



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

**Diseño e implementación de un prototipo de sistema biométrico para mejorar el registro de acceso de personal utilizando reconocimiento facial en la empresa JVA Tecnología**

Silva Echeverría, Josué Leonidas

Departamento de Ciencias de la Energía y Mecánica

Carrera de Ingeniería Mecatrónica

Trabajo de Titulación, previo a la obtención del Título de Ingeniero Mecatrónico

Ing. Mendoza Chipantasi, Darío José M. Sc.

2023

Latacunga

## Reporte de verificación de contenido

# INFORME DE DETECCIÓN DE PLAGIO

EL INFORME CERTIFICA QUE EL DOCUMENTO ADJUNTO

*Tesis\_Josue.docx*

FUE REVISADO CON EL SERVICIO DE PREVENCIÓN DE PLAGIO MY.PLAGRAMME.COM Y TIENE:

SIMILITUD

**8%**

RIESGO DE PLAGIO

**21%**

PARÁFRASIS

1%

CITAS INCORRECTAS


0%

Nombre del archivo: Tesis\_Josue.docx

Archivo verificado: 2023-02-16

Informe generado: 2023-02-16

Firma:



Ing. Darío Mendoza M. Sc.

C.C. 0603110834



Departamento de Ciencias de la Energía y Mecánica

Carrera de Ingeniería Mecatrónica

### Certificación

Certifico que el trabajo de titulación: **“Diseño e implementación de un prototipo de sistema biométrico para mejorar el registro de acceso de personal utilizando reconocimiento facial en la empresa JVA Tecnología”** fue realizado por el señor **Silva Echeverría, Josué Leonidas**; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Latacunga, 17 de febrero de 2023

Firma:

Ing. Mendoza Chipantasi, Dario José M. Sc.

C. C 0603110834



**Departamento de Ciencias de la Energía y Mecatrónica**  
**Carrera de Ingeniería Mecatrónica**

**Responsabilidad de Autoría**

Yo, **Silva Echeverría, Josué Leonidas**, con cédula de ciudadanía n°1805352349, declaro que el contenido, ideas y criterios del trabajo de titulación: **“Diseño e implementación de un prototipo de sistema biométrico para mejorar el registro de acceso de personal utilizando reconocimiento facial en la empresa JVA Tecnología”** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

**Latacunga, 17 de febrero de 2023**

Firma:

**Silva Echeverría, Josué Leonidas**

C. C 1805352349



Departamento de Ciencias de la Energía y Mecatrónica

Carrera de Ingeniería Mecatrónica

**Autorización de Publicación**

Yo, **Silva Echeverría, Josué Leonidas**, con cédula de ciudadanía n° 1805352349, autorizó a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Diseño e implementación de un prototipo de sistema biométrico para mejorar el registro de acceso de personal utilizando reconocimiento facial en la empresa JVA Tecnología"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 17 de febrero de 2023

Firma:

.....  
**Silva Echeverría, Josué Leonidas**

C. C 1805352349

### **Dedicatoria**

*Esta tesis se la dedico a mi familia, que me ha brindado todo el apoyo necesario para la culminación de mi carrera profesional. Esta etapa ha sido larga y a veces difícil, pero gracias a su apoyo constante y amor incondicional, he podido superar todos los obstáculos y llegar hasta aquí. Ustedes han sido mi roca y mi fuente de motivación, y estoy eternamente agradecido por todo lo que han hecho por mí. Gracias por creer en mí incluso cuando yo mismo dudaba, y por siempre estar ahí con una sonrisa y un abrazo cuando más los necesitaba. Esta tesis es una muestra de mi arduo trabajo y dedicación, pero también es un reflejo de su influencia en mi vida. Gracias por ser mi ejemplo a seguir y por enseñarme que, con esfuerzo y determinación, todo es posible. Con todo mi amor y gratitud, dedico esta tesis a ustedes, mis queridos padres.*

## **Agradecimiento**

*Para la realización de la presente tesis agradezco a mis queridos padres, por su amor y ayuda incomparable. También a mis hermanos María Victoria y Enoc Emilio: que gracias a su motivación obtuve las fuerzas necesarias para el cumplimiento de mis metas en cuanto a la obtención de mi título profesional. A las autoridades, personal docente y personal administrativo de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga, que con su vasto y oportuno conocimiento científico, experimental, tecnológico y técnico me han favorecido de las sabias enseñanzas para mi carrera profesional.*

*Como creyente en Dios y en el Señor Jesucristo que me ha hecho entender el propósito del hombre en la tierra que me ha fortalecido en todo momento a través de su palabra en la Biblia. Josué 1:9. "Yo te he ordenado que seas fuerte y valiente, que no temas ni desmayes porque yo soy el Señor tu Dios".*

**ÍNDICE DE CONTENIDOS**

Carátula .....	1
Reporte de verificación de contenido .....	2
Certificación .....	3
Responsabilidad de Autoría .....	4
Autorización de Publicación .....	5
Dedicatoria.....	6
Agradecimiento.....	7
Índice de contenidos .....	8
Índice de tablas .....	14
Índice de figuras .....	16
Resumen .....	20
Abstract.....	21
Capítulo I: Aspectos generales y marco teórico.....	22
Antecedentes.....	22
Planteamiento del problema .....	24
Justificación e importancia.....	25
Objetivos .....	26
<i>Objetivo general</i> .....	26
<i>Objetivos específicos</i> .....	27
<i>Metas</i> .....	27
Hipótesis .....	28



Variables de investigación.....	28
<i>Variable Independiente</i> .....	28
<i>Variable dependiente</i> .....	28
Marco teórico.....	29
<i>Visión artificial</i> .....	29
<i>Componentes del sistema de visión artificial</i> .....	29
<i>Biometría</i> .....	31
<i>Etapas de un sistema de identificación biométrica</i> .....	31
<i>Reconocimiento facial</i> .....	32
<i>Técnicas de extracción de características</i> .....	33
<i>Métodos de entrenamiento de reconocimiento de rostros</i> .....	34
<i>Anti-Spoofing</i> .....	34
<i>Base de datos</i> .....	35
<i>SQL</i> .....	36
<i>Norma ISO 9241</i> .....	37
<i>Lenguaje de Programación a utilizar en el desarrollo</i> .....	38
Python.....	38
OpenCV .....	38
Capítulo II: Diseño y selección de componentes del sistema .....	40
Metodología .....	40
Requerimientos del sistema .....	40

<i>Identificación de necesidades</i> .....	40
<i>Métricas</i> .....	41
<i>Matriz necesidades-métricas</i> .....	42
Planteamiento de especificaciones .....	43
Arquitectura del prototipo.....	44
<i>Esquema del prototipo</i> .....	44
Agrupación de los elementos del esquema.....	45
Alternativas y selección de componentes.....	46
Alternativas y selección de la tarjeta programable para visión artificial .....	47
<i>Alternativa 1. Raspberry Pi3 Model A+</i> .....	47
<i>Alternativa 2. Raspberry Pi3 Model B+</i> .....	47
<i>Alternativa 3. LattePanda Delta</i> .....	48
<i>Selección de la mejor alternativa de tarjeta programable</i> .....	49
Alternativas y selección de la cámara.....	50
<i>Alternativa 1. Cámara Web HD 480dpi</i> .....	50
<i>Alternativa 2. Webcam USB Mini Computer Camera</i> .....	50
<i>Alternativa 3. C270 HD Webcam</i> .....	51
<i>Selección de la mejor alternativa de la cámara</i> .....	52
Alternativas y selección de la pantalla.....	52
<i>Alternativa 1. Pantalla LCD táctil capacitiva de 7 pulgadas (H) con estuche</i> .....	52
<i>Alternativa 2. Pantalla LCD táctil capacitiva de 7 pulgadas (B)</i> .....	53

<i>Alternativa 3. Pantalla táctil capacitiva IPS de 5 pulgadas .....</i>	<b>54</b>
<i>Selección de la mejor alternativa para la pantalla.....</i>	<b>54</b>
<b>Alternativas y selección de opción biométrica .....</b>	<b>55</b>
<i>Alternativa 1. Lector de huella dactilar biométrico digital Fingerprint Kookye.....</i>	<b>55</b>
<i>Alternativa 2. Lector de huella digital FPM10A.....</i>	<b>55</b>
<i>Alternativa 3. Suprema RealSCAN-G10.....</i>	<b>56</b>
<i>Selección de la mejor alternativa biométrica.....</i>	<b>57</b>
<b>Capítulo III: Desarrollo e implementación del sistema .....</b>	<b>58</b>
<b>Diseño de la estructura mecánica.....</b>	<b>58</b>
<b>Análisis estático del diseño.....</b>	<b>59</b>
<i>Análisis de la estructura de soporte de pantalla.....</i>	<b>62</b>
<i>Análisis de estructura de soporte del lector de huella digital .....</i>	<b>68</b>
<b>Construcción del prototipo.....</b>	<b>72</b>
<b>Implementación para el reconocimiento facial .....</b>	<b>74</b>
<i>Configuración para el reconocimiento facial.....</i>	<b>76</b>
<i>Funcionamiento para la identificación facial.....</i>	<b>78</b>
<b>Implementación del subsistema de detección de vida .....</b>	<b>79</b>
<b>Implementación del subsistema del sensor biométrico .....</b>	<b>83</b>
<i>Configuración del lector de huella digital .....</i>	<b>84</b>
<i>Funcionamiento del lector de huella digital.....</i>	<b>84</b>
<b>Implementación del subsistema de la base de datos.....</b>	<b>85</b>

Subsistema de base de datos de acceso remoto .....	87
Conexión entre la aplicación en Python a las bases de datos.....	89
Implementación del subsistema de notificación por correo electrónico.....	90
Implementación del subsistema de generación de reporte.....	91
<i>Reporte de usuarios</i> .....	92
<i>Historial de registro</i> .....	92
<i>Planilla de Asistencia</i> .....	93
Envío de reporte por correo electrónico .....	94
Diseño de la interfaz de usuario.....	95
Capítulo IV: Pruebas de funcionamiento y análisis de resultados.....	98
Análisis del funcionamiento del sistema biométrico .....	98
Pruebas de funcionamiento de la interfaz del usuario.....	100
<i>Registro de usuarios</i> .....	103
Registro facial. ....	103
Registro manual por huella digital. ....	103
<i>Configuración</i> .....	104
Añadir usuario.....	104
Eliminar usuario.....	105
<i>Reporte</i> .....	106
Pruebas de funcionamiento.....	107
<i>Primer escenario</i> .....	107

<i>Segundo escenario</i> .....	108
<i>Tercer escenario</i> .....	110
<i>Cuarto escenario</i> .....	111
<i>Quinto escenario</i> .....	113
<i>Sexto escenario</i> .....	114
<i>Séptimo escenario</i> .....	116
<i>Octavo escenario</i> .....	118
Validación de hipótesis .....	121
Capítulo V: Conclusiones y Recomendaciones.....	128
Conclusiones.....	128
Recomendaciones .....	130
Bibliografía .....	132
Anexos .....	138

## ÍNDICE DE TABLAS

<b>Tabla 1</b> <i>Necesidades del usuario</i> .....	<b>41</b>
<b>Tabla 2</b> <i>Características técnicas del sistema</i> .....	<b>41</b>
<b>Tabla 3</b> <i>Simbología de correlación entre necesidades y métricas</i> .....	<b>42</b>
<b>Tabla 4</b> <i>Resultados obtenidos de la matriz necesidades-métricas</i> .....	<b>43</b>
<b>Tabla 5</b> <i>Especificaciones generales del sistema</i> .....	<b>44</b>
<b>Tabla 6</b> <i>Criterio de análisis para la selección de alternativa</i> .....	<b>46</b>
<b>Tabla 7</b> <i>Matriz de selección de la tarjeta programable</i> .....	<b>49</b>
<b>Tabla 8</b> <i>Matriz de selección de la cámara</i> .....	<b>52</b>
<b>Tabla 9</b> <i>Matriz de selección de la pantalla</i> .....	<b>54</b>
<b>Tabla 10</b> <i>Matriz de selección del sensor biométrico</i> .....	<b>57</b>
<b>Tabla 11</b> <i>Datos recolectados de la medición del dedo índice en gramos-fuerza</i> .....	<b>60</b>
<b>Tabla 12</b> <i>Datos recolectados de la medición del dedo pulgar en gramos-fuerza</i> .....	<b>61</b>
<b>Tabla 13</b> <i>Promedio de la fuerza en los dedos de cada persona</i> .....	<b>61</b>
<b>Tabla 14</b> <i>Desglose de elementos diseñados para imprimir</i> .....	<b>72</b>
<b>Tabla 15</b> <i>Conexión entre el sensor de huella dactilar y el módulo USB-TTL</i> .....	<b>83</b>
<b>Tabla 16</b> <i>Promedio tiempo de procesamiento</i> .....	<b>99</b>
<b>Tabla 17</b> <i>Datos recogidos del primer escenario</i> .....	<b>108</b>
<b>Tabla 18</b> <i>Datos recogidos del segundo escenario</i> .....	<b>109</b>
<b>Tabla 19</b> <i>Datos recogidos del tercer escenario</i> .....	<b>111</b>
<b>Tabla 20</b> <i>Datos obtenidos del cuarto escenario</i> .....	<b>112</b>
<b>Tabla 21</b> <i>Datos recogidos del quinto escenario</i> .....	<b>114</b>
<b>Tabla 22</b> <i>Datos recogidos del sexto escenario</i> .....	<b>115</b>
<b>Tabla 23</b> <i>Datos recogidos del séptimo escenario</i> .....	<b>117</b>
<b>Tabla 24</b> <i>Datos recogidos del octavo escenario</i> .....	<b>119</b>
<b>Tabla 25</b> <i>Datos recopilados</i> .....	<b>120</b>

<b>Tabla 26</b> <i>Porcentaje de promedio de efectividad de las pruebas</i> .....	<b>120</b>
<b>Tabla 27</b> <i>Ejemplo para el factor sanción</i> .....	<b>121</b>
<b>Tabla 28</b> <i>Datos recogidos del prototipo</i> .....	<b>122</b>
<b>Tabla 29</b> <i>Datos del tiempo del registro manual</i> .....	<b>123</b>
<b>Tabla 30</b> <i>Datos para validación de hipótesis</i> .....	<b>124</b>
<b>Tabla 31</b> <i>Prueba t para medias de dos muestras emparejadas</i> .....	<b>127</b>

## ÍNDICE DE FIGURAS

<b>Figura 1</b> <i>Ejemplo de una aplicación de llenado de botella mediante visión artificial</i> .....	<b>29</b>
<b>Figura 2</b> <i>Etapas en un sistema de identificación biométrica</i> .....	<b>32</b>
<b>Figura 3</b> <i>Reconocimiento facial, técnicas Anti-spoofing</i> .....	<b>35</b>
<b>Figura 4</b> <i>Sistema de base de datos</i> .....	<b>36</b>
<b>Figura 5</b> <i>Lenguaje de consulta estructurada SQL</i> .....	<b>37</b>
<b>Figura 6</b> <i>Logo de Python</i> .....	<b>38</b>
<b>Figura 7</b> <i>Logo de OpenCV</i> .....	<b>39</b>
<b>Figura 8</b> <i>Matriz necesidades-métricas</i> .....	<b>42</b>
<b>Figura 9</b> <i>Esquema del prototipo</i> .....	<b>45</b>
<b>Figura 10</b> <i>Agrupación de los elementos del esquema del prototipo</i> .....	<b>45</b>
<b>Figura 11</b> <i>Sistemas y subsistemas del prototipo</i> .....	<b>46</b>
<b>Figura 12</b> <i>Raspberry Pi3 Model A+</i> .....	<b>47</b>
<b>Figura 13</b> <i>Raspberry Pi3 Model B+</i> .....	<b>48</b>
<b>Figura 14</b> <i>LattePanda Delta</i> .....	<b>48</b>
<b>Figura 15</b> <i>Cámara Web HD 480dpi</i> .....	<b>50</b>
<b>Figura 16</b> <i>Webcam USB Mini Computer Camera</i> .....	<b>51</b>
<b>Figura 17</b> <i>Cámara web HD C270</i> .....	<b>51</b>
<b>Figura 18</b> <i>Pantalla LCD táctil capacitiva de 7 pulgadas (H) con estuche</i> .....	<b>53</b>
<b>Figura 19</b> <i>Pantalla LCD táctil capacitiva de 7 pulgadas (B)</i> .....	<b>53</b>
<b>Figura 20</b> <i>Pantalla táctil capacitiva IPS de 5 pulgadas</i> .....	<b>54</b>
<b>Figura 21</b> <i>Lector de huella dactilar biométrico digital Fingerprint Kookye</i> .....	<b>55</b>
<b>Figura 22</b> <i>Lector de huella digital FPM10A</i> .....	<b>56</b>
<b>Figura 23</b> <i>Suprema RealSCAN-G10</i> .....	<b>56</b>
<b>Figura 24</b> <i>Diseño CAD del prototipo de sistema biométrico</i> .....	<b>58</b>
<b>Figura 25</b> <i>Diseño CAD del prototipo dividido en partes</i> .....	<b>59</b>



<b>Figura 26</b> <i>Medición de fuerza en el dedo tanto para hombre y mujer</i> .....	<b>60</b>
<b>Figura 27</b> <i>Soporte de pantalla dividida en tres zonas críticas</i> .....	<b>62</b>
<b>Figura 28</b> <i>Sección crítica seleccionada del soporte de pantalla</i> .....	<b>63</b>
<b>Figura 29</b> <i>Sección transversal de la zona 3 de análisis</i> .....	<b>65</b>
<b>Figura 30</b> <i>Simulación del factor de seguridad en el soporte de pantalla</i> .....	<b>67</b>
<b>Figura 31</b> <i>Simulación del desplazamiento del soporte de pantalla</i> .....	<b>68</b>
<b>Figura 32</b> <i>Descomposición de la fuerza en el lector de huella digital</i> .....	<b>68</b>
<b>Figura 33</b> <i>Diseño del soporte del lector de huella digital</i> .....	<b>69</b>
<b>Figura 34</b> <i>Áreas paralelas a la fuerza cortante en la muñeca</i> .....	<b>70</b>
<b>Figura 35</b> <i>Simulación del factor de seguridad del soporte de lector de huella digital</i> .....	<b>71</b>
<b>Figura 36</b> <i>Impresión 3D de los elementos de la estructura</i> .....	<b>73</b>
<b>Figura 37</b> <i>Esquema de conexión</i> .....	<b>74</b>
<b>Figura 38</b> <i>Ensamble del prototipo de sistema biométrico</i> .....	<b>74</b>
<b>Figura 39</b> <i>Diagrama de secuencia de la configuración para el reconocimiento facial</i> .....	<b>76</b>
<b>Figura 40</b> <i>Diagrama de secuencia del entrenamiento de la red neuronal</i> .....	<b>77</b>
<b>Figura 41</b> <i>Archivo .xml e histograma concatenado generado del entrenamiento</i> .....	<b>78</b>
<b>Figura 42</b> <i>Reconocimiento facial</i> .....	<b>78</b>
<b>Figura 43</b> <i>Obtención de la Malla Facial de MediaPipe</i> .....	<b>79</b>
<b>Figura 44</b> <i>Representación de los 6 puntos de referencia del ojo</i> .....	<b>80</b>
<b>Figura 45</b> <i>Trazado de la proporción de las distancias de los ojos</i> .....	<b>81</b>
<b>Figura 46</b> <i>Identificación de un rostro real y un rostro falso</i> .....	<b>82</b>
<b>Figura 47</b> <i>Diagrama de secuencia del algoritmo de detección de vida</i> .....	<b>82</b>
<b>Figura 48</b> <i>Diagrama de conexión entre el sensor de huellas dactilares y USB-TTL</i> .....	<b>83</b>
<b>Figura 49</b> <i>Diagrama secuencial de configuración del sensor de huella digital</i> .....	<b>84</b>
<b>Figura 50</b> <i>Diagrama secuencial del funcionamiento de la huella digital</i> .....	<b>85</b>
<b>Figura 51</b> <i>Creación de las tablas en la base de datos local en HeidiSQL</i> .....	<b>87</b>

<b>Figura 52</b> <i>Detalles de la base de datos creada en FreeSQLdatabase</i> .....	<b>87</b>
<b>Figura 53</b> <i>Información de acceso para la base de datos remota</i> .....	<b>88</b>
<b>Figura 54</b> <i>Base de datos en phpMyAdmin</i> .....	<b>89</b>
<b>Figura 55</b> <i>Conexión establecida entre Python y la base de datos HeidiSQL</i> .....	<b>90</b>
<b>Figura 56</b> <i>Notificación de atraso por correo electrónico</i> .....	<b>91</b>
<b>Figura 57</b> <i>Reporte de usuarios</i> .....	<b>92</b>
<b>Figura 58</b> <i>Reporte de historial de registro</i> .....	<b>93</b>
<b>Figura 59</b> <i>Planilla de Asistencia</i> .....	<b>94</b>
<b>Figura 60</b> <i>Envío del reporte generado por correo electrónico</i> .....	<b>95</b>
<b>Figura 61</b> <i>Interfaz de Usuario</i> .....	<b>96</b>
<b>Figura 62</b> <i>Diagrama secuencial de registro de usuario</i> .....	<b>97</b>
<b>Figura 63</b> <i>Autenticación por registro facial y registro dactilar</i> .....	<b>98</b>
<b>Figura 64</b> <i>Ventana 1 para iniciar sesión</i> .....	<b>100</b>
<b>Figura 65</b> <i>Mensajes de error al inicio de sesión</i> .....	<b>101</b>
<b>Figura 66</b> <i>Ventana 2 del menú de opciones</i> .....	<b>101</b>
<b>Figura 67</b> <i>Ventana 4 con la tabla de registro de usuarios</i> .....	<b>102</b>
<b>Figura 68</b> <i>Ventana 5 con la tabla de registro de historial</i> .....	<b>102</b>
<b>Figura 69</b> <i>Ventana 3 para el registro de ingreso</i> .....	<b>103</b>
<b>Figura 70</b> <i>Mensaje de aviso de registro de usuario por huella digital</i> .....	<b>103</b>
<b>Figura 71</b> <i>Ventana 6 para añadir usuario</i> .....	<b>104</b>
<b>Figura 72</b> <i>Mensaje de error al añadir un nuevo usuario</i> .....	<b>105</b>
<b>Figura 73</b> <i>Ventana 7 para eliminar un usuario</i> .....	<b>105</b>
<b>Figura 74</b> <i>Mensaje de error al no seleccionar un usuario para eliminar</i> .....	<b>106</b>
<b>Figura 75</b> <i>Mensaje de confirmación para eliminar usuario</i> .....	<b>106</b>
<b>Figura 76</b> <i>Mensaje de aviso de generación de reporte</i> .....	<b>106</b>
<b>Figura 77</b> <i>Prototipo evaluado con un solo rostro</i> .....	<b>107</b>

<b>Figura 78</b> <i>Prototipo evaluado con dos rostros</i> .....	<b>109</b>
<b>Figura 79</b> <i>Prototipo evaluado con un rostro y una foto</i> .....	<b>110</b>
<b>Figura 80</b> <i>Prototipo evaluado con un rostro conocido y un rostro desconocido</i> .....	<b>112</b>
<b>Figura 81</b> <i>Prototipo evaluado con tres rostros conocidos</i> .....	<b>113</b>
<b>Figura 82</b> <i>Prototipo evaluando dos rostros conocidos y un rostro falso</i> .....	<b>115</b>
<b>Figura 83</b> <i>Prueba con iluminaria</i> .....	<b>116</b>
<b>Figura 84</b> <i>Prototipo evaluado con dos rostros con mejor iluminación</i> .....	<b>117</b>
<b>Figura 85</b> <i>Prototipo evaluado con tres rostros con mejor iluminación</i> .....	<b>118</b>

## Resumen

El presente proyecto de investigación se plantea el diseñar e implementar un prototipo de sistema biométrico para mejorar el registro de acceso de personal utilizando reconocimiento facial en la empresa JVA TECNOLOGÍA. Este prototipo pretende agilizar el proceso de registro de usuarios y generación de reportes. Para implementación del sistema biométrico por reconocimiento facial se utiliza el lenguaje de programación de Python para la adquisición y procesamiento de los rostros, entrenar la red neuronal e identificar a los usuarios. A esto se suma una técnica Anti-spoofing que permita dar una seguridad al sistema, la autenticación requiere que el usuario pestañee frente a la cámara para prevenir la falsificación de identidad y verificar su identidad en cuestión de unos pocos segundos. El diseño de la interfaz gráfica se basa en la normativa ISO 9241, cuenta con verificación de usuario y clave, botones de acción, mensajes informativos y mensajes de error. Se tiene una ventana en la interfaz donde se logra visualizar el nombre, la hora, día, mes y año en el momento de registro del usuario. Además, automáticamente el sistema permite guardar la información obtenida en una base de datos, la cual se consigue observar los parámetros previamente expuestos remotamente vía web. Previo al uso del sistema es necesario que el usuario añada sus datos personales, huella digital y malla facial a la base de datos. Se cuenta una alternativa biométrica de registro donde el personal puede registrarse a través del sensor de huella dactilar. Adicional a esto, si una persona reincide en varios atrasos el sistema envía una notificación por correo electrónico sobre su incumplimiento a su jornada laboral de trabajo. Finalmente, se logra generar tres tipos de reportes en formato de salida .xlsx: reporte de usuarios, reporte de historial de registro y planilla de asistencia.

*Palabras clave:* Sistema biométrico, reconocimiento facial, reportes, anti-spoofing.

### **Abstract**

This research project aims to design and implement a prototype biometric system to improve the registration of personnel access using facial recognition in the company JVA TECNOLOGÍA. This prototype aims to streamline the process of user registration and report generation. To implement the biometric facial recognition system, the Python programming language is used to acquire and process faces, train the neural network and identify users. To this is added an Anti-spoofing technique to provide security to the system, authentication requires the user to blink in front of the camera to prevent identity forgery and verify their identity in a matter of a few seconds. The graphical interface design is based on ISO 9241 standards, with user and password verification, action buttons, informational messages and error messages. There is a window in the interface where the name, time, day, month and year at the time of user registration are displayed. In addition, the system automatically saves the information obtained in a database, which allows to observe the parameters previously exposed remotely via web. Prior to using the system, it is necessary for the user to add his personal data, fingerprint and facial mesh to the database. There is a biometric registration alternative where personnel can register through the fingerprint sensor. In addition to this, if a person is repeatedly late, the system sends an e-mail notification about his/her non-compliance with the working day. Finally, three types of reports are generated in .xlsx output format: user report, registration history report and attendance sheet.

*Key words:* Biometric system, facial recognition, reports, anti-spoofing.

## **Capítulo I:**

### **Aspectos generales y marco teórico**

En este capítulo se presentan los aspectos generales del proyecto, tales como: antecedentes, planteamiento del problema, justificación, objetivos, metas, hipótesis, variable dependiente e independiente, además del marco teórico.

#### **Antecedentes**

Domínguez (1996) en su trabajo de investigación “El procesamiento digital de imágenes”, en el Jet Propulsion Laboratory de 1964 cuando el Ranger 7 transmitió imágenes de la Luna, las cuales fueron corregidas y mejoradas a través de un procesamiento realizado por una computadora. Estas técnicas iniciales proporcionaron la base para la mejora continua de los métodos utilizados en la restauración y el enriquecimiento de imágenes. Este hecho es relevante ya que marca el inicio de una nueva era en la manipulación y mejora de imágenes, lo que ha permitido una mayor comprensión y apreciación de nuestro mundo y el universo que nos rodea. Por lo tanto, se puede afirmar que el procesamiento digital de imágenes es una tecnología clave en la investigación científica y en la vida cotidiana.

Existen varios algoritmos de aprendizaje para el reconocimiento facial, como Face Recognition, FaceNet, OpenFace, entre otros. La función más importante es reconocer la cara del usuario con una sola foto o varias al cargar y personalizar el sistema. Varios algoritmos, además del reconocimiento facial mencionados anteriormente, también tienen modelos de detección de edad y emoción, uno de los cuales es DeepFace, mediante el cual se pueden detectar las emociones del usuario y juzgar si el usuario está feliz o enojado, sorprendido o incluso triste. El algoritmo se ha utilizado en la plataforma de Facebook (Serengil & Ozpinar, 2020).

