



**UNIVERSIDAD DE GUAYAQUIL**  
**FACULTAD DE INGENIERÍA INDUSTRIAL**  
**DEPARTAMENTO ACADÉMICO DE GRADUACIÓN**

**TRABAJO DE TITULACIÓN**  
**PREVIO A LA OBTENCIÓN DEL TÍTULO DE**  
**INGENIERO EN TELEINFORMÁTICA**

**ÁREA**  
**TECNOLOGÍA ELECTRÓNICA**

**TEMA**  
**PROTOTIPO DE UNA CERRADURA ELÉCTRICA DE**  
**HUELLA DIGITAL UTILIZANDO ARDUINO CON**  
**COMUNICACIÓN BLUETOOTH**

**AUTOR**  
**HERNÁNDEZ PAREJA OMAR ISAÁC**

**DIRECTORA DEL TRABAJO**  
**ING. ELECT. GALLEGOS ZURITA DIANA ERCILIA, MG**

**GUAYAQUIL, OCTUBRE 2019**



**ANEXO XI.- FICHA DE REGISTRO DE TRABAJO  
DE TITULACIÓN  
FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:			
Prototipo de una cerradura eléctrica de huella digital utilizando arduino con comunicación bluetooth			
AUTOR(ES) (apellidos/nombres):		Hernández Pareja Omar Isaác	
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):		Ing. Gallegos Zurita Diana Ercilia / Ing. Parra López Rodolfo Antonio	
INSTITUCIÓN:		Universidad de Guayaquil	
UNIDAD/FACULTAD:		Ingeniería Industrial	
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:		Ingeniería en Teleinformática	
FECHA DE PUBLICACIÓN:		11 Junio 2020	No. DE PÁGINAS: 93
ÁREAS TEMÁTICAS:		Tecnología Electrónica	
PALABRAS CLAVES/ KEYWORDS:		Cerradura Biométrica, Seguridad domiciliar, micro SD, bluetooth.	
<b>RESUMEN/ABSTRACT</b> (100-150 palabras): El presente proyecto propone una alternativa tecnológica a la seguridad domiciliar para los ciudadanos que poseen bajos recursos, mediante el diseño de un prototipo, como la cerradura biométrica basado en arduino, además, de permitir el acceso remoto mediante un aplicativo móvil utilizando conexión vía bluetooth. El sistema cuenta con un sensor de huella dactilar, el cual es capaz de leer las huellas que habíamos registrado con anterioridad en una base de datos, para así, enviar estos datos de lectura a la placa de arduino y a su vez accionando el servomotor para la apertura de la cerradura de forma automática y cerrarla en un tiempo de 7 segundos. Además, cuenta con un lector de tarjeta micro SD para visualizar la hora de entrada al domicilio, se desarrollaron las encuestas para conocer la aceptación del prototipo en cuanto al funcionamiento y el costo.			
ADJUNTO PDF:		SI <input checked="" type="checkbox"/> X	NO <input type="checkbox"/>
CONTACTO CON AUTOR/ES:		Teléfono: 0969862594 Hernández Pareja Omar Isaac	E-mail: isaachernandezpareja@gmail.com
CONTACTO CON LA INSTITUCIÓN:		Nombre: Ing. Ramón Maquilón Nicola, MG	
		Teléfono: 593-2658128	
		E-mail: direccionTi@ug.edu.ec	



**ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE  
AUTORIZACIÓN DE LICENCIA GRATUITA**



**INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO COMERCIAL DE LA  
OBRA CON FINES NO ACADÉMICOS**

**FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

---

**LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA  
CON FINES NO ACADÉMICOS**

Yo, **HERNÁNDEZ PAREJA OMAR ISAÁC**, con C.C. No. **0926396714**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es “**PROTOTIPO DE UNA CERRADURA ELÉCTRICA DE HUELLA DIGITAL UTILIZANDO ARDUINO CON COMUNICACIÓN BLUETOOTH**” son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN\*, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.

---

**HERNÁNDEZ PAREJA OMAR ISAÁC**  
C.C.No. 0926396714



## ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD

FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA



## CERTIFICADO PORCENTAJE DE SIMILITUD

### CERTIFICADO PORCENTAJE DE SIMILITUD

Habiendo sido nombrada ING. GALLEGOS ZURITA DIANA ERCILIA, tutora del trabajo de titulación, certifico que el presente trabajo de titulación ha sido elaborado por HERNÁNDEZ PAREJA OMAR ISAÁC, C.C.: 0926396714, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: **“PROTOTIPO DE UNA CERRADURA ELÉCTRICA DE HUELLA DIGITAL UTILIZANDO ARDUINO CON COMUNICACIÓN BLUETOOTH”**, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio (URKUND) quedando el 6% de coincidencia.

The screenshot displays the URKUND web interface. At the top, it shows the document name 'OmarIsaacHernandezParejaURKUND.docx' with ID 'D64956748', submitted on '2020-03-06 07:03 (-05:00)' by 'omar.hernandezp@ug.edu.ec'. The recipient is 'diana.gallegosz.ug@analysis.orkund.com'. A message link is provided. Below, it states '6% de estas 16 páginas, se componen de texto presente en 9 fuentes.' The 'Lista de fuentes' (List of sources) section is active, showing a table with columns 'Categoría' and 'Enlace/nombre de archivo'. The sources listed are:

Categoría	Enlace/nombre de archivo
Blue icon	Marlon Acebo L.docx
Blue icon	TESIS-MARCO SACOTO.docx
Blue icon	TESIS - DESARROLLO DE UN DISPOSITIVO PORTÁTIL QUE GENERE ALERTAS EN CASO...
Blue icon	Tesis-Yamili Yagual Romero.docx
Blue icon	PLUAS LINDAO DORA.docx

At the bottom of the interface, there are buttons for '0 Advertencias', 'Reiniciar', 'Exportar', and 'Compartir'.

<https://secure.orkund.com/view/62981141-800706-511106>



Firmado electrónicamente por:  
**DIANA ERCILIA  
GALLEGOS  
ZURITA**

Ing. Diana Ercilia Gallegos Zurita, MG.  
TUTORA DE TRABAJO DE TITULACIÓN  
C.C. 1204926313

Fecha: 3 de marzo del 2020



## ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR DEL TRABAJO DE TITULACIÓN

**FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 3 Marzo 2020

Sr (a).

**Ing. Annabelle Lizarzaburu Mora, MG.**

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

**FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL**

Ciudad. -

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación **“PROTOTIPO DE UNA CERRADURA ELÉCTRICA DE HUELLA DIGITAL UTILIZANDO ARDUINO CON COMUNICACIÓN BLUETOOTH”** del estudiante **HERNÁNDEZ PAREJA OMAR ISAÁC**, indicando que ha cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, **CERTIFICO**, para los fines pertinentes, que el estudiante está apto para continuar con el proceso de revisión final.

Atentamente,



Firmado electrónicamente por:  
**DIANA ERCILIA  
GALLEGOS  
ZURITA**

**Ing. Diana Gallegos Zurita, MG.**  
**TUTORA DE TRABAJO DE TITULACIÓN**  
**C.C. 1204926313**

FECHA: 3 de marzo del 2020



**ANEXO VIII.- INFORME DEL DOCENTE REVISOR**  
**FACULTAD DE INGENIERÍA INDUSTRIAL**  
**CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 24 Abril 2020

Sr (a).

**Ing. Annabelle Lizaraburu Mora, MG.**

Director (a) de Carrera Ingeniería en Telemática / Telemática

**FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL**

Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación **PROTOTIPO DE UNA CERRADURA ELÉCTRICA DE HUELLA DIGITAL UTILIZANDO ARDUINO CON COMUNICACIÓN BLUETOOTH** del estudiante **HERNÁNDEZ PAREJA OMAR ISAÁC**. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimiento de los siguientes aspectos:

Cumplimiento de requisitos de forma:

El título tiene un máximo de 13 palabras.

La memoria escrita se ajusta a la estructura establecida.

El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad.

La investigación es pertinente con la línea y sublíneas de investigación de la carrera.

Los soportes teóricos son de máximo 13 años.

La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:

El trabajo es el resultado de una investigación.

El estudiante demuestra conocimiento profesional integral.

El trabajo presenta una propuesta en el área de conocimiento.

El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica el que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente



Firmado electrónicamente por:

**RODOLFO**  
**ANTONIO PARRA**  
**LOPEZ**

**Ing. Rodolfo Antonio Parra López, MG.**

**REVISOR DE TRABAJO DE TITULACIÓN**

**C.C. 0909770448**

FECHA: 24/04/2020

### **Dedicatoria**

Dedico este proyecto de tesis a mis abuelos, padres y hermanas por ser mi motor y apoyo en este proceso.

### **Agradecimiento**

Agradezco a mis abuelos Carlos Pareja y Rosa Ávila por su experiencia de enfrentar la vida y el apoyo, me han ayudado en la elaboración de cada proceso de la tesis.

A mis padres y hermanas por la paciencia y el apoyo incondicional

A mi tutora la Ing. Elect. Diana Gallegos, por la paciencia, experiencia y la dedicación que ha representado en la elaboración del presente proyecto de titulación.

Y a mis amigos que me mostraron su apoyo y confianza depositada en mí, dándome siempre sus ánimos para sobresalir en cada proceso.



## Índice del contenido

Nº	Descripción	Pág.
	<b>Introducción</b>	1

### Capítulo I El problema

Nº	Descripción	Pág.
1.1	Definición del problema	2
1.1.1	Planteamiento del problema	3
1.1.2	Formulación del problema	3
1.1.3	Sistematización del problema	3
1.2	Objetivos de la investigación	3
1.2.1	Objetivo general	3
1.2.2	Objetivos específicos	3
1.3	Delimitación del problema	4
1.3.1	Delimitación geográfica	4
1.4	Justificación e importancia	4
1.5	Alcance	5

### Capítulo II Marco teórico

Nº	Descripción	Pág.
2.1	Antecedentes	6
2.2	Marco conceptual	8
2.2.1	Sistemas biométricos	8
2.2.1.1	Identificación y verificación	9
2.2.1.2	Rasgos biométricos	10
2.2.1.3	Característica de la biometría	10
2.2.1.4	Beneficios e inconvenientes de la biometría	10
2.2.1.5	Métodos de identificación biométrica	11
2.2.1.6	Métodos del sistema biométrico	15

2.2.1.7	Tipos de dispositivos biométricos de huella dactilar	15
2.2.1.8	Relación de la biometría y la seguridad	18
2.2.1.9	Seguridad	18
2.2.1.9.1	Tipos de seguridad	19
2.2.1.9.2	Seguridad de acceso físico	19
2.2.1.10	Cerradura	10
2.2.1.10.1	Tipos de cerradura	20
2.3	Marco Tecnológico	22
2.3.1	Arduino	22
2.3.2	Micro SD card adapter	23
2.3.3	Módulo bluetooth HC-05	23
2.3.4	Módulo RTC DS3231 Real time clock	24
2.3.5	Módulo lector de huella Finger print R307	25
2.3.6	LCD 16×2 por I2C	26
2.3.7	Servomotor	26
2.3.8	Resistencia	27
2.3.9	Pulsadores	27
2.3.10	App inventor 2	28
2.4	Marco Legal	28
2.4.1	Marco legal en el Ecuador	28
2.4.2	Marco legal en el exterior	29

### **Capítulo III**

#### **Metodología**

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
3.1	Diseño de la investigación	30
3.2	Enfoque de la investigación	30
3.3	Método de la investigación	30
3.3.1	Método bibliográfico	30
3.3.2	Método explorativo	31
3.3.3	Método descriptivo	31
3.4	Población y muestra	31

3.5	Técnicas e instrumentos	33
3.6	Encuestas	33
3.7	Análisis de los resultados de la encuesta	33
3.8	Resultado general	42

## **Capítulo IV**

### **Desarrollo de la propuesta**

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
4.1	Introducción	43
4.2	Desarrollo	43
4.2.1	Etapa 1	43
4.2.1.1	Diseño de circuitos	43
4.2.2	Etapa 2	48
4.2.2.1	Codificación	48
4.2.3	Etapa 3	49
4.2.3.1	Creación de la aplicación móvil	49
4.3	Diseño general del sistema	50
4.4	Presupuesto	51
4.5	Conclusiones	52
4.6	Recomendaciones	52
5.0	Anexo	53
5.1	Codificación en arduino	53
5.2	Construcción del prototipo de cerradura biométrica con huella dactilar	69
	Bibliografía	76

## Índice de Tablas

<b>Nº</b>	<b>Descripción</b>	<b>Pág.</b>
1	Características de los sistemas biométricos	14
2	Ficha técnica del lector de huella ZK L7000U.	16
3	Ficha técnica del ML10 Series.	17
4	Ficha técnica del Zkteco F21	17
5	Ficha técnica del Huella T1200	18
6	Especificaciones Técnicas De Tipos de Arduino	22
7	Comparación de los módulos de Bluetooth	24
8	Población del sector	31
9	Muestra total por encuestar	33
10	Porcentaje si cuentan con algún sistema tecnológico en su domicilio	34
11	Porcentaje si han escuchado de un sistema biométrico	35
12	Porcentaje para conocer si están dispuesto a tener el sistema	36
13	Porcentaje si les gustaría tener un registro en su cerradura	37
14	Porcentaje si les gustaría contar con el sistema	38
15	Porcentaje sobre la utilización de su celular en la cerradura	39
16	Porcentaje sobre la aceptación del costo de la cerradura biométrica	40
17	Porcentaje de aceptación del costo de la cerradura con registro	41
18	Materiales y costos del prototipo	51

## Índice de figuras

<b>Nº</b>	<b>Descripción</b>	<b>Pág.</b>
1	Mapa de las calles donde se realizará la encuesta	4
2	Diagrama de bloques del proceso de identificación biométrico	9
3	Diagrama de bloques del proceso de verificación biométrico	10
4	Tablet de escritura para firma digital	11
5	Escáner celular de reconocimiento facial	12
6	Partes externas del ojo	12
7	Análisis del espectro de la voz humana	13
8	Características de una huella dactilar	13
9	Geometría de la mano	13
10	Módulo general del sistema biométrico (Basado en Wayman)	15
11	ZK L7000U	16
12	ML10 Series	16
13	Zkteco F21	17
14	Huella T1200	18
15	Cerradura sobrepuesta de barra fija	20
16	Cerradura sobrepuesta, PHILIPS	20
17	Chapa eléctrica, LLOYDS	20
18	Cerradura inteligente Touch-to-open	21
19	Cerrojo Smart Code	21
20	Cerradura Smart Door Lock	21
21	Módulo Micro SD	23
22	Módulo RTC DS3231 Real time clock	24
23	Error habitual del sensor mostrado en Monitor Serie (Arduino IDE	25
24	Módulo lector de huella Finger print R307	25
25	Pantalla LCD 16x2 con el protocolo I2C	26
26	Servomotor	26
27	Resistencias	27
28	Pulsadores	27

29	App Inventor	28
30	Porcentaje si cuentan con algún sistema tecnológico en su domicilio	34
31	Porcentaje si han escuchado de un sistema biométrico	35
32	Porcentaje para conocer si están dispuesto a tener el sistema	36
33	Porcentaje si les gustaría tener un registro en su cerradura	37
34	Porcentaje si les gustaría contar con el sistema	38
35	Porcentaje sobre la utilización de su celular en la cerradura	39
36	Porcentaje sobre la aceptación del costo de la cerradura biométrica	40
37	Porcentaje de aceptación del costo de la cerradura con registro	41
38	Conexión del módulo bluetooth HC-05 en el arduino Mega	44
39	Conexión del módulo fingerprint R307 en el arduino Mega	44
40	Conexión en el prototipo del módulo R307 en el arduino Mega	45
41	Los cuatros patrones principales	45
42	Proceso común de escaneo de la huella digital	45
43	Conexión del RTC DS3231 en el arduino Mega	46
44	Codificación del módulo RTC 3231 en Arduino IDE	46
45	Conexión del módulo Adapter MicroSD en el arduino Mega	46
46	Registro de ingreso en la cerradura. Elaborado por el autor	47
47	Cerradura rediseñada con servomotor	48
48	Mensaje del enrolamiento de la huella principal en Monitor	48
49	Esquema de la aplicación en App Inventor	49
50	Diagrama de bloque de la aplicación App inventor	50
51	Diagrama de Flujo del funcionamiento general del prototipo	50
52	Diagrama de flujo sobre añadir una nueva huella dactilar al prototipo	51
53	Conexión del sensor R307 al arduino Mega	69
54	Conexión del bluetooth y del sensor de huella R307	70
55	Conexión del RTC DS3231 con el bluetooth y el R307	70
56	Adapter micro SD con RTC DS3231, bluetooth y R307	71
57	Pantalla LCD 16x2, micro adapter, RTC DS3231, bluetooth y R307	72
58	Página principal del sitio web <a href="http://ai2.appinventor.mit.edu/">http://ai2.appinventor.mit.edu/</a>	72
59	Proceso de registro en la página web de App inventor	73
60	Cuadro de bienvenida del sitio web	73
61	Creación de la aplicación para la cerradura	74

62	Creación del diagrama de bloque para la cerradura	74
63	Generar el archivo para el dispositivo móvil	75
64	Codificación en Arduino	75



**ANEXO XIII.- RESUMEN DEL TRABAJO DE  
TITULACIÓN (ESPAÑOL)**

**FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



---

**“PROTOTIPO DE UNA CERRADURA ELÉCTRICA DE HUELLA DIGITAL  
UTILIZANDO ARDUINO CON COMUNICACIÓN BLUETOOTH”**

**Autor:** Hernández Pareja Omar Isaác

**Tutor:** Ing. Diana Ercilia Gallegos Zurita, MG.

**Resumen**

El presente proyecto propone una alternativa tecnológica a la seguridad domiciliaria para los ciudadanos que poseen bajos recursos, mediante el diseño de un prototipo, como la cerradura biométrica basado en arduino, además, de permitir el acceso remoto mediante un aplicativo móvil utilizando conexión vía bluetooth. El sistema cuenta con un sensor de huella dactilar, el cual es capaz de leer las huellas que habíamos registrado con anterioridad en una base de datos, para así, enviar estos datos de lectura a la placa de arduino y a su vez accionando el servomotor para la apertura de la cerradura de forma automática y cerrarla en un tiempo de 7 segundos. Además, cuenta con un lector de tarjeta micro SD para visualizar la hora de entrada al domicilio, se desarrollaron las encuestas para conocer la aceptación del prototipo en cuanto al funcionamiento y el costo.

**Palabras Claves:** Cerradura Biométrica, Seguridad domiciliaria, micro SD, bluetooth.





**ANEXO XIV.- RESUMEN DEL TRABAJO DE  
TITULACIÓN (INGLÉS)**

**FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

---



**“PROTOTYPE OF AN ELECTRIC FINGERPRINT LOCK USING ARDUINO WITH  
BLUETOOTH COMMUNICATION”**

**Author:** Hernández Pareja Omar Isaac

**Advisor:** EE Gallegos Zurita Diana Ercilia, MG

**Abstract**

This project proposes a technological alternative to home security for low-income citizens by designing a prototype, such as the biometric lock based on arduino, as well as allowing remote access through a mobile application using Bluetooth connection. The system has a fingerprint sensor, which is capable of reading the fingerprints previously registered in a database, so as to send this reading data to the arduino plate and in turn driving the servomotor to open the lock automatically and close it in a time of 7 seconds. In addition, it has a micro SD card reader to display the time of entry to the house. Surveys were developed to know the acceptance of the prototype in terms of operation and cos

**Keywords:** Biometric lock, Home security, micro SD, bluetooth.

## **Introducción**

En la actualidad, la mayoría de los ciudadanos no cuentan con un sistema tecnológico que refuerce la seguridad en sus domicilios por el alto costo de los equipos, es por eso que optan por cambiar la cerradura tradicional de metal a una eléctrica, pero el funcionamiento no cambia pues el método de vulneración en ambas cerraduras es de introducir una llave para abrirla, esta opción sigue siendo vulnerable debido a la clonación de llaves y al método del bumping [1].

El presente sistema propone una solución al problema del alto índice delincriminal domiciliario además del mencionado con anterioridad, de una manera eficiente, rápida y amigable por medio del reconocimiento de la huella dactilar de cada habitante en el domicilio, una vez validada compara con las huellas almacenadas en la base de datos, dando así paso para el enrolamiento, presenta el registro de entrada al domicilio, el método utilizado es el bluetooth que permite la apertura de la puerta a una distancia máxima de 10 metros de la cerradura al celular.

