



**UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERIA INDUSTRIAL
CARRERA DE INGENIERÍA EN TELEINFÓRMÁTICA**

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

**ÁREA
TECNOLOGÍAS DE LOS ORDENADORES
SISTEMA EN TIEMPO REAL**

**TEMA
“DISEÑO DE UN PROTOTIPO DE PORTERO
ELECTRÓNICO AUTOMÁTICO CON RECONOCIMIENTO
FACIAL MEDIANTE EL USO DE
MICROCONTROLADORES”**

**AUTOR
VELIZ CHANCAY AMARILIS DAYANA**

**DIRECTOR DEL TRABAJO
ING. SIST. PINCAY BOHÓRQUEZ FREDDY STEVE, MG.**

GUAYAQUIL, JULIO 2020



**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:			
Diseño de un prototipo de portero electrónico automático con reconocimiento facial mediante el uso de microcontroladores.			
AUTOR(ES) (apellidos/nombres):		Veliz Chancay Amarilis Dayana	
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):		Ing. Sist. Pincay Bohórquez Freddy Steve, Mg./ Ing. Castillo León Rosa	
INSTITUCIÓN:		Universidad de Guayaquil	
UNIDAD/FACULTAD:		Facultad de Ingeniería Industrial	
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:		Ingeniera en Teleinformática	
FECHA DE PUBLICACIÓN:		22 de Octubre del 2020	No. DE PÁGINAS: 111
ÁREAS TEMÁTICAS:		Tecnologías de los ordenadores, sistema en tiempo real.	
PALABRAS CLAVES/ KEYWORDS:		Reconocimiento facial, algoritmos, microcontrolador, Base de datos, Patrones.	
RESUMEN/ABSTRACT (100-150 palabras):			
<p>El presente trabajo de investigación tiene como objetivo principal diseñar un prototipo de portero electrónico automático, que su característica principal sea el uso de patrones biométricos faciales, con un sistema automático de control de acceso en tiempo real, denominado “Face Access”, permitiendo la notificación mediante correo electrónico de usuarios permitidos o desconocidos. La metodología a utilizar es: diseño técnico, experimental y esquemático, a su vez el uso de herramientas como encuestas en línea realizada a empresas que prestan servicios de seguridad en la ciudad de Guayaquil, con el fin de resolver las inconsistencias que existen en los sistemas de control de acceso basados biometría facial, validando pruebas de funcionamiento del sistema con diferentes parámetros biométricos dando a conocer su efectividad y precisión mediante el uso de Raspberry Pi como microcontrolador, siendo totalmente viable para su implementación si así se desea.</p> <p>The main objective of the present research work is to design a prototype of an electronic door entry system, whose main characteristic is the use of facial biometric patterns, with an automatic access control system in real time, called “Face Access”, allowing notification via email from permitted or unknown users. The methodology to be used is: technical, experimental and schematic design, in turn the use of tools such as online surveys carried out to companies that provide security services in the city of Guayaquil, in order to resolve the inconsistencies that exist</p>			

in the systems access control system based on facial biometrics, validating system performance tests with different biometric parameters, making known its effectiveness and precision through the use of Raspberry Pi as a microcontroller, being totally viable for implementation if desired.

ADJUNTO PDF:	SI	X	NO
CONTACTO CON AUTOR/ES:	Teléfono: 0996922694		E-mail: amarilis.velizc@ug.edu.ec
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramón Maquilón Nicola		
	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, **VELIZ CHANCAY AMARILIS DAYANA**, con C.C. No. **0940104698**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es “**DISEÑO DE UN PROTOTIPO DE PORTERO ELECTRÓNICO AUTOMÁTICO CON RECONOCIMIENTO FACIAL MEDIANTE EL USO DE MICROCONTROLADORES**” 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.

VELIZ CHANCAY AMARILIS DAYANA
C.C.No. **0940104698**



**ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Habiendo sido nombrado **ING. FREDDY STEVE PINCAY BOHORQUEZ**, tutor del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por **VELIZ CHANCAY AMARILIS DAYANA**, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERA EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: “**DISEÑO DE UN PROTOTIPO DE PORTERO ELECTRÓNICO AUTOMÁTICO CON RECONOCIMIENTO FACIAL MEDIANTE EL USO DE MICROCONTROLADORES**”, ha sido orientado durante todo el periodo de ejecución en el programa antiplagio (URKUND) quedando el 1% de coincidencia.

URKUND

Document Information

Analyzed document	TESIS VELIZ CHANCAY.docx (D80458057)
Submitted	10/2/2020 4:03:00 AM
Submitted by	
Submitter email	adveliz4@gmail.com
Similarity	1%
Analysis address	freddy.pincayb.ug@analysis.urkund.com

Sources included in the report

W	URL: https://es.wikipedia.org/wiki/Usuario:Davisclick/Taller Fetched: 10/28/2019 7:53:31 AM	3
W	URL: https://docplayer.es/81224271-Biometric-access-control-system.html Fetched: 10/30/2019 8:05:47 PM	1
W	URL: https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20... Fetched: 7/24/2020 11:28:57 PM	1
SA	PROYECTO DE TITULACIÓN.pdf Document PROYECTO DE TITULACIÓN.pdf (D25413243)	1

<https://secure.urkund.com/view/76979373-265041-281388#/>

ING. FREDDY STEVE PINCAY BOHORQUEZ, MG
DOCENTE TUTOR
CC: 0919786285
FECHA: 5/10/2020



**ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR DEL
TRABAJO DE TITULACIÓN
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 05 de Octubre del 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 **“DISEÑO DE UN PROTOTIPO DE PORTERO ELECTRÓNICO AUTOMÁTICO CON RECONOCIMIENTO FACIAL MEDIANTE EL USO DE MICROCONTROLADORES”** de la estudiante **VELIZ CHANCAY AMARILIS DAYANA**, 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 la estudiante está apta para continuar con el proceso de revisión final.

Atentamente,

ING. FREDDY STEVE PINCAJ BOHORQUEZ
TUTOR DE TRABAJO DE TITULACIÓN
CC: 0919786285
FECHA: 05/10/2020



ANEXO VIII.- INFORME DEL DOCENTE REVISOR

FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA



Guayaquil, 13 de octubre de 2020

Sr (a).

Ing. Annabelle Lizaraburu 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 REVISIÓN FINAL del Trabajo de Titulación “**DISEÑO DE UN PROTOTIPO DE PORTERO ELECTRÓNICO AUTOMÁTICO CON RECONOCIMIENTO FACIAL MEDIANTE EL USO DE MICROCONTROLADORES**” de la estudiante **VELIZ CHANCAY AMARILIS DAYANA**. 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 16 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 5 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 la estudiante está apta para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,

ING. ROSA ELIZABETH CASTILLO LEÓN, MG.

C.C: 0922372610

FECHA: 13 DE OCTUBRE DE 2020

Dedicatoria

Dedico este trabajo de titulación a las personas que me dieron la vida, y me enseñaron a afrontar situaciones adversas que con su entusiasmo y amor incondicional, nunca dejaron que me rinda, convirtiéndose en mis pilares fundamentales, mis padres: Freddy Véliz Contreras y Paula Chancay Ponce.

A mis Abuelitos: Ricardo Véliz, María Contreras, quienes han percibido mis triunfos durante toda mi vida y desde el cielo cuidándome siempre, Lidia Ponce y Gregorio Chancay.

A mis hermanos: Tito, Jamileth, por ser mi inspiración y compañeros de vida.

Agradecimiento

A Dios por ser mi guía espiritual, cada miembro de mi familia, en especial a mis padres Freddy y Paula, a mis tías Cecibel Ponce y Jaqueline Bajaña, quienes palpitaron el esfuerzo y perseverancia de mi vida universitaria.

A mis amigos incondicionales y aquellas personas especiales que conocí en el transcurso de estos años, no me alcanzará la vida para agradecer todo su cariño y apoyo.

A mis directores de trabajo: Ing. Freddy Pincay Bohórquez e Ing. Rosa Castillo León, por brindarme sus conocimientos y paciencia durante el desarrollo de este proyecto.

A la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación: Por haberme adjudicado una beca, incentivo económico importante para poder culminar esta etapa.

Índice General

N°	Descripción	Pág.
	Introducción	1

Capítulo I

El problema

N°	Descripción	Pág.
1.1	Planteamiento del problema	3
1.2	Formulación del problema	4
1.3	Sistematización del problema	4
1.4	Objetivos de la investigación	4
1.4.1	Objetivo general	4
1.4.2	Objetivos específicos	4
1.5	Justificación e importancia	5
1.6	Delimitación	5
1.7	Hipótesis	6
1.8	Análisis de variables	6
1.9	Variable dependiente	6
1.10	Variable independiente	6
1.11	Operacionalización de las variables	6

Capítulo II

Marco Teórico

N°	Descripción	Pág.
2.1	Antecedente de la investigación	7
2.2	Marco Teórico	8
2.3	Evolución de los porteros electrónicos	8
2.4	Reconocimiento Facial	10
2.5	Técnicas de reconocimiento facial	11

N°	Descripción	Pág.
2.5.1	Técnicas basadas en apariencia.	12
2.5.2	Técnicas basadas en modelos.	13
2.6	Algoritmos de reconocimiento facial.	13
2.6.1	Técnica PCA.	13
2.6.2	Técnica LDA.	14
2.6.3	Técnica 3D.	15
2.6.4	Técnicas de Análisis de la Textura de la Piel.	15
2.6.5	Patrón binario Local (LBP).	15
2.6.6	Descripción del algoritmo LBP	16
2.6.7	Extracción de las características faciales	17
2.7	Biometría facial.	18
2.7.1	Técnicas de biometría facial	18
2.7.1.1	Eigenfaces	18
2.7.1.2	FisherFaces	19
2.8	Reconocimiento del rostro	19
2.8.1	Distancia euclidiana en Python	19
2.9	Software de reconocimiento facial.	20
2.9.1	Microsoft Visual Studio	20
2.9.2	EmguCV	20
2.9.3	OpenCV	21
2.10	Microcontroladores	21
2.11	Xampp	23
2.12	Raspbian	24

N°	Descripción	Pág.
2.13	Módulos de la cámara Raspberry Pi	25
2.14	Relé	26
2.15	Cerradura solenoide	28
2.16	Marco Contextual	29
2.17	Marco conceptual	30
2.17.1	Algoritmo	30
2.17.2	Base de datos.	30
2.17.3	Cerradura electrónica.	30
2.17.4	Control de sistemas.	31
2.17.5	Microcontrolador	31
2.17.6	Patrones	31
2.17.7	Reconocimiento facial.	31
2.17.8	Técnica	32
2.18	Marco legal	32

Capítulo III

Metodología y Propuesta

N°	Descripción	Pág.
3.1	Propuesta	34
3.2	Metodología	34
3.3	Enfoque de la investigación	34
3.4	Método de la investigación	34
3.5	Método de diseño.	35
3.6	Instrumento de Investigación	37
3.6.1	La encuesta.	37

N°	Descripción	Pág.
3.6.2	Tabulación y análisis de datos de las encuestas.	37
3.6.3	Determinación del tamaño de la muestra	37
3.6.4	Resultados de la encuesta	38
3.7	Factibilidad técnica	49
3.8	Factibilidad Operacional	50
3.9	Esquema general del proyecto	50
3.10	Proceso de versión de control	52
3.10.1	Estructura de la base de datos	52
3.10.1.1	Información de ambiente de Programación	52
3.10.2	Servidor XAMPP	53
3.10.3	Implementación de servidor de correo electrónico	54
3.10.4	Activación del puerto GPIO5 de la Raspberry	55
3.10.4.1	Diagrama del circuito del portero electrónico	55
3.11	Resultados	56
3.11.1	Descripción de la funcionalidad	56
3.11.2	Registro de Control de acceso	57
3.11.3	Control de Acceso	58
3.11.4	Funcionamiento de portero en conexión	60
3.12	Notificación vía correo electrónico	61
3.13	Pruebas de funcionamiento	61
3.14	Conclusiones	64
3.15	Recomendaciones	64
	Anexos	66
	Referencia bibliográfica	89

Índice de tablas

N°	Descripción	Pág.
1	Operacionalización de las variables	6
2	Diferencias entre módulos	21
3	Lista de variables para la determinación de la muestra.	38
4	Uso de control de. acceso	39
5	Conocimientos sobre el sistema de reconocimiento facial.	40
6	Opinión sobre la aceptación de un portero electrónico con reconocimiento facial como control de acceso.	41
7	Opinión sobre el presupuesto.	42
8	Ventajas de un portero electrónico con reconocimiento facial.	43
9	Herramienta tecnológica de confort.	44
10	Viabilidad del uso del prototipo de Portero electrónico a comparación con las tarjetas.	45
11	Grado de satisfacción como usuario en cuanto al prototipo	46
12	Consideración ante las expectativas de funcionalidad del prototipo.	47
13	Grado de satisfacción para el usuario al utilizar su propio rostro como acceso.	48
14	Software	49
15	Hardware	49
16	Descripción de la Base de datos	52
17	Estructura del ambiente de Programación	53
18	Detalles de la configuración de correo	54
19	Efectividad y precisión de la simulación del control de acceso	62

Índice de figuras

N°	Descripción	Pág.
1	Portero de primera generación.	9
2	Portero de segunda generación.	9
3	Portero de tercera generación	9
4	Reconocimiento facial	10
5	Diagrama que muestra una propuesta de taxonomía para las técnicas de reconocimiento facial.	12
6	Componentes principales o eigenfaces	13
7	Ficherfaces	14
8	Patrones Binarios Locales.	15
9	Alineación de vecinos	16
10	Ejemplo básico de operador LBP	17
11	OpenCv y Raspberry Pi,	20
12	Raspberry pi3	22
13	XAMPP	22
14	. Raspbian	23
15	Cámara Rasperry	24
16	Cámara Rasperry Pi NoIR	25
17	Estructura de un relé	26
18	Relé	26
19	Diagrama electrónico de conexión a Rasperry	27
20	Cerradura solenoide 12V.	27
21	Estructura de un selenoide	28
22	Gestores de base de datos	29
23	Diseño de la investigación	36
24	Uso de control de acceso	39

N°	Descripción	Pág.
25	Conocimientos sobre el sistema de reconocimiento facial	40
26	Opinión sobre la aceptación de un portero electrónico con reconocimiento facial como control de acceso	41
27	Opinión sobre el presupuesto	42
28	Ventajas de un portero electrónico con reconocimiento facial.	43
29	Herramienta tecnológica de confort	44
30	Viabilidad del uso del prototipo de Portero electrónico a comparación con las tarjetas	45
31	Grado de satisfacción como usuario en cuanto al prototipo	46
32	Consideración ante las expectativas de funcionalidad del prototipo.	47
33	Grado de satisfacción para el usuario al utilizar su propio rostro como acceso	48
34	Diagrama del diseño del sistema de control de acceso	50
35	Diagrama de la función del portero electrónico	51
36	Ejecución del código git clone en Github	52
37	Creación de la base de datos “sisfacial”.	53
38	Diagrama del proceso de envío y recepción de notificación por correo.	54
39	Diagrama del circuito eléctrico del portero electrónico	56
40	Menú de Face Access	56
41	Opción de registro de Face Access	57
42	Registro de Face Access	57
43	Imágenes extraídas para el registro en escala de grises	58
44	Usuario desconocido	59
45	Usuario permitido	59
46	Propuesta del diseño físico del portero electrónico automático	60

N°	Descripción	Pág.
47	Notificación del sistema automático de control de acceso.	61
48	Porcentaje de efectividad del diseño del prototipo	63
49	Grado de precisión del sistema automático de control de acceso.	63

Índice de anexos

N°	Descripción	Pág.
1	Reformar la política de seguridad de la información	67
2	Decreto presidencial ante crisis sanitaria	68
3	Encuesta dirigida a empresas de seguridad de la ciudad de Guayaquil	69
4	Bitácora de Compañía de Seguridad en la ciudad de Guayaquil	71
5	Descarga de repositorio de Github	75
6	Instalación de XAMPP	78
7	Programación de “listaPermitidos.py”	80
8	Programación de “Reconocimiento.py”	82
9	Programación de “menu.py”	84
10	Programación de “capture.py”	85
11	Pruebas de funcionalidad en usuarios	86



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

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



**“DISEÑO DE UN PROTOTIPO DE PORTERO ELECTRÓNICO AUTOMÁTICO
CON RECONOCIMIENTO FACIAL MEDIANTE EL USO DE
MICROCONTROLADORES”**

Autor: Veliz Chancay Amarilis Dayana

Tutor: Ing. Sist. Pincay Bohórquez Freddy, Mg.

Resumen

El presente trabajo de investigación tiene como objetivo principal diseñar un prototipo de portero electrónico automático, que su característica principal sea el uso de patrones biométricos faciales, con un sistema automático de control de acceso en tiempo real, denominado “Face Access”, permitiendo la notificación mediante correo electrónico de usuarios permitidos o desconocidos. La metodología a utilizar es: diseño técnico, experimental y esquemático, a su vez el uso de herramientas como encuestas en línea realizada a empresas que prestan servicios de seguridad en la ciudad de Guayaquil, con el fin de resolver las inconsistencias que existen en los sistemas de control de acceso basados biometría facial, validando pruebas de funcionamiento del sistema con diferentes parámetros biométricos dando a conocer su efectividad y precisión mediante el uso de Raspberry Pi como microcontrolador, siendo totalmente viable para su implementación si así se desea.

Palabras Claves: Reconocimiento facial, Algoritmos, Microcontrolador, Base de datos, Patrones.



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

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



**“DESIGN OF A PROTOTYPE ELECTRONIC DOOR ENTRY SYSTEM WITH
FACIAL RECOGNITION USING MICROCONTROLLERS”**

Author: Veliz Chancay Amarilis Dayana

Advisor: Ing. Sist. Pincay Bohórquez Freddy, Mg.

Abstract

The main objective of the present research work is to design a prototype of an electronic door entry system, whose main characteristic is the use of facial biometric patterns, with an automatic access control system in real time, called “Face Access”, allowing notification via email from permitted or unknown users. The methodology to be used is: technical, experimental and schematic design, in turn the use of tools such as online surveys carried out to companies that provide security services in the city of Guayaquil, in order to resolve the inconsistencies that exist in the systems access control system based on facial biometrics, validating system performance tests with different biometric parameters, making known its effectiveness and precision through the use of Raspberry Pi as a microcontroller, being totally viable for implementation if desired.

Keywords: Facial recognition, algorithms, microcontroller, database, patterns

Introducción

La tecnología que se emplea al ingresar a las instalaciones de alguna edificación o vivienda son sistemas que comprenden en una intercomunicación convencional, lo cual facilita la solicitud de acceso, este método de control ha ido desarrollándose con el paso del tiempo y a su vez simplificando varias necesidades según el tipo de usuario y su adaptación, como es el caso de un portero electrónico.

La primera generación del portero electrónico funcionaba con baterías y su fuente de alimentación era totalmente con corriente continua, solo la utilizaban en las viviendas de clase alta, luego con la implementación de transformadores se dejó a un lado el uso de las baterías, ahora se tenía un modelo electromecánico, posteriormente la implementación de micrófonos y el remplazo por los circuitos electrónicos en su estructura, hasta su avance más reciente que es la incorporación de imágenes, se requiere seguir con nuevas automatizaciones derivadas del sistema de control de acceso como el reconocimiento facial.

La automatización como técnica actual se puede implementar mediante el uso de microcontroladores ejecutar programas múltiples a la vez, y así poder controlar a los dispositivos que se conectan a sí mismo, se considera como una opción ideal para este tipo de proyectos ya que es de bajo consumo energético.

Para el diseño del prototipo, en el primer capítulo del documento se encuentra el análisis de todas las características de los elementos necesarios para el diseño del portero electrónico automático, con la finalidad de cumplir con los objetivos establecidos presentan la justificación de la problemática, en el segundo capítulo se muestra la metodología de investigación, el esquema con los elementos fundamentales del sistema y la determinación del algoritmo adecuado para la detección de rostros que se pueda ajustar al prototipo y las técnicas biométricas como mecanismo de autenticación que se emplearán, con la ayuda de la incorporación de cámaras de alta resolución que tengan la capacidad de capturar los aspectos faciales necesarios.

Esto nos permitirá el control sobre la apertura y cierre de la puerta hacia una instalación, es decir añadir como característica principal el reconocimiento del rostro de las personas autorizadas. El reconocimiento de los rostros de un individuo es una tarea que los seres humanos hacen el esfuerzo y de forma rutinaria, en la actualidad el procesamiento digital de imágenes está incluido en varias aplicaciones tales como, interacción entre humano y máquina debido a la inteligencia artificial, además de la identificación biométrica, etc.

Entrenar un sistema de seguridad para el control de acceso bajo ciertas condiciones específicas y lograr que sea posible la detección lo convierte en un reto, en el tercer capítulo se documenta la implementación del proyecto aplicando los elementos previamente seleccionadas desde el análisis de requisitos del prototipo para el correcto funcionamiento tomando en cuenta importantes recursos para el hardware, en el último capítulo se presenta la validación de los resultados del del prototipo y la muestra de su funcionalidad.

Capítulo I

El problema

1.1. Planteamiento del problema

En la actualidad las fallas en los sistemas de control de acceso han permitido implementar una serie de características y funciones con la finalidad de establecer la seguridad física de instalaciones, debido a la ausencia de mecanismos mecánicos, eléctricos o electrónicos que permitan apoyar las actividades realizadas por el equipo de trabajo de seguridad.

La falta de mecanismos de apertura y cierre, como cerraduras electrónicas, consideradas como medidas de protección pasivas, conllevan a que no se permita retardar de manera general la entrada de intrusos que tengan básicamente la intención de causar daños o sustraer cualquier tipo de documento e información de vital importancia para la instalación e incluso pérdidas de objetos o materiales que allí se encuentran. Según la encuesta de Victimización y Percepción de Inseguridad 2011, del Instituto Nacional de Estadística y Censos (INEC), en la prevalencia de delitos a hogares determina que en el Ecuador 4 de cada 100 hogares han sido víctimas por lo menos una vez de robo a la vivienda, registrando con mayor índice delictivo a la Región Oriente, estos resultados fueron declarados información de interés nacional por la junta de Gobierno del INEIGI (Instituto Nacional de Estadística y Geografía).

La ubicación del equipo de control de acceso no suele estar en sitios estratégicos logrando que sean mal manipulados o estén instalados en sitios sin control de seguridad. Dentro de un área controlada al no proveer el acceso a los intereses de protección, tampoco a los materiales documentos e información existentes que se manejan en las áreas limitadas y de exclusión, sin un sistema de control de acceso electrónico correctamente instalado, permite la intromisión de personas no autorizadas, lo que lo convierte en vulnerable ante hechos delictivos ya que no se cumplen los parámetros de seguridad que allí se quiere lograr.

Adicional el mecanismo tradicional o convencional no suele llevar un respaldo de la hora de ingreso del usuario, lo que implica que el sistema de control de acceso en general no brinda la confiabilidad realista, más aún si los usuarios no experimentan un registro basado en imágenes, en el mercado actual se puede encontrar con gran número de aplicaciones de alto nivel sobre este tema, pero no se ofrece la opción de reconocimiento facial para el ingreso, limitándose al uso de credenciales o en uso de llaves.

1.2. Formulación del problema

¿Qué inconsistencias de seguridad existen en los sistemas de control de acceso basados en detección de patrones del rostro, para permitir el acceso de personas autorizadas a través del uso de fotos o videos de un usuario, y la incidencia que tendría diseñar un portero electrónico automático con reconocimiento facial en tiempo real?

1.3. Sistematización del problema

Surge la necesidad de optimizar los procesos al momento del ingreso de un usuario hacia una instalación, mediante el diseño de un prototipo innovad y eficaz, pero sobre todo que brinde la seguridad, a partir de ello se da el inicio a este proyecto de tesis. Como procedimiento de investigación se desea contestar las siguientes preguntas:

- ¿Qué dificultades técnicas se evidencian al momento de realizar el diseño del prototipo de portero electrónico?
- ¿Qué características de funcionalidad se deben tomar en cuenta al momento de realizar pruebas de para el diseño del proyecto?
- ¿Cuáles son las vulnerabilidades existentes en la detección facial en porteros electrónicos?
- ¿Qué beneficios ofrece el diseño de este portero electrónico dentro de una empresa o establecimiento?

1.4. Objetivos de la investigación

1.4.1. Objetivo general.

Diseñar un prototipo de portero electrónico automático con reconocimiento facial mediante el uso de microcontroladores.

1.4.2. Objetivos específicos.

- Analizar las características de los componentes en cuanto a microcontroladores y componentes a utilizar en el diseño del proyecto.
- Describir la funcionalidad de los porteros electrónicos.
- Mostrar el diseño del prototipo mediante esquemas y diagramas de bloque.
- Validar pruebas de funcionamiento del sistema con diferentes datos biométricos.

1.5. Justificación e importancia

Gracias a los avances tecnológicos en la actualidad ha permitido elevar el nivel de confort, en cuanto a procesos de la vida cotidiana, permitiendo que los dispositivos que se utilizan sean capaces de realizar tareas de forma casi autónomas. En este sentido la automatización de equipos o dispositivos se encargan de la regulación o integración de todos los sistemas, entre ellos se tienen: la detección de la presencia de personas, medición de la temperatura, nivel de la luz, entre otros, y al mismo tiempo se puede interactuar entre personas con la ayuda de teléfonos inteligentes (smartphones), pantallas táctiles, Computadoras, Etc.

Este proyecto estará diseñado para ofrecer confort y accesibilidad al momento de acceder al interior de una instalación, el objetivo es que el usuario al momento de ingresar al inmueble no tenga que utilizar botones ni códigos, sino que el desbloqueo de la entrada sea únicamente el reconocimiento facial mediante parámetros biométricos. Este aporte al de sistemas automatizados de electrónica busca determinar si el uso de plataformas de código abierto y de bajo costo provee resultados satisfactorios, lo cual brindaría la posibilidad de extender su uso en diferentes áreas.

1.6. Delimitación

El presente trabajo de investigación tiene como finalidad mostrar el diseño de un prototipo de portero electrónico automático, que tenga como característica principal el uso de patrones biométricos faciales, el control podrá dar paso automáticamente mediante el reconocimiento a cuyos rostros estén guardados dentro del sistema, el registro insertado en la base de datos relacionales como MySQL, permitiendo así que el prototipo mediante una cámara web (usb), capture y procese la imagen, realizando las comparaciones en tiempo real al momento del ingreso a una distancia prudente de máximo 30 cm, este reconocimiento activará el solenoide y la base de datos del personal, la que determinará si es de confianza darle el acceso, la puerta se abrirá permitiendo el ingreso, caso contrario el personal que desee ingresar el sistema lo reconocerá como usuario desconocido, al momento de que el usuario desea ausentarse de cuyo departamento o instalación deberá presionar de forma manual un botón permitiendo así la apertura de la puerta nuevamente.

Se propone analizar varios métodos de factibilidad técnicas para llevar a cabo el diseño, mediante el uso de microcontroladores y demás componentes, además de examinar diferentes plataformas de código libre para la implementación del sistema, detallar las

técnicas y determinar algoritmos necesarios enfocados en el reconocimiento facial que se ajusten mejor al prototipo, con el fin de validar las pruebas de funcionamiento con diferentes rostros para realizar mejoras en el sistema simulado.

1.7. Hipótesis

¿Cómo el diseño de un prototipo de portero electrónico automático con reconocimiento facial aporta a las técnicas de automatización mediante el uso de microcontroladores para así lograr la seguridad de los elementos existentes en una instalación?

1.8. Análisis de variables

1.8.1. Variable dependiente.

Diseño de un prototipo de portero electrónico automático con reconocimiento facial.

1.8.2. Variable independiente.

- a) Aporte a las técnicas de automatización electrónica y control.
- b) Nivel de beneficio de seguridad del portero electrónico.

1.9. Operacionalización de las variables

Tabla 1 Operacionalización de las variables

Variable	Tipo de Variable	Definición	Características para medir	Definición Operacional	Dimensiones
Diseño de un prototipo de portero electrónico automático con reconocimiento facial	Dependiente	Control automático de acceso y confort.	Programación de permisos e identificación de usuarios.	Cualitativo	Recursos técnicos.
Aporte a las técnicas de automatización electrónica y control	Independiente	Evaluación de factibilidad técnica y económica de integración de sistemas automatizados	Sistemas de control y supervisión.	Cualitativo	Recursos técnicos.
Nivel de beneficio de seguridad del portero electrónico	Independiente	Identificación de usuarios no autorizados	Índices de inseguridad.	Cuantitativo	Integridad.