En el proyecto de tesis “Desarrollo de un sistema de control de acceso de personal empleando reconocimiento facial respaldado con técnicas de aprendizaje profundo”,

desarrollado por el estudiante Muñoz Vega (2021), ex alumno de la Universidad de las Fuerzas Armadas ESPE Sede Latacunga, reconoce que el modelo FaceNet obtiene mejores resultados en el rendimiento y precisión al momento de realizar el reconocimiento facial, además se implementó un algoritmo Anti-spoofing en tiempo real en donde se tiene la predicción correcta de un rostro real y un rostro falso.

Además, Navas y Obando (2021) en su investigación “Diseño e implementación de un prototipo de sistema de seguridad integral con el fin monitorear el acceso de automóviles, utilizando visión artificial y chatbot para el ingreso al conjunto residencial”, redacta que se utilizó la red neuronal MobileNet permitiendo que la misma genere un aprendizaje por repetición al detectar el objeto, logrando que la red neuronal tenga un desempeño óptimo.

Actualmente, los relojes biométricos con reconocimiento facial o de huellas dactilares permiten guardar la asistencia de los empleados y registrarlos en el sistema durante horarios fijos de trabajo, con generación de reportes que se almacenan para una transferencia manual de datos.

El reloj marcador biométrico Zkteco MB10 con reconocimiento facial y huella digital, es un dispositivo revolucionario para la gestión del tiempo y el registro de empleados. Este dispositivo es altamente innovador ya que ofrece diversos métodos de verificación, incluyendo reconocimiento facial, huella dactilar, tarjeta, contraseña y combinaciones de estos. Además, cuenta con funciones básicas de control de acceso que agilizan los procesos de entrada y salida de los empleados. La comunicación se realiza a través de la interfaz TCP/IP o mediante un cable USB, lo que permite una transferencia manual de datos. Esta característica permite una mayor flexibilidad y versatilidad en la gestión de datos y tiempos de los empleados. En resumen, es una herramienta clave para la optimización de procesos en el lugar de trabajo, lo que a su vez aumenta la eficiencia y la productividad de los empleados y la empresa en general. (ZKTECO, 2020).

La empresa JVA Tecnología importa y distribuye productos, suministros y repuestos tecnológicos a todo el país como: computadoras, laptops, accesorios, cámaras, impresoras y más, además, se ofrece un servicio de mantenimiento y ayuda para solucionar problemas informáticos de diferentes tipos, donde sus trabajadores tienen horarios fijos de trabajo para su hora de ingreso y salida, ocasionando una saturación de personal, ya que poseen un sistema ineficiente al momento de realizar el registro de asistencia.

### **Planteamiento del problema**

En la empresa JVA Tecnología, al igual que otras empresas, poseen un sistema deficiente para los estándares actuales en el control de acceso del personal autorizado, se debe ingresar la hora de entrada y salida manualmente, este proceso puede generar filas y que exista una saturación a la hora de ingreso y de salida, causando un control defectuoso, que conlleva además errores en el registro, sea por un error humano o casos del ingreso de personas no autorizadas, lo que ocasiona inseguridad e incomodidad del personal.

Existen empresas, instituciones públicas o privadas en las que actualmente el registro de su personal lo manejan de forma tradicional, lo que representa el riesgo de que la información deje de ser confidencial o que se extravíen documentos importantes. Si no se tiene un registro digital, es difícil y poco eficiente consultar la información o generar informes sobre el acceso de los empleados en cualquier momento que sea necesario.

Mediante el método tradicional es necesario el contacto entre los trabajadores y tomando en cuenta la realidad mundial por el Covid-19, esta enfermedad se puede propagar cuando una persona infectada exhala partículas infectadas que contienen el virus. En algunas circunstancias, estas partículas pueden contaminar las superficies que tocan o pueden ser introducidas por otras personas al tocarse los ojos, nariz o boca con las manos contaminadas, por lo tanto, no sería una forma segura de registrar la asistencia de los empleados.



Por otro lado, habitualmente se utilizan diversos métodos para identificar a las personas, tales como: usuario y contraseña, número de identificación personal, tarjeta de identificación por radiofrecuencia, llaves, pasaporte, licencia de conducir, por mencionar algunos; los recursos utilizados por estos métodos pueden perderse, olvidarse, compartirse, manipularse o robarse, ocasionando varios problemas de suplantación de identidad. Debido a estas desventajas, tener a disposición un sistema biométrico mediante reconocimiento facial permite a la empresa mejorar el registro del personal para que este sea eficiente, óptimo y sobre todo fiable.

### **Justificación e importancia**

Las técnicas de identificación biométricas brindan una solución confiable para la identificación, ya que se basan en los rasgos físicos del cuerpo humano que son únicos, exclusivos, permanentes e intransferibles, generar este prototipo de sistema biométrico mediante reconocimiento facial brindará seguridad y tranquilidad a los propietarios al saber que el personal registrado está autorizado para ingresar y crear un ambiente seguro para los empleados.

El registro de datos ofrece diversas ventajas para la empresa, mejorando su eficacia y agilidad. Algunos trabajos se realizarán de manera más rápida y eficiente debido a la simplificación de los procesos, permitiendo una consulta rápida de información o la generación de informes sobre el acceso de los empleados en cualquier momento que sea necesario. Esta característica agregará valor a la empresa, ya que la información y el conocimiento se convertirán en activos más importantes para la misma.

El trabajo de tesis propuesto incluirá una técnica Anti-spoofing para contrarrestar la suplantación de identidad, éstas son técnicas capaces de distinguir automáticamente entre una biometría real y una sintética. Estos métodos constituyen retos de alta complejidad en ingeniería ya que no deben ser invasivos, deben ser amigables con el usuario, rápidos y de

buen desempeño. En la cual se basan en la detección de micro-movimientos realizados por parte del usuario, como pestañar, asentir, sonreír, observar en diferentes direcciones entre otros. Y que con ello disminuya la probabilidad de detecciones erróneas.

Con este sistema no solo se pretende brindar seguridad y confort al usuario sino incentivar el uso de herramientas actuales como el reconocimiento facial, de este modo se intenta dar una solución tecnológica, en donde se tiene el conocimiento y los instrumentos necesarios para implementar este tipo de sistemas con un bajo costo y utilizando ingeniería nacional. Será una herramienta tecnológica a medida del tamaño de la empresa, ya que si hay más usuarios se puede ampliar la base de datos y no incurrir en más gastos, esta información está pensada para ser accesible, remotamente vía web, lo que permite que el personal que controla los ingresos pueda ver los registros generados por el sistema en tiempo real.

Tomando en cuenta la realidad mundial por el Covid-19 el uso de esta tecnología, permite la identificación del usuario de manera automática y se realiza sin necesidad de contacto, lo que prioriza la salud del personal ante esta situación, a su vez facilita y agiliza el proceso de registro.

Este proyecto propone innovar en varios sectores estratégicos que busquen mejorar sus sistemas de seguridad, registro y monitoreo de personal adaptándose a las nuevas tecnologías al implementar un sistema biométrico de reconocimiento facial en la empresa JVA Tecnología se propone una solución rápida, eficiente, accesible y sobre todo fiable a la hora de reconocer y registrar al personal.

## **Objetivos**

### ***Objetivo general***

Diseñar e implementar un prototipo de sistema biométrico para mejorar el registro de acceso de personal utilizando reconocimiento facial en la empresa JVA Tecnología.

**Objetivos específicos**

- Investigar el estado del arte sobre métodos de reconocimiento facial a través de la recolección de información técnica y de publicaciones.
- Diseñar la estructura mecánica que soportará el prototipo.
- Implementar los algoritmos necesarios para un correcto procesamiento de imágenes que permitan obtener los datos para el entrenamiento y reconocimiento facial.
- Desarrollar una etapa de seguridad mediante una técnica Anti-spoofing que permita dar seguridad y robustez al sistema, disminuyendo la probabilidad de detecciones erróneas.
- Crear una base de datos accesible remotamente acorde a las necesidades de la empresa JVA Tecnología.
- Elaborar una interfaz gráfica intuitiva y de fácil manejo que sea amigable con el usuario.
- Ejecutar pruebas experimentales del funcionamiento para analizar la fiabilidad y la velocidad del sistema.
- Validar la hipótesis a través de los datos obtenidos para determinar si se cumplió el objetivo del proyecto.

**Metas**

- Se investigará el estado del arte sobre métodos de reconocimiento facial a través de la recolección de información técnica y de publicaciones, se realizará en la primera y segunda semana del primer mes.
- Se diseñará la estructura mecánica que soportará el prototipo, se realizará en la tercera y cuarta semana del primer mes.
- Se implementarán los algoritmos necesarios para un correcto procesamiento de imágenes que permitan obtener los datos para el entrenamiento y reconocimiento facial, se realizará en la primera y segunda semana del segundo mes.

- Se desarrollará una etapa de seguridad mediante un método Anti-spoofing que permita dar seguridad y robustez al sistema, disminuyendo la probabilidad de detecciones erróneas, se realizará en la tercera y cuarta semana del segundo mes.
- Se creará una base de datos accesible remotamente acorde a las necesidades de la empresa JVA Tecnología, se realizará en la primera semana del tercer mes.
- Se automatizará la recopilación de datos necesarios para la generación de reportes del acceso del personal, se realizará en la segunda semana del tercer mes.
- Se elaborará una interfaz gráfica intuitiva y de fácil manejo, amigable con el usuario, se realizará en la tercera y cuarta semana del tercer mes.
- Se ejecutarán pruebas experimentales del funcionamiento para analizar la fiabilidad y la velocidad del sistema, se realizará en la primera y segunda semana del cuarto mes.
- Se validará la hipótesis a través de los datos obtenidos para determinar si se cumplió el objetivo del proyecto, se realizará en la tercera y cuarta semana del cuarto mes.

### **Hipótesis**

¿El diseño e implementación de un prototipo de sistema biométrico mejorará la eficiencia en el registro de acceso de personal utilizando reconocimiento facial en la empresa JVA Tecnología?

### **Variables de investigación**

#### ***Variable Independiente***

Diseño e implementación de un prototipo de sistema biométrico utilizando reconocimiento facial.

#### ***Variable dependiente***

Mejorar la eficiencia en el registro de acceso de personal en la empresa JVA Tecnología.

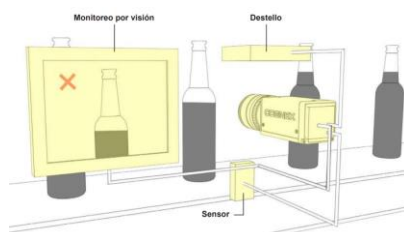
## Marco teórico

### *Visión artificial*

La visión artificial es una parte de la inteligencia artificial que permite a las computadoras obtener, procesar y analizar imágenes del mundo real con el fin de extraer información para resolver algún problema o saber lo que se está haciendo y tomar decisiones rápidas. Tal como los seres humanos usan sus ojos para poder observar, y el cerebro para comprender el mundo que los rodea, este efecto se pretende en las máquinas por medio de la visión artificial, para que pueda conducirse según una determinada situación en la que esté expuesto. Algunos de sus usos más característicos son el control de calidad, clasificación, medición, posición, identificación, entre otros (García, 2012).

### Figura 1

*Ejemplo de una aplicación de llenado de botella mediante visión artificial*



*Nota.* Tomado de (COGNEX, 2018).

### **Componentes del sistema de visión artificial**

La combinación correcta de los componentes seleccionados para un proceso de visión artificial, como resultado se tiene una mejor calidad de imagen y video que permite un realce previo al procesamiento digital de la imagen. Los componentes principales de un sistema de visión artificial incluyen:

- **Iluminación:** La iluminación se encarga de alumbrar al objeto adecuadamente a inspeccionar, su meta es destacar al máximo las características que se requieren

analizar, así como también negar otras partes, al siluetear una pieza se oscurecen detalles de la superficie y queda expuesto sus bordes para un posterior estudio. Las técnicas de iluminación dependen directamente de la correcta ubicación y tipo de fuente de luz con respecto a la pieza (COGNEX, 2018).

- **Lente:** El lente de la cámara se encarga de establecer la resolución y calidad de la imagen capturada. Las lentes se utilizan para llevar la luz al sensor de la cámara de una manera controlada, lo que resulta en una imagen nítida. Existen dos tipos de lentes: lentes intercambiables y lentes fijos. Con la combinación correcta del lente y extensión se conseguirá una imagen lo mejor posible (COGNEX, 2018).
- **Sensor:** El sensor de la cámara transforma la luz recibida del lente en una imagen digital y la envía al procesador para su posterior análisis. Los dos tipos de sensores más comúnmente utilizados para convertir la luz en señales eléctricas son el dispositivo de carga acoplada (CCD) y el semiconductor complementario de óxido metálico (CMOS). Una imagen consiste en una combinación de píxeles, donde la luz baja crea píxeles oscuros y la luz brillante produce píxeles claros (COGNEX, 2018).
- **Procesador:** El procesamiento se enfoca en extraer la información de una imagen digital. Este proceso se realiza por software y consta de algoritmos que ejecutan la inspección, medición y si es necesario las compara, finalmente se toma una decisión y se notifica los resultados (COGNEX, 2018).
- **Comunicación:** Para que los sistemas de visión artificial funcionen adecuadamente, se requiere una comunicación fluida y eficiente entre los distintos componentes. Esto se logra generalmente a través de señales de entrada y salida discretas o de información transmitida a través de conexiones seriales, como RS-232 o Ethernet, para que los datos puedan ser registrados o utilizados por un dispositivo (COGNEX, 2018).

## ***Biometría***

La biometría es una tecnología de reconocimiento automático de personas en función de sus características fisiológicas o del comportamiento propias de cada individuo. Estas características físicas son únicas, registrables y medibles, mediante el cual se utilizan diferentes métodos de medición de éstas; generalmente se considera que las mediciones fisiológicas brindan el beneficio de permanecer más constantes durante toda la vida o períodos largos en la persona. La biometría fisiológica se caracteriza por depender del rasgo estrictamente físico del cuerpo humano a la hora de identificar personas, mientras que la biometría de comportamiento está sujeta a una acción realizada por el individuo (INCIBE, 2016).

Las principales tecnologías biométricas fisiológicas son:

- Reconocimiento de la huella dactilar
- Reconocimiento facial
- Reconocimiento de iris/retina
- Reconocimiento de la geometría de dedos/mano

Las principales biometrías de comportamiento son:

- Reconocimiento de voz
- Reconocimiento de firma
- Reconocimiento de la forma de andar

### ***Etapas de un sistema de identificación biométrica***

Los sistemas biométricos de identificación, cualquiera que sea el método de reconocimiento utilizado, se basan en un esquema que consiste en dos fases distintas:

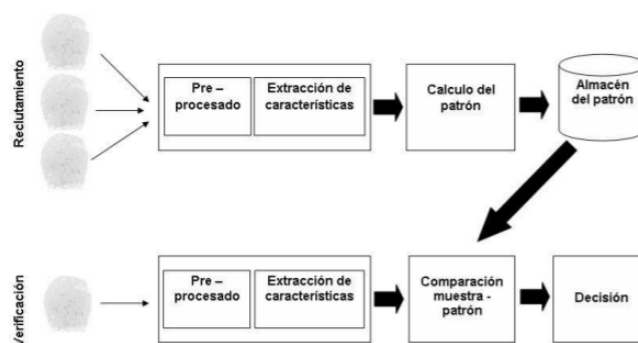
- **Reclutamiento:** Durante el primer paso del proceso de identificación biométrica, se colectan varias muestras del usuario, las cuales son procesadas para generar un

patrón. Este patrón se obtiene a partir de la media de las características distintivas de las muestras, y se guarda en una base de datos. Este proceso se realiza bajo supervisión para asegurarse de que se capturaron correctamente los datos y de que la identidad de la persona se está registrando adecuadamente en el sistema.

- **Verificación:** Una vez que se ha registrado el patrón del usuario en la base de datos, se procede a utilizar estos datos para el reconocimiento del sistema. Primero se captura la muestra del usuario, luego se procesa para extraer el patrón y se comparan sus características con el patrón almacenado en la base de datos. A partir de esta comparación, se determina si el reconocimiento es exitoso o no (Ruiz, Rodriguez, & Olivares, 2009).

## Figura 2

### *Etapas en un sistema de identificación biométrica*



*Nota.* Tomado de (Sánchez, Ávila, & Pereda, 1999).

### **Reconocimiento facial**

El reconocimiento facial es una técnica de identificación de identidad de una persona mediante una imagen o video de su rostro. Se caracteriza en que sus datos permiten medir de forma cuantitativa los patrones que se extraen, los cuales persisten a lo largo del tiempo.

Durante la fase de identificación se utilizan algoritmos de inteligencia artificial o de aprendizaje automático para analizar los aspectos clave como la distancia entre los ojos, ángulo de



mandíbula, longitud de la nariz, entre otros; y se compara la información obtenida del rostro para establecer un porcentaje de similitud entre las características faciales que se tiene guardada y la nueva información; y se toma la decisión de reconocer o no a la persona (Arguello, 2011).

### ***Técnicas de extracción de características***

La extracción de rasgos en imágenes y secuencias faciales se refiere al proceso de obtener información en el que se examina el rostro como un todo y se identifican áreas relevantes, tales como los ojos, cejas y boca. Algunas técnicas de extracción son:

- PCA (Análisis de componentes principales): Es un algoritmo de reducción de dimensionalidad que le permite encontrar un vector que mejor simbolice la distribución y clasificación de un conjunto de imágenes. El objetivo es mostrar la imagen en el mejor sistema de coordenadas al disminuir el número de componentes finales que tendrá la imagen (Hernández, 2010).
- LDA (Análisis Discriminante Lineal): Esta técnica se aplica cuando se tienen medidas continuas en las variables independientes para cada observación. Para reducir el costo computacional, se transforma un conjunto de datos en un espacio de menor dimensión con una separación clara de las clases. La técnica semejante es el análisis de discriminación de correspondencia cuando se trata de variables independientes categóricas (Raschka, 2014).
- LPP (Proyecciones de preservación de la localidad): Esta técnica ejecuta una reducción dimensional y requiere montar gráficos que incluyen información del entorno como un grupo de datos. La representación de gráficos es generada por el algoritmo, puede ser visto como una aproximación discreta lineal, aunque surge naturalmente de la geometría del vector (Hernández, 2010).

### **Métodos de entrenamiento de reconocimiento de rostros**

Existen diferentes tipos de entrenamiento de reconocimiento de rostros, algunos de sus métodos principales son:

- **Eigenfaces:** Este método está basado en las propiedades matemáticas de la imagen digitalizada, utiliza el álgebra lineal y el análisis de componentes principales (PCA) para realizar el reconocimiento facial, el cual el patrón que representa a una imagen debe estar constituido por los elementos más relevantes de ella, esta técnica contiene datos redundantes que ocasionan un método de clasificación de alto costo computacional. Este método requiere que las imágenes sean frontales y en condiciones análogas a la iluminación (Gottumukkal & Asari, 2003).
- **Fisherfaces:** Este método cuenta con todas las ventajas del Eigenfaces frente a otras técnicas, tales como la eficiencia, velocidad del sistema y capacidad de operar en muchas caras en un menor tiempo. Utiliza el Discriminante lineal de Fisher (FLD) que ayuda a reducir las dimensiones de las caras y se encarga de clasificar. Además, es menos sensible a variaciones en la iluminación y a los ángulos de las caras en las imágenes (Granja, Moreno, Cabrera, & Valle, 2020).
- **Local Binary Patterns Histograms (LBPH):** Es una técnica basada en un operador binario local, diseñado para identificar tanto el rostro frontal como el lateral del ser humano. Muestra mejoras referentes a los métodos anteriores, ya que es más robusto ante cambios de iluminación. Este método divide en varias regiones la imagen del rostro a las que se les aplica un histograma, y se obtiene un operador LBPH que detalla la información independiente de cada región (Alvarado & Fernández, 2012).

### **Anti-Spoofing**

Anti-Spoofing es un conjunto de técnicas que buscan comprobar que un usuario es un ser vivo y no una imagen, esto requiere que el usuario realice ciertas acciones frente a la

cámara, tales como parpadear, sonreír o mover alguna parte de su cuerpo. Un sistema Anti-Spoofing detecta la suplantación de identidad, inmediatamente bloquea y alerta sobre ello a las autoridades o entidades competente, protegiendo así los derechos de los usuarios y empresas con las que interactúan a diario. Existen métodos diferentes para detectar fraudes en los sistemas biométricos, la mayoría de ellos son funciones preprogramadas, pero con el desarrollo del Deep Learning, los algoritmos automáticamente extraen características que ofrecen una solución más fiable que autentifica y verifica al usuario en cuestión de segundos (Akhtar, Alfarid, & Kale, 2011).

### **Figura 3**

*Reconocimiento facial, técnicas Anti-spoofing*



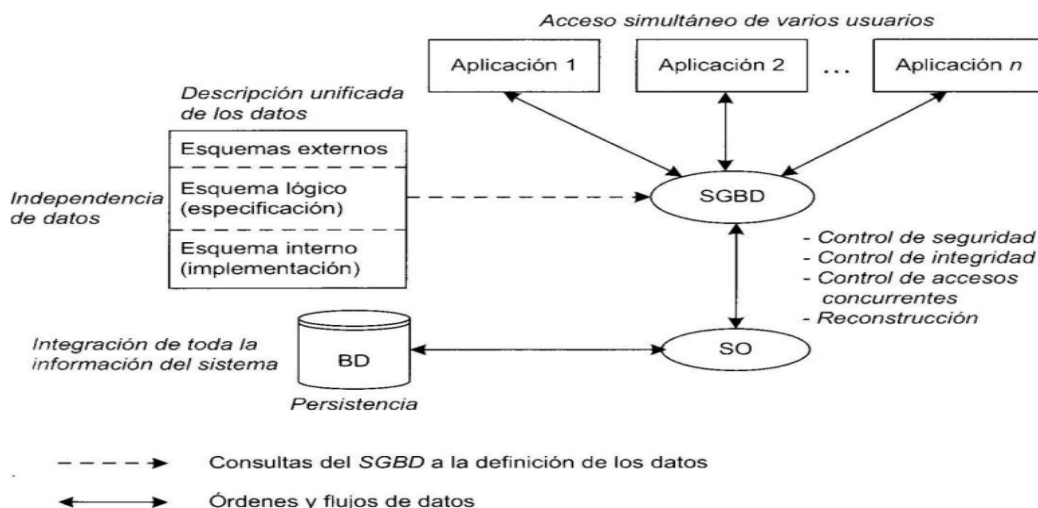
*Nota.* Tomado de (Prensario TI Latin America, 2021).

### **Base de datos**

El término base de datos surgió en 1963 y, se define como un conjunto de datos lógicamente relacionados entre sí que se encuentran agrupados o estructurados. Las técnicas de base de datos se han desarrollado para recopilar, organizar y unificar los datos obtenidos del sistema, en la cual permiten compartir y mejorar la accesibilidad, productividad, tener un respaldo y evitar la redundancia sin perder los distintivos puntos de vista de los usuarios (Gómez, 2013).

Figura 4

Sistema de base de datos



Nota. Tomado de (Celma, Casamayor, & Mota, 2003).

## SQL

SQL es un lenguaje de programación que utilizan las bases de datos relacionales para analizar, consultar y definir los datos, además de permitir el control de acceso. SQL es un estándar internacional reconocido por organismos de estándares como ISO y ANSI. Al usar SQL se debe manejar una sintaxis definida por un grupo de reglas que interactúan con la base de datos y permiten realizar varias funcionalidades como crear procedimientos almacenados, crear nuevas tablas, asignar permisos y entre otros, en la base de datos (Microsoft, 2022).

## Figura 5

### Lenguaje de consulta estructurada SQL



*Nota.* Tomado de (European Knowledge Center for Information Technology, 2019).

### Norma ISO 9241

La norma ISO 9241 establece el concepto de usabilidad aplicado a sistemas interactivos, pero no un proceso específico en la evaluación del diseño. Se especifican los criterios para las pantallas de visualización que aseguran una lectura cómoda, segura y eficiente al realizar las tareas (INEN, 2014).

Las medidas de la norma son:

- El diseño se basa en el entendimiento explícito de los usuarios, trabajos y entornos.
- Los usuarios participan en el proceso de diseño y creación.
- La evaluación basada en el usuario dirige y mejora el diseño.
- El diseño es un proceso continuo y recurrente.
- Se considera la experiencia total del usuario en el diseño.
- El equipo de diseño cuenta con habilidades y enfoques diversos y multidisciplinarios.

### ***Lenguaje de Programación a utilizar en el desarrollo***

Para el procesamiento digital de imágenes mediante visión artificial se desarrolla en el lenguaje de programación Python con librerías externas.

**Python.** Python es un lenguaje de programación de alto nivel y gratuito con una sintaxis fácil de entender y legible. Es un lenguaje versátil que permite la programación en diferentes paradigmas, incluyendo orientada a objetos, imperativa y funcional. Es multiplataforma donde se puede desarrollar y ejecutar los programas en diferentes sistemas operativos como Linux, Windows, Mac, entre otros. El lenguaje Python es adecuado para realizar análisis de datos, inteligencia artificial, programación de redes neuronales, desarrollo web, desarrollo en dispositivos embebidos, etc., que se aplican en los diferentes campos científico-tecnológico (Delgado, 2022).

### **Figura 6**

*Logo de Python*



*Nota.* Tomado de (Python, 2022).

**OpenCV.** OpenCV es una biblioteca de código abierto que brinda soporte a Python para la visión artificial y el aprendizaje automático. Tiene una amplia variedad de algoritmos, más de 2500, que pueden ser utilizados para identificar objetos, caras, clasificar, generar modelos 3D, entre otras cosas. Además, ofrece una infraestructura para aplicaciones de visión por computadora en tiempo, procesamiento y análisis de datos. Tiene una licencia Berkeley Software Distribution (BSD), que permite utilizar y modificar el código sin algún tipo de

impedimento, de la cual muchas compañías aportan con su desarrollo permanente, tal es el caso de Google (Gracia, 2013).

### **Figura 7**

*Logo de OpenCV*



*Nota.* Tomado de (Gracia, 2013).

## Capítulo II:

### Diseño y selección de componentes del sistema

En este capítulo se detallan la metodología, los requerimientos del sistema, la arquitectura y el proceso de selección de los elementos del sistema.

#### **Metodología**

La metodología de diseño aplicada para este trabajo de titulación se basa en el proceso genérico de desarrollo de un producto, que mediante un proceso estructurado se pueden detallar los requerimientos del sistema, las especificaciones, la arquitectura del producto, la selección de componentes, con el objetivo de lograr un diseño que satisfaga las necesidades del usuario.

#### **Requerimientos del sistema**

##### ***Identificación de necesidades***

También conocido como la voz de usuario, es parte fundamental dentro del diseño y pertenece a la fase de desarrollo de concepto. Se centra en aglomerar todas las peticiones del usuario sin diferenciar entre necesidades o deseos, las cuales serán traducidas en términos de las métricas del sistema.

- Básica (B): Considerado elemental.
- Unidimensional (U): Aumentan la satisfacción.
- Estimulante (E): Complace al usuario, pero su ausencia no genera insatisfacción.



**Tabla 1***Necesidades del usuario*

#	Necesidades	Tipo
1	El sistema biométrico debe registrar al usuario por reconocimiento facial.	B
2	El sistema biométrico debe contar con una técnica anti-spoofing.	B
3	La interfaz de usuario del sistema biométrico debe ser interactivo.	U
4	El sistema biométrico debe tener una apariencia amigable y atractiva.	E
5	El sistema biométrico debe generar un reporte cuando sea requerido.	B
6	El sistema biométrico debe ser sencillo de controlar o manejar.	U
7	El sistema biométrico debe ser liviano.	E
8	El sistema biométrico debe tener una alternativa de registro adicional a la visión.	B
9	El sistema biométrico debe permitir añadir nuevos usuarios.	B
10	El sistema biométrico no debe tener un alto costo.	E

**Métricas**

También conocido como la voz del ingeniero, son las características técnicas de diseño que garantizan que el sistema satisface las demandas del usuario, las cuales deben cuantificarse o medirse para su posterior análisis.