En los siguientes capítulos se detalla la elaboración del prototipo también con su codificación para que los ciudadanos, puedan implementarlo en su vivienda para conocer más sobre la tecnología que hay en el mercado, además de que los materiales pueden ser adquiridos en el país, el prototipo elaborado está optimizado en los precios para ser accesible al bolsillo de los ciudadanos.

## **Capítulo I**

### **El problema**

#### **1.1 Definición del Problema**

##### **1.1.1 Planteamiento del Problema**

La tecnología evoluciona a pasos agigantados contribuyendo en la comodidad, confiabilidad y seguridad en la vida cotidiana del ser humano, no obstante, a pesar de contribuir grandes beneficios, la misma se ha transformado en instrumento para la delincuencia.

En el concepto de seguridad se derivan, la pública, que está constituida por el cargo exclusivo del Gobierno Nacional junto con el apoyo de las Fuerzas Militares y de la Policía Nacional, que tienen como finalidad garantizar los derechos y salvaguardar la seguridad de los habitantes. Y la privada, que sus prestaciones están a cargo para el sector privado únicamente garantizando la seguridad de empleador.

El problema de la inseguridad en el Ecuador es tan significativo en el ámbito de robos a domicilios, que hubo una disminución, entre el periodo de enero y mayo del año 2019, mostrando un total de 4.587, con relación al mismo periodo del 2018 con 5,551, “Según datos del Ministerio de Gobierno” [2].

Hoy en día, las tecnologías de información nos permiten medir las características informáticas a través de la automatización de procesos, dando así lugar, a los sistemas biométricos que posibilita los procesos de identificación, tales como: registrar la identidad; y procesos de verificación como: confirmar identidad.

Los sistemas biométricos, que su característica es de registrar en el sistema, una imagen ya sea de la huella dactilar, voz o iris surgió para contrarrestar el método de vulnerabilidad las cerraduras como es el bumping, el cual consiste en que la llave manipulada encaja con la mayoría de las cerraduras, introduce en la cerradura del cilindro y se golpea con el fin de hacer que los cilindros se salten simultáneamente, dándose así el giro de la llave y la apertura de la cerradura sin forzarla.

Apoyados en esta necesidad, se identificó la oportunidad de introducir dispositivos que estén a la vanguardia de la tecnología como son las cerraduras de huella dactilar bajo

tecnología biométrica con las cuales, se pretende contribuir a la seguridad en el acceso y control residencial.

### **1.1.2 Formulación del problema**

¿Cuál es la situación actual del Ecuador por la que es necesario utilizar un sistema biométrico con huella dactilar?

### **1.1.3 Sistematización del problema**

¿Los equipos que se requiere son accesibles en el país?

¿El dispositivo que se plantea desarrollar reducirá costos con respecto a empresas que ofrecen el mismo servicio?

¿La arquitectura de la cerradura biométrica está completamente hecha en el internet o requiere de una programación única para cada vivienda?

¿El prototipo cumple con los requisitos de seguridad?

¿Se podría vulnerar la aplicación que incluye la comunicación bluetooth de la cerradura biométrica?

## **1.2 Objetivos de la Investigación**

### **1.2.1 Objetivo General.**

Desarrollar una cerradura biométrica con huella dactilar utilizando arduino junto con la comunicación bluetooth para brindar seguridad y rápido control de acceso a las viviendas.

### **1.2.2 Objetivos Específicos.**

- Detallar los elementos y la arquitectura de la cerradura biométrica con la vanguardia de la tecnología.
- Evaluar el nivel de aceptación del prototipo de seguridad en un sector de la ciudad de Guayaquil.
- Desarrollar el prototipo de cerradura biométrica que pueda competir en el mercado de la seguridad.
- Implementar un medio inalámbrico para que ambos sistemas, la cerradura biométrica y la aplicación Android, puedan comunicarse.

### 1.3 Delimitación de Tema

Este proyecto consiste en el desarrollo de un prototipo de cerradura biométrica que permite acceder a las residencias mediante la utilización de la huella dactilar, es por eso, que antes se debe registrar la huella para que el sistema la almacene en su base de datos, con esto poder identificar al usuario en tiempo real de quien ingresa a la vivienda, estos datos son almacenados en el módulo de la memoria micro SD para luego poder ser extraída manualmente y colocarla en el celular.

#### 1.3.1 Delimitación Geográfica

El proyecto se realizará en un determinado sector del suburbio oeste de la ciudad de Guayaquil, que comprende desde la calle Buena Fe hasta El Guabo entre Ismael Pérez Castro y Av35, en las calles mencionadas todos los días el sector se convierte en comercial de vendedores ambulantes como recicladores.



Fig. 1- Mapa de las calles donde se realizará la encuesta. Elaborado por google maps.

#### 1.4 Justificación e importancia.

La propuesta es brindar seguridad en las viviendas por la alta cifra de la delincuencia en lo que va del año 2018 y 2019 [2], la lucha contra el crimen de parte de la Policía Nacional junto a la Alcaldía de Guayaquil no abastece, debido a la alta población, es por eso que los ciudadanos deben tomar sus propias medidas o alternativas para su seguridad.

En los siguientes capítulos se plantea la realización del prototipo de cerradura biométrica como alternativa accesible y recomendable para la ciudadanía, que es rápido y seguro, por el reconocimiento de la huella dactilar.

La función principal del prototipo de cerradura biométrica es de utilizar la huella dactilar de los residentes en las viviendas para poder ingresar, actualmente es el método más seguro porque, en comparación con los otros sistemas que la vulnerabilidad es desapercibida por el usuario, en cambio, este sistema requiere la autorización del usuario con el fin, de percatarse que personas ajenas a la vivienda desean vulnerar el sistema, puesto que si desean copiar la huella en el sensor por medio de silicona, plástico o jabón el sistema les denegará el acceso porque al lector no le resultará óptimo leer varias bifurcaciones y crestas que se encuentran alojados en los materiales para la vulneración del equipo, además que cada individuo posee la huella como característica única en el mundo.

Con la comunicación Bluetooth podemos ingresar a nuestras viviendas o establecimiento de una manera más rápida porque se tiene una aplicación instalada en el celular la cual reconocerá al usuario, gracias a la comunicación bluetooth dicha aplicación funciona con una distancia de 10 metros o 30 pies.

### **1.5 Alcance**

Se realizará una investigación previa de los elementos que se necesiten para el prototipo que sean accesibles en el mercado de tecnología en el país como también en la economía de los usuarios, para así competir con las empresas que desarrollan este dispositivo.

Además de una encuesta para evaluar a una determinada población de un específico sector de la ciudad de Guayaquil para comprobar el nivel de aceptación del prototipo como un sistema vanguardista de seguridad en las viviendas.

El desarrollo de este proyecto se enfoca en que el dispositivo tiene un lector biométrico de huella dactilar y una comunicación bluetooth conectado con el microcontrolador arduino mega.

## Capítulo II

### Marco Teórico

#### 2.1 Antecedentes

El principio básico de la biometría empezó desde la época de los faraones, en el Valle del Nilo (Egipto), el cual consistía, en verificar a los habitantes del pueblo por sus rasgos físicos como cicatriz, medidas, color de los ojos, tamaño de dentadura para identificar a los que participaban en operaciones comerciales, judiciales y los que utilizaban dichos depósitos comunitarios de cosechas. Este método les permitía a los guardias reconocer a cada propietario y de esa manera así ellos poder disponer correctamente de sus cosechas.

En China del siglo XV, los mercaderes también utilizaban este método, a diferencia de los egipcios, los chinos utilizaban tintas en las manos de esta forma lograban una impresión para identificar a los niños que trabajen de manera adecuada.

Durante el siglo XIX un grupo de investigadores de criminología tuvieron interés de querer relacionar las tendencias criminales con las características físicas, pues uno de los métodos era documentar los rasgos faciales en forma de fotografía, es decir, que tomaban las medidas del rostro de las personas, este método fue conocido como Bertillonage, hubo una gran cantidad de datos obtenidos con equipos de medición, pero dichos datos no eran concluyentes, la idea resultó efectiva, por este motivo se comenzó con el desarrollo de la identificación mediante la huella dactilar.

En 1985, los doctores Leonard Flom y Aran Safir crearon el algoritmo de reconocimiento de iris con el concepto de que no hay dos iris iguales, con esta investigación el doctor Flom le propuso al Dr Daugman la creación de un algoritmo automatizado en 1994 que fue patentada junto con la empresa Iridian Technologies [3]. La agencia nuclear de defensa comenzó a trabajar con IriScan y a su vez desarrollar un prototipo, 18 meses después, estaría disponible para uso empresarial.

Al pasar de los años el método de identificación biométrica ha ido evolucionando junto con el avance de la tecnología aportando comodidad, seguridad y confiabilidad en la vida cotidiana del hombre.

Es por eso que ya no solo se utiliza la huella digital o el reconocimiento de iris, sino que también se incorporó la firma digital, el reconocimiento facial y de voz y así prevenir la

suplantación de identidad para cualquier actividad maliciosa en la que el atacante se hace pasar por terceros y a su vez cometer delitos como: fraudes, ciberacoso, extorsión, entre otros.

De acuerdo con el autor (Escobar,2015) en su investigación titulada “Cifrado caótico de plantilla de huella dactilar en sistemas biométricos” afirma que los sistemas biométricos son capaces de medir métodos automáticos para las características fisiológicas o comportamientos del individuo, estos a su vez han sido utilizados tanto para identificar y autenticar a las personas, siendo la huella dactilar la característica más utilizada, debido que es más práctico, seguro, de gran aceptación y sus bajos costos de implementación.

Según la revista (SoluciónArg, 2015) hace mención en el artículo “BioAcces” lo cual determina que las huellas digitales humanas son únicas para cada individuo y que suelen ser utilizadas como certificado de identidad. Pues es muy usada en el ámbito de la criminalística. Actualmente este sistema se está expandiendo de forma acelerada para el control de espacios físicos, recursos de computación, de redes, cuentas bancarias, registro de ingreso y salida de empleados, todo esto para realizar las operaciones de grado sensible e identificar las veces que sea necesario a las personas.

De acuerdo con el autor (Ferrer,2016) comenta sobre el uso de la biometría e indica que cada vez es más cotidiano debido a que se encuentra incorporado en los celulares inteligentes, además de que por medio de este método las contraseñas convencionales están llegando a su fin, por esto, se necesita tener una infraestructura actualizada exclusivamente para hacerle frente a las amenazas cibernéticas que cada vez van en aumento.

El autor (Martinez,2016) en su artículo “Tecnología Biométrica” publicado por BBVA Innovation Center hace mención destacando a la señal vocal como otro método efectivo para la autenticación de las personas, pues está siendo utilizado por los bancos HSBC y First Direct del Reino Unido, consiste en que las ondas sonoras del usuario, están creadas de manera única e independientemente de su estado de salud o ánimo. Estas entidades bancarias utilizan puramente software, pues poseen servidores y filtros de los cuales son capaces de extraer la información de la señal vocal y así transformarla en algoritmos matemáticos para su rápida respuesta de comparación en fracción de segundos. Los usuarios no necesitan ningún instrumento adicional para gozar este beneficio, debido a que los bancos cuentan con el sistema. Este método es muy fácil para identificar a las personas y así consulten sus cuentas bancarias a través de una llamada al call center o mediante la aplicación del banco.



En Ecuador es común que las entidades bancarias hagan uso del sistema biométrico del reconocimiento facial, FacePhi es la compañía que trabaja con la mayoría de las entidades bancarias en el Ecuador, llegó al país en el 2005 para implementar en el Banco Guayaquil [4] y en el Banco del Pacífico[5], el reconocimiento de facial en los dispositivos móviles mediante el acceso de la cámara frontal de nuestros smartphones y así permite el registro de la cuenta para evitar fraudes o suplantación de identidad.

FacePhi brinda tecnología a las diferentes entidades bancarias como: Banco Guayaquil, Banco Pichincha y Banco del Pacífico tienen los servicios:

- SelphID que permite al usuario abrir una cuenta en cualquier lugar mediante la captura de su cédula y la selfie validando datos como la comparación facial de la cédula con la base existente del estado [6].
- Selphi permite realizar aprobaciones de transacciones mediante la selfie, extrayendo las características principales del usuario para convertirlas en un patrón que se enviará al servidor de la institución [7].
- Look&Phi es otra solución para realizar la validación de transacciones mediante la biometría ocular, se obtiene un patrón encriptado descartando los puntos susceptibles como los cambios de variación del entorno [8].

Otra tecnología que posee el Banco Guayaquil de FacePhi, es PhiVox permite al usuario identificarse mediante el patrón de la voz donde se enviará al servidor del banco como almacenamiento del registro biométrico en el call center [9], la entidad bancaria Banco Bolivariano posee la tecnología del SelphID [10].

## **2.2 Marco Conceptual**

### **2.2.1 Sistemas biométricos**

La biometría se origina del griego (bios) que significa vida y (metrón) que es medida, pues este sistema es utilizado durante las últimas décadas como método de identificación, el cual es muy utilizado en las empresas por su utilidad de registrar a sus trabajadores (hora de entrada-break-hora de salida) mediante la huella dactilar de cada uno, es por eso que estos sistemas brindan seguridad exclusiva de que ninguna persona externa a la empresa puede entrar con el fin de cometer delitos.

Es por eso que estos sistemas biométricos son método de identificación y verificación de una persona utilizando la biometría estática, es por eso que la huella dactilar al ser una

característica inherente de la persona, tiene como ventaja la comodidad del usuario y facilidad de traslado sin la posibilidad de perder u olvidar porque siempre están con la persona además de que no se puede transmitir de forma deliberada (Marquez Moreno, Niño Garzón, & Luengas Contreras, 2017).

Estos sistemas lograron posesionarse actualmente como el método más importante en la seguridad y vigilancia. Desde sus inicios eran uso exclusivo de grandes compañías por sus costos elevados, pero debido a la alta producción se convirtieron en insumos de gran ayuda generando así estrategia que dificulten la suplantación de las personas.

### 2.2.1.1 Identificación y verificación

#### Identificación

El sistema reconoce la identidad del usuario si está registrada como alguien preexistente, es decir, el dispositivo sabe de quién se trata. Este proceso es de combinación uno a muchos (1: N), el cual consiste en tomar una muestra de la huella y analizarla en la base de datos existente.



Fig. 2.-Diagrama de bloques del proceso de identificación biométrico.

#### Verificación

El sistema confirma si se trata del usuario registrado en su base de datos, esto quiere decir que se toma la muestra de la huella para ser comparada con otra registrada. Este proceso es de combinación uno a uno (1:1), si coincide la verificación el dispositivo le da los privilegios y accesos al usuario.



Fig. 3.-Diagrama de bloques del proceso de verificación biométrica

### 2.2.1.2 Rasgos biométricos

Los sistemas biométricos deben de cumplir con determinados requisitos y condiciones en su utilización de los métodos de identificación y verificación tales como:

- Universalidad: Cada persona tiene las mismas características
- Singularidad o Univocidad: Característica diferenciable entre personas.
- Estabilidad: Continuidad a lo largo del tiempo de uso y en diferentes condiciones ambientales
- Cuantificable: Calculado de forma numérica
- Aceptabilidad: Aprobación de las personas
- Rendimiento: Alto nivel de precisión
- Usurpación: Resistencia a técnicas fraudulentas

### 2.2.1.3 Característica de la biometría

- Características Estructurales o Estáticas: Están en determinadas partes del cuerpo en el ser humano tales como: los ojos, retina, piel, rostro y huella dactilar.
- Características Funcionales o Dinámicas: Se consideran mediante el aspecto del movimiento corporal, por ejemplo: El manuscrito, movimiento de la boca o reconocimiento de voz

### 2.2.1.4 Beneficios e inconvenientes de la biometría

#### Beneficios

- La huella dactilar es una característica única e irrepetible en cada persona, solo se debe ponerla en el escáner y listo. Esto ahorra tiempo y esfuerzo en cualquier lugar.

- Imposible a pérdida, debido que es una parte de nuestro cuerpo y no un elemento externo (llaves, NFC o tarjetas).
- Reduce los costos de mantenimiento, no se necesita renovar en determinado tiempo por caducidad.
- De uso fácil, pues no se requiere tener conocimientos avanzados ni periodo de adaptación para utilizarlo.
- Aumenta la seguridad, solo pueden tener acceso al espacio establecido las personas que estén registradas en la base de datos del sistema.
- Control presencial, estos sistemas no permite la suplantación de otras identidades ya que era muy común prestarse las llaves, compartir el numero o la tarjeta del compañero para cometer irregularidades en el registro.

### **Inconvenientes**

- El sistema es poco recomendable en sitios de alta concurrencia donde los usuarios acceden de manera eventual.
- Actividades laborales pueden afectar a la huella dactilar, como la manipulación de químicos o sustancias que manchen el lector biométrico.

### **2.2.1.5 Métodos de identificación biométrica**

#### **Reconocimiento de firmas**

Esta tecnología es muy económica si se quiere implementar porque solo se necesita de una tableta de escritura conectada a una computadora, este aspecto está relacionado a la localización del inicio-final, concavidad y el grado de inclinación del trazo, esta consistencia es creada debido a la práctica a lo largo del tiempo por esta razón el patrón es reconocible como identificación biométrica. La única desventaja que el usuario nunca firma de manera idéntica dos veces. (Santamaría, 2017).



*Fig. 4.-Tablet de escritura para firma digital*

## Reconocimiento facial

Este método es el menos exacto en comparación con las huellas dactilares debido a que su clasificación en la apariencia de la persona intenta medir la distancia del rostro, el ancho de nariz, la distancia del ojo a la boca o la distancia de la mandíbula.

El primer proceso es la obtención de una imagen actual o una imagen bidimensional de la persona, el cual no debe estar desplazada a más de 35 grados, este proceso dura entre veinte a treinta segundos. (Gómez, 2016).

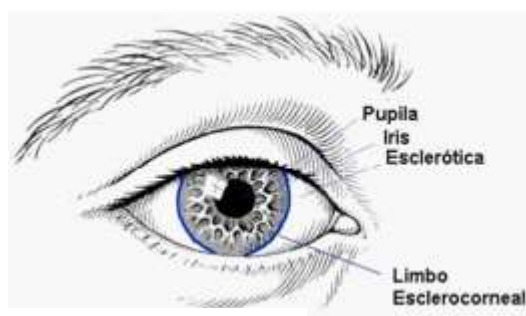


*Fig.5.- Escáner celular de reconocimiento facial*

## Patrón del iris.

Es uno de los métodos más confiables en los sistemas biométricos puesto que el iris posee 266 puntos únicos mientras que la generalidad de sistemas biométricos poseen entre 13 a 60 características distintas, además de que cada ojo es único y estable con el paso del tiempo y a diferentes cambios en el ambiente del clima.

Las lecturas del iris son tomadas con una cámara infrarrojos especializada de alta resolución, este proceso dura aproximadamente uno o dos segundos consiste fotografiar las variables a una distancia establecida de 30 cm como: la posición, iluminación, ángulo de captura y cierre de parpados, (Miranda, 2016).