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

Capítulo II

Marco teórico

2.1. Antecedentes de la investigación

El equipamiento que conlleva un portero electrónico es cada vez más popular en todo tipo de empresa, casas unifamiliares, negocios, bloque de viviendas, empresa o cualquier tipo de edificación, es en esta época cuando su éxito se ha instaurado en nuestra sociedad, es por eso que se considera importante lograr entender el funcionamiento del prototipo que se va a desarrollar se necesita entender y conocer las características básica de los porteros electrónicos disponibles que existen en el mercado, así como sus desventajas y las ventajas que puedan conllevar, sobre todo por ser hasta el momento una de las tecnologías innovadoras que se ha desarrollado en este campo.

Aunque el portero electrónico convencional mantiene una cuota importante en el mercado , ya que esta es de uso en domicilios y edificios, en cualquier punto este dispositivo ha dejado de ser solo un elemento para abrir la puerta de las visitas sin salir de una casa u otro inmueble, para luego convertirse en uno de los dispositivos más indispensables para la seguridad dentro de una instalación, está también el hecho de que muchas personas consideran hacer domótico su hogar siendo capaz de automatizarla aportando a la gestión energética, bienestar y comunicaciones, y que puedan estar integrados por medio de redes interiores y exteriores reduciendo el uso de cableado.

Los porteros electrónicos se consideran como uno de los factores más importantes en el mercado, debido al increíble ritmo alcista del sector de la construcción de innovación en los últimos años, por ejemplo en el mercado de los porteros electrónicos se está encontrando con algunos cambios que obligan a una redefinición de la tecnología, así como se está pasando de las tradicionales instalaciones de carácter vertical, es decir, edificios de un único acceso para varios pisos, a instalaciones más complejas como urbanizaciones, edificios con varios cerramientos, sistemas de intercomunicación, etc. La penetración de estos dispositivos está aumentando considerablemente, por lo que se le considera un importante tecnológico para la sociedad.

En la búsqueda de una solución viable y funcional para la adquisición de las imágenes. (Ochoa, 2015) Realizó pruebas con varias cámaras web para determinar el tamaño y calidad de la imagen que se vayan a utilizar, de tal manera que se consiguiera una imagen que tuviera la suficiente resolución para identificar a la persona que tocará la puerta y a su vez, con un

tamaño de archivo pequeño que agilizará su transferencia a través de la red de internet; de esta manera se trata de minimizar el tiempo de respuesta del sistema de portero electrónico. Este producto en el mercado brinda la mayor comodidad y seguridad en diferentes instalaciones permitiendo a los usuarios anticiparse a robos, manteniendo una vigilancia total usándolo como sistema de seguridad y uno de estos medios son los porteros electrónicos, que sirva como prevención al momento del ingreso de personas no identificadas. (Alvear Erazo, 2018).

En los últimos años las técnicas de procesamiento de imagen y video han tomado un rol más significativo en la implementación de esquemas de seguridad basado en sistemas de vigilancia además del análisis de imágenes permite realizar tareas tales como la identificación de criminales o personal autorizado, detección de comportamiento criminal o peligroso, la identificación de vehículos y la determinación de velocidades y comportamiento irregulares de los mismos. (Poveda, Merchan, & Poveda, 2017).

2.2. Marco teórico

En muchas instalaciones el control de acceso forma parte del esquema de seguridad que busca limitar el ingreso a criminales o personas no autorizadas, los esquemas tradicionales implican la identificación del personal autorizado mediante gafetes provistos de alguna de tecnología de identificación, como por ejemplo RFID, que permita acceso a las instalaciones a través de puertas, barreras o molinetes (Poveda, Merchan, & Poveda, 2017).

Los porteros electrónicos cumplen un rol fundamental en el ingreso a la instalación, por ende, automatizar este proceso depende del personal administrativo de tal departamento, se debe considerar que el llevar un registro de los usuarios permitidos y desconocidos aportaría a incrementar la seguridad de dicho espacio, y que mejor oportunidad de aprovechar la tecnología al máximo aportando técnicas biométricas y de reconocimiento de rostros.

2.3. Evolución de los porteros electrónicos

Tomando como referencia la historia de los porteros electrónicos se puede dividir en tres generaciones. La funcionalidad de los primeros porteros eléctricos era totalmente con corriente continua, incluso se denoto que utilizaban zumbadores o mejor conocidos como buzzer (en inglés), de los cuales utilizaban baterías y su concepto derivaba netamente de la telefonía, se usaban principalmente para viviendas unifamiliares de fácil acceso para la clase alta.



Figura N°1. Portero de primera generación. Información tomada de eservicios.com. Elaborado por el autor.

En la segunda generación ya estos dispositivos contenían transformadores, por lo cual se suprimió el uso de las baterías y se independizó su funcionamiento ya que se separó la corriente continua únicamente para el audio y la corriente alterna para el resto del circuito.

Esta fue la generación en la que aparecieron las centrales de portería y la intercomunicación, los mecanismos ya eran electromecánicos e incluso utilizaban relés. Además, se agregan un sistema de video, con cámaras y monitores.



Figura N° 2. Portero de segunda generación. Información tomada de la página [Arquelec](http://Arquelec.com). Elaborado por el autor.

La tercera generación, es decir, en la actualidad se incorporó la amplificación electrónica, en la cual muchos mecanismos electromecánicos han sido remplazados por circuitos electrónicos.



Figura N° 3. Portero de tercera generación. Información tomada de la página surcatel.com. Elaborado por el autor.

El portero electrónico cumple dos funciones las cuales son esenciales; seguridad y comodidad. Ubicado en un lugar estratégico y de fácil acceso para los usuarios, se logra una rápida y efectiva comunicación con la persona que está ingresando a la instalación, con la

ayuda del reconocimiento facial mediante técnica biométricas faciales, con la facilidad de accionar la chapa eléctrica conectada y desbloquear la cerradura y permite abrir la puerta para acceder a una instalación. (Gualpa Carrión, 2017). Con la evolución de los porteros cada vez se han propuesta varios sistemas integrados como:

- Porteros electrónicos
- Porteros Telefónicos
- Porteros con sistema de llamada digital (para reducir conexión por cables)
- Video portero

Los sistemas que están más elaborados incluyen controles de accesos, interfaces con PCs, y otras automatizaciones derivadas del concepto de culpable. Existen varios sistemas de comunicación que se instalan en los edificios, comercios y empresas (Gualpa Carrión, 2017)

- Portero electrónico convencional
- Portero electrónico
- Portero telefónico
- Video portero
- Intercomunicador de ascensor
- Central de consejería
- Control de accesos
- Sistemas de intercomunicación hospitalarios
- Sistemas de intercomunicación para supermercados

2.4. Reconocimiento Facial



Figura N° 4. Reconocimiento facial. Información tomada de cnet.com. Elaborado por el autor.

La tecnología que emplea el reconocimiento facial ha ganado tracción tanto en el sector público como en el privado últimamente, debido a su capacidad para verificar e identificar con precisión a las personas, pero, al igual que con varios procesos tecnológicos en los últimos años, la publicidad ha superado ocasionalmente la realidad. Muchos de los usuarios

tienen altas expectativas de reconocimiento facial y creen en una mentalidad de "configurarlo y olvidarlo".

En realidad, estos sistemas necesitan un nivel de cuidado y alimentación para asegurar el más alto nivel de efectividad. Por ejemplo, debe existir una base de datos de rostros desde donde trabajar para alertar al operador de una persona de interés el origen de esta base de datos debe determinarse.

La naturaleza del sitio también es importante, ya que eso determinará varios factores, por lo que es importante dedicar tiempo a la debida diligencia, más allá de los aspectos tecnológicos, hay factores regulatorios que también deben considerarse al instalar un sistema de reconocimiento facial. Las leyes de privacidad son cada vez más estrictas en todo el mundo y las soluciones biométricas capturan datos confidenciales que garantizan sistemas de protección robustos (digifort, 2019).

Al configurar el algoritmo que mejor se ajuste al prototipo, este codifica automáticamente la imagen facial, realizando de forma exitosa el registro en la base de datos, él de este modo se obtiene una lista de usuarios permitidos, para luego realizar la comparación en tiempo real de los perfiles almacenados en este campo.

De forma obligatoria se lleva a cabo un proceso manual que, al ingresar al menú, la cual permite escoger la opción a realizar durante el inicio, registro y control hacia el sistema que se denominará "Face Access", la cual examina minuciosamente las imágenes previamente guardadas en la base de datos, para verificar los resultados del sistema automático de reconocimiento facial fijándose en las características únicas, con el fin de determinar si se trata de un usuario permitido o desconocido.

2.5. Técnicas de reconocimiento facial

Durante las últimas décadas se han desarrollado un gran número de algoritmos para el reconocimiento facial, según, estos algoritmos se pueden clasificar en dos grandes grupos. En primer lugar, las técnicas basadas en apariencia, que analizan la textura de la imagen a partir de la cual se aplicarán diferentes técnicas estadísticas y se extraerá la información. En segundo lugar, las técnicas basadas en modelos, estas por su parte, extraen las características tanto de la forma del rostro como de la textura de la cara, además dentro de cada una de estas clasificaciones, se encuentran distintos subapartados. En la figura N°5. se muestra de forma más esquemática la clasificación de las técnicas.

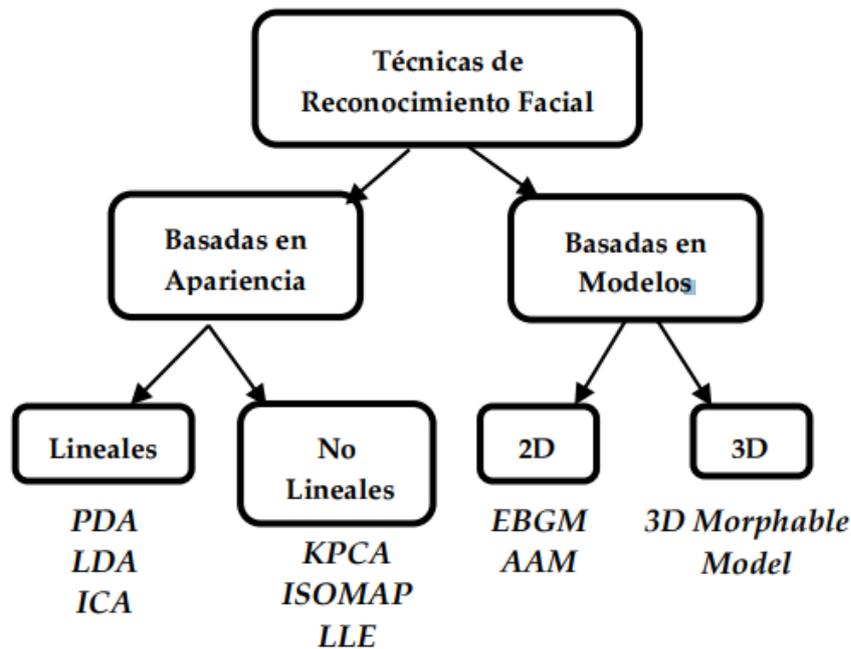


Figura N° 5. Diagrama que muestra una propuesta de taxonomía para las técnicas de reconocimiento facial. Información tomada www.uab.cat, Elaborado por el autor.

2.5.1. Técnicas basadas en apariencia.

Las técnicas basadas en apariencia transforman el problema de reconocimiento facial en un problema de análisis de espacio donde se pueden aplicar diferentes técnicas estadísticas. De este tipo de técnicas destaca su aplicabilidad en imágenes de baja resolución o mala calidad, su rapidez de ejecución ya que se pueden implantar en sistemas en tiempo real, o debido a su baja complejidad. Sin embargo, también tienen varios inconvenientes. Uno de los inconvenientes es que para conseguir buenos resultados se requiere un conjunto de muestras considerable para la fase de entrenamiento. También aspectos como los cambios en la iluminación, la pose o la expresión de la cara tienen un gran impacto en los resultados finales. Dependiendo del método empleado, estos inconvenientes tendrán un impacto mayor o menor. Dentro de las técnicas basadas en apariencia se encuentran las técnicas lineales (con algoritmos como el PCA, el LDA o el ICA) y las no lineales (con el KPCA, el ISOMAP o LLE).

2.5.2. Técnicas basadas en modelos.

Las técnicas basadas en modelos tratan de obtener características biométricas de las imágenes para realizar el reconocimiento, se tienen en cuenta aspectos como la distancia entre los ojos, el grosor de la nariz, el tamaño de la boca, etc. Estos sistemas requieren un conocimiento previo de las imágenes, además de ser más lentos y complejos que los sistemas

basados en apariencia. Sin embargo, son más robustos frente a cambio de orientación o expresión de la cara y se ven menos afectados por cambios en la iluminación o las sombras. Dentro de las técnicas basadas en modelos, cuentan con dos divisiones: las técnicas 2D y las 3D. Las técnicas 2D ofrecen una descripción precisa de las diferentes partes que componen la cara (ojos, nariz, boca...) y diferentes propiedades como la distancia que hay entre las partes. Las técnicas que utilizan imágenes en 3D, en cambio, ofrecen información relativa a la forma, la profundidad y la textura de la cara. Así, las técnicas 3D mejoran los resultados de las técnicas 2D además de poder reconocer caras desde distintos ángulos o perspectivas. Sin embargo, el tiempo de cómputo es superior y en muchas ocasiones se requiere de instrumental de captación especializado.

2.6. Algoritmos de reconocimiento facial

2.6.1. Técnica PCA.

PCA (Principal Component Analysis) es un algoritmo de reducción dimensional que permite encontrar los vectores que mejor representan la distribución de un grupo de imágenes (OpenCV Org, 2017). esta técnica proyecta las imágenes faciales sobre un espacio que abarca las variaciones significativas entre las imágenes faciales conocidas. Estas proyecciones reciben el nombre de componentes principales o eigenfaces. La matriz de transformación está formada por los eigenfaces con los valores más significativos, es decir se obtiene una imagen media de un rostro a partir de los eigenfaces principales (Ramon & Gimeno, 2017). Esta técnica es muy sensible a cambios debido a la iluminación en diferentes imágenes de una misma persona.

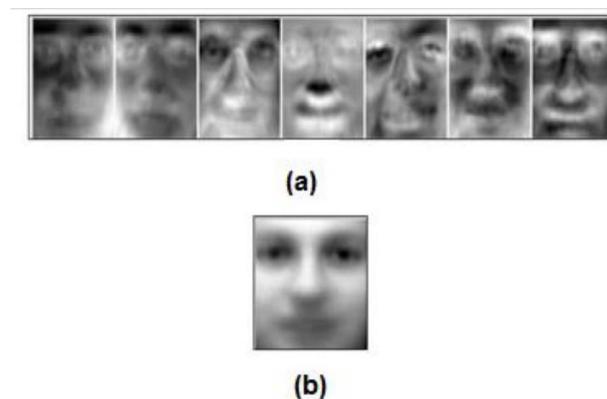


Figura N° 6. Componentes principales o eigenfaces. Información tomada de upcommons.upc.edu. Elaborado por el autor.

2.6.2. Técnica LDA.

(Linear Discriminant Analysis) utiliza la información entre imágenes de la misma persona para crear un conjunto de vectores de características también llamado Fisherfaces, donde las variaciones entre los diferentes rostros se resaltan y los cambios debidos a la iluminación, expresión facial y orientación de la cara no. Es decir, maximiza la varianza de las muestras entre diferentes imágenes, y la minimiza entre muestras de las mismas imágenes. La efectividad de esta técnica depende en gran medida de los datos de entrada (OpenCV Org, 2017). Si las muestras se toman en un ambiente iluminado y se intenta reconocer los rostros en escenas con poca iluminación, entonces el método presentará errores.

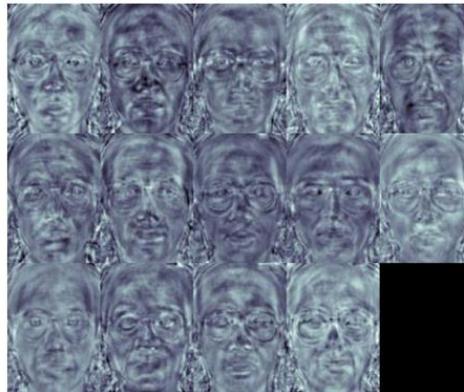


Figura N° 7. Fisherfaces. Información tomada de OpenCVOrg.com. Elaborado por el autor.

Técnica de patrones Locales o Geométricos. En esta técnica se comparan y se extraen diferentes características geométricas de los rostros. Existen dos clases, una está basada en los vectores característicos extraídos del perfil, y la otra a partir de una vista frontal.

2.6.3. Técnica 3D.

Esta técnica utiliza cámaras en 3D para captar información sobre la forma del rostro, posteriormente se la utiliza para identificar los rasgos más significativos como, por ejemplo, la barbilla, el contorno de los ojos, la nariz o los pómulos. Los cambios de iluminación no afectan a esta técnica y puede reconocer un rostro que se encuentre en diferentes ángulos, incluso de perfil. Esto representa una ventaja sobre las otras técnicas (S.Li & Jain, 2015). El principal problema es la dificultad de calibrar y sincronizar las cámaras 3D para obtener imágenes confiables en la fase de reconocimiento.

2.6.4. Técnicas de Análisis de la Textura de la Piel.

Esta técnica utiliza y analiza los detalles visuales de la piel, como, líneas únicas, ciertos patrones, manchas, cicatrices del rostro. Cuando se utiliza este algoritmo no se tiene que buscar en toda la base de datos, ya que se puede descartar imágenes fácilmente resaltando los detalles mencionados. Hay estudios que demuestran que, al unir esta técnica con las técnicas convencionales, el porcentaje de identificación de un rostro puede aumentar hasta un 25% (S.Li & Jain, 2015)

2.6.5. Patrón binario Local (LBP).

Esta técnica consiste en un simple pero eficiente operador de textura, es decir, analiza los rasgos de un rostro por medio de la información de sus píxeles. En cada segmento dividido de un rostro se obtiene un píxel central y otros píxeles alrededor de este, comparando el valor de estos píxeles se obtiene un número decimal, que al final formará un vector o histograma único para cada rostro. La robustez frente a variaciones de iluminación es la propiedad más importante de esta técnica, además, gracias a su simplicidad computacional se puede analizar imágenes en tiempo real (OpenCV Org, 2017)

En la siguiente figura se muestra una imagen con LBPH (Local Binary Pattern Histogram), sometida a diferentes niveles de iluminación.

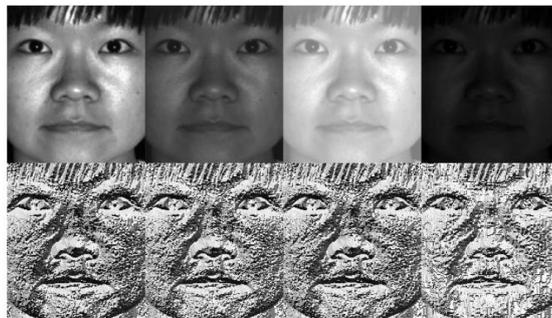


Figura N° 8. Patrones Binarios Locales. Información tomada de OpenCV Org. Elaborado por el autor.

La representación propuesta consiste en dividir la imagen LBP en m regiones más pequeñas y extraer el histograma de cada uno. El Vector de características mejorado se obtiene contactando los histogramas locales (no los fusiona). Estos histogramas se denominan histogramas de patrones binarios locales.

2.6.6. Descripción del algoritmo LBP.

Se calcula un código binario que describe el patrón de la textura local umbral de los vecinos por el valor de gris de pixel central. La expresión para calcular LBP generalizado se indica en la ecuación siguiente:

$$LBP_{(x_c, y_c)} = \sum_{p=0}^{p-1} 2^p (i_p - i_c)$$

Donde (x_c, y_c) es el pixel central con intensidad i_c ; i_n siendo la intensidad del pixel vecino, s es la función de signo definida como se indica en la ecuación

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

Esto permite capturar detalles muy finos en imágenes. Poco después de la publicación del operador, se observó que un vecindario fijo no codifica detalles que difieren en escala. Así que el operador se extendió para utilizar un vecindario variable. La idea es alinear un número abreviado de vecinos en un círculo con un radio variable, lo que permite capturar los siguientes vecinos.

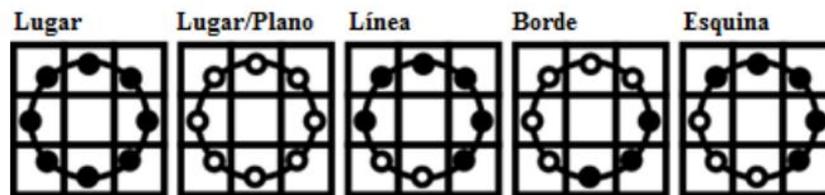


Figura N° 9. Alineación de vecinos. Información tomada de Open Oro. Elaborado por el autor.

Par un punto dado (X_c, Y_c) la posición del vecino (X_p, Y_p) se puede calcular con la ecuación. $X_p = X_c + R \cos(\frac{2\pi p}{p})$ Para la posición en x y con la ecuación $Y_p = Y_c - R \sin(\frac{2\pi p}{p})$ para la posición en y. donde R es el radio del círculo y P es el número de puntos de muestra.

El operador es una extensión de los códigos LBP originales, por lo que a veces se llama Extended LBP (también conocido como LBP Circular). Si su coordenada de puntos en el círculo no corresponde a coordenadas de imagen, el punto es interpolado. Por definición, el operador LBP es robusto contra las transformaciones de grises monótonas. Si la imagen es rotada, estos pixeles a su alrededor de cada vecino se moverán correspondientemente junto al perímetro de la muestra, resultando en un distinto valor de LBP.

2.6.7. Extracción de las características faciales.

La extracción de características en imágenes y secuencias de imágenes faciales consiste en extraer información asociada con la activación de los diferentes músculos del rostro, esta tarea puede realizarse en forma global u holística en donde se analiza el rostro como un solo conjunto o localmente en donde se seleccionan regiones de interés del rostro como ojos, cejas y boca, extracción de características se emplea para obtener la información que resulta relevante de cara a realizar una comparación, durante las últimas décadas se han desarrollado un gran número de algoritmos para llevar a cabo dicha extracción en el ámbito del reconocimiento facial.

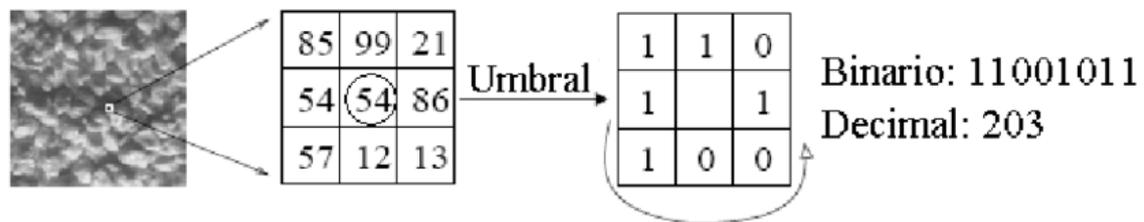


Figura N° 10. Ejemplo básico de operador LBP, Información tomada de ww.uctunexpo.autanabooks.com. Elaborado por el autor.

En la figura N° 10, se muestra un ejemplo de la operación básica LBP para el cálculo de un píxel dado. Una operación de umbralización $S()$ transforma los elementos de la matriz construida a partir de píxel central y sus vecinos, en binarios comparándolos con el valor del elemento central. Los números obtenidos son concatenados en dirección de las manecillas del reloj y un nuevo valor de etiqueta para el píxel central es calculado, el operador LBP es usado a menudo para vecindades circulares con diferentes radios, este descriptor es robusto a cambios de monótonos de iluminación y además relativamente fácil de calcular.

2.7. Biometría facial.

Permite determinar la identidad de una persona analizando su rostro. A diferencia de otras biometrías tipo iris o huella dactilar esta tecnología no es intrusiva y no necesita de colaboración por parte del usuario. Sólo es necesario que su rostro sea adquirido por una cámara web. (EcuRed, 2015)

2.7.1. Técnicas de biometría facial.

- **Sistemas tradicionales:** están basados en la correlación. Van desde la forma más simple, conocido como template matching, (donde únicamente se comparan distintos modelos de reconocimiento), o técnicas que utilizan clasificaciones mediante redes neuronales y plantillas deformables
- **Sistemas locales o geométricos:** en este caso, se analizan vectores característicos extraídos del perfil del individuo que se quiere estudiar, aunque también se pueden comprobar los rasgos que pueden observarse de la vista frontal de la cara.
- **Otras técnicas:** los reconocimientos faciales utilizando análisis tridimensionales (mediante sensores especiales) o las técnicas de estudio de textura de la piel, son las novedades más importantes de la Biometría facial. En el primer caso se determinan rasgos como la barbilla, el contorno de los ojos o los pómulos. Por otra parte, en el segundo análisis se comprueban detalles como líneas únicas, patrones faciales, manchas o cicatrices.

Por último, la Biometría facial también ha integrado en los últimos años sistemas de reconocimiento mediante vídeo. El problema de utilizar estos sistemas de videovigilancia (habituales en controles de seguridad), es la baja calidad de las imágenes grabadas, así como el pequeño tamaño con el que se observan las caras en estos estudios. (EcuRed, 2015)

2.7.1.1. *Eigenfaces.*

En una imagen de entrada existen componentes principales o características comunes como: ojos, labio, nariz y distancias entre estos componentes, esos componentes principales son llamados eigenfaces. El algoritmo de reconocimiento de rostro Eigenfaces sigue los siguientes pasos: El primer paso es poseer un conjunto de imágenes de entrenamiento de diferentes personas, compuesto en lo posible de subconjuntos de imágenes para cada persona que contengan diferentes posturas, condiciones de iluminación, etc. Este proceso es conocido como etapa de entrenamiento, donde las imágenes poseen el mismo tamaño. (Ezpinoza Olguín & Jorquera Guillen , 2015).

2.7.1.2. *FisherFaces*

Esta técnica considera las imágenes de entrenamiento de un mismo individuo como clases, por lo tanto, existen el mismo número de clases que personas. Una vez definida las clases se procede a calcular dos matrices: la matriz de dispersión entre clases y la matriz de dispersión dentro de clases. Una vez calculada estas matrices se obtiene una matriz de

proyección donde cada columna será la base del nuevo subespacio, denominada Fisherfaces. (Belhumeur, Hespanha , & Kriegman , 2018)

2.8. Reconocimiento del rostro

Los histogramas son construidos, por las etiquetas de los píxeles. Una concatenación de todas las descripciones para cada bloque lleva a la obtención de la geometría global del rostro codificada en un solo vector. Las ventajas de tales propuestas radican en su robustez a cambios en la pose, expresión e iluminación.

Finalizada la extracción de características se llega a la última fase, cuyo objetivo es determinar qué imagen del conjunto de entrenamiento es más parecida a la imagen de la base de datos, a partir de sus representaciones mediante las LBP. Para calcular la distancia se usa la distancia euclídea con el fin de tomar una decisión

En esta fase se analiza la distancia entre la proyección de la imagen del usuario donde se quiere hacer el reconocimiento y las correspondientes a las imágenes de entrenamiento en la base de datos. El resultado corresponderá con el acierto que se obtuvo en reconocer al usuario con respecto a las cien imágenes almacenadas.