**Tabla 2***Características técnicas del sistema*

#	Métricas	Unidades
1	Dimensiones	Milímetros (mm)
2	Masa total	Kilogramos (kg)
3	Comunicación de la interfaz	Tiempo de ejecución (s)
4	Diseño UX/UI	Número de ventanas interactivas (n)
5	Visión artificial	Tiempo de registro (s)
6	Código del programa	Número de líneas de código (n)
7	Modularidad	Número de partes (n)
8	Funcionamiento Ininterrumpible	Tiempo de funcionamiento (s)
9	Objeto de base de datos	Número de rutinas (n)
10	Costo de manufactura	Dólar (USD \$)

### Matriz necesidades-métricas

En la figura 8 se muestra la matriz de Necesidades-Métricas para el presente trabajo de titulación, donde se añaden las necesidades del usuario con sus índices de importancia predeterminados y las métricas preestablecidas, instituyendo así los compromisos técnicos a cumplir.

**Figura 8**

### Matriz necesidades-métricas

Tipo de Necesidad	Importancia	Necesidades	Métricas										Ponderación necesidades	Ponderación en %	
			1	2	3	4	5	6	7	8	9	10			
			Dimensiones	Masa total	Comunicación de la interfaz	Diseño UX/UI	Visión Artificial	Código del programa	Modularidad	Funcionamiento ininterrumpible	Objeto de base de datos	Costo de manufactura			
1	B	5	El sistema biométrico debe registrar al usuario por reconocimiento facial.					++	++					50	21.7
2	B	5	El sistema biométrico debe contar con una técnica anti-spoofing.					++	+					40	17.4
3	U	4	La interfaz de usuario del sistema biométrico debe ser interactivo.			+			+					24	10.4
4	E	3	El sistema biométrico debe tener una apariencia amigable y atractiva.				+			-	+			12	5.22
5	B	5	El sistema biométrico debe generar un reporte cada vez que se lo necesite.								+			5	2.17
6	U	4	El sistema biométrico debe ser sencillo de controlar o manejar.			+			-			+		16	6.96
7	E	3	El sistema biométrico debe ser liviano.	+	+		+			-			-	33	14.3
8	B	5	El sistema biométrico debe tener una alternativa de registro adicional a la visión						+					15	6.52
9	B	5	El sistema biométrico debe permitir añadir nuevos usuarios.						++			+		25	10.9
10	E	3	El sistema biométrico no debe tener un alto costo.							-			+	10	4.35
			<b>Incidencia</b>	6	6	20	15	42	94	6	20	15	7	230	100
			<b>Incidencia en %</b>	2.61	2.6	8.7	6.52	18.3	40.9	2.6	8.7	6.5	3	100	

En la tabla 3 se puede observar la simbología de correlación utilizada para la matriz Necesidades-Métricas. Y para la tabla 4, los resultados se presentan en orden decreciente según el porcentaje de incidencia.

**Tabla 3**

### Simbología de correlación entre necesidades y métricas

Simbología	Factor de incidencia	Valor numérico
++	Fuerte	5
+	Medio	3
-	Bajo	2
	Nulo	0

**Tabla 4**

*Resultados obtenidos de la matriz necesidades-métricas*

<b>Orden</b>	<b>Métricas</b>	<b>Porcentaje de incidencia</b>
1	Código del programa	40,9
2	Visión artificial	18,3
3	Comunicación de la interfaz	8,7
4	Funcionamiento ininterrumpible	8,7
5	Diseño UX/UI	6,5
6	Objeto de base de datos	6,5
7	Costo de manufactura	3
8	Dimensiones	2,61
9	Masa total	2,6
10	Modularidad	2,6

Los parámetros más relevantes para el diseño en relación a los requerimientos del usuario son la facilidad o uso intuitivo del software (experiencia de usuario), la visión artificial, y comunicación de la interfaz. De importancia media se considera el funcionamiento ininterrumpible, el diseño UX/UI, objeto de base de datos y el costo de manufactura. Los aspectos como la dimensión, masa total y modularidad se consideran de baja importancia para el diseño.

### **Planteamiento de especificaciones**

En la tabla 5 se puntualizan las especificaciones generales del sistema, donde se marcan los criterios que se debe cumplir con el proyecto para satisfacer al usuario y con sus pertinentes resultados.

**Tabla 5***Especificaciones generales del sistema*

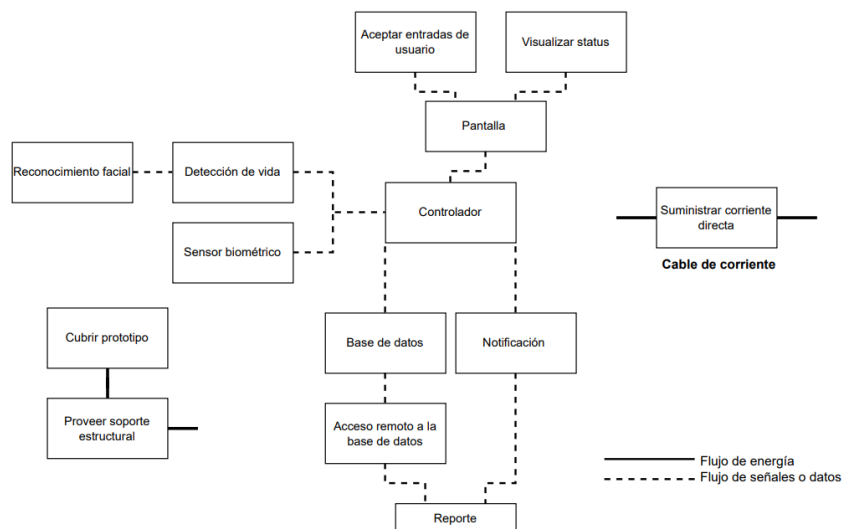
<b>#</b>	<b>Parámetros</b>	<b>Especificación</b>
1	Programación	Inglés, lenguaje estándar y con mayor documentación en el área.
2	Visión artificial	Reconocimiento facial menor a 1 segundo.
3	Costo de manufactura	Menor a \$800
4	Dimensiones	Máximo 40x40x40 centímetros
5	Masa total	Máximo 4 kg
6	Arquitectura	Mínimo 2 módulos
7	Anti-spoofing	Menor a 5 segundos

**Arquitectura del prototipo*****Esquema del prototipo***

El esquema de la figura 9 representa la interrelación del equipo con los elementos constitutivos del prototipo. Se presentan los elementos funcionales como el reconocimiento del usuario y elementos físicos como: la cámara para visión artificial, micro controlador, pantalla interactiva, lector de huella dactilar y estructura mecánica. Para mayor claridad, solo se muestran las conexiones fundamentales del sistema. Las selecciones específicas definen parcialmente la arquitectura del producto. Es fundamental para el prototipo que esté sujeta a una estructura fija, que sirva de soporte para cada uno de los elementos. El reconocimiento del usuario depende de dos alternativas, uno por visión artificial basada en la biometría del rostro y otro por huella dactilar. Las entradas del usuario permiten visualizar y administrar la base de datos de registros de acceso del personal. Y la corriente alimentará a los dispositivos electrónicos y eléctricos.

**Figura 9**

*Esquema del prototipo*

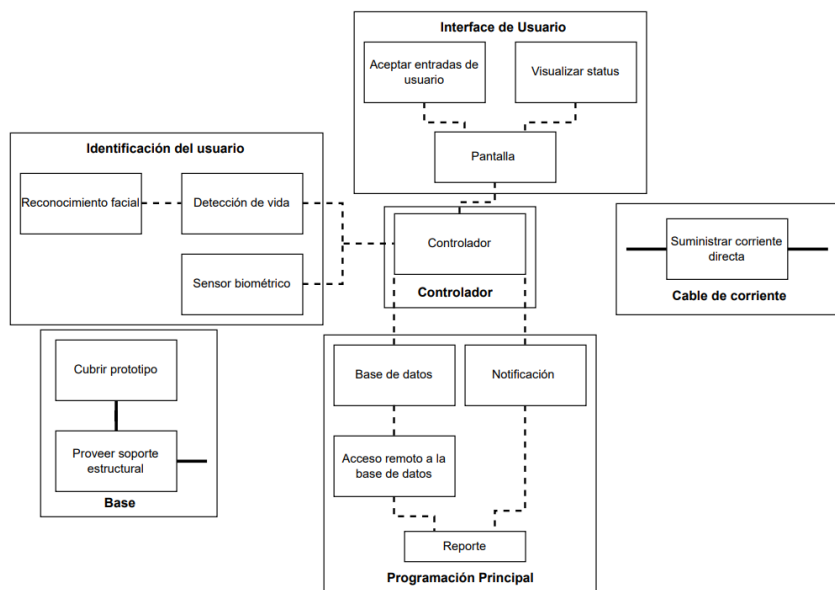


**Agrupación de los elementos del esquema**

La agrupación de los elementos del esquema es un procedimiento para manipular la complejidad del sistema y con ello tener una idea más clara del prototipo.

**Figura 10**

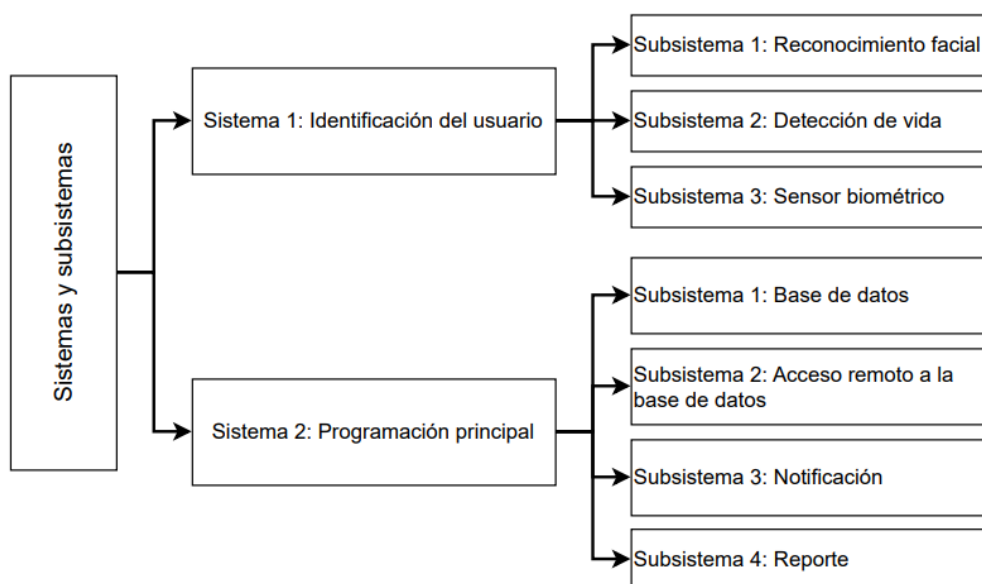
*Agrupación de los elementos del esquema*



Para formar el sistema, se incluyen varios sistemas y subsistemas en la organización de los componentes del diseño del prototipo, lo que juntos permiten una identificación precisa del usuario para su registro posterior en la base de datos, esta agrupación se puede visualizar en la figura 11.

**Figura 11**

*Sistemas y subsistemas del prototipo*



### Alternativas y selección de componentes

Se presentan opciones con distintas características para cada componente que permitan elegir una solución adecuada. Se establece un criterio de análisis y selección de alternativa con mayor ponderación. Dicho análisis se lo realiza con el siguiente criterio:

**Tabla 6**

*Criterio de análisis para la selección de alternativa*

Simbología	Descripción	Valor numérico
+	Fuerte	1
-	Bajo	-1
0	Medio	0

## Alternativas y selección de la tarjeta programable para visión artificial

### **Alternativa 1. Raspberry Pi3 Model A+**

La Raspberry Pi3 Model A+ es de tamaño reducido y compacto con un procesador Broadcom BCM2837B0, con una memoria RAM de 512 MB, posee un único puerto USB 2.0, un puerto HDMI, un puerto CSI para conectar una cámara, una entrada microSD y conectividad de WIFI de doble banda de 2.4 GHz y 5 GHz (Raspberry Pi, 2018).

### **Figura 12**

*Raspberry Pi3 Model A+*



*Nota.* Tomado de (Raspberry Pi, 2018).

### **Alternativa 2. Raspberry Pi3 Model B+**

La Raspberry Pi3 Model B+ posee de: un procesador Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC @ 1.4GHz, una memoria RAM de 1 GB, un puerto HDMI, 4 puertos USB 2.0, un puerto CSI para conectar una cámara y un puerto DSI para conectar una pantalla. En cuanto a conectividad se tiene una tarjeta de red, Gigabit Ethernet sobre USB 2.0 limitada hasta los 300 Mbps o Wi-Fi a doble banda 2.4 GHz y 5 GHz (HasdZone, 2021).

**Figura 13***Raspberry Pi3 Model B+*

*Nota.* Tomado de (HasdZone, 2021).

**Alternativa 3. LattePanda Delta**

La LattePanda Delta, posee de: una CPU Intel Celeron N4100 de cuatro núcleos de 1,1 GHz hasta 2,40 GHz. Tiene una memoria RAM de 4 GB y de almacenamiento de 32 GB, un ventilador de refrigeración activo montado, soporta los sistemas operativos de Windows, LattePanda SBC o Linux. Para la conectividad se tiene una entrada de conexión Gigabit Ethernet y WI-FI 802.11ac (Manuals, 2022).

**Figura 14***LattePanda Delta*

*Nota.* Tomado de (Manuals, 2022).



### **Selección de la mejor alternativa de tarjeta programable**

Se procede a seleccionar un dispositivo accesible para la aplicación y que permita una rápida respuesta de procesamiento computacional, facilitando el proceso de algoritmos de reconocimiento facial sin afectar el rendimiento del mismo.

**Tabla 7**

*Matriz de selección de la tarjeta programable*

Criterio de selección	Alternativas		
	Raspberry Pi3 Model A+	Raspberry Pi3 Model B+	LattePanda Delta
CPU	-	-	+
Memoria RAM	-	0	+
Puertos USB	-	0	+
Conectividad	+	+	+
Sencillez de Programación	0	0	0
Precio	+	+	-
Suma +	2	2	4
Suma -	3	1	1
Suma 0	1	3	1
Evaluación	-1	1	3
Lugar	3	2	1

De acuerdo con la tabla 7, la tarjeta programable seleccionada es la alternativa 3, LattePanda Delta, que ofrece las prestaciones necesarias para el desarrollo del prototipo: posee un procesador que optimiza los recursos al momento de realizar aplicaciones con visión e inteligencia artificial, el tamaño de la placa es reducido, la programación es compatible con el lenguaje Python, la velocidad de procesamiento computacional es rápida y el costo es accesible para la empresa, por lo tanto resulta en una placa idónea para la implementación del prototipo y que no requiere de sobredimensionamientos en prestaciones como ofrece la otra alternativa.

## **Alternativas y selección de la cámara**

### ***Alternativa 1. Cámara Web HD 480dpi***

La cámara posee un sensor CMOS de 1/7", chipset VGA 2072, una relación de resolución de VGA 480 píxeles, ángulo de visión de 120°, píxeles físicos de 30 W, posee un micrófono incorporado, conexión de entrada USB, la longitud de línea USB de 120 cm (NOVICOMPU).

### **Figura 15**

*Cámara Web HD 480dpi*



*Nota.* Tomado de (NOVICOMPU).

### ***Alternativa 2. Webcam USB Mini Computer Camera***

La webcam USB Mini computer Camera posee un sensor de tipo CMOS, la resolución de 1280\*720p, la conexión es a través USB2.0, video HD completo de 1080p con enfoque manual y corrección de luz avanzada para un video limpio y claro, un rango dinámico de más de 72dB, compensación de color automático, modo de video de color de 24 bits y es compatible con diferentes sistemas operativos (TOMTOP, 2020).

**Figura 16**

*Webcam USB Mini Computer Camera*



*Nota.* Tomado de (TOMTOP, 2020).

***Alternativa 3. C270 HD Webcam***

La cámara web HD C270 tiene una resolución máxima de 720p/30fps en pantalla panorámica, lente de plástico y enfoque fijo. El campo visual diagonal es de 55° y corrección de iluminación automática. La forma de conexión es mediante un puerto USB-A (Logitech, 2022).

**Figura 17**

*Cámara web HD C270*



*Nota.* Tomado de (Logitech, 2022).

### Selección de la mejor alternativa de la cámara

**Tabla 8**

*Matriz de selección de la cámara*

Criterio de selección	Alternativas		
	Cámara Web HD 480 dpi	Webcam USB mini computer camera	C270 HD Webcam
Resolución	-	+	+
Conexión	0	0	0
Enfoque	0	+	0
Tipo de sensor	+	+	-
Compensación de color	-	0	+
Apariencia	0	+	0
Protección	0	+	0
Suma +	1	5	2
Suma -	2	0	1
Suma 0	4	2	4
Evaluación	-1	5	1
Lugar	3	1	2

De acuerdo con la tabla 8, la cámara seleccionada es la alternativa 2, Webcam USB mini computer camera, que consta con una resolución de video aceptable para el prototipo y es óptima para tener el reconocimiento facial, ya que una correcta adquisición de imagen da un paso muy importante para que el reconocimiento tenga éxito.

### Alternativas y selección de la pantalla

#### ***Alternativa 1. Pantalla LCD táctil capacitiva de 7 pulgadas (H) con estuche***

La Pantalla LCD táctil capacitiva de 7 pulgadas (H) con estuche de la marca Waveshare tiene una resolución de 1024x600 pixeles, soporta diferentes sistemas operativos como Linux base de NVIDIA, Raspbian, Ubuntu, Windows; el puerto de conexión de pantalla es de HDMI/VGA, panel de visualización IPS, ángulo de visión de 170°, 5 puntos de contacto, el estuche es de policarbonato y posee una certificación CE (WAVESHARE, 2021).

**Figura 18**

*Pantalla LCD táctil capacitiva de 7 pulgadas (H) con estuche*



*Nota.* Tomado de (WAVESHARE, 2021).

**Alternativa 2. Pantalla LCD táctil capacitiva de 7 pulgadas (B)**

La Pantalla LCD táctil capacitiva de 7 pulgadas (B) de la marca Waveshare, tiene una resolución de 800x480 píxeles, un puerto de visualización HDMI, bajo consumo de energía, 5 puntos de contacto, soporta sistemas operativos como Raspbian, Ubuntu, Retropie, Win10 y posee una certificación CE (WAVESHARE, 2021).

**Figura 19**

*Pantalla LCD táctil capacitiva de 7 pulgadas (B)*



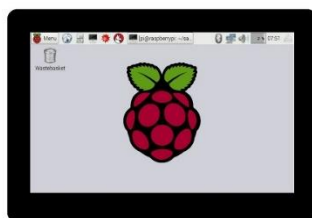
*Nota.* Tomado de (WAVESHARE, 2021).

### **Alternativa 3. Pantalla táctil capacitiva IPS de 5 pulgadas**

La pantalla táctil capacitiva IPS de 5 pulgadas tiene una resolución de 800x480 píxeles, la pantalla es de vidrio templado y puede tener hasta 5 puntos táctiles dependiendo del sistema operativo, consumo bajo de energía, puerto de pantalla DSI, soporta diferentes sistemas operativos como Ubuntu, Kali, Win10, entre otros (WAVESHARE, 2020).

#### **Figura 20**

*Pantalla táctil capacitiva IPS de 5 pulgadas*



*Nota.* Tomado de (WAVESHARE, 2020).

### **Selección de la mejor alternativa para la pantalla**

#### **Tabla 9**

*Matriz de selección de la pantalla*

Criterio de selección	Alternativas		
	Pantalla LCD táctil capacitiva de 7 pulgadas (H) con estuche	Pantalla LCD táctil capacitiva de 7 pulgadas (B)	Pantalla táctil capacitiva IPS de 5 pulgadas
Resolución	+	-	0
Soporte de SO	0	0	0
Ángulo de Visión	+	0	-
Puertos de Conexión	+	-	0
Panel de Visualización	+	+	+
Apariencia	+	0	+
Protección	+	-	0
Suma +	6	1	2
Suma -	0	3	1
Suma 0	1	3	4
Evaluación	6	-2	1
Lugar	1	3	2

De acuerdo con la tabla 9, la pantalla seleccionada es la alternativa 1, pantalla LCD táctil capacitiva de 7 pulgadas (H) con estuche, que consta con una resolución aceptable para la aplicación, permite una rápida instalación y conexión con la tarjeta programable. Se puede interactuar más eficazmente por de la pantalla táctil, concediendo una navegación más sencilla y natural.

### **Alternativas y selección de opción biométrica**

#### ***Alternativa 1. Lector de huella dactilar biométrico digital Fingerprint Kookye***

El módulo de lector de huella dactilar biométrico digital Fingerprint Kookye posee una capacidad de almacenamiento de 1000 huellas, archivo de firma de 256 bytes, archivo de plantilla de 512 bytes, tasa de aceptación falsa <0.001%, tiempo de búsqueda de huella de 1 segundo, el voltaje de alimentación es de corriente continua de 3.8-7.0V, corriente de trabajo <65 mA y el área de ventana es de 14.5x19.4 mm (ELECTROSTORE, 2019).

#### **Figura 21**

*Lector de huella dactilar biométrico digital Fingerprint Kookye*



*Nota.* Tomado de (ELECTROSTORE, 2019).

#### ***Alternativa 2. Lector de huella digital FPM10A***

El módulo de lector de huella digital FPM10A posee un almacenamiento de hasta 200 huellas en la memoria flash del dispositivo, el tiempo de muestreo es de 1 segundo para la

lectura, el voltaje de operación es de 3.3 V, la corriente de operación es de 100 mA – 150 mA, las dimensiones de ventana es de 14x18 mm. Además, el lector contiene un led verde que se enciende cada vez que se está trabajando con el sensor (Tecnopura, 2020).

### **Figura 22**

*Lector de huella digital FPM10A*



*Nota.* Tomado de (Tecnopura, 2020).

### **Alternativa 3. Suprema RealSCAN-G10**

El escáner de captura de huella Suprema RealSCAN-G10 posee una superficie amplia para el reconocimiento de una huella rotada / 4 huellas / 2 pulgares, protección IP54, resolución de 500 dpi, área del sensor 89x80 mm, un peso de 1.8 kg, conectividad de USB 2.0, y es compatible con diferentes sistemas operativos como de sus deferentes versiones de Windows y Linux (Suprema ID, 2021).

### **Figura 23**

*Suprema RealSCAN-G10*



*Nota.* Tomado de (Suprema ID, 2021).



### Selección de la mejor alternativa biométrica

**Tabla 10**

*Matriz de selección del sensor biométrico*

Criterio de selección	Alternativas		
	Lector de huella dactilar biométrico digital Fingerprint Kookye	Lector de huella digital FPM10A	Suprema RealSCAN-G10
Resolución	-	-	+
Soporte de SO	+	+	0
Conectividad	+	+	+
Almacenamiento	+	-	0
Tamaño	+	0	-
Apariencia	0	0	+
Suma +	4	2	3
Suma -	1	2	1
Suma 0	1	2	2
Evaluación	3	0	2
Lugar	1	3	2

De acuerdo con la tabla 10, la alternativa seleccionada es el lector de huella dactilar biométrico digital Fingerprint Kookye, que consta con un procesador DSP de alta velocidad, almacenamiento de 1000 muestras, soporta la entrada de huellas dactilares, el procesamiento de imágenes, comparación y la búsqueda de las mismas, y tiene una elevada sensibilidad de reconocimiento de huellas tanto en húmedo como en seco.

### Capítulo III:

#### Desarrollo e implementación del sistema

En este capítulo se presentan el diseño de la estructura, construcción e implementación del prototipo de sistema biométrico para monitorear el control de acceso de personal utilizando visión artificial.

#### Diseño de la estructura mecánica

La concepción y los requerimientos descritos en el capítulo anterior son la base para el diseño de la estructura mecánica, con el fin de establecer la forma y el tamaño adecuado del prototipo, la misma que fue diseñado en Autodesk Inventor. A continuación, se visualiza el diseño final de la estructura del prototipo de sistema biométrico.

#### Figura 24

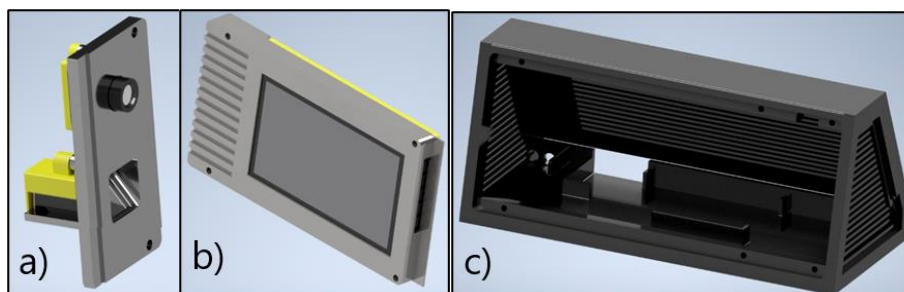
*Diseño CAD del prototipo de sistema biométrico*



En el modelo se detalla el diseño de las piezas y componentes que forman parte del prototipo, mismos que se realizan tomando en cuenta el tamaño de cada elemento y con el propósito de facilitar el ensamblaje final se ha optado por dividirlo en 3 módulos como se muestra en la figura 25.

## Figura 25

*Diseño CAD del prototipo dividido en partes*



*Nota.* a) Se encuentran la cámara y el sensor de huella digital con sus soportes. b) Se encuentra la pantalla con su respectivo soporte. c) Se muestra toda la carcasa del prototipo.

### **Análisis estático del diseño**

Se describe el análisis estático que se realiza en las partes cruciales de la estructura, con el fin de comprobar que el diseño mecánico es el adecuado. El análisis se ejecuta mediante computador, el software Autodesk Inventor permite generar simulaciones para demostrar el factor de seguridad de la pieza y la variación de la deformación.

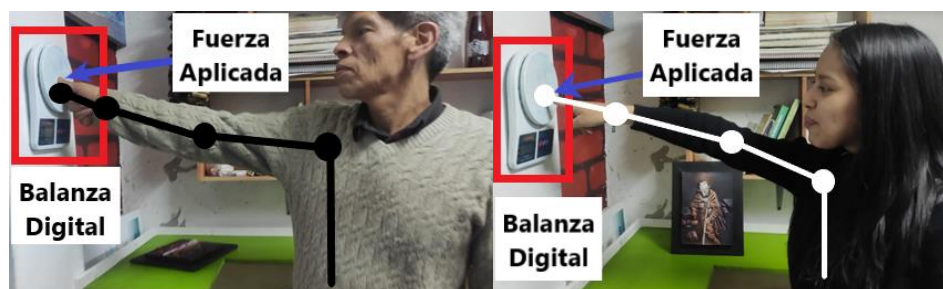
La fuerza de empuje es la cantidad de fuerza necesaria para aplicar una presión que actúa como una carga puntual sobre el sistema, este valor puede variar ampliamente dependiendo de varios factores, como la musculatura, la flexibilidad y la salud de la persona. Los dedos más comúnmente utilizados para interactuar con pantallas táctiles son el dedo índice y el dedo pulgar. Esto se debe a que estos dos dedos son los que tienen mayor movilidad y precisión en la punta, lo que los hace ideales para presionar botones y hacer gestos en pantallas táctiles.

Para determinar la carga puntual se procedió a medir la fuerza de ambos dedos mencionados anteriormente en 10 personas, utilizando una balanza digital en una posición neutral como se muestra en la figura 26, se mide en 10 ocasiones diferentes con el objetivo de

reducir la variación en las mediciones. El grupo de prueba estaba compuesto de una cantidad equilibrada de hombres y mujeres sin ninguna condición médica en las manos.

**Figura 26**

*Medición de fuerza en el dedo tanto para hombre y mujer*



En las tablas 11 y 12 se presenta los datos obtenidos de las personas.