*Fig. 6.-Partes externas del ojo*

### Reconocimiento de voz.

Está basado en las variaciones de la voz donde cada palabra se descompone en segmentos, obteniendo 3 o 4 tonos dominantes, que a su vez son capturados en forma digital y almacenados en un espectro que se conoce como plantilla de la voz (voice print)

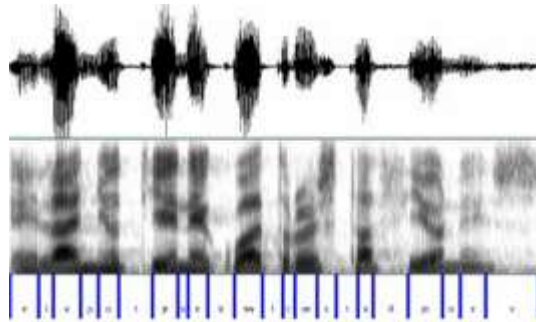


Fig. 7.-Análisis del espectro de la voz humana

### Huella dactilar

La huella se conforma por una serie de líneas oscuras que representa la cresta que a su vez hay una serie de espacios blancos llamados los valles, este sistema se basa en la ubicación y dirección de las terminaciones de cresta, bifurcación, deltas y valles

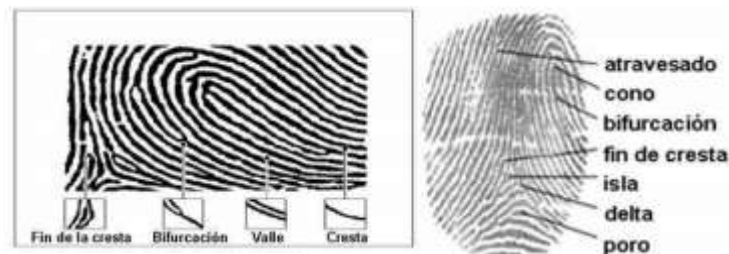


Fig. 8.- Características de una huella dactilar

### Geometría de la mano

El sistema biométrico de la mano consta de la combinación de imágenes individuales de los dedos, se extraen datos como las longitudes, anchuras, alturas, posiciones relativas y articulaciones. (Caballero, 2016).



Fig. 9.- Geometría de la mano

**Tabla 1.- Características de los sistemas biométricos**

<b>Características Biométricas</b>	<b>Universalidad</b>	<b>Fiabilidad</b>	<b>Prevención de ataques</b>	<b>Uso Fácil</b>	<b>Aceptabilidad</b>	<b>Costos</b>	<b>Permanencia</b>	<b>Tamaño del lector</b>
<b>Reconocimiento de Firmas</b>	Alta	Media	Media	Alta	Media	Bajo	Baja	Pequeño
<b>Reconocimiento Facial</b>	Media	Alta	Media	Alta	Muy Alta	Medio	Media	Medio
<b>Patrón del Iris</b>	Alta	Muy Alta	Alta	Media	Media	Muy Alto	Alta	Muy Grande
<b>Reconocimiento de Voz</b>	Media	Alta	Media	Alta	Alta	Bajo	Media	Pequeño
<b>Huella Dactilar</b>	Alta	Alta	Alta	Alta	Media	Medio	Alta	Pequeño
<b>Geometría de la mano</b>	Alta	Alta	Baja	Media	Media	Alto	Media	Grande

*Información adaptada de Sistemas Biométricos. Elaborado por los autores César Tolosa y Borja Álvaro*

### 2.2.1.6 Módulos del sistema biométrico

Los modelos de los sistemas biométricos configuran la estructura del sistema de reconocimiento de patrones donde se recogen un conjunto de datos biométricos, estos datos se extraen y se comparan por 5 subsistemas:

- Recolección de datos
- Transmisión de datos
- Procesamiento de señal
- Almacenamiento de datos
- Toma de decisión

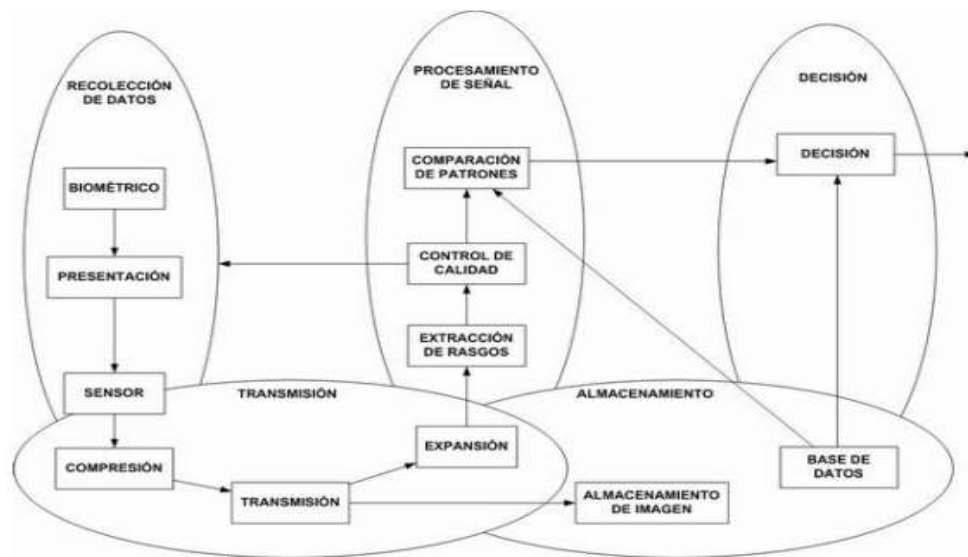


Fig. 10.- Módulo general del sistema biométrico (Basado en Wayman)

### 2.2.1.7 Tipos de dispositivos biométricos de huella dactilar

Actualmente en el Ecuador existen diversos equipos biométricos que están enfocados en la seguridad de hogares, empresas e instituciones. Por eso a continuación se mostrará dispositivos biométricos de huella dactilar con sus especificaciones técnicas y su precio en el mercado:

- ZK L7000U





Fig. 11.- ZK L7000U

**Tabla 2-** Ficha técnica del lector de huella ZK L7000U.

Capacidad de huellas	500 huellas
Fuente de alimentación	4 baterías alcalinas AA
Desbloqueo de respaldo	Llave
Interfaz	USB 2.0
Resolución del sensor	500 dpi
Precio	\$249.00

Información obtenida de Biometrics Control y Seguridad.

- ML10 Series



Fig. 12.- ML10 Series.

**Tabla 3-** *Ficha técnica del ML10 Series.*

Capacidad de huellas	180 huellas
Fuente de alimentación	4 baterías alcalinas AA
Desbloqueo de respaldo	Llave mecánica
Interfaz	USB 2.0
Resolución de sensor	500 dpi
Precio	\$177.99

*Información obtenida de CTS Solutions.*

- Zkteco F21



*Fig. 13.- Zkteco F21*

**Tabla 4.-** *Ficha técnica del Zkteco F21*

Capacidad de huellas	3000 huellas
Fuente de alimentación	12V DC 3A
Desbloqueo de respaldo	Por teclado
Interfaz	USB Host
Resolución de sensor	500 dpi
Precio	\$235.00

*Información obtenida de Tecnosmart*

- Huella T1200



*Fig. 14.- Huella T1200*

**Tabla 5.- Ficha técnica del Huella T1200**

Capacidad de huellas	100 huellas
Fuente de alimentación	batería de 9v
Desbloqueo de respaldo	Contraseña
Interfaz	Bluetooth 2.0
Resolución de sensor	500 dpi
Precio	\$321.00

*Información obtenida de Ferromadera*

#### **2.2.1.8 Relación de la biometría y la seguridad.**

Los sistemas biométricos se correlacionan con la seguridad, porque su principal característica es brindar protección a nuestros bienes e información. Se utiliza determinada parte de nuestro cuerpo como una capa extra de seguridad al uso de equipos en nuestra vida cotidiana

#### **2.2.1.9 Seguridad**

Puede definirse de manera general como salvaguardar las propiedades e integridad física de una o varias personas. Conjunto de sistemas y acciones dispuestas a eliminar, reducir, controlar la información, riesgos, vulnerabilidad y amenazas

#### **2.2.1.9.1 Tipos de Seguridad.**

Existe varios tipos de seguridad como: bioseguridad, seguridad ciudadana, seguridad humana, seguridad informática, seguridad jurídica, seguridad laboral, seguridad social, seguridad vial, seguridad bancaria, seguridad privada, seguridad de la información.

En este proyecto se centrará en el estudio de los siguientes tipos de seguridad:

##### **Seguridad Ciudadana**

Se la define como el proceso de establecer estrategias exhaustivas para fortalecer y proteger el orden civil, eliminando posibles amenazas de violencia logrando así mejorar la calidad de vida de la población de forma segura y pacífica.

##### **Seguridad de la información**

Es un conjunto de medidas preventivas para asegurar la identificación y gestión de los activos de la información, existen tres fundamentos básicos:

- Confidencialidad: Proporciona acceso a los usuarios autorizados y denegar a los no autorizados
- Integridad: Garantiza que la información obtenida no sea manipulada.
- Disponibilidad: La facilidad de poder acceder a la información o utilizar el servicio siempre que se lo requiera.

#### **2.2.1.9.2 Seguridad de acceso físico**

Dispositivos de medidas de seguridad que evitan el acceso a personas no autorizadas en cualquier establecimiento, por eso se requiere capacidad de identificación para esto existe varios métodos que manejan el control de acceso:

- Guardias de seguridad
- Detectores de Metales
- Protección Electrónica
- Sistemas Biométricos

#### **2.2.1.10 Cerradura**

Mecanismo metálico que se fija en puertas, cajas, cofres, armarios con la función de impedir la apertura, a menos que tenga la llave correspondiente para abrir o cerrar los pestillos.

### 2.2.1.10.1 Tipos de cerradura

En el mercado actual existen muchos tipos de cerraduras tales como: las mecánicas convencionales y las electrónicas-mecánicas, estas se clasifican dependiendo de su uso como: la entrada principal o dormitorios.



*Fig. 15.- Cerradura sobrepuesta de barra fija, FANAL. Fuente:*  
<http://www.homedepot.com.mx/comprar/es/centro/cerradura-sobreponer-barra-fija-izq>.



*Fig. 16.- Cerradura sobrepuesta, PHILIPS. Fuente:*  
<http://www.homedepot.com.mx/comprar/es/centro/cerradura-de-sobreponer-izquierda>



*Fig. 17.- Chapa eléctrica, LLOYDS. Fuente:*  
<http://www.homedepot.com.mx/comprar/es/centro/chapaelectrica-p-video-interfon>.



*Fig. 18.- Cerradura inteligente Touch-to-open, Kwikset. Fuente:*  
*<http://www.homedepot.com.mx/comprar/es/centro/cerrojosmart-code-niquel-satin>.*



*Fig. 19.- Cerrojo Smart Code, Kwikset. Fuente:*  
*<http://www.homedepot.com.mx/comprar/es/centro/cerrojosmart-key-bluetooth-ns>.*



*Fig. 20.- Cerradura Smart Door Lock, SAMSUNG. Fuente:*  
*<http://www.samsungdigitallife.com/SHS5050.php>.*

## 2.3 Marco Tecnológico

### 2.3.1 Arduino

Es una placa electrónica con bases de hardware abierto para los desarrolladores, permite crear diferentes tipos de aplicaciones electrónicas con el microcontrolador mediante un conjunto de instrucciones enviadas a la placa [11].

De software libre con patente de Arduino llamada IDE (Entorno de desarrollo integrado), es ejecutable en ordenadores de Mac, Windows y Linux, este dispositivo se ha vuelto muy popular como método de comienzo para el aprendizaje en el mundo de la electrónica.

**Tabla 6-** *Especificaciones Técnicas De Tipos de Arduino*

<b>Modelo</b>	<b>Pro-Mini</b>	<b>Nano</b>	<b>Uno</b>	<b>Mega</b>	<b>Leonardo</b>	<b>Micro</b>
<b>Desmontable</b>	No	No	Si	No	No	No
<b>Conexión</b>	Serial / Módulo USB Externo	Micro USB	USB B	USB B	Micro USB	MicroUSB
<b>Voltaje de Operación</b>	3.3 V o 5VDC	5VDC	5VDC	5VDC	5VDC	3.3 V o 5 VDC
<b>Corriente máxima</b>	40mA	40mA	40mA	40mA	40mA	40Ma
<b>Pines Digitales</b>	14	14	14	54	20	12
<b>Pines Analógicos</b>	6	8	6	16	12	4
<b>Pines PWM</b>	6	6	6	15	7	5
<b>Memoria Ram</b>	2 KB	2 KB	2 KB	8 KB	2.5 KB	2.5 KB
<b>Memoria EEPROM</b>	0.512 KB	0.512 KB A 1 KB	1 KB	4 KB	1 KB	1 KB

<b>Memoria</b>	16 o 32	16 o 32	32 KB	256 KB	32 KB	2 KB
<b>Flash</b>	KB	KB				
	3.35 V –					
<b>Voltaje de</b>	12 VDC	7 – 12	7 – 12	7 – 12 VDC	7 – 12 VDC	3.35 – 12
<b>Alimentación</b>	5- 12VDC	VDC	VDC			VDC 5 – 12VDC

**Imagen  
Referencial**



*Información adaptada de CreateArduino. Elaborado por el autor.*

### 2.3.2 Micro SD card adapter

Este módulo de tarjeta utiliza comunicación SPI (Interfaz Periférica Serial) que tiene una ranura para la incorporación de la tarjeta microSD en donde se guardará los datos almacenados como imágenes, videos, archivos y codificación.

Soporta tarjetas micro SD y micro SDHC posee un circuito integrado de conversión de voltaje para comunicación de 3.3 V o 5 V, con interfaz SPI.



*Fig. 21.- Módulo Micro SD*

### 2.3.3 Módulo bluetooth HC-05



Este módulo nos permite la conexión entre el arduino con un Smartphone, celular o pc de forma inalámbrica, es de comunicación bluetooth 2.0 compatible con cualquier celular Android.

Es un módulo maestro-esclavo, lo que quiere decir que puede recibir y enviar datos en serie cuando los datos son enviados en serie desde un dispositivo que tenga un bluetooth



maestro (Smartphones, PC), es importante tener una aplicación en el celular para enviar entradas al módulo para luego transferirla al Arduino.

**Tabla 7.- Comparación de los módulos de Bluetooth**

Características	HC-05	HC-06
<b>Tamaño</b>	27mm X 13 mm X 2mm	27mm X 12.5 mm X 2.4mm
<b>Tipo de Programación</b>	Comando AT + SPP	Comando AT + SPP
<b>Sensibilidad</b>	-80 dBm	-80 dBm
<b>Voltaje de operación</b>	3.1 – 4.2 V	1.8 – 3.6 V
<b>Consumo de corriente</b>	8 mA	8.5 mA
<b>Versión bluetooth</b>	2.0	2.0
<b>Roles</b>	Master - Slave	Slave
<b>Imagen Referencial</b>		

*Información obtenida de la investigación directa. Elaborado por el autor.*

### 2.3.4 Módulo RTC DS3231 Real time clock

Es un oscilador de cristal alimentada con una pila pequeña de 3v de alimentación para no perder la sincronización en caso de corte de energía en el circuito, donde su función es la de una señal de reloj ejecutando segundos, minutos, horas, días, meses y año incluyendo las correcciones para año bisiesto con un formato de 24 horas o 12 horas con su indicador AM/PM.

Se debe de tener instalada la librería DS3231 que tiene como funcionalidad para la lectura de reloj, configuración de reloj y alarmas para el reloj en tiempo real de alta precisión.



*Fig. 22.- Módulo RTC DS3231 Real time clock*

### 2.3.5 Módulo lector de huella Finger print R307

Sensor de detección y verificación de huellas dactilares, capaz de almacenar hasta 120 huellas en la memoria micro SD, por este motivo se debe guardarla en una base de datos para su posterior escaneo de lectura y comparación de las huellas del usuario.

Se debe tener instalado la librería de Adafruit, una vez instalada abrimos el ejemplo “enroll” que viene establecido por defecto en la librería que se instaló, este ejemplo sirve para escanear y guardar las huellas dactilares que queramos para más adelante reconocerlas.

La velocidad de transmisión es 9600 baudios, el error común que se encuentra en el sensor de no reconocerlo, es debido a la definición de los pines Tx y Rx del sensor al arduino, es por eso que se debe definir con anterioridad los puertos seriales. Si el arduino a utilizar no tiene puertos seriales deberá definir los pines como softwareSerial para permitir la comunicación serie sobre los demás pines digitales.

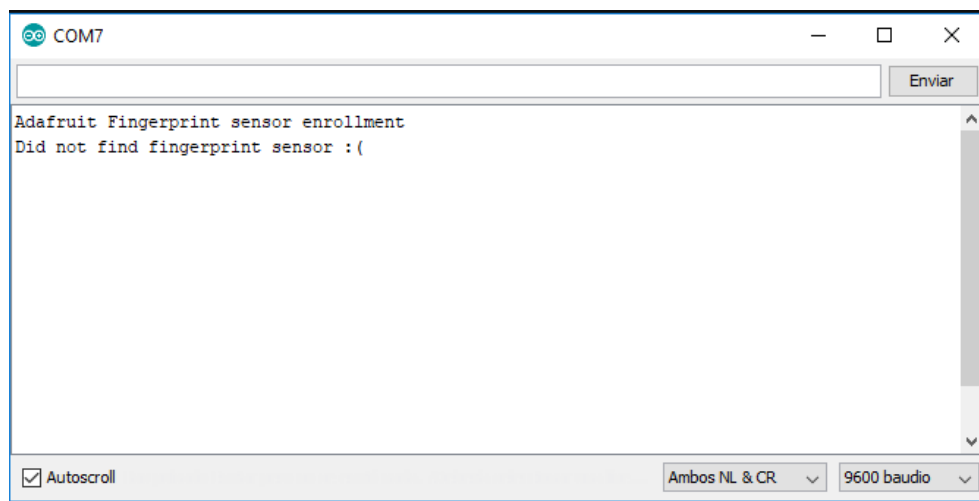


Fig 23.- Error habitual del sensor mostrado en Monitor Serie (Arduino IDE). Elaborado por el autor



Fig. 24.- Módulo lector de huella Finger print R307

### 2.3.6 LCD 16×2 por I2C

Es un display que presenta 2 línea de 16 caracteres de 8 x 5 pixeles cada uno, en su interior dispone una luz trasera (backlight) que permite usar aun sin luz, en la parte de atrás se divisa una plaquetita adicional conectada a los 16 pines del lcd, esta interface se llama I2C que es un protocolo que trabaja de forma sincronizada por una señal de reloj



*Fig 25. Pantalla LCD 16x2 con el protocolo I2C.*

### 2.3.7 Servomotor

Es un dispositivo de movimiento mecánico (giros por ejes) que operan generalmente entre rangos de 180° pero puede ser modificado hasta los 360°, en pulsos digitales que controla movimientos de velocidad y precisión.

Funciona con alimentación de (4.8 a 6 V) con una secuencia de pulsos a frecuencia de 50 Hz donde cada ciclo dura 20 ms



*Fig. 26.- Servomotor.*

### 2.3.8 Resistencia

Es un componente que ofrece oposición al paso de la corriente eléctrica, su función es de reducir la intensidad o las caídas de tensión, esto quiere decir limitar la corriente para que no supere la cantidad que necesita el circuito



*Fig. 27.- Resistencias*

### 2.3.9 Pulsadores

Son interruptores con solo dos posiciones de abrir o cerrar el circuito en forma permanente, cuando se lo acciona se logra que varíe la posición logrando así abrir el circuito que estaba cerrado o cerrando el circuito que estaba abierto, que permanece así hasta que se vuelva a accionar.



*Fig. 28.- Pulsadores*

### 2.3.10 App Inventor 2

Entorno web de desarrollo para dispositivos con sistema operativo móvil Android, fácil de usar, donde se construirá la interfaz del usuario con la herramienta App Inventor Designer y la función de los componentes con App Inventor Blocks Editor. Capaz de generar el instalador de archivo de extensión apk o un generador de código QR.