2.8.1. Distancia euclidiana en Python.

La distancia euclídea es una de las medidas más básicas para calcular distancias. Esta distancia se define como la distancia directa entre dos puntos en un plano. El ejemplo más claro es la distancia entre dos puntos en un plano de dos dimensiones de coordenadas x e y. Si tuviéramos dos puntos P1 y P2 con coordenadas (x1, x1) y (x2, y2) respectivamente, el cálculo de la distancia euclídea entre los mismos sería

$$d_E(P_1, P_2) = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2}$$

Se deduce a partir del teorema de Pitágoras. En general, la distancia euclídea entre dos puntos $P = (P_1, P_2)$ y $Q = (Q_1, Q_2, \dots, Q_n)$ en el espacio euclídeo n-dimensional vendría definida como:

$$d_E(P, Q) = \sqrt{\sum_{i=1}^n (P_i - Q_i)^2}$$

2.9. Software de reconocimiento facial

2.9.1. Microsoft Visual Studio.

Microsoft Visual Studio es un entorno integrado (IDE, por sus siglas en inglés) para sistemas operativos Windows. Soporta múltiples lenguajes de programación tales como C++, C#, Visual Basic .NET, F#, Java, Python, Ruby, PHP; al igual que entornos de web como ASP.NET MVC, Django, etc., a lo cual sumarle las nuevas capacidades online bajo Windows Azure en forma del editor Mónaco. También es compatible con XML / XSLT, HTML / XHTML, JavaScript y CSS. Visual Studio permite a los desarrolladores crear aplicaciones, sitios y aplicaciones web, así como servicios web en cualquier entorno que soporte la plataforma .NET (a partir de la versión .NET 2002). Así se pueden crear aplicaciones que se comuniquen entre estaciones de trabajo, páginas web, dispositivos móviles, dispositivos embebidos, consolas, etc. (Microsoft, 2015)

2.9.2. EmguCV.

Es una plataforma cruzada .Net ligada a la librería de Intel OpenCV de procesamiento de imágenes, permitiendo que las funciones de OpenCV sean llamadas desde .Net, compatible con lenguajes como C#, VB, VC ++, etc. EmguCV está escrito en C#, puede ser compilado en forma Mono (Monodevelop) por lo cual puede ejecutarse en cualquier plataforma que contenga la forma Mono, incluyendo Linux/Solaris y Mac. Es necesario descargar todos los dlls que vienen incluidos en EmguCV para el uso de esta plataforma (Microsoft, 2015)

2.9.3. OpenCV.

OpenCV viene de las siglas Open Source Computer Vision Library, es una librería abierta desarrollada por Intel en el año 1999, contiene alrededor de 500 funciones. Esta librería proporciona un alto nivel de funciones para el procesado de imágenes. Algunas de las características que permite OpenCV son operaciones básicas, procesamiento de imágenes, análisis estructural, análisis de movimiento, reconocimiento del modelo, reconstrucción 3D, calibración de cámara, etc. (Bradski & Kaehler, s.f.)



Figura N° 11. OpenCv y Raspberry Pi, Información tomada de booleanbite.com. Elaborado por el autor.

La biblioteca de visión de computadora de código abierto denominada como OpenCV, es una biblioteca de empleo útil en este diseño de sistema de control de acceso, ya que entre sus características están, reconocimiento de texto, detección de objetos, aprendizaje automático, creación de mapas de profundidad y entre ellos el reconocimiento facial. A partir de ahí, se realizará operaciones de imagen en la Raspberry Pi 3 para reconocimiento facial con OpenCV y Python.

2.10. Microcontroladores

Los bloques de funcionamiento de un microcontrolador son similares a los de una computadora lo que nos permite tratarlo como un pequeño dispositivo de cómputo, ajustable a cualquier tipo de sistema operativo, para que pueda ser configurado y establecer las librerías necesarias para que el funcionamiento del sistema sea autónomo.

Se analizará los diversos tipos de hardware que pueden ser utilizados en el diseño del prototipo de portero electrónico con reconocimiento facial, para sí lograr definir el microcontrolador a utilizar en el proyecto.

A continuación, se puede observar distintos módulos y su comparación:

Tabla 2. Diferencias entre módulos

Características/ Tarjetas de	CPU	Procesador	Codificador de video	Cámara	Conectividad Wireless	Costo	Facilidad de adquisición
Banana BPI-M64	PI ARM Mali-400MP2	Allw inner A64 bit cuádruple núcleo Cortex A53 procesador @1.2 Gz	H264 hasta 1080p@60fps	MPI CSI	WIFI 802.11 b/g/n (2.4Ghz) y BT 4.0 LE	\$85	Dentro del país
Raspberry Pi 3	ARM1 @700MH	Boadcom BCM2837 cuádruple núcleo córtex A53 procesador @1.2 GHz(4x-2760 DMIPS)	Full HD H264 codificación de video	MPI CSI	WIFI 802.11 b/g/n (2.4Ghz) y BT 4.1 LE	\$150	Dentro del país
ODROID-C2	Quintuple núcleo (3+2) ARM Mali-450	Amlogic S905 cuádruple núcleo Cortex A53 procesador @3.0 Ghz(4x-4600 DMIPS)	H264 hasta 1080p@60fps	No CSI	No WIF-BT	\$55	Fuera del país
Arduino UNO	N/A	ATMega 32B	N/A	N/A	N/A	\$15	Dentro del país

Información tomada del trabajo de titulación, Elaborado por Amarilis Dayana Veliz Chancay

Después de analizar las características de los módulos con los cuales se puede realizar visión artificial, se ha determinado que la mejor opción es la Raspberry pi3 porque tiene mejores ventajas como: su codificación de video, CPU, procesador y cumple con las especificaciones tanto de hardware como software que se va a requerir en este proyecto. Una de las desventajas que se puede presenciar es su costo elevado, pero recompensa el hecho de que es asequible dentro del país.



Figura N° 12. Raspberry pi3. Información tomada de xataka.com. Elaborado por el autor.

2.11. Xampp



Figura N° 13. XAMPP. Información tomada de Google.com. Elaborado por el autor.

Es una distribución de Apache pequeña y ligera que contiene el desarrollo web más común tecnologías en un solo paquete. Su contenido, pequeño tamaño y portabilidad la convierten en la herramienta ideal para estudiantes desarrollando y probando aplicaciones en PHP y MySQL. Como su nombre lo indica, la versión ligera es un pequeño paquete que contiene el servidor HTTP Apache, PHP, MySQL, phpMyAdmin, Openssl y SQLite.A. (Fastly, 2020)

A continuación, se describen los componentes de XAMPP:

- **Apache:** el servidor web de código abierto es la aplicación más usada globalmente para la entrega de contenidos web. Las aplicaciones del servidor son ofrecidas como software libre por la Apache Software Foundation.
- **MySQL/MariaDB:** conMySQL, XAMPP cuenta con uno de los sistemas relacionales de gestión de bases de datos más populares del mundo. En combinación con el servidor

web Apache y el lenguaje PHP, MySQL sirve para el almacenamiento de datos para servicios web. En las versiones actuales de XAMPP esta base de datos se ha sustituido por MariaDB, una ramificación (“Fork”) del proyecto MySQL.

- **PHP:** es un lenguaje de programación de código de lado del servidor que permite crear páginas web o aplicaciones dinámicas. Es independiente de plataforma y soporta varios sistemas de bases de datos. Se utiliza este lenguaje debido a su simplicidad, ya que está preparado para realizar diversas aplicaciones web, gracias a la extensa librería y funciones con las que está dotado gracias a las características avanzadas para la programación del sistema de reconocimiento facial, que conlleva al correcto funcionamiento del portero electrónico.
- **Perl:** este lenguaje de programación se usa en la administración del sistema, en el desarrollo web y en la programación de red. También permite programar aplicaciones web dinámicas. (Digitalguide-IONOS, 2019)

2.12. Raspbian

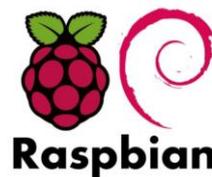


Figura N° 14. Raspbian. Información tomada de xatakahome.com. Elaborada por el autor.

Raspbian es el sistema operativo recomendado para Raspberry Pi (al estar optimizado para su hardware) y se basa en una distribución de GNU/Linux llamada Debian.

Para instalar Raspbian en nuestra Raspberry Pi disponemos de dos versiones; una más completa con entorno gráfico y otra más reducida sin entorno gráfico:

- **Raspbian Pixel:** Versión completa con entorno gráfico de Raspbian, es decir, la versión de escritorio con menús, ventanas, iconos, fondos de pantalla, etc. utilizado por la mayoría de los usuarios como ordenador de sobremesa.
- **Raspbian Lite:** Versión reducida sin entorno gráfico, es decir, la versión en modo consola sin gráficos. Esta opción generalmente es para usuarios avanzados con conocimientos de Linux que utilizan la Raspberry Pi como servidor.

Los relevadores principalmente se usan en sistemas que requieran controlar una carga o usar un interruptor que pueda ser controlado eléctrica o mecánicamente. Una de las aplicaciones originales fue usarlos para diseñar máquinas de estado finito o autómatas. Una de las aplicaciones actuales es el de controlar cargas inductivas o resistivas mediante pulsos de control digital. Los relés también son usados en equipos de pruebas, sistemas de comunicación, seguridad, medición, circuitos de potencia., inversores o sistemas de potencia foto-voltaicos. (Torres, 2017)

2.13. Módulos de la cámara Raspberry Pi

Para el diseño del prototipo de portero electrónico automático, el uso de una cámara es imprescindible, se debe establecer cómo configurarlo o adaptarlo la Raspberry correspondiente qué vamos a utilizar, y determinar su compatibilidad. Los Raspberry Pi ofrece un puerto dedicado para añadir una extensión de cámara. al estar integrado en la placa principal, todo es más fácil de instalar y configurar, especialmente en Raspbian.

Primero se necesita habilitar el puerto de la cámara y luego se tendrá una serie de comandos para configurarlos, realizar una visión artificial o la adquisición de imágenes y videos. La Fundación Raspberry Pi ofrece dos modelos de cámara que se muestran a continuación:

Cámara Raspberry pi V2.1



Figura N° 15. Cámara Raspberry. Información tomada de es.rs-online.com. Elaborado por el autor.

Este es el primer modelo disponible, ha sido actualizado en 2018 (para v2). Abre una cámara de alta calidad con un sensor de 8 megapíxeles que te permite obtener imágenes en HD (estáticas de 3280 x 2464 píxeles) y videos a resoluciones de 1080p30, 720p60 y 640x480p90. Este modelo es compatible con cualquier modelo de Raspberry Pi (1,2,3 y probablemente 4) y fácil de instalar en Raspbian.

Cámara Raspberry Pi NoIR

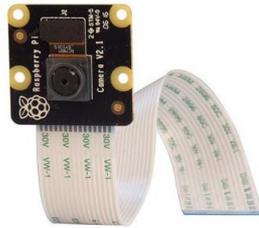


Figura N° 16. Cámara Raspberry Pi NoIR. Información tomada de alibaba.com. Elaborado por el autor.

Este es casi el mismo la versión tienen las mismas capacidades la única diferencia es la capacidad de tomar fotografías por infrarrojo el precio también es un poco más alto, se utiliza a menudo para cámaras de seguridad o para tomar fotos en un entorno de poca luz. La placa de cámara Raspberry Pi NoIR se conecta a cualquier Raspberry Pi o Compute Module para crear fotografías y vídeo HD. La Pi NoIR (sin infrarrojos) es igual que el módulo de cámara estándar, pero sin filtro de infrarrojos. Por tanto, es excelente para fotografía y vídeo en la oscuridad.

El módulo utiliza el sensor de imagen IMX219PQ de Sony que ofrece imágenes de vídeo de alta velocidad y alta sensibilidad. El módulo Pi NoIR ofrece contaminación de imagen reducida como ruido de patrón fijo y borrones. Dispone también de funciones de control automático como el control de exposición, el balance de blancos y la detección de luminancia.

Ventajas

- Infrarrojos
- Imágenes de alta calidad
- Alta capacidad de datos
- Enfoque fijo de 8 megapíxeles
- Compatible con 1080p, 720p60 y VGA90
- Sensor de imagen CMOS Sony IMX219PQ
- Cable plano de 15 contactos

A su vez para la conexión se necesitará de un cable plano de 15 cm fijado a las ranuras del módulo directamente en el puerto de interfaz serie de su cámara Pi (CSI). Una vez conectado, puede acceder a la placa de cámara a través de la capa de abstracción multimedia (MMAL) o el vídeo para API de Linux (V4L). También hay bibliotecas como Picamera Python y muchas otras que puede encontrar en línea. Debe tomar en cuenta que se necesitan LED de infrarrojos para iluminación al utilizar el módulo de cámara Pi NoIR en la oscuridad.

2.14. Relé.

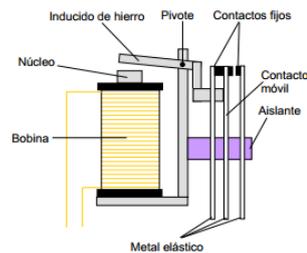


Figura N° 17. Estructura de un relé. Información tomada de josehervas.es. Elaborado por el autor.

Un relé es un dispositivo que hará de interruptor, de cortador de circuitos, es el encargado de abrir un circuito en el cual permitirá a apertura de la puerta, previamente accionado por el sistema de reconocimiento facial, será el encargado de realizar la activación de la puerta existen muchos tipos de relés, a continuación, se muestran los más comunes en el mercado:

Relé electromecánico: Este relé está formado por una bobina que al paso de corriente crea un campo magnético que atrae una pieza metálica, provocando el corte de electricidad. Cuando la corriente cesa, cesa también el campo magnético, la pieza vuelve a su sitio y la corriente se reestablece. Dentro de este tipo de relés hay varios subtipos, de núcleo móvil, reed, armadura, polarizado, pero se basan todos en el mismo principio, con una disposición u otra.

Relé de estado sólido (SSR Solid State Relay): Un relé de estado sólido es un dispositivo de conmutación electrónico en el que una pequeña señal de control controla una carga de corriente o tensión más grande. Esto se hace por medio de transistores. La diferencia fundamental con el relé electromagnético es que este no tiene partes móviles por lo que su vida útil es mucho más larga.

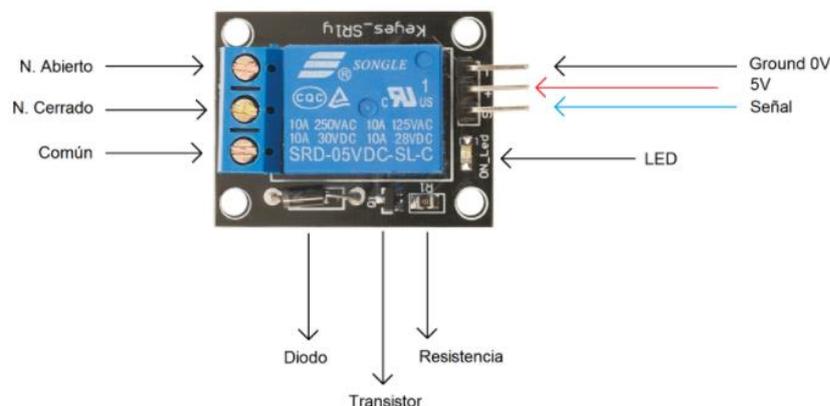


Figura N° 18. Relé. Información tomada de josehervas.es. Elaborado por el autor.

Como se visualiza hay dos partes diferenciadas, una con la parte que se conectará a 220V AC y otra a la que va conectada la electrónica DC. En la parte de AC se distingue que hay 3 contactos, uno con normalidad abierto otro normalmente cerrado y otro común, esto sirve para que cuando el relé esté inactivo, el circuito quede abierto o cerrado. En el sistema de reconocimiento facial será conectada en normalmente cerrado para que a pesar de tener el relé intercalado pueda encender la lámpara manualmente cuando Raspian no actúe. La parte electrónica DC hace referencia al siguiente esquema:

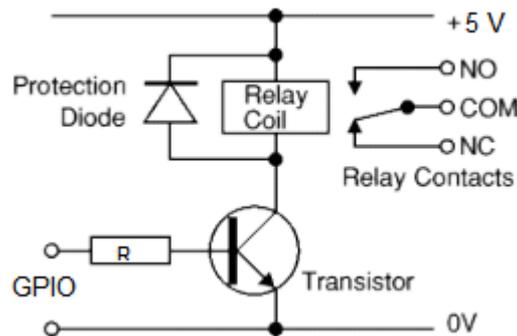


Figura N° 19. Diagrama electrónico de conexión a Raspberry. Información tomada de josehervas.es. Elaborado por el autor.

2.15. Cerradura solenoide

Un solenoide consiste en una bobina de cable eléctrico, ya que es el componente que hace que funcionen los relés y contactores, así como otros elementos electromecánicos. Cuando dicha bobina es alimentada por el voltaje y la corriente apropiados, puede atraer o repeler, acero u otras partes ferromagnéticas. Esas partes, a su vez, se pueden conectar a elementos que hacen un trabajo útil para esta presentación de proyecto, en caso de relés y contactores, será el encargado de abrir la cerradura de la puerta.



Figura N° 20. Cerradura solenoide 12V. Información tomada de e-ika.com. Elaborado por el autor.

Se acota que además es un dispositivo electromecánico, es un tipo de transductor que convierte la energía eléctrica en desplazamiento lineal. Normalmente se utiliza para el accionamiento de válvulas neumáticas o hidráulicas. Consiste en una bobina inductiva enrollada alrededor de una armadura de acero o hierro. La bobina está formada de tal manera que la armadura puede moverse dentro y fuera del cuerpo del solenoide (a diferencia del relé y el contratista). La armadura se usa para proporcionar la fuerza mecánica requerida para que la bobina que empuja y tira de un eje.

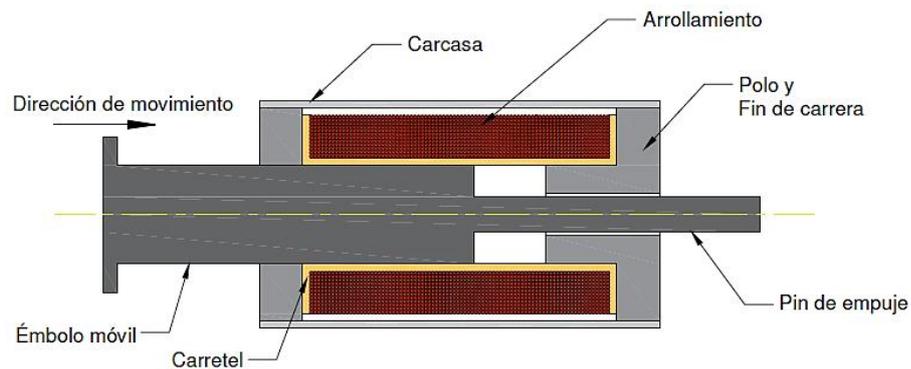


Figura N° 21. Estructura de un solenoide. Información tomada de sc.ehu.es. Elaborado por el autor.

El circuito magnético del solenoide es el camino de las líneas del flujo magnético a través de un medio metálico, tanto como el aire. El patón de estas líneas es toroidal. Las líneas de flujo pasan por el exterior del arrollamiento a través de la carcasa metálica y se concentran en el núcleo del mismo en donde el émbolo se mueve. La eficiencia magnética del solenoide es determinada por la longitud del camino, el entrehierro del circuito magnético y la permeabilidad del material. Por ello la utilización de la carcasa, la cual brinda el retorno de las líneas de flujo de un material de alta permeabilidad, en vez de a través del aire, disminuyendo de esta manera la reluctancia. (Ferreya, 2016)

2.16. Marco Contextual

Se desea plantear el diseño según el ámbito de seguridad, un prototipo de portero electrónico que tenga como función principal el reconocimiento de rostros mediante estándares biométricos elegidos durante la descripción de elementos a utilizar en este proyecto, con la ayuda de un microcontrolador, conectado a una cámara infrarroja, utilizando el algoritmo LBP (Local Binary Patterns) que consiste en llevar imagen integral de un punto, llevar su clasificación en cascada, posteriormente la detección del rostro, procesará la imagen

mediante los datos almacenados en la base de datos, se extraerá las características faciales, para finalmente dar paso al reconocimiento facial utilizando una cerradura electrónica y un relé activador de la cerradura del portero.

2.17. Marco conceptual

Para desarrollar este trabajo de titulación se procederá a obtener conocimientos sobre el significado de cada elemento que se utilizarán en el diseño del prototipo de portero electrónico mediante el reconocimiento facial se detallan a continuación alguno de los términos más substanciales:

2.17.1. Algoritmo.

Un algoritmo se puede definir como una secuencia de instrucciones que representan un modelo de solución para determinado tipo de problemas. O bien como un conjunto de instrucciones que realizadas en orden conducen a obtener la solución de un problema. Los algoritmos son independientes de los lenguajes de programación. Pueden escribirse y luego ejecutarse en un lenguaje diferente de programación. (Robledano, 2019)

2.17.2. Base de datos.

Base de Datos es el conjunto de datos organizados, relacionados y almacenados en un mismo contexto que nos permite guardar grandes cantidades de información. Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en un disco que permite el acceso directo a ellos y un conjunto de programas que manipulan ese conjunto de datos. (Gil Lucero , 2015)



Figura N° 22. Gestores de base de datos. Información tomada de diarlu.com. Elaborado por Amarilis Dayana Veliz Chanca.

2.17.3. Cerradura electrónica.

La cerradura electrónica no es más que una evolución de la mecánica, aquella que todos conocemos por tener cilindro, pestillo, resbalón, engranajes, etc. No obstante, la diferencia se encuentra en su mecanismo, que ya no es “mecánico” como tal, sino electrónico esto quiere decir que ya no hace falta una llave que accione el mecanismo por lo que la gran ventaja de este tipo de cerraduras es el control de acceso que proporcionan limitado y de alta seguridad ya que solo se pueden activar con personas autorizadas que el sistema reconoce como aptas. (Carrod Electrónica Online S. , 2020)

2.17.4. Control de sistemas.

El control de sistemas y procesos está formado por un conjunto de dispositivos de diverso orden. Pueden ser de tipo eléctrico, neumático, hidráulico, mecánico, entre otros. El tipo o los tipos de dispositivos están determinados, en buena medida, por el objetivo a alcanzar. Pero un sistema de control no se establece como tal solo por contar con estos dispositivos, sino que debe seguir la lógica de al menos 3 elementos base: una variable a la que se busca controlar, un actuador y un punto de referencia o set-point. (Gandhi, 2019)

2.17.5. Microcontrolador.

Un microcontrolador es un circuito integrado digital que puede ser usado para muy diversos propósitos debido a que es programable. Está compuesto por una unidad central de proceso (CPU), memorias (ROM y RAM) y líneas de entrada y salida (periféricos). (Sherlin, 2014).

2.17.6. Patrones.

Son formas “estandarizadas” de resolver problemas comunes de diseño en el desarrollo de software.

Las ventajas del uso de patrones son evidentes:

- Conforman un amplio catálogo de problemas y soluciones
- Estandarizan la resolución de determinados problemas
- Condensan y simplifican el aprendizaje de las buenas prácticas
- Proporcionan un vocabulario común entre desarrolladores
- Evitan “reinventar la rueda” (Sánchez, 2017)

2.17.7. Reconocimiento facial.

El reconocimiento facial es una solución biométrica que emplea un algoritmo automático para verificar o reconocer la identidad de una persona en función de sus características fisiológicas. (Kimaldi, 2020)

2.17.8. Técnica.

Una técnica es el concepto universal del procedimiento que se realiza para ejecutar una determinada tarea. En el uso de la técnica se emplean muchas herramientas, con el fin de concretar los objetivos de la responsabilidad adquirida. La técnica no puede considerarse una ciencia o parte de ella, en vista de que las técnicas se generalizan para todo campo en el que sea necesario aplicar un procedimiento o reglaje para hacer algo, según la necesidad que se presente la técnica se adaptara a la situación. (Concepto definicion, 2019)

2.18. Marco legal

Se muestran distintos artículos que obtienen una relación con el tema, que de acuerdo con esta interpretación se consideran los medios que ayudan a ejecutar el proyecto bajo un marco legal. Ver anexo 1. Según la RESOLUCIÓN NO. SEPS-IGT-IGPJ-ISTI-2015-010, de la reforma de seguridad de la información sostiene lo siguiente:

Artículo 1.- OBJETIVOS

- a) Minimizar los riesgos mediante la prevención del incidente de seguridad, reducir su potencial impacto.
- b) Adoptar controles dentro de la institución, para que la información está protegida contra: divulgación a los usuarios no autorizados (confidencialidad) modificación inadecuada (integridad) y sus faltas de acceso cuando se la necesita (disponibilidad).
- c) Plantear estrategias basadas en riesgos y promover un comportamiento responsable en Seguridad de la Información.

Artículo 2.- ALCANCE DE LA APLICABILIDAD

La política de Seguridad de la Información, se aplica para salvaguardar la información física o digital recibida o que sea producto de los procesos gobernantes, agregados de valor, habilitantes de asesoría y de apoyo; información relacionada con la correspondencia almacenada o custodiada en medios digitales o físicos.

La información que se intercambie con otras Instituciones del Estado con organizaciones de la economía de popular y solidaria y la de usuarios externos que presten servicios a la institución estarán regulados a través de los respectivos convenios contratos normas técnicas acuerdo a la confidencialidad y otro que se suscriban para el efecto.

Según la corte Constitucional emite favorable de constitucionalidad a la declaratoria de estado de excepción contenida en el Decreto Ejecutivo Nro.1017 de 16 de marzo de 2020 y establece las siguientes disposiciones que deberán ser observadas durante la vigencia del estado de Excepción.

En ejercicio de las facultades que lo confieren a los artículos 164,165 y 166 de la constitución de la república. (Ver anexo 2)

DECRETA:

Artículo 1.- ESTABLECER como zona especial de seguridad toda la provincia del Guayas, de conformidad a lo dispuesto en el artículo 165, numeral 5, de la constitución de la Republica del Ecuador.

Artículo 2.- DETERMINAR que la zona especial de seguridad requiere de regulaciones especiales, estará conformada por los cantones de la provincia del Guayas y, con especial atención en los cantones de Guayaquil, Daule, Durán y Samborondón, En toda la zona especial de seguridad se realizará una gestión integral en el marco de la emergencia sanitaria y el estado de excepción, que permita mitigar los riesgos, precautelar la salud, proteger la población, evitar el contagio del virus COVID-19 y recuperar las condiciones idóneas para la atención de la emergencia sanitaria.

Artículo 3.- DISPONER a las Fuerzas Armadas la conformación de la Fuerza Tarea Conjunta con mando y medios necesario, misma que establecerá una planificación que incluya una Policía Nacional.

Artículo 4.- DISPONER al gobernador de la provincia del Guayas la dirección de las acciones interinstitucionales en la zona especial de seguridad, para lo cual se articulará con las siguientes autoridades: el General o Almirante designado por el Ministerio de Defensa Nacional, quien estará a cargo de la Fuerza de Mando; la autoridad designada por el Ministerio de Salud Pública, y el Oficial General de la Policía Nacional designado por el Ministro de Gobierno.

Artículo 5.- La zona especial de seguridad determinada en los artículos 1 y 2 del presente decreto estará bajo disposición del Comité de Operaciones de Emergencia Nacional, por lo cual todas las iniciativas y regulaciones que se propongan respecto de la misma, deberán ser aprobadas por esta instancia, previo a su implementación.

Capítulo III

Metodología y Propuesta

3.1. Propuesta

Previo a un análisis de factibilidad técnica y operacional se propone presentar el diseño técnico y esquemático en base a pruebas de funcionalidad por medio de simulaciones de un portero electrónico con reconocimiento facial mediante el uso de Raspberry pi3 como microcontrolador, complementado con la creación de un sistema automático de control de acceso llamado “Face Access”, que permitan la creación de una base de datos de las personas autorizadas, enlazadas a un servidor de correo electrónico donde se recibirán una notificación del ingreso de las mismas y en caso de no pertenecer a dicho registro se emitirá también una alerta de que una persona desconocida ha tratado de ingresar a dicho departamento, espacio o instalación donde se desea ser implementado.

3.2. Metodología

En esta investigación es cuantitativa, y dentro de la investigación cuantitativa el diseño técnico, experimental y esquemático para la descripción de las etapas o fases del desarrollo del sistema de control de acceso del portero electrónico automático con reconocimiento facial, con el fin de llevar a cabo la simulación documentando cada paso y procedimientos.

3.3. Enfoque de la investigación

La orientación del diseño de este prototipo se demostrará en la funcionalidad de un portero no convencional con tecnología de reconocimiento facial, demostrando qué se puede satisfacer la necesidad de cualquier entidad a su vez conseguir una mayor seguridad al llevar un registro de todas las personas autorizadas y las que no estén autorizadas queden en evidencia vía correo electrónico, también se desea conseguir que sus componentes sean de fácil acceso al usuario al igual que la manejabilidad de su sistema de control de acceso, para poder así dar a conocer este proyecto como una opción viable enfocada hacia la seguridad y comodidad del usuario.

3.4. Método de la investigación

Según (Hernandez, Fernandez, & Baptista, 2013) en su libro “Metodología de la Investigación”, detallan que los trabajos de investigación se encuentran sustentados en dos enfoques principales los cuales son: el enfoque cuantitativo y el enfoque cualitativo. El

enfoque de la investigación es un proceso sistemático, disciplinado y vigilado que está directamente enlazado a las formas de investigación. Por lo tanto, durante la elaboración de este trabajo de titulación se describe que el método de diseño cumple con los requisitos que se ajusten a la investigación, con el cual se logrará conseguir los objetivos planteados anteriormente y así constatar las necesidades al momento de la realización de la práctica. La metodología de diseño para el proyecto y a su vez herramientas como encuestas en línea, realizada a una determinada población de personas para así obtener finalmente datos que fueron analizados e interpretados de forma estadística.

3.5. Método de diseño.

Se entiende como método de diseño la forma de representación del proceso que desarrolla el diseñador en su labor. Los modelos y métodos de diseños se pueden enmarcar dentro del campo que los expertos califican como “Investigación de diseño”, cuyo objetivo genérico es establecer nuevas formas o recomendaciones que potencien la eficiencia en el diseño. (Chaur, 2015).

A continuación, se presenta mediante diagrama de flujos la identificación de las etapas o fases que se desarrollaran en el proceso de simulación del proyecto, con el fin de resolver las inconsistencias de seguridad que existen en los sistemas de control de acceso basados biometría facial, demostrando que la incidencia de usar el diseño de un portero electrónico automático con reconocimiento facial en tiempo real mediante el uso de Raspberry Pi como microcontrolador, sería totalmente viable para su implementación si así se desea.

1. Fase de detección

Recolección de 100 imágenes a través de cámara de video a una distancia de 30 cm.

2. Pre-procesado de la imagen

Extracción de la información biométrica, alineación de cara, establecer tamaño de imágenes sin formato, y etiquetarlas.

3. Extracción de las características faciales

La información biométrica de los rasgos faciales e imágenes en escala de grises se almacenan estableciendo patrones binarios por medio del algoritmo LBPH.

4. Fase de registro en la BD

La información de la biometría se almacena en la base de datos llamada “sisfacial”

5. Fase de comparación con la BD de registro

La captura del rostro en tiempo real es comparada con las 100 imágenes de la base de datos determinando su identidad.

6. Fase de toma de decisiones

Se identifica y permite el acceso de la puerta al individuo registrado caso contrario se mostrará la imagen con una etiqueta desconocida la cual no permitirá la apertura del portero electrónico, en ambas situaciones el administrador será notificado vía correo electrónico.

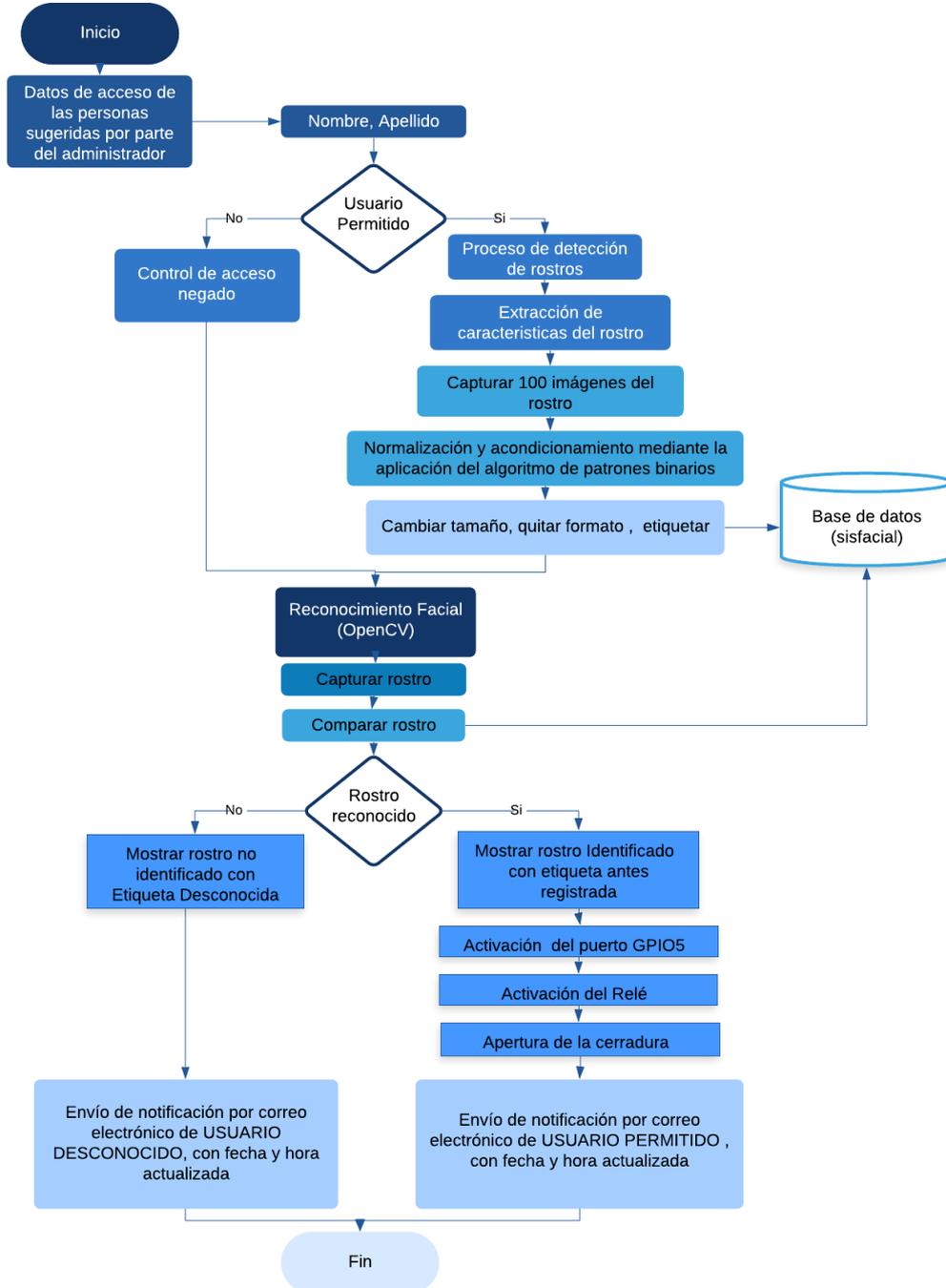


Figura N° 23. Diseño de la investigación. Elaborado por Veliz Chancay Amarilis Dayana.

3.6. Instrumento de Investigación

3.6.1. La encuesta.

Según (Ronsabay, 2014) la encuesta es el estudio que permite mediante una muestra de una población determinada la obtención de información que puede ser utilizada de una forma muy importante para términos de investigación, con datos cuantitativos a preguntas que se desea reflejar de un tema de investigación teniendo como resultado datos estadísticos que permiten la viabilidad de la propuesta.

Para la elaboración de esta tesis se ha tomado en cuenta diferentes factores para la recolección e información utilizando las TICS como medio de recaudo más abundante como la encuesta, misma que fue realizada a través de un formulario en línea, ver anexo 3.

3.6.2. Tabulación y análisis de datos de las encuestas.

La información será tomada de encuestas realizadas en línea las diferentes entidades que prestan servicios de seguridad en la ciudad de Guayaquil. Algunas de ellas se dedican a la importación, distribución y comercialización de equipos de seguridad electrónica, como: alarmas, paneles, sistemas contra incendio, detectores de humo, baterías, sirenas, a nivel nacional, por ende, lo que se lograría con este proyecto es llevar a cabo la propuesta de que se incluya como una opción eficaz y viable, el sistema de acceso mediante reconocimiento facial, para hacer que en estas entidades su avance y nivel tecnológico sea cada vez más evidente.

Como parte de la investigación cuantitativa de este proyecto, debido a la situación actual de pandemia, surge la necesidad de recopilar datos desde el directorio digital del Ecuador (Edina S.A. , 2019), donde consta que en la ciudad de Guayaquil existen 88 compañías de vigilancia y seguridad legalmente constituidas e inscritas en el Registro Mercantil, que cuentan con permisos de operación, información recopilada en una bitácora, ver anexo 4.

3.6.3. Determinación del tamaño de la muestra.

Para determinar el tamaño de la muestra se utilizará la siguiente ecuación

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

Tabla 3. Lista de variables para la determinación de la muestra.

<i>Variable</i>	<i>Descripción</i>	<i>Valores</i>
<i>n</i>	Tamaño de la muestra a calcular.	X
<i>N</i>	Tamaño de la población.	88
<i>Z</i>	Nivel de confianza de la estimación (95%).	1.96
<i>p</i>	Probabilidad de éxito.	0.5
<i>q</i>	Probabilidad de fracaso.	0.5
<i>e</i>	Error máximo admisible (5%).	0.05

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

El valor por encontrar es el tamaño de la muestra (*n*), por ese motivo en la tabla 2 se muestra como incógnita representado por “*x*”.

La resolución de la ecuación del tamaño de la muestra se presenta a continuación:

$$n = \frac{(88)(1.96)^2(0.5)(0.5)}{(88 - 1)(0.05)^2 + (0.5)(0.5)(1.96)^2}$$

$$n = \frac{(88)(3.8416)(0.25)}{(87)(0.0025) + (0.25)(3.8416)}$$

$$n = \frac{84.5152}{0.2175 + 0.9604}$$

$$n = \frac{84.5152}{1,1779}$$

$$n = 71.75$$

$$n = 72$$

Por lo tanto, el número de empresas de seguridad en la ciudad de Guayaquil a encuestar es de 72, una vez conocido el número de la muestra se procede a contactar a las compañías registradas en la bitácora, se determina el medio por el cual le será enviado el enlace del formulario para que procedan con el relleno de esta, posterior análisis en cada respuesta obtenida.

3.6.4. Resultados de la encuesta.

Se realizó la recolección de información necesaria y a la vez la validación de cada una de las respuestas que se utilizaron en la encuesta, logrando, así como resultado un estudio estadístico como se detalla a continuación. La siguiente encuesta está orientada a determinar los requerimientos, sobre los cuales se dará el de un diseño de prototipo de portero electrónico automático con reconocimiento facial mediante el uso de microcontroladores, como parte de investigación de trabajo de titulación.

1. ¿Qué sistema para el control de acceso ha utilizado?

Tabla 4. Uso de control de. acceso

	Nro. de encuestados	Porcentaje
Huella Digital	48	67%
Tarjeta Magnética	8	11%
Reconocimiento facial	11	15%
Otro	5	7%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

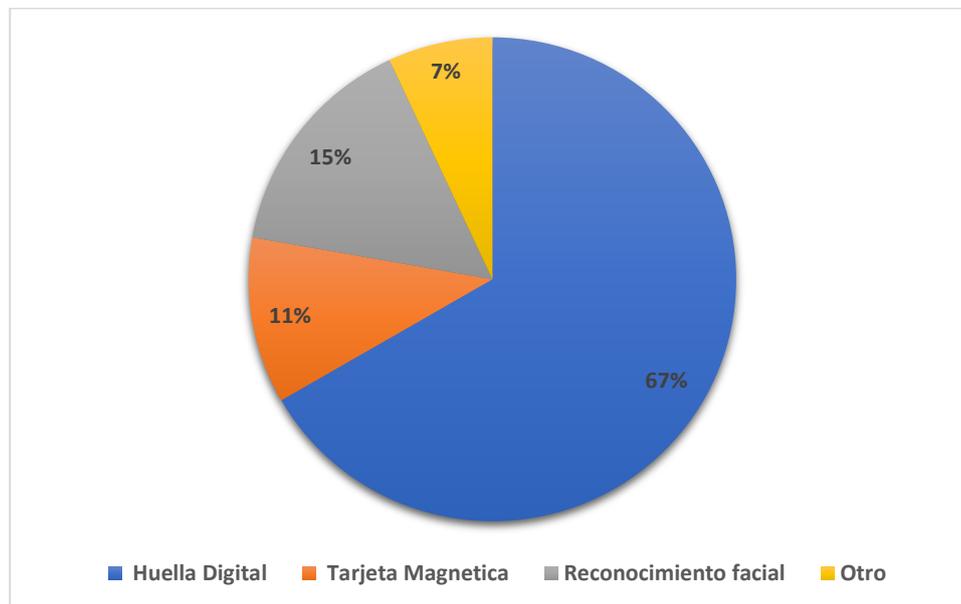


Figura N° 24. Uso de control de acceso. Información tomada de la encuesta realizada en el presente trabajo de titulación, Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. - De los resultados de esta interrogantes se obtiene que el 67% de las empresa de seguridad en la Ciudad de Guayaquil han utilizado la Huella Digital como control de acceso a los diferentes establecimiento o entidades, mientras que un 11% indicó que ha utilizado la Tarjeta magnética, de igual forma, se puede observar que el reconocimiento facial como parte de control de acceso solo lo han usado 11 personas , lo que equivale a un 15%, cifra considerable en comparación con el resto de herramientas utilizadas.

2. ¿Conoce usted en qué consiste el sistema de reconocimiento facial?

Tabla 5. Conocimientos sobre el sistema de reconocimiento facial.

Descripción	Nro. de encuestados	Porcentaje
Si	66	92%
No	6	8%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

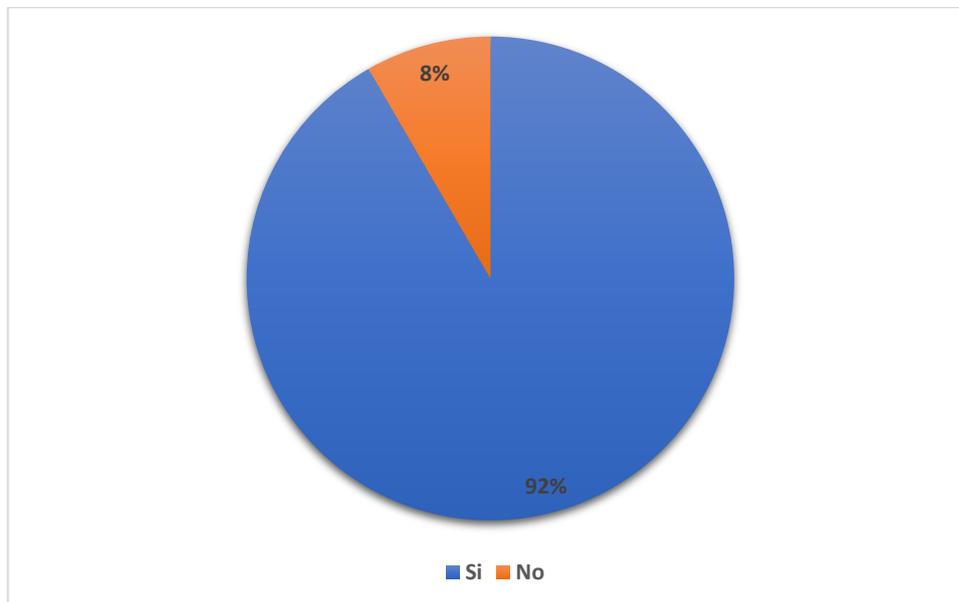


Figura N° 25. Conocimientos sobre el sistema de reconocimiento facial. Información tomada de la encuesta realizada en el presente trabajo de titulación, Elaborado por Veliz Chancay Amarilis Dayana.

Análisis.- La pregunta siguiente resalta los conocimientos que tienen los usuarios y como proveedor de servicios de seguridad acerca de la implementación del reconocimiento facial, en la cual se ha determinado según la encuesta que el 8% de la muestra, no tiene conocimientos sobre este sistema, mientras tanto se tiene como respuesta positiva a un 92%, cifra que no llena las expectativas, por lo tanto, se brindó una breve redacción del significado del sistema, por ende la cifra se considera cambiante.

3. ¿Le gustaría que las entidades a las que presta servicios de seguridad cuenten con un portero electrónico de reconocimiento facial al ingreso?

Tabla 6. Opinión sobre la aceptación de un portero electrónico con reconocimiento facial como control de acceso.

Descripción	Nro. de encuestados	Porcentaje
Si	67	93%
No	5	7%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

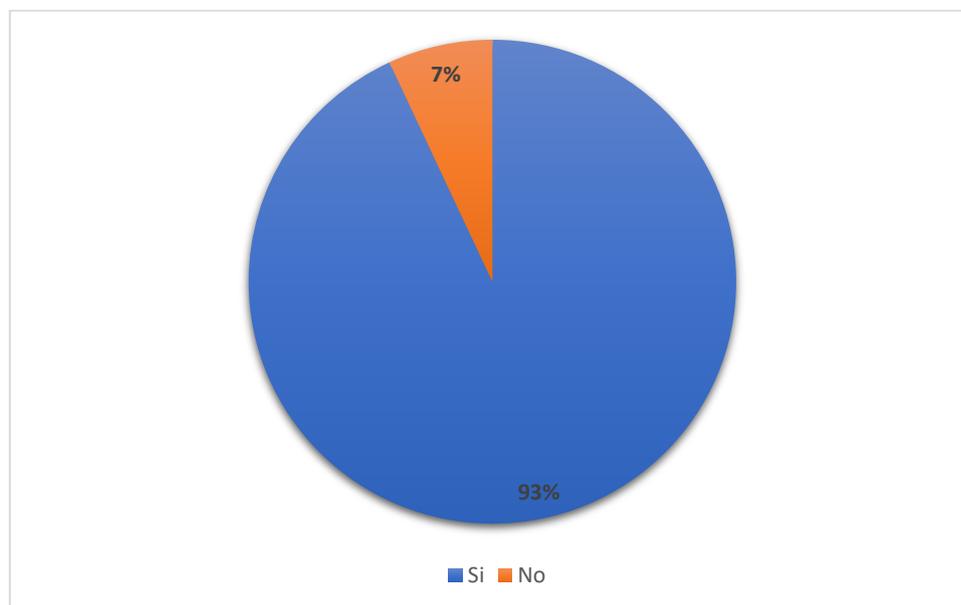


Figura N° 26. Opinión sobre la aceptación de un portero electrónico con reconocimiento facial como control de acceso. Información tomada de la encuesta realizada en el presente trabajo de titulación, Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. - En esta pregunta se evidencia que el 93% de las personas encuestadas están de acuerdo o al menos tienen una respuesta positiva sobre la aceptación a qué se utiliza un portero electrónico con reconocimiento facial en las entidades que se prestan servicio a su vez orientado al usuario y el 7 % opinó diferente.

4. Según su criterio, ¿Cuánto estaría dispuesto a invertir en un sistema de control de acceso con reconocimiento facial?

Tabla 7. Opinión sobre el presupuesto.

Descripción	Nro. de encuestados	Porcentaje
\$0 - \$100	17	24%
\$101 - \$200	20	28%
\$201 - \$300	19	26%
\$301 - más	16	22%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

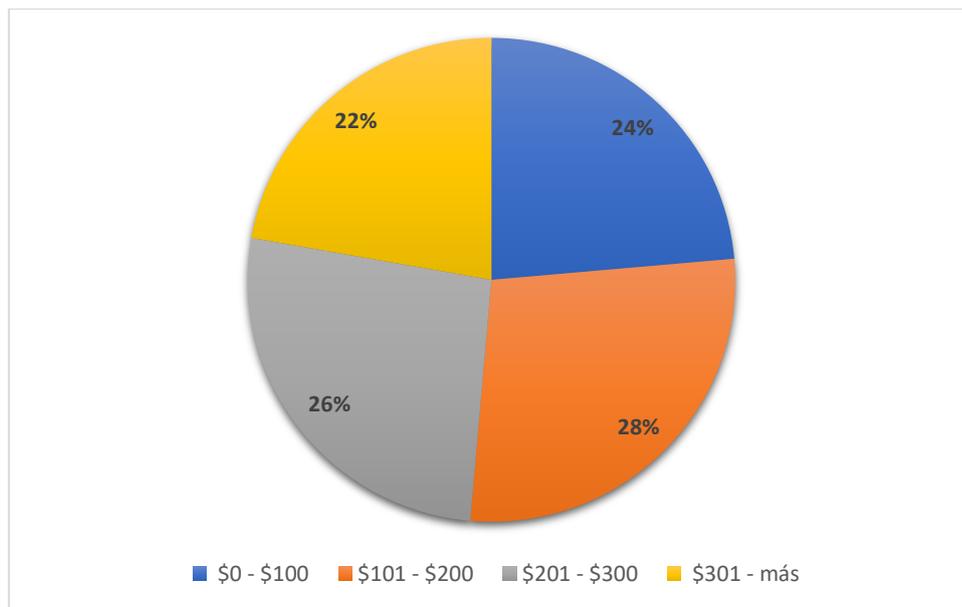


Figura N° 27. Opinión sobre el presupuesto. Información tomada de la encuesta realizada en el presente trabajo de titulación. Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. - Según el criterio de las empresas de seguridad referente al presupuesto que se pueda invertir en este sistema se determina que el 22% está dispuesto a gastar más de 301 dólares, el 26% estaría dispuesto a pagar en el rango de 201 a 300 dólares, el 28% pagaría entre 101 a 200 dólares y para finalizar se visualiza que el 24% de la muestra sólo estaría dispuesto a pagar el mínimo valor de 100 dólares.

5. ¿Cuáles cree usted que son las ventajas de utilizar un portero electrónico con reconocimiento facial?

Tabla 8. Ventajas de un portero electrónico con reconocimiento facial.

Descripción	Nro. de encuestados	Porcentaje
Fácil de usar	10	14%
Alta seguridad	43	60%
No necesito llaves	19	26%
Otro	0	0%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

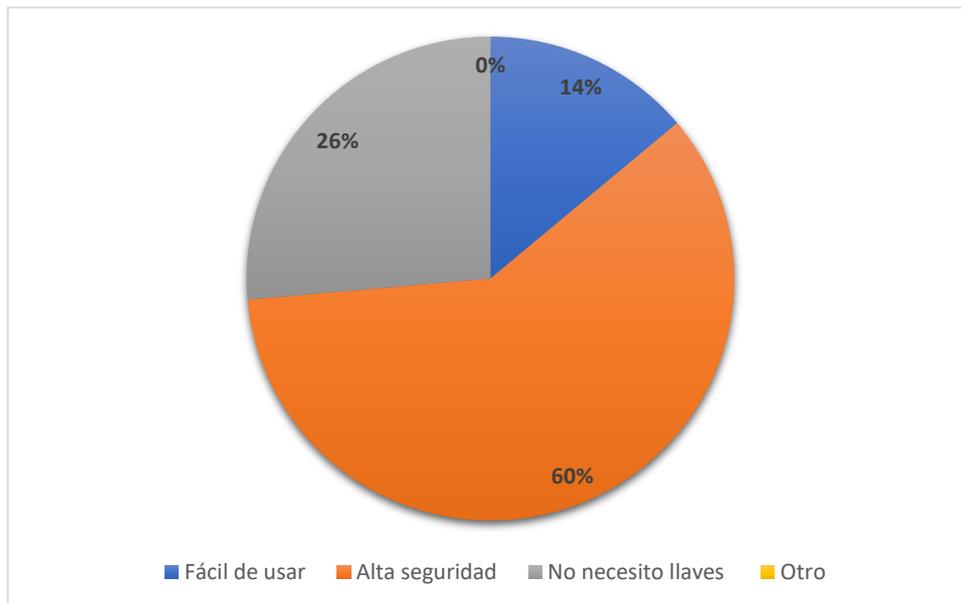


Figura N° 28. Ventajas de un portero electrónico con reconocimiento facial. Información tomada de la encuesta realizada en el presente trabajo de titulación. Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. -Se visualiza que el 60% de las compañías encuestadas considera que una de las ventajas principales de este prototipo será la alta seguridad, el 26% indica que no necesitar llaves para lograr el ingreso hacia una entidad es también una buena ventaja y el 14% se ha dejado influenciar por el fácil de uso que tendría.

6. ¿Qué herramienta tecnológica considera viable para el registro de personal autorizado o no autorizado?

Tabla 9. Herramienta tecnológica de confort.

Descripción	Nro. de encuestados	Porcentaje
Correo electrónico	47	65%
WhatsApp	17	24%
Almacenamiento en La Nube	8	11%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

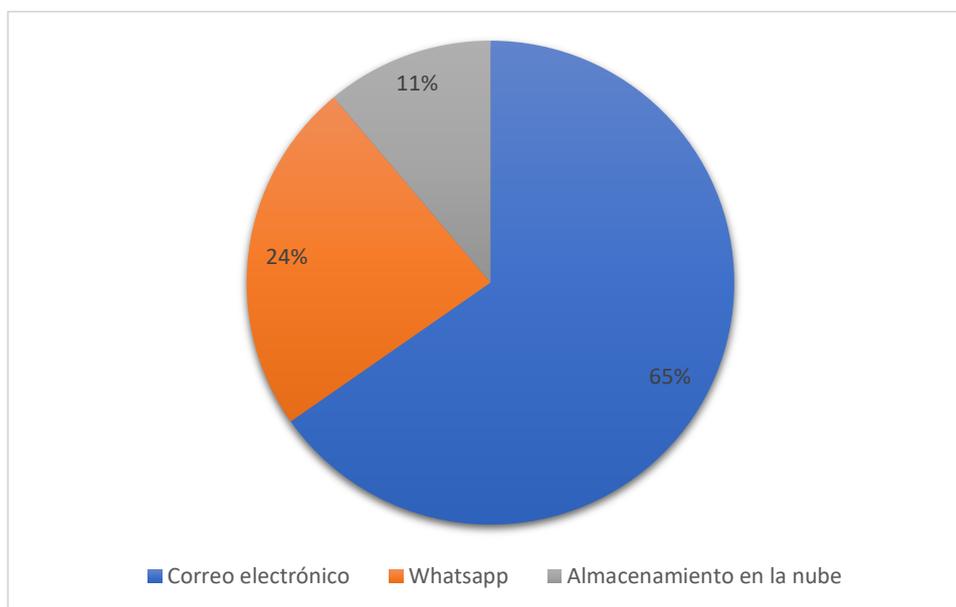


Figura N° 29. Herramienta tecnológica de confort. Información tomada de la encuesta realizada en el presente trabajo de titulación. Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. – Se brindó opciones sobre las herramienta tecnológicas que se considerarían viable para el uso del sistema de control de acceso, según los resultados de esta pregunta encuestada se determina que el 65% de la muestra prefiere utilizar el correo electrónico mientras que el 24% por ciento desea utilizar whatsapp, por otro lado se ofreció como opción el almacenamiento en la nube de la cual se determinó que únicamente el 11% se encuentra interesado en utilizar esta herramienta.

7. ¿Considera viable el uso de un portero electrónico con reconocimiento facial ya que presenta menos errores que la desprogramación de las tarjetas?

Tabla 10. Viabilidad del uso del prototipo de Portero electrónico a comparación con las tarjetas.

Descripción	Nro. de encuestados	Porcentaje
Si	62	86%
No	10	14%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana.

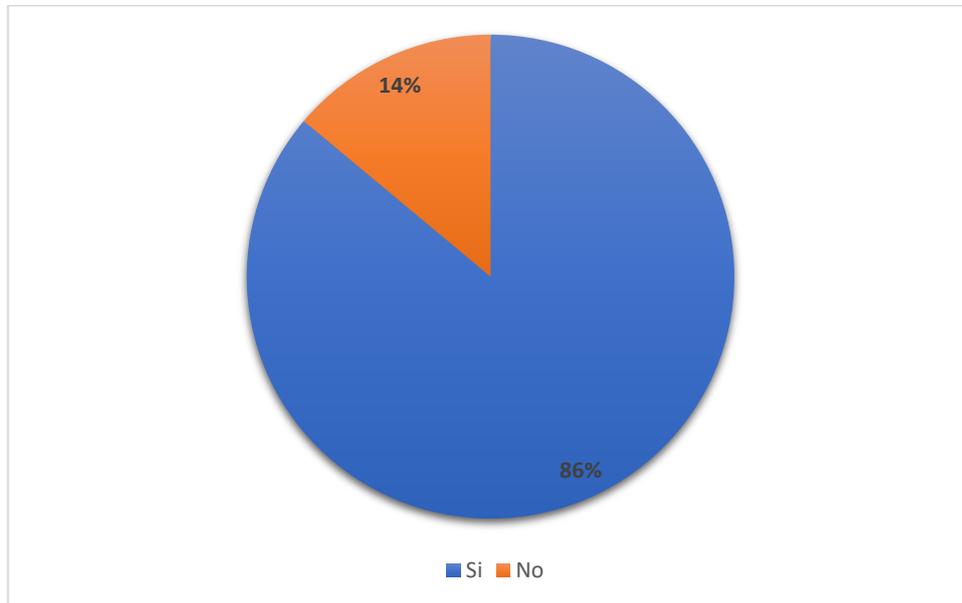


Figura N° 30. Viabilidad del uso del prototipo de portero electrónico a comparación con las tarjetas. Información tomada de la encuesta realizada en el presente trabajo de titulación. Elaborado Veliz Chancay por Amarilis Dayana.

Análisis. – Según los datos de esta pregunta se toma en consideración el prototipo de portero electrónico con reconocimiento facial como un como una alternativa a la utilización de tarjetas magnéticas, por ende, la respuesta que se tuvo pues favorable con un 86% ya que indicaron que si sería viable mientras que por el lado negativo se tiene únicamente al 14%.

8. ¿Cuál es el grado de satisfacción que usted tendría con un portero de reconocimiento facial al ingreso de una instalación?

Tabla 11. Grado de satisfacción como usuario en cuanto al prototipo.

Descripción	Nro. de encuestados	Porcentaje
Muy satisfecho	48	67%
Satisfecho	20	28%
Poco satisfecho	3	4%
Insatisfecho	1	1%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana

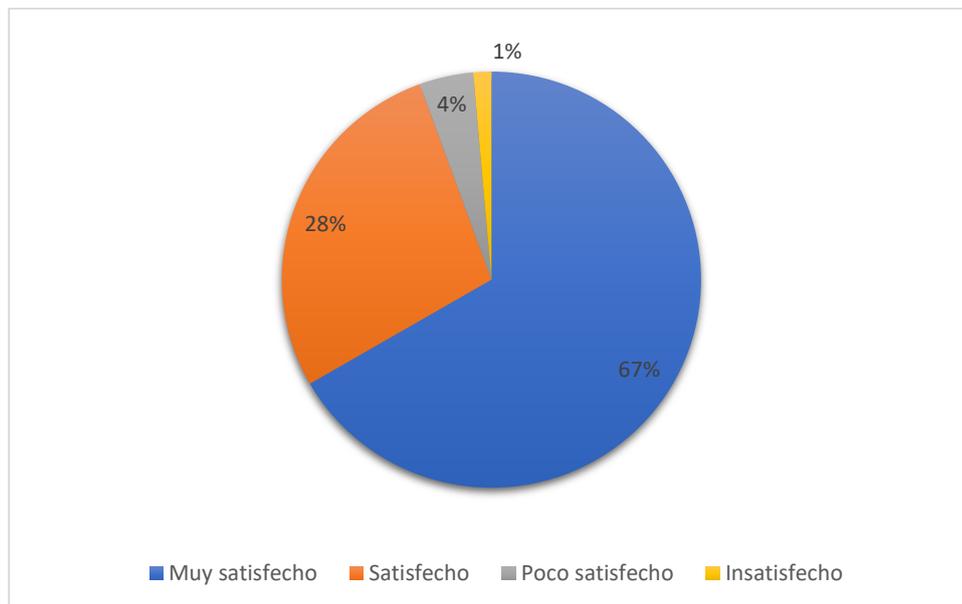


Figura N° 31. Grado de satisfacción como usuario en cuanto al prototipo. Información tomada de la encuesta realizada en el presente trabajo de titulación. Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. - En esta pregunta se trata de medir al grado de satisfacción que como usuario tendrían al utilizar el prototipo de portero electrónico con reconocimiento facial en la cual como resultado se tiene que el 67% de las compañías encuestadas se encontrarían muy satisfechas, mientras que el 28% sería satisfecho, el 4% Poco satisfecho y tan solo el 1% mostró insatisfecho.

9. ¿Considera que la implementación de un sistema de portero electrónico con reconocimiento facial satisface sus expectativas de funcionalidad al ser rápido y sencillo?

Tabla 12. Consideración ante las expectativas de funcionalidad del prototipo.

Descripción	Nro. de encuestados	Porcentaje
Si	68	94%
No	4	6%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana

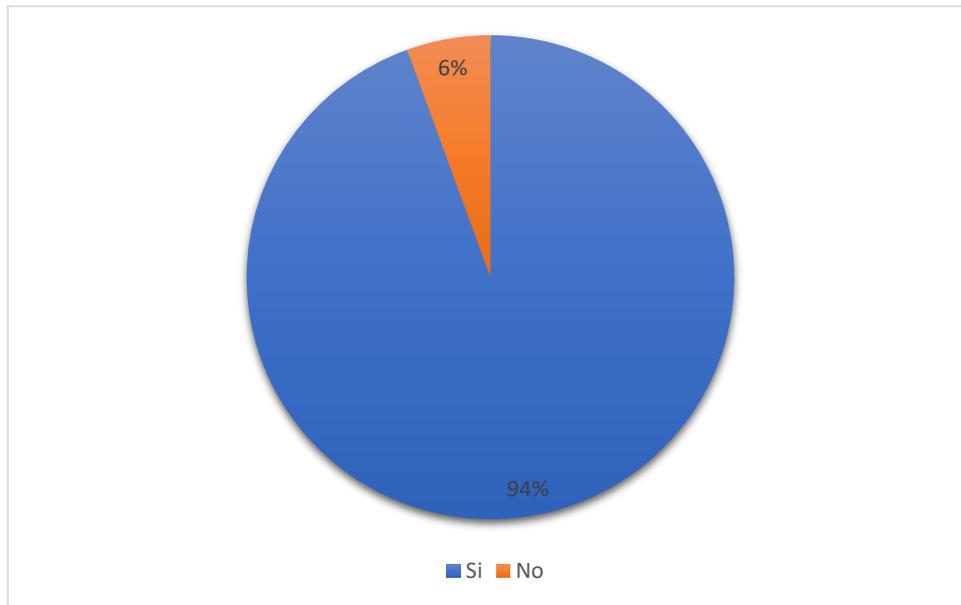


Figura N° 32. Consideración ante las expectativas de funcionalidad del prototipo. Información tomada de la encuesta realizada en el presente trabajo de titulación. Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. – En esta pregunta se requiere determinar si las personas o usuarios en la compañía de seguridad considera que la funcionabilidad del portero electrónico cumple a sus expectativas traduce rápido y sencillo de utilizar en la cual se mostró que el 94 % indicó que sí mientras que el 6% de las compañías indicaron que no.

10. ¿Qué grado de satisfacción le aportaría el hecho de utilizar su propio rostro como acceso ya que mediante este se elimina el uso de tarjetas o llaves?

Tabla 13. Grado de satisfacción para el usuario al utilizar su propio rostro como acceso.

Descripción	Nro. de encuestados	Porcentaje
Muy satisfecho	43	60%
Satisfecho	26	36%
Indiferente	1	1%
Poco satisfecho	1	1%
Insatisfecho	1	1%
Total	72	100%

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana

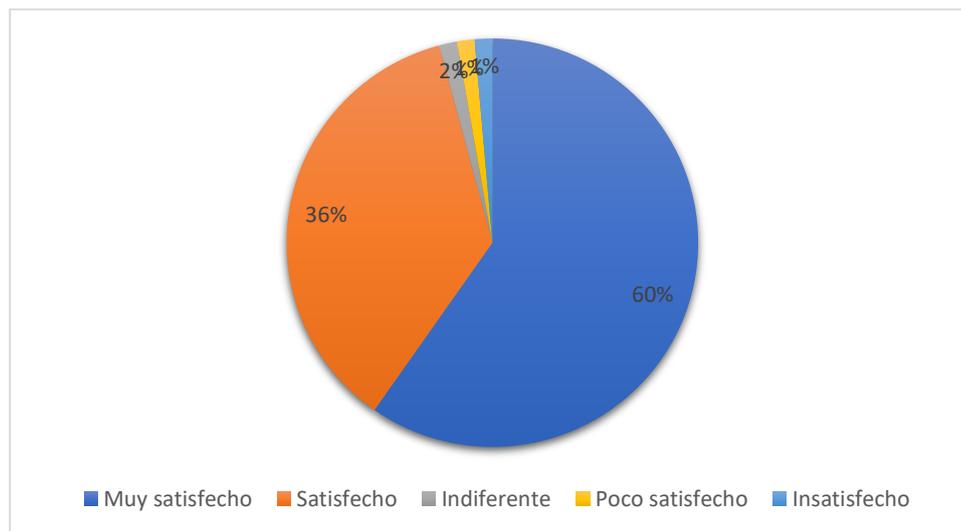


Figura N° 33. Grado de satisfacción para el usuario al utilizar su propio rostro como acceso. Información tomada de la encuesta realizada en el presente trabajo de titulación. Elaborado por Veliz Chancay Amarilis Dayana.

Análisis. – Según los datos obtenidos se observa que el grado de satisfacción de las compañías de seguridad con respecto al empleo de su propio rostro como acceso a cualquier entidad, está dado en que el 60% se encuentra muy satisfechos, el 36% se encuentra satisfecho, siendo las respuestas más relevantes ya que, en los niveles de Poco satisfecho, indiferente e insatisfecho se mostró el 1%.

3.7. Factibilidad técnica

Los elementos que se proponen para el diseño del portero electrónico con reconocimiento facial son económicos y asequibles dentro del país tanto en hardware como software, a continuación, se muestra el análisis técnico de los componentes previamente especificados que se ajustan al diseño del proyecto.

Tabla 14. Software

Herramientas	Descripción
Sistema Operativo	Windows 10, Debian GNU/Linux
Interfaz	Powershell, Git Bash, Git, Open CV
Base de datos	Xampp (MySQL, Apache)
Lenguajes de programación	Python, Raspbian
Programa de diseño del circuito	Fritzing

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana

Para la gestión de la base de datos durante el de diseño del sistema de control de acceso, se tomaron en cuenta la utilización de diversos softwares de código libre detallados en la **Tabla 14** cumplen con estándares que se ajustan a la simulación del prototipo, gracias su fácil acceso, bajo costo, rápida corrección de errores facilitando el trabajo y así como usuario administrar de manera eficiente su operación con total autonomía.

El procesamiento y ejecución de los datos que se emplearán para la simulación del prototipo de portero electrónico también requiere de hardware y un servidor, que logrará establecer una conexión a la red, con lo que se logra la compartición del almacenamiento de la información.

Tabla 15. Hardware

Herramientas	Descripción
Procesador	Core i5 7th Generación
Memoria	8 Gb RAM
Disco Duro	1 TB
Dispositivos	Cámara Web, Teclado, Mouse.

Información tomada de la investigación directa. Elaborado por Veliz Chancay Amarilis Dayana

3.8. Factibilidad Operacional

El sistema de control de acceso automático con reconocimiento facial como parte del funcionamiento del portero electrónico, está orientado a usuarios con la previa autorización del personal administrativo, ya que serán los encargados de conceder los permisos de registros y a su vez recibir las notificaciones por medio de correo electrónico.

Mediante la encuesta realizada al grupo de compañías seguridad y vigilancia de la ciudad de Guayaquil, se determina la factibilidad operacional a través de los siguientes incisos:

De la pregunta 3, se obtiene el resultado de que, según el criterio de las empresas de seguridad, están de acuerdo con que las entidades para las que prestan sus servicios deberían contar con un portero electrónico de reconocimiento facial al ingreso, para automatizar el proceso de control de ingreso del personal.

De la pregunta 5 y 6, se obtiene que los usuarios consideran que este sistema cuenta con un nivel de seguridad muy alto, a su vez consideran que el servidor de correo electrónico es el adecuado de las notificaciones.

De la pregunta 10, como aporte adicional a la automatización del registro y control, los usuarios consideraran muy satisfactorio el hecho de utilizar su propio rostro como acceso sin necesidad de llaves o tarjetas.

3.9. Esquema general del proyecto

El desarrollo de la simulación del prototipo de portero electrónico con reconocimiento facial estará comprendido en dos partes, el primero será el sistema controlador, cuyo esquema se presenta en la figura 34 en la cual consta la estructura del proceso como tal de recopilación de información de los datos del usuario como registro, comparación con las bases de datos, biométricos faciales y posterior acceso.

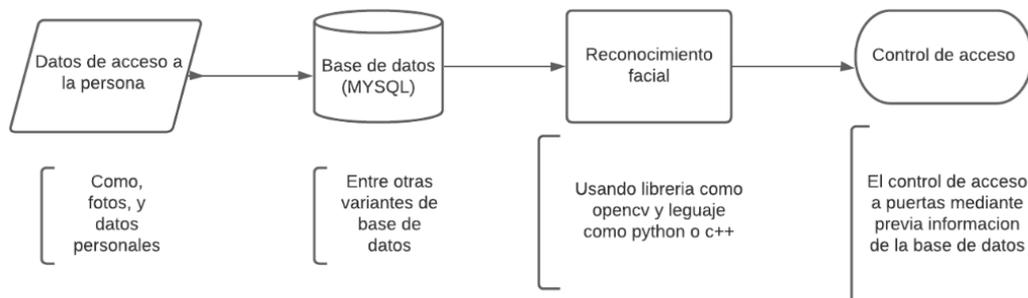


Figura N°34. Diagrama del diseño del sistema de control de acceso. Elaborado por Veliz Chancay Amarilis Dayana.

La segunda parte de la presentación es la propuesta del diseño electrónico del portero, cuya finalidad es mostrar que tan viable sería su función física, conformada por el microcontrolador que se ha elegido para el desarrollo del proyecto, Raspberry Pi, una cámara, el módulo relé y la cerradura selenoide. Cuando el control de acceso sea ejecutado en su menú, el proceso de reconocimiento facial da paso a la activación con pulsos eléctricos generados que activarán el puerto GPIO5, que es el pin que va a correr si y solo si se cumple la función de la comparación biométrica facial y cumplirá el proceso de reconocimiento, caso contrario se emitirá un error, que se verá reflejado en la no activación de la cerradura, y notificación vía correo electrónico de un usuario desconocido con la fecha y hora en tiempo real.

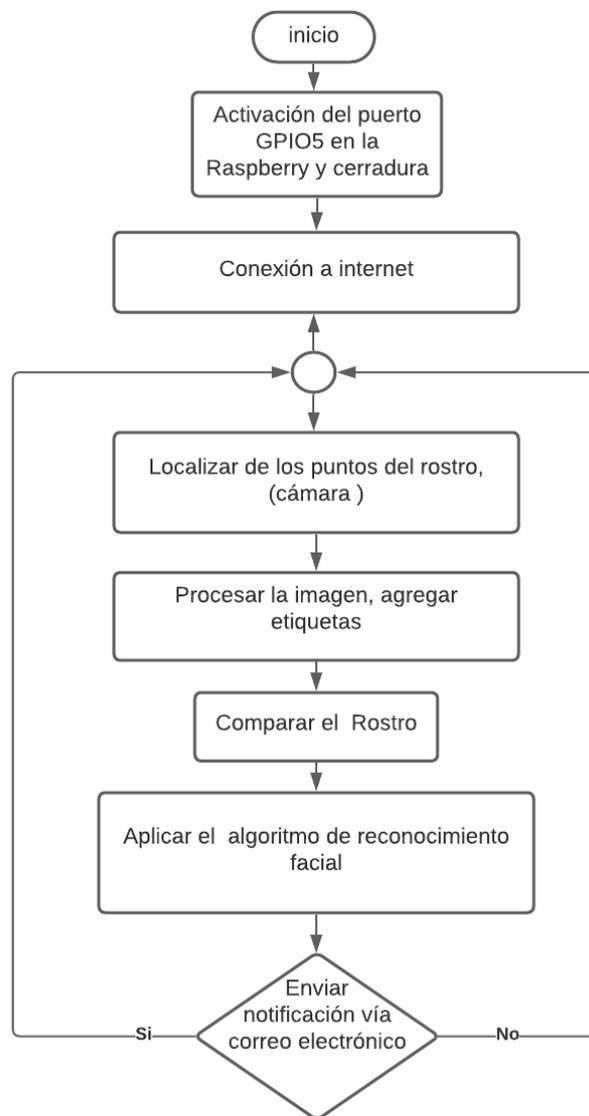
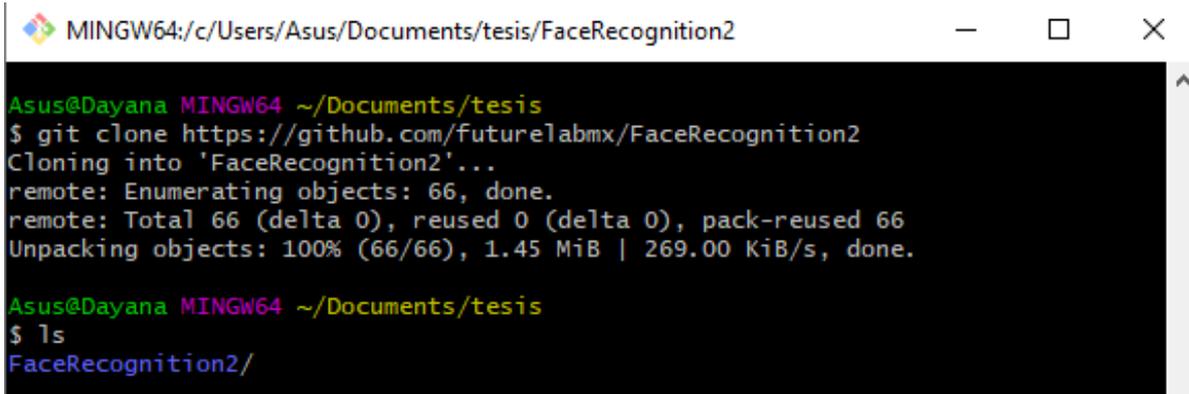


Figura N°35. Diagrama de la función del portero electrónico. Elaborado por Veliz Chancay Amarilis Dayana.

3.10. Proceso de versión de control

A través de una bifurcación se procede a administrar el cambio que se realicen a los códigos del proyecto de software, para el reconocimiento facial, mediante la descarga de un repositorio de Github, ver anexo 5, que contiene los archivos que se usaran para la simulación del proyecto. Así mismo, se usará un sistema de control de versión distribuida llamada Git, mediante el código *git clone*.



```

MINGW64:/c:/Users/Asus/Documents/tesis/FaceRecognition2
Asus@Dayana MINGW64 ~/Documents/tesis
$ git clone https://github.com/futurelabmx/FaceRecognition2
Cloning into 'FaceRecognition2'...
remote: Enumerating objects: 66, done.
remote: Total 66 (delta 0), reused 0 (delta 0), pack-reused 66
Unpacking objects: 100% (66/66), 1.45 MiB | 269.00 KiB/s, done.

Asus@Dayana MINGW64 ~/Documents/tesis
$ ls
FaceRecognition2/
  
```

Figura N° 36.24. Ejecución del código *git clone* en Github. Elaborado por Veliz Chancay Amarilis Dayana.

Esto permitirá el fácil acceso al repositorio para realizarle los cambios que sugiere el sistema de control de acceso del portero electrónico automático. Se realizarán los cambios en:

- La estructura de la base de datos
- La implementación de servidor de correo electrónico
- La activación del puerto GPIO5 de la Raspberry

3.10.1. Estructura de la base de datos.

3.10.1.1. Información de ambiente de Programación.

Tabla 16. Descripción de la Base de datos

Parámetro	Datos
Gestor de la Base de datos	phpMyAdmin 5.0.2
Dominio	127.0.0.1
Interfaz	MySQL, Apache

Información tomada de la investigación directa. Elaborado por Amarilis Dayana Veliz Chancay.

Se determina que para el desarrollo de la base de datos del sistema de control de acceso se utilizará XAMPP en su versión 3.2.4, el cual incluye un paquete de instalación de software libre que consiste en un sistema de gestión de base de datos MySQL y de servidor de Apache, convirtiendo este equipo en uno de los componentes principales del desarrollo del sistema de control de acceso.

Tabla 17. Estructura del ambiente de Programación

Parámetro	Datos
Lenguaje de Programación	Python
Servidor Web	XAMPP
Puerto	8088
Visión Artificial	OpenCV

Información tomada de la investigación directa. Elaborado por Amarilis Dayana Veliz Chancay.

3.10.2. Servidor XAMPP.

La base de datos requiere de la instalación del servidor de Xampp v3.2.4 ver anexo 6, el cual permitirá el levantamiento de esta, se realiza la activación de Apache puertos 80 ,443 y MySQL con su puerto por defecto 3306. Una vez realizado el levantamiento del servidor de MySQL, se crea la base de datos, en ese caso se le agregó el nombre de “sisfacial”, posteriormente la creación de la tabla “usuarios permitidos” con 4 columnas, que corresponden al identificador, nombre, apellido y estado como se puede visualizar en la figura N°37.

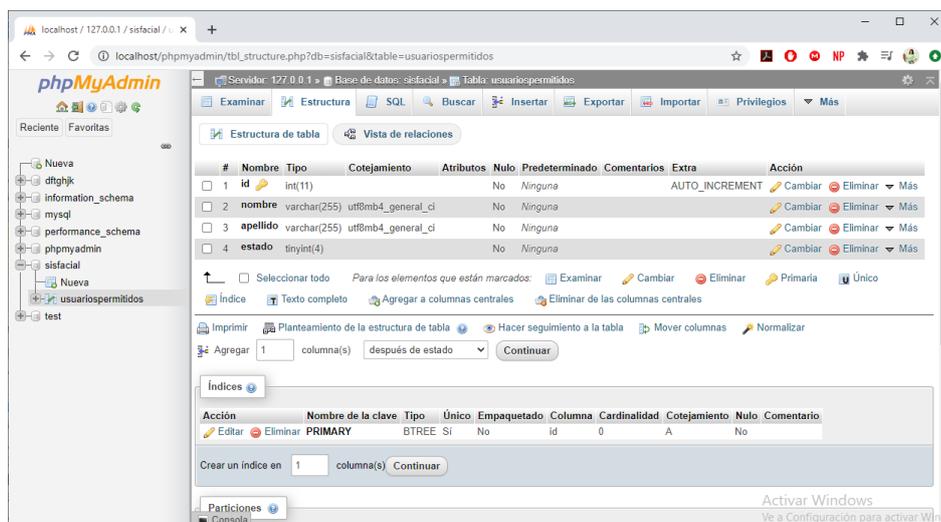


Figura N° 37 Creación de la base de datos “sisfacial”. Elaborado por Veliz Chancay Amarilis Dayana.

3.10.3. Implementación de servidor de correo electrónico.

Cuando se finalice la configuración de la base de datos, para el control de acceso del portero electrónico, como punto específico se sugiere que los usuarios administradores tengan la posibilidad de recibir notificaciones de los usuarios permitidos, previamente registrados y que el sistema notifique que un usuario desconocido ha intentado acceder. Para ello se procederá a ingresar los cambios en el archivo ejecutable de Python llamado “listaPermitidos” ver anexo 7, del repositorio de Github antes descargado. Cabe recalcar que el archivo puede ser modificado en cualquier momento, sujeto a cambios del administrador.

Tabla 18. Detalles de la configuración de correo

Librerías	Descripción
smtpplib	Se define un objeto de sesión de cliente SMTP que se puede usar para enviar correo a cualquier máquina de Internet con un daemon de escucha SMTP o ESMTP.
pendulum	Es un paquete de Python para facilitar la manipulación de las fechas y horas.
Correos de prueba	
Saliente	accesescontrol@gmail.com
Entrante	adveliz4@gmail.com

Información tomada de la investigación directa. Elaborado por Amarilis Dayana Veliz Chanca.

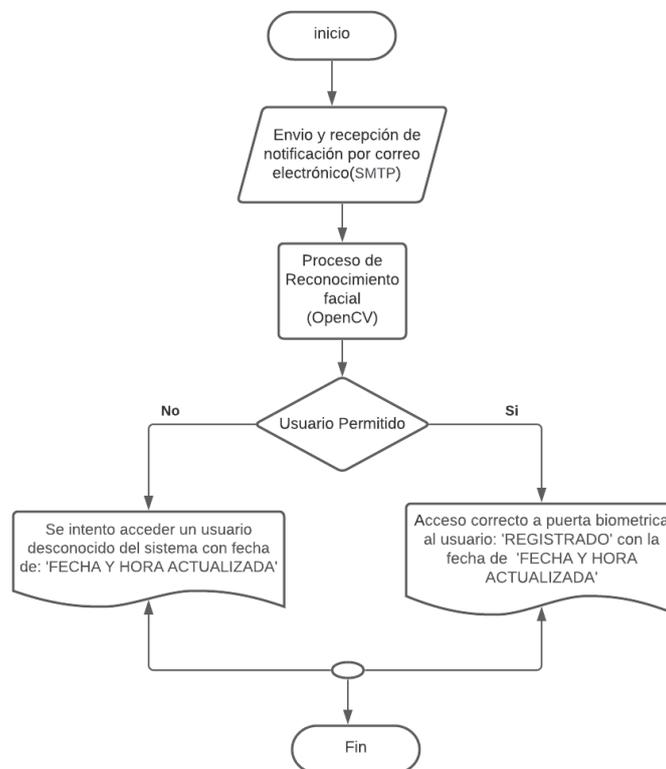


Figura N°38. Diagrama del proceso de envío y recepción de notificación por correo. Elaborado por Veliz Chanca Amarilis Dayana.

3.10.4. Activación del puerto GPIO5 de la Raspberry.

Según como refleja en el archivo ejecutable de Python llamado “reconocimiento” , ver anexo 8 . Se importa la librería al gpio, se declaran los pines de la raspberry y se coloca las variables|

```
import RPi.GPIO as GPIO
relay_pin = [5]
```

Cuando la predicción del reconocimiento facial tenga una exactitud menor a 100, significa que la persona fue reconocida, entonces el sistema de control es el encargado de enviar el pulso eléctrico, que activará la función de GPIO5 en la raspberry, cuya función es de indicar al pin del relay que 1 es encendido y 0 apagado.

```
GPIO.output (Relay_pin, 1)
GPIO.output (Relay_pin, 0)
```

3.10.4.1. Diagrama del circuito del portero electrónico.

GPIO son los pines de la Raspberry PI que, al momento del reconocimiento, el pulso puede ser de 3.3v, pero se tiene que el bloqueo del selenoide requiere de al menos 7 a 12v para que su funcionamiento sea correcto. Debido a esto, se necesitará usar una fuente de alimentación externa y un relé para poder operar la cerradura.

El circuito refleja la potencia de la señal producida por la Raspberry Pi, el transistor cumple la función de mover la cantidad suficiente de corriente y elevarla para que el relé accione, con la corriente proporcionada por el GPIO5. El diodo cumple la función de suprimir la negatividad siendo un elemento antirretorno para proteger al transistor del breve alto del voltaje que producirá el relé cuando esté desconectado.

Se procede a realizar la conexión del VCC y GND del módulo de relé a 5V y GND de Raspberry Pi, para luego conectar el pin de señal del módulo de relé al GPIO5 de Raspberry Pi3.

El módulo del relé se conecta con la fuente de alimentación de CC de forma negativa al negativo del bloqueo de la puerta del selenoide. Se conecta el positivo de la fuente de alimentación de CC al conector común del relé y luego se conecta normalmente abierto desde el módulo de relé al positivo de la cerradura de la puerta del selenoide.

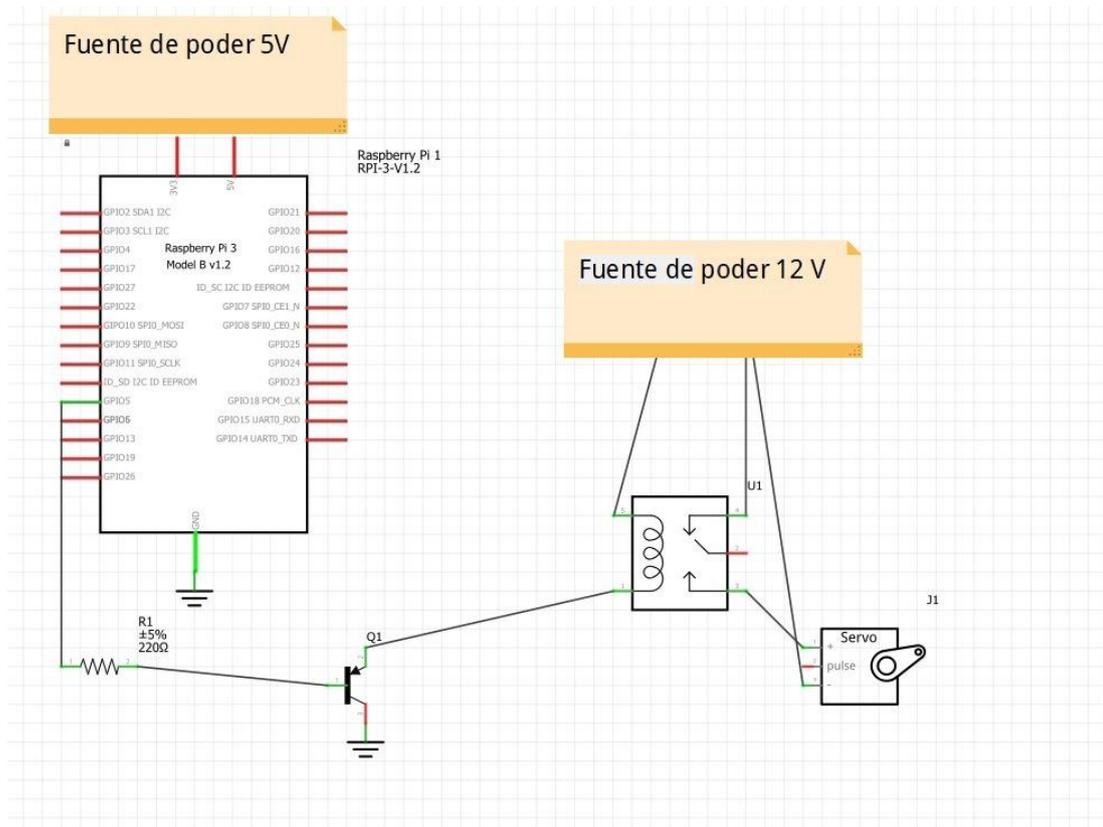


Figura N° 3925. Diagrama del circuito eléctrico del portero electrónico. Elaborado por Veliz Chancay Amarilis Dayana.

3.11. Resultados

3.11.1. Descripción de la funcionalidad.

El funcionamiento de la simulación del proyecto, según su menú está comprendido en 3 fases: Inicio, registro y control de acceso. Para la simulación se utilizará la consola en Windows Powershell, como se visualiza en la figura N°40, este proceso fue ejecutado en las líneas de comando “menu”, ver anexo 9, del repositorio Git.

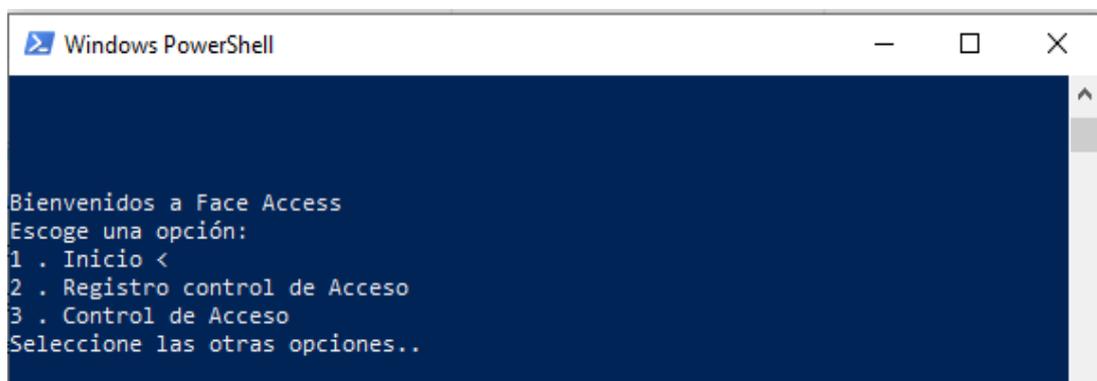
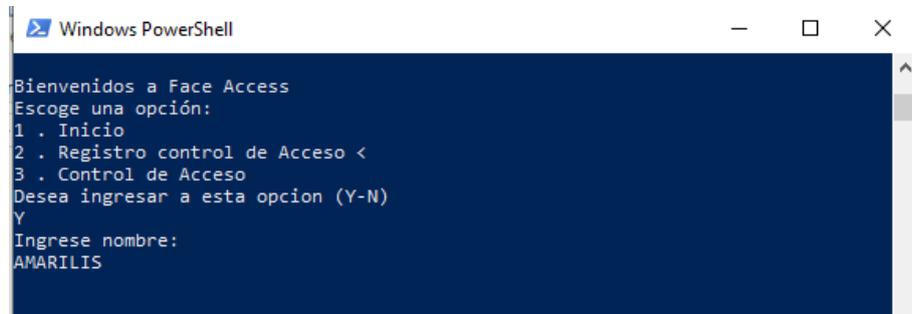


Figura N°40. Menú de Face Access. Elaborado por Veliz Chancay Amarilis Dayana.

3.11.2. Registro de Control de acceso.

El proceso de registro de control de acceso, se realizará la petición de ingreso del nombre, mismo que se guardará en la base de datos ya creada.



```
Windows PowerShell
Bienvenidos a Face Access
Escoge una opción:
1 . Inicio
2 . Registro control de Acceso <
3 . Control de Acceso
Desea ingresar a esta opción (Y-N)
Y
Ingrese nombre:
AMARILIS
```

Figura N°41. Opción de registro de Face Access. Elaborado por Veliz Chancay Amarilis Dayana.

En la interfaz las líneas de comando que se ejecutarán del repositorio “capture”, ver anexo 10, la cual se describe con la activación de la cámara web, para la simulación del reconocimiento facial con el método de patrones binarios locales, y se procederá a realizar el proceso de extracción de los parámetros del rostro en diferentes regiones, a las que se les aplica un histograma con el que se obtiene el operador LBPH que describe información independiente por región. Estas descripciones locales son entonces concatenadas para construir una descripción global del rostro por medio de una etiqueta del nombre que realizó el registro, si se presiona la tecla ESC se cierra el programa.

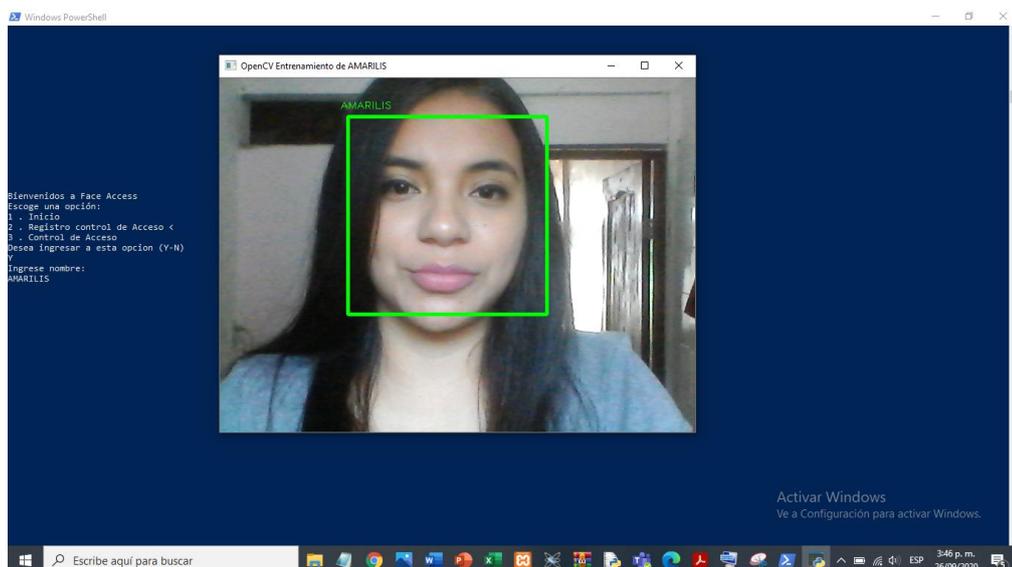


Figura N°42. Registro de Face Access. Elaborado por Veliz Chancay Amarilis Dayana

El entrenamiento almacenará todos los rostros en un mismo tamaño y las convertirá en escala de grises, como se muestra en la figura N°43 se aprecia que son 100 imágenes del rostro en tiempo real, es importante que los rostros que vayan a ser tomados, tengan una variedad de expresiones, como cambios en las condiciones de luz o incluso las personas deberían presentar distintos peinados, además se los debe tomar en un ambiente donde vaya a ser implementado, esto permitirá que sea más robusto en el reconocimiento.



Figura N° 43. Imágenes extraídas para el registro en escala de grises. Elaborado por Veliz Chancay Amarilis Dayana.

3.11.3. Control de Acceso.

En este trabajo se estudiará la técnica dependiente de pose Patrones Locales Binarios (LBP), puesto que no requiere un equipamiento especializado para la captura de imágenes o capturas muy específicas controladas. El descriptor o algoritmo de Patrones Binarios Locales (LBP) es uno de los más conocido y ampliamente usado en el contexto de reconocimiento de rostros.

Se obtiene valores de confianza efectivos la cual permite realizar el reconocimiento, la condición de las líneas de comando ejecutados en la fase de “reconocimiento” del archivo de Python, revisar anexo 8, en la cual se especifica que si los valores de confianza efectivos para realizar el reconocimiento son mayores a 100 que es la cantidad de imágenes que se han guardado en la base de datos, lo reconocerá como desconocido, como se visualiza en la figura N°44.

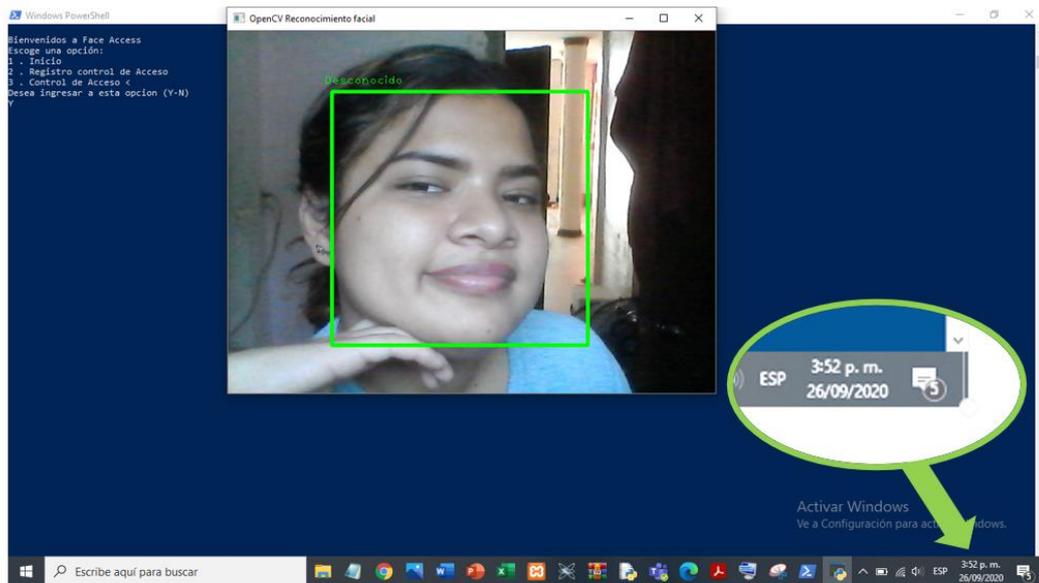


Figura N°44. Usuario desconocido. Elaborado por Veliz Chancay Amarilis Dayana.

Caso contrario si de la ruta en la cual se ha almacenado las imágenes corresponden a las etiquetas en un rango de menor o igual a 100, el sistema extraerá las características del rostro almacenado, clasificará las etiquetas, dando paso al reconocimiento y en la ventana de OpenCV se mostrará la imagen del video en tiempo real con el nombre del registro en la base de datos del proceso de entrenamiento como se visualiza en la figura N°45.

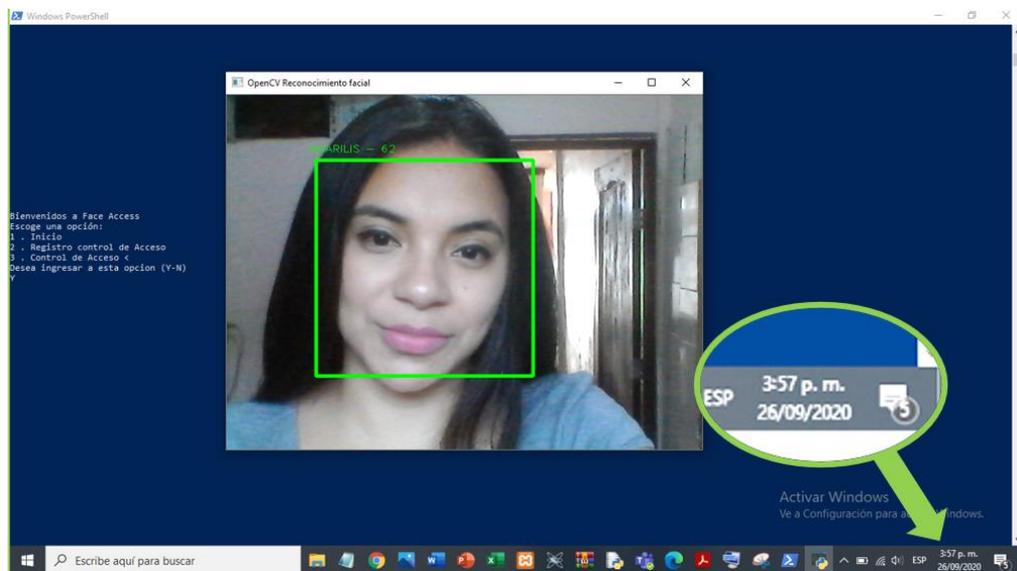


Figura N°45. Usuario permitido. Elaborado por Veliz Chancay Amarilis Dayana.

3.11.4. Funcionamiento de portero en conexión.

El sistema de control de acceso “Face Access” al ser ejecutado, a través del reconocimiento facial utilizando Raspberry Pi, se podrá identificar el rostro de una persona para el acceso. El control podrá dar paso solo a las personas cuyos rostros estén guardados dentro del sistema. Este acceso será realizado solo en tiempo real, no se podrá introducir videos, ni fotografías en la parte externa, ya que la cámara extraerá y clasificará las partes del rostro en tiempo real. La puerta se abre permitiendo ingresar al personal autorizado y acto seguido se realizará el envío de la notificación vía correo electrónico.



Figura N°46. Propuesta del diseño físico del portero electrónico automático. Elaborado por Veliz Chancay Amarilis Dayana.

3.12. Notificación vía correo electrónico

Este proceso de envío y recepción de correo descrito en la figura N°38, obedece a la línea de comandos del archivo “listaPermitidos” ver anexo 7, en el cual se importan dos librerías, descritas en la **Tabla 16**, definiendo que mediante el servidor SMTP, se logró en el envío de las notificaciones como se visualizan en la figura N°47. Se extrae la hora y fecha del ingreso por parte del usuario permitido y desconocido, esta información es tomada del proceso de control de acceso de menú de “Face Access” como se muestran en las figuras 44 y 45, en tiempo real la notificación es emitida vía correo electrónico previamente configurado, cabe

recalcar una vez más que estas condiciones son programables de forma sencilla para que los usuarios administradores puedan realizar cambios y se ajusten a la necesidades de la instalación, departamento o espacio en el que se desee realizar la implementación de este prototipo.

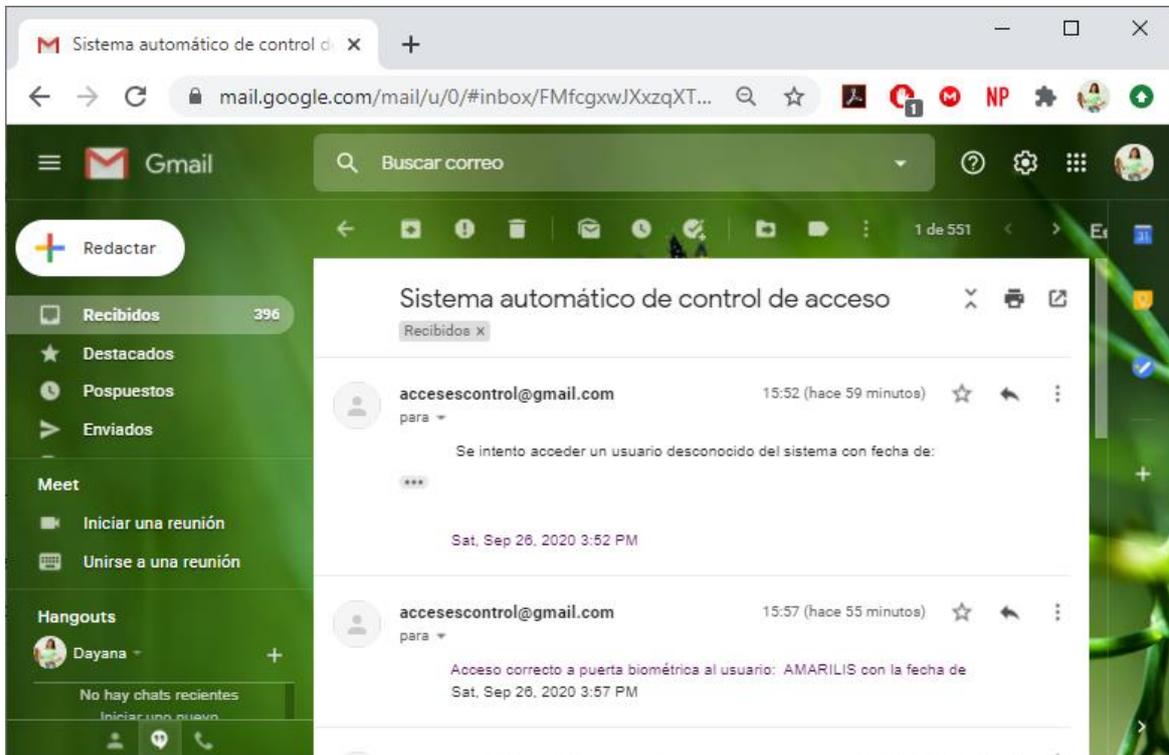


Figura N°47. Notificación del sistema automático de control de acceso. Elaborado por Veliz Chancay Amarilis Dayana.

3.13. Pruebas de funcionamiento

Para ejecutar las pruebas del funcionamiento se registraron 4 usuarios dentro del menú de “Face Access”. Se puede observar los intentos realizados y los aciertos que se obtienen con cada usuario.

En la tabla descrita el SI representa uno lógico y NO representa cero lógico, para determinar cuál es la efectividad del equipo se usó la mediana y para determinar la precisión la desviación estándar.

Tabla 19 Efectividad y precisión de la simulación del control de acceso

Usuario	Intentos										Promedio	Porcentaje	Desviación Estándar
	1	2	3	4	5	6	7	8	9	10			
1	1	1	0	1	1	1	1	1	1	1	0,9	90%	0,3
2	1	1	1	0	1	1	1	1	1	1	0,9	90%	0,3
3	1	1	1	0	1	1	1	1	1	1	0,9	90%	0,3
4	1	1	1	1	1	1	1	1	1	1	1	100%	0,0
5	1	1	0	1	1	1	1	1	1	1	0,9	90%	0,3
6	1	1	0	0	1	1	1	1	1	1	0,8	80%	0,4
7	1	0	1	0	1	1	1	1	1	1	0,8	80%	0,4
8	1	1	1	1	1	1	1	1	1	1	1	100%	0,0
9	1	1	1	1	1	1	1	1	1	1	1	100%	0,0
10	1	1	1	1	1	1	1	1	1	1	1	100%	0,0
11	1	1	0	0	1	1	1	1	1	1	0,8	80%	0,4
12	1	1	1	1	1	1	1	1	1	1	1	100%	0,0
13	1	1	1	0	1	1	1	1	1	1	0,9	90%	0,3
14	1	1	1	1	1	1	1	1	1	1	1	100%	0,0
15	1	1	1	1	1	1	1	1	1	1	1	100%	0,0
Promedio de efectividad												97%	0,10

Información tomada de la investigación directa. Elaborado por Amarilis Dayana Veliz Chancay.

Se observa que para el usuario 8, 9, 10, 12, 14, 15 se tiene la más alta efectividad con el 100% de intentos, que sí pudieron acceder, para los usuarios 6, 7, 11 con el peor caso de efectividad con el 80 % y en el caso de los demás usuarios se obtuvo una efectividad del 90%, que estos datos siguen siendo considerablemente buenos, de estos resultados obtenidos se determina que es un porcentaje aceptable para el proceso de identificación de los usuarios. Se demostró el porcentaje de efectividad para el ingreso de los usuarios, por medio del cálculo del promedio de los intentos, lo cual facilita el cálculo de la desviación estándar, este dato representará la precisión, teniendo como resultado que los usuarios de 100 de efectividad obtuvieron una desviación de 0, y el peor de los casos se tiene a los usuarios 6, 7, 11, que se muestran como una desviación estándar de 0,4.



Figura N°48. Porcentaje de efectividad del diseño del prototipo. Elaborado por Veliz Chancay Amarilis Dayana.

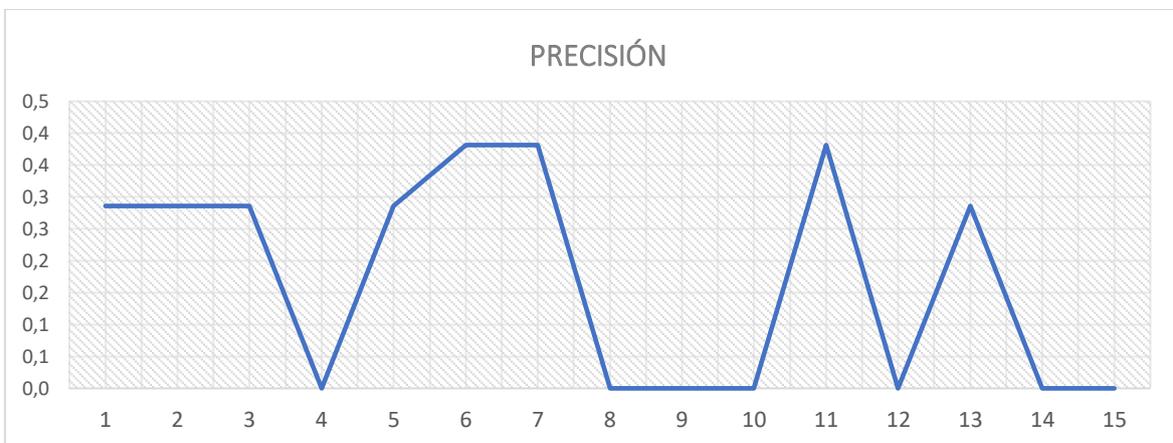


Figura N°49. Grado de precisión del sistema automático de control de acceso. Elaborado por Veliz Chancay Amarilis Dayana.

Los intentos que se realizaron en la simulación de ingreso al sistema fueron satisfactorios en su mayoría, esto significa para la base de datos en la Raspberry Pi, la persona que haya realizado mejor el proceso de registro será la personas con más exactitud de aciertos, ya que al realizar la extracción de las características faciales y posterior comparación se tendrá el fácil acceso, ver anexo 11, por ende, se complementa con el proceso de apertura de la cerradura del portero electrónico.

También se verificó que la notificación del acceso vía correo electrónico fue exitosa e inmediata, se toma en cuenta que la recepción de los mensajes es igual a la cantidad de intentos que se realizó a cada uno de los usuarios, con su respectiva descripción de usuario permitido o desconocido, con la fecha y hora en tiempo real.

3.14. Conclusiones

- El uso de Raspberry PI3 como microcontrolador para el desarrollo de la simulación de este proyecto fue ajustable, ya que pudo ser configurado, se logró establecer las librerías necesarias como OpenCV, que ofrece una variedad de servicios para el proceso de reconocimiento facial, funcionamiento del sistema, al igual que cada uno de los componentes expuestos.
- En cuanto a la funcionalidad de los porteros electrónicos, su sensibilidad esta dada en las frecuencias mínimas emitidas por el microcontrolador cuando se realiza el reconocimiento, estos picos presentes en el inicio y fin de la señal son los que ayudarían en la activación del relé dando paso que el selenoide actúe en la apertura de la puerta.
- El diseño de este prototipo de portero electrónico entre la puerta de calle y el usuario deseado en función de abrepuertas con reconocimiento facial, y su sistema de control de acceso cumple con las factibilidades técnicas se incluyen elementos tales como la privacidad entre usuarios al mostrar un registro único, en la base de datos para la comparación y registro.
- Las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única como datos biométricos en el sistema de control de acceso, comprueban un 97% de efectividad el funcionamiento del prototipo, siendo un modelo de gestión que puede ser tomado para su implementación.

3.15. Recomendaciones

- En el desarrollo del código se debe tener en cuenta las dependencias de Python que se administran con pip en la línea de comandos para el completo funcionamiento de la aplicación.
- La infraestructura como tal del prototipo de debe ser de cuarta generación, es decir debe tener un gran alcance de datos para que el sistema no tenga inconvenientes de conexión, se recomendaría el uso de un módulo a Raspberry Pi zero 1.3 para poder recibir datos con una tarjeta SIM.
- El administrador de correo electrónico debe mantener una excelente conexión de internet, con el fin de evitar fallas en el sistema automático de control de acceso, para el proceso de envío y recepción de las notificaciones por electrónico

- En caso de realizar la implementación del prototipo para la Raspberry Pi se recomienda montar un sistema de refrigeración con disipadores de calor y ventiladores, ya que esta placa en ciertas ocasiones produce calor, y su temperatura límite es de 85 °C.
- Se recomienda que mientras la base de datos y la capacidad de memoria del microcontrolador sea mayores, mayor será la efectividad y precisión de datos ya que se verá reflejado en la cantidad de imágenes o datos biométricos recopile, en menor tiempo, se necesitaría como mínimo 8Gb de memoria, con un tiempo de retardo de 0,03s.

ANEXOS

Anexo 1

Reformar la política de seguridad de la información

Artículo 1.- OBJETIVOS:

Minimizar los riesgos mediante la prevención de los incidentes de seguridad, reducir su potencial impacto.

Adoptar controles dentro de la Institución, para que la información este protegida contra: divulgación a usuarios no autorizados (confidencialidad) modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad).

Plantear estrategias basadas en riesgo y promover un comportamiento responsable en Seguridad de la Información.

Artículo 2.- ALCANCE DE APLICABILIDAD

La política de Seguridad de la información se aplica para salvaguardar la información física o digital recibida o que sea producto de los procesos gobernantes, agregadores de valor, habilitantes de asesoría y de apoyo; información relacionada con la correspondencia almacenada o custodiada en medios digitales o físicos.

La información que se intercambie con otras Instituciones del Estado, con organizaciones de la Economía Popular y Solidaria; y la de usuarios externos que presten servicios a la Institución, estarán regulados a través de los respectivos convenios, contratos, normas técnicas, acuerdos de confidencialidad y otros que se suscriban para el efecto.

Anexo 2

Decreto presidencial ante crisis sanitaria

N^o 1019

LENÍN MORENO GARCÉS

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

“primera línea de defensa contra crisis sanitarias que pueden devastar pueblos, sociedades y economías en todo el mundo⁷”; y,

En ejercicio de las facultades que le confieren los artículos 164, 165 y 166 de la Constitución de la República,

DECRETA:

Artículo 1.- ESTABLECER como zona especial de seguridad toda la provincia del Guayas, de conformidad a lo dispuesto en el artículo 165, numeral 5, de la Constitución de la República del Ecuador.

Artículo 2.- DETERMINAR que la zona especial de seguridad que requiere de regulaciones especiales, estará conformada por todos los cantones de la provincia del Guayas, y, con especial atención en los cantones de Guayaquil, Daule, Durán y Samborondón. En toda la zona especial de seguridad se realizará una gestión integral en el marco de la emergencia sanitaria y del estado de excepción, que permita mitigar los riesgos, precautelar la salud, proteger a la población, evitar el contagio del virus COVID-19 y recuperar las condiciones idóneas para la atención de la emergencia sanitaria.

Artículo 3.- DISPONER a las Fuerzas Armadas la conformación de la Fuerza de Tarea Conjunta con mando y medios necesarios, misma que establecerá una planificación que incluya a la Policía Nacional.

Artículo 4.- DISPONER al Gobernador de la provincia del Guayas la dirección de las acciones interinstitucionales en la zona especial de seguridad, para lo cual se articulará con las siguientes autoridades: el General o Almirante designado por el Ministerio de Defensa Nacional, quien estará a cargo de la Fuerza de Mando; la autoridad designada por el Ministerio de Salud Pública, y el Oficial General de la Policía Nacional designado por el Ministerio de Gobierno.

Artículo 5.- La zona especial de seguridad determinada en los artículos 1 y 2 del presente decreto estará bajo disposición del Comité de Operaciones de Emergencia Nacional, por lo cual todas las iniciativas y regulaciones que se propongan respecto de la misma deberán ser aprobadas por esta instancia, previo a su implementación.

⁷ <https://www.who.int/world-health-day/previous/2007/es/>

Anexo 3**Encuesta dirigida a empresas de seguridad de la ciudad de Guayaquil**

La siguiente encuesta está orientada a determinar los requerimientos, sobre los cuales se dará el desarrollo de un prototipo de portero electrónico automático con reconocimiento facial mediante el uso de microcontroladores, como parte de investigación de trabajo de titulación.

1. ¿Qué sistema para el control de acceso ha utilizado?

- a) Huella Digital
- b) Tarjeta Magnetica
- c) Reconocimiento facial
- d) Otro especifique

2. ¿Conoce usted en qué consiste el sistema de reconocimiento facial?

- a) Si
- b) No

En caso de que la respuesta anterior haya sido "No", en breves palabras se define que el sistema de reconocimiento facial es:

"Una solución biométrica que emplea un algoritmo automático para verificar o reconocer la identidad de una persona en función de sus características fisiológicas"

3. ¿Le gustaría que las entidades a las que presta servicios de seguridad cuenten con un portero electrónico de reconocimiento facial al ingreso?

- a) Si
- b) No

4. Según su criterio, ¿Cuánto estaría dispuesto a invertir en un sistema de control de acceso con reconocimiento facial?

- a) \$0 - \$100
- b) \$101 - \$200
- c) \$201 - \$300
- d) \$301 – más

5. ¿Cuáles cree usted que son las ventajas de utilizar un portero electrónico con reconocimiento facial?

- a) Fácil de usar
- b) Alta seguridad
- c) No necesito llaves

- 6. ¿Qué herramienta tecnológica considera viable para el registro de personal autorizado o no autorizado?**
 - a) Correo electrónico
 - b) Whatsapp
 - c) Almacenamiento en La Nube
- 7. ¿Considera viable el uso de un portero electrónico con reconocimiento facial ya que presenta menos errores que la desprogramación de las tarjetas?**
 - a) Si
 - b) No
- 8. ¿Cuál es el grado de satisfacción que usted tendría con un portero de reconocimiento facial al ingreso de una instalación?**
 - a) Muy satisfecho
 - b) Satisfecho
 - c) Poco satisfecho
 - d) Insatisfecho
- 9. ¿Considera que la implementación de un sistema de portero electrónico con reconocimiento facial satisface sus expectativas de funcionalidad al ser rápido y sencillo?**
 - a) Si
 - b) No
- 10. ¿Qué grado de satisfacción le aportaría el hecho de utilizar su propio rostro como acceso ya que mediante este se elimina el uso de tarjetas o llaves?**
 - a) Muy satisfecho
 - b) Satisfecho
 - c) Indiferente
 - d) Poco satisfecho
 - e) Insatisfecho

Anexo 4**Bitácora de compañías de seguridad en la ciudad de Guayaquil**

COMPAÑÍAS DE SEGURIDAD Y VIGILANCIA EN LA CIUDAD DE GUAYAQUIL SEGÚN EDINA.COM			
N°	NOMBRE	DIRECCIÓN	CONTACTO
1	Acopron Security Cia. Ltda.	C.C. Albán Borja" Planta alta Oficina. # 123, Av. Pdte. Carlos Julio Arosemena Tola, Guayaquil	098 093 5996
2	Active Security Company	Juan Aurelio, 7, Guayaquil	(04) 601-8258
3	Agusegpro Cia. Ltda	Guayaquil	04) 242-8332
4	Alconsa	Av. Hermano Miguel, Guayaquil	422925205
5	Alerta Red Cía. Ltda.	Maracaibo & Guaranda, Guayaquil	04) 233-4530
6	Armiled	Guayaquil	(04) 265-5878
7	Arseg	Cdla Bolivariana Mz K Villa 19, Guayaquil	(04) 239-9170
8	ARSEGEC	Calle 8ava 101 y, Guayaquil	(04) 200-3821
9	Astroseg CIA. LTDA.	Guayaquil	(04) 228-0478
10	Bitajon C. LTDA	Cdla Albatroz Calle Pinzón 103, Rosa Lince S, Guayaquil	239-9322
11	Bits Seguridad Cia. Ltda. (Especialistas en Cámaras de Seguridad)	Manzana J, Guayaquil	(04) 510-1217
12	BodyGuard	Guayaquil	(04) 460-5756
13	Casecon Cia. Ltda.	Adelaida Velasco Galdós, Guayaquil	(04) 502-4895
14	Cenase Cia. Ltda.	Cdla. Miraflores Av. Guayas #303 entre la tercera y cuarta, Guayaquil	(04) 460-8055
15	Citius International Security	Kennedy Norte, Av José Castillo y Nahim Isaias Mz 801 Solar 3, Guayaquil	098 723 1577
16	Compañía de Seguridad Fuerzasein Cia. Ltda	Cdla Sauces 8 / Mz. 454 Solar F-41, Guayaquil 090507	(04) 600-9941
17	Compañía de Seguridad Privada Omniguard Cia. Ltda.	Unnamed Road, Guayaquil	600-8210
18	Compañía De Seguridad Condor Cia. Ltda	Av de Las Americas, Guayaquil	099 934 7924

19	Copse Cía. Ltda.	Av Isidro Ayora Calle Principal Mucho Lote 7ma Etapa Mz 2361, Guayaquil,	(04) 217-4895
20	Corpdeprot Cia. Ltda.	Unnamed Road, Guayaquil	04) 238-8599
21	COSMOSEG	Guayaquil	(04) 504-5098
22	Cuport Cia. Ltda.	Guayaquil Cdla. ALbatros Mz 5 Sl 18	(04) 203-2103
23	Cuprovyg Cia Ltda	Tungurahua 1019, y, Guayaquil 0	(04) 604-7136
24	Custosecurity Cia. Ltda	Miguel Hurtado Antonio 907, Guayaquil	99 103 6168
25	División de Seguridad y Protección D.S.P. Cía. Ltda.	Camilo Destruge Illingworth E, Guayaquil	04) 605-5290
26	ECUAPROT	Ecuador, Dr Orión L Laguno Márquez, Guayaquil	099 785 2359
27	Ecusegu Cia Ltda	Av. 12A, Guayaquil	(04) 226-2858
28	Empresa De Seguridad Kafirim	Ing Jorge Perrone Galarza, Guayaquil	099 772 3137
29	Empresa de seguridad Seproamerica Cia. Ltda.	Matriz Guayaquil: Cdla. La Alborada 6ta. Etapa Mz. 628 Villa 15	(04) 603-5059
30	FERJEM Seguridad	Av. Francisco de Orellana, Guayaquil	(04) 504-4617
31	FORSEMAX	Av. 6 S-O, Guayaquil	(04) 605-4354
32	Forsemax CIA LTDA	Jose Salcedo 306 y, Guayaquil	04) 605-0235
33	Fortius	Guayaquil	(04) 268-1438
34	G4S Guayaquil	Guayaquil	(04) 605-4354
35	G4S Secure Solutions	Av. 42 N-O, Guayaquil	04) 600-9070
36	GEVISE CIA LTDA	Av. Guillermo pareja rolando sn y tercera herradura edificio d'bronce piso 2 oficina 201, Guayaquil	(04) 600-5203
37	GPS - Empresa Seguridad Privada (Centro Operativo Inteligente)	Avenida 33 NO, Guayaquil	096 279 5655
38	Grupo de Seguridad Diamante	Alborada 10 Mz 303 Villa 19, Guayaquil	(04) 460-3936
39	GuarpriEcuador	Av. 24 NO, Guayaquil	(04) 605-4354
40	GUAYPRO	Alborada IV etapa MZ: FB V6 Planta Baja, Guayaquil	099 077 5192
41	ICSSE Guayaquil Cia. Ltda Seguridad Privada	Guayaquil	096 773 2270
42	Insevig Cía Ltda.	Guayaquil	(04) 232-6220

43	INVESCOL	Av. 120 Entre M. Galecio Y Piedrahita, Av. del Ejército, Guayaquil	(04) 239-7626
44	LAAR Seguridad	Av. 9 NO 702, Guayaquil	04) 269-0234
45	Liderman	Cdla La FAE Mz 33 Villa 12, Guayaquil	(04) 239-5098
46	Lion Security ALSZ	Cdla. Albatros mz 29 villa 5, Guayaquil	04) 268-3573
47	Mafiros Seguridad	Avenida 41A NO, Guayaquil	(04) 201-3310
48	Máxima SecurityMax Cía. Ltda.	Av. 24 NO 124, Guayaquil	(04) 238-0900
49	Máxima Seguridad & Security Max	Av Primera 114, Guayaquil	(04) 504-5098
50	Maxima Seguridad Integral Cia. Ltda MSI	Alfredo Valenzuela, Guayaquil	098 226 0876
51	Maximseg	Guayaquil	(04) 390-7163
52	Nova Novaseg Calidad Y Excelencia(GRUPO NOVA)	Guayaquil	(04) 265-5878
53	Nova Security S.A. - Empresa de seguridad, Importación y distribución de equipos de seguridad electrónica en Guayaquil Mayoristas	Cdla. Guayaquil Mz 20 Solar 4	099 368 1324
54	Oceansecurity Cia. Ltda.	Cdla. La Garzota, Mz. 12, Solar 5.	(04) 262-6810
55	OPTISEG Cía Ltda	Cdad. de la Paz, Guayaquil	098 730 8739
56	Optiseg Cía Ltda.	Av. Luis Plaza Dañin,	(04) 239-0789
57	Oxígenos del Guayas	Av Pedro Menéndez Gilbert & Av. Plaza Dañin, Guayaquil	(04) 229-2553
58	Prosecurity EC	Av. de las Américas y Av. Alarcón Edificio Sky Building, Guayaquil	099 719 6141
59	Protegarva Cía Ltda	Cdla FAE mz 1 solar, Calle 18, Guayaquil	099 566 7928
60	Protemaxi Seguridad Privada	Cristobal Colon Fontanarrosa 548, Guayaquil	(04) 252-3895
61	provica	Chimborazo &, Guayaquil	
62	Provintel Cía Ltda	Carlos Cueva Tamariz 501, Guayaquil	(02) 205-3552
63	SATFORCE	Leonidas García Ortiz 714, Guayaquil	(04) 288-6345
64	SecurityMax Cía. Ltda.	Guayaquil	(04) 220-1145
65	SEFIEM	Urdesa Central, M55, S7, Calle 2da #612 entre Ficus, y, Guayaquil	(04) 372-8320

66	Segonza Cia. Ltda.	Vía Guayaquil - Salinas Km 16.5, Mz 39, Solar 3, Puerto Hondo, Guayaquil	099 735 9761
67	Seguiresa Cia. Ltda.	Pedro Carbo 112 y, Guayaquil	(04) 256-0281
68	Segup CIA LTDA	Mucho Lote 1 MZ 2462 V 22, Guayaquil	096 374 1624
69	Seguridad Electrónica Cía. Ltda.	Guayaquil	(04) 238-9056
70	Seguridad OCAVIP CIA. LTDA. Guayaquil	Piedrahita 1503, Guayaquil	(04) 228-0387
71	Seguridad Privada Reyciel	Ingeniero Felipe Pezo Campuzano, Guayaquil	099 539 0031
72	Seguridad y Servicios SegSer	18° Paseo 19B, Guayaquil	(04) 228-0237
73	Segurtrust Trust Cia Ltda	Guayaquil Avenida Juan Tanca Marengo Urdenor 2, manzana 225 solar 11, Guayaquil	095 886 3693
74	Seinpri Seguridad Privada	Guayacanes 4ta Et. Este Mz. 201. V. 4, Guayaquil	04) 603-5426
75	Sepronac CIA Ltda	2° Pasaje 1 NE, Guayaquil	(04) 228-0533
76	Seprotec Security	Guayaquil	(04) 231-5844
77	SESEI Cía. Ltda.	Cdla. Garzota 1 Mz. 4, Villa 2, Guayaquil 090501	098 715 8302
78	Soriseg Cia Ltda	Av Primera, Guayaquil	097 990 7982
79	SW The Security World Cia. Ltda.	Guayaquil	(04) 239-6720
80	Swat Seguridad	Calle a, 1, Guayaquil	(04) 504-6900
81	Tadesec Cia. Ltda	Av. Luis Plaza Dañin SN, Guayaquil	(04) 228-7248
82	Target Seguridad Máxima Cia. Ltda	Avenida Francisco de Orellana, Samanes 7 Manzana 2246 Villa 18	(04) 600-1702
83	TROYANSEG CIA. LTDA.	Calle 7, Guayaquil	095 896 4801
84	Veincustodia Cia. Ltda	Noroeste de Guayaquil Veincustodia Cia. Ltda	099 555 3808
85	Vicosa	Calle 13E NE, Guayaquil	099 766 7388
86	Vicustodia Cia. Ltda.	Av 6 SO, Guayaquil	(04) 239-7626
87	Vimase	Luiz Alcívar Elizalde 327, Guayaquil	(04) 201-3010
88	Viteseg	Ciano, Guayaquil	099 911 4000

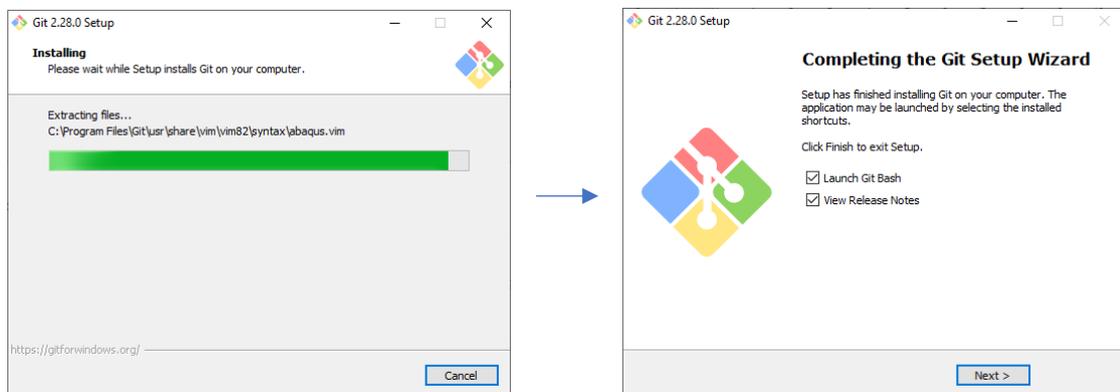
Anexo 5

Descarga de repositorio de Github

Seguir un proyecto existente en Git, debes ir al directorio del proyecto y usar el siguiente comando:

```
$ git init
```

Esto crea un subdirectorio nuevo llamado `.git`, el cual contiene todos los archivos necesarios del repositorio – un esqueleto de un repositorio de Git, siendo la interfaz de línea de comandos compatibles con github que permite además de descargar repositorio crear uno propio para subir a github.



Estando en el Git Bash se puede los comandos de Linux así nos dirigirá a documentos y cree una carpeta llamada y se descargan los archivos ahí directamente.

```
MINGW64:/c/Users/Asus/Documents/tesis
'sesion 7 triptico.docx'
'wondershare Filmora 9'/
WPS-PIN-4/
WPS-PIN-4.rar

Asus@Dayana MINGW64 ~/Documents
$ mdir tesis
bash: mdir: command not found

Asus@Dayana MINGW64 ~/Documents
$ mldir tesis
bash: mldir: command not found

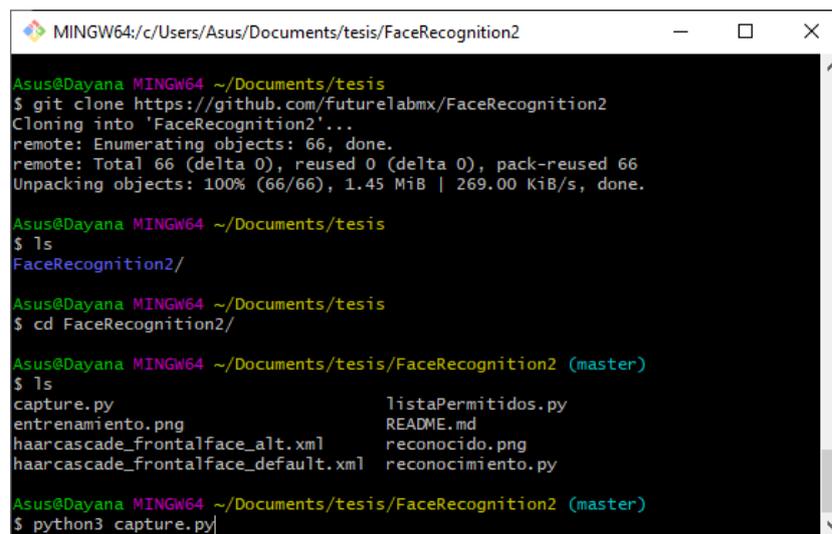
Asus@Dayana MINGW64 ~/Documents
$ mkdir tesis

Asus@Dayana MINGW64 ~/Documents
$ cd tesis/

Asus@Dayana MINGW64 ~/Documents/tesis
$ ls

Asus@Dayana MINGW64 ~/Documents/tesis
$ |
```

Use el comando git clone para clonar todo el proyecto de reconocimiento en dicha carpeta, Es una distinción importante, ya que Git recibe una copia de casi todos los datos que tiene el servidor. Cada versión de cada archivo de la historia del proyecto es descargada por defecto cuando ejecutas git clone. De hecho, si el disco de tu servidor se corrompe, puedes usar cualquiera de los clones en cualquiera de los clientes para devolver el servidor al estado en el que estaba cuando fue clonado.



```

MINGW64:/c/Users/Asus/Documents/tesis/FaceRecognition2
Asus@Dayana MINGW64 ~/Documents/tesis
$ git clone https://github.com/futurelabmx/FaceRecognition2
Cloning into 'FaceRecognition2'...
remote: Enumerating objects: 66, done.
remote: Total 66 (delta 0), reused 0 (delta 0), pack-reused 66
Unpacking objects: 100% (66/66), 1.45 MiB | 269.00 KiB/s, done.

Asus@Dayana MINGW64 ~/Documents/tesis
$ ls
FaceRecognition2/

Asus@Dayana MINGW64 ~/Documents/tesis
$ cd FaceRecognition2/

Asus@Dayana MINGW64 ~/Documents/tesis/FaceRecognition2 (master)
$ ls
capture.py          listaPermitidos.py
entrenamiento.png  README.md
haarcascade_frontalface_alt.xml  reconocido.png
haarcascade_frontalface_default.xml  reconocimiento.py

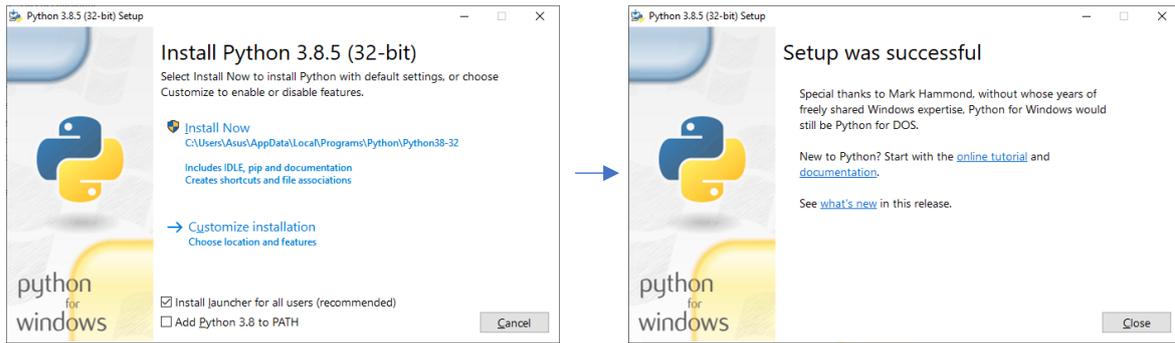
Asus@Dayana MINGW64 ~/Documents/tesis/FaceRecognition2 (master)
$ python3 capture.py

```

Se realiza la clonación del repositorio, que utiliza el protocolo de transferencia SSH. archivos programables en Python.

Nombre	Fecha de modificación	Tipo	Tamaño
__pycache__	10/09/2020 9:15 p. m.	Carpeta de archivos	
att_faces	28/08/2020 11:12 p. m.	Carpeta de archivos	
.gitignore	8/05/2018 11:41 a. m.	Documento de te...	1 KB
capture	29/08/2020 12:37 a. m.	Python File	3 KB
entrenamiento	8/05/2018 11:41 a. m.	Archivo PNG	711 KB
haarcascade_frontalface_alt	8/05/2018 11:41 a. m.	Documento XML	899 KB
haarcascade_frontalface_default	8/05/2018 11:41 a. m.	Documento XML	909 KB
listaPermitidos	10/09/2020 8:59 p. m.	Python File	5 KB
menu	14/09/2020 6:05 p. m.	Python File	2 KB
README.md	8/05/2018 11:41 a. m.	Archivo MD	3 KB
reconocido	8/05/2018 11:41 a. m.	Archivo PNG	527 KB
reconocimiento	4/10/2020 5:36 p. m.	Python File	4 KB

Se instala python



```

Simbolo del sistema - pip install opencv-contrib-python
Microsoft Windows [Versión 10.0.18362.1016]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Asus>pip install
ERROR: You must give at least one requirement to install (see "pip help install")
WARNING: You are using pip version 20.1.1; however, version 20.2.2 is available.
You should consider upgrading via the 'c:\users\asus\appdata\local\programs\python\python38-32\python.exe -m pip install --upgrade pip' command.

C:\Users\Asus>python --version

C:\Users\Asus>ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Asus>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Asus>pip install opencv-contrib-python
Collecting opencv-contrib-python
  Downloading opencv_contrib_python-4.4.0.42-cp38-cp38-win32.whl (29.9 MB)
    | 18.8 MB 409 kB/s eta 0:00:28
  
```

A continuación, se instalan las librerías de Python que es el *opencv contrib* viene incluido un montón de paquetes como *numpy* que es una librería que maneja *arrays*.

```

Simbolo del sistema
C:\Users\Asus>pip install
ERROR: You must give at least one requirement to install (see "pip help install")
WARNING: You are using pip version 20.1.1; however, version 20.2.2 is available.
You should consider upgrading via the 'c:\users\asus\appdata\local\programs\python\python38-32\python.exe -m pip install --upgrade pip' command.

C:\Users\Asus>python --version

C:\Users\Asus>ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Asus>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Asus>pip install opencv-contrib-python
Collecting opencv-contrib-python
  Downloading opencv_contrib_python-4.4.0.42-cp38-cp38-win32.whl (29.9 MB)
    | 29.9 MB 328 kB/s
Collecting numpy>=1.17.3
  Downloading numpy-1.19.1-cp38-cp38-win32.whl (10.9 MB)
    | 10.9 MB 190 kB/s
Installing collected packages: numpy, opencv-contrib-python
Successfully installed numpy-1.19.1 opencv-contrib-python-4.4.0.42
WARNING: You are using pip version 20.1.1; however, version 20.2.2 is available.
You should consider upgrading via the 'c:\users\asus\appdata\local\programs\python\python38-32\python.exe -m pip install --upgrade pip' command.

C:\Users\Asus>
  
```

Básicamente lo que es el jefe del proyecto es el *header_frontalfaces.xml* que es un archivo que se generó a partir de millones de rostros que ya tiene las interacciones que tiene que hacer para reconocer el rostro, como fotos, videos y en tiempo real, son las coordenadas de la cara de una persona. }

Anexo 6

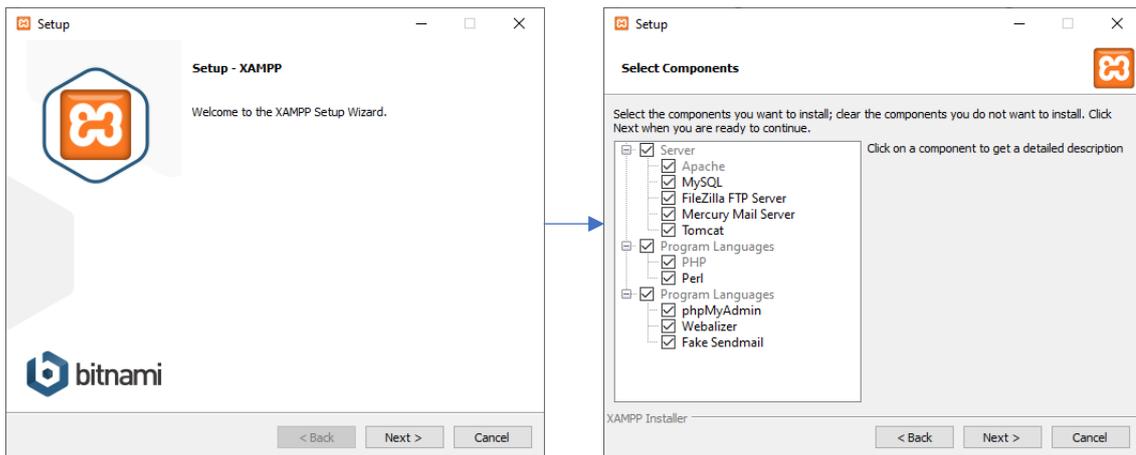
Instalación de XAMPP

Paso 1: Las versiones con PHP 5.5, 5.6 o 7 se pueden descargar gratuitamente desde la página del proyecto Apache Friends para Windows

Paso 2: Ejecutar el archivo .exe

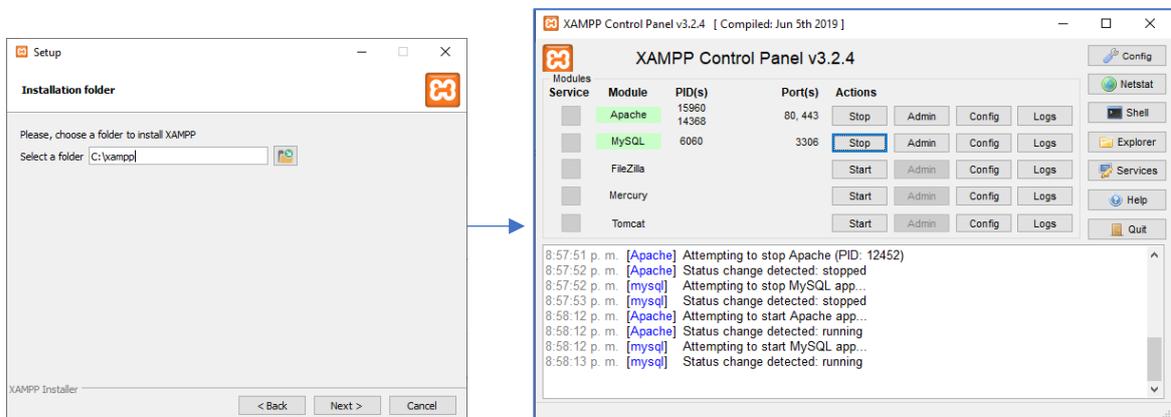
Paso 3: Iniciar el asistente de instalación

Paso 4: selección de los componentes del software

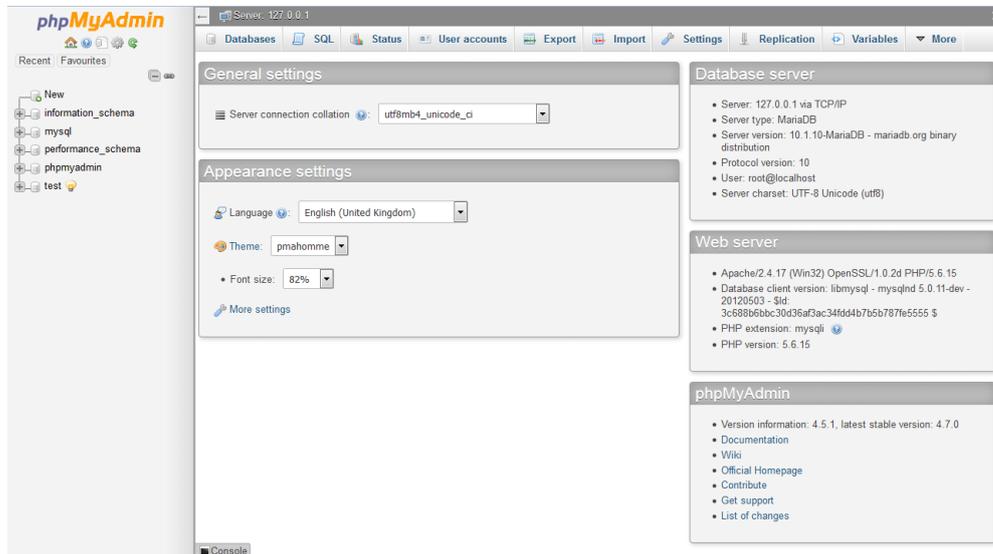


Paso 5: Seleccionamos la carpeta donde se guarde y listo, se tiene ya el ingreso al panel de control de xampp

Una causa frecuente de fallos en el uso de Apache es un **puerto bloqueado**. La configuración estándar XAMPP suele asignar al servidor web el puerto principal 80 y el puerto SSL 443, pero suelen estar bloqueados por otros programas. En la figura anterior se muestra un conflicto con el programa de mensajería instantánea Skype, que está usando los puertos 80 y 443, por lo que el servidor no se puede iniciar.



Haciendo clic en la tecla “Admin” de la base de datos se abre **phpMyAdmin**, donde se pueden administrar las bases de datos del proyecto web que se quiere probar con XAMPP. También se puede acceder a la interfaz de administración para la base de datos MySQL en *localhost/phpmyadmin/*.



Anexo 7

Programación de “listaPermitidos.py”

```

listaPermitidos.py - C:\facerecognition\listaPermitidos.py (3.8.5)
File Edit Format Run Options Window Help
import mysql.connector
my_list = list()
import smtplib
import pendulum

class flabianos:

    def __init__(self):

        mydb = mysql.connector.connect(
            host="localhost",
            user="root",
            password="",
            database="sisfacial"
        )

        mycursor = mydb.cursor()

        mycursor.execute("SELECT nombre FROM usuariospermitidos")

        myresult = mycursor.fetchall()
        for row in myresult:
            my_list.append(row[0])
        self.Invitados= my_list

    def TuSiTuNo(self,EllosSi):
        #print(self.Invitados)
        if EllosSi in self.Invitados:
            print('Bienvenido {}'.format(EllosSi))

            SMTPserver = 'smtp.gmail.com'
            sender = 'accesescontrol@gmail.com'
            destination = ['adveliz4@gmail.com']
            fechahoy=pendulum.now().to_day_datetime_string()
            USERNAME = "accesescontrol@gmail.com"
            PASSWORD = "DayeliBM20"

            # typical values for text_subtype are plain, html, xml
            text_subtype = 'plain'

            content="""\
Acceso correcto a puerta biométrica al usuario: """+EllosSi+"" con la fecha de
"""+fechahoy

            subject="Sistema automático de control de acceso"

            import sys
            import os
            import re

            from smtplib import SMTP_SSL as SMTP      # this invokes the secure SMTP protocol (port 465, uses SSL)
            # from smtplib import SMTP                # use this for standard SMTP protocol (port 25, no encryption)

            # old version
            # from email.MIMEText import MIMEText
            from email.mime.text import MIMEText

            try:
                msg = MIMEText(content, text_subtype)
                msg['Subject']= subject
                msg['From'] = sender # some SMTP servers will do this automatically, not all

                conn = SMTP(SMTPserver)
                conn.set_debuglevel(False)
                conn.login(USERNAME, PASSWORD)
                try:
                    conn.sendmail(sender, destination, msg.as_string())

            finally:
                conn.quit()
                print("Mensaje enviado")

```

Activar Windows
Ve a Configuración para

Activar Windows
Ve a Configuración para

Ln: 1 Col: 0

```

listaPermitidos.py - C:\facerecognition\listaPermitidos.py (3.8.5)
File Edit Format Run Options Window Help

    finally:
        conn.quit()
        print("Mensaje enviado")

    except:
        sys.exit( "mail failed; %s" % "CUSTOM_ERROR" ) # give an error message
else:
    print('Lo siento {}, no tiene permitido la entrada'.format(EllosSi))
    SMTPserver = 'smtp.gmail.com'
    sender = 'accesescontrol@gmail.com'
    destination = ['adveliz4@gmail.com']
    fechahoy=pendulum.now().to_day_datetime_string()
    USERNAME = "accesescontrol@gmail.com"
    PASSWORD = "DayeliBM20"

    # typical values for text_subtype are plain, html, xml
    text_subtype = 'plain'

    content="""\
    Se intento acceder un usuario desconocido del sistema con fecha de:
    """+fechahoy

    subject="Sistema automtico de control de acceso"

    import sys
    import os
    import re

    from smtplib import SMTP_SSL as SMTP # this invokes the secure SMTP protocol (port 465, uses SSL)
    # from smtplib import SMTP # use this for standard SMTP protocol (port 25, no encryption)

    # old version
    # from email.MIMEText import MIMEText
    from email.mime.text import MIMEText

    try:
        msg = MIMEText(content, text_subtype)
        msg['Subject']= subject
    import sys
    import os
    import re

    from smtplib import SMTP_SSL as SMTP # this invokes the secure SMTP protocol (port 465, uses SSL)
    # from smtplib import SMTP # use this for standard SMTP protocol (port 25, no encryption)

    # old version
    # from email.MIMEText import MIMEText
    from email.mime.text import MIMEText

    try:
        msg = MIMEText(content, text_subtype)
        msg['Subject']= subject
        msg['From'] = sender # some SMTP servers will do this automatically, not all

        conn = SMTP(SMTPserver)
        conn.set_debuglevel(False)
        conn.login(USERNAME, PASSWORD)
        try:

            conn.sendmail(sender, destination, msg.as_string())

        finally:
            conn.quit()
            print("Mensaje enviado")

    except:
        sys.exit( "mail failed; %s" % "CUSTOM_ERROR" ) # give an error message

```

Activar Windows
Ve a Configuracin para

Activar Windows
Ve a Configuracin para

Ln: 1 Col: 0

Anexo 8

Programación de “Reconocimiento.py”

```

reconocimiento.py - C:\facerecognition\reconocimiento.py (3.8.5)
File Edit Format Run Options Window Help
#OpenCV module
import cv2
#Modulo para leer directorios y rutas de archivos
import os
#OpenCV trabaja con arreglos de numpy
import numpy
import mysql.connector
#Se importa la lista de personas con acceso al laboratorio
from listaPermitidos import flabianos
flabs=flabianos()
validst=2
# Parte 1: Creando el entrenamiento del modelo
print('Formando...')

#Directorio donde se encuentran las carpetas con las caras de entrenamiento
dir_faces = 'att_faces/orl_faces'

#Tamaño para reducir a miniaturas las fotografías
size = 4

# Crear una lista de imagenes y una lista de nombres correspondientes
(images, lables, names, id) = ([], [], {}, 0)
for (subdirs, dirs, files) in os.walk(dir_faces):
    for subdir in dirs:
        names[id] = subdir
        subjectpath = os.path.join(dir_faces, subdir)
        for filename in os.listdir(subjectpath):
            path = subjectpath + '/' + filename
            lable = id
            images.append(cv2.imread(path, 0))
            lables.append(int(lable))
            id += 1
(im_width, im_height) = (112, 92)

# Crear una matriz Numpy de las dos listas anteriores
(images, lables) = [numpy.array(lis) for lis in [images, lables]]
# OpenCV entrena un modelo a partir de las imagenes
model = cv2.face.LBPHFaceRecognizer_create()
model.train(images, lables)

# Parte 2: Utilizar el modelo entrenado en funcionamiento con la camara
face_cascade = cv2.CascadeClassifier( 'haarcascade_frontalface_default.xml')
cap = cv2.VideoCapture(0)

while True:
    #leemos un frame y lo guardamos
    rval, frame = cap.read()
    frame=cv2.flip(frame,1,0)

    #convertimos la imagen a blanco y negro
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)

    #redimensionar la imagen
    mini = cv2.resize(gray, (int(gray.shape[1] / size), int(gray.shape[0] / size)))

    """buscamos las coordenadas de los rostros (si los hay) y
    guardamos su posicion"""
    faces = face_cascade.detectMultiScale(mini)
    validt=0
    for i in range(len(faces)):
        face_i = faces[i]
        (x, y, w, h) = [v * size for v in face_i]
        face = gray[y:y + h, x:x + w]
        face_resize = cv2.resize(face, (im_width, im_height))

```

Ln: 1 Col: 0

```

reconocimiento.py - C:\facerecognition\reconocimiento.py (3.8.5)
File Edit Format Run Options Window Help

# Intentado reconocer la cara
prediction = model.predict(face_resize)

#Dibujamos un rectangulo en las coordenadas del rostro
cv2.rectangle(frame, (x, y), (x + w, y + h), (0, 255, 0), 3)

# Escribiendo el nombre de la cara reconocida
# La variable cara tendra el nombre de la persona reconocida
cara = '%s' % (names[prediction[0]])

#Si la prediccion tiene una exactitud menor a 100 se toma como prediccion valida
if prediction[1]<100 :
    #Ponemos el nombre de la persona que se reconoció
    cv2.putText(frame, '%s - %.0f' % (cara,prediction[1]),(x-10, y-10), cv2.FONT_HERSHEY_PL
    #En caso de que la cara sea de algun conocido se realizara determinadas acciones
    #Busca si los nombres de las personas reconocidas estan dentro de los que tienen acces
    #print(cara)
    while(validt==0):
        flabs.TuSiTuNo(cara)
        validt=1

#Si la prediccion es mayor a 100 no es un reconocimiento con la exactitud suficiente
elif prediction[1]>101 and prediction[1]<500:
    #flabs=flabianos()
    #Si la cara es desconocida, poner desconocido
    cv2.putText(frame, 'Desconocido',(x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
    while(validst==2):
        flabs.TuSiTuNo("desconocido")
        validst=1
    #Mostramos la imagen
    cv2.imshow('OpenCV Reconocimiento facial', frame)

#Si se presiona la tecla ESC se cierra el programa
key = cv2.waitKey(10)
if key == 27:
    cv2.destroyAllWindows()
    break

```

Ln: 1 Col: 0

Anexo 9

Programación de “menu.py” “”

```

menu.py - C:\facerecognition\menu.py (3.8.5)
File Edit Format Run Options Window Help
import keyboard
import sys
import os
selected = 1

def show_menu():
    global selected
    print("\n" * 30)
    print("Bienvenidos a Face Access")
    print("Escoge una opción:")
    menu="Inicio"
    for i in range(1, 4):
        if i==1:
            variable="1"
        if(i==2):
            menu="Registro control de Acceso"
            variable="2"
        elif i==3:
            menu="Control de Acceso"
            variable="3"
        elif i==4:
            variable="4"
            menu="Salir"
        print(variable+" . "+menu+" {2}".format(i, ">" if selected == i else " ", "<" if selected == i else " "))

    if(selected==1):
        print("Seleccione las otras opciones..")
    elif selected==2:
        print("Desea ingresar a esta opcion (Y-N)");
        opcion= input()
        if opcion =='Y' :
            print("Ingrese nombre: ")
            nombre = input()
            os.popen('python capture.py '+nombre).read()
        else:
            selected=3
            show_menu()

    elif selected==3:
        print("Desea ingresar a esta opcion (Y-N)");
        opcion= input()
        if opcion =='Y' :
            os.popen('python reconocimiento.py').read()
        else:
            selected=1
            show_menu()

    elif selected==4:
        print("Saliendo...")
        exit()

def up():
    global selected
    if selected == 1:
        return
    selected -= 1
    show_menu()

def down():
    global selected
    if selected == 4:
        return
    selected += 1
    show_menu()

show_menu()
keyboard.add_hotkey('up', up)
keyboard.add_hotkey('down', down)
keyboard.wait()

```

Activar
Ve a Cop
Ln: 1 Col: 0

Anexo 10

Programación de “capture.py”

```

capture.py - C:\facerecognition\capture.py (3.8.5)
File Edit Format Run Options Window Help

#OpenCV module
import cv2
#Modulo para leer directorios y rutas de archivos
import os
#OpenCV trabaja con arreglos de numpy
import numpy

#Obtener el nombre de la persona que estamos capturando
import sys
import mysql.connector
nombre = sys.argv[1]

#Directorio donde se encuentra la carpeta con el nombre de la persona
dir_faces = 'att_faces/orl_faces'
path = os.path.join(dir_faces, nombre)

#Tamaño para reducir a miniaturas las fotografías
size = 4
validate=1
#Si no hay una carpeta con el nombre ingresado entonces se crea
if not os.path.isdir(path):
    os.mkdir(path)

#Cargamos la plantilla e inicializamos la webcam
face_cascade = cv2.CascadeClassifier('haarcascade_frontalface_default.xml')
cap = cv2.VideoCapture(0)

img_width, img_height = 112, 92

#Ciclo para tomar fotografías
count = 0
while count < 100:
    #leemos un frame y lo guardamos
    rval, img = cap.read()
    img = cv2.flip(img, 1, 0)

    #convertimos la imagen a blanco y negro
    gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)

    #redimensionar la imagen
    mini = cv2.resize(gray, (int(gray.shape[1] / size), int(gray.shape[0] / size)))

    """buscamos las coordenadas de los rostros (si los hay) y
    guardamos su posicion"""
    faces = face_cascade.detectMultiScale(mini)
    faces = sorted(faces, key=lambda x: x[3])

    if faces:
        face_i = faces[0]
        (x, y, w, h) = [v * size for v in face_i]
        face = gray[y:y+h, x:x+w]
        face_resize = cv2.resize(face, (img_width, img_height))

        #Dibujamos un rectangulo en las coordenadas del rostro
        cv2.rectangle(img, (x, y), (x + w, y + h), (0, 255, 0), 3)
        #Ponemos el nombre en el rectagulo
        cv2.putText(img, nombre, (x - 10, y - 10), cv2.FONT_HERSHEY_PLAIN, 1, (0, 255, 0))
        #El nombre de cada foto es el numero del ciclo
        #Obtenemos el nombre de la foto
        #Despues de la ultima sumamos 1 para continuar con los demas nombres
        pin=sorted([int(n[:n.find('.')]) for n in os.listdir(path)
                    if n[0]!='.' ]+[0])[-1] + 1

        #Metemos la foto en el directorio
        cv2.imwrite('%s/%s.png' % (path, pin), face_resize)
        #Contador del ciclo
        count += 1

    #Mostramos la imagen
    cv2.imshow('OpenCV Entrenamiento de '+nombre, img)

    while (validate==1):
        mydb = mysql.connector.connect(
            host="localhost",
            user="root",
            password="",
            database="sisfacial"
        )
        mycursor = mydb.cursor()
        separador = " "
        finalstring = nombre.split(separador)
        sql = "INSERT INTO usuariospermitidos (nombre, apellido) VALUES (%s, %s)"
        val = (nombre,nombre)
        mycursor.execute(sql, val)
        mydb.commit()

        print(mycursor.rowcount, "Guardado en la base de datos.")
        validate=0

    #Si se presiona la tecla ESC se cierra el programa
    key = cv2.waitKey(10)
    if key == 27:
        cv2.destroyAllWindows()
        break

```

Anexo 11

Pruebas de funcionalidad en usuarios

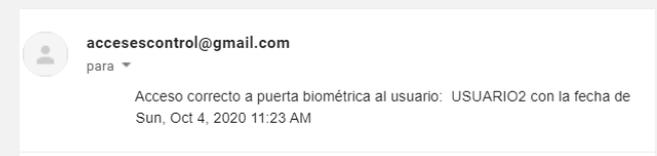
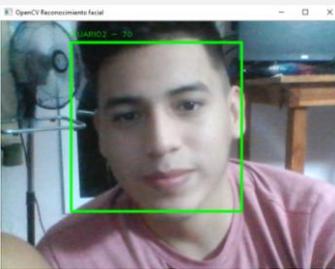
USUARIO1

NOTIFICACIÓN



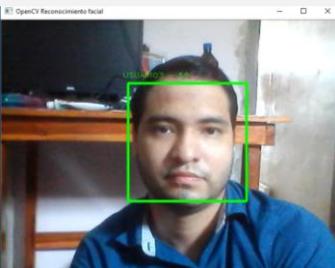
USUARIO2

NOTIFICACIÓN



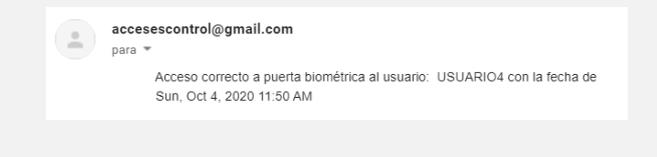
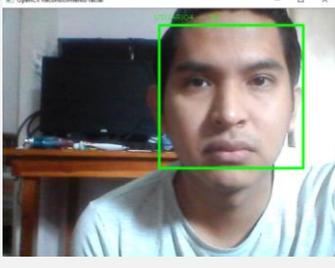
USUARIO3

NOTIFICACIÓN



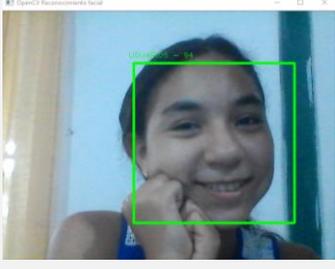
USUARIO4

NOTIFICACIÓN



USUARIO5

NOTIFICACIÓN



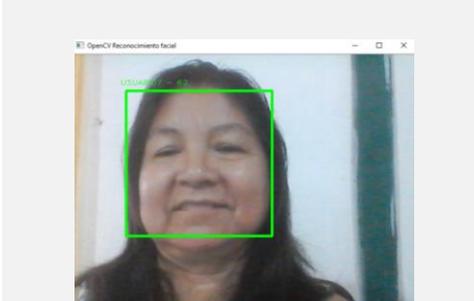
USUARIO6



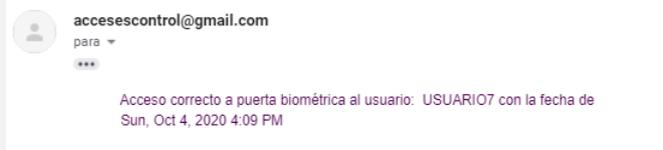
NOTIFICACIÓN



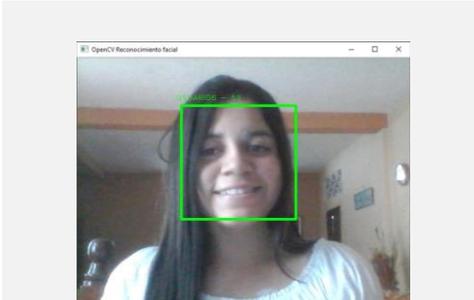
USUARIO7



NOTIFICACIÓN



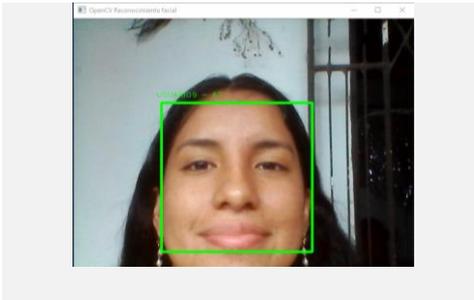
USUARIO8



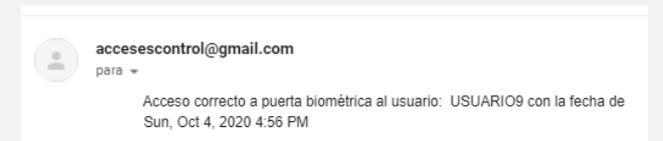
NOTIFICACIÓN



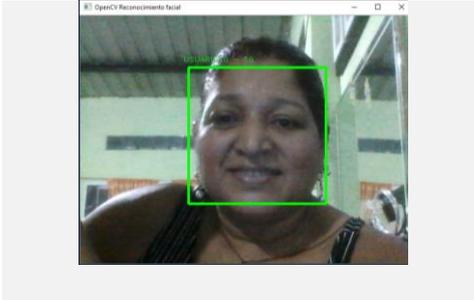
USUARIO9



NOTIFICACIÓN



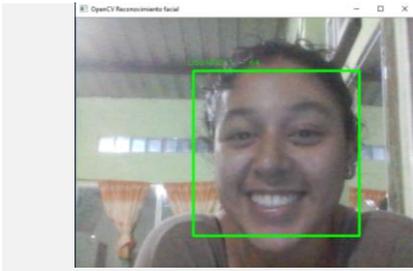
USUARIO10



NOTIFICACIÓN



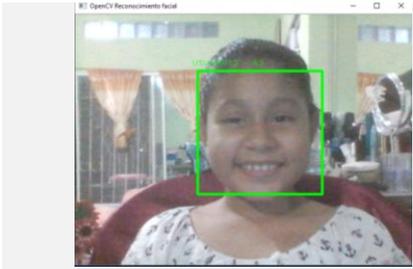
USUARIO11



NOTIFICACIÓN



USUARIO12



NOTIFICACIÓN



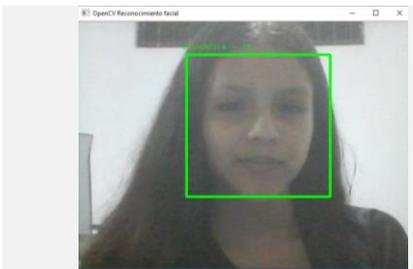
USUARIO13



NOTIFICACIÓN



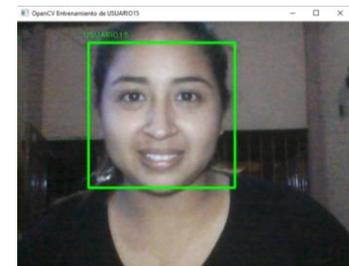
USUARIO14



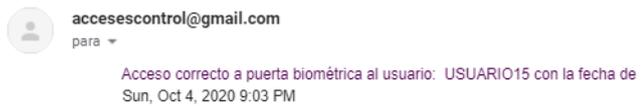
NOTIFICACIÓN



USUARIO15



NOTIFICACIÓN



3.16. Referencia bibliográfica

- Alvear Erazo, R. (2018). *Repositorio Digital Universidad De Las Américas*. Obtenido de Tecnologías Tecnología en Exportaciones e Importaciones: <http://dspace.udla.edu.ec/handle/33000/9426>
- Belhumeur, Hespanha , & Kriegman . (2018). Eigenfaces vs. Fisherfaces. *ecognition Using Class Specic Linear Projection. Transactions on pattern analysis and Machine Intelligence*, 711,720.
- Bertomeu, P. (Abril de 2010). *Diposit*. Obtenido de Diposit: <http://diposit.up.edu/dspace/bitstream/2445/99003/1/entrevista%20pf.pdf>
- Bradski, & Kaehler. (s.f.). *Learning OpenCV Vision with the OpenCV Library*. Obtenido de www.cse.iitk.ac.in
- California Institute of Technology. (2016). *Spitzer, Space Telescope*. Obtenido de http://legacy.spitzer.caltech.edu/espanol/edu/learn_ir/
- Carrod Electrónica Online S. . (2020). *Carrod Electrónica Online S*. Obtenido de <https://www.carrod.mx/products/cerradura-electronica-solenoid-12-v-para-puerta>
- Carvajal, L. (8 de junio de 2017). *Carvajal.com*. Obtenido de <https://www.lizardo-carvajal.com/el-metodo-deductivo-de-investigacion/>
- Chaur , B. (2015). *Metodologías de diseño*. Obtenido de Ingeniería del diseño: <https://www.tdx.cat/bitstream/handle/10803/6837/05Jcb05de16.pdf?sequence=5&isAllowed=y>
- Cobo , A. (2016). *PHP y MySQL - Tecnología para el desarrollo de aplicaciones web*. Ediciones Díaz de Santos.
- Conceptodefinicion. (17 de Julio de 2019). *ConceptoDefinicion*. Obtenido de <https://conceptodefinicion.de/tecnica/>
- CONSTITUCION DE LA REPUBLICA DEL ECUADOR. (2008). Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf
- digifort. (2019). SAFR from real networks. *Facial Recognition_&_Machine Learning_SAFR*, (págs. 1,2). Chile.
- Digitalguide-IONOS. (03 de 09 de 2019). *Digitalguide-IONOS*. Obtenido de Instala tu servidor local XAMPP en unos pocos pasos:

- <https://www.ionos.es/digitalguide/servidores/herramientas/instala-tu-servidor-local-xampp-en-unos-pocos-pasos/>
- EcuRed*. (5 de Marzo de 2015). Obtenido de Biometría facial:
https://www.ecured.cu/Biometría_facial
- Ezpinoza Olguín, D., & Jorquera Guillen, P. (Junio de 2015). *PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO*. Obtenido de FACULTAD DE INGENIERÍA, ESCUELA DE INGENIERÍA INFORMÁTICA:
http://opac.pucv.cl/pucv_txt/txt-1000/UCD1453_01.pdf
- Fastly. (2020). *Apache Friends*. Obtenido de XAMPP Apache + MariaDB + PHP + Perl.
- Ferreyra, M. (2016). *Universidad Nacional de Cordoba*. Obtenido de Diseño de cerradura electromecánica con control RFID.
- Gandhi, M. (27 de Noviembre de 2019). *Autycom - Innovación Inteligente*. Obtenido de ¿Qué es un sistema de control?: <https://www.autycom.com/que-es-un-sistema-de-control/>
- Gil Lucero, A. A. (24 de Julio de 2015). *BASE DE DATOS USAC PUERTO BARRIOS*. Obtenido de <https://usacdatospb.wordpress.com/2015/07/11/que-son-las-bases-de-datos/>
- Gualpa Carrión, S. (2017). *Repositorio Digital Institucional de la Escuela Politécnica Nacional*. Obtenido de BIBDIGITAL:
<https://bibdigital.epn.edu.ec/handle/15000/4103>
- Hernandez, Fernandez, & Baptista. (2013). *epacartagena.gov*. Mexico: JRP.
- Kimaldi. (2020). *Blog / Biometría / Reconocimiento facial*. Obtenido de https://www.kimaldi.com/blog/biometria/reconocimiento_facial/
- Microsoft. (1 de Septiembre de 2015). *Desarrollo de la plataforma universal de Windows*. Obtenido de <https://visualstudio.microsoft.com/es/vs/features/universal-windows-platform/>
- Nora. (Junio de 2014). *Faud*. Obtenido de http://www.faud.unsj.edu.ar/descargas/blogs/apuntes-de-ctedra-mtodos-y-estrategias-de-diseo_Metodos%20y%20Estrategias%20de%20Dise%C3%B1o.pdf
- Ochoa, A. (Enero de 2015). *Univeridad Veracruzana, Repositorio Institucional*. Obtenido de <https://cdigital.uv.mx/handle/123456789/46819>
- OpenCV Org. (2017). Obtenido de http://docs.opencv.org/modules/contrib/doc/facerec/facerec_tutorial.html.

- Poveda, M., Merchan, F., & Poveda, H. (2017). *Universidad Tecnológica de Panamá*. Obtenido de IMPLEMENTACIÓN DE SISTEMA DE RECONOCIMIENTO: https://www.researchgate.net/profile/Hector_Poveda/publication/275024108_Implementacion_de_sistema_de_reconocimiento_facial_en_tiempo_real_para_control_de_acceso/links/552ef15c0cf2d495071a92c1/Implementacion-de-sistema-de-reconocimiento-facial-en-tiempo-r
- Ramon, & Gimeno, R. (2017). *Estudio de técnicas de reconocimiento facial*. Obtenido de http://upcommons.upc.edu/bitstream/handle/2099.1/9782/PFC_RogerGimen
- Robledano, Á. (18 de Junio de 2019). *OpenWebinars S.L*. Obtenido de Qué es un algoritmo informático: <https://openwebinars.net/blog/que-es-un-algoritmo-informatico/>
- Ronsabay, J. (2014). *Gimnasia Cerebral*. Obtenido de <http://tugimnasiacerebral.com/herramientas-de-estudio/que-es-una-encuesta-caracteristicas-y-como-hacerlas>
- S.Li, & Jain, A. (2015). Handbook of face recognition. 2.
- Sánchez, M. Á. (22 de Noviembre de 2017). *Clean Code*. Obtenido de Patrones de Diseño de Software: <https://medium.com/all-you-need-is-clean-code/patrones-de-dise%C3%B1o-b7a99b8525e>
- Saúl, G. (16 de Junio de 2020). *330ohms*. Obtenido de <https://blog.330ohms.com/2020/06/16/como-conectar-un-solenoid-a-arduino/#:~:text=Para%20controlar%20un%20solenoid%20con,una%20se%C3%B1al%20digital%20de%20control>.
- Sherlin. (22 de Febrero de 2014). *Electrónica teórica y práctica*. Obtenido de <https://sherlin.xbot.es>
- Thibaud, C. (2015). *MySQL 5: instalación, implementación, administración, programación*. Ediciones.
- Torres, D. (9 de Octubre de 2017). *HETPRO*. Obtenido de <https://hetpro-store.com/TUTORIALES/que-es-un-relevador-o-rele/>