**Tabla 11**

*Datos recolectados de la medición del dedo índice en gramos-fuerza*

# Persona	Dedo Índice (gf)									
	Muestras									
	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Persona 1	1958	1762	1928	1610	1557	1859	2315	1987	2027	1997
Persona 2	1615	1523	1487	1789	1345	1274	1462	1326	1174	1456
Persona 3	1723	1468	1449	1562	1414	1663	1345	1452	1487	1563
Persona 4	1445	1456	1522	1407	1236	1547	1865	1547	1584	1465
Persona 5	1840	1645	1478	1896	1587	1698	1789	1687	1877	1824
Persona 6	1698	1745	1874	1765	1623	1678	1742	1763	1654	1851
Persona 7	1895	1741	1864	1862	1459	1628	1782	1615	1699	1742
Persona 8	1712	1645	1662	1523	1589	1648	1695	1742	1732	1616
Persona 9	1887	1852	1624	1587	1652	1785	1691	1749	1856	1685
Persona 10	1745	1638	1662	1789	1873	1852	1741	1698	1723	1792

**Tabla 12**

*Datos recolectados de la medición del dedo pulgar en gramos-fuerza*

<b>Dedo Pulgar (gf)</b>										
<b># Persona</b>	<b>Muestras</b>									
	<b>#1</b>	<b>#2</b>	<b>#3</b>	<b>#4</b>	<b>#5</b>	<b>#6</b>	<b>#7</b>	<b>#8</b>	<b>#9</b>	<b>#10</b>
<b>Persona 1</b>	1816	2715	2560	2371	2465	2576	2016	2308	2587	2186
<b>Persona 2</b>	2556	2432	2419	2312	2418	2462	2387	2369	2246	2275
<b>Persona 3</b>	2319	2147	2563	2458	2631	2456	2411	2545	2626	2415
<b>Persona 4</b>	2136	2121	2277	2348	2256	2344	2145	2487	2315	2142
<b>Persona 5</b>	2285	2378	2551	2449	2423	2419	2561	2513	2416	2465
<b>Persona 6</b>	2187	2068	1976	2163	2047	2314	2318	2364	2158	2097
<b>Persona 7</b>	2074	2449	2301	2019	1972	2036	2404	2036	2165	2241
<b>Persona 8</b>	2310	2410	2263	2319	2008	2045	2163	2174	2186	2237
<b>Persona 9</b>	2265	2016	2398	2241	2635	2154	2457	2231	1965	2014
<b>Persona 10</b>	2031	2451	2322	2274	2349	2371	2261	2285	2031	2312

Una vez tomadas las mediciones de las 10 personas se determina la media de la fuerza de cada dedo. En la tabla 13 se visualiza los resultados obtenidos.

**Tabla 13**

*Promedio de la fuerza en los dedos de cada persona*

<b># Persona</b>	<b>Media de la fuerza (gf)</b>	
	<b>Dedo Índice</b>	<b>Dedo Pulgar</b>
<b>Persona 1</b>	1900	2360
<b>Persona 2</b>	1445,1	2387,6
<b>Persona 3</b>	1512,6	2457,1
<b>Persona 4</b>	1507,4	2257,1
<b>Persona 5</b>	1732,1	2446
<b>Persona 6</b>	1739,3	2169,2
<b>Persona 7</b>	1728,7	2169,7
<b>Persona 8</b>	1656,4	2211,5
<b>Persona 9</b>	1736,8	2237,6
<b>Persona 10</b>	1751,3	2268,7
<b>Promedio</b>	1670,97	2296,45

Teniendo en cuenta los resultados de la tabla 13 la fuerza mayor de empuje se produce con el dedo pulgar de 2296,45 *gf*, seguido del dedo índice con una fuerza 1670,97 *gf*. Por lo cual se selecciona la fuerza mayor para realizar el análisis estático:

$$F = 2296,45 \text{ gf} = 2,296 \text{ N}$$

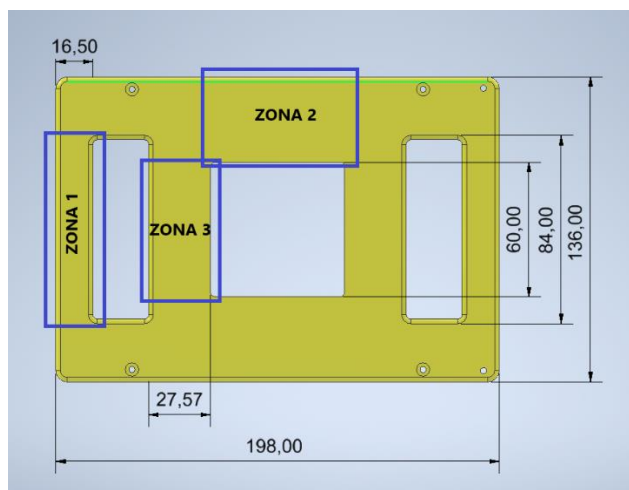
### **Análisis de la estructura de soporte de pantalla**

La estructura de soporte de pantalla es el elemento encargado de sobrellevar la fijación de la pantalla en el prototipo. Se debe considerar las propiedades del material y la fuerza que se somete a la estructura. La carga puntual parte del contacto de la pantalla con el dedo del usuario, que actuará como una carga puntual sobre la estructura de soporte.

Las propiedades mecánicas del PLA que se deben considerar en el elemento son: el esfuerzo a la fluencia de 2,58 *MPa* y el módulo de elasticidad es de 3150 *MPa*. En la figura 27 se muestra la estructura de soporte de pantalla dividida en tres zonas críticas.

### **Figura 27**

*Soporte de pantalla dividida en tres zonas críticas*

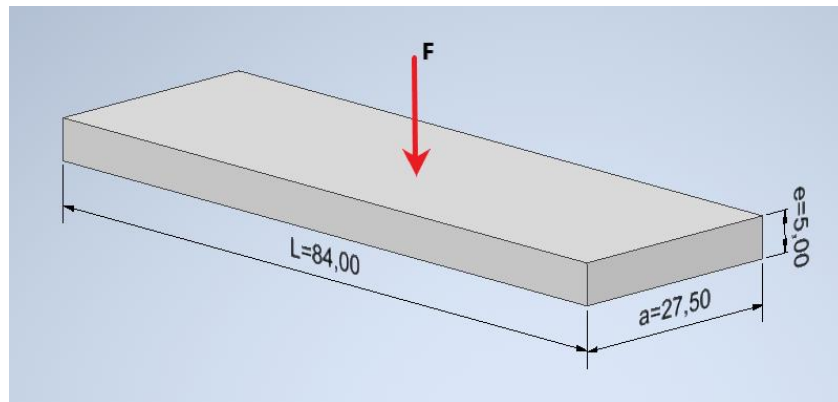


En éstas tres zonas se tienen en cuenta su sección transversal, longitud y ubicación. La zona 1 tiene una mayor longitud y una menor sección transversal, la zona 2 tiene la mayor

sección transversal, pero éstas se encuentran ambas en el extremo, por lo tanto, van a tener una menor deformación y no se van a considerar. Por tal motivo la sección crítica que se va a examinar es la zona 3, que al momento de realizar el análisis ésta actúa como una viga con los apoyos fijos y una carga central.

### Figura 28

*Sección crítica seleccionada del soporte de pantalla*



*Nota.* Se detalla cada uno de sus datos, donde: F = carga puntual, L= longitud de la viga, e = espesor de la viga y a = longitud de la sección transversal.

**Factor de seguridad ( $n$ ):**

$$n = \frac{S_y}{\sigma} \quad (1)$$

Donde:

$S_y$ = Esfuerzo de fluencia

$\sigma$ = Esfuerzo de flexión

**El esfuerzo de flexión ( $\sigma$ ):**

$$\sigma = \frac{M_{\max}}{S} \quad (2)$$

Donde:

$M_{max}$  = Momento máximo

$S$  = Módulo de resistencia

**Momento máximo ( $M_{max}$ ):**

$$M_{max} = \frac{F * L}{8} \quad (3)$$

Donde:

$F$  = Fuerza de la carga puntual

$L$  = Longitud de la viga

**Módulo de resistencia ( $S$ ):**

$$S = \frac{I}{c} \quad (4)$$

Donde:

$I$  = Inercia

$c$  = Es la distancia desde el eje neutro a la fibra más alejada de la sección transversal

**Inercia ( $I$ ):**

$$I = \frac{b * h^3}{12} \quad (5)$$

Donde:

$b$  = Base

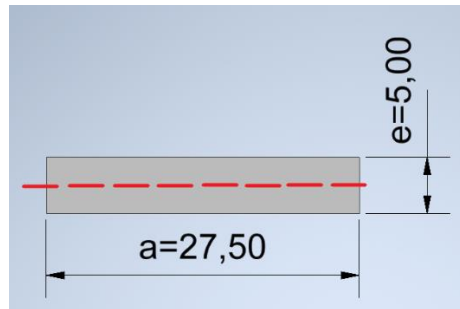
$h$  = Altura

Se aplica la ecuación 5 para la sección transversal de la zona 3:



**Figura 29**

Sección transversal de la zona 3 de análisis



$$I = \frac{b * h^3}{12}$$

$$I = \frac{a * e^3}{12} \quad (6)$$

Se procede a reemplazar la ecuación (2), ecuación (3), ecuación (4) y ecuación (6) en la ecuación (1) para determinar el factor de seguridad de la viga.

$$n = \frac{S_y}{\sigma}$$

$$n = \frac{S_y}{\frac{M_{\max}}{S}}$$

$$n = \frac{a * e^2 * S_y}{6 * M_{\max}}$$

$$n = \frac{8 * a * e^2 * S_y}{6 * F * L}$$

$$n = \frac{8 * (0,0275 \text{ m}) * (0,005 \text{ m})^2 * (2,58 \text{ MPa})}{6 * (2,296 \text{ N}) * (0,084 \text{ m})}$$

$$n = 12,26$$

**Deflexión máxima ( $Y_{max}$ ):**

$$Y_{max} = -\frac{F * L^3}{192 * E * I} \quad (7)$$

Donde:

$F$ = Fuerza de la carga puntual

$L$ = Longitud de la viga

$E$ = Módulo de Elasticidad

$I$ = Inercia

Reemplazando la ecuación (6) en la ecuación (7) y reemplazando los valores se obtiene la deformación máxima de la viga:

$$Y_{max} = -\frac{12 * F * L^3}{192 * E * a * e^3}$$

$$Y_{max} = -\frac{12 * 2,296 \text{ N} * (0.084 \text{ m})^3}{192 * 3150 \text{ MPa} * 0.0275 \text{ m} * (0.005 \text{ m})^3}$$

$$Y_{max} = -7,854824 * 10^{-6} \text{ m} = -7,854824 * 10^{-3} \text{ mm}$$

Se procede a calcular el límite de flexión recomendado:

$$Y_{max}^r = \frac{L}{360} \quad (8)$$

Donde:

$L$ = Longitud de la viga

Se reemplaza el valor de la longitud de la viga en la ecuación (8) para calcular el límite de flexión máxima recomendado:

$$Y_{max}^r = \frac{L}{360}$$

$$Y_{max}^r = \frac{0.084 \text{ m}}{360}$$

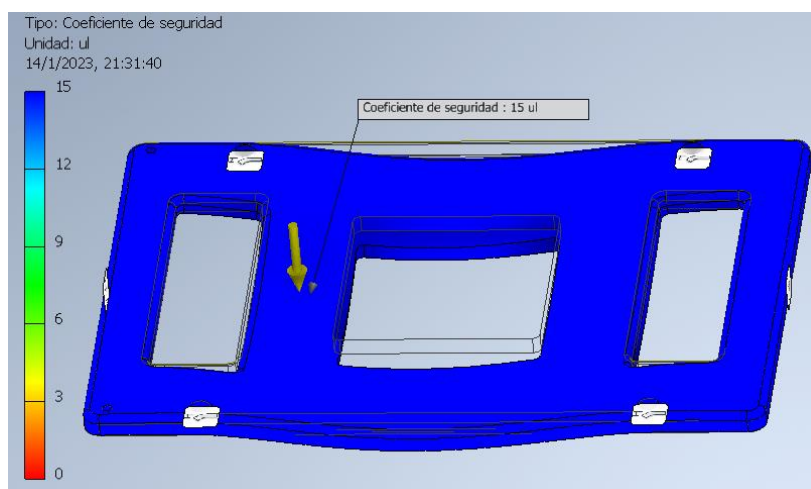
$$Y_{max}^r = 2.3333 * 10^{-4} \text{ m} = 0.2333 \text{ mm}$$

El valor de deflexión máximo calculado  $Y_{max} = -7,854824 * 10^{-6} \text{ m}$  es menor al recomendado  $Y_{max}^r = 2.3333 * 10^{-4} \text{ m}$ . Se puede verificar que la estructura satisface las necesidades del diseño.

Se enfatiza en que a pesar de tener fuerzas bajas que no suponen un esfuerzo a la estructura, es recomendable realizar la simulación para inspeccionar cómo se comporta el elemento. Por lo cual se realiza un análisis de elementos finitos como se muestra en la figura 30, el factor de seguridad señala un valor de 15, lo que indica un sobredimensionamiento, pero no se toman en cuenta los cambios en el material por el bajo costo y la facilidad de obtención del PLA.

### Figura 30

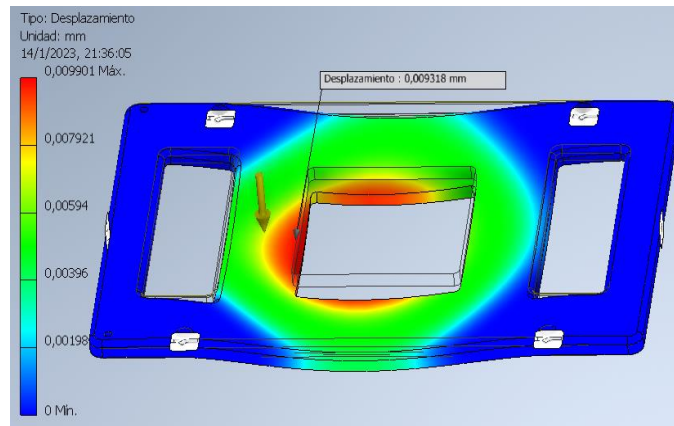
*Simulación del factor de seguridad en el soporte de pantalla*



En el análisis de la deformación mostrado en la figura 31, llega a ser mínimo con un valor de  $0.009318 \text{ mm}$ , mismo que no simboliza ningún inconveniente con el diseño, calificándolo como aceptable para soportar la carga que se produzca en la pantalla.

### Figura 31

*Simulación del desplazamiento del soporte de pantalla*

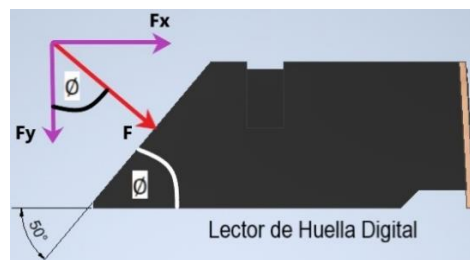


### ***Análisis de estructura de soporte del lector de huella digital***

El soporte es el elemento encargado para la fijación del lector de huella digital por lo cual debe soportar cualquier carga que se pueda ejecutar sobre sí mismo. Se selecciona nuevamente la mayor fuerza que se produce con el dedo pulgar de  $2,296 \text{ N}$  para realizar el análisis estático. En la figura 32 se señala la descomposición de la fuerza ya que al momento de hacer contacto el dedo con el lector, éste tiene una inclinación de  $50^\circ$ .

### Figura 32

*Descomposición de la fuerza en el lector de huella digital*



Las componentes de la fuerza son:

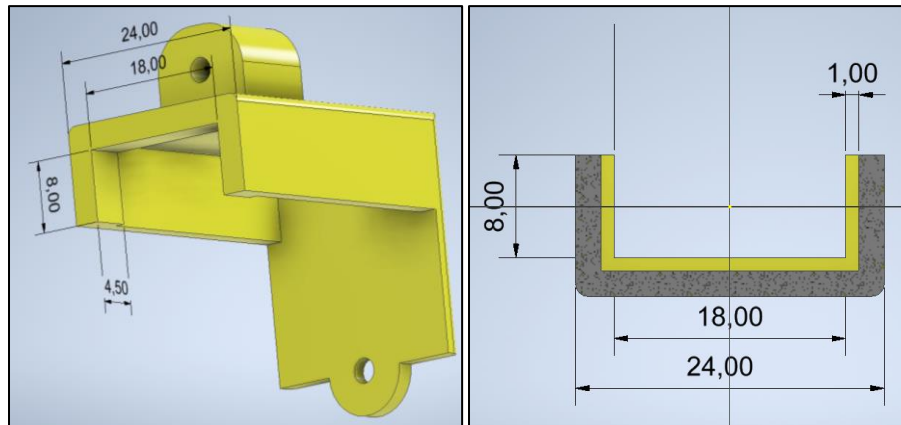
$$F_x = F * \sin(\varnothing) = 2,296 \text{ N} * \sin(50^\circ) = 1.7588 \text{ N}$$

$$F_y = F * \cos(\varnothing) = 2,296 \text{ N} * \cos(50^\circ) = 1.4758 \text{ N}$$

Se centra con la componente  $F_x$  ya que es la fuerza que trata de afectar al soporte del sensor. En la figura 33 se muestra el soporte del lector de huella digital donde se define la parte crítica que es la cuña, la cual va a soportar toda la fuerza de empuje del dedo. La componente  $F_x$  se encuentra paralela a la superficie de la cuña, lo que significa que está sometida a esfuerzo cortante.

### Figura 33

*Diseño del soporte del lector de huella digital*



a)

b)

*Nota.* a) Se muestra todo el componente del soporte del lector de huella digital. b) Se indica la parte de la cuña a analizar con sus respectivas dimensiones.

**Factor de seguridad ( $n$ ):**

$$n = \frac{S_y}{\tau} \quad (9)$$

Donde:

$S_y$  = Esfuerzo de fluencia

$\tau$  = Esfuerzo cortante

**Esfuerzo cortante ( $\tau$ ):**

$$\tau = \frac{F}{A} \quad (10)$$

Donde:

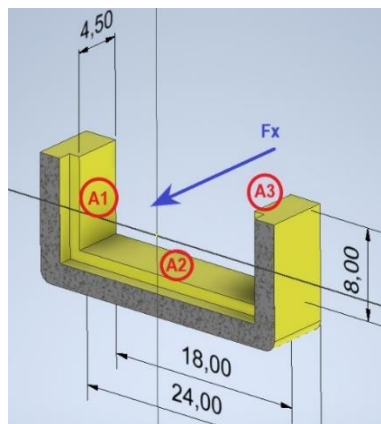
$F$  = Fuerza cortante

$A$  = Área

Para calcular el área es necesario sumar todas las áreas que están alineadas con la fuerza, en la figura 34 se muestran las áreas paralelas a la fuerza cortante en la cuña.

### Figura 34

*Áreas paralelas a la fuerza cortante en la cuña*



$$A_t = A_1 + A_2 + A_3$$

$$A_t = 4,5 \text{ mm} * 8 \text{ mm} + 18 \text{ mm} * 4,5 \text{ mm} + 4,5 \text{ mm} * 8 \text{ mm}$$

$$A_t = 153 \text{ mm}^2 = 1,53 * 10^{-5} \text{ m}^2$$

Se reemplaza la ecuación (10) en la ecuación (9) para determinar el factor de seguridad teniendo en cuenta que el área ( $A$ ) debe ser el área total ( $A_t$ ) de todas las áreas paralelas.

$$n = \frac{S_y}{\tau}$$

$$n = \frac{S_y}{\frac{F_x}{A_t}}$$

$$n = \frac{S_y * A_t}{F_x}$$

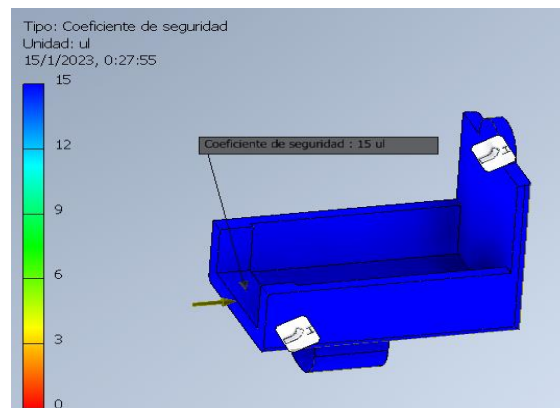
$$n = \frac{(2,58 \text{ MPa}) * 1,53 * 10^{-5} \text{ m}^2}{1.7588 \text{ N}}$$

$$n = 22,4437$$

De igual forma se realiza la simulación por análisis de elementos finitos, en la figura 35 se puede visualizar el factor de seguridad donde se reafirma la certeza del diseño en el soporte de huella digital con un factor de seguridad máximo de 15, debido a que el elemento tiene un pequeño tamaño, el valor tiende a ser mucho mayor.

### Figura 35

*Simulación del factor de seguridad del soporte de lector de huella digital*

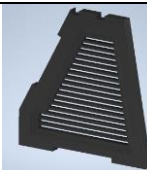
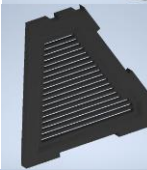


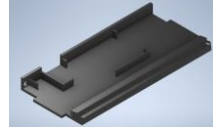
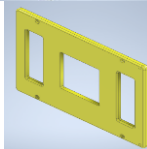



## Construcción del prototipo


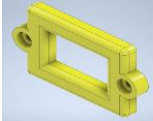
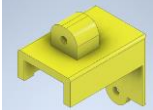
Las partes de la estructura del prototipo son diseñadas en el software CAD Autodesk Inventor que se los exporta con la extensión STL, se transforman a código G utilizando el software Cura para posteriormente realizar la impresión 3D utilizando un filamento PLA con 1.75 mm de diámetro, esta elaboración se lleva a cabo mediante el uso de una impresora Anycubic 3D. En la tabla 14 se muestra las piezas a imprimir con su respectivo gráfico, y también el tiempo de impresión de cada elemento.

**Tabla 14**

*Desglose de elementos diseñados para imprimir*

Nombre (cantidad)	Tiempo de impresión (H:m)	Anexo Plano	Gráfico
Caja tapa lateral derecha (1)	0:38	A-01	
Caja tapa lateral izquierda (1)	0:38	A-02	
Caja tapa lateral (1)	0:20	A-03	
Caja tapa superior (1)	0:22	A-04	
Base caja (1)	0:35	A-05	
Soporte de pantalla (1)	0:17	A-06	
Parte superior pantalla (1)	0:25	A-07	

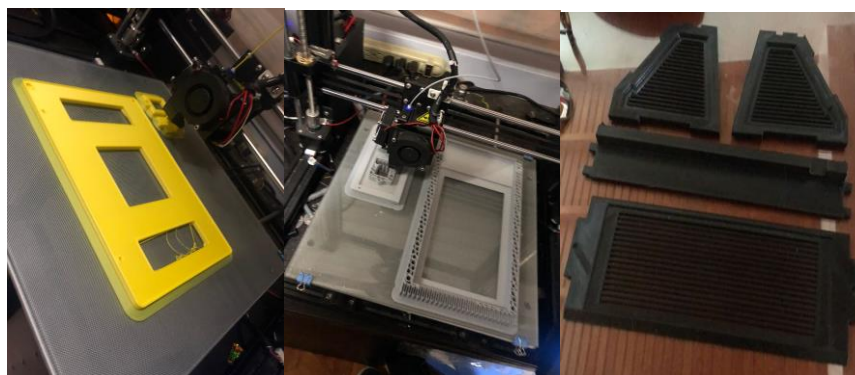


Nombre (cantidad)	Tiempo de impresión (H:m)	Anexo Plano	Gráfico
Parte superior sensor y cámara (1)	0:20	A-08	
Soporte de cámara (1)	0:07	A-09	
Soporte del lector de huella dactilar (1)	0:11	A-10	

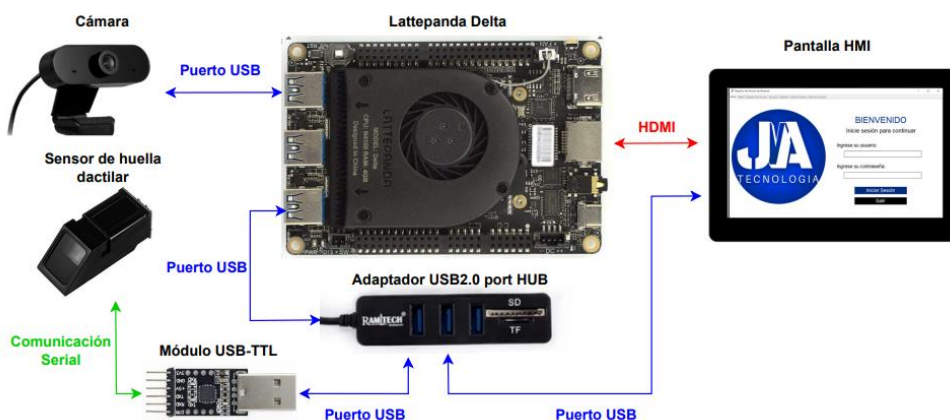
Cada componente está planificado de manera tal que sea posible armarlo parte por parte y después incorporarlos a la estructura externa de la caja. Se procede a imprimir todas las piezas correspondientes como se visualiza en la figura 36 y se realiza la remoción de soportes y limpieza de los mismos para facilitar el montaje.

### Figura 36

*Impresión 3D de los elementos de la estructura*



En la figura 37 se muestra el esquema de conexión que tiene la tarjeta Lattepanada Delta, el sensor de huella dactilares, la cámara y la pantalla.

**Figura 37***Esquema de conexión*

Finalmente, la figura 38 indica el prototipo ya ensamblado con todos sus elementos correspondientes.

**Figura 38***Ensamble del prototipo de sistema biométrico*

### Implementación para el reconocimiento facial

El reconocimiento facial consiste en dos etapas clave: detección de rostro e identificación de la persona. En la primera etapa se utiliza un algoritmo de detección de rostro

para encontrar y localizar los rostros. En la siguiente etapa se utiliza la red neuronal entrenada para comparar y reconocer los rostros presentes en tiempo real.

Para la detección facial se utilizará la librería de MediaPipe Face Detection, que es un detector de rostros liviano y de buen rendimiento diseñado para la inferencia de GPU móvil. La razón principal que se utiliza es debido a sus predicciones ligeras y muy precisas con lo que respecta a detección de rostros, este algoritmo deriva del modelo de MobileNetV1/V2 (MediaPipe, 2020).

Al momento de inicializar el modelo de detección de rostros de mediapipe, se deben proporcionar dos parámetros al crear un objeto de modelo de cara.

- La selección de modelo (0 y 1). Índice entero 0: para seleccionar un modelo de corto alcance, funciona mejor para rostros menores a un metro de la cámara. Índice entero 1: para seleccionar un modelo a rango completo, funciona mejor para rostros hasta 5 metros de distancia de la cámara. Por lo tanto, se maneja con el modelo de índice entero 0.
- El valor mínimo de confianza va desde  $[0.0, 1.0]$ , es la confianza en los resultados de detección para que se considere exitosa, se puede ajustar según los requisitos y la imagen de entrada. Por defecto se utiliza un valor predeterminado de 0.5.

Al aplicar el modelo de detección de rostros de mediapipe se proporciona un cuadro delimitador y 6 puntos de referencia faciales: ojo derecho, ojo izquierdo, punta de la nariz, centro de la boca, trago de la oreja derecha y trago de la oreja izquierda.

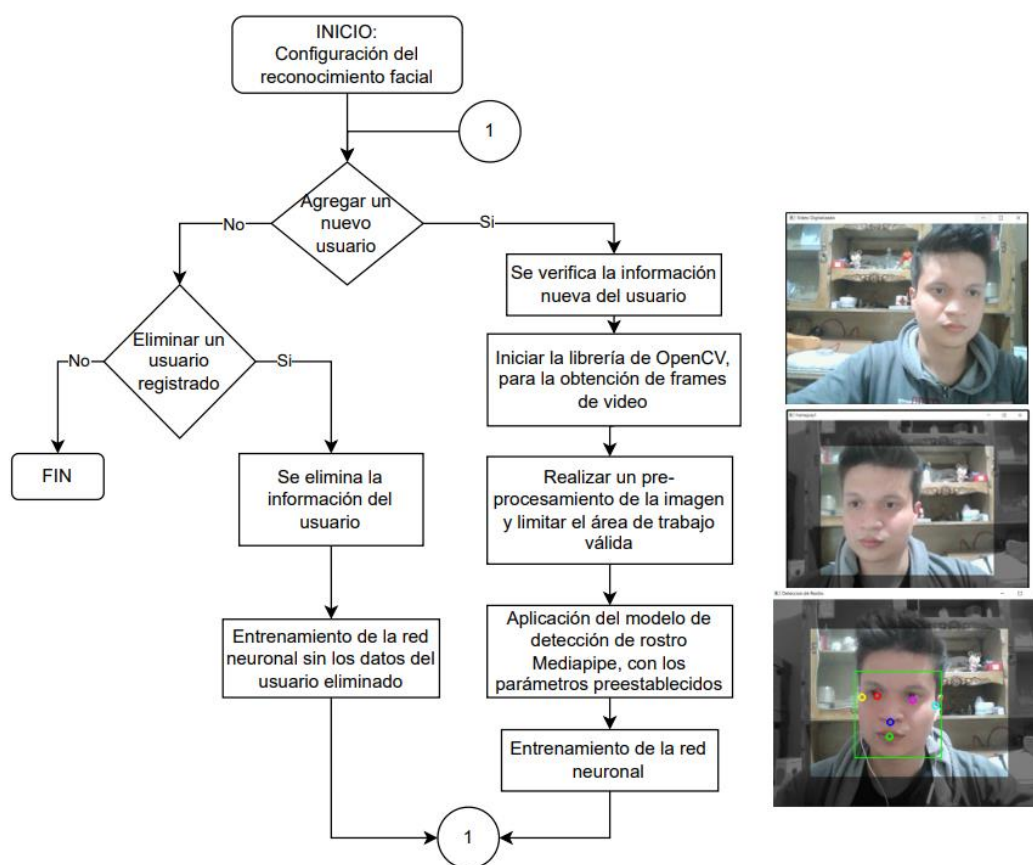
Con este procedimiento de Mediapipe se logra detectar varios rostros simultáneamente, por lo que se extraen solo los valores correspondientes a los rostros que se pueden confirmar como tales.

## Configuración para el reconocimiento facial

Al agregar un nuevo usuario se debe capturar su imagen facial y almacenarla en el banco de imágenes del sistema de reconocimiento. La calidad de la imagen capturada y la cantidad de imágenes almacenadas afectarán la precisión de la identificación facial. Por otro lado, al eliminar un usuario es importante asegurarse de que su imagen facial sea eliminada de la base de datos para evitar cualquier conflicto con la identificación de otras personas. En la figura 39 se muestra el diagrama de secuencia resumida de la configuración para el reconocimiento facial.

**Figura 39**

*Diagrama de secuencia de la configuración para el reconocimiento facial*

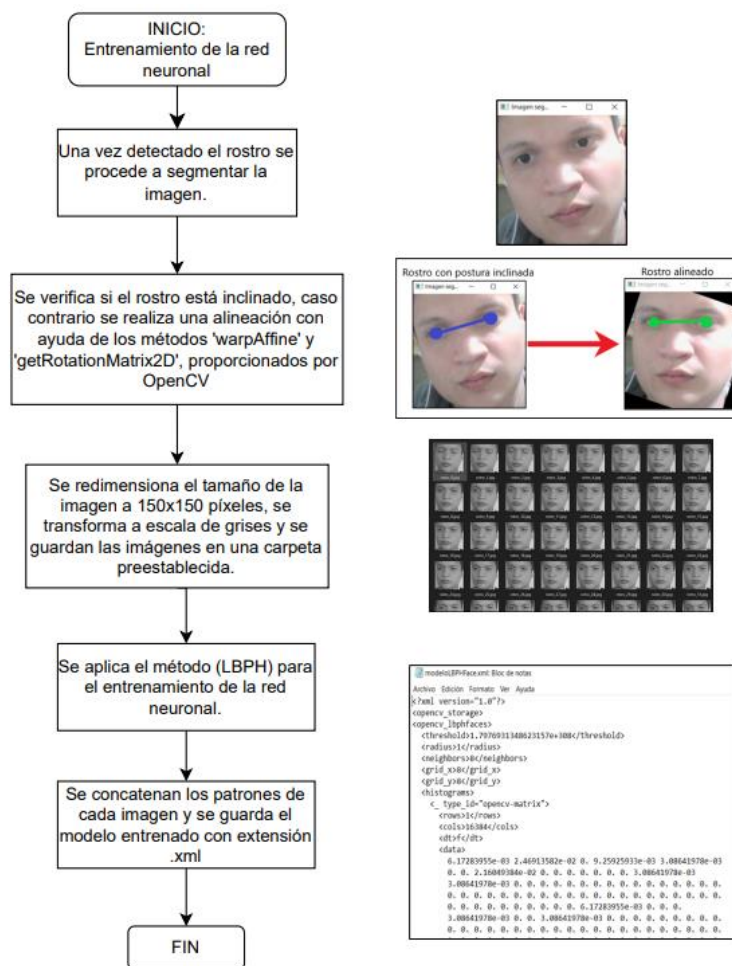


*Nota.* El entrenamiento de la red neuronal se muestra en la figura 40.

Para el entrenamiento de la red neuronal se aplica el método de reconocimiento de rostro LBPH. Al modelo se le entrenará con muestras obtenidas de la detección del rostro. En la figura 40 se indica el proceso para el entrenamiento de la red neuronal.

**Figura 40**

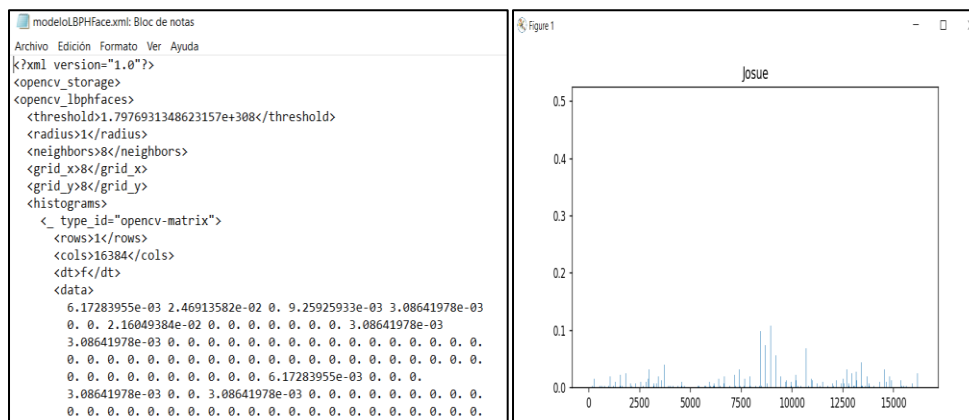
*Diagrama de secuencia del entrenamiento de la red neuronal*



En la figura 41 se puede observar en la parte izquierda los datos de entrenamiento de la red neuronal, incluyendo los pesos finales y los parámetros utilizados en el método LBPH, en la imagen derecha la obtención del histograma de los patrones binarios locales concatenados, que servirá para la identificación facial de la persona.

Figura 41

Archivo .xml e histograma concatenado generado del entrenamiento

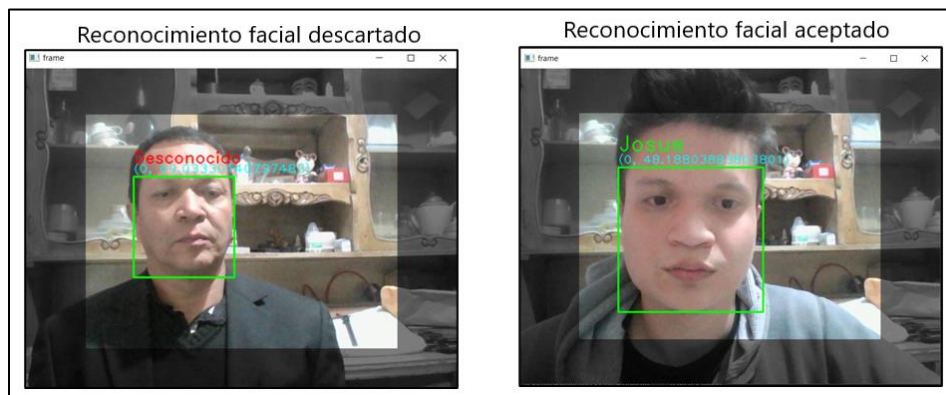


### Funcionamiento para la identificación facial

Para la fase de la identificación facial se utiliza la red neuronal previamente entrenada. Se ejecuta la detección nueva del rostro, en la cual se aplica la función 'predict' y esta devolverá una etiqueta y un valor de asociado a la imagen de entrada determinada. Este valor se le puede comparar con valor umbral para aceptar o desechar el reconocimiento.

Figura 42

Reconocimiento facial



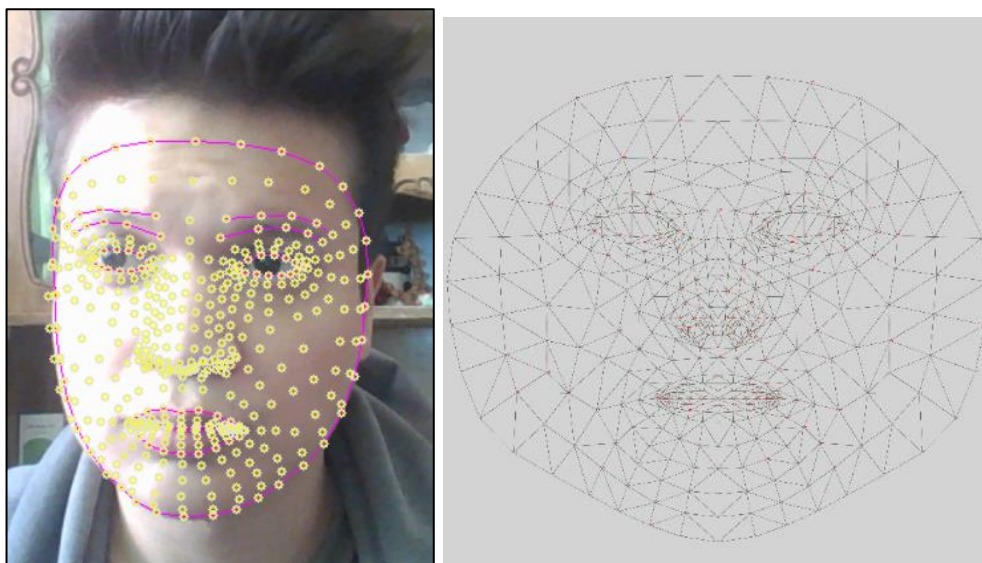
*Nota.* En la imagen izquierda se muestra el reconocimiento facial descartado con un valor de 69,03 y en la imagen derecha el reconocimiento facial aceptado con un valor de 48,18.

### Implementación del subsistema de detección de vida

La técnica Anti-spoofing ha sido implementada adaptando la detección de parpadeo ocular en tiempo real, esta técnica requiere que el usuario realice el movimiento de pestañar frente a la cámara ya que ayudará a evitar la suplantación de identidad, puesto que permite autenticar y verificar al usuario en cuestión de segundos. Se utiliza la librería de MediaPipe Face Mesh ya que es una solución que proporciona 468 puntos de referencia faciales en 3D. Posee una arquitectura de modelo ligero con aceleración de GPU en todo el proceso, y maneja el aprendizaje automático (ML) para inferir la superficie facial 3D (MediaPipe, 2022).

#### Figura 43

*Obtención de la Malla Facial de MediaPipe*

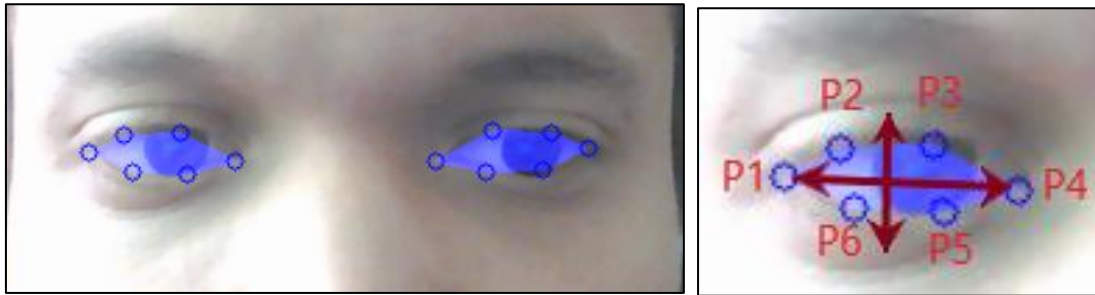


*Nota.* En la imagen izquierda se indican los puntos faciales obtenidos en tiempo real. En la imagen derecha se muestra la disposición de los 468 puntos. Tomado de (MediaPipe, 2022).

Se extraen estructuras faciales específicas, en términos de detección de parpadeo, solo interesa dos conjuntos de estructuras faciales: los ojos. Cada ojo está representado por 6 coordenadas  $(x, y)$ , la primera empieza desde la esquina izquierda del ojo y los demás puntos en el sentido horario de las agujas del reloj del resto de la región.

### Figura 44

Representación de los 6 puntos de referencia del ojo



En el trabajo de investigación de Soukupová y Čech en su artículo de (2016), “Real-Time Eye Blink Detection using Facial Landmarks”, se utiliza una ecuación que refleja la relación de aspecto ocular (EAR):

$$EAR = \frac{\|p_2 - p_6\| + \|p_3 - p_5\|}{2\|p_1 - p_4\|} \quad (11)$$

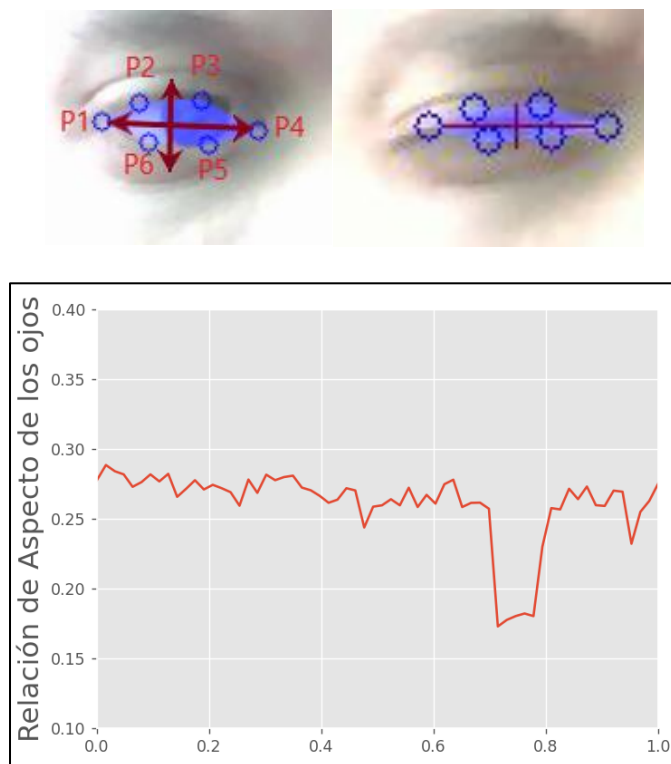
Donde  $(p_1, p_2, p_3, p_4, p_5, p_6)$  son los puntos de las ubicaciones de referencia faciales 2D.

El denominador de la ecuación 11 calcula la diferencia entre los puntos de los ojos horizontales y el numerador calcula la distancia entre los puntos de referencia de los ojos verticales. El resultado de esta relación es constante mientras el ojo está abierto, pero se aproxima a cero cuando se produce un parpadeo, es decir, cuando se cierran los ojos.



**Figura 45**

*Trazado de la proporción de las distancias de los ojos*

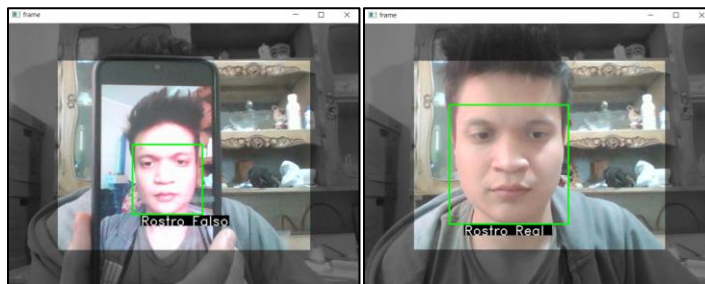


*Nota.* Arriba a la izquierda: se visualiza los puntos de referencia cuando el ojo está abierto. Arriba a la derecha: se visualiza los puntos de referencia cuando el ojo está cerrado. Abajo: se dibuja el trazado de la relación de aspecto de los ojos a lo largo del tiempo. La caída en la relación de aspecto señala un parpadeo.

De acuerdo a la gráfica obtenida en la figura 45 de la relación de aspecto del ojo se procede a tomar un valor de umbral fijo y comparar la relación de aspecto del ojo en tiempo real para verificar que efectivamente se realizó el pestañeo, y con ello tener una predicción de un rostro real o un rostro falso.

## Figura 46

*Identificación de un rostro real y un rostro falso*

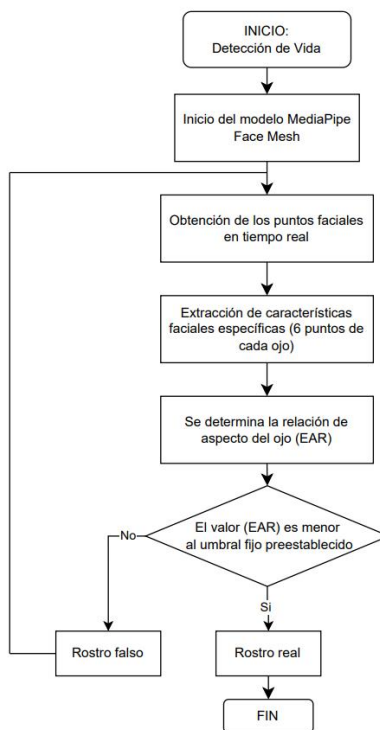


*Nota.* En la figura izquierda se muestra un rostro falso desde un móvil que no pestaña, mientras que en la imagen derecha se muestra un rostro que si pestaña e indica que es real.

Se observa en la figura 47 el diagrama de secuencia de la detección de vida implementado en el sistema.

## Figura 47

*Diagrama de secuencia del algoritmo de detección de vida*

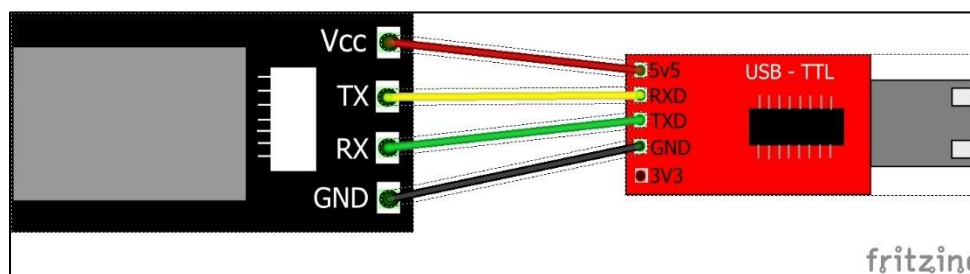


## Implementación del subsistema del sensor biométrico

Para el lector de huella dactilar biométrico digital Fingerprint Kookye se utiliza el módulo USB Serial a TTL CP2102 para la comunicación con la tarjeta LattePanda. Se conecta el sensor al adaptador como se muestra a continuación:

**Figura 48**

*Diagrama de conexión entre el sensor de huellas dactilares y USB-TTL*



*Nota.* Se muestra la conexión de los pines entre el sensor y el módulo USB-TTL. Por el Autor.

**Tabla 15**

*Conexión entre el sensor de huella dactilar y el módulo USB-TTL*

Sensor de huella dactilar (color de cable)	Módulo USB-TTL
VCC (rojo)	5 V
GND (negro)	GND
TXD (amarillo)	RXD
RXD (verde)	TXD

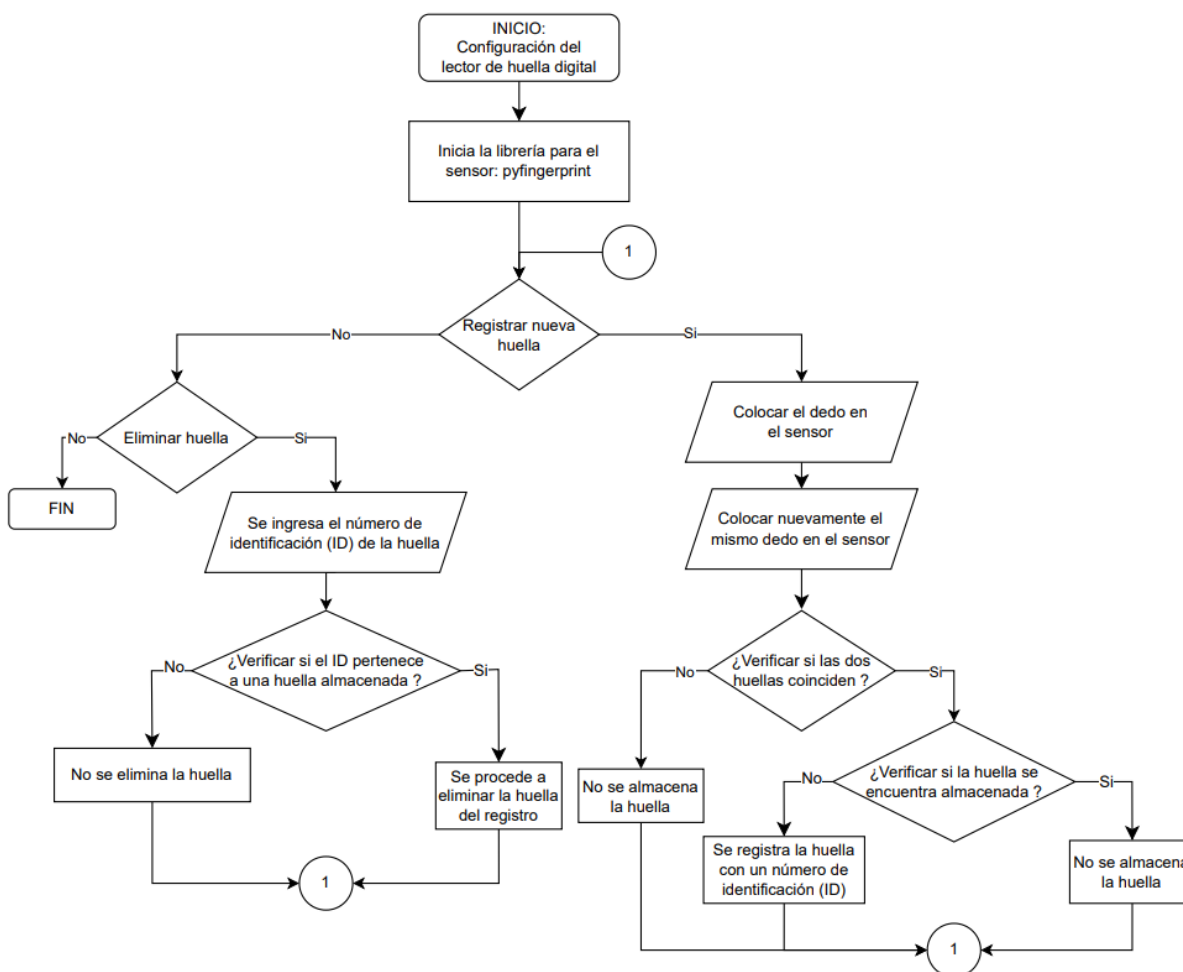
Se conecta el módulo USB-TTL a uno de los puertos USB de la LattePanda. Se usa el módulo porque el sensor es alimentado por 5 V y los TXD/RXD solo tienen un nivel lógico de 3,3 V. Por lo tanto, si se realiza una conexión directa con la LattePanda podría dañarse sus pines.

## Configuración del lector de huella digital

En el diagrama secuencial de la figura 49 se indica de forma resumida la configuración del sensor de huellas dactilares para el registro de una nueva huella o la eliminación de ésta.

**Figura 49**

*Diagrama secuencial de configuración del sensor de huella digital*



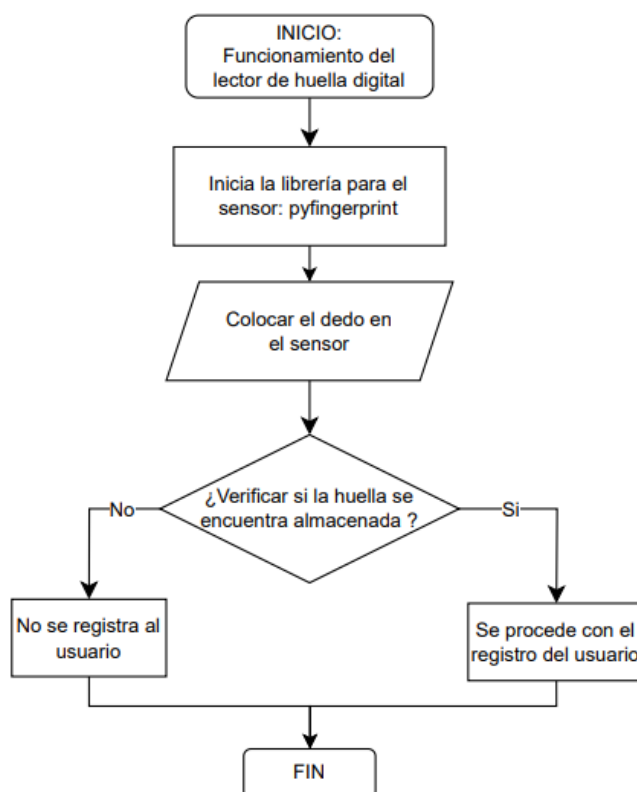
## Funcionamiento del lector de huella digital

El sensor de huella digital funciona capturando la imagen de la huella dactilar de un usuario y comparándola con una base de datos de huellas dactilares previamente almacenadas. Cuando un usuario toca el sensor con su dedo, las características únicas de su

huella son registradas y comparadas con las huellas previamente almacenadas. Si la huella capturada coincide con una de las almacenadas, el sistema registra el acceso.

### Figura 50

*Diagrama secuencial del funcionamiento de la huella digital*



### Implementación del subsistema de la base de datos

Para la creación de la base de datos local se utiliza el software libre y de código abierto HeidiSQL que permite acceder a servidores MySQL, MariaDB, Percona Server, entre otros. El software cuenta con un sistema de sesiones para gestionar el trabajo. Cuando se inicia el programa, se tiene que configurar la sesión:

- Tipo de red: MariaDB or MySQL (TCP/IP)
- Nombre del host:127.0.0.1
- Usuario: root (predeterminada por defecto en MariaDB).

- Contraseña: Se coloca la contraseña de la base de datos.
- Puerto: 3306
- Base de datos: Se eligen las bases de datos.

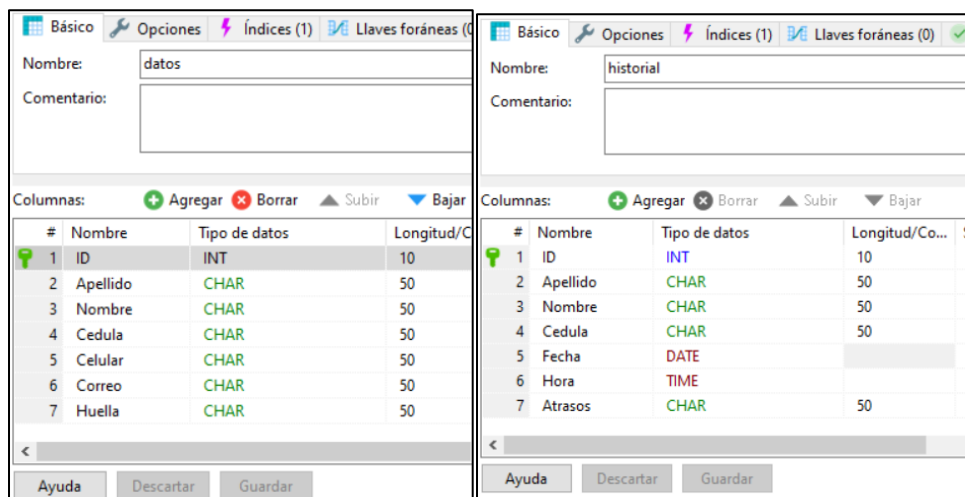
Para la creación de una base de datos local en HeidiSQL, se requiere la realización del siguiente procedimiento:

1. Acceder a la sesión de HeidiSQL y hacer clic derecho sobre el nombre de la sesión.
2. Seleccionar la opción "Crear Nuevo" y posteriormente "Base de Datos".
3. En la ventana emergente, ingresar el nombre deseado para la base de datos, en este caso "registro", y presionar "Aceptar".
4. Hacer clic derecho sobre la base de datos recién creada y seleccionar la opción "Crear Nuevo" y luego "Tabla".
5. Especificar un nombre para la tabla y presionar "Agregar" para crear los campos correspondientes.
6. Para cada campo, ingresar un nombre y especificar sus propiedades.
7. Guardar los cambios mediante la opción "Guardar".

Es importante destacar que este procedimiento debe ser realizado con precaución para garantizar la integridad de la base de datos y evitar errores en el registro de información.

**Figura 51**

Creación de las tablas en la base de datos local en HeidiSQL



### Subsistema de base de datos de acceso remoto

Para crear una base de datos de conexión remota se utiliza el servicio web gratuito de FreeSQLdatabase, se debe ingresar con una cuenta o registrarse para poder acceder a los servicios de alojamiento de base de datos MySQL.

Al momento de registrarse solo se debe colocar únicamente un correo electrónico, la cual va a estar enlazado con la cuenta. Para completar el registro se debe ir al correo y seleccionar el enlace para verificar la cuenta. Una vez verificada la cuenta, se obtendrán los detalles de la base de datos creada en FreeSQLdatabase como se muestra en la figura 52.

**Figura 52**

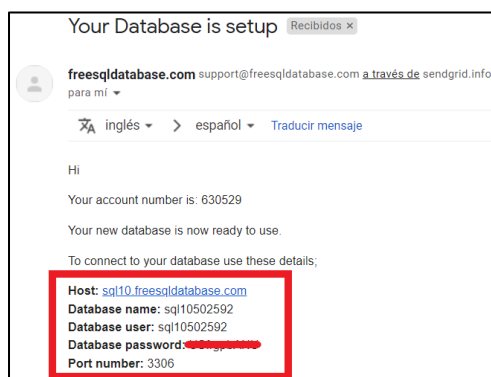
Detalles de la base de datos creada en FreeSQLdatabase

Database Details						
Database Host	Database Name	Database Username	Database Password	Size	Status	Delete
sql10.freesqldatabase.com	sql10502592	sql10502592	Check your emails	0.00MB	Live	<input type="checkbox"/>

La contraseña para acceder a la base de datos se enviará al correo con todos los parámetros previamente mencionados.

### Figura 53

#### *Información de acceso para la base de datos remota*



Se verifica la base de datos en el gestor local de MySQL, se puede utilizar el software previamente visto HeidiSQL. Se debe añadir una nueva sesión en el administrador de sesiones y se introducirán todos los parámetros de acceso que ofrece FreeSQLdatabase. Una vez dentro de la base de datos, se debe crear la tabla de registro y configurar las propiedades de cada variable.

Para poder acceder a la base de datos creada remotamente, se tiene que dirigir a la página web de phpMyAdmin, que ofrece un servicio gratuito para administrar la base de datos, permite crear, editar y eliminar tablas, realizar copias de seguridad e importar datos. Se ingresa a través del enlace: <http://www.phpmyadmin.co>. Una vez dentro se coloca el servidor Host, el usuario y la contraseña de la base de datos. Finalmente, se podrá apreciar la tabla con los parámetros previamente establecidos en HeidiSQL.



Figura 54

Base de datos en phpMyAdmin

ID	Apellido	Nombre	Cedula	Fecha	Hora	Atrasos
11	Silva	Josue	1805352349	2022-07-02	00:23:49	6
12	Silva	Josue	1805352349	2022-07-02	13:38:37	6
13	Silva	Josue	1805352349	2022-07-02	13:39:31	6
14	Silva	Josue	1805352349	2022-07-02	13:40:11	6
18	Silva	Josue	1805352349	2023-01-25	12:04:33	3
19	Silva	Josue	1805352349	2023-01-25	12:04:55	3
20	Silva	Josue	1805352349	2023-01-25	13:00:16	3
21	Silva	Josue	1805352349	2023-01-25	13:00:16	3
22	Silva	Josue	1805352349	2023-01-25	13:18:47	3
23	Silva	Josue	1805352349	2023-01-25	13:23:27	3
24	Silva	Josue	1805352349	2023-01-25	13:24:19	3
25	Silva	Josue	1805352349	2023-01-25	13:30:06	3
26	Martinez	Marcos	1805205554	2023-01-25	20:06:33	0
27	Martinez	Marcos	1805205554	2023-01-25	20:07:25	1
28	Cisneros	Luis	1804359550	2023-01-25	20:16:54	2
29	Silva	Maria	1804914685	2023-01-25	20:17:48	2
30	Silva	Maria	1804914685	2023-01-25	20:29:13	2
31	Martinez	Marcos	1805205554	2023-01-25	20:38:58	1
32	Silva	Josue	1805352349	2023-01-26	11:42:40	4
33	Silva	Josue	1805352349	2023-01-26	11:44:25	4
34	Silva	Josue	1805352349	2023-01-26	11:46:13	4
35	Silva	Josue	1805352349	2023-01-26	11:50:48	4
36	Martinez	Marcos	1805205554	2023-01-26	20:50:07	2

### Conexión entre la aplicación en Python a las bases de datos

Para tener acceso a la base de datos desde Python es necesario instalar una de las bibliotecas que lo permiten, para la aplicación se instaló el módulo `mysql-connector-python`, después se debe crear una instancia de conexión `mysql.connector` con los parámetros de cada base de datos:

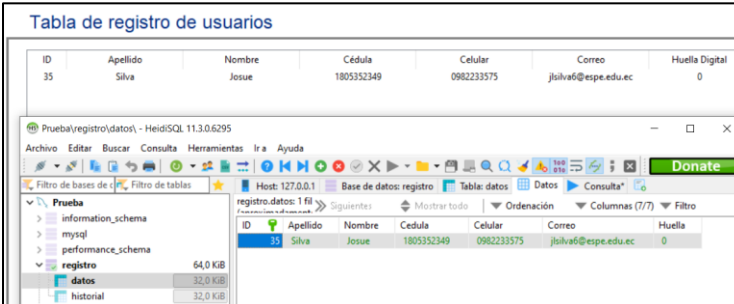
- `host`: Nombre del host
- `user`: Usuario
- `passwd`: Contraseña
- `db`: Nombre de la base de datos

Se requiere aplicar un lenguaje de manipulación de datos (DML), que les permite a los usuarios realizar tareas de consulta o gestión de datos. El dialecto que se aplicará es SQL para poder recuperar o manipular las bases de datos. Sus principales sentencias utilizadas son:

- SELECT \* FROM: Obtener información desde la base de datos.
- INSERT INTO: Insertar información dentro de las tablas.
- DELETE FROM: Eliminar información de la base de datos.
- UPDATE: Si es necesario realizar algún cambio en los datos.

**Figura 55**

*Conexión establecida entre Python y la base de datos HeidiSQL*



ID	Apellido	Nombre	Cédula	Celular	Correo	Huella Digital
35	Silva	Josue	1805352349	0982233575	jsilva6@espe.edu.ec	0

### Implementación del subsistema de notificación por correo electrónico

Para mandar un correo electrónico desde Python, se necesita instalar la librería `smtplib` y `email.message`. El módulo de Python `smtplib` utiliza el protocolo SMTP (Protocolo simple de transferencia de correo) para enviar correos electrónicos. Y el módulo `email.message` se maneja para ajustar la estructura del correo electrónico como el asunto, dirección y el contenido del correo (Rubio, 2021).

Se debe crear un objeto de la clase `EmailMessage()` que almacenará los detalles del mensaje de correo electrónico. Donde se podrá especificar el asunto, la dirección de correo del remitente y receptor, asimismo el contenido del mensaje que contendrá un mensaje de texto sin formato.

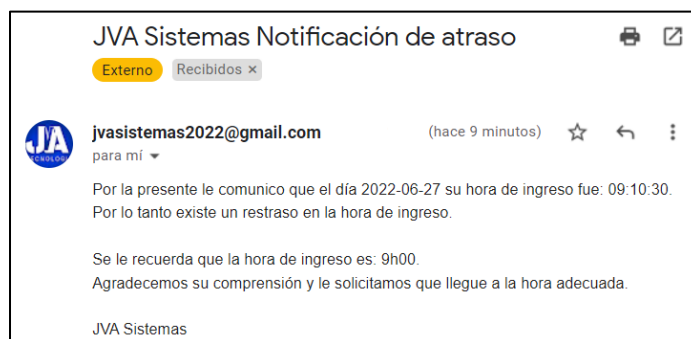
La configuración del servidor de correo electrónico se utiliza para enviar y recibir correos electrónicos. La cual maneja el protocolo SMTP para poder enviar dichos correos a otros servidores. En la aplicación se utilizará el servidor de Gmail, dicho servidor de correo es

smtp.gmail.com. De forma preestablecida, Gmail niega el acceso a clientes de terceros desconocidos que ingresan a su cuenta, por lo cual en la cuenta se debe habilitar la configuración de acceso a aplicaciones menos seguras.

Otro ajuste en el servidor SMTP es el puerto de correo que la aplicación utilizará para enviar el correo electrónico a otros servidores. El puerto predeterminado es el SMTP 587 que utiliza el cifrado TLS para garantizar que se entregue de forma segura el correo electrónico. Después de esto, se lleva a cabo el envío del correo electrónico usando send\_message con el objeto que previamente ha sido configurado con todos los parámetros del mensaje.

## Figura 56

*Notificación de atraso por correo electrónico*



## Implementación del subsistema de generación de reporte

La generación de reporte se lo hará en formato de salida .xlsx ya que la empresa JVA Tecnología se encuentra más familiarizada con Excel. Esto asegurará un mayor manejo del personal técnico para la organización y la consolidación de los datos, así como para una futura representación gráfica y tablas dinámicas. Se plantean realizar tres reportes:

- Reporte de usuarios
- Reporte de historial de registro
- Planilla de Asistencia


### Reporte de usuarios

Es el reporte detallado y actualizado de todos los empleados registrados en el sistema, independientemente de cuál sea su función de usuario. Los campos que poseen son:

- ID: Es el número que da la base de datos al empleado para identificarlo.
- Información del empleado: Se presentan los datos personales del empleado, como: apellido, nombre, cédula, celular, dirección de correo electrónico.
- Huella Digital: Se indica la posición de almacenamiento de la huella digital en el sensor de huellas dactilares.

### Figura 57

#### Reporte de usuarios

	A	B	C	D	E	F	G	
1	 <b>JVA Sistemas</b>							
2	<b>Reporte de Usuarios</b>							
3								
4	<b>Fecha de reporte:</b>	2023-01-29						
5	<b>Hora de reporte:</b>	22:47:15						
6								
7	<b>ID</b>	<b>Apellido</b>	<b>Nombre</b>	<b>Cédula</b>	<b>Celular</b>	<b>Correo</b>	<b>Huella</b>	
8	19	Silva	Josue	1805352349	0956435643	jjsilva6@espe.edu.ec	1	
9	22	Martinez	Marcos	1805205554	0999001718	marcos_77silva@hotmail.com	3	
10	23	Solis	Frank	1805341615	0956453474	neosilva31@gmail.com	4	
11	24	Jurado	Paula	1850458785	0983052558	abigailsy2003@hotmail.com	5	
12	25	Cisneros	Luis	1804359550	0995303404	luisicis316@gmail.com	2	
13	26	Mera	Andres	1850775378	0996459063	jvasistemas@hotmail.com	6	

### Historial de registro

Es el reporte de cada registro que se va concatenando en el sistema y ofrece una información sensible sobre el acceso del personal. Sus parámetros que posee son:

- ID: Es el número que da la base de datos al empleado para identificarlo.
- Información del empleado: Se presentan los datos personales del empleado, los cuales son: apellido, nombre y cédula.
- Fecha: Indica la fecha de registro.

- Hora: Indica la hora que se realizó el registro.
- Atrasos: Indica el número de atrasos que tiene el usuario.

**Figura 58***Reporte de historial de registro*

	A	B	C	D	E	F	G
1	 <b>JVA Sistemas</b>						
2	<b>Reporte de historial de registro</b>						
3							
4	<b>Fecha de reporte:</b>		2023-01-29				
5	<b>Hora de reporte:</b>		22:47:15				
6							
7	<b>ID</b>	<b>Apellido</b>	<b>Nombre</b>	<b>Cédula</b>	<b>Fecha</b>	<b>Hora</b>	<b>Atrasos</b>
8	1	Silva	Josue	1805352349	2023-01-23	13:53:11	0
9	2	Silva	Josue	1805352349	2023-01-23	13:56:05	1
10	3	Silva	Josue	1805352349	2023-01-23	13:56:50	1
11	4	Silva	Josue	1805352349	2023-01-24	17:47:38	2
12	5	Silva	Maria	1804914685	2023-01-24	18:23:29	0
13	6	Mera	Andres	1850775378	2023-01-24	18:26:45	0
14	7	Cisneros	Luis	1804359550	2023-01-24	18:26:52	0
15	8	Cisneros	Luis	1804359550	2023-01-24	18:26:58	1
16	9	Cisneros	Luis	1804359550	2023-01-24	18:29:10	1
17	10	Mera	Andres	1850775378	2023-01-24	18:29:16	1
18	11	Mera	Andres	1850775378	2023-01-24	18:29:48	1
19	12	Cisneros	Luis	1804359550	2023-01-24	18:29:52	1
20	13	Mera	Andres	1850775378	2023-01-24	18:30:02	1
21	14	Mera	Andres	1850775378	2023-01-24	18:30:06	1
22	15	Mera	Andres	1850775378	2023-01-24	18:30:36	1

***Planilla de Asistencia***


Es el reporte general del cálculo de horas trabajadas y se opta por crear un sólo reporte para todos los empleados. Los campos que posee el informe de Planilla de Asistencia son:

- Fecha de registro: Fecha en el que se realizó la carga del cómputo.
- Datos del empleado: Indica la información del usuario.
- Horario de inicio-salida: Para un evento con horario establecido se indican los umbrales de tiempo asignados.
- Jornada Laboral: Se indican los registros de ingreso, descanso y salida.
- Tiempos calculados: Se exhiben los tiempos obtenidos calculados durante el día, excluyendo las salidas designadas especialmente. A continuación, se brinda el detalle de cada valor:
  - Tiempo asignado: Las horas designadas para cada día, ya sea para horarios regulares o para turnos flexibles.

- Tiempo de jornada: Es el tiempo durante el cual el empleado se encontraba en su puesto de trabajo.
- Tiempo de ausencia por el descanso: Es el tiempo excedido por el empleado entre la entrada y salida del descanso.
- Salida temprana: Es el tiempo que el empleado salió más temprano que la hora de salida específica.

**Figura 59**

*Planilla de Asistencia*

 <b>JVA Sistemas</b> <b>Planilla de Asistencia</b>														
Fecha de reporte:		2023-01-29												
Hora de reporte:		22:47:16												
Fecha	Empleado			Horario		Jornada			Tiempos Calculados					
	Apellido	Nombre	Cédula	Entrada	Salida	Entrada	Descanso	Salida	Asign.	Jornada	Atraso	Descanso	Salida Tem.	
Lun 2023-01-23	Silva	Josue	1805352349	09:00:00	18:00:00	13:56:05	None	None	08:00:00	--	--	--	--	
Mar 2023-01-24	Silva	Josue	1805352349	09:00:00	18:00:00	17:47:38	18:37:07	18:39:31	08:00:00	00:49:56	08:47:38	00:02:24	00:00:00	
Mar 2023-01-24	Cisneros	Luis	1804359550	09:00:00	18:00:00	18:26:58	18:29:10	18:29:52	08:00:00	00:19:44	9:26:58	00:00:42	00:00:00	
Mar 2023-01-24	Mera	Andres	1850775378	09:00:00	18:00:00	18:29:16	18:29:48	18:30:02	08:00:00	00:00:36	9:29:16	00:00:14	00:00:00	
Mar 2023-01-24	Carrera	Pedro	1801199215	09:00:00	18:00:00	18:46:21	None	None	08:00:00	--	--	--	--	
Mar 2023-01-24	Freire	Josue	1804964920	09:00:00	18:00:00	18:50:55	18:52:32	18:57:35	08:00:00	00:01:44	9:50:55	00:05:03	00:00:00	
Mar 2023-01-24	Silva	Maria	1804914685	09:00:00	18:00:00	18:54:31	18:54:46	18:55:04	08:00:00	00:00:43	9:54:31	00:00:18	00:00:00	
Mie 2023-01-25	Silva	Josue	1805352349	09:00:00	18:00:00	13:18:47	13:23:27	13:24:19	08:00:00	00:10:27	04:18:47	00:00:52	04:31:54	
Mie 2023-01-25	Martínez	Marcos	1805205554	09:00:00	18:00:00	20:07:25	20:38:58	None	08:00:00	--	--	--	--	
Mie 2023-01-25	Cisneros	Luis	1804359550	09:00:00	18:00:00	20:16:54	None	None	08:00:00	--	--	--	--	
Mie 2023-01-25	Silva	Maria	1804914685	09:00:00	18:00:00	20:17:48	20:29:13	None	08:00:00	--	--	--	--	
Jue 2023-01-26	Silva	Josue	1805352349	09:00:00	18:00:00	11:42:40	11:44:25	11:46:13	08:00:00	00:06:20	02:42:40	00:01:48	06:11:12	
Jue 2023-01-26	Silva	Maria	18049685	09:00:00	18:00:00	13:47:01	None	None	08:00:00	--	--	--	--	
Jue 2023-01-26	Martínez	Marcos	1805205554	09:00:00	18:00:00	19:59:53	20:10:38	20:11:39	08:00:00	00:49:13	10:59:53	00:01:01	00:00:00	
Jue 2023-01-26	Solis	Frank	1805341615	09:00:00	18:00:00	20:36:03	None	None	08:00:00	--	--	--	--	
Sab 2023-01-28	Silva	Josue	1805352349	09:00:00	18:00:00	8:21:31	8:22:02	8:34:08	08:00:00	02:56:49	00:00:00	00:12:06	06:31:34	
Sab 2023-01-28	Mera	Andres	1850775378	09:00:00	18:00:00	11:31:35	13:34:53	13:57:09	08:00:00	--	--	00:22:16	--	
Sab 2023-01-28	Cisneros	Luis	1804359550	09:00:00	18:00:00	13:35:17	13:55:50	13:56:52	08:00:00	--	--	00:01:02	--	

**Envío de reporte por correo electrónico**

El reporte generado será enviado a la dirección de correo electrónico de la compañía, para tener una copia de los datos y poder acceder a ellos en cualquier momento o desde cualquier dispositivo cuando sea necesario. La accesibilidad del reporte es fundamental ya que proporciona un acceso equitativo a la información obtenida del prototipo.

## Figura 60

*Envío del reporte generado por correo electrónico*



## Diseño de la interfaz de usuario

El sistema presentado cuenta con un HMI (Human Machine Interface) diseñado para mejorar la interacción y la eficiencia en la gestión de registros de personal. Este HMI ofrece una serie de funcionalidades clave para la administración de usuarios, incluyendo la adición y eliminación de usuarios, la visualización de los registros y la generación de informes. Con este HMI se brinda una interfaz de usuario amigable e intuitiva, que permite a los usuarios realizar estas tareas de manera eficaz y sin la necesidad de tener conocimientos técnicos previos. De esta manera, se asegura una gestión eficiente y confiable de los registros de personal, garantizando la integridad de los datos.

Según la norma ISO 9241 “Requisitos ergonómicos para trabajos con pantallas de visualización de datos”, se diseñó la interfaz de usuario garantizando una lectura cómoda, segura y eficiente para desempeñar las tareas y sobre todo fácil de aprender a utilizar.

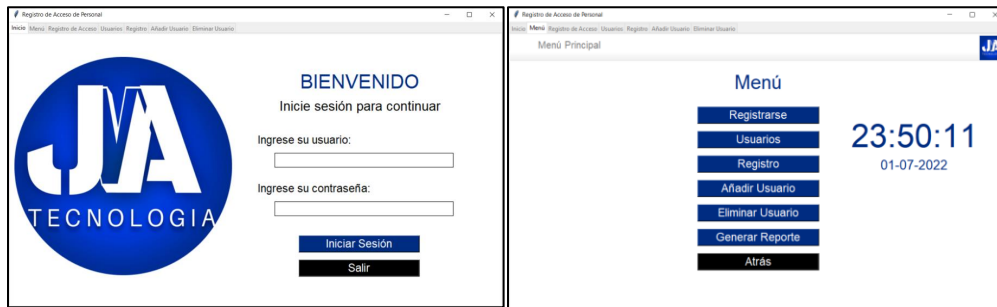
- Se recomienda máximo 3 fuentes de letra, en la interfaz se utilizó la fuente Arial.
- Se recomienda máximo 3 tamaños de letra, en la interfaz se utilizó: 18 para títulos y 15 para cuerpo.

- Se recomienda utilizar colores acromáticos y colores oscuros neutrales.
- Uso de colores 4 o 5 mínimo y máximo 11.

En la figura 61, se muestra la interfaz de usuario.

## Figura 61

### Interfaz de Usuario

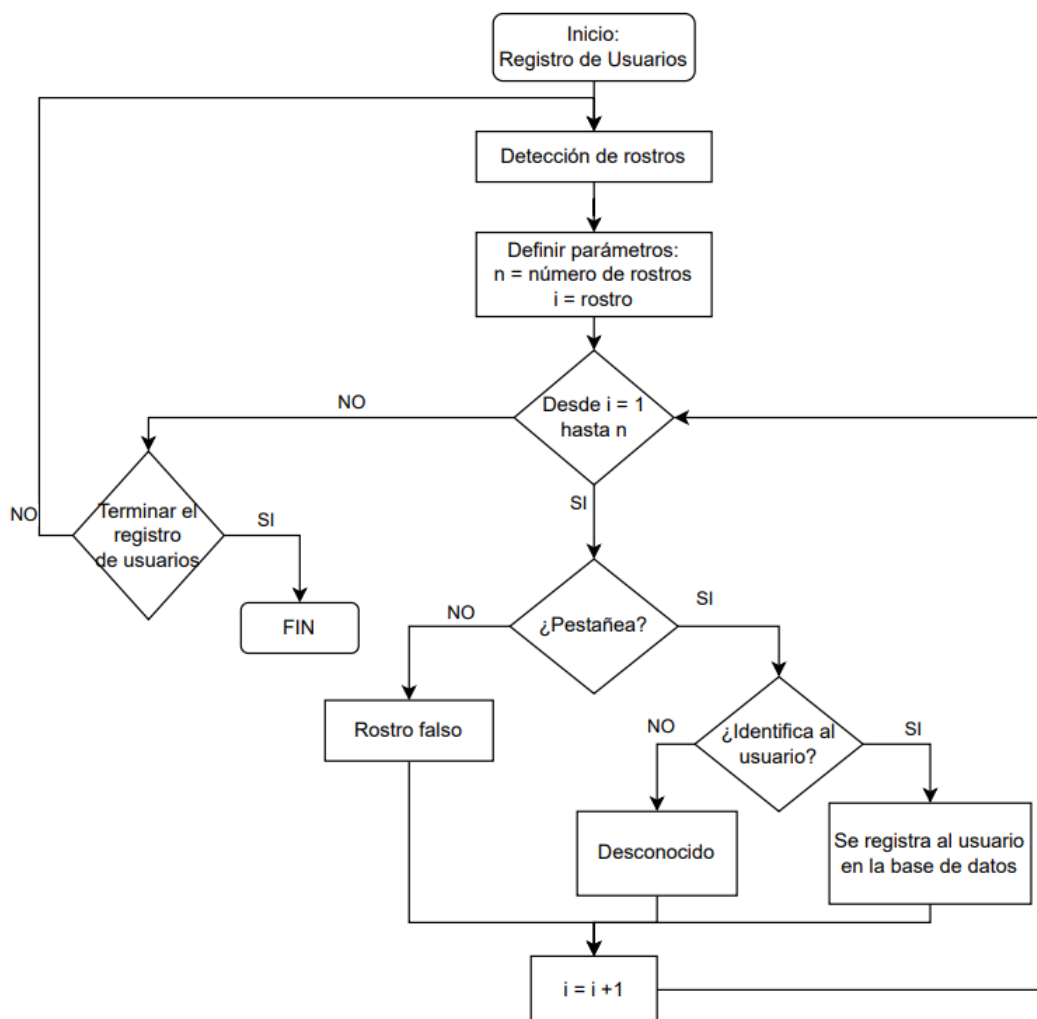


El diagrama secuencial ilustra el proceso de registro de usuarios por reconocimiento facial en el prototipo, presentado de manera simplificada.



Figura 62

Diagrama secuencial de registro de usuario



## Capítulo IV:

### Pruebas de funcionamiento y análisis de resultados

En el presente capítulo se presenta un análisis del procesamiento del sistema biométrico, pruebas de la interfaz de usuario y pruebas de funcionamiento del prototipo, además, para validar la hipótesis planteada, se analiza el tiempo requerido para generar reportes de asistencia en la empresa de forma automática con el prototipo y de forma manual con una persona.

#### Análisis del funcionamiento del sistema biométrico

Para analizar el funcionamiento del sistema biométrico implementado se realizaron 11 intentos de prueba a 15 personas distintas para el reconocimiento facial y el registro dactilar.

#### Figura 63

*Autenticación por registro facial y registro dactilar*



En la tabla 16 se muestra un promedio del tiempo que tarda en realizar el registro facial y registro dactilar por persona, además se calcula la confiabilidad y asertividad del sistema en cada una de las pruebas.

- Promedio de registro facial: Es el promedio del tiempo de las 11 iteraciones realizadas para el registro facial por la persona.

- Confiabilidad registro facial: Es el porcentaje en las que el sistema de reconocimiento facial ha funcionado correctamente durante los 11 intentos realizados por la persona.
- Promedio de registro dactilar: Es el promedio del tiempo de las 11 iteraciones realizadas para el registro dactilar por la persona.
- Confiabilidad registro dactilar: Es el porcentaje en las que el registro dactilar ha funcionado correctamente durante los 11 intentos realizados por la persona.

**Tabla 16***Promedio tiempo de procesamiento*

<b>Persona</b>	<b>Promedio de registro facial (segundos)</b>	<b>Confiabilidad registro facial</b>	<b>Promedio de registro dactilar (segundos)</b>	<b>Confiabilidad registro dactilar</b>
<b>1</b>	5,40	0,91	3,96	0,91
<b>2</b>	5,07	0,91	3,83	0,82
<b>3</b>	5,69	0,73	4,50	0,82
<b>4</b>	4,75	0,82	4,62	1,00
<b>5</b>	5,45	0,73	3,98	0,91
<b>6</b>	6,10	0,82	4,02	0,91
<b>7</b>	6,36	0,91	4,19	0,91
<b>8</b>	5,82	0,82	4,26	0,91
<b>9</b>	4,91	0,82	4,07	0,82
<b>10</b>	4,69	1,00	4,51	0,82
<b>11</b>	5,42	0,73	4,20	0,91
<b>12</b>	5,92	0,82	4,19	0,82
<b>13</b>	5,19	0,82	3,94	0,91
<b>14</b>	5,24	0,82	4,07	0,91
<b>15</b>	4,32	1,00	4,07	0,91
<b>Promedio</b>	5,36	0,84	4,16	0,88

*Nota.* En el Anexo B-01 se encuentra el resultado de las 11 pruebas realizados a 15 personas.

El promedio del registro mediante reconocimiento facial es 5.36 segundos, siendo mínimo de 4.62 segundos y el máximo de 6.36 segundos con un asertividad del 84%, mientras

que el registro mediante huella dactilar es de 4.16 segundos con una efectividad del 88%. Esto es bueno ya que el promedio del tiempo de registro de forma manual es de 20 segundos.

### Pruebas de funcionamiento de la interfaz del usuario

El proceso de autenticación y de registros realizado por el prototipo es controlado por una interfaz de usuario, la cual permite realizar ciertos procesos como se describe a continuación:

1. Inicio: Permite iniciar sesión y ser capaz de modificar ciertos parámetros dentro de la base de datos.

### Figura 64

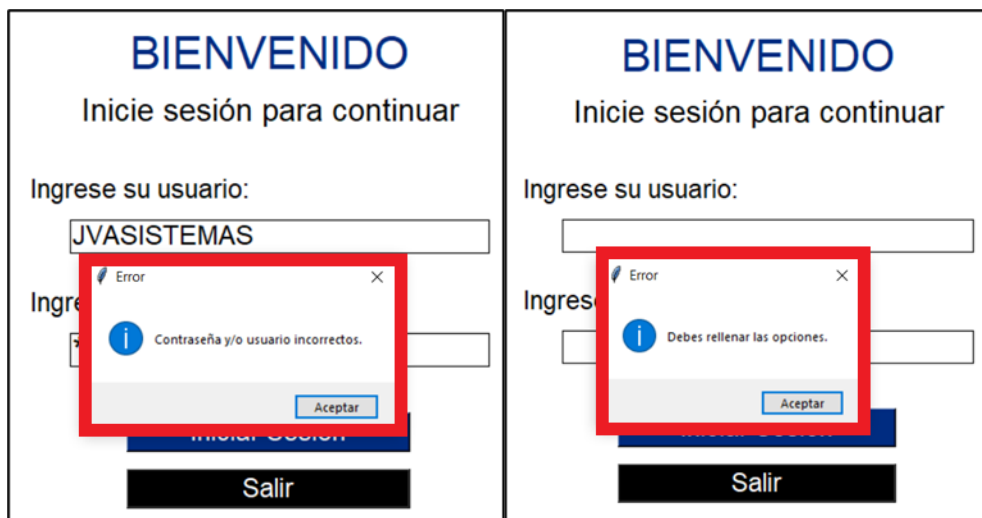
*Ventana 1 para iniciar sesión*



En la figura 65, aparece un cuadro de diálogo que muestra si existe un error en el ingreso de contraseña o usuario, mientras que, en la parte derecha si los campos de usuario o contraseña se encuentran vacíos el sistema muestra otro error.

**Figura 65**

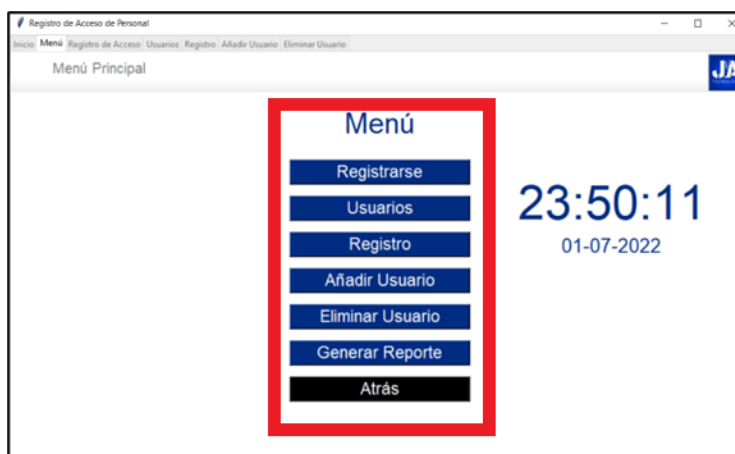
*Mensajes de error al inicio de sesión*



2. Menú de opciones: permite al usuario desplazarse a través de sus diferentes opciones: Registrarse, Usuarios, Registro, Añadir usuario, Eliminar usuario y Generación de reporte.

**Figura 66**

*Ventana 2 del menú de opciones*



3. Tabla de registro de usuarios: permite visualizar los datos personales del usuario como su ID del sistema, nombre, apellido, cédula, celular, correo y la posición de almacenamiento de la huella digital.

**Figura 67**

*Ventana 4 con la tabla de registro de usuarios*

The screenshot shows a web application window titled 'Registro de Acceso de Personal'. The main content area is titled 'Usuarios' and contains a table labeled 'Tabla de registro de usuarios'. The table has 7 columns: ID, Apellido, Nombre, Cédula, Celular, Correo, and Huella Digital. There are 8 rows of data. Below the table is a blue button labeled 'Atrás'.

ID	Apellido	Nombre	Cédula	Celular	Correo	Huella Digital
1	Silva	Josue	180532349	0987654321	jhsilva@espe.edu.ec	1
6	Mera	Andres	1850775378	0996459063	jvasistema@hotmail.com	2
7	Freire	Josue	1804964920	0960895922	jotzue.phreire@gmail.com	3
8	Cineros	Luis	1804399550	0995303404	luis316@gmail.com	4
9	Camera	Pedro	1801199215	0995629511	pedrocamera1905@gmail.c	5
10	Silva	Maria	1804914685	0960901782	torc_mry1997@vodafone.co	6
15	Martinez	Marcos	1805205554	0999001718	marcos_775hva@hotmail.c	7
17	Jurado	Paula	1850458785	0983052558	abigaly2003@hotmail.cor	9
18	Solis	Frank	1805041615	0956453234	neosiva31@gmail.com	8

4. Tabla de registro de historial: permite visualizar el historial de todos los usuarios con su respectivo ID del sistema, nombre, apellido, fecha de registro, hora de registro y atrasos hasta ese momento.

**Figura 68**

*Ventana 5 con la tabla de registro de historial*

The screenshot shows a web application window titled 'Registro de Acceso de Personal'. The main content area is titled 'Historial de usuarios' and contains a table labeled 'Tabla de registro de historial'. The table has 7 columns: ID, Apellido, Nombre, Cédula, Fecha, Hora, and Atrasos. There are 14 rows of data. Below the table is a blue button labeled 'Atrás'.

ID	Apellido	Nombre	Cédula	Fecha	Hora	Atrasos
40	Freire	Josue	1804964920	2023-01-24	18:58:02	1
41	Silva	Maria	1804914685	2023-01-24	18:59:04	1
42	Silva	Maria	1804914685	2023-01-24	18:59:18	1
43	Silva	Maria	1804914685	2023-01-24	18:59:38	1
44	Silva	Maria	1804914685	2023-01-24	18:59:48	1
45	Silva	Josue	180532349	2023-01-24	19:00:33	2
46	Cineros	Luis	1804399550	2023-01-24	19:01:49	1
47	Cineros	Luis	1804399550	2023-01-24	19:02:09	1
48	Mera	Andres	1850775378	2023-01-24	19:03:15	1
49	Mera	Andres	1850775378	2023-01-24	19:03:34	1
50	Silva	Josue	180532349	2023-01-24	19:03:55	2
51	Freire	Josue	1804964920	2023-01-24	19:06:30	1
52	Cineros	Luis	1804399550	2023-01-24	19:06:56	1
53	Freire	Josue	1804964920	2023-01-24	19:07:10	1
54	Cineros	Luis	1804399550	2023-01-24	19:07:25	1

## Registro de usuarios

**Registro facial.** Permite al usuario ingresar su registro por medio de reconocimiento facial ya sea en la hora de ingreso, inicio de la hora del almuerzo, fin de la hora del almuerzo y hora de salida.

### Figura 69

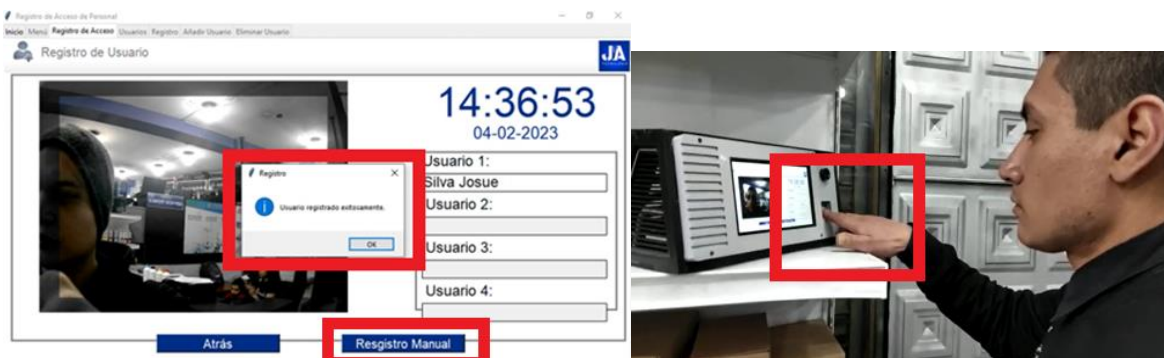
*Ventana 3 para el registro de ingreso*



**Registro manual por huella digital.** En el registro manual por medio del sensor de huellas dactilares se muestra el mensaje de aviso que se registró exitosamente al empleado.

### Figura 70

*Mensaje de aviso de registro de usuario por huella digital*



## Configuración

**Añadir usuario.** Admite añadir un nuevo usuario con sus datos personales, huella digital y malla facial a la base de datos.

### Figura 71

*Ventana 6 para añadir usuario*



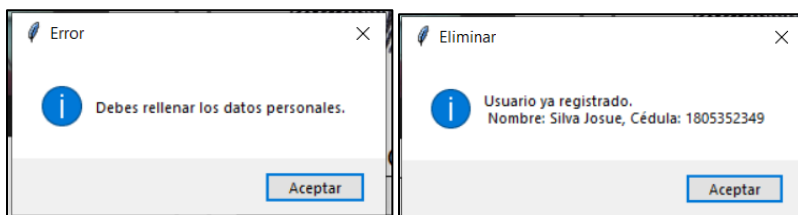
El tiempo promedio que se demora una persona en registrar sus datos correctamente es de 3 minutos, ya que se debe verificar que el nuevo usuario no se encuentre registrado en el sistema, el tiempo de obtención de imágenes del rostro y el tiempo de colocar correctamente la huella digital en el sensor.

En la figura 72, se muestran las notificaciones de advertencias si se produce algún error al añadir el usuario.



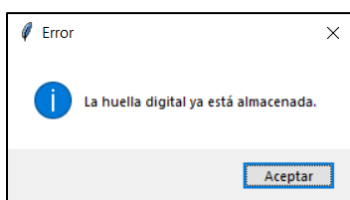
Figura 72

Mensaje de error al añadir un nuevo usuario



a)

b)



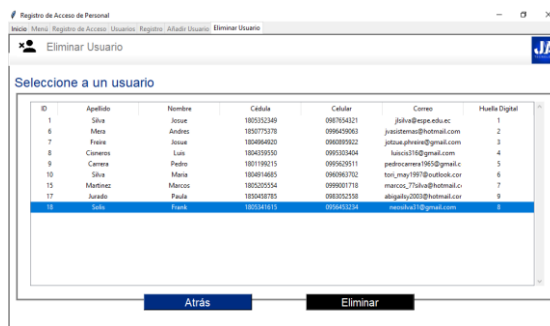
c)

*Nota.* a) Se muestra un aviso si se deja alguna opción en blanco. b) se muestra un aviso si se repite algún usuario que ya se encuentra registrado. c) se indica un aviso cuando ya se encuentra la huella digital almacenada en el sistema.

**Eliminar usuario.** Permite borrar todos los datos relacionados al usuario.

Figura 73

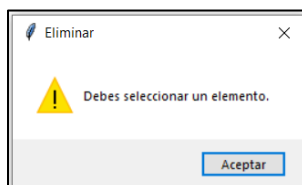
Ventana 7 para eliminar un usuario



En la ventana de eliminar usuario se presenta un mensaje de error si no se ha seleccionado algún usuario.

### Figura 74

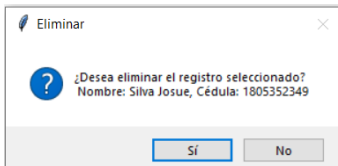
*Mensaje de error al no seleccionar un usuario para eliminar*



En la ventana de eliminar usuario, antes de eliminar al usuario se presenta una ventana de confirmación para eliminarlo.

### Figura 75

*Mensaje de confirmación para eliminar usuario*

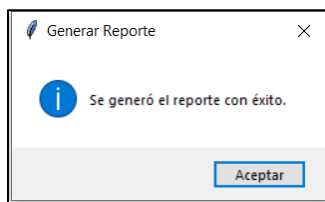


### Reporte

Cuando se seleccione la generación de reporte, se mostrará una ventana de aviso de que se ha generado el reporte exitosamente.

### Figura 76

*Mensaje de aviso de generación de reporte*



## Pruebas de funcionamiento

En este apartado se presentan las pruebas de funcionamiento que permiten demostrar la eficiencia y seguridad del reconocimiento facial. Para ello se propuso ocho posibles escenarios en las que el prototipo trabajaría, cabe recalcar que, los seis primeros escenarios tuvieron las mismas condiciones de iluminación lo que facilita la comparación entre escenarios.

### Primer escenario

En el primer escenario el prototipo debe reconocer solamente a un rostro conocido. Se ejecutó 5 pruebas a 4 personas distintas.

- Personas: número de personas.
- Prueba: número de iteración.
- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar al usuario.

## Figura 77

*Prototipo evaluado con un solo rostro*



**Tabla 17***Datos recogidos del primer escenario*

Personas	Prueba	Rostro 1: Persona		Tiempo de registro
		Identifica	No identifica	
<b>Persona 1</b>	1	1		6,49
	2	1		4,91
	3	1		5,32
	4	1		3,69
	5	1		6,47
<b>Persona 2</b>	1	1		4,81
	2	1		3,65
	3	1		5,23
	4	1		8,37
	5		1	5,47
<b>Persona 3</b>	1	1		4,98
	2	1		5,45
	3	1		3,85
	4	1		5,25
	5	1		5,45
<b>Persona 4</b>	1	1		4,75
	2	1		4,62
	3	1		5,21
	4		1	6,85
	5	1		5,65

Se obtiene que el promedio del tiempo de registro es de 5,32 segundos, con una asertividad cercano del 90%, en los casos que ha fallado se debe a que la persona se ubicaba un poco más alejado del área de reconocimiento.

### **Segundo escenario**

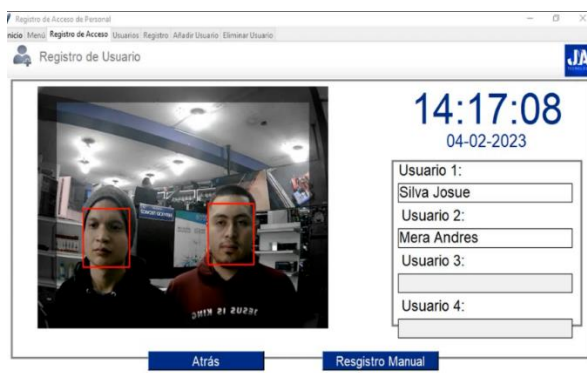
Para el segundo escenario se consideró que el prototipo trabajaría con dos rostros conocidos. Se ejecutó 5 pruebas de grupos de 2 personas.

- Grupo: número de grupo para las pruebas.
- Prueba: número de iteración.

- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar a los usuarios.

**Figura 78**

*Prototipo evaluado con dos rostros*

**Tabla 18**

*Datos recogidos del segundo escenario*

Grupos	Prueba	Rostro 1: Persona		Rostro 2: Persona		Tiempo de registro
		Identifica	No identifica	Identifica	No identifica	
Grupo 1	1	1		1		6,20
	2	1		1		6,35
	3	1			1	6,78
	4		1	1		6,01
	5	1		1		6,84
Grupo 2	1		1	1		7,02
	2	1		1		6,32
	3	1		1		6,45
	4	1			1	6,97
	5	1		1		5,96
Grupo 3	1	1		1		5,99
	2		1	1		6,56
	3	1			1	6,98
	4	1		1		6,01
	5	1		1		6,10
Grupo 4	1	1			1	7,01
	2	1		1		6,32
	3	1		1		6,87
	4		1	1		7,13
	5	1		1		6,74

Se obtiene que el promedio del tiempo de registro es de 6,53 segundos por las dos personas, con una asertividad del 80% para el individuo 1 y el individuo 2, en los casos que ha fallado se debe a cambios de intensidad de luz.

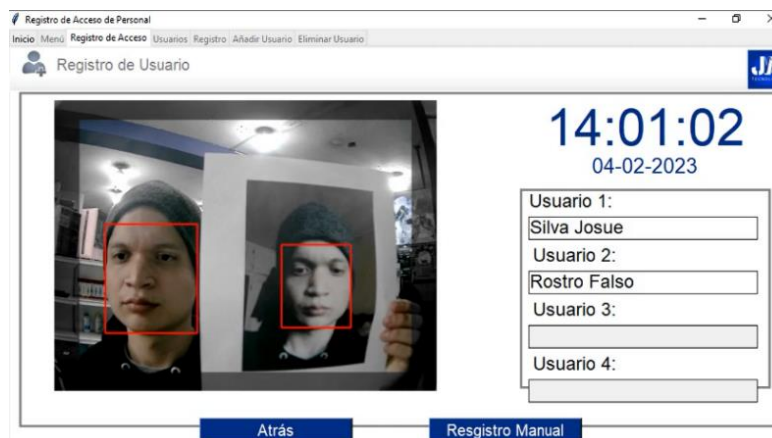
### ***Tercer escenario***

Para el tercer escenario el prototipo trabajó con un rostro conocido y una foto. Se ejecutó 5 pruebas a 4 personas con una fotografía.

- Grupo: número de grupo para las pruebas.
- Prueba: número de iteración.
- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar al usuario.

### **Figura 79**

*Prototipo evaluado con un rostro y una foto*



**Tabla 19***Datos recogidos del tercer escenario*

Personas	Prueba	Rostro 1: Persona		Rostro 2: Foto		Tiempo de registro
		Reconoce	No reconoce	Identifica	No identifica	
Persona 1	1	1			1	5,88
	2	1			1	6,46
	3	1			1	5,98
	4		1		1	7,69
	5	1			1	6,69
Persona 2	1	1			1	5,96
	2	1			1	6,52
	3	1			1	6,97
	4		1		1	7,58
	5	1			1	5,57
Persona 3	1	1			1	7,98
	2		1		1	7,02
	3	1			1	5,03
	4	1			1	5,65
	5	1			1	6,21
Persona 4	1	1			1	6,35
	2	1			1	5,48
	3	1			1	7,09
	4		1		1	6,54
	5	1			1	5,91

En el tercer escenario se calcula un tiempo de registro promedio de 6,43 segundos para ambos rostros, con una asertividad del 80% para persona conocida y un 100% no identifica la fotografía.

#### **Cuarto escenario**

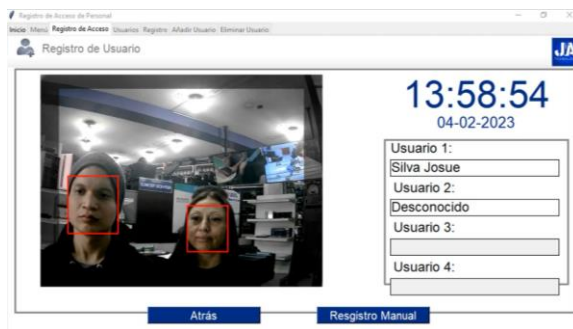
En el cuarto escenario se realiza pruebas con una persona conocida y una persona desconocida. Se ejecutó 5 pruebas a grupos de 2 personas, un total de 4 grupos.

- Grupo: número de grupo para las pruebas.
- Prueba: número de iteración.

- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar al usuario.

**Figura 80**

*Prototipo evaluado con un rostro conocido y un rostro desconocido*

**Tabla 20**

*Datos obtenidos del cuarto escenario*

Grupos	Pruebas	Rostro 1: Persona		Rostro 2: Persona (Desconocido)		Tiempo de registro
		Identifica	No Identifica	Identifica	No Identifica	
Grupo 1	1	1			1	5,12
	2		1		1	7,51
	3	1			1	5,64
	4	1		1		7,64
	5	1			1	5,36
Grupo 2	1	1			1	5,37
	2	1			1	6,02
	3	1			1	5,97
	4	1			1	6,32
	5	1			1	5,49
Grupo 3	1	1			1	6,04
	2	1			1	6,75
	3	1		1		7,83
	4	1			1	5,68
	5		1		1	6,15
Grupo 4	1	1			1	5,02
	2	1		1		7,45
	3	1			1	6,35
	4	1			1	6,14
	5	1			1	5,94



Para el cuarto escenario se calcula un tiempo de registro promedio de 6,19 segundos para las dos personas, con una asertividad del 90% para el rostro conocido y un 85% de asertividad que no identifica al rostro desconocido. En los casos que ha fallado se debe por cambios en la iluminación.

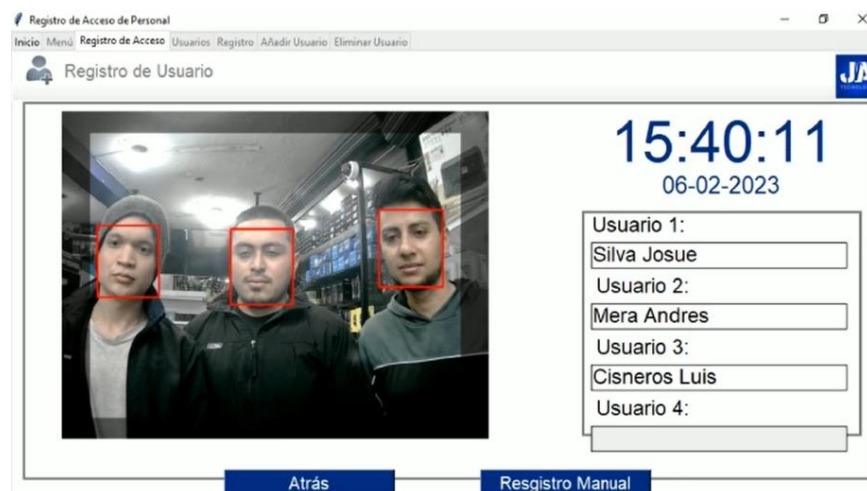
### **Quinto escenario**

En el quinto escenario se trabajó con tres rostros conocidos. Se efectuó 5 pruebas de grupos de 3 personas, un total de 4 grupos.

- Grupo: número de grupo para las pruebas.
- Prueba: número de iteración.
- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar al usuario.

### **Figura 81**

*Prototipo evaluado con tres rostros conocidos*



**Tabla 21***Datos recogidos del quinto escenario*

Grupos	Pruebas	Rostro 1: Persona		Rostro 2: Persona		Rostro 3: Persona		Tiempo de registro
		Identifica	No identifica	Identifica	No Identifica	Identifica	No Identifica	
<b>Grupo 1</b>	1	1		1		1		9,54
	2	1		1		1		9,68
	3		1	1		1		11,65
	4	1			1	1		10,95
	5	1		1		1		10,58
<b>Grupo 2</b>	1		1	1		1		10,65
	2	1		1			1	11,54
	3	1			1	1		11,96
	4	1		1			1	9,99
	5		1	1		1		10,07
<b>Grupo 3</b>	1	1		1			1	11,85
	2	1		1		1		9,32
	3	1			1	1		10,03
	4	1		1			1	11,78
	5		1	1			1	11,68
<b>Grupo 4</b>	1	1			1		1	9,98
	2		1	1		1		11,84
	3	1		1		1		9,048
	4	1		1		1		10,98
	5	1		1		1		10,68

Para este escenario se calcula un tiempo de registro promedio de 10,69 segundos para los tres rostros, con una asertividad del 75% para el primer individuo y un 80% para el segundo individuo y un 70% para el tercer individuo. En los casos que ha fallado se debe a que los rostros se encuentran un poco alejados del área de reconocimiento, por lo tanto, no obtiene los datos suficientes para identificar a la persona.

### **Sexto escenario**

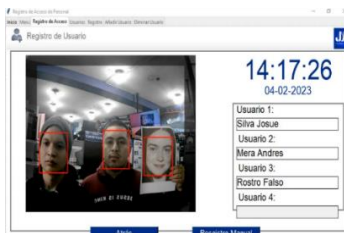
En el sexto escenario se realizó pruebas con tres rostros, dos conocidos y una foto. Se ejecutó 5 pruebas a grupos de dos personas con una foto, un total de 4 grupos.

- Grupo: número de grupo para las pruebas.

- Prueba: número de iteración.
- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar al usuario.

**Figura 82**

*Prototipo evaluando dos rostros conocidos y un rostro falso*

**Tabla 22**

*Datos recogidos del sexto escenario*

Grupos	Pruebas	Rostro 1: Persona		Rostro 2: Persona		Rostro 3: Foto		Tiempo de registro
		Identifica	No identifica	Identifica	No identifica	Identifica	No identifica	
<b>Grupo 1</b>	1		1	1			1	9,89
	2	1		1			1	9,05
	3	1			1		1	10,01
	4		1	1			1	11,08
	5	1		1		1		11,91
<b>Grupo 2</b>	1		1	1			1	9,51
	2	1			1	1		11,95
	3	1		1			1	9,68
	4	1			1		1	10,56
	5	1		1		1		11,63
<b>Grupo 3</b>	1	1		1			1	10,64
	2		1	1			1	9,84
	3	1			1		1	11,01
	4	1		1			1	10,35
	5	1		1			1	10,68
<b>Grupo 4</b>	1	1			1		1	9,63
	2	1		1			1	9,45
	3	1		1			1	9,31
	4	1		1			1	11,67
	5	1		1			1	9,32

En el sexto escenario se obtiene un tiempo de registro promedio de 10,36 segundos para los tres rostros, con una asertividad del 80% para el primer individuo, un 75% para el segundo y un 85% que no identifica a la foto. En los caos que ha fallado en las personas se debe a cambios de intensidad de luz, y que el rostro se encontraba alejado del área de reconocimiento. En el caso de la fotografía las fallas se deben a que se intentó manipular la foto para que detectara el pestañeo el sistema.

### ***Séptimo escenario***

Se plantea colocar una luminaria para comprobar cómo responde el sistema para el sétimo y octavo escenario.

### **Figura 83**

#### *Prueba con iluminaria*

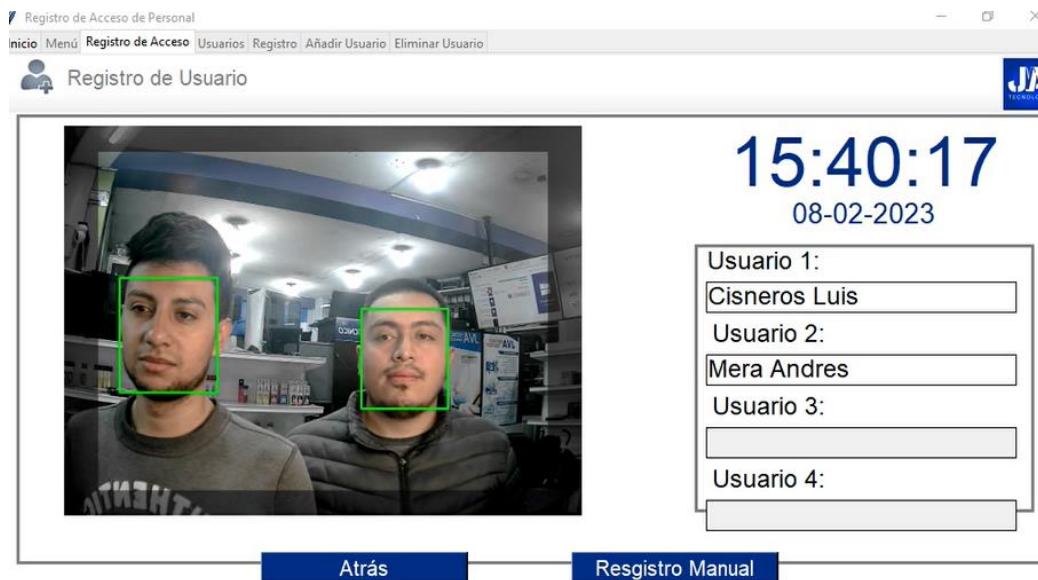


En el séptimo escenario se realizó pruebas con unos dos rostros conocidos. Se ejecutó 5 pruebas a dos personas, en total dos grupos.

- Grupo: número de grupo para las pruebas.
- Prueba: número de iteración.
- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar al usuario.

**Figura 84**

*Prototipo evaluado con dos rostros con mejor iluminación*

**Tabla 23**

*Datos recogidos del séptimo escenario*

Grupos	Prueba	Rostro 1: Persona		Rostro 2: Persona		Tiempo de registro
		Identifica	No identifica	Identifica	No identifica	
<b>Grupo 1</b>	1	1			1	5,37
	2	1		1		6,35
	3	1		1		5,95
	4	1		1		5,76
	5	1		1		6,87
<b>Grupo 2</b>	1	1		1		7,02
	2	1			1	6,19
	3	1		1		6,45
	4	1		1		6,91
	5	1		1		7,08

En el séptimo escenario se obtiene un tiempo de registro promedio de 6,395 segundos para las dos personas, con una asertividad del 100% para el primer individuo, un 80% para el

segundo individuo. El fallo se debe a que los rostros se encuentran alejados del área de reconocimiento para la identificación facial.

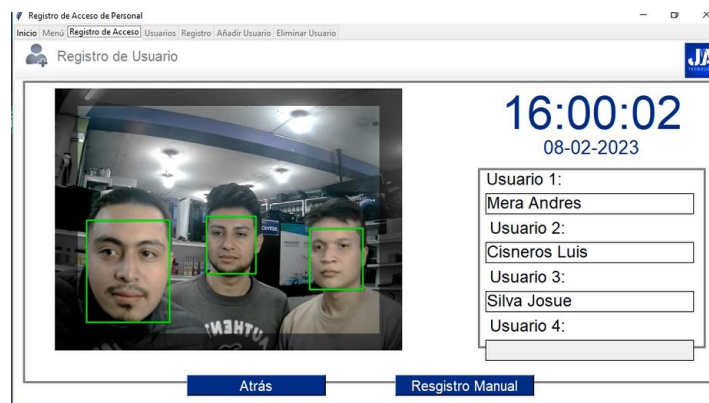
### **Octavo escenario**

En el octavo escenario se realizó pruebas con unos tres rostros conocidos. Se ejecutó 5 pruebas a tres personas, en total dos grupos.

- Grupo: número de grupo para las pruebas.
- Prueba: número de iteración.
- Rostro: si se le identifica o no al usuario.
- Tiempo de registro: es el tiempo que se toma en el registrar al usuario.

### **Figura 85**

*Prototipo evaluado con tres rostros con mejor iluminación*



**Tabla 24***Datos recogidos del octavo escenario*

Grupos	Pruebas	Rostro 1: Persona		Rostro 2: Persona		Rostro 3: Persona		Tiempo de registro
		Identifica	No identifica	Identifica	No Identifica	Identifica	No Identifica	
<b>Grupo 1</b>	1	1		1		1		12,56
	2		1	1			1	10,96
	3	1		1		1		10,33
	4	1			1	1		11,34
	5	1		1		1		9,22
<b>Grupo 2</b>	1	1			1	1		12,05
	2	1		1		1		10,86
	3	1		1		1		11,31
	4	1		1			1	10,42
	5		1	1		1		10,81

En el octavo escenario se obtiene un tiempo de registro promedio de 10,986 segundos para los tres rostros, con una asertividad del 80% para el primer individuo, un 80% para el segundo y un 80% para el tercero. El fallo se debe a que los rostros se encuentran alejados del área de reconocimiento para la identificación facial.

Los datos recopilados en los distintos escenarios son presentados en la siguiente tabla 23. Donde el tiempo: es el tiempo promedio en segundos del registro total por cada prueba. Tiempo por rostro: es el tiempo promedio que se lleva a cada rostro. Asertividad: es el porcentaje de identificación correcta para los rostros conocidos. Foto: es el porcentaje de que no identifica a la fotografía. Desconocido: es el porcentaje que no identifica al usuario desconocido.

**Tabla 25***Datos recopilados*

Escenario / Parámetros	Tiempo (s)	Tiempo por rostro (s)	Asertividad Rostro 1 Conocido (%)	Asertividad Rostro 2 Conocido (%)	Asertividad Rostro 3 Conocido (%)	Foto no identifica (%)	Desconocido no identifica (%)
Primer Escenario	5,32	5,32	0,9	-	-	-	-
Segundo Escenario	6,53	3,27	0,8	0,8	-	-	-
Tercer Escenario	6,43	3,22	0,8	-	-	1	-
Cuarto Escenario	6,19	3,10	0,9	-	-	-	0,85
Quinto Escenario	10,69	3,56	0,75	0,8	0,7	-	-
Sexto Escenario	10,36	3,45	0,8	0,75	-	0,85	-
Séptimo Escenario	6,39	3,19	1	0,8	-	-	-
Octavo Escenario	10,98	3,66	0,8	0,8	0,8	-	-

En cualquier escenario la asertividad para reconocer un rostro falso o desconocido es superior al 85%. Mientras más personas existan dentro de la etapa de reconocimiento, menos asertividad tiene el sistema de reconocimiento facial, por este motivo, la validación de hipótesis debe ser realizada con un solo rostro ya que tiene un asertividad del 90%.

**Tabla 26***Porcentaje de promedio de efectividad de las pruebas*

Número de rostros	% efectividad
1	0,9
2	0,8
3	0,75
2 (con luz)	0,9
3 (con luz)	0,8

Teniendo en cuenta la tabla 26 es importante destacar que la iluminación juega un papel crucial en el reconocimiento facial. Cuanto mejor sea la iluminación, más precisos serán los resultados del reconocimiento. Con una iluminación adecuada, el sistema de



reconocimiento facial puede capturar claramente las características faciales, lo que permite una identificación más precisa y efectiva.

### Validación de hipótesis

Para medir la mejora en los registros, se registró y midió el tiempo (segundos) que las personas a través de la forma manual y forma automática se demoran en generar los registros y seguimientos en las actividades de los trabajadores dentro de la empresa.

**Forma Manual:** Una persona es encargada de registrar y generar registros de los trabajadores.

**Forma Automática:** El prototipo es encargado de realizar los registros de los trabajadores.

Además, se toma en cuenta un factor adicional llamado “sanción”, se añade este factor dentro de los datos siempre y cuando el sistema de reconocimiento facial o dactilar no reconozca a la primera iteración. El factor sanción es igual a 3 debido a que el usuario tendrá que repetir esta acción por segunda iteración y un máximo de tercera iteración.

### Tabla 27

*Ejemplo para el factor sanción*

Tiempo (segundos)	Validación	Tiempo total
$t_{registro} \textit{ Facial} = 6.49$	Si	$t_{registro} \textit{ Facial} = 6.49$
$t_{registro} \textit{ Dactilar} = 5.84$	No	$t_{registro} \textit{ Dactilar} * Sanción = 17.52$

En la tabla 28, se muestran los datos recogidos del prototipo durante la autenticación de 25 muestras en un periodo de tres días a los trabajadores, pero analizados de uno en uno.

**Tabla 28***Datos recogidos del prototipo*

#	Registro facial (s)	Reconoce	Tiempo(s) total con sanción	#	Registro huella (s)	Reconoce	Tiempo(s) total con sanción	Tiempo(s) del sistema biométrico + Reportes
<b>1</b>	6,49	Si	6,49	<b>1</b>	5,84	No	17,52	<b>23,36</b>
<b>2</b>	4,91	Si	4,91	<b>2</b>	4,26	Si	4,26	<b>8,52</b>
<b>3</b>	5,32	Si	5,32	<b>3</b>	4,41	Si	4,41	<b>8,82</b>
<b>4</b>	3,69	Si	3,69	<b>4</b>	3,50	Si	3,5	<b>7,00</b>
<b>5</b>	6,47	Si	6,47	<b>5</b>	2,59	Si	2,59	<b>5,18</b>
<b>6</b>	4,81	Si	4,81	<b>6</b>	3,54	Si	3,54	<b>7,08</b>
<b>7</b>	3,65	Si	3,65	<b>7</b>	3,39	Si	3,39	<b>6,78</b>
<b>8</b>	5,23	Si	5,23	<b>8</b>	5,26	Si	5,26	<b>10,52</b>
<b>9</b>	8,37	Si	8,37	<b>9</b>	6,89	Si	6,89	<b>13,78</b>
<b>10</b>	5,47	Si	5,47	<b>10</b>	3,04	No	9,12	<b>12,16</b>
<b>11</b>	4,98	No	14,94	<b>11</b>	4,20	Si	4,2	<b>8,40</b>
<b>12</b>	5,45	Si	5,45	<b>12</b>	3,89	Si	3,89	<b>7,78</b>
<b>13</b>	3,85	Si	3,85	<b>13</b>	4,52	Si	4,52	<b>9,04</b>
<b>14</b>	5,25	Si	5,25	<b>14</b>	4,10	Si	4,1	<b>8,20</b>
<b>15</b>	5,45	Si	5,45	<b>15</b>	4,20	Si	4,2	<b>8,40</b>
<b>16</b>	4,75	Si	4,75	<b>16</b>	3,50	Si	3,5	<b>7,00</b>
<b>17</b>	4,62	Si	4,62	<b>17</b>	3,65	Si	3,65	<b>7,30</b>
<b>18</b>	5,21	Si	5,21	<b>18</b>	4,10	Si	4,1	<b>8,20</b>
<b>19</b>	6,85	Si	6,85	<b>19</b>	2,98	Si	2,98	<b>5,96</b>
<b>20</b>	5,65	Si	5,65	<b>20</b>	3,56	Si	3,56	<b>7,12</b>
<b>21</b>	6,54	Si	6,54	<b>21</b>	4,22	Si	4,22	<b>8,44</b>
<b>22</b>	5,98	Si	5,98	<b>22</b>	5,02	No	15,06	<b>20,08</b>
<b>23</b>	6,32	Si	6,32	<b>23</b>	3,98	Si	3,98	<b>7,96</b>
<b>24</b>	6,52	Si	6,52	<b>24</b>	3,65	Si	3,65	<b>7,30</b>
<b>25</b>	5,89	Si	5,89	<b>25</b>	2,59	Si	2,59	<b>5,18</b>

En la tabla 28 el tiempo del reconocimiento facial es lo que tarda en detectar y comprobar de que sea un rostro verdadero, si identifica al usuario en menos de tres intentos no se coloca el factor de sanción, caso contrario se coloca el factor de sanción. El tiempo de registro por huella digital es el tiempo que le toma al usuario colocar adecuadamente el dedo en el sensor, si lo identifica menos de tres intentos no se coloca el factor sanción, caso contrario se coloca el factor de sanción. Finalmente se obtiene la el tiempo total que es la suma del registro facial y el registro por huella digital.

En la tabla 29 se muestra el tiempo que los trabajadores tardan en registrar su asistencia o actividades de forma manual, además se incluye el tiempo en el que una persona externa genera los reportes de los trabajadores.

**Tabla 29**

*Datos del tiempo del registro manual*

#	Tiempo Normal(s)	Tiempo de reportes(s)	Tiempo Total(s)
1	17	25	42
2	18	25	43
3	20	32	52
4	16	26	42
5	19	34	53
6	18	28	46
7	20	25	45
8	18	27	45
9	15	32	47
10	15	25	40
11	20	32	52
12	18	29	47
13	20	29	49

#	Tiempo Normal(s)	Tiempo de reportes(s)	Tiempo Total(s)
14	20	30	50
15	17	25	42
16	18	25	43
17	15	31	46
18	17	25	42
19	16	31	47
20	18	27	45
21	20	29	49
22	19	30	49
23	15	28	43
24	18	34	52
25	20	35	55

Con los datos numéricos de la tabla 28, tabla 29 y teniendo en cuenta que son variables cuantitativas y muestras relacionadas o emparejadas, se procede a realizar la validación de hipótesis mediante el método de t - Student, la cual permite apreciar si la hipótesis alternativa o nula son válidas.

### Tabla 30

*Datos para validación de hipótesis*

#	Tiempo Antes (Manual)	Tiempos Después (Automático)
1	42	23,36
2	43	8,52
3	52	8,82
4	42	7
5	53	5,18
6	46	7,08
7	45	6,78

#	Tiempo Antes (Manual)	Tiempos Después (Automático)
8	45	10,52
9	47	13,78
10	40	12,16
11	52	8,4
12	47	7,78
13	49	9,04
14	50	8,2
15	42	8,4
16	43	7
17	46	7,3
18	42	8,2
19	47	5,96
20	45	7,12
21	49	8,44
22	49	20,08
23	43	7,96
24	52	7,3
25	55	5,18

El método T-Student requiere la definición de la hipótesis alternativa y nula, por lo tanto, las hipótesis para la validación del presente proyecto son:

**Hipótesis Nula (Ho)** = El diseño e implementación de un sistema biométrico no mejora la eficiencia en los registros.

**Hipótesis Alternativa (Hi)** = El diseño e implementación de un sistema biométrico mejora la eficiencia en los registros.

Sabiendo que:

$\alpha$  = Nivel de significancia

$n$  = Número de datos.

$S_d$  = Desviación estándar muestral.

$t$  = Estadístico t.

$gl$  = Grados de libertad.

$\bar{d}$  = Promedio de las diferencias

Teniendo en cuenta las siguientes ecuaciones:

$$S_d = \sqrt{\frac{\sum(d_i - \bar{d})^2}{n - 1}} = 6,56$$

$$t = \frac{\bar{d}}{S_d / \sqrt{n}} = \frac{37,45}{\frac{6,56}{\sqrt{25}}} = 28,50$$

$$gl = (n - 1) = 24$$

Se trabajó con un nivel de significancia de 10% equivalente a 0.1, además, teniendo una cantidad de datos igual a 25, se obtiene que el valor crítico de t-student (una cola) es:

$$t_{(1 - \alpha)(n - 1)} = 1,31$$

Debido a que:

$$t > t_{(1 - \alpha)(n - 1)} \quad o \quad 28,50 > 1,31$$

**Tabla 31***Prueba t para medias de dos muestras emparejadas*

	<b>Tiempos Después (Automático)</b>	<b>Tiempo Antes (Manual)</b>
<b>Media</b>	9,1824	46,64
<b>Varianza</b>	18,03301067	16,82333333
<b>Observaciones</b>	25	25
<b>Coefficiente de correlación de Pearson</b>	-0,238212067	
<b>Diferencia hipotética de las medias</b>	0	
<b>Grados de libertad</b>	24	
<b>Estadístico t</b>	-28,5099304	
<b>P(T&lt;=t) una cola</b>	1,46849E-25	
<b>Valor crítico de t (una cola)</b>	1,317835934	
<b>P(T&lt;=t) dos colas</b>	2,93697E-25	
<b>Valor crítico de t (dos colas)</b>	1,71088208	

Se anula la hipótesis nula, de esta manera se valida la hipótesis alternativa, demostrando así que el trabajo realizado si permite cumplir con el objetivo planteado.

## Capítulo V:

### Conclusiones y Recomendaciones

#### Conclusiones

- El método utilizado para el reconocimiento facial fue LBPH. Es un método de extracción de características de imágenes que se basa en la distribución local de patrones binarios en una imagen facial. Este método ha demostrado tener una alta precisión para el reconocimiento de patrones faciales como: nariz, boca, ojos y aspectos relevantes o característicos del rostro.
- El diseño de la estructura mecánica del prototipo de sistema biométrico se realizó con el análisis estático de la estructura de soporte de pantalla, el cual dio resultados favorables en el análisis de deformación en el soporte de pantalla. El valor de deflexión máximo calculado fue de  $-7,854824 * 10^{-6}m$  menor al recomendado  $2.3333 * 10^{-4}m$ . Se puede verificar que la estructura satisface las necesidades del diseño.
- La etapa de procesamiento de imágenes utiliza librerías MediaPipe en combinación con OpenCV las cuales permiten predicciones ligeras y precisas que facilitan crear una área de trabajo válida con alineación del rostro. Todo esto permite entrar a la fase de entrenamiento en donde se aplica el método de reconocimiento de rostro LBPH, proceso que facilita entrenar a la red y hallar el valor de umbral, el cual se puede comparar para aceptar o desechar el reconocimiento.
- La técnica Anti-spoofing que se seleccionó fue la detección de parpadeo ocular en tiempo real, la cual requiere que el usuario realice el movimiento de pestañar frente a la cámara para evitar la suplantación de identidad, autenticar y verificar



al usuario en cuestión de segundos; mediante la base de datos MediaPipe Face Mesh que analiza 468 puntos de referencia faciales en 3D.

- El software para la base de datos que se implementó en la empresa JVA Tecnología se llama HeidiSQL, la cual permite acceder a los servidores locales MySQL y MariaDB. Además, admite ser usada de forma remota mediante el servicio web gratuito de FreeSQLdatabase para poder acceder a los servicios de alojamiento de base de datos MySQL.
- La interfaz gráfica del usuario fue elaborada con tkinter un toolkit de Python, dicha interfaz es de fácil manejo y amigable debido a que el usuario posee varias opciones en su menú principal como: registrarse, usuarios, registro, añadir o eliminar usuario y generar reportes. Además, la interfaz puede desplegar ventanas que indican si el registro fue correcto o no.  
En la etapa de registro el sistema es capaz de enviar un correo electrónico al usuario si existe un retraso en la hora de ingreso, lo cual presenta grandes ventajas para que la persona realice sus registros laborales de forma idónea. La opción de “Generar Reportes” del menú en la interfaz gráfica, puede crear planillas de asistencias, reportes de historial de registro y reportes de usuarios en formato de salida .xlsx o también conocido como Excel, lo que permite mayor eficiencia y eficacia durante el control de registros dentro de la empresa.
- Las pruebas realizadas con el sistema implementado muestran que la fiabilidad y la velocidad del sistema son muy buenas siempre y cuando no existan más de 2 personas en la etapa de reconocimiento. Además, las pruebas muestran que al existir más de tres rostros la asertividad del sistema baja a 70%, mientras que para dos rostros su asertividad es de 80% y para un solo rostro aumenta al 90%. Así también, se obtuvo resultados con una mejor iluminación de un 90% para

dos rostros y 80% para tres rostros. Como dato adicional el prototipo tiene un asertividad mayor de 85% al momento de detectar fotografías o desconocidos en cualquier escenario.

- Para validar la hipótesis se utilizó la prueba t-Student que permite comparar el antes y un después de una muestra, permitiendo conocer si la implementación del prototipo influye en la mejora del registro del personal de la empresa JVA Tecnología. Con un nivel de significancia de 10%, se obtiene: Estadístico  $t >$  Valor crítico o también  $28,50 > 1,31$ . Este resultado acepta la hipótesis alternativa y valida que: El diseño e implementación de un sistema biométrico mejora la eficiencia en los registros.

### **Recomendaciones**

- Es importante recolectar información de fuentes confiables ya que proporcionan la base teórica del diseño e implementación del prototipo del sistema biométrico para mejorar el registro de acceso de personal que utiliza reconocimiento facial, para así obtener conocimiento valioso sobre visión artificial, sus componentes, biometría, lenguajes de programación y Anti-Spoofing, por lo que se recomienda seguir actualizándose sobre este tema.
- Se recomienda estudiar detalladamente los aspectos técnicos de algoritmos, lenguajes de programación, bases de datos y técnicas Anti-Spoofing, ya que esto permitirá lograr un sistema biométrico que sea eficiente con una interfaz intuitiva y accesible para el usuario.
- Se sugiere que el prototipo sea usado individualmente debido a que en las pruebas realizadas con el prototipo el nivel de asertividad disminuye cuando existen más de 3 rostros a un 70%.

- Para que la base de datos funcione remotamente es fundamental crear una base principal que se pueda conectar con servicio web gratuito de FreeSQLdatabase y esta pueda acceder sin ninguna dificultad a los servicios de alojamiento de base de datos MySQL. Sin embargo, se debe tomar en cuenta que las librerías usadas sean compatibles con el hardware y software usado para el prototipo y la ejecución sea correcta.
- Para el uso correcto del prototipo es fundamental tomar en cuenta las condiciones del factor lumínico, debido a que es una variable importante para una correcta ejecución del sistema por lo que se recomienda una iluminación plana del rostro o aquella iluminación que no genere sombras. Además, el usuario se debe registrar sin mascarilla, sin lentes o cualquier objeto que modifique su morfología facial.

### Bibliografía

- Akhtar, Z., Alfarid, N., & Kale, S. (2011). *Face Recognition Systems Under Spoofing Attacks*.  
doi:02.ACE.2011.02.132
- Alvarado, J., & Fernández, J. (2012). Análisis de textura en imágenes a escla de grises, utilizando patrones locales binarios (LBP). *ENGI Revista electrónica de la Facultad de Ingeniería*, 1-6.
- Arguello, H. (2011). Recognition Systems Based on the facial Imagen. *Avances en Sistemas e Informática*, 7-13. Obtenido de [https://www.researchgate.net/publication/267296150\\_Sistemas\\_de\\_reconocimiento\\_basados\\_en\\_la\\_imagen\\_facial\\_Recognition\\_systems\\_based\\_on\\_the\\_facial\\_image](https://www.researchgate.net/publication/267296150_Sistemas_de_reconocimiento_basados_en_la_imagen_facial_Recognition_systems_based_on_the_facial_image)
- Bujarra. (18 de Junio de 2019). *Usando un lector de huellas dactilares en Raspberry Pi*. Obtenido de <https://www.bujarra.com/usando-un-lector-de-huellas-dactilares-en-raspberry-pi/>
- Celma, M., Casamayor, J., & Mota, L. (2003). *Base de Datos*. España: Pearson Education.
- COGNEX. (2018). *Introducción a la Visión Artificial*. Estados Unidos. Obtenido de [https://bcnvision.es/uploads/videotutoriales/uploads/guias%20por%20sectores/introduccion%20a%20la%20vision%20artificial\\_compressed.pdf](https://bcnvision.es/uploads/videotutoriales/uploads/guias%20por%20sectores/introduccion%20a%20la%20vision%20artificial_compressed.pdf)
- Delgado, S. (2022). *Aprende Python*. Obtenido de [https://aprendepython.es/\\_downloads/907b5202c1466977a8d6bd3a2641453f/aprendepython.pdf](https://aprendepython.es/_downloads/907b5202c1466977a8d6bd3a2641453f/aprendepython.pdf)
- Domínguez, A. (1996). *Procesamineto digital de imágenes*. México: Perfiles Educativos.

ELECTROSTORE. (2019). *Lector de huella dactilar biométrico digital FingerPrint Kookye*.

Obtenido de <https://grupoelectrostore.com/shop/placas-para-programacion/raspberry/accesorios-para-raspberry/lector-de-huella-dactilar-biometrico-digital-fingerprint-kookye/>

European Knowledge Center for Information Technology. (2019). *Base de datos*. Recuperado el 21 de 5 de 2022, de <https://www.ticportal.es/glosario-tic/base-datos-database>

García, E. M. (2012). *Visión Artificial* (Primera ed.). España: OPENLIBRA.

Gómez, M. D. (2013). *Base de Datos*. México. Obtenido de [http://www.cua.uam.mx/pdfs/conoce/libroselec/Notas\\_del\\_curso\\_Bases\\_de\\_Datos.pdf](http://www.cua.uam.mx/pdfs/conoce/libroselec/Notas_del_curso_Bases_de_Datos.pdf)

Gottumukkal, R., & Asari, V. (2003). *System level design of real time face recognition architecture based on composite PCA*. AMC.

Gracia, L. (9 de 10 de 2013). *Un poco de java*. Obtenido de <https://unpocodejava.com/2013/10/09/que-es-opencv/>

Granja, I., Moreno, D., Cabrera, F., & Valle, P. (2020). *Image Processing for identification of people as a security system in domiciliary zones*. doi:10.18502/keg.v5i2.6233

Harmouch, M. (5 de Julio de 2020). *Dev Genius*. Obtenido de <https://blog.devgenius.io/face-recognition-based-on-lbph-algorithm-17acd65ca5f7>

HasdZone. (24 de Agosto de 2021). *Análisis: Raspberry Pi 3 Modelo B+*. Obtenido de <https://hardzone.es/reviews/perifericos/analisis-raspberry-pi-3-modelo-b/>

Hernández, R. (2010). *Estudio de Técnicas de Reconocimiento Facial*. Barcelona, España. Obtenido de

[http://upcommons.upc.edu/bitstream/handle/2099.1/9782/PFC\\_RogerGimeno.pdf?sequence=1](http://upcommons.upc.edu/bitstream/handle/2099.1/9782/PFC_RogerGimeno.pdf?sequence=1)

INCIBE. (2016). *Tecnologías biométricas aplicadas a la ciberseguridad*. España. Obtenido de [https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\\_tecnologias\\_biometricas\\_aplicadas\\_ciberseguridad\\_metad.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf)

INEN. (2014). *NTE INEN-ISO 9241-11*. Quito. Obtenido de [https://www.normalizacion.gob.ec/buzon/normas/nte\\_inen\\_iso\\_9241-11.pdf](https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_9241-11.pdf)

Logitech. (2022). *C270 HD Webcam*. Obtenido de <https://www.logitech.com/es-ar/products/webcams/c270-hd-webcam.960-000694.html>

Manuals. (11 de Abril de 2022). *LATTEPANDA LPDF0543 Delta 432 Tiny Ultimate User Manual*. Obtenido de <https://manuals.plus/lattepanda/lpdf0543-delta-432-tiny-ultimate-manual#axzz7VvHvngmD>

MediaPipe. (2020). *MediaPipe Face Detection*. Obtenido de [https://google.github.io/mediapipe/solutions/face\\_detection.html](https://google.github.io/mediapipe/solutions/face_detection.html)

MediaPipe. (2022). *MediaPipe Face Mesh*. Obtenido de [https://google.github.io/mediapipe/solutions/face\\_mesh](https://google.github.io/mediapipe/solutions/face_mesh)

Microsoft. (2022). *Access SQL: conceptos básicos, vocabulario y sintaxis*. Obtenido de <https://support.microsoft.com/es-es/office/access-sql-conceptos-b%C3%A1sicos-vocabulario-y-sintaxis-444d0303-cde1-424e-9a74-e8dc3e460671#:~:text=SQL%20es%20un%20lenguaje%20de%20computaci%C3%B3n%20para%20trabajar%20con%20conjuntos,SQL%20para%20trabajar%20c>

Mott, R. L. (2009). *Resistencia de Materiales* (Quinta ed.). México: PEARSON EDUCACIÓN.

- Muñoz Vega, E. P. (2021). *Desarrollo de un sistema de control de acceso de personal empleando reconocimiento facial respaldado con técnicas de aprendizaje profundo*. Latacunga. Obtenido de <http://repositorio.espe.edu.ec/handle/21000/25302>
- Navas, L., & Obando, C. (2021). *Diseño e implementación de un prototipo de sistema de seguridad integral con el fin monitorear el acceso de automóviles, utilizando visión artificial y chatbot para el ingreso al conjunto residencial*. Latacunga. Obtenido de <http://repositorio.espe.edu.ec/handle/21000/25388>
- NOVICOMPU. (s.f.). *Cámara Web HD 480dpi*. Obtenido de [https://www.novicompu.com/camara-web-hd-480dpi-4066/p?idsku=2796&cmp\\_id=13178496464&adg\\_id=124248877404&kwd=&device=c&gclid=Cj0KCQjw-pCVBhCFARIsAGMxhAf8DUAZK5oxwdBf-Do-RI8slHX0iC02lniTrjFD8f-qeMn\\_JWENswIaAq6CEALw\\_wcB](https://www.novicompu.com/camara-web-hd-480dpi-4066/p?idsku=2796&cmp_id=13178496464&adg_id=124248877404&kwd=&device=c&gclid=Cj0KCQjw-pCVBhCFARIsAGMxhAf8DUAZK5oxwdBf-Do-RI8slHX0iC02lniTrjFD8f-qeMn_JWENswIaAq6CEALw_wcB)
- Prensario TI Latin America. (12 de Diciembre de 2021). *VisionPass es destacado en la evaluación antispoofing de iBeta*. Obtenido de <https://prensariotila.com/visionpass-es-destacado-en-la-evaluacion-antispoofing-de-ibeta/>
- Programador Clic. (2020). *Operadores de funciones LBP y HOG*. Obtenido de <https://programmerclick.com/article/31321760626/>
- Python. (2022). Obtenido de <https://www.python.org/>
- QUISH. (2022). *Reconocimiