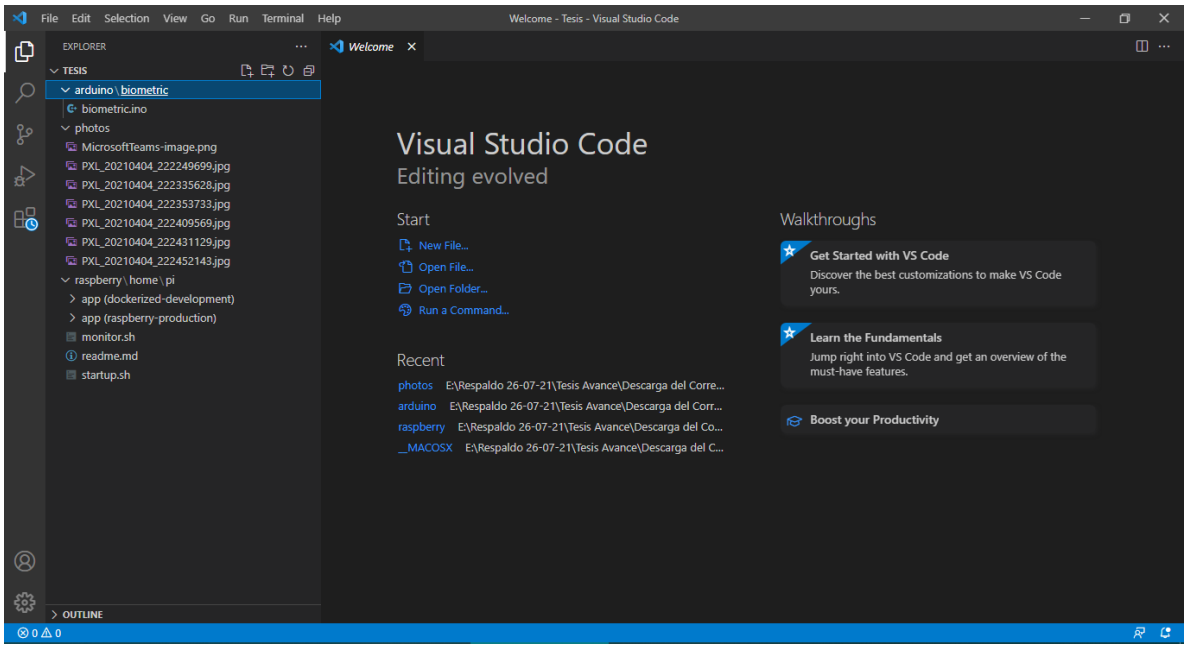


Figura 3. 9: Carpeta Arduino

Fuente: (Autor)

En este paso se tiene la carpeta Arduino, en la cual se encuentra el código del biométrico, teniendo estas 589 líneas de código.

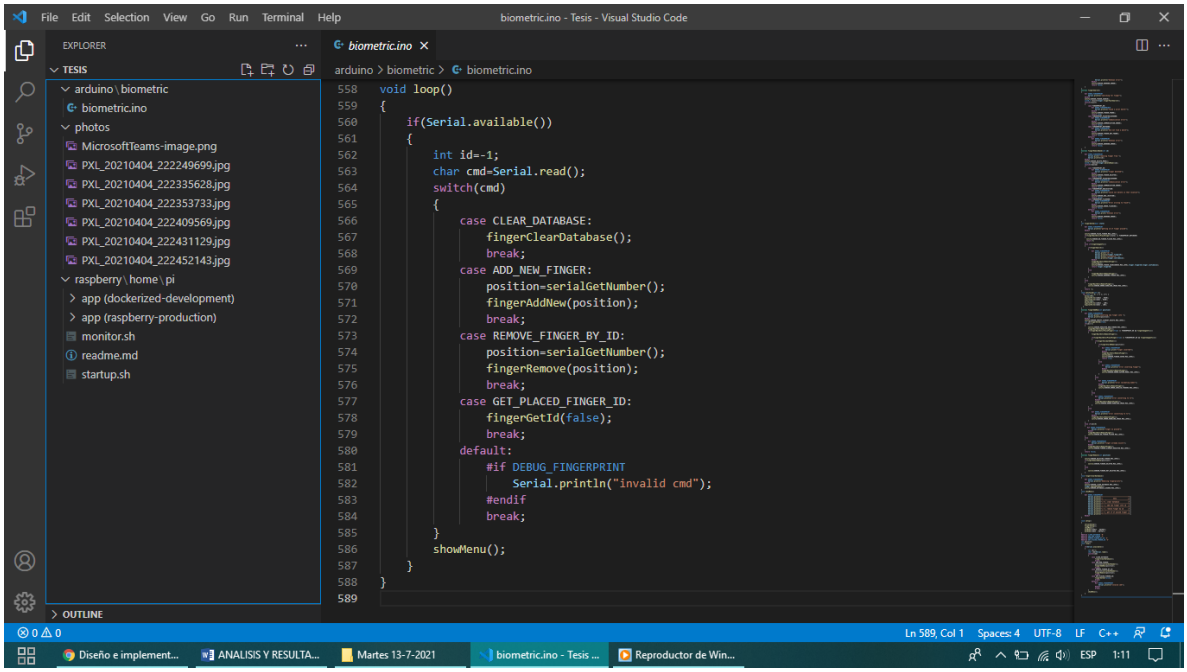


Figura 3. 10: Comunicación inalámbrica

Fuente: (Autor)

Dentro del código hay constantes que se envían a la Raspberry Pi 3, ya que el Arduino se comunica con la Raspberry Pi 3 inalámbricamente, si el dedo se encuentra presente en el lector biométrico, mandara la notificación de que un trabajador ha ingresado.

El setup es la primera función donde se ejecuta el Arduino, comienza elaborando el void setup la primera vez.

```
void setup()

{

   serialSetup();

   fingerSetup();

   showMenu();

   pinMode(ledOut , OUTPUT);
```

```
  pinMode(ledIn , OUTPUT);
```

Si se quiere encontrar el serial setup, se ejecuta el comando ctrl F, esto hace reflejar una pequeña ventana en la parte superior del código y se pulsa la tecla enter, mientras no haya un código serial listo, se espera a que el código serial esté listo para comunicarse e iniciar con la comunicación begin la comunicación serial.

```
pinMode(ledOut , OUTPUT);

pinMode(ledIn , OUTPUT);
```

Para identificar los pines del módulo Arduino, referente a poner la huella o sacar huella se tiene que los dos pines son salidas lo cual ledOut y ledInt, se los encuentra en la línea de código 4 y 5 en el pin (4 y A5) está conectado el sensor.

```
const int ledOut = 4;

const int ledIn = A5;
```

La configuración de los caracteres en el código, loop se los define como: limpiar la base de datos “0”, agregar huella”1”, borrar huella”3” o colocar el dedo”4”.

```
#define CLEAR_DATABASE '0'
#define ADD_NEW_FINGER '1'
#define REMOVE_FINGER_BY_ID '3'
#define GET_PLACED_FINGER_ID '4'
```

Inmediatamente, se ejecuta el void loop, las funciones que se elaboran previamente mencionadas son las que se ejecutan constantemente como un bucle.

```
void loop()
```

```
{
   if(Serial.available())
   {
      int id=-1;
      char cmd=Serial.read();
      switch(cmd)
      {
         case CLEAR_DATABASE:
            fingerClearDatabase();
            break;
         case ADD_NEW_FINGER:
            position=serialGetNumber();
            fingerAddNew(position);
            break;
         case REMOVE_FINGER_BY_ID:
            position=serialGetNumber();
            fingerRemove(position);
            break;
         case GET_PLACED_FINGER_ID:
            fingerGetId(false);
            break;
```

```
        default:
            #if DEBUG_FINGERPRINT
                Serial.println("invalid cmd");
            #endif
            break;
    }
    showMenu();
  }
}
```

En el loop, si hay mensajes por el puerto serie o hay mensajes viniendo de la Raspberry Pi 3, se va a leer un carácter, si ese carácter es limpiar la base de datos cero, agregar nueva huella o eliminar la huella entonces ejecutará una acción, la Raspberry Pi 3 le manda un uno, y automáticamente el sistema agrega una nueva huella y ejecuta la acción de agregarlo al sistema.

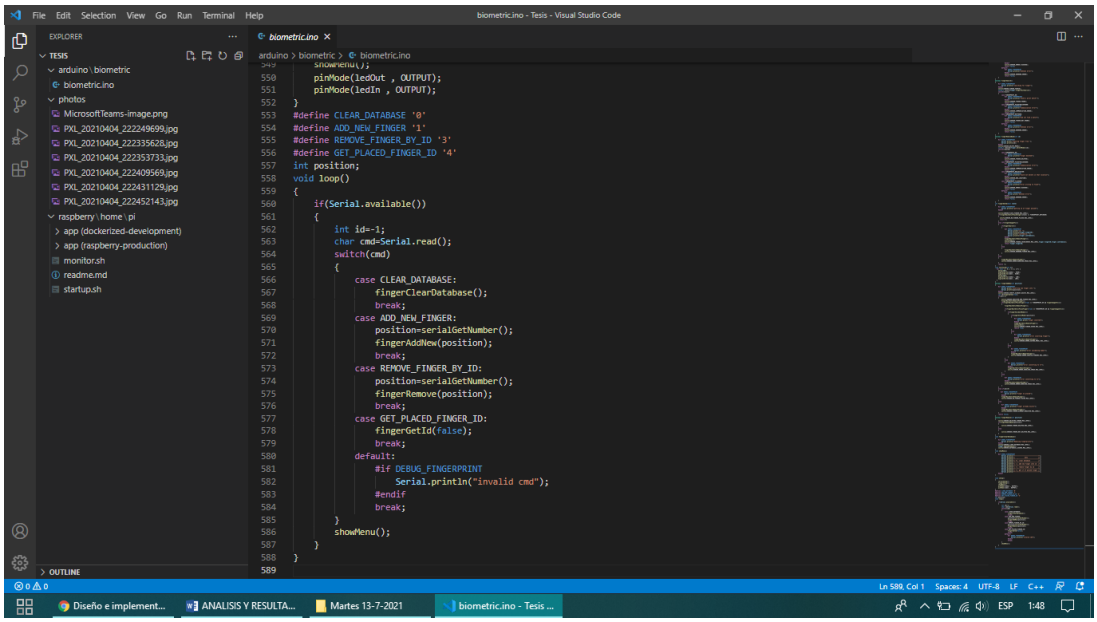


Figura 3. 11: Comunicación del Raspberry Pi 3

Fuente: (Autor)

El módulo de Arduino siempre está atendiendo a lo que pida la Raspberry Pi 3, en este análisis se une los componentes del proyecto, como son: los cables, resistencias, leds, Arduino y Raspberry Pi 3, como se muestra en la figura.

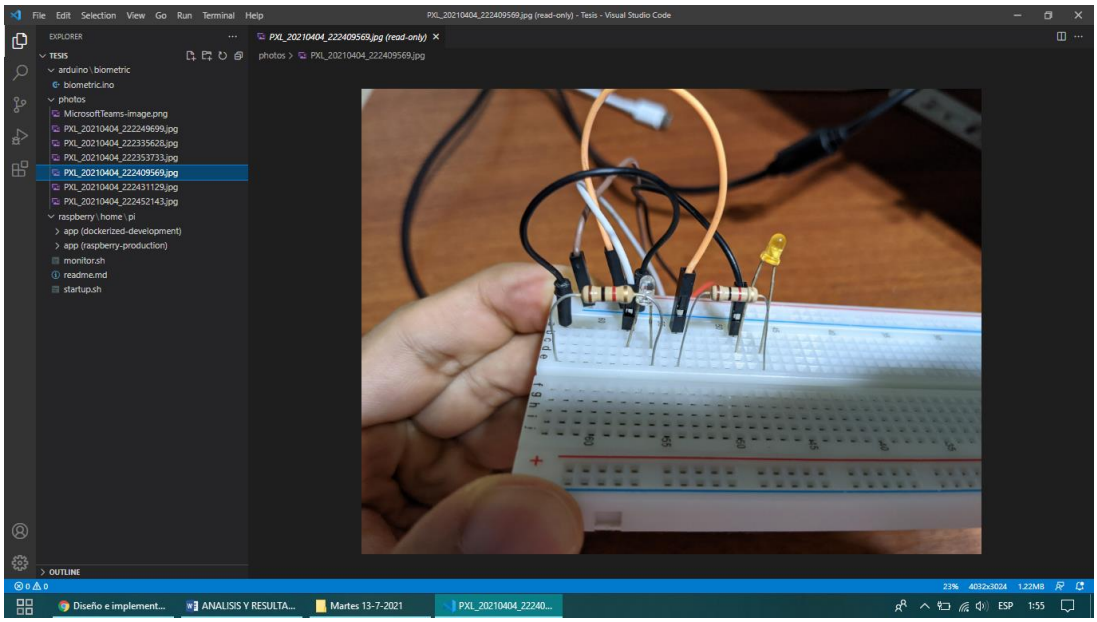


Figura 3. 12: Diseño de Protoboard

Fuente: (Autor)

El diseño comienza desde el Protoboard, se colocan dos resistencias de 1 KΩ cada una, paralelo a la resistencia se coloca el led amarillo, la parte de color dorado de la resistencia se unirá a la parte negativa del led, la parte positiva del led está conectada a un cable de color negro, este cable proviene del Arduino, mientras tanto el led azul se lo ubica en la siguiente resistencia, la parte negativa del led se une a la terminal de color dorado de la resistencia, la parte positiva del led se conecta al cable blando, este cable proviene del Arduino, la alimentación de voltaje para el Protoboard está suministrado por el Arduino.

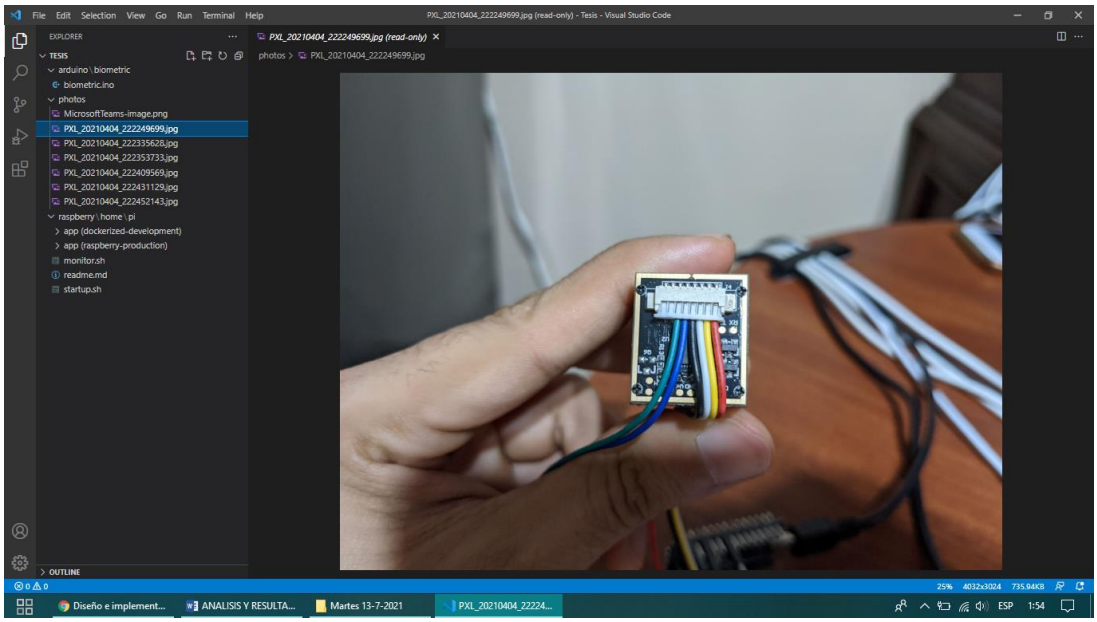


Figura 3. 13: Parte posterior del lector de huella

Fuente: (Autor)

En este paso, se observa la parte posterior del lector de huella, se verifica los pines de conexión para la comunicación de información con el módulo de Arduino.

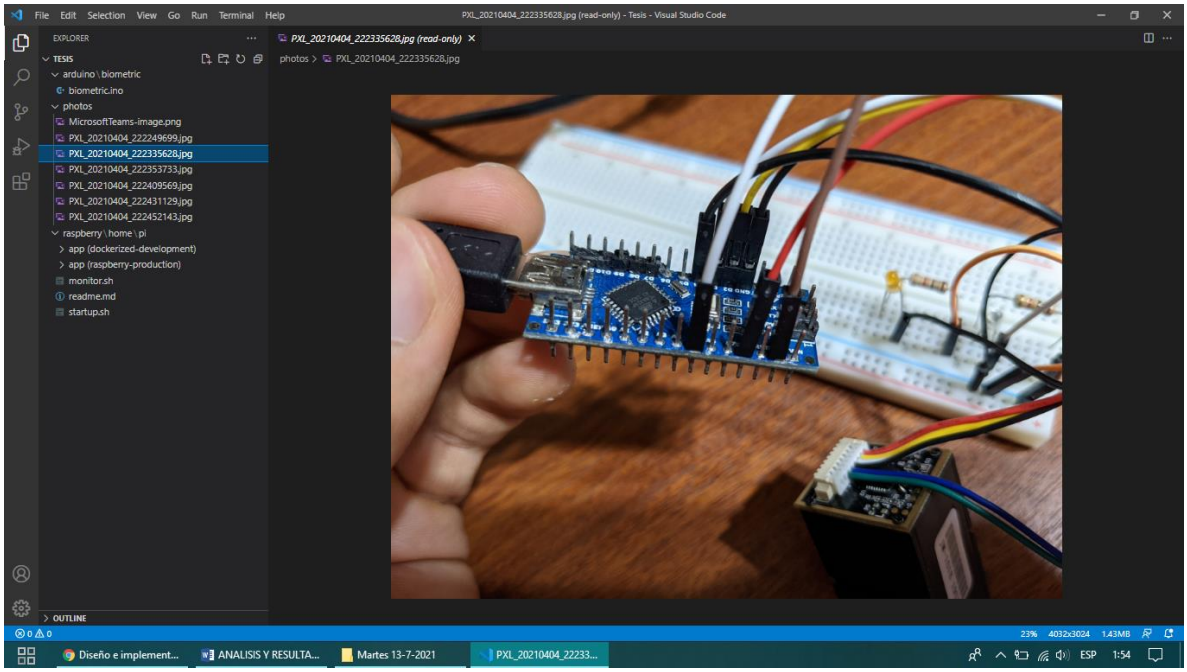


Figura 3. 14: Conexión del cableado

Fuente: (Autor)

En esta imagen se conectan los cables jumper hacia el Arduino, el primer cable de color café está conectado al pin VIN (este pin es una fuente de alimentación de voltaje externo el cual suministra voltaje de 5 volts).

El cable rojo está ubicado en el pin cuatro donde la salida del pin es de 5 v, además el cable blanco se encuentra en el pin siete, lo cual es una entrada o salida digital.

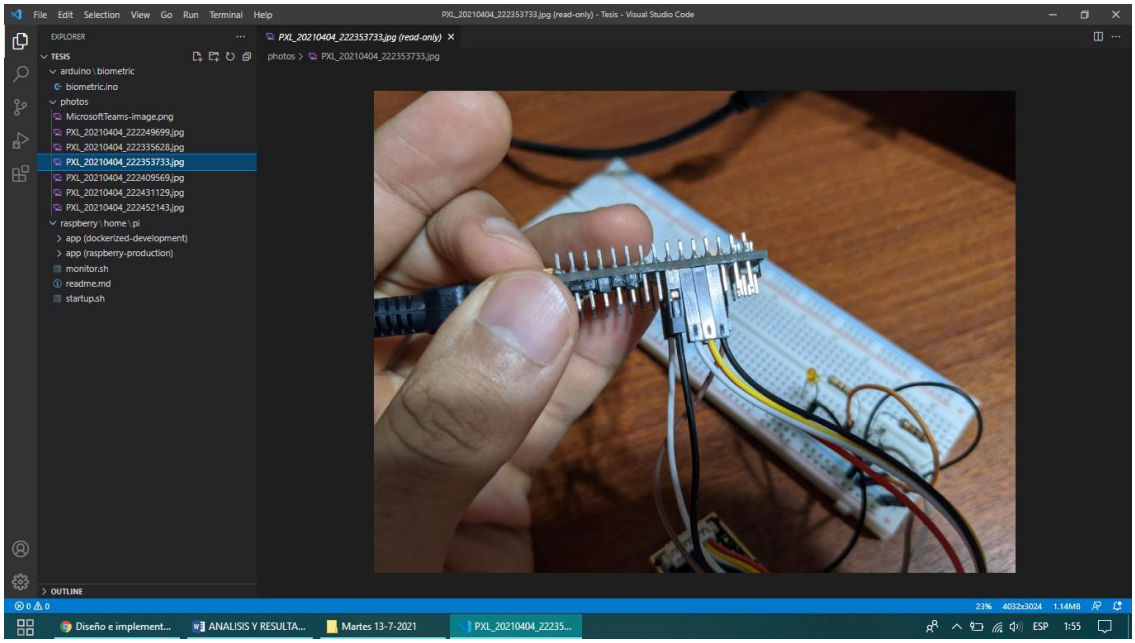


Figura 3. 15: Conexión de tierra

Fuente: (Autor)

El cable negro ubicado en el pin cuatro, es GND lo que representa una conexión a tierra; el cable amarillo, blanco y negro están ubicados en el pin D2, D3 y D4, son salidas y entradas digitales. Una señal digital es una señal eléctrica, representada por el símbolo 0 o 1 lo cual representa una lógica positiva o una lógica negativa.

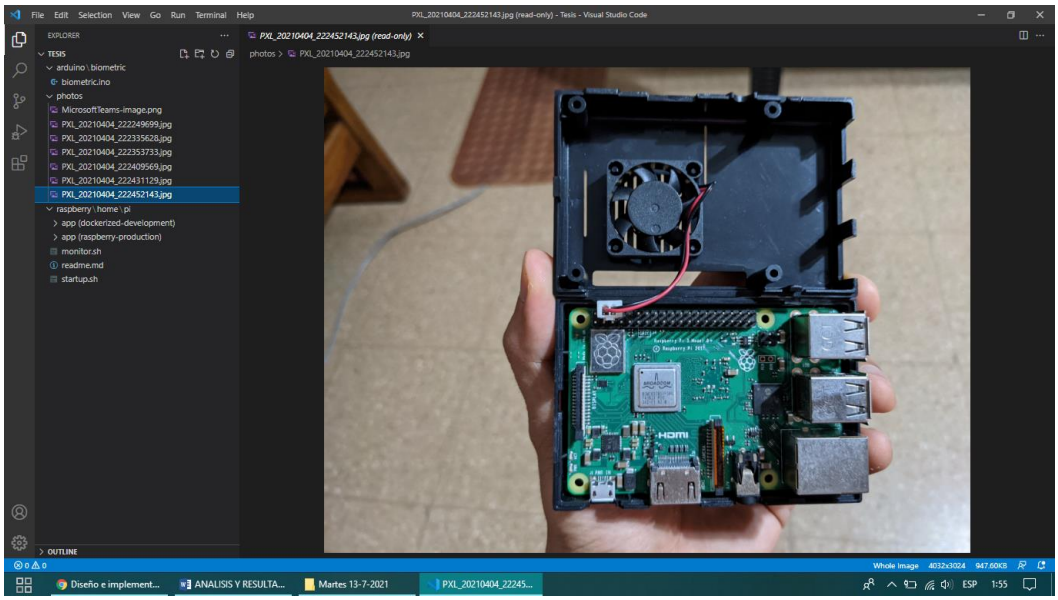


Figura 3. 16: Módulo Raspberry Pi 3

Fuente: (Autor)

Y por último el módulo Raspberry Pi 3, se lo ensambla en su estuche el cual tiene un diseño propio para las salidas de los componentes como ser el pin de carga, la entrada del cable UTP y sus entradas USB, se le agrega un mini ventilador, este ventilador sirve para enfriar los componentes, es necesario una fuente de refrigeración, ya que todos los aparatos electrónicos emiten calor, y se recomienda un sistema de ventilación.

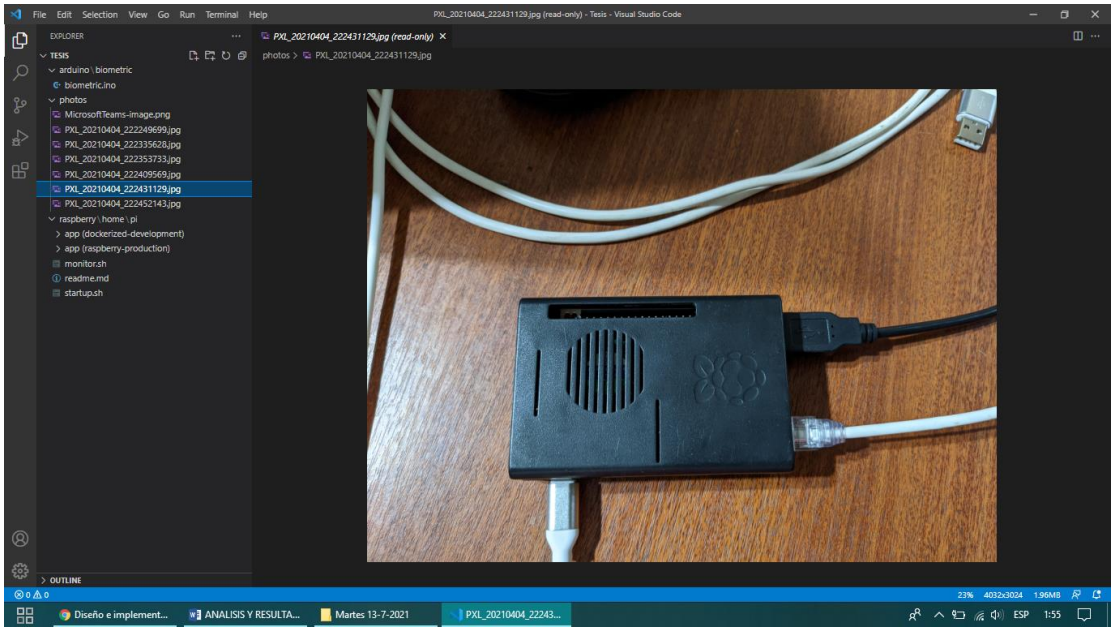


Figura 3. 17: Raspberry Pi 3 conectado al módulo, Fuente: (Autor)

En este último paso, se observa la Raspberry Pi 3 ensamblada en su estuche, y conectado al módulo, está el cable de red que sería el cable UTP, el cable de voltaje que es el que le suministra los 5 V y el cable USB que es el que se enlaza con el Arduino.

En este paso se ingresa a la carpeta raspberry/home/pi, y se obtienen dos carpetas: app (dockerized-development) y la carpeta app (raspberry-production).

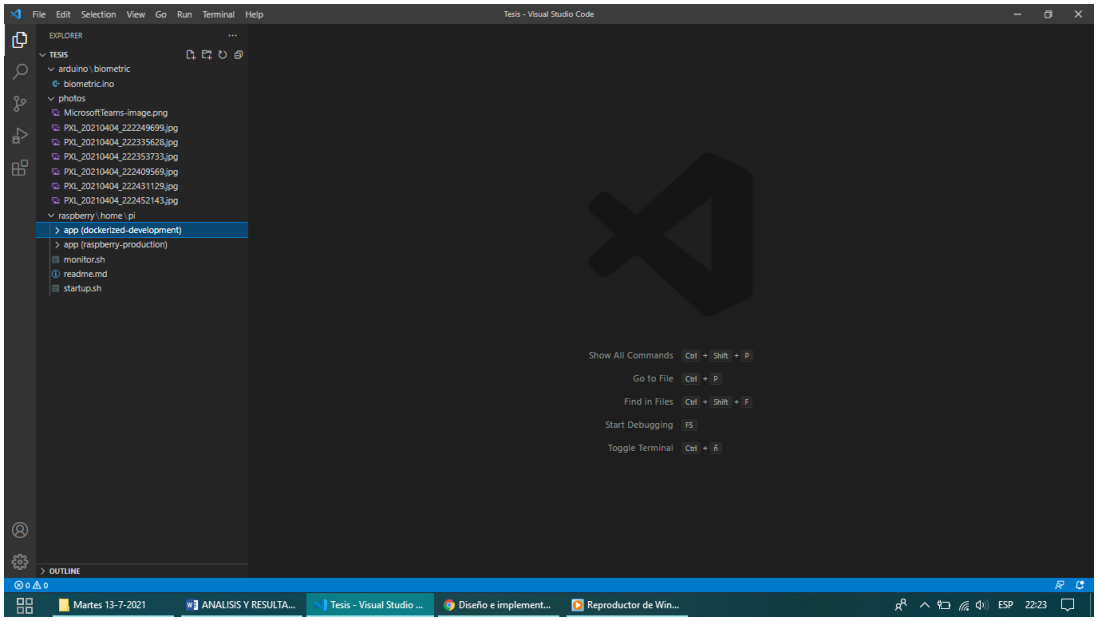


Figura 3. 18: Carpeta APP

Fuente: (Autor)

Al ejecutar la carpeta app siendo su nombre (dockerized-development), es donde se almacena el desarrollo del programa, y en la carpeta app (raspberry-production) se desglosan varias cantidades de líneas de código, las cuales tienen diferentes accesos en la Raspberry Pi 3.

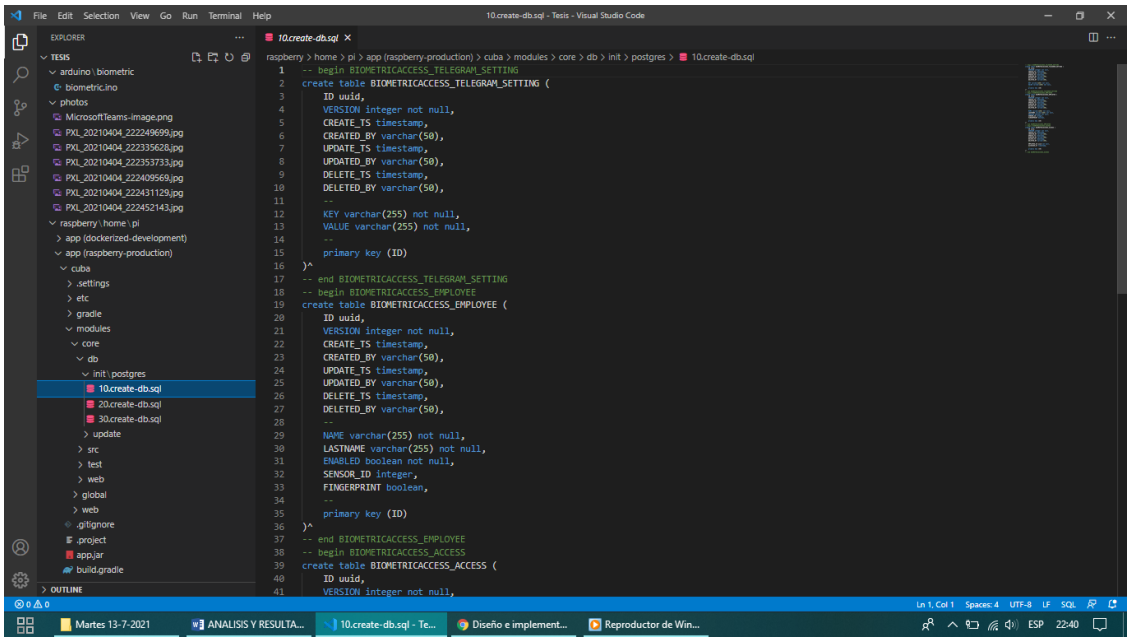


Figura 3. 19: Archivo Cuba

Fuente: (Autor)

En la carpeta app (raspberry-production) nos dirigimos al archivo "cuba", este es el programa java, en el cual se desplazan algunas pestañas y se verá una interfaz, la app.jar resulta ser la interfaz web.

En el documento "modules" se desglosan en más archivos siendo una de estas la carpeta core, y luego db que se ingresan en el documento init, en la cual se encuentran en el SQL que crea la base de datos donde se tiene la configuración de la aplicación Telegram, además los empleados y también el acceso que se aprecia en la interfaz.

```
-- begin BIOMETRICACCESS_TELEGRAM_SETTING
create table BIOMETRICACCESS_TELEGRAM_SETTING (
    ID uuid,
    VERSION integer not null,
    CREATE_TS timestamp,
    CREATED_BY varchar(50),
    UPDATE_TS timestamp,
    UPDATED_BY varchar(50),
    DELETE_TS timestamp,
    DELETED_BY varchar(50),
    --
```

```
    KEY varchar(255) not null,
    VALUE varchar(255) not null,
    --
    primary key (ID)
)^
-- end BIOMETRICACCESS_TELEGRAM_SETTING
-- begin BIOMETRICACCESS_EMPLOYEE
create table BIOMETRICACCESS_EMPLOYEE (
    ID uuid,
    VERSION integer not null,
    CREATE_TS timestamp,
    CREATED_BY varchar(50),
    UPDATE_TS timestamp,
    UPDATED_BY varchar(50),
    DELETE_TS timestamp,
    DELETED_BY varchar(50),
    --
    NAME varchar(255) not null,
    LASTNAME varchar(255) not null,
    ENABLED boolean not null,
    SENSOR_ID integer,
    FINGERPRINT boolean,
    --
    primary key (ID)
)^
-- end BIOMETRICACCESS_EMPLOYEE
-- begin BIOMETRICACCESS_ACCESS
create table BIOMETRICACCESS_ACCESS (
    ID uuid,
    VERSION integer not null,
    CREATE_TS timestamp,
    CREATED_BY varchar(50),
```

```
    UPDATE_TS timestamp,
    UPDATED_BY varchar(50),
    DELETE_TS timestamp,
    DELETED_BY varchar(50),
    --
    EMPLOYEE_ID uuid not null,
    ACCESSED_AT timestamp,
    --
    primary key (ID)
)^
-- end BIOMETRICACCESS_ACCESS
```

El mismo software es muy eficiente porque crea registros por sí mismo, luego se tendrá la carpeta “src” y al ser seleccionada se abrirá un conjunto de registros, se procede a abrir global que es una carpeta más de nuestro software, y en el archivo entity se puede encontrar las entidades, dónde se tienen los accesos, que es la que permite comunicar con la base de datos.

```
 public class Access extends StandardEntity {
    public static final String ENTITY_NAME = "biometricaccess_Access";
    private static final long serialVersionUID = 21425945118699104l1L;
```

En esta línea de código se obtiene un campo employee_ID y accessed_At, y si se regresa a la base de datos se tiene el acceso al ID del empleado y la hora de acceso de dicho usuario.

```
@JoinColumn(name = "EMPLOYEE_ID")
    protected Employee employee;


    @Column(name = "ACCESSED_AT")
    protected Date accessedAt = new Date();
```

Para hacer más fácil el conjunto de código, es necesario describirlo en una clase java, los campos necesarios a utilizar en la base requieren que el programa pueda instanciar la clase acceso con estos siguientes campos.

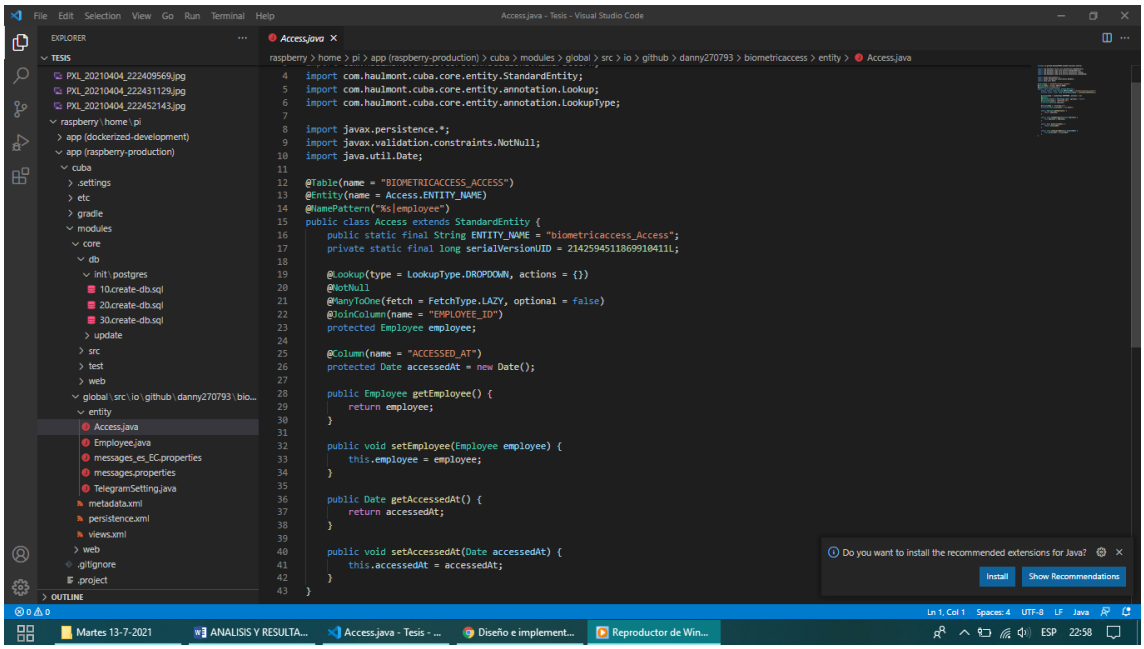


Figura 3. 20: Comunicación con la base de datos

Fuente: (Autor)

java internamente se comunica con la base de datos, y para la entidad visual se ingresa al archivo denominado web, inmediatamente se abre el documento src y se ejecuta la siguiente carpeta web, hasta llegar al archivo screens, en la cual se visualizan todas las pantallas que el aplicativo utilizará, al momento en que se enlace al internet.

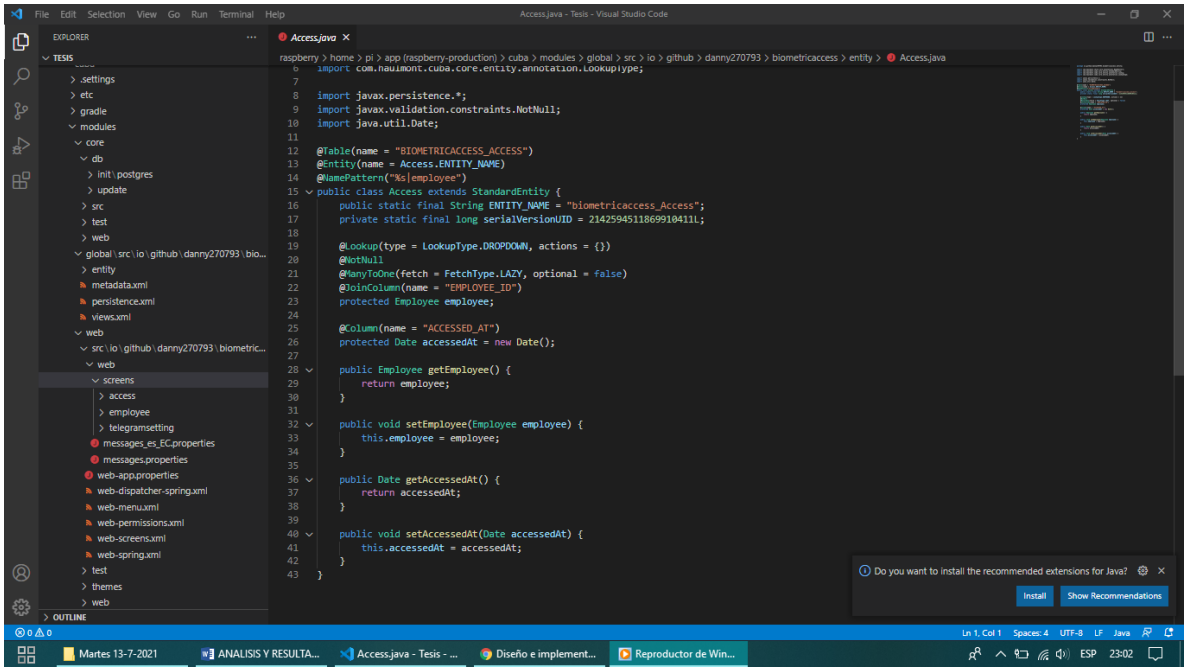


Figura 3. 21: Registro de acceso

Fuente: (Autor)

Al visualizar la pantalla de empleados, se registra el acceso y se selecciona el archivo browse, para ver el listado de empleados se puede visualizar en una tabla.

```
<groupTable id="employeesTable"
            width="100%"
            dataContainer="employeesDc">
```

Para identificar al trabajador se requiere de un formato, el cual sea sencillo de interpretar al momento de registrar sus datos, por lo cual el registro en columnas es lo más eficiente.

```
 <columns>
        <column id="name"/>
        <column id="lastname"/>
        <column id="enabled"/>
        <column id="fingerprint"/>
        <column id="sensor_id"/>
      </columns>
```

En esta configuración de código se encuentra en SQL, que es una anotación especial para que cargue la clase en employee, que esta llega ser una entidad del programa.

```
<?XML version="1.0" encoding="UTF-8" standalone="no"?>
<window xmlns="http://schemas.haulmont.com/cuba/screen/window.xsd"
    xmlns:c="http://schemas.haulmont.com/cuba/screen/jpql_condition.xsd"
    caption="msg://employeeBrowse.caption"
    focusComponent="employeesTable"
    messagesPack="io.github.danny270793.biometricaccess.web.screens.employee">
  <data readOnly="true">
    <collection id="employeesDc"
            class="io.github.danny270793.biometricaccess.entity.Employee">
      <view extends="_local"/>
      <loader id="employeesDl">
        <query>
          <![CDATA[select e from biometricaccess_Employee e]]>
        </query>
```

```
        </loader>
    </collection>
</data>
<dialogMode height="600"
            width="800"/>
<layout expand="employeesTable"
        spacing="true">
    <filter id="filter"
            applyTo="employeesTable"
            dataLoader="employeesDl">
        <properties include=".*"/>
    </filter>
```

Cuando haya la necesidad de editar a un empleado, se accede a la función de edit, no se escribe en el formato HTML, como tal se lo registra como XML y el programa en java lo transforma a HTML, como se muestra en el programa.

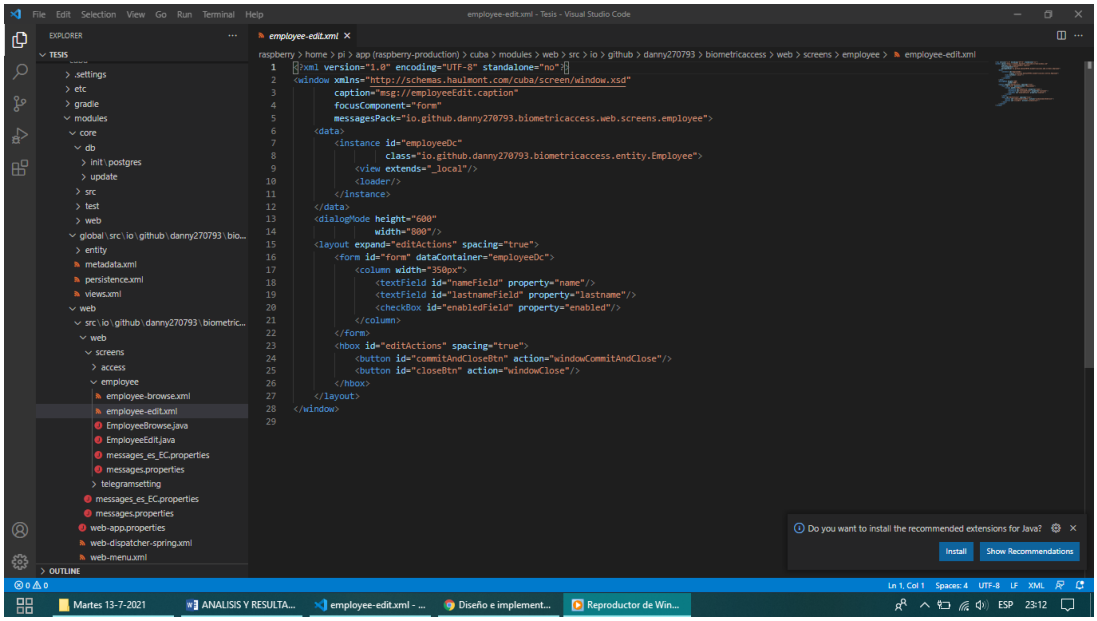


Figura 3. 22: Código interfaz

Fuente: (Autor)

En la presente imagen se aprecia el código de la interfaz de edición del empleado, en esta ejecución del esquema se observa el código en el programa “Python” el cual se desglosa en la

configuración Telegram, que es un programa gratuito y que se encarga de enviar los mensajes al aplicativo Telegram.

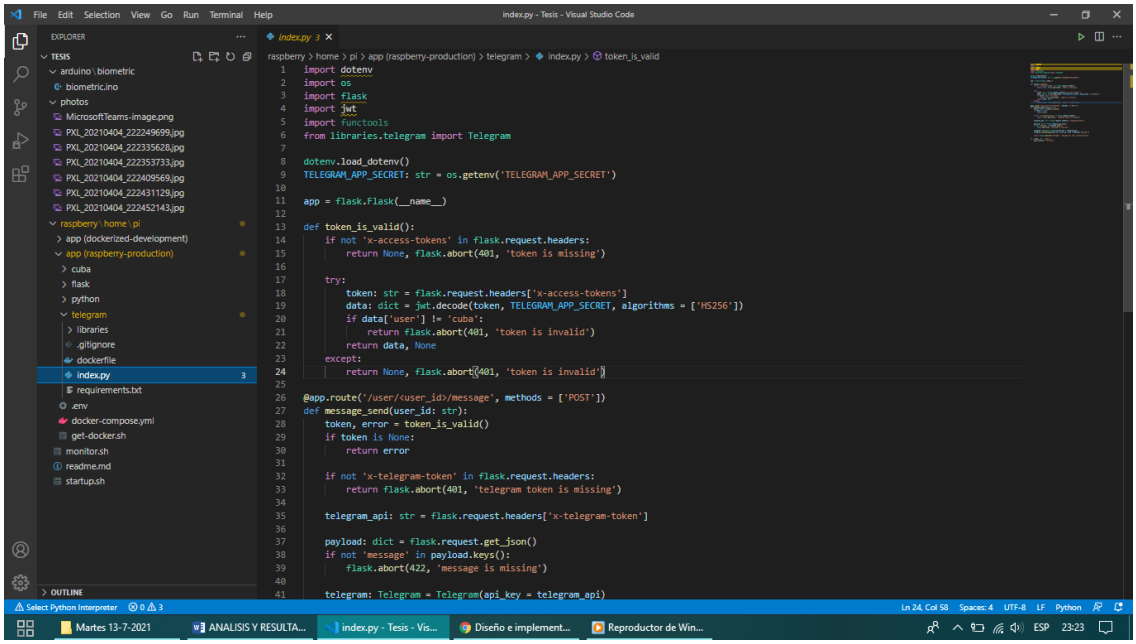


Figura 3. 23: Codificación del programa

Fuente: (Autor)

Con esta codificación de programa se generan los mensajes de Telegram y se crea un servidor llamado Flask, el cual lo único que va a hacer es escuchar los mensajes, cuando se mande un mensaje del /user/<user_id>/message'.

import dotenv

import os

import Flask

import jwt

import functools

from libraries.telegram import Telegram

dotenv.load_dotenv()

TELEGRAM_APP_SECRET: str = os.getenv('TELEGRAM_APP_SECRET')

app = Flask.Flask(__name__)

```
def token_is_valid():
    if not 'x-access-tokens' in Flask.request.headers:
        return None, Flask.abort(401, 'token is missing')

    try:
        token: str = Flask.request.headers['x-access-tokens']
        data: dict = jwt.decode(token, TELEGRAM_APP_SECRET, algorithms = ['HS256'])
        if data['user'] != 'cuba':
            return Flask.abort(401, 'token is invalid')
        return data, None
    except:
        return None, Flask.abort(401, 'token is invalid')

@app.route('/user/<user_id>/message', methods = ['POST'])
def message_send(user_id: str):
    token, error = token_is_valid()
    if token is None:
        return error

    if not 'x-telegram-token' in Flask.request.headers:
        return Flask.abort(401, 'telegram token is missing')

    telegram_api: str = Flask.request.headers['x-telegram-token']

    payload: dict = Flask.request.get_json()
    if not 'message' in payload.keys():
        Flask.abort(422, 'message is missing')

    telegram: Telegram = Telegram(api_key = telegram_api)
    telegram.send_message(user_id = user_id, text = payload['message'])

    return Flask.jsonify({'message': 'message was sent successfully'})
```

```
if __name__ == '__main__':
    app.run(host = '0.0.0.0')
```

Lo que hace este comando es que después de la consulta que le llega, se obtiene el json lo que es el contenido y crea un objeto Telegram.

Al ingresar a la carpeta Flask, se ingresa al archivo index.py, en lo cual se registran los datos del usuario como ser la huella dactilar del empleado a contratar.

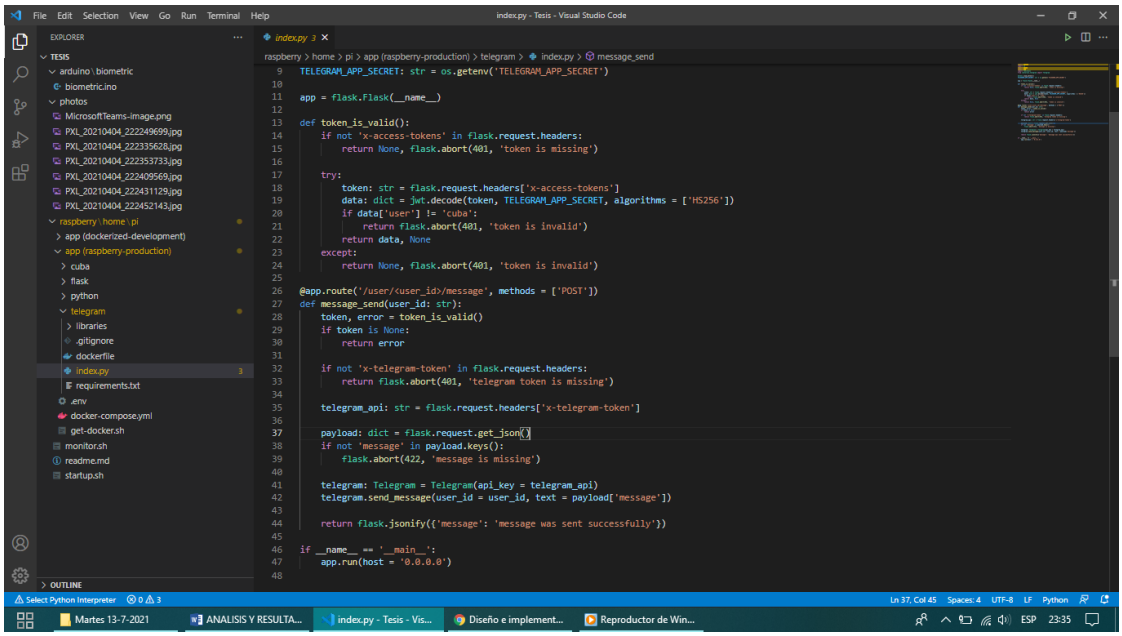


Figura 3. 24: Comunicación con Telegram

Fuente: (Autor)

Se crea una librería donde existe la comunicación con Telegram directamente y el index.py, es el que se comunica con el lector de huella, entonces cuando se le pida al archivo cuba registrar la huella, el archivo cuba lo que hará es mandarle un mensaje a Python con la palabra register e internamente se comunica con el lector de huellas y agrega la huella que se le está pidiendo agregar.

```
@app.route('/register/<user_id>', methods = ['GET'])
def register(user_id):
    try:
        fingerprint = Fingerprint.instance()
        position = fingerprint.add_new_finger(int(user_id))
```

```
        fingerprint.close()
        addInQueue('state', str(position))
        return " [x] register: %s" % position
    except Exception as e:
        Logger.debug(format_exc())
        return Flask.abort(500, 'error')
```

Con la siguiente codificación se verifica cuando se pone la huella, e inmediatamente también se tiene el ID de la huella dactilar.

```
@app.route('/access/control', methods = ['GET'])
def access():
    try:
        Logger.debug('fingerprint=Fingerprint.instance()')
        fingerprint=Fingerprint.instance()
        Logger.debug('position = fingerprint.get_id()')
        position = fingerprint.get_id()
        Logger.debug('fingerprint.close()')
        fingerprint.close()
```

Pero si resulta que el ID de la huella es 0, quiere decir que se colocó un dedo que no es válido, pero si es diferente a 0, entonces si es un usuario válido.

```
if position != -1:
```

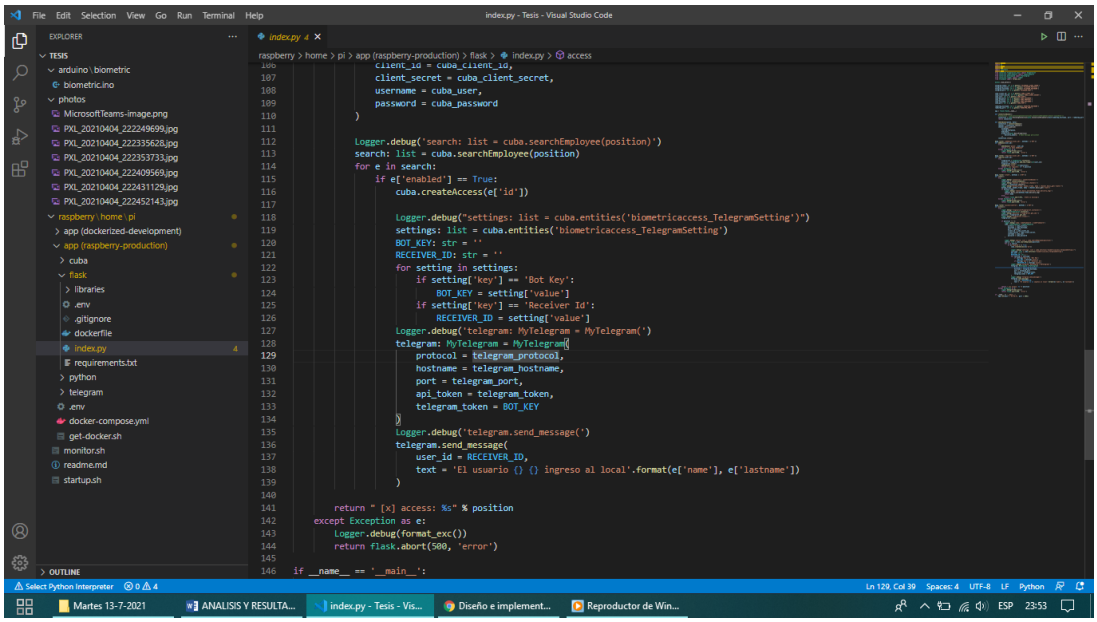


Figura 3. 25: Registro

Fuente: (Autor)

Automáticamente en java, el programa busca en los registros un parámetro que coincida con algún usuario que ya esté agregado, y una vez que encuentra al empleado se genera un mensaje hacia la aplicación Telegram.

```
Logger.debug('search: list = cuba.searchEmployee(position)')
        search: list = cuba.searchEmployee(position)
        for e in search:
            if e['enabled'] == True:
                cuba.createAccess(e['id'])


                Logger.debug("settings: list = cuba.entities('biometricaccess_TelegramSetting')"
)
                settings: list = cuba.entities('biometricaccess_TelegramSetting')
                BOT_KEY: str = ''
                RECEIVER_ID: str = ''
                for setting in settings:
                    if setting['key'] == 'Bot Key':
                        BOT_KEY = setting['value']
                    if setting['key'] == 'Receiver Id':
```

```
            RECEIVER_ID = setting['value']
        Logger.debug('telegram: MyTelegram = MyTelegram(')
        telegram: MyTelegram = MyTelegram(
            protocol = telegram_protocol,
            hostname = telegram_hostname,
            port = telegram_port,
            api_token = telegram_token,
            telegram_token = BOT_KEY
        )
        Logger.debug('telegram.send_message(')
        telegram.send_message(
            user_id = RECEIVER_ID,
            text = 'El usuario {} {} ingreso al local'.format(e['name'], e['lastname'])
        )
```

Concluida la parte de la programación y diseño del proyecto técnico, se destacará la aplicación de descarga para el dispositivo móvil y también su enlace a internet.

En este paso nos enlazamos inalámbricamente al equipo Raspberry Pi 3, inicialmente este dispositivo debe estar conectado por un cable de red UTP partiendo del router hacia la Raspberry Pi 3, entonces se generará una dirección IP proveniente de la Raspberry Pi 3 la cual se necesita identificará para poder enlazarla inalámbricamente.

Se debe descargar la aplicación Network IP Scanner ya que es un software libre, el cual se lo puede obtener desde Play Store en nuestro celular, una vez instalada esta nos ayudará a escanear las IP cercanas a nuestra ubicación.

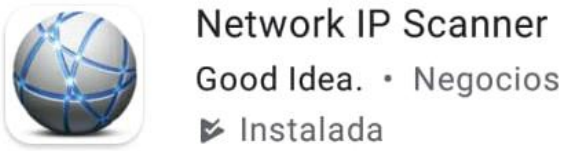


Figura 3. 26: Ícono Network IP Scanner

Fuente: (Autor)

Una vez instalado Network IP Scanner se abre la aplicación para identificar la Raspberry Pi 3.

Figura 3. 27: Menú Principal de la app descargada

Fuente: (Autor)

En la computadora se tiene que descargar el programa PuTTY, este software es gratuito y no tiene dificultades para trabajar con los protocolos SSH, se lo puede conseguir en el siguiente

link: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html; al ingresar se abrirá la siguiente ventana.

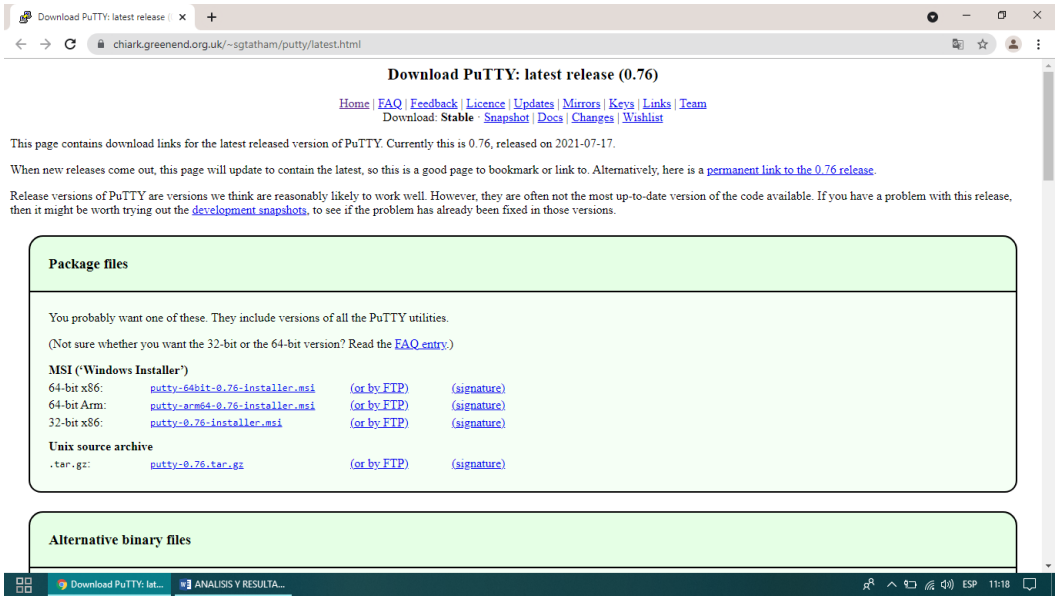


Figura 3. 28: Programa PUTTY

Fuente: (Autor)

Se selecciona la opción: 64-bit x86: putty-64bit-0.76-installer.msi , una vez descargado este archivo, se selecciona en el computador la herramienta PuTTY.

Se abre el programa PuTTY, muestra una ventana emergente donde se tiene que colocar la IP obtenida del programa IP Scanner, es la IP que se necesita para la Raspberry Pi 3, con la ayuda del programa se obtiene la siguiente dirección: 192.168.2.103; al registrar la IP se selecciona "Open" en la siguiente ventana emergente que se muestra a continuación.

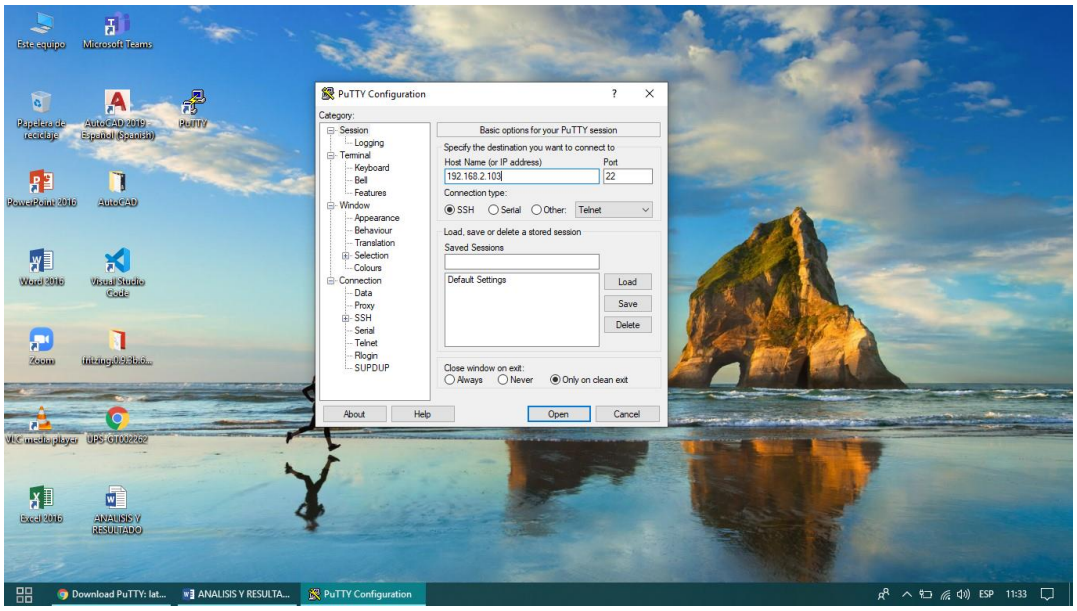


Figura 3. 29: Ingreso al programa PUTTY

Fuente: (Autor)

Esto genera una nueva ventana donde se pone como ingreso de acceso: pi y su clave: raspberry.

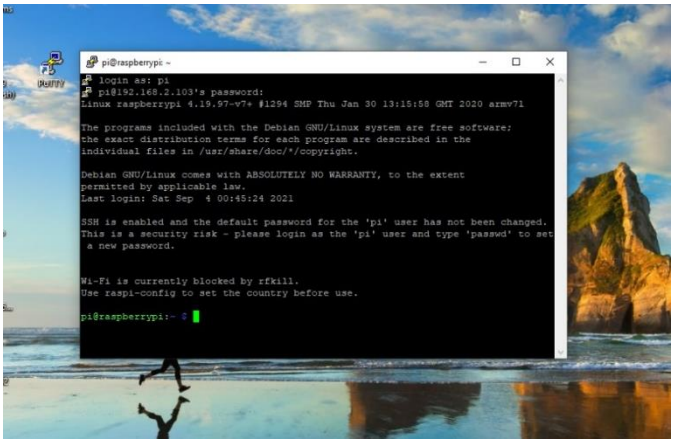


Figura 3. 30: Conexión Raspberry

Fuente: (Autor)

Para establecer la conexión Raspberry Pi 3, se ejecuta las siguientes líneas de código que se tiene a continuación:

```
sh startup.sh telegram

sh startup.sh Flask

sh startup.sh cuba
```

sh startup.sh python

Al ejecutar cuatro veces las terminales independientes dentro del programa PuTTY, se ingresan los siguientes terminales: sh startup.sh Telegram, sh startup.sh Flask, sh startup.sh cuba y sh startup.sh Python, en cuatro ventanas distintas como se muestra en la figura.

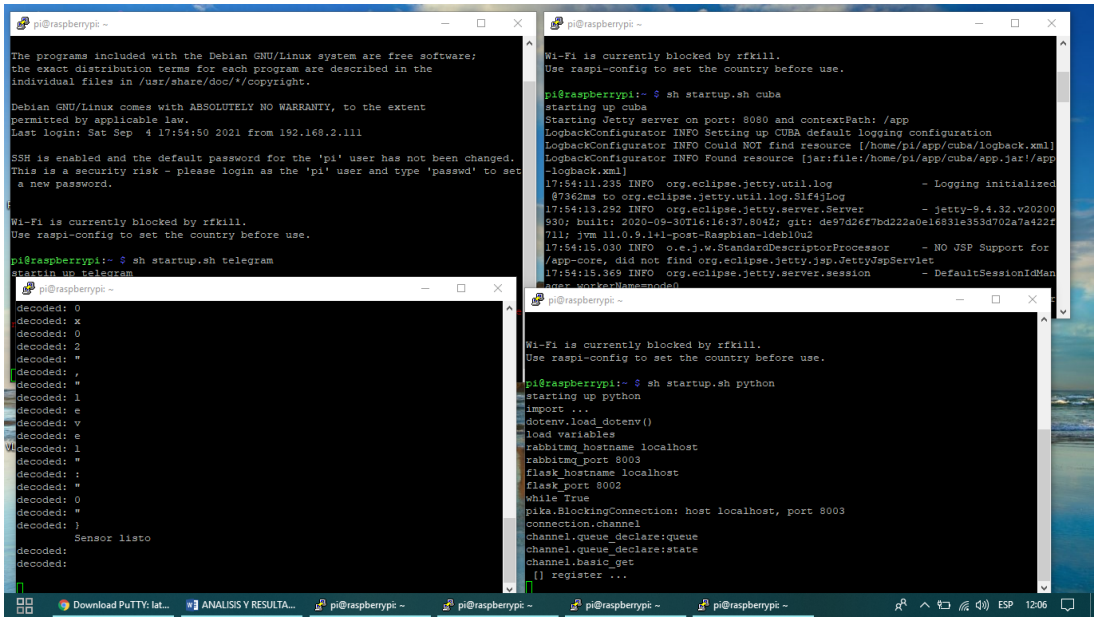


Figura 3. 31: Ventanas con direcciones IP

Fuente: (Autor)

Ya teniendo las ventanas se abre el programa Google Chrome, se coloca la dirección IP de la Raspberry Pi 3: http://192.168.2.103:8080/app/#login, para entrar a la página se debe poner nuestras credenciales.

Usuario: admin

Contraseña: admin

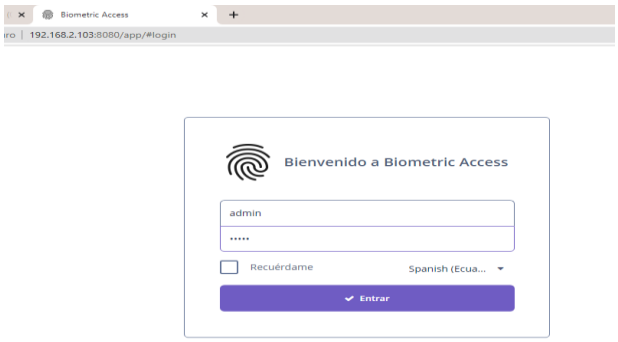


Figura 3. 32: Ingreso de plataforma del biométrico

Fuente: (Autor)

Al ingresar a la plataforma virtual del biométrico se requieren las herramientas necesarias de este proyecto las cuales son: Telegram, Empleados y Accesos.

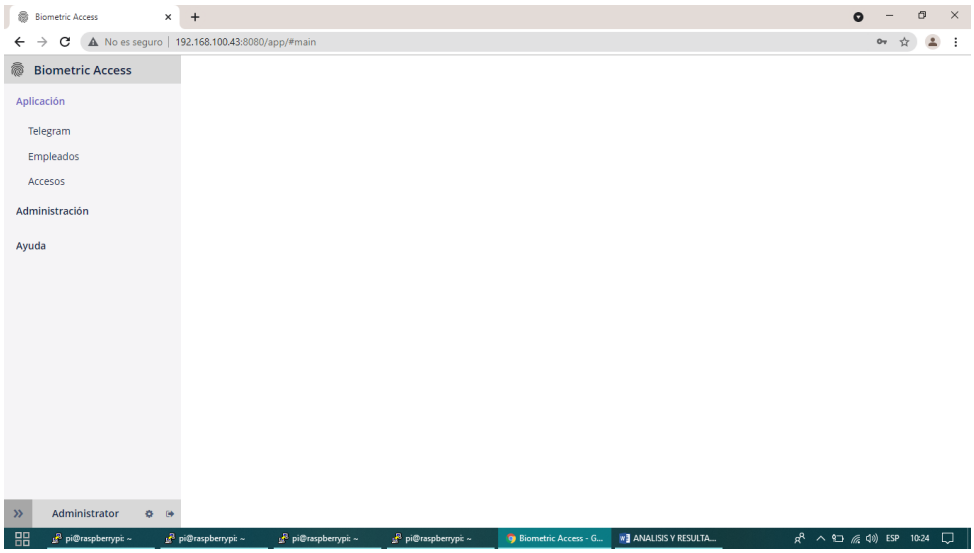


Figura 3. 33: Plataforma del biométrico

Fuente: (Autor)

Para poder asociar el ID en la aplicación Telegram se debe ir a la siguiente página web: https://t.me/userinfobot, este link genera el bot encargado de reservar el ID personal para Telegram generando un mensaje el cual llega por texto al aplicativo Telegram.

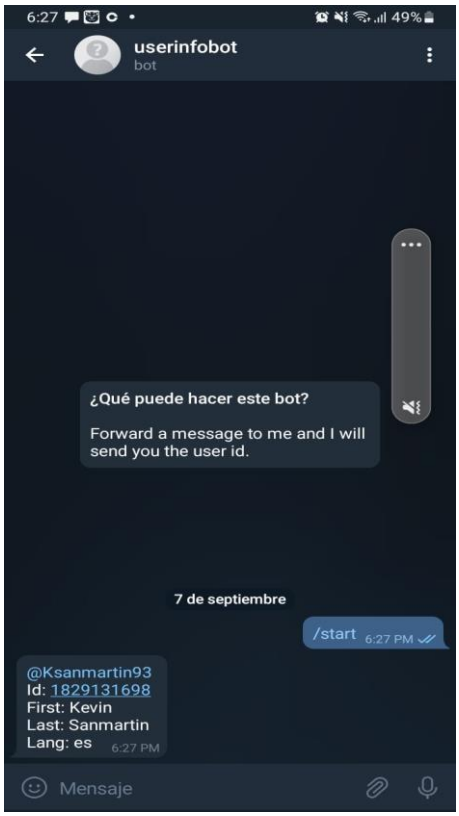


Figura 3. 34: Mensaje de la aplicación de Telegram

Fuente: (Autor)

Regresando a la página del biométrico se hace la siguiente configuración, con el dispositivo móvil se accede al aplicativo Telegram, se selecciona Receiver ID e ingresamos a la opción Editar, esto abre la página de configuración y el ID que le pertenece al gerente del almacén, se ingresan los números del ID en el ícono denominado valor, el cual tiene una pestaña en blanco donde habrá que colocar el ID previamente obtenido como se muestra en la figura 46 y, para concluir los cambios se selecciona OK, esto hace guardar los cambios teniendo lista la configuración en el teléfono conectado con el biométrico y cada vez que los trabajadores entren y salgan del almacén, su registro ira directamente al teléfono móvil del gerente del almacén.

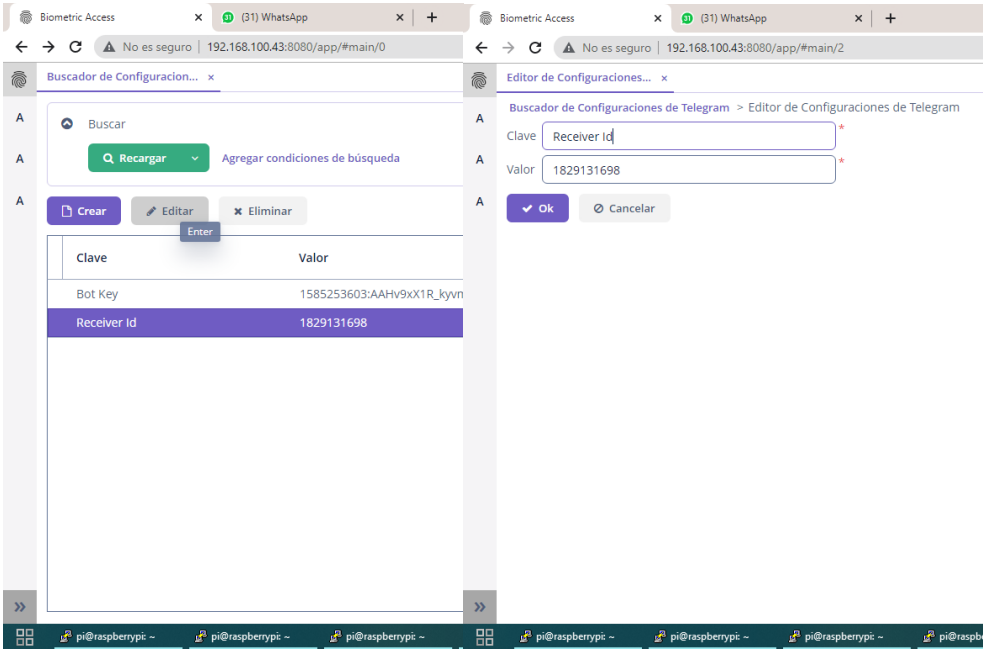


Figura 3. 35: Registro de los empleados

Fuente: (Autor)

Para el registro de empleados, se ingresa en la opción de crear y se registran en la ventana el Nombre y Apellido del trabajador, una vez llenos estos parámetros, se selecciona la opción de Activo al momento de realizar el registro tiene que habilitar esta opción.

La opción Activo lo que hace es que el usuario este constando en la lista de empleados y al momento de registrar su huella el sistema lo reconozca, pero si se deshabilita esta opción, aunque este la huella constando en el sistema el biométrico no lo reconocerá.

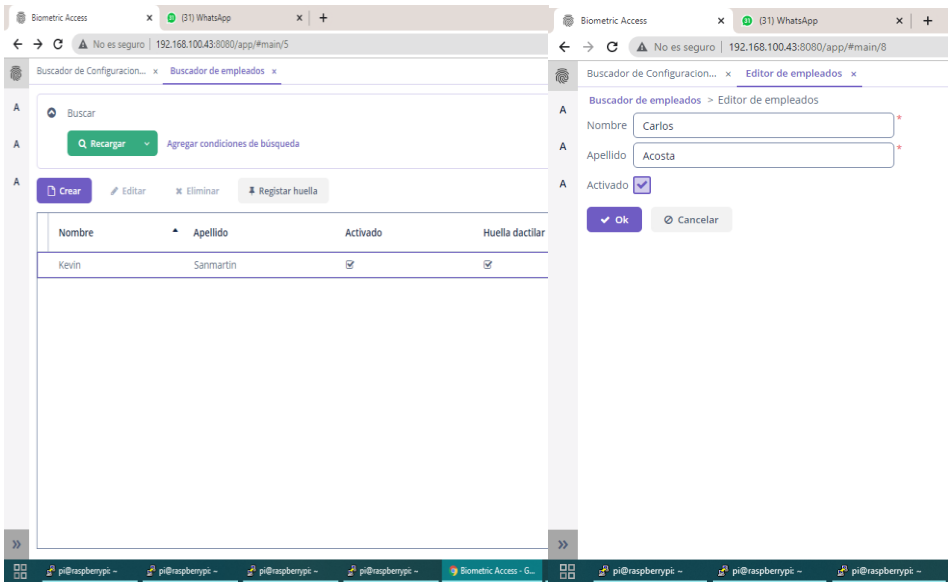


Figura 3. 36: Configuraciones de la lista de los empleados

Fuente: (Autor)

Teniendo la configuración lista, se procede a seleccionar donde se encuentra el nombre del trabajador, se selecciona la opción registrar huella y con esto el trabajador tendrá que hacer lo siguiente.

Al momento de seleccionar registrar huella se encenderá un led azul indicando que el sistema está a la espera de que el empleado ponga la huella, y al instante se enciende un led amarillo indicando que retire la huella, este paso lo tiene que hacer tres veces, una vez realizado el procedimiento descrito, se encenderán los dos leds al mismo tiempo indicando que el registro ha sido exitoso.

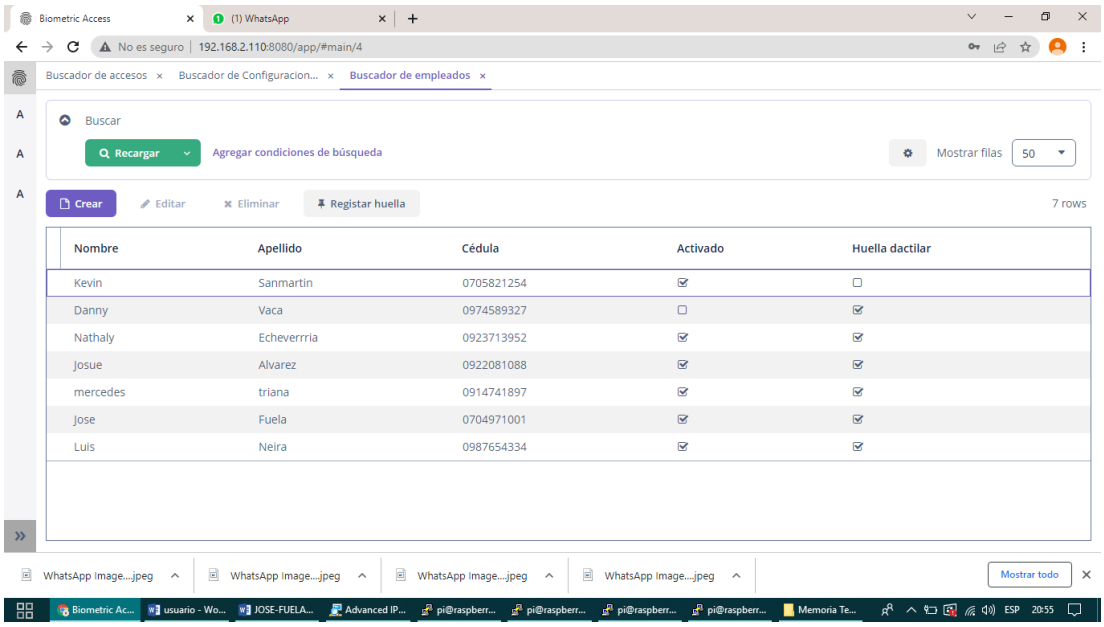


Figura 3. 37: Explicación de la lista para editar

Fuente: (Autor)

Para editar o eliminar la lista de los trabajadores, solo se selecciona a los usuarios dando clic en el nombre, por ejemplo: Carlos Acosta, la ventana de Carlos se pondrá en celeste y se puede realizar cualquier tipo de modificación.

En la opción accesos se ingresa directamente al registro de los trabajadores, los que han ingresado a su jornada de trabajo y los que no, esta herramienta ayuda a ver el desempeño de los usuarios en tiempo real ya que lleva un registro del día, mes y año, es muy práctico proporcionando gran utilidad al momento de elaborar un rol de pagos.

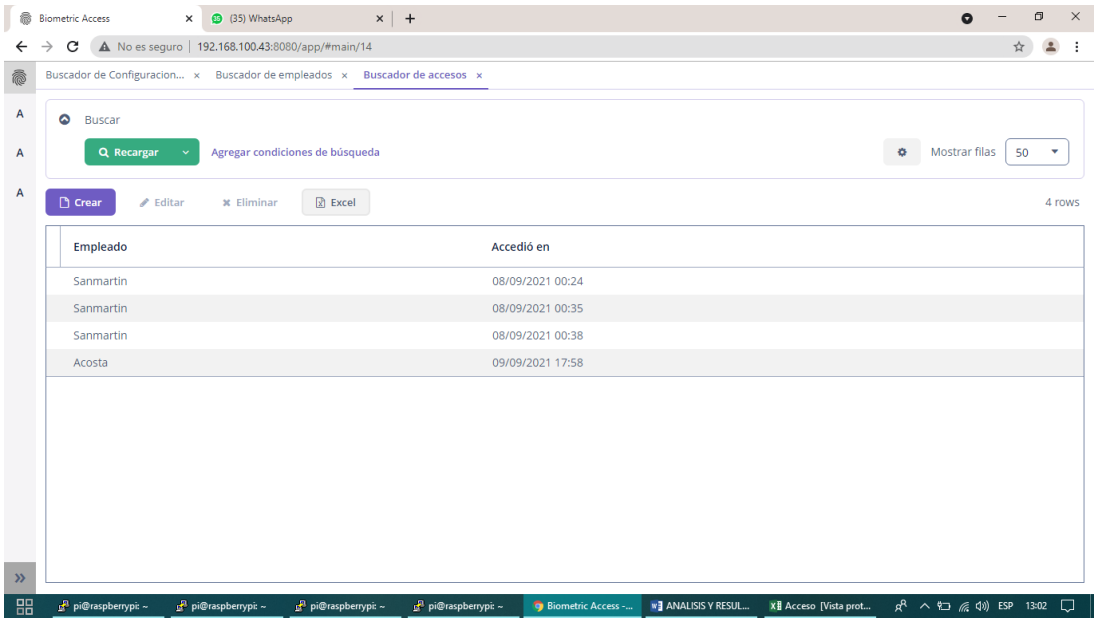


Figura 3. 38: Descarga del registro realizado

Fuente: (Autor)

Esta plataforma cuenta con una hoja de Excel, la cual es fácil de descargar y para ello se selecciona la opción con el ícono Excel, automáticamente se descargará el registro de los empleados.

Si se desea modificar dicho registro, se selecciona el apellido del trabajador y este se pondrá de color celeste, la opción de editar y eliminar se activará según el usuario lo requiera.

CAPITULO IV: RESULTADOS

Luego del diseño, ensamble y programación del sistema biométrico propuesto para su implementación en la empresa “Phonix-Cell” por motivo de estudio, como resultado se obtuvo un dispositivo cuyo sistema permitirá llevar un control de horarios de ingreso y salida del personal de empleados, lo cual permitirá hacer cumplir las jornadas laborales dispuestas por la empresa.

4.1 Características generales del sistema

Las características del biométrico se comprenden del sistema en general, desde el protoboard, que en cuya placa se encuentran los elementos básicos del circuito y también de un elemento principal como el sensor de huellas e incluyendo una Raspberry Pi 3 al sistema, este pequeño pero poderoso módulo es la base para la configuración hacia la plataforma web del sistema, hasta el momento de su funcionamiento no han presentado inconvenientes en cuanto al correcto desempeño.

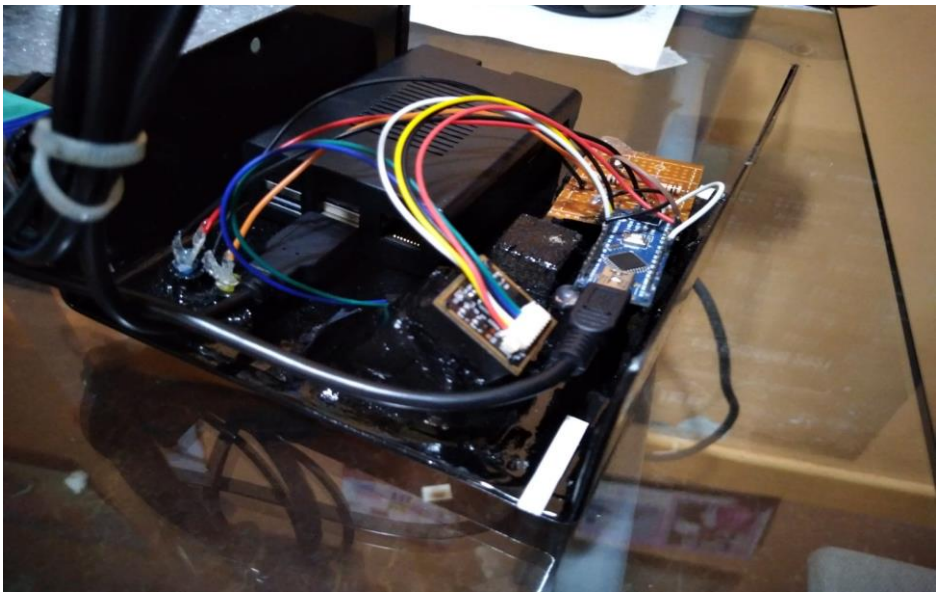


Figura 4. 1: Sistema biométrico

Fuente: (Autor)

4.2 Características técnicas del sistema biométrico

4.2.1 Características técnicas del Arduino nano

Este dispositivo cuenta con un microcontrolador: ATmega 328P y una memoria flash de 32 Kb (2 Kb usados por el Bootloader), y su memoria SRAM de 2 Kb, esto le permite procesar la información de manera rápida, sin que el sistema presente latencia durante el proceso de registro o edición de huellas dactilares de los empleados de la empresa.

4.2.2 Características técnicas de la Raspberry Pi 3

Este elemento tiene 1 Gb de memoria RAM, cuenta con un procesador BCM2837 ARM v8 de 64 bits y 4 núcleos que funciona a 1.2 GHz. Se lo estableció con este módulo ya que el tráfico de red de hoy en día tiene bastante demanda en lo que es el consumo de datos y, gracias a estas prestaciones nuestra página web no se colgará al momento de ingresar un usuario o ver el registro de actividades.

Figura 4. 2: Módulo Raspberry Pi 3 conectado

Fuente: (Autor)

4.3 Sistema de enlace del biométrico

4.3.1 Estructura de enlace

Para que el dispositivo se pueda comunicar a la red, debe de tener la misma IP del establecimiento, por ejemplo: Si el router del establecimiento tiene una IP 192.168.4.100, el dispositivo debe de estar vinculado con la misma IP, es decir: 192.168.4.100. La calidad de transferencia de datos depende de la velocidad con la que trabaje el router, de 15 a 20 Gb es aceptable, tendría un buen rendimiento y de 20 Gb en adelante un excelente rendimiento.

4.4 Carga eléctrica del sistema

4.4.1 Fuente de voltaje

Se usaron dos fuentes de energía: carga rápida y carga lenta, con la carga rápida el sistema funcionaba con normalidad, pero después de media hora el adaptador presentó una temperatura inusual al tacto más tibio de lo normal. Por ende, se lo desconectó y se procedió a conectar el siguiente cargador de carga lenta, el módulo permaneció el mismo tiempo conectado, pero este se mantenía tibio y sin ningún inconveniente.

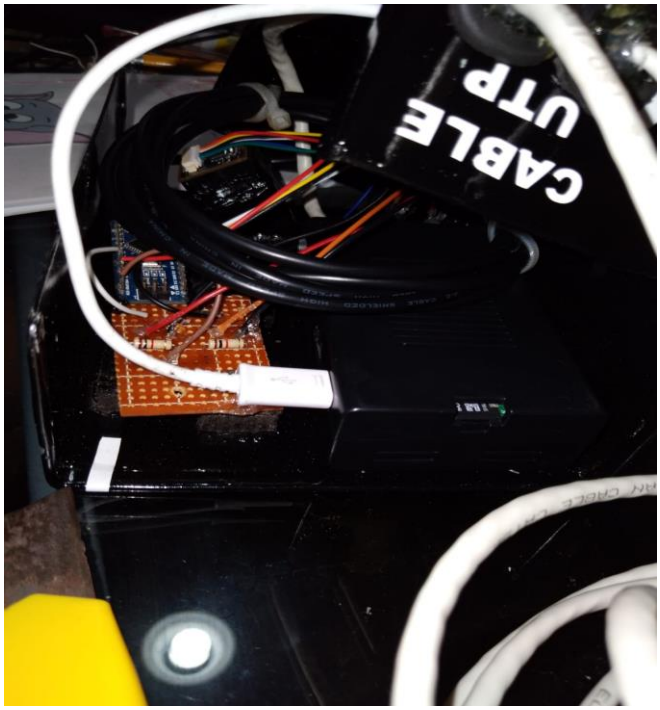


Figura 4. 3: Alimentación de energía al dispositivo

Fuente: (Autor)

4.5 Resultados de las muestras dactilares

4.5.1 Constancia de registro en la plataforma web

La persona registrada en el sistema tendrá que cumplir con el horario de trabajo establecido por la empresa, dicho usuario tiene que colocar su dedo en el lector biométrico, cuyo dispositivo encenderá una luz amarilla indicando que retire el dedo; y al hacerlo se encenderán dos leds: uno de color amarillo y otro led de color azul indicando que si consta en el sistema y que su registro ha sido exitoso.

Figura 4. 4: Constancia del registro en el dispositivo

Fuente: (Autor)

Por ende, una persona no registrada en el sistema al momento de colocar su huella, el sistema encenderá un led de color amarillo, indicando que lo retire y al momento de retirarlo no se generará nada porque dicha persona no es un usuario de la empresa.

Figura 4. 5: Usuario no registrado en el dispositivo

Fuente: (Autor)

Este método de registro cuenta con un listado de empleados y es muy importante de establecer, ya que personas ajenas a la empresa suelen invadir el espacio de trabajo para vender información de márquetin a terceros.

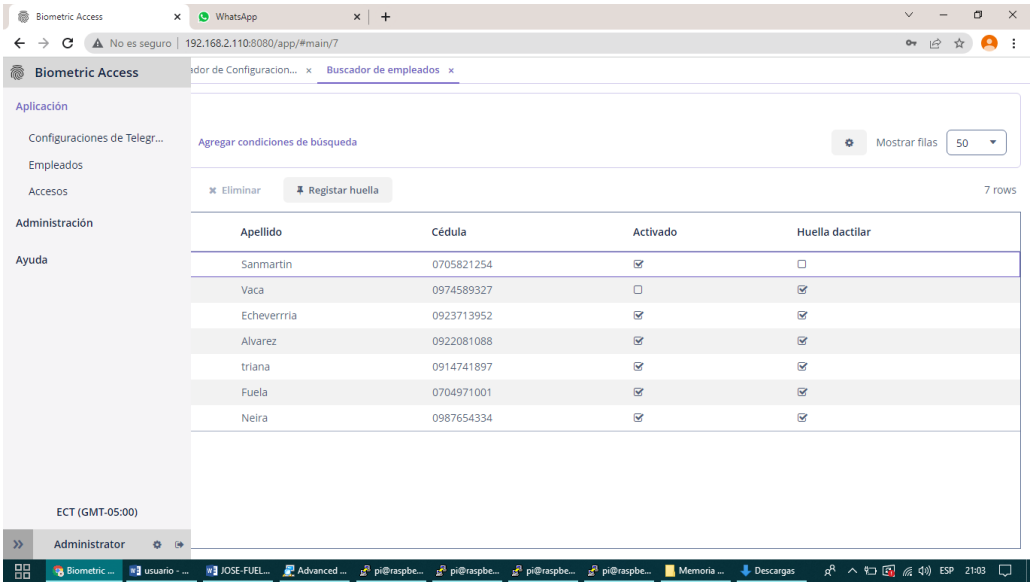


Figura 4. 6: Usuarios registrados en la plataforma web

Fuente: (Autor)

4.5.2 Respuesta del sistema biométrico

El gerente o trabajador que coloque su huella en el biométrico registrará la hora y fecha de su acceso automáticamente en el sistema de monitoreo que sería la computadora o el dispositivo móvil del dueño.

Figura 4. 7: Monitoreo de acceso por medio del aplicativo web

Fuente: (Autor)

Este software de acceso es un listado donde el registro de los usuarios queda guardado; por cada persona que ingrese su huella el sistema lo guardara.

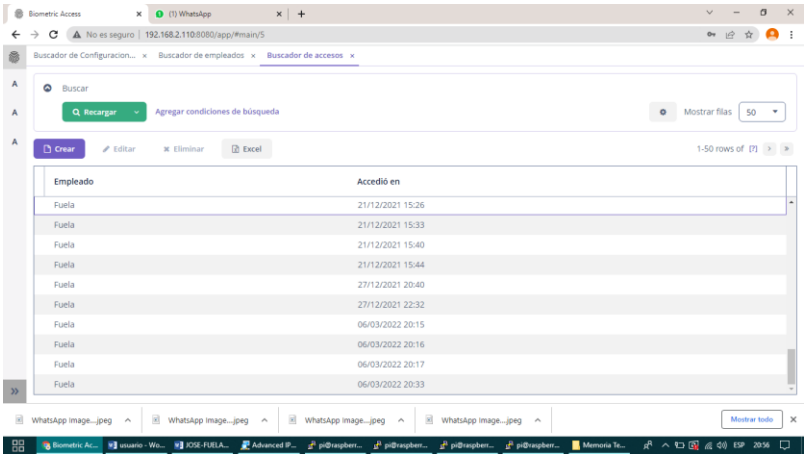


Figura 4. 8: Plataforma de acceso en tiempo real del sistema biométrico

Fuente: (Autor)

4.5.3 Notificación de mensajería del sistema vía Telegram

Lo importante de un registro es tener acceso a la información individual de cada trabajador en el sistema web, constantemente este método de enlace se asocia con la mensajería de Telegram para así generar un mensaje cada vez que alguien ingrese a la empresa, Telegram ya no solo es una mensajería entre amigos si no una herramienta más de trabajo.

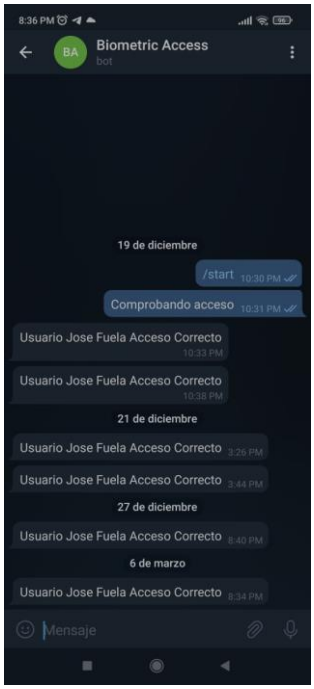


Figura 4. 9: Notificación de mensajería vía Telegram

Fuente: (Autor)

4.6 Análisis de resultados

El dispositivo biométrico no es nada nuevo hoy en día, pero la mensajería de notificación por mensajes a una red social es lo nuevo que se propuso en este trabajo de titulación, en medio de un mercado tecnológico competitivo este software cumple con los estándares de seguridad, registro y mensajería establecidos desde sus inicios.

CONCLUSIONES

- Se realizó la codificación para enlazar las aplicaciones hacia el aplicativo web en el que se establecen cuatro comandos, los cuales son: Telegram, Flask, Cuba y Python, dichos comandos son los que generan las comunicaciones de la Raspberry Pi 3 hacia el portal web, sin este procedimiento no sería posible el registro de las actividades en el módulo del biométrico que se encuentra en el almacén.

- El beneficio de este sistema biométrico es que se diseñó una interfaz en la que se puede registrar a un trabajador nuevo, sin que la presencia del gerente se halle en las instalaciones, lo único que se necesita es que la persona que vaya a laborar coloque su huella dactilar en el lector biométrico y, remotamente donde quiera que se encuentre el gerente del almacén lo puede registrar desde el aplicativo web.

- Gracias a los softwares de simulación como Proteus y Fritzing se pudo desarrollar a cabalidad el diseño de conexión que posteriormente sería guía para la fabricación de la placa PCB que contiene pare de los elementos que se enlazan al Arduino.

- En caso de que el gerente del almacén sufra algún desperfecto de software en su celular o es robado, él puede ingresar desde el aplicativo web del biométrico a ver los registros de los trabajadores, y también desde la misma página se puede cerrar el vínculo de Telegram que está asociado al móvil, sin necesidad de tener el celular a la mano.

- Para optimizar la conectividad a internet se realizó mediante cable ethernet (UTP) ya que ofrece mejores prestaciones de velocidad y estabilidad en la trasmisión de datos evitando latencia en el envío de datos.

- Este dispositivo puede ser mejorado con una pantalla LCD o algún audio que facilite la interacción de los procedimientos de registro a quien lo quiera innovar, ya que por falta de presupuesto no se los incorporó dentro del proyecto, la parte externa del módulo está elaborada en metal ya que estos dispositivos contienen elementos muy delicados y siendo este un metal rígido si llega a sufrir alguna caída, podrá resistir el

golpe sin comprometer a los integrados, a diferencia de los que son elaborados en plástico, estos durante una caída se suelen partir dejando al descubierto sus componentes electrónicos.

RECOMENDACIONES

- Para tener una buena conectividad con el sistema biométrico y la base de datos, se recomienda contar con buena señal de internet, y así evitar problemas con de envió del mensaje informativo hacia el dispositivo móvil de gerencia.

- Se recomienda evitar exponer al sol o instalar el dispositivo en sitios calientes, puesto que la temperatura afecta al rendimiento del dispositivo de seguridad, pudiendo ocasionar reinicios inesperados.

- Se recomienda no mojar la caja del sistema biométrico ya que cuenta con un orificio de enfriamiento, el cual tiene un ventilador que ingresa aire desde el exterior para enfriar los componentes electrónicos, y si este adsorbe agua las conexiones podrían hacer cortocircuito ocasionando un daño en el mismo.

- Implementar un seminario que esté orientado particularmente hacia los distintos tipos de sensores biométricos que existen en la actualidad.

- Incorporar más prácticas en los laboratorios a la malla curricular de ingeniería electrónica.

- Sería de gran ayuda que los seminarios cuenten con los instaladores originales de los programas a utilizar, ya que en internet no siempre se encuentra el mismo instalador.

REFERENCIAS

Baldeón, p. (marzo de 2016). Diseño e implantación de reloj biométrico en base a tecnología Arduino para monitoreo celular en la escuela luis pallares de yaruquí. Quito: universidad tecnológica israel.

Chaglia, L., Miranda , M., & Vasquez, J. (2011). Sistema publicitario inteligente con Raspberry Pi3, aplicación Android y hardware. *Apuntia Brava*, *13*(1), 1 - 14.

Cortes , O., Jimy, A., Medina, A., & Francisco , A. (2010). Sistemas de seguridad basados en biometria. *Scientia Et Technica*, *XVII*(46), 98 - 102.

Cortez, O., Medina, F., & Muriel, J. (2010). Sistema de seguridad basado en biometria. *Scientia Et Technica*, *XVII*(46), 98-102.

Diaz, V. (2013). Sistemas biométricos en materia criminal: un estudio comparado. *IUS*, *7*(31), 28- 47.

Gonzalez , R., & Perez, S. (2012). Leyes de protección de datos personales en el mundo y la protección de datos biométricos,. *Seguridad*.

Herrero, J., & Sanchez, J. (2015). Una mirada al mundo Arduino. *Revista Tecnologí@ y desarrollo*, 1-28.

Lopez, F., & Gustavo , J. (2013). Diseño e Implementación de Software y Hardware de un Registrador de Variables Eléctricas con Comunicaciones Ethernet Basado en Tecnología Arduino y Sistema de Supervisión HMI. *Departamento de Eléctrica y Electrónica, Escuela Politécnica del Ejército Sede Latacunga*, 1- 10.

Madrigal, C., Ramirez, J., & Hoyos, J. (2007). Diseño de un sistema biométrico de identificación usando sensores capacitivos para huellas dactilares. *Revista facultad de Ingenieria, 39*, 21-32.

Mendoza , A., & Mendoza, C. (2016). Sistemas de reconocimiento facial, como herramienta para la búsqueda. *Sinapsis La Rev. científica del ITSUP*, *8*(1930), 2-6.

Perez, H. (Agosto de 2018). SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS PARA EL INGRESO DE PERSONAL A LA EMPRESA ELECTROSERVICIOS QUERUBÍN DE LA CIUDAD DE PUYO. Ambato: Universidad Tecnica De Ambato .

Perez, S. (2016). Tecnologías biométricas aplicadas a la ciberseguridad. *10 incibe*, *1*.

Quintanilla , G. (2020). Legislación, riesgos y retos de los sistemas biométricos. *Revista chilena de derecho y tecnologia*, *9*(1), 19-25.

Ruiz, M., & Olivares , J. (2009). Una mirada a la biometria. *Revista Avances en Sistemas e Informática,*, *6*(2), 29 -38.

Ruiz, M., Rodriguez, J., & Olivares , J. (2009). Una mirada a la biometria. *Revista Avances en Sistemas e Informática*, *6*(2), 29 - 38.

Salcedo, M., & Cendros, J. (2016). USO DEL MINICOMPUTADOR DE BAJO COSTO "RASPBERRY PI" EN ESTACIONES METEOROLÓGICAS. *Télématique*, *15*(1), 62-84.

Vargas, M., Castillo, G., & Sandoval , J. (2015). Arduino una Herramienta Accesible para el Aprendizaje de Programación. *Revista de Tecnología e Innovación*, *2*(4), 810-815.

Vega, A., & Rivas, F. (2014). Internet de los objetos empleando Arduino para la gestión eléctrica domiciliaria. *Revista Escuela de Administración de Negocios*(77), 24-71.