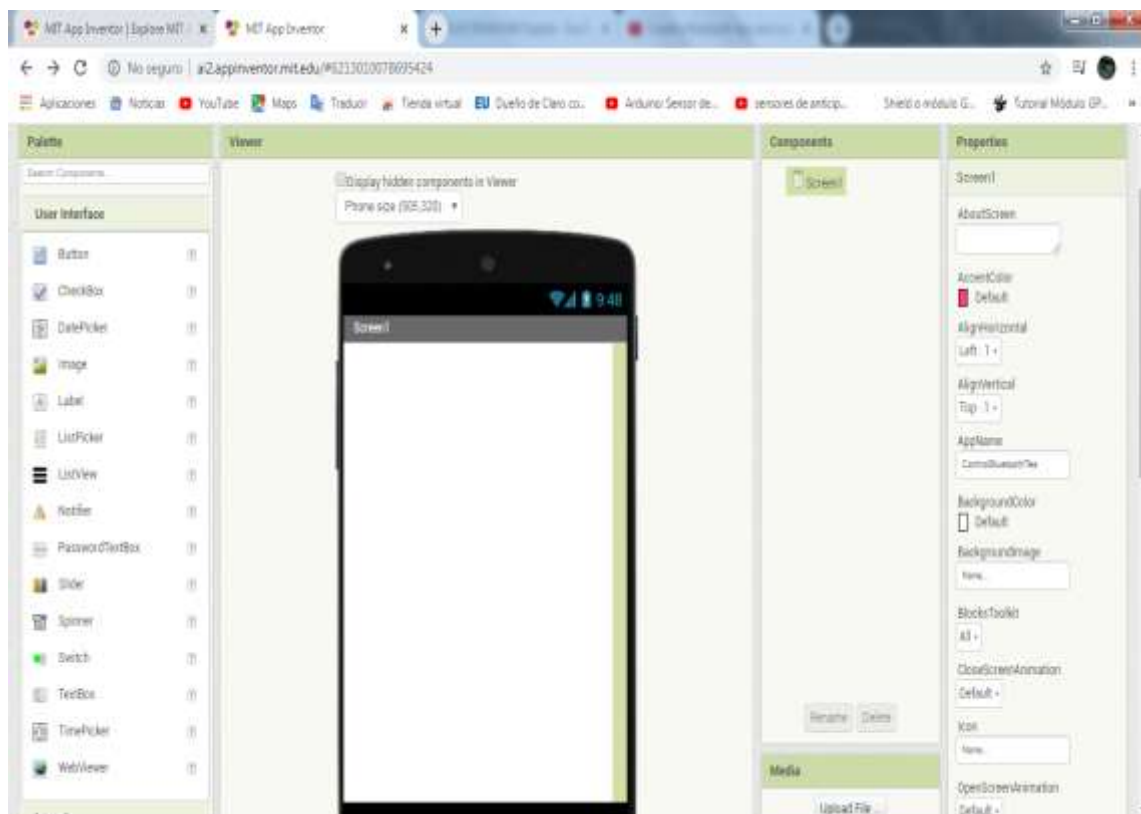


Fig. 29.- App Inventor

## 2.4 Marco Legal

### 2.4.1 Marco legal en el Ecuador.

El presente proyecto está enfocado en el Registro Oficial No 320 Ley de Propiedad Intelectual que indica como responsable al escritor de crear el documento como propietario de los derechos del autor.

En la Constitución de la República del Ecuador en su art. 350 menciona que el sistema de enseñanza empleado por la Educación Superior tiene como objetivo el formar académicamente y profesionalmente con la visión científica y humanista a los alumnos, dicha investigación científica y tecnológica deberá promover la innovación, desarrollo y

difusión de los saberes para la construcción de soluciones en beneficio al país en relación con los objetivos del régimen de desarrollo.

#### **2.4.2 Marco legal en el exterior.**

Debido a que en el Ecuador no existe todavía una ley establecida sobre los datos de los sistemas biométricos, es por eso que se opta por seguir la ley general del Reglamento Europeo de Protección de Datos (GDPR) dictaminada por en el órgano internacional del reglamento 2016/679 detallado en el siguiente artículo:

Artículo 9 Tratamiento de categorías especiales de datos personales establece mecanismos de prohibición sobre el tratamiento de los datos personales con la intención de revelar origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, y el tratamiento de datos genéticos, además si son dirigidos para identificar a inequívocamente de su orientación sexual o vida sexual de la persona.

## **Capítulo III**

### **Metodología**

#### **3.1 Diseño de la investigación**

En el presente trabajo será de analizar el sistema biométrico con cerradura de huella dactilar y comunicación bluetooth, es por eso que se ha recurrido a un diseño no experimental que se aplicará de forma transversal. Puesto que el tema a tratar es considerado como una investigación de tipo descriptivo, explorativo y sustento teórico suficiente, con el fin de dar a conocer una solución viable tecnológica al problema como es la inseguridad en los domicilios.

El diseño de la investigación se utiliza para analizar y recopilar las variables especificadas en el problema de investigación mediante un conjunto de métodos y procedimientos. (Montano,2018)

#### **3.2 Enfoque de la investigación.**

Se emplea gran variedad de materiales para recoger información, observaciones, historias de vida y las problemáticas que aborda el tema, además del significado que tiene en los encuestados. Es por eso que el enfoque mixto constituye en la unión de los métodos cualitativos y cuantitativos con el fin de tener una idea clara del fenómeno que se está estudiando, estos métodos son conjuntados de tal manera que conservan la estructura y procedimientos originales.

El enfoque mixto es la vinculación de los datos cuantitativos y cualitativos que procesa, recolecta y analiza un mismo estudio de investigaciones para solucionar una problemática. (Ruiz,2017).

#### **3.3 Método de la investigación.**

##### **3.3.1 Método bibliográfico**

Recopilación de documentos que constituyen sobre el conocimiento de investigaciones existentes del tema, la información que se utilizó para la búsqueda de temas relevantes de tecnologías biométricas, así como una comunicación accesible como lo es el bluetooth.

### 3.3.2 Método explorativo

Al ser un tema poco explorado como es la seguridad biométrica domiciliaria en el país por parte de la ciudadanía, se hicieron uso de métodos en diferentes sitios del internet, artículos y poster científicos para poder referirse al caso estudiado en la comunidad establecida del suburbio oeste.

Problema concreto de estudio que propone una visión general mediante investigaciones. (Martínez de Sanchez,2013).

### 3.3.3 Método descriptivo

En este método se logró identificar cual es el grado de la delincuencia domiciliaria en el sector del suburbio oeste, con qué frecuencia sufren los usuarios además de las perspectivas que tienen sobre el problema y una solución óptima de bajo costo.

Con la finalidad de la recopilación de los datos se llega a dar una idea clara de la problemática. (Yanez, 2018).

## 3.4 Población y muestra

Para esta investigación se tomó como población a las personas adultas encargadas de cada vivienda en el sector señalado con anterioridad, debido que viven aproximadamente 105 familias, dos por cada vivienda. Datos obtenidos previamente antes de realizar la encuesta mediante censo de las viviendas por cada cuadra del sector del suburbio oeste.

**Tabla 8.- Población del sector**

Sector por cuadras	Población
Cuadra C	20
Cuadra D	25
Cuadra E	28
Cuadra F	32
Total	105

*Información tomada desde la investigación de campo. Elaborado por el autor*

Se realizó una muestra estratificada donde se procedió a dividir la población debido al interés como es la vivienda, obviando los locales que estaban en las cuadras, además teniendo las siguientes consideraciones: 95% de nivel de confianza y su indicador de límite



de error de 5%, todo esto para garantizar que la muestra sea fiable, se utilizó los siguientes datos para calcular la muestra

n= Tamaño de la muestra

N= Población o universo

z= Nivel de confianza

p= Probabilidad a favor

q= Probabilidad en contra.

e= Error muestral

$$n = \frac{z^2 * p * q * N}{e^2(N - 1) + z^2 * p * q}$$

$$n = \frac{95^2 * 0.5 * 0.5 * 105}{5^2(105 - 1) + 95^2 * 0.5 * 0.5}$$

**n= 49 personas**

$$\text{coef} = \frac{49}{105} = 0.466$$

$$20 \times 0.466 = 9.32$$

$$25 \times 0.466 = 11.65$$

$$28 \times 0.466 = 13.04$$

$$32 \times 0.466 = 14.91$$

**Tabla 9 .- Muestra total por encuestar**

<b>Sector por cuadra</b>	<b>Población a encuestar</b>
Cuadra C	9
Cuadra D	12
Cuadra E	13
Cuadra F	15
Total encuestados	49

*Información obtenida mediante la fórmula de la muestra estratificada. Elaborado por el autor*

### **3.5 Técnicas e instrumentos**

Diversas formas en que la investigación puede llevarse a cabo con el fin de obtener información de una determinada muestra seleccionada para facilitar la búsqueda de soluciones a los problemas que se está estudiando, es de mucha importancia estas herramientas debido que se pueden obtener datos relevantes y necesarios para el desarrollo de la investigación.

### **3.6 Encuestas**

Este método fue seleccionado porque nos permitirá hacer un análisis gráfico de los datos que se obtienen, mediante la formulación de 8 preguntas en formato encuesta para los habitantes del sector Suburbio Oeste.

Este método de investigación mediante la encuesta está considerado como una recopilación de datos con el fin de obtener información relevante de la problemática, esto puede ser llevado a cabo dependiendo de qué metodología haya usado el investigador junto con los objetivos que desea alcanzar. (Question Pro, 2016)

### **3.7 Análisis de los resultados de la encuesta**

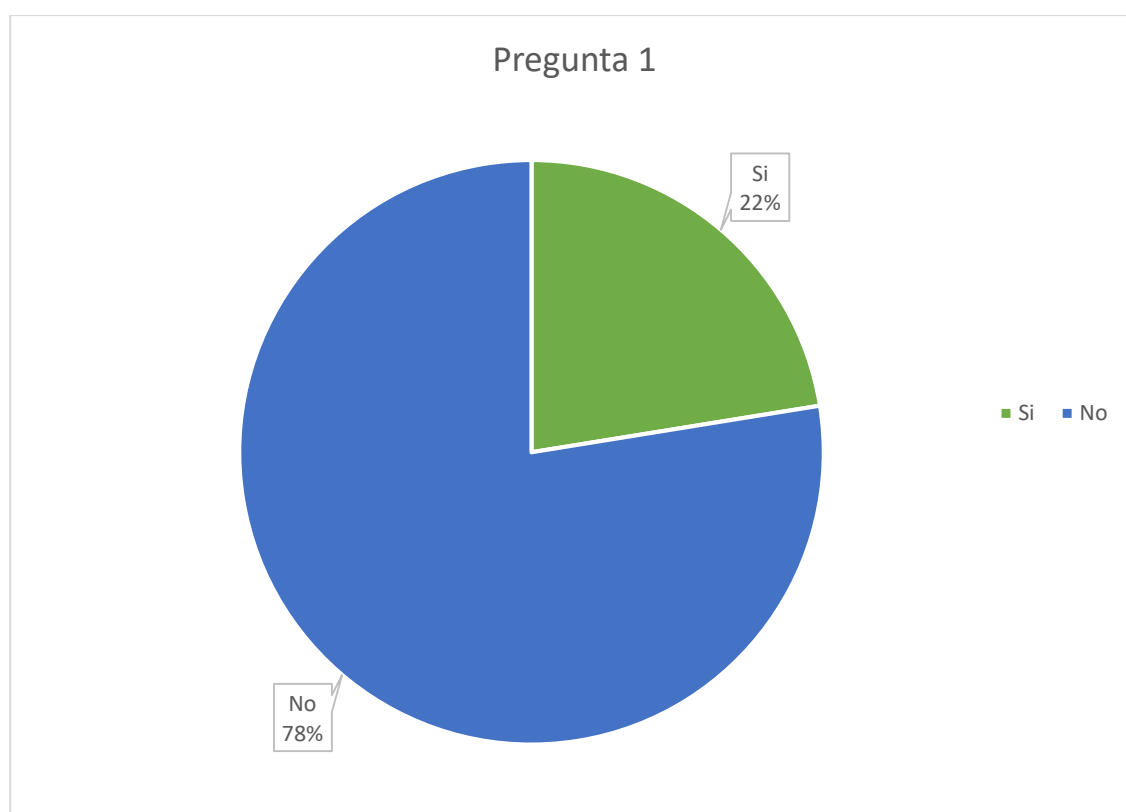
Se detallará el respectivo análisis de cada pregunta de la encuesta en el sector del suburbio oeste de la ciudad de Guayaquil para conocer el nivel de aceptación del prototipo de la cerradura biométrica de huella dactilar con comunicación bluetooth.

**1) ¿Su domicilio cuenta con algún sistema electrónico o tecnológico para prevenir robos?**

**Tabla 10 .-** *Porcentaje si cuentan con algún sistema tecnológico en su domicilio*

Respuestas	Frecuencia	%
Si	11	22%
No	38	78%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



*Fig 30.- Porcentaje si cuentan con algún sistema tecnológico en su domicilio. Elaborado por el autor*

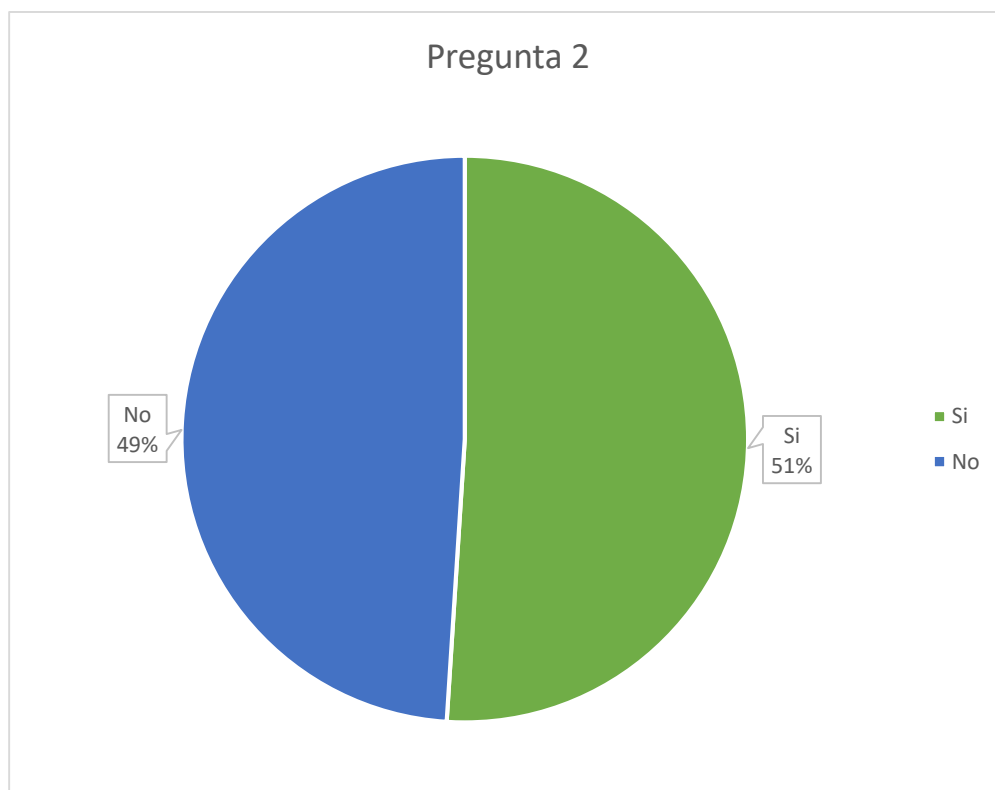
El 22% que corresponde a 11 encuestados mencionan que, si poseen un sistema tecnológico para prevenir robos, tal como el sistema de video vigilancia, mientras que el resto 78% de 38 encuestados no dispone de ningún sistema por el costo de adquisición.

**2) ¿Ha escuchado que exista un sistema de seguridad que utiliza la huella dactilar con el propósito de identificar solo a los residentes del domicilio?**

**Tabla 11 .- Porcentaje si han escuchado de un sistema biométrico**

Respuestas	Frecuencia	%
Si	25	51%
No	24	49%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



*Fig. 31.- Porcentaje si han escuchado de un sistema biométrico. Elaborado por el autor*

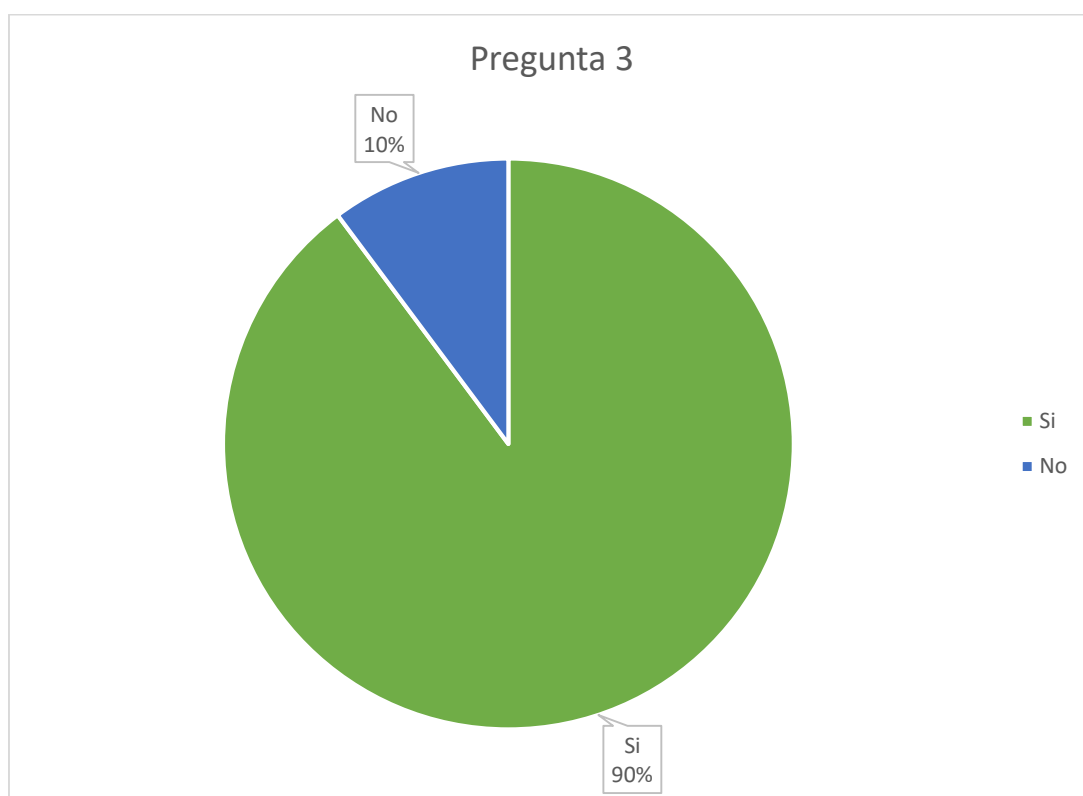
Con la mayoría del 51%, las personas del sector conocen lo que es un sistema biométrico debido a que trabajan en compañías que dispone de esta tecnología como es el registro de entrada mediante la huella dactilar, pero el 49% no conocen porque se dedican al comercio ambulante en el sector.

**3) ¿Estaría dispuesto a tener un sistema de seguridad para saber quiénes apertura la puerta de ingreso en su domicilio?**

**Tabla 12 .-** *Porcentaje para conocer si están dispuesto a tener el sistema*

Respuestas	Frecuencia	%
Si	44	90%
No	5	10%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



*Fig. 32.- Porcentaje para conocer si están dispuesto a tener el sistema. Elaborado por el autor*

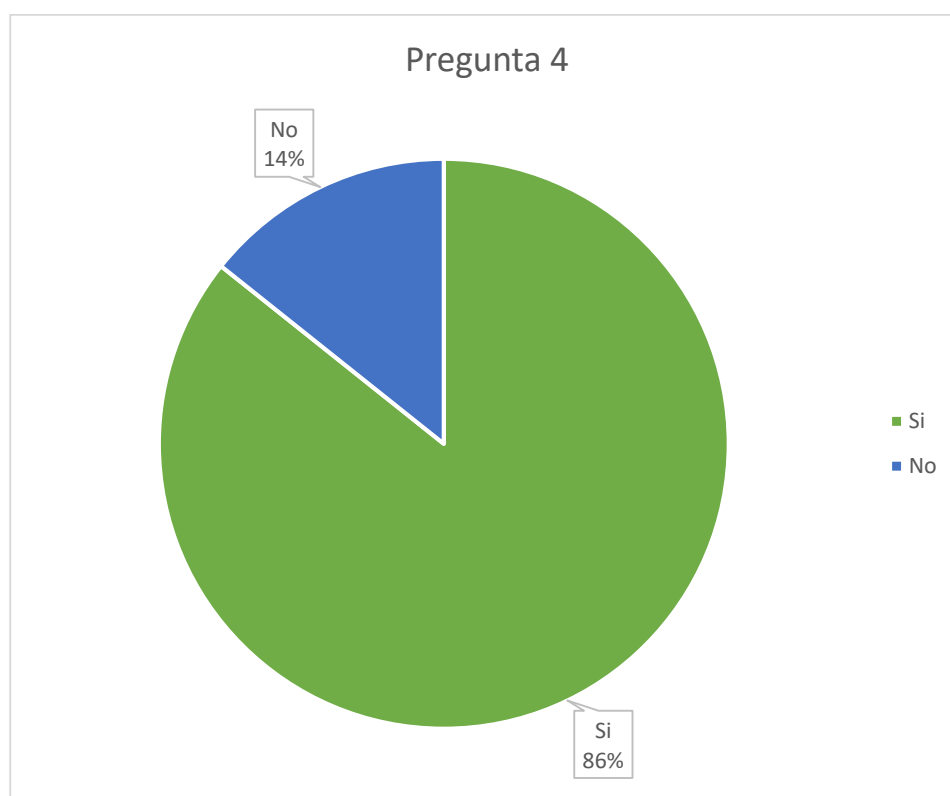
La mayoría de las personas encuestadas están de acuerdo en obtener el sistema de la cerradura de huella dactilar pues aseguran que sabrán quien entra en su domicilio, mientras que 5 encuestados están conforme con el sistema de video vigilancia adquirido.

**4) ¿Le gustaría que el sistema guarde un registro de las personas que acceden a su domicilio las 24/7?**

**Tabla 13 .-** *Porcentaje si les gustaria tener un registro en su cerradura*

Respuestas	Frecuencia	%
Si	42	86%
No	7	14%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



*Fig 33.- Porcentaje si les gustaría tener un registro en su cerradura. Elaborado por el autor*

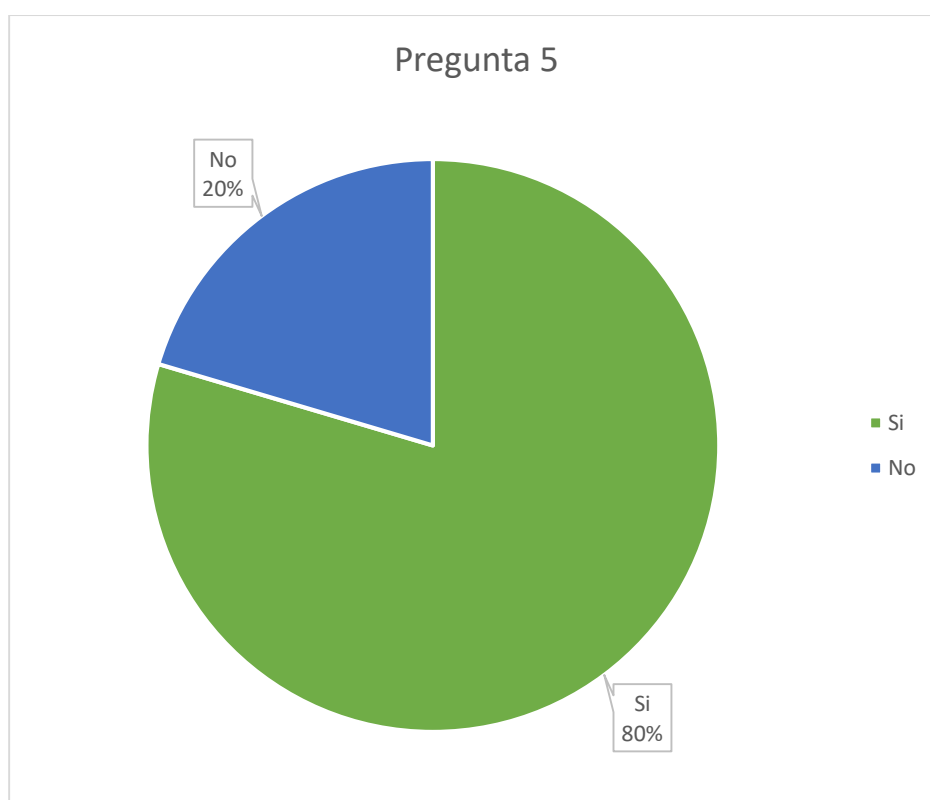
Gran porcentaje quiere que el sistema guarde un registro de entrada para tener un control de entrada de los habitantes del domicilio, pero 7 encuestados opinan que no porque sienten que vulneran su privacidad.

**5) ¿Le gustaría contar con un sistema de seguridad como es la cerradura biométrica con huella dactilar de comunicación bluetooth?**

**Tabla 14 .-** *Porcentaje si les gustaría contar con el sistema*

Respuestas	Frecuencia	%
Si	39	80%
No	10	20%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



*Fig 34.- Porcentaje si les gustaría contar con el sistema Elaborado por el autor*

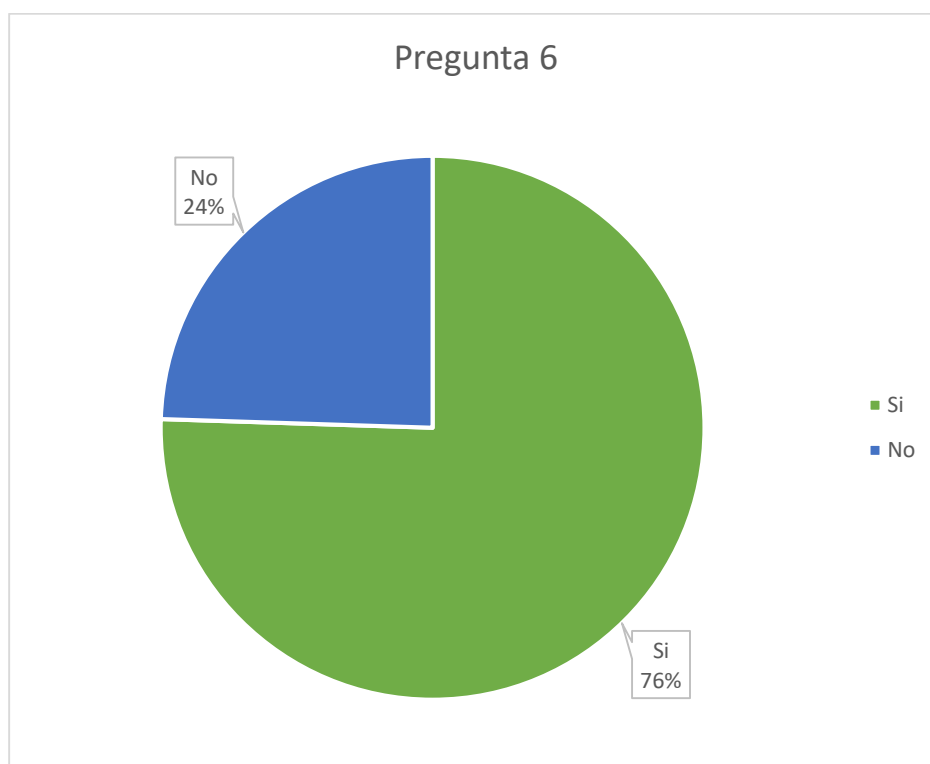
La mayoría si le gusta la idea de tener el sistema en su domicilio porque lo ven innovador y seguro, pero 10 encuestado no desean el producto debido a que se sienten conforme con el sistema de video vigilancia que disponen.

**6) ¿Cómo adicional a la cerradura de huella dactilar utilizaría su celular con una aplicación instalada para la apertura de la cerradura en su domicilio?**

**Tabla 15 .-** Porcentaje sobre la utilización de su celular en la cerradura

Respuestas	Frecuencia	%
Si	37	76%
No	12	24%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



*Fig. 35.-Porcentaje sobre la utilización de su celular en la cerradura. Elaborado por el autor*

Los 37 encuestados estarían dispuestos a utilizar su celular como una alternativa a la huella dactilar y los 12 encuestados opinan que no, debido a que pueden sufrir robos de sus celulares y así el ladrón se les puede ingresar a la vivienda.

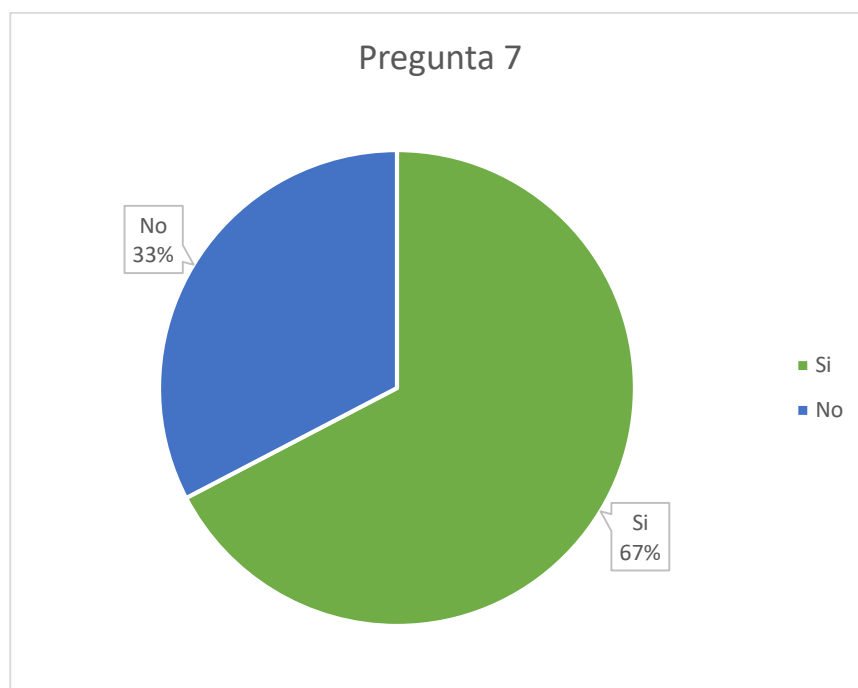


**7) ¿Estaría dispuesto adquirir el sistema de la cerradura de huella dactilar con comunicación bluetooth a un precio de \$60?**

**Tabla 16 .-** *Porcentaje sobre la aceptación del costo de la cerradura biometrica*

Respuestas	Frecuencia	%
Si	33	67%
No	16	33%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



**Fig. 36.-** *Porcentaje sobre la aceptación del costo de la cerradura biométrica. Elaborado por el autor*

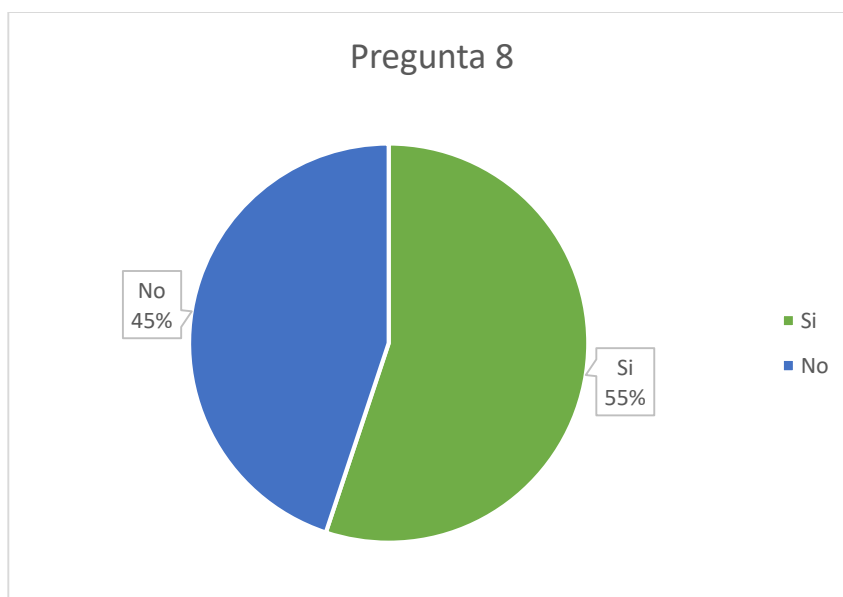
La mayoría de encuestados les parece barato el sistema en comparación con otras tecnologías de seguridad pues están de acuerdo que pueden obtener el sistema, pero 16 encuestados opinan que no, porque no disponen del dinero para adquirir el sistema.

**8) ¿Estaría dispuesto adquirir el sistema de la cerradura de huella dactilar con comunicación bluetooth además de tener un registro de apertura de la vivienda a un precio de \$90?**

**Tabla 17 .-Porcentaje de aceptación del costo de la cerradura con registro**

Respuestas	Frecuencia	%
Si	27	55%
No	22	45%
Total	49	100%

*Información tomada de la encuesta. Elaborado por el autor*



*Fig. 37.- Porcentaje sobre la aceptación del costo de la cerradura biométrica con registro. Elaborado por el autor*

Añadiéndole la función del registro de apertura del domicilio no les pareció conveniente porque se elevó el precio estipulado por los encuestados, es por eso que prefieren el sistema sencillo de la huella dactilar con comunicación bluetooth, pero 27 encuestados si desean adquirir el sistema con la función adicional.

### **3.8 Resultado general**

Los resultados de la encuesta fueron concluyentes, debido a que la mayoría conoce lo que es un sistema biométrico y como puede beneficiarlos en sus domicilios debido a sus trabajos en oficinas donde es común divisar este sistema, mientras que el otro porcentaje no conocía debido a su labor, que es el comercio ambulante en el sector, a todos los encuestados se les dio una breve introducción de la función del sistema de cerradura de la huella dactilar con comunicación bluetooth antes de que vayan desarrollando la encuesta en mención para que conozcan los beneficios que les puede traer el sistema.

Todos los encuestados tenían un rango de edad de 35 a 57 años, ellos conocían el funcionamiento básico del bluetooth, desde como vincular un nuevo dispositivo hasta como el método de envío de datos porque lo utilizaban para pasarse canciones del momento, esto facilitó que tengan una idea general de como funcionaria la aplicación instalada en el dispositivo móvil, al mencionar este otro método de apertura de la cerradura, las personas se preocupan de la idea de que pasaba si su celular sea robado, esto generó temor sobre la aplicación a tal grado de no querer usarla pero se les dijo que en la mayoría de los celulares tienen la opción de bloquear las aplicaciones con una contraseña ya sea mediante patrón o huella dactilar y solo utilizarlas por las contraseñas que el usuario eligió.

## **Capítulo IV**

### **Desarrollo de la propuesta**

#### **4.1 Introducción**

En el Ecuador está viviendo el auge de la delincuencia, los ciudadanos viven en zozobra porque el estado no les brinda la seguridad que necesitan, es por eso que mucho de ellos se ven obligados a tomar medidas adicionales, pero en su mayoría no lo hacen porque un sistema de seguridad es un costo elevado de adquisición, es por eso que se desarrolla este prototipo de cerradura huella dactilar con comunicación bluetooth a un precio accesible para la población.

#### **4.2 Desarrollo**

La elaboración del prototipo de la cerradura de huella dactilar con comunicación bluetooth estará dividido por etapas, de las cuales son las secuencias que siguió el autor de este documento.

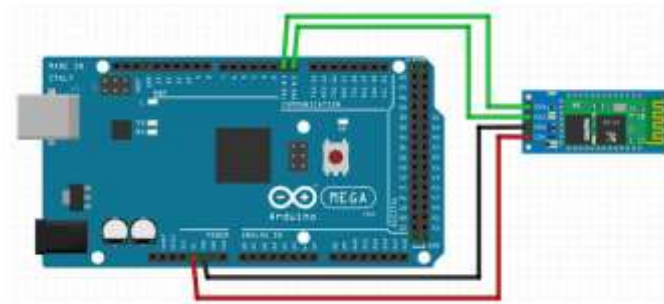
##### **4.2.1 Etapa 1**

###### **4.2.1.1 Diseño de circuitos.**

En esta etapa se procedió a conectar cada uno de los elementos establecidos en el arduino, verificando las conexiones de entrada en la placa Mega, se utilizó este componente debido que posee una gran cantidad de memoria para almacenar la programación de los diferentes módulos que se utilizará además de la gran cantidad que posee de pines digital que los demás, es por eso que se debe conocer las funciones de cada placa de arduino que se vaya a utilizar en futuros proyectos, el primer elemento en instalar fue el módulo de bluetooth HC-06.

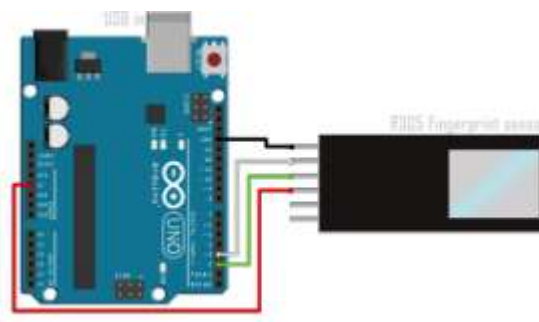
El módulo de Bluetooth cuenta con pines de protocolo Rx y Tx, al igual que el arduino, la conexión será del Rx(HC-06) al Tx(Mega) y Tx(HC-06) al Rx(Mega), esto quiere decir (Rx-pin0) y (Tx-pin1) porque los datos que está enviando el módulo de bluetooth debe de estar receptando la placa de arduino para que exista una fluidez en la comunicación por ese motivo se coloca los Rx con los Tx y viceversa, además en este prototipo la función será de ser esclavo bajo las órdenes del celular, por este motivo es el primer dispositivo que necesita la instalación de la codificación en el módulo, una vez subida la programación en el módulo, se procede a desconectar solamente el cable de la fuente de alimentación del módulo de

bluetooth para que no exista errores por parte del Hc-06 al subir los demás códigos. La siguiente parte del diseño nos sirve para poder hacer la comunicación de la cerradura con el bluetooth, debido a que el HC-06 trabaja como esclavo, por lo tanto, recibe la señal o búsqueda que hace nuestro dispositivo móvil para acoplarlo mediante una contraseña como es: 1234, luego reconocer el bluetooth del celular con la comunicación de la aplicación móvil



*Fig. 38.- Conexión del módulo bluetooth HC-05 en el arduino Mega*

El siguiente será el lector de huella Finger print R307, solo se conectarán a la placa los pines de alimentación y los Tx-Rx, como se está trabajando en el arduino Mega, este posee 4 puertos seriales a diferencia con las demás, por eso el Tx del lector va al Rx del arduino esto quiere decir (Tx-pin10) y (Rx-pin11). Luego de subirle el código se deberá añadir la huella por defecto de la librería Adafruit con el ejemplo Enroll, este ejemplo permitirá añadir una huella principal, el cual es la referencia para poder ingresar las demás. Si se obvia este proceso el sensor no añadirá ninguna huella



*Fig 39.- Conexión del módulo fingerprint R307 en el arduino Mega*

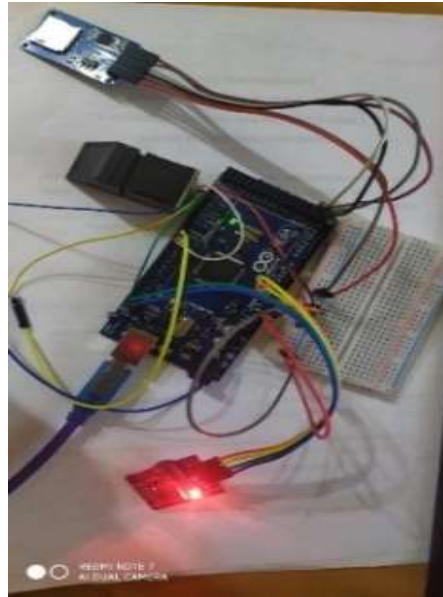


Fig 40.- Conexión en el prototipo del módulo fingerprint R307 en el arduino Mega

En la comparación de la huella dactilar se utiliza la técnica más antigua, pero de mayor utilización, aceptada a nivel global, la cual fue desarrollada por Galton y Purkinje dicho proceso distingue las diferentes huellas de los usuarios por sus patrones como: arco, arco entolado, espiral y bucle



Fig.41.- Los cuatro patrones principales. Elaborado por KEOGH, Eamonn. *The Science of Fingerprints*

En el proceso de escaneo se realiza la comparación de las minucias que están almacenadas utilizando un algoritmo estadístico, el cual consiste en calcular la distancia que existe entre cada una de ellas para luego transformarlas a una longitud-fija de 32byte

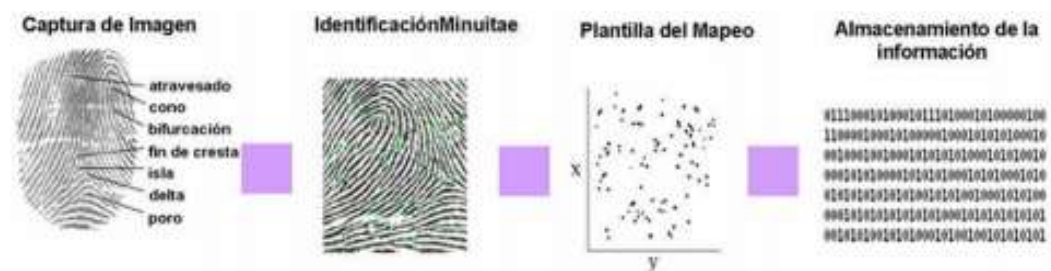


Fig. 42.- Proceso común de escaneo de la huella digital. Elaborado por Ian, *Biometric Technology dor DLID*

El RTC DS3231 funciona como una señal de reloj dando el tiempo real, esto se acoplará al módulo micro SD y a la huella dactilar para saber en qué momento ingresan al domicilio.

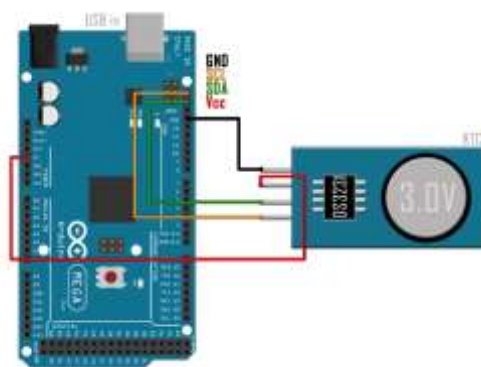


Fig 43.- Conexión del RTC DS3231 en el arduino Mega

Así como se hizo en el módulo R307, en el rtc se subirá el código al elemento estableciendo la fecha y hora actual manualmente, para más adelante volver a subir el mismo código, pero con la diferencia de que las líneas de comando que establecen la fecha será puesta como comentario añadiendo dos slash en la línea.

```

17 // The following lines can be uncommented to set the date and time
18 rtc.setDOW(FRIDAY); // Set Day-of-Week to SUNDAY
19 rtc.setTime(3, 9, 0); // Set the time to 12:00:00 (24hr format)
20 rtc.setDate(6, 3, 2020); // Set the date to January 1st, 2014
21 }

```

Fig. 44.- Codificación del módulo RTC 3231 en Arduino IDE

Se acopla al proyecto el módulo micro Sd card adapter que cumple la función de guardar los registros de entradas en la vivienda además de guardar las huellas dactilares, para mejor visibilidad y estética el prototipo contara con una pantalla led de 16x2 conectada junto a un protocolo síncrono como es el I2C.

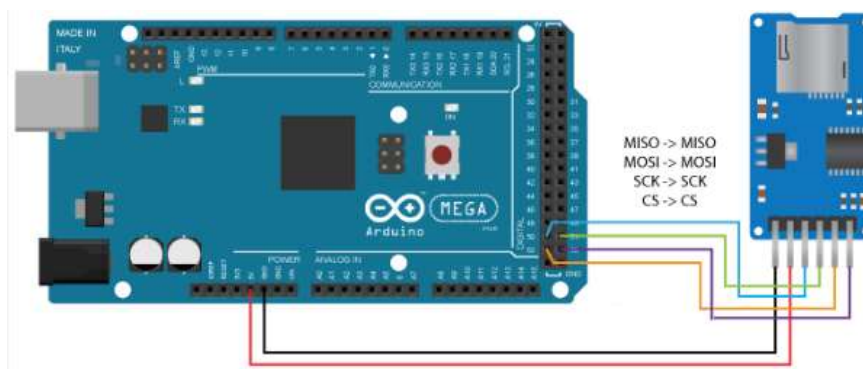


Fig. 45.- Conexión del módulo Adapter MicroSD en el arduino Mega



```

Door lock system started at 04:53:38 and day
13.03.2020

Door lock system started at 04:55:32 and day
13.03.2020

Door lock system started at 04:56:20 and day
13.03.2020

Door lock system started at 04:57:12 and day
13.03.2020

Door lock system started at 05:05:14 and day
13.03.2020

13.03.2020 - 05:05:41 Intento de abrir
13.03.2020 - 05:05:45 - Usuario guardado en el
ID# 16 confidencialidad : 53 - door open
Door lock system started at 05:06:01 and day
13.03.2020

13.03.2020 - 05:06:17 Intento de abrir
13.03.2020 - 05:06:20 - Usuario guardado en el
ID# 16 confidencialidad : 64 - door open
13.03.2020 - 05:06:26 - Añadir nuevo usuario.
Se requiere identificación!
13.03.2020 - 05:06:31 - El usuario no tiene
permiso para añadir mas usuarios
13.03.2020 - 05:06:34 - Añadir nuevo usuario.
Se requiere identificación!
13.03.2020 - 05:06:38 - Se añadido nuevo

```

*Fig 46.- Registro de ingreso en la cerradura. Elaborado por el autor*

Y por último la conexión de la cerradura con el servomotor, la cerradura de sobreponer es común en las residencias, se le hizo unos ajustes como quitar el resorte de la placa que ajustaba abrir el resbalón y poner seguro en la petaca, es por eso que se soldó con estaño la varilla que va sujeta al resbalón y petaca para cuando se presione el botón de escanear, se proceda a verificar la huella dactilar y así poder abrir la cerradura de forma paralela y aplastar el botón cerrar para poner el servomotor con la cerradura en su estado inicial.

El servomotor tendrá un pulso de cuando en el sistema se lea la huella dactilar o se utilice la aplicación del celular esto hará que jale la petaca y el resbalón a 90 grados logrando la apertura de la cerradura, luego de 7 segundos el servomotor tendrá un pulso donde el engranaje este en su posición inicial, con esto se cierra la cerradura.

El servomotor a utilizar es el MG995 con un ángulo de rotación hasta 120 grados, 60 grados por cada dirección con un voltaje de alimentación de 4.5 a 7 voltios, el torque soporta 8.5 kg·cm (4.8 V), 10 kg·cm (6 V) dependiendo de su voltaje de alimentación, con una duración de aproximadamente 3 a 5 años, inmune a daños como: humedad, sobrecalentamiento, vibración debido a la localización del servomotor.





### 4.2.3 Etapa 3

#### 4.2.3.1 Creación de la aplicación móvil.

Para una mejor comunicación entre estos módulos se creó una aplicación para los celulares, trabajado mediante un software libre llamado App Inventor, dicha aplicación contara con botones del cual sus funcionamientos serán el de:

- Conectar la aplicación del celular al prototipo por bluetooth, si la conexión es exitosa se mostrará un mensaje que dirá Estado: Conectado. Si dicha conexión no se realiza con éxito mostrara otro mensaje Falla de conexión.  
Desconectar: El funcionamiento es de cortar la conexión bluetooth del celular y el dispositivo.
- Abrir: Con la comunicación del bluetooth este botón nos da la opción de abrir la cerradura a una distancia aproximada de 5 metros. Se cerrará la cerradura automáticamente después de 7 segundo.
- Salir

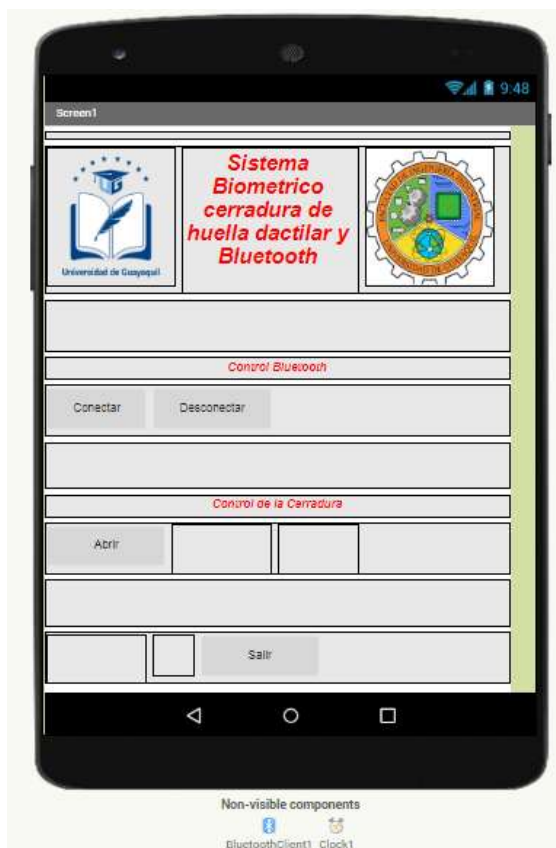


Fig 49.- Esquema de la aplicación en App Inventor. Elaborado por el autor

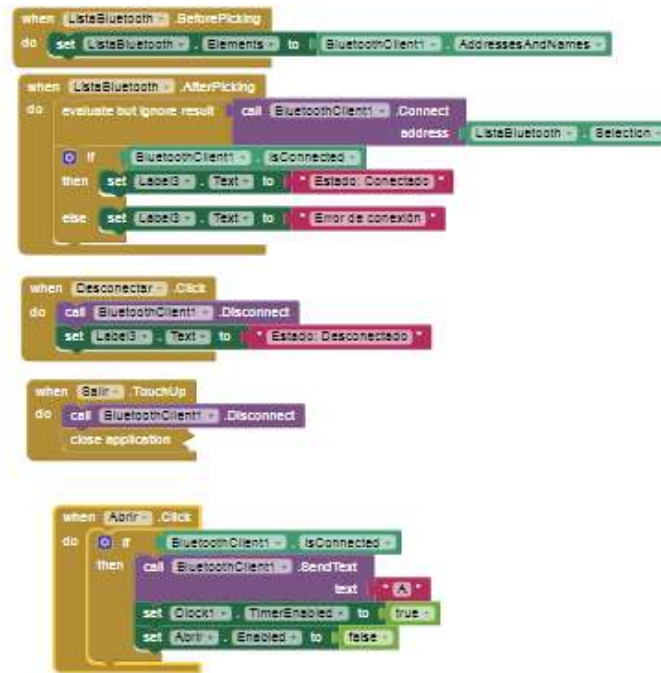


Fig.50 Diagrama de bloque de la aplicación App inventor. Elaborado por el autor

### 4.3 Diseño General del sistema.

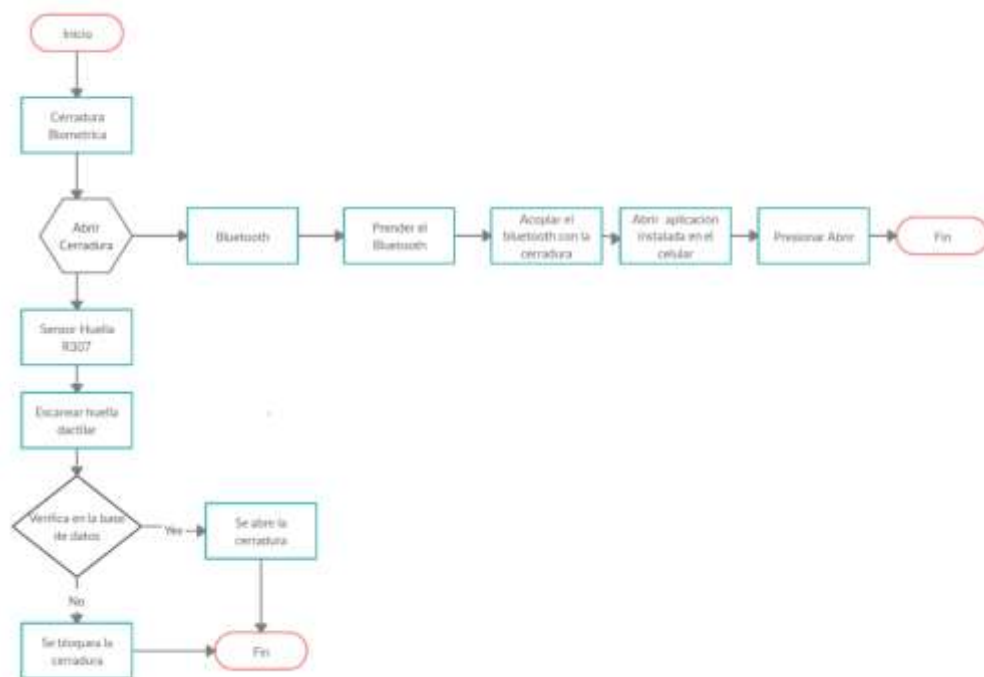


Fig 51.- Diagrama de Flujo del funcionamiento general del prototipo. Elaborado por el autor

Se observa el diagrama de bloques sobre el funcionamiento del sistema, donde el usuario tendrá la libertad de elegir el método de la apertura de la cerradura, si es mediante la huella o el bluetooth.

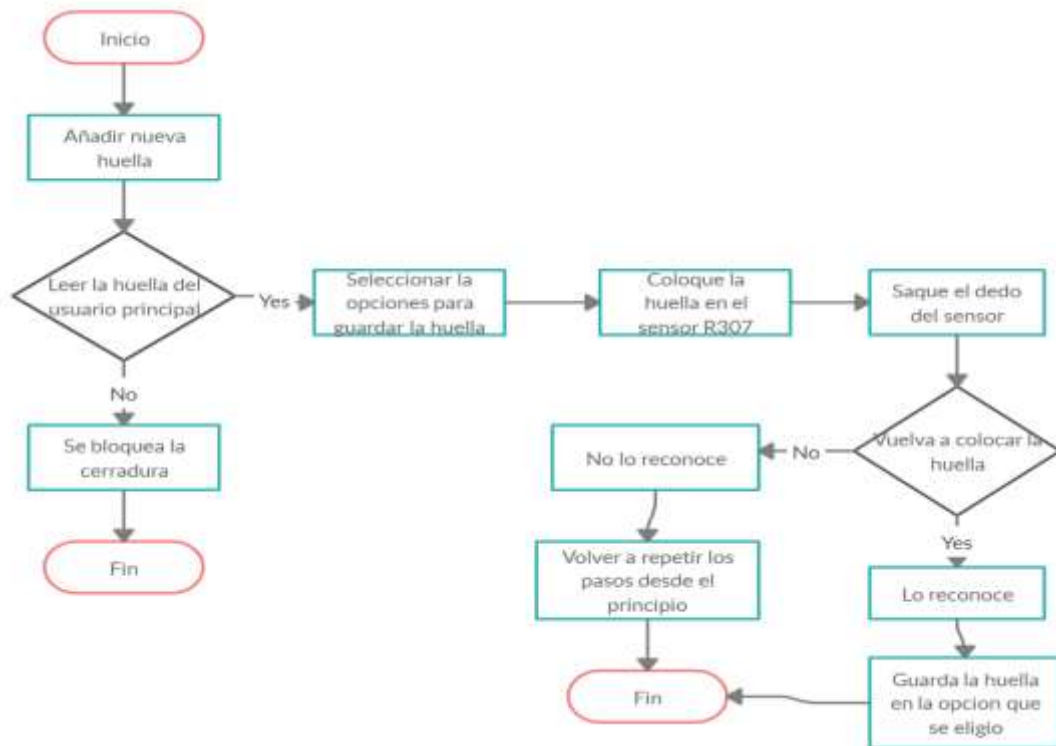


Fig 52.- Diagrama de flujo sobre añadir una nueva huella dactilar al prototipo. Elaborado por el autor

#### 4.4 Presupuesto

Los materiales propuestos en esta investigación fueron comprados en la ciudad de Guayaquil, si desea conseguirlos puede hacerlo en la zona denominada de “las electrónicas” que comprende la calle Venezuela que se interseca desde la calle José Mascote hasta la Av. Machala.

**Tabla 18.-** Materiales y costos del prototipo

Materiales	Cantidad	P. Unitario	Costo
<b>Arduino Mega</b>	1	\$19.49	\$19.49
<b>Bluetooth HC-06</b>	1	\$10.00	\$10.00
<b>Micro Sd Card</b>	1	\$8.00	\$8.00
<b>Micro SD - 2GB</b>	1	\$4.00	\$4.00
<b>LCD 16x2 I2C</b>	1	\$5.50	\$5.50
<b>RTC DS3231</b>	1	\$2.45	\$9.00
<b>Cables</b>	10	\$1.50	\$1.50
<b>Resistencia 2k</b>	3	\$0.10	\$0.30
<b>Pulsadores</b>	3	\$0.50	\$1.50

<b>Servomotor</b>	1	\$3.80	\$3.80
<b>Huella RB307</b>	1	\$36.00	\$36.00
<b>Total</b>			\$99.09

*Información elaborada por el autor*

#### 4.5 Conclusiones

- El objetivo de esta investigación era de crear una cerradura biométrica con los materiales accesibles y de bajo costo, que este capaz de competir con el mercado ecuatoriano en seguridad biométrica. Además de que la elaboración del prototipo sea tan explícita, con el fin de que lo puedan realizar las personas que no tengan un conocimiento básico sobre electrónica y programación.
- Mediante la encuesta se percibió un alto nivel de aceptación por parte de los encuestado del sector en querer implementarlo en un futuro, por lo novedoso del prototipo, el precio y por las funciones que posee.
- Con la comunicación inalámbrica del bluetooth es de gran ayuda para personas que vivan solas o discapacitadas da la ventaja de poder abrir la puerta a visitantes hasta los 10 metros entre la cerradura y el celular.

#### 4.6 Recomendaciones

- Para mayor eficiencia en la manipulación de datos en tiempo real de los ingresos a la vivienda ubicado en la tarjeta micro SD se recomienda el uso del módulo wifi ESP8266 que le permitirá acceder a los datos a cualquier lugar siempre y cuando esté conectado el dispositivo biométrico y el celular a la red de internet.
- Verificar los pines del sensor de huella dactilar, este dispositivo es sensible a los cambios de voltaje, esto quiere decir que si llegase a conectar mal la alimentación se quemará además que el sensor se verifica si funciona cuando una luz independiente del modelo este prendida, si la luz todavía no se enciende verificar los conectores Tx y Rx del sensor y de arduino que dependerá de cual se esté usando.
- Con el avance de equipos tecnológicos como los smartwatches es posible crear una aplicación en sitios como Android Studio y Android Wear con la función de conectar el smartwatch con la cerradura vía bluetooth, luego abrir la aplicación creada que cuente con un solo botón donde se pulse para abrir el dispositivo.

## 5 Anexo

### 5.1 Codificación en Arduino

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27,20,4); // librería LCD con el protocolo I2C
//Librería de la huella dactilar
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
int getFingerprintIDez();
SoftwareSerial mySerial(10, 11); // Se utiliza esos dos pines en el Arduino Mega
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
//Librería de la señal del reloj
#include <DS3231.h>
DS3231 rtc(SDA, SCL); // En el 3231 que es la señal de reloj se utiliza SDA y SCL como
interfaz de hardware
//Libreria del módulo adapter micro SD
#include <SPI.h>
#include <SD.h>
File myFile;
//Librería del servomotor
#include <Servo.h>
Servo miServo;
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
int escanear = 13; //Pin del pulsador para escanear la huella
int añadir = 12; //Pin para añadir una nueva huella
int servomotor = 6; //Pin para la señal del servomotor
int usuario_princi = 1; //Añade el usuario principal para poder ingresar nuevas huellas
int grados_servo = 180; //Grados de utilización del servomotor para abrir la cerradura
int cerrar_servo = 0; // Para poner en el estado inicial o en este caso cerrar
String file_name_to_save = "Registro_entrada.txt"; //El nombre del archivo que se
guarda en la memoria micro SD
bool scanning = false;
int counter = 0;
int id_ad_counter = 0;
bool id_ad = false;
uint8_t num = 1;
bool id_selected = false;
uint8_t id;
bool first_read = false;
bool main_user = false;
bool add_new_id = false;
bool door_locked = true;
void setup() {
  Serial.begin(57600); //Se inicia la comunicación RX y TX en el sensor de huella
  rtc.begin(); //Se inicia el conteo inicial del reloj módulo rtc 3231
  SD.begin(53); //Inicia el módulo adapter micro SD en el Arduino Mega se utiliza el pin
```

```

////////// Para escribir nuevos archivos de datos de ingreso, reescribir y cerrarlos//////////
myFile = SD.open(file_name_to_save, FILE_WRITE); //Se crea el nuevo archivo
myFile.print("Comienza el Sistema de cerradura ");
myFile.print(rtc.getTimeStr());myFile.print("          y          el          dia          ");
myFile.print(rtc.getDateStr());
myFile.println(" ");myFile.println(" ");
myFile.close();
lcd.init();          //Se ve en el LCD
lcd.backlight();
lcd.setCursor(0,0);
lcd.print("  Presione escanear  ");
lcd.setCursor(0,1);
lcd.print(" –Puerta bloqueada- ");
//////////Define los pines de entrada y salida//////////
pinMode(escanear,INPUT);
pinMode(añadir,INPUT);
miServo.attach(servomotor);
miServo.write(cerrar_servo); //Puerta cerrada
finger.begin(57600);        // Velocidad de los datos de la huella
}

void loop() {

//////////Abrir y cerrar automáticamente por la aplicación//////////
if(Serial.available(>0)
{
char Received = Serial.read();
if (Received == 'A')
{
miServo.write(180);
delay (7000);
miServo.write(90);
delay (0);
}
//////////Cuando se presiona el boton de escanear//////////
if(digitalRead(escanear) && !id_ad)
{
myFile = SD.open(file_name_to_save, FILE_WRITE);
myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
myFile.println(" – Intento de abrir la puerta");
myFile.close();
scanning = true;
lcd.setCursor(0,0);
lcd.print("  Coloque el dedo  ");
lcd.setCursor(0,1);
lcd.print("ESCANEANDO-----");
}
while(scanning && counter <= 60)
{
getFingerprintID();

```

```

delay(100);
counter = counter + 1;
if(counter == 10)
{
  lcd.setCursor(0,0);
  lcd.print(" Coloque el dedo ");
  lcd.setCursor(0,1);
  lcd.print("ESCAÑEANDO -----");
}

if(counter == 20)
{
  lcd.setCursor(0,0);
  lcd.print(" Coloque el dedo ");
  lcd.setCursor(0,1);
  lcd.print("ESCAÑEANDO ----");
}

if(counter == 40)
{
  lcd.setCursor(0,0);
  lcd.print(" Coloque el dedo ");
  lcd.setCursor(0,1);
  lcd.print("ESCAÑEANDO ----");
}

if(counter == 50)
{
  lcd.setCursor(0,0);
  lcd.print(" Coloque el dedo ");
  lcd.setCursor(0,1);
  lcd.print("ESCAÑEANDO----- ");
}
if(counter == 59)
{
  lcd.setCursor(0,0);
  lcd.print(" Sin Tiempo! ");
  lcd.setCursor(0,1);
  lcd.print(" Volver a Intentar! ");
  myFile = SD.open(file_name_to_save, FILE_WRITE);
  myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
  myFile.println(" – Sin tiempo de escaneo!");
  myFile.close();
  delay(2000);
  if(door_locked)
  {
    lcd.setCursor(0,0);
    lcd.print(" Presione escanear ");
    lcd.setCursor(0,1);
    lcd.print(" –Puerta Bloqueada");
  }
}

```



```

    }
    else
    {
        lcd.setCursor(0,0);
        lcd.print(" Presione escanear ");
        lcd.setCursor(0,1);
        lcd.print(" -Puerta abierta- ");
        miServo.write(180);
        delay (7000);
        miServo.write(0);
        delay (0);
    }
}

}
scanning = false;
counter = 0;

/////////////////////////////////////////Boton de añadir huella/////////////////////////////////////////
if(digitalRead(añadir) && !id_ad)
{
    myFile = SD.open(file_name_to_save, FILE_WRITE);
    myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
    myFile.println(" – El Nuevo usuario requiere permiso!");
    myFile.close();

    add_new_id = true;

    lcd.setCursor(0,0);
    lcd.print(" Escaneo huella principal");
    lcd.setCursor(0,1);
    lcd.print(" Primero el dedo! ");

    while (id_ad_counter < 40 && !main_user)
    {
        getFingerprintID();
        delay(100);
        id_ad_counter = id_ad_counter+1;
        if(!add_new_id)
        {
            id_ad_counter = 40;
        }
    }
    id_ad_counter = 0;
    add_new_id = false;

    if(main_user)
    {
        lcd.setCursor(0,0);

```

```

    lcd.print(" Añadir la nueva en ID# ");
    lcd.setCursor(0,1);
    lcd.print(" Base de datos ");
    delay(1500);
    print_num(num);
    id_ad = true;
    myFile = SD.open(file_name_to_save, FILE_WRITE);
    myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
    myFile.println(" – Permiso garantizado para añadir");
    myFile.close();
}
else
{
    lcd.setCursor(0,0);
    lcd.print("ERROR! Solo principal");
    lcd.setCursor(0,1);
    lcd.print("Usuario desea añadir IDs");
    delay(1500);
    if(door_locked)
    {
        lcd.setCursor(0,0);
        lcd.print(" Presione escanear ");
        lcd.setCursor(0,1);
        lcd.print(" –Puerta bloqueada- ");
    }
    else
    {
        lcd.setCursor(0,0);
        lcd.print(" Presione escanear ");
        lcd.setCursor(0,1);
        lcd.print(" -Puerta cerrada- ");
    }
    id_ad = false;
    myFile = SD.open(file_name_to_save, FILE_WRITE);
    myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
    myFile.println(" – El usuario no tiene permiso para añadirse");
    myFile.close();
}
}

if(digitalRead(escanear) && id_ad)
{

    id=num;
    while (! getFingerprintEnroll() );
    id_ad = false;
    lcd.clear();
    lcd.setCursor(0,0);
    lcd.print(" Nueva ID guardada ");
    lcd.setCursor(4,1);

```

```

lcd.print("la ID #");
lcd.setCursor(11,1);
lcd.print(id);
delay(3000);
if(door_locked)
{
  lcd.setCursor(0,0);
  lcd.print(" Presione escanear ");
  lcd.setCursor(0,1);
  lcd.print(" -Puerta bloqueada- ");
}
else
{
  lcd.setCursor(0,0);
  lcd.print(" Presione escanear ");
  lcd.setCursor(0,1);
  lcd.print(" -Puerta abierta- ");
  miServo.write(180);
  delay (7000);
  miServo.write(0);
  delay (0);
}
add_new_id = false;
main_user = false;
id_ad = false;
}
if(digitalRead(añadir) && id_ad)
{
  num = num + 1;
  if(num > 16)
  {
    num=1;
  }
  print_num(num);
}
}
//end of void
//////////Añadir nueva huella desde 1 hasta 127 huellas se pueden guardar//////////
void print_num(uint8_t)
{
  if (num == 1)
  {
    lcd.setCursor(0,0);
    lcd.print("Selección ID número");
    lcd.setCursor(0,1);
    lcd.print(">1 2 3 4 ");
    delay(500);
  }
  if (num == 2)
  {

```

```

    lcd.setCursor(0,0);
    lcd.print("Seleccion ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 1 >2  3  4  ");
    delay(500);
}
if (num == 3)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 1  2 >3  4  ");
    delay(500);
}
if (num == 4)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 1  2  3 >4  ");
    delay(500);
}
if (num == 5)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(">5  6  7  8  ");
    delay(500);
}
if (num == 6)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 5 >6  7  8  ");
    delay(500);
}
if (num == 7)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 5  6 >7  8  ");
    delay(500);
}
if (num == 8)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");

```

```

    lcd.setCursor(0,1);
    lcd.print(" 5  6  7 >8  ");
    delay(500);
}
if (num == 9)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(">9 10 11 12 ");
    delay(500);
}
if (num == 10)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 9 >10 11 12 ");
    delay(500);
}
if (num == 11)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 9 10 >11 12 ");
    delay(500);
}
if (num == 12)
{
    lcd.setCursor(0,0);
    lcd.print("Seleccione ID numero");
    lcd.setCursor(0,1);
    lcd.print(" 9 10 11 >12 ");
    delay(500);
}
}

```

//////////Leerá las nuevas huellas almacenadas en la base de datos//////////

```

uint8_t getFingerprintID()
{
    uint8_t p = finger.getImage();
    switch (p)
    {
        case FINGERPRINT_OK:
            break;
        case FINGERPRINT_NOFINGER: return p;
        case FINGERPRINT_PACKETRECEIVEERR: return p;
        case FINGERPRINT_IMAGEFAIL: return p;
        default: return p;
    }
}

```

```

    }
    // OK Exitó!
    p = finger.image2Tz();
    switch (p)
    {
        case FINGERPRINT_OK: break;
        case FINGERPRINT_IMAGEMESS: return p;
        case FINGERPRINT_PACKETRECEIVEERR: return p;
        case FINGERPRINT_FEATUREFAIL: return p;
        case FINGERPRINT_INVALIDIMAGE: return p;
        default: return p;
    }
    // OK converted!
    p = finger.fingerFastSearch();
    if (p == FINGERPRINT_OK)
    {
        scanning = false;
        counter = 0;
        if(add_new_id)
        {
            if(finger.fingerID == main_user_ID)
            {
                main_user = true;
                id_ad = false;
            }
            else
            {
                add_new_id = false;
                main_user = false;
                id_ad = false;
            }
        }
        else
        {
            miServo.write(cerrar_servo); //Puerta abierta
            lcd.clear();
            lcd.setCursor(0,0);
            lcd.print("  Usuario emparejado  ");

            lcd.setCursor(0,1);
            lcd.print(" ID: #");

            lcd.setCursor(6,1);
            lcd.print(finger.fingerID);

            lcd.setCursor(9,1);
            lcd.print("%: ");

            lcd.setCursor(12,1);
            lcd.print(finger.confidence);

```

```

myFile = SD.open(file_name_to_save, FILE_WRITE);
myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
myFile.print(" – Usuario emparejado en el ID# "); myFile.print(finger.fingerID);
myFile.print(" confianza: "); myFile.print(finger.confidence); myFile.println(" –
Puerta Abierta");
myFile.close();
door_locked = false;
delay(4000);
lcd.setCursor(0,0);
lcd.print(" Presione escanear ");
lcd.setCursor(0,1);
lcd.print(" -Puerta abierta- ");
miServo.write(180);
delay (7000);
miServo.write(0);
delay (0);
delay(50);
}
} // Fin dedo OK
else if(p == FINGERPRINT_NOTFOUND)
{
  scanning = false;
  id_ad = false;
  counter = 0;
  lcd.setCursor(0,0);
  lcd.print(" No emparejado ");
  lcd.setCursor(0,1);
  lcd.print(" Intente otra vez! ");
  add_new_id = false;
  main_user = false;
  myFile = SD.open(file_name_to_save, FILE_WRITE);
  myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
  myFile.print(" – No localizado en la base");
  myFile.close();
  delay(2000);
  if(door_locked)
  {
    lcd.setCursor(0,0);
    lcd.print(" Presione escanear ");
    lcd.setCursor(0,1);
    lcd.print(" –Puerta bloqueada- ");
  }
  else
  {
    lcd.setCursor(0,0);
    lcd.print(" Presiona escanear ");
    lcd.setCursor(0,1);
    lcd.print(" -Puerta abierta- ");
    miServo.write(180);
    delay (7000);
  }
}

```

```

        miServo.write(0);
        delay (0);
    }
    delay(2);
    return p;
} //
} //
int getFingerprintIDez() {
    uint8_t p = finger.getImage();
    if (p != FINGERPRINT_OK) return -1;
    p = finger.image2Tz();
    if (p != FINGERPRINT_OK) return -1;
    p = finger.fingerFastSearch();
    if (p != FINGERPRINT_OK) return -1;
    // Búsqueda exitosa!
    return finger.fingerID;
}
/////////Añadir nueva huella a la base de datos/////////
uint8_t getFingerprintEnroll() {
    int p = -1;
    if(!first_read)
    {
        lcd.setCursor(0,0);
        lcd.print("Añadir nueva en el ID# ");
        lcd.setCursor(14,0);
        lcd.print(id);
        lcd.setCursor(0,1);
        lcd.print(" Coloque el dedo ");
    }
    while (p != FINGERPRINT_OK) {
        p = finger.getImage();
        switch (p) {
            case FINGERPRINT_OK:
                lcd.setCursor(0,0);
                lcd.print(" Imagen tomada! ");
                lcd.setCursor(0,1);
                lcd.print(" ");
                delay(100);
                first_read = true;
                break;
            case FINGERPRINT_NOFINGER:
                lcd.setCursor(0,0);
                lcd.print("Añadir en el ID# ");
                lcd.setCursor(14,0);
                lcd.print(id);
                lcd.setCursor(0,1);
                lcd.print(" Coloque el dedo ");
                break;
            case FINGERPRINT_PACKETRECEIVEERR:
                lcd.setCursor(0,0);

```



```

    lcd.print(" Comunicacion ");
    lcd.setCursor(0,1);
    lcd.print("  ERROR!  ");
    delay(1000);
    break;
case FINGERPRINT_IMAGEFAIL:
    lcd.setCursor(0,0);
    lcd.print("  -Imagen  ");
    lcd.setCursor(0,1);
    lcd.print("  ERROR!  ");
    delay(1000);
    break;
default:
    lcd.setCursor(0,0);
    lcd.print("  -Desconocido  ");
    lcd.setCursor(0,1);
    lcd.print("  ERROR!  ");
    delay(1000);
    break;
}
}
// OK exitoso!
p = finger.image2Tz(1);
switch (p) {
case FINGERPRINT_OK:
    lcd.setCursor(0,0);
    lcd.print("Image convertida!");
    lcd.setCursor(0,1);
    lcd.print("          ");
    break;
case FINGERPRINT_IMAGEMESS:
    lcd.setCursor(0,0);
    lcd.print("Imagen muy sucia!");
    lcd.setCursor(0,1);
    lcd.print("          ");
    delay(1000);
    return p;
case FINGERPRINT_PACKETRECEIVEERR:
    lcd.setCursor(0,0);
    lcd.print(" Comunicacion ");
    lcd.setCursor(0,1);
    lcd.print("  ERROR!  ");
    delay(1000);
    return p;
case FINGERPRINT_FEATUREFAIL:
    lcd.setCursor(0,0);
    lcd.print(" No huella dactilar ");
    lcd.setCursor(0,1);
    lcd.print("Caracteristicas encontradas ");
    delay(1000);

```

```

    return p;
case FINGERPRINT_INVALIDIMAGE:
    lcd.setCursor(0,0);
    lcd.print(" No huella dactilar ");
    lcd.setCursor(0,1);
    lcd.print("Caracteristicas encontradas ");
    delay(1000);
    return p;
default:
    lcd.setCursor(0,0);
    lcd.print(" -Desconocido ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    return p;
}
    lcd.setCursor(0,0);
    lcd.print(" Remover dedo! ");
    lcd.setCursor(0,1);
    lcd.print(" ");
    delay(2000);
    p = 0;
    while (p != FINGERPRINT_NOFINGER) {
        p = finger.getImage();
    }
    lcd.setCursor(0,1);
    lcd.print("ID# ");
    lcd.setCursor(4,1);
    lcd.print(id);
    p = -1;
    lcd.setCursor(0,0);
    lcd.print("Coloque otra vez ");
    lcd.setCursor(0,1);
    lcd.print("el mismo dedo ");
    while (p != FINGERPRINT_OK) {
        p = finger.getImage();
        switch (p) {
            case FINGERPRINT_OK:
                lcd.setCursor(0,0);
                lcd.print(" Imagen tomada! ");
                lcd.setCursor(0,1);
                lcd.print(" ");
                break;
            case FINGERPRINT_NOFINGER:
                lcd.setCursor(0,0);
                lcd.print("Aplaste otra vez ");
                lcd.setCursor(0,1);
                lcd.print("Mismo dedo ");
                break;
            case FINGERPRINT_PACKETRECEIVEERR:

```

```

    lcd.setCursor(0,0);
    lcd.print(" Comunicacion ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    break;
case FINGERPRINT_IMAGEFAIL:
    lcd.setCursor(0,0);
    lcd.print(" -Imagen ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    break;
default:
    lcd.setCursor(0,0);
    lcd.print(" -Desconocido ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    break;
}
}
// OK exitosa!
p = finger.image2Tz(2);
switch (p) {
case FINGERPRINT_OK:
    lcd.setCursor(0,0);
    lcd.print("Imagen convertida!");
    lcd.setCursor(0,1);
    lcd.print(" ");
    break;
case FINGERPRINT_IMAGEMESS:
    lcd.setCursor(0,0);
    lcd.print("Imagen muy sucia!");
    lcd.setCursor(0,1);
    lcd.print(" ");
    delay(1000);
    return p;
case FINGERPRINT_PACKETRECEIVEERR:
    lcd.setCursor(0,0);
    lcd.print(" Comunicacion ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    return p;
case FINGERPRINT_FEATUREFAIL:
    lcd.setCursor(0,0);
    lcd.print(" No huella dactilar ");
    lcd.setCursor(0,1);
    lcd.print("Características encontradas ");

```

```

    delay(1000);
    return p;
case FINGERPRINT_INVALIDIMAGE:
    lcd.setCursor(0,0);
    lcd.print(" Comunicacion ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    return p;
default:
    lcd.setCursor(0,0);
    lcd.print(" -Desconocida ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    return p;
}

// OK converted!
lcd.setCursor(0,0);
lcd.print(" Creando modelo ");
lcd.setCursor(0,1);
lcd.print("Para ID# ");
lcd.setCursor(8,1);
lcd.print(id);
p = finger.createModel();
if (p == FINGERPRINT_OK) {
    lcd.setCursor(0,0);
    lcd.print(" Coincide impresion! ");
    lcd.setCursor(0,1);
    lcd.print(" ");
    delay(1000);
} else if (p == FINGERPRINT_PACKETRECEIVEERR) {
    lcd.setCursor(0,0);
    lcd.print(" Comunicacion ");
    lcd.setCursor(0,1);
    lcd.print(" ERROR! ");
    delay(1000);
    return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
    lcd.setCursor(0,0);
    lcd.print("Huella dactilar lo hizo ");
    lcd.setCursor(0,1);
    lcd.print("no emparejado ");
    delay(1000);
    return p;
} else {
    lcd.setCursor(0,0);
    lcd.print(" -Desconocido ");
    lcd.setCursor(0,1);

```

```

    lcd.print("  ERROR!  ");
    delay(1000);
    return p;
}
    lcd.setCursor(0,1);
    lcd.print("ID# ");
    lcd.setCursor(4,1);
    lcd.print(id);
    p = finger.storeModel(id);
    if (p == FINGERPRINT_OK) {
        lcd.setCursor(0,0);
        lcd.print("  Guardada  ");
        lcd.setCursor(0,1);
        lcd.print("      ");
        myFile = SD.open(file_name_to_save, FILE_WRITE);
        myFile.print(rtc.getDateStr()); myFile.print(" -- "); myFile.print(rtc.getTimeStr());
        myFile.print(" -- New fingerprint stored for ID# "); myFile.println(id);
        myFile.close();
        delay(1000);
        first_read = false;
        id_ad = false;
        } else if (p == FINGERPRINT_PACKETRECEIVEERR) {
        lcd.setCursor(0,0);
        lcd.print(" Comunicacion ");
        lcd.setCursor(0,1);
        lcd.print("  ERROR!  ");
        delay(1000);
        return p;
    } else if (p == FINGERPRINT_BADLOCATION) {
        lcd.setCursor(0,0);
        lcd.print("No se puede almacenar ");
        lcd.setCursor(0,1);
        lcd.print("En la locacion");
        delay(1000);
        return p;
    } else if (p == FINGERPRINT_FLASHERR) {
        lcd.setCursor(0,0);
        lcd.print("Error al escribir");
        lcd.setCursor(0,1);
        lcd.print("flash      ");
        delay(1000);
        return p;
    } else {
        lcd.setCursor(0,0);
        lcd.print("  -Desconocido ");
        lcd.setCursor(0,1);
        lcd.print("  ERROR!  ");
        delay(1000);
        return p;
    } }

```

## 5.2 Construcción del prototipo de cerradura biométrica con huella dactilar

### Paso 1

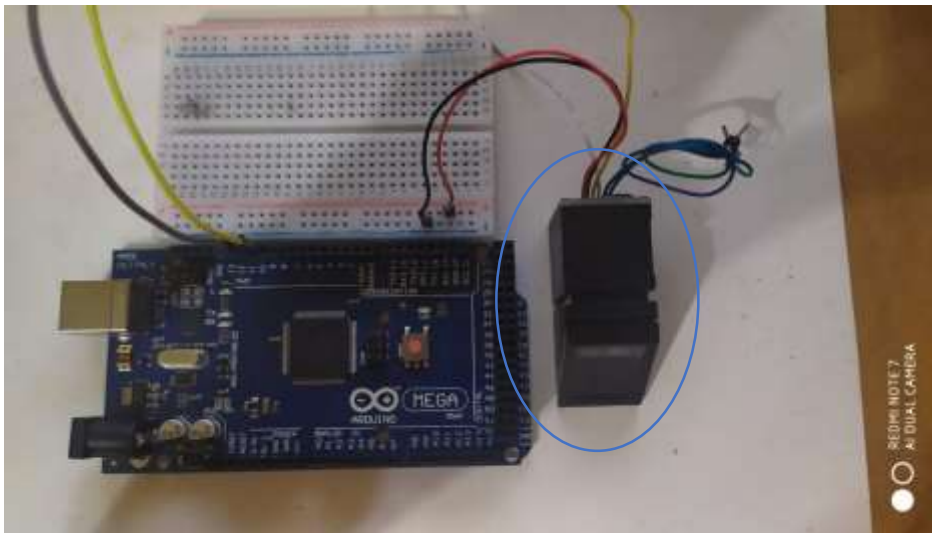
Se procede a añadir la huella dactilar con su respectiva librería, luego se realiza las conexiones del el sensor de huella R307 como se observa en la imagen, dicho sensor posee 6 cables de los cuales solo se van trabajar con 4, el de Vcc que va a 5 voltios, GND que va a Tierra, y los dos cables Tx y Rx que trabaja en el arduino en este caso el Mega y se elige cualquiera de los siguientes pines: 10, 11, 12, 13, 14, 15, 50, 51, 52, 53, A8 (62), A9 (63), A10 (64), A11 (65), A12 (66), A13 (67), A14 (68), A15 (69).

Los dos cables que quedan no son compatibles con arduino.

Debemos declarar estos pines como SoftwareSerial que es una comunicación en serie de 0 y 1.

Ejemplo: `#include <SoftwareSerial.h>`

`SoftwareSerial mySerial (10, 11); // Se utiliza esos dos pines en el Arduino Mega`



*Fig. 53 Conexión del sensor R307 al arduino Mega. Elaborado por el autor*

### Paso 2

Añadimos el módulo de bluetooth conectando los puntos de alimentación Vcc, GND y los cables Tx que van conectado en el Rx del arduino en este caso el pin 0 y Rx que va conectado en el Tx del arduino en el pin 1.

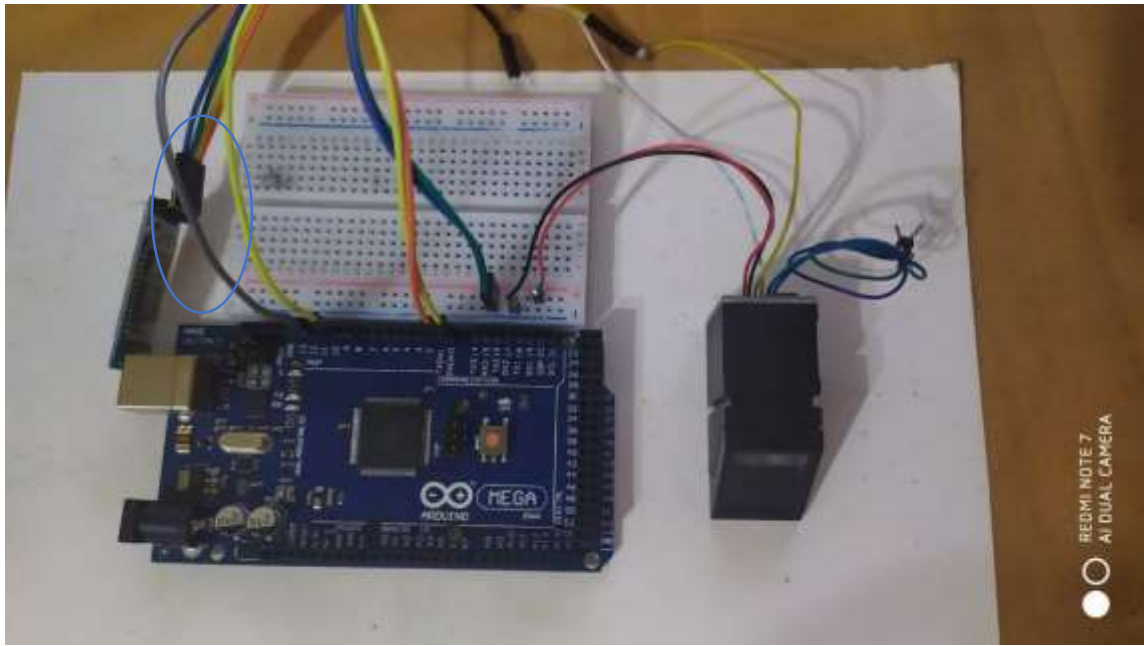


Fig. 54 Conexión del bluetooth y del sensor de huella R307

### Paso 3

El módulo RTC DS3231, que es la señal de reloj contiene una pila de 3 voltios de respaldo, en caso de cortes o fallas de energía, además mantiene activa la señal sin perder el registro de la fecha actual y se alimenta de los siguientes puntos: Vcc y GND, los pines restantes, el SDA que es la entrada para los datos que va en el pin 16 y el SCL que es la entrada del reloj que va en el pin 17

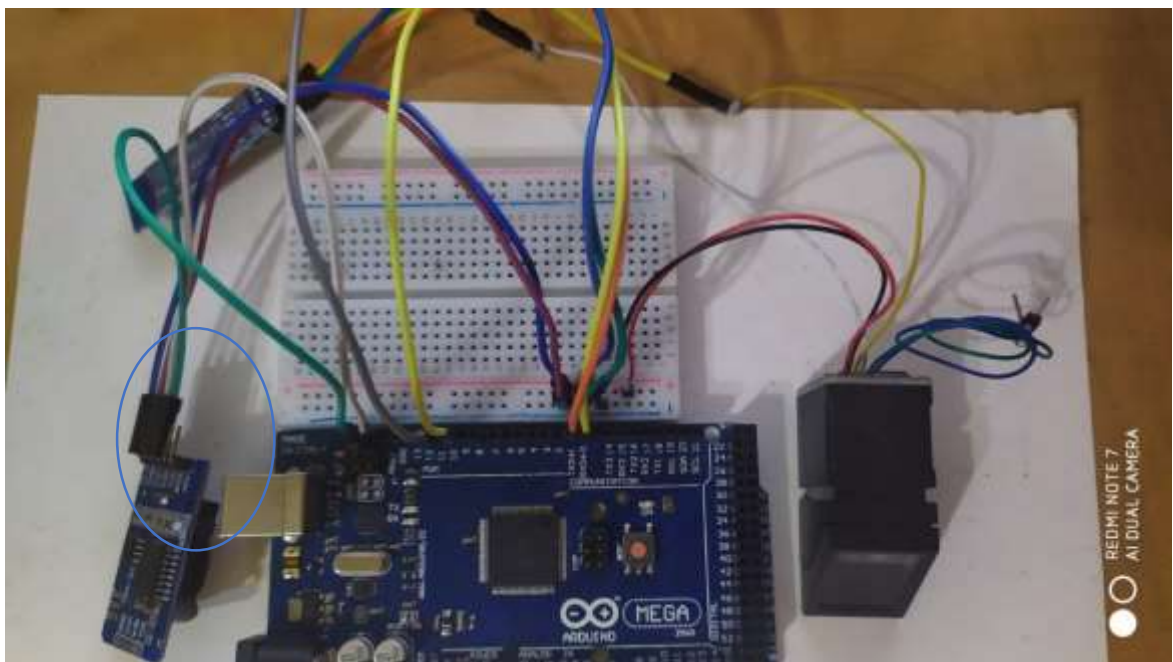
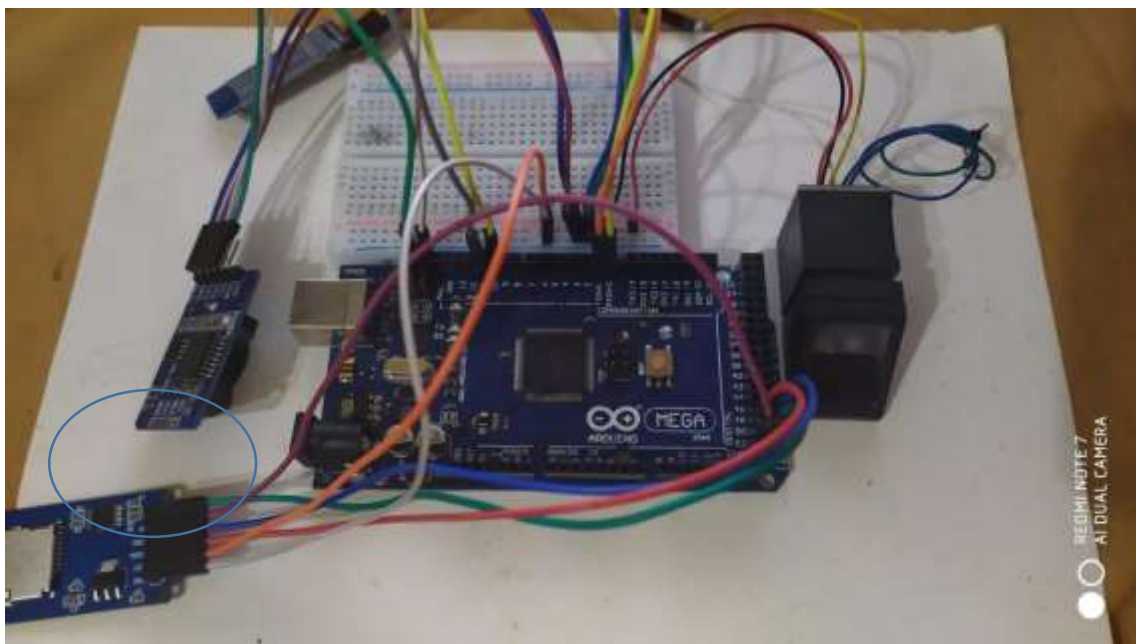


Fig 55 Conexión del RTC DS3231 con el bluetooth y el R307

#### Paso 4

El módulo Micro SD Card Adapter dispone de una ranura donde se inserta la memoria micro SD y así después poderla extraer de una forma manual y divisar quiénes han ingresado a la vivienda, este módulo cuenta de 6 pines, cuales dos son de Vcc y GND y los 4 restantes que son:

- CS: El chip de selección, es el habilita al integrado hacia donde quiere viajar los datos, esta señal es opcional va conectado en el pin 53.
- SCK: Señal de reloj, rige la velocidad en la que viajan los datos va conectado en el pin 52
- MOSI: Salida maestra entrada esclava, es la transmisión de los datos hacia otro integrado que va conectado en el pin 51
- MOSO: Entrada maestra salida esclava, esta señal es la entrada del dispositivo donde se recepta la transmisión del otro integrado donde va conectado en el pin 50.



*Fig. 56 Adapter micro SD con RTC DS3231, bluetooth y R307*

#### Paso 5

Se recomienda añadirle al lcd 16x2 el adaptador basado en el PCF8574, este adaptador que tiene una comunicación I2C, permite ahorrar cables, tiempo además que incluye un potenciómetro en la parte de atrás donde se gradúa la intensidad de la pantalla, se alimenta



los cables Vcc y GND y los cables restantes el SDA que es la señal de datos va en el pin 20, mientras que el SCL la señal de reloj va en el pin 21

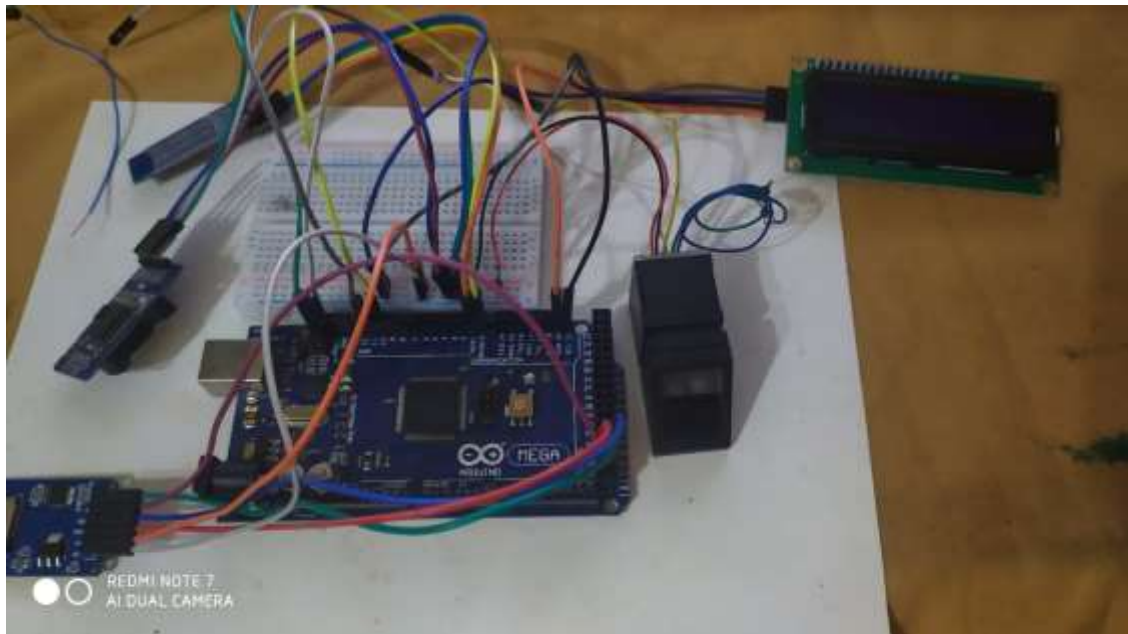


Fig.57 Pantalla LCD 16x2, micro adapter, RTC DS3231, bluetooth y R307

## Paso 6

Ya terminado de ensamblar el prototipo, se procede a la creación de la aplicación, en este caso es App Inventor, ¡para poder empezar a trabajar se debe dar click en la opción **Create Apps!**



Fig. 58 Página principal del sitio web <http://ai2.appinventor.mit.edu/>.



## Paso 9

Se coloca los botones para poder accionar la cerradura, el label que es un cuadro de texto, las imágenes que son opcional, se debe de subir al sitio mediante la carga de la computadora. Para seleccionar cualquiera de los componentes mencionados, se debe de dar click y arrastrar con el mouse a la pantalla del celular.



Fig 61. Creación de la aplicación para la cerradura

## Paso 10

Al igual que en el proceso anterior, los bloques se arrastran con el mouse hacia la pantalla, cabe mencionar que el sitio web posee la opción de guardado automático cada segundo.

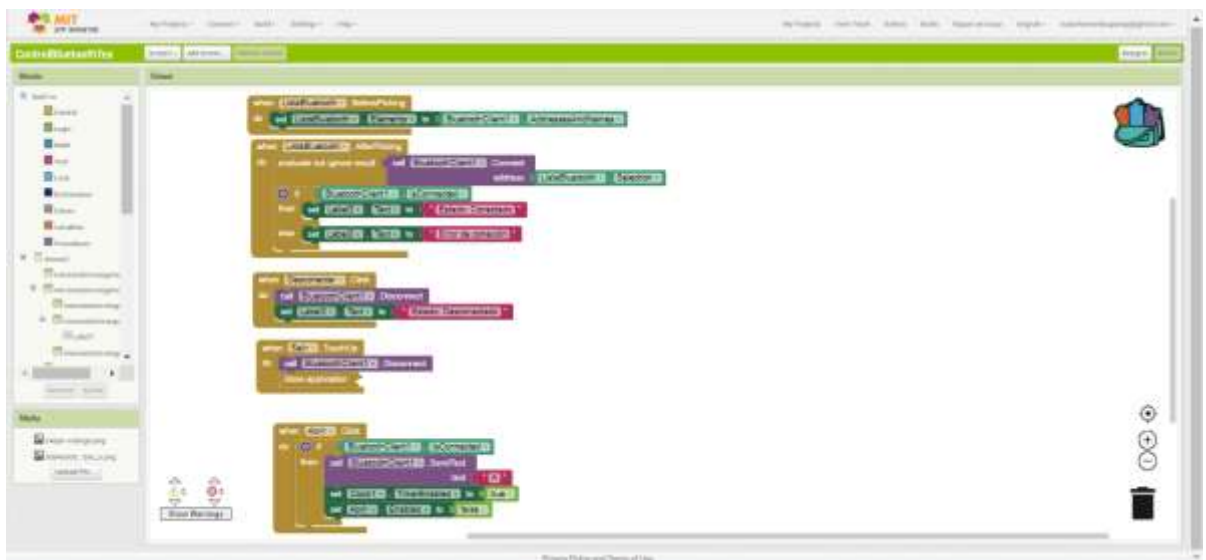


Fig 62. Creación del diagrama de bloque para la cerradura

## Paso 11

Una vez terminado los diagramas de bloque se debe construir el archivo para el dispositivo móvil en la opción de **Build**, esta opción brinda dos alternativas para obtener el archivo:

- Código QR: Se necesita del lector de la cámara del celular, no todos los dispositivos tienen un lector de código qr.
- Save: Genera el archivo y lo guarda en la carpeta **Descargas** de la computadora, para luego proceder a pasarla al celular, para poder instalarla.



Fig 63. Generar el archivo para el dispositivo móvil

## Paso 12

Y, por último, se copia la codificación que está en **Anexo>7.1 Codificación en Arduino**, conectar el prototipo ya elaborado, en el puerto USB y dar clic en el software en la opción **Subir** y listo, el proyecto ya está terminado y listo para su requerimiento.

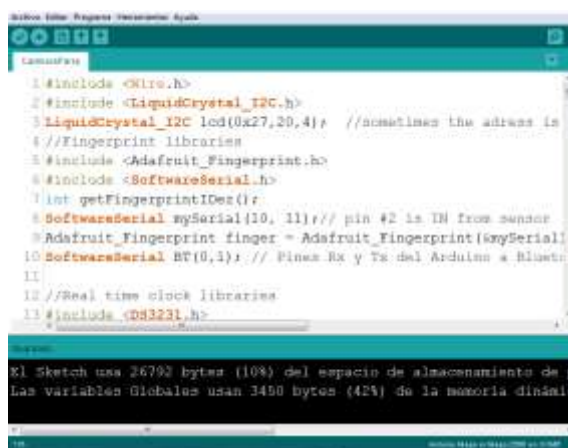


Fig 64. Codificación en Arduino

### Bibliografía

- [1] Sucunza, R. (20 de Marzo de 2018). *SUKON*. Obtenido de SUKON: <https://www.sukot.com/que-es-el-bumping/>
  - [2] (MDG), D. d. (31 de 07 de 2019). *Ministerio de gobierno*. Obtenido de Ministerio de gobierno: <http://cifras.ministeriodegobierno.gob.ec/comisioncifras/inicio.php>
  - [3] Janices, P. (Junio de 2015). *CXO*. Obtenido de CXO: <https://www.cxo-community.com/2015/06/biometria-reconocimiento-por-iris.html>
  - [4] *FacePhi*. (08 de 09 de 2015). Obtenido de FacePhi: <https://www.facephi.com/es/noticias/sala-prensa/facephi-lleva-su-sistema-de-reconocimiento-facial-a-ecuador-gracias-a-un-acuerdo-con-banco-guayaquil/>
  - [5] *FacePhi*. (04 de 12 de 2015). Obtenido de FacePhi: <https://www.facephi.com/es/noticias/sala-prensa/facephi-implanta-su-tecnologia-en-banco-del-pacifico-de-ecuador-para-sus-clientes-de-banca-movil/>
  - [6] *FacePhi*. (s.f.). Obtenido de FacePhi: <https://www.facephi.com/es/contenido/selphid/>
  - [7] *FacePhi*. (s.f.). Obtenido de FacePhi: <https://www.facephi.com/es/contenido/selphi/>
  - [8] *FacePhi*. (s.f.). Obtenido de FacePhi: <https://www.facephi.com/es/contenido/lookphi/>
  - [9] *FacePhi*. (s.f.). Obtenido de FacePhi: <https://www.facephi.com/en/content/phivox-en/>
  - [10] *FacePhi*. (s.f.). Obtenido de FacePhi: <https://www.facephi.com/es/contenido/casos-de-exito/>
  - [11] *Arduino*. (s.f.). Obtenido de Arduino: <https://arduino.cl/que-es-arduino>
- Bueno, C. T. (s.f.). *Sistemas Biometricos*. Obtenido de [https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web\\_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf](https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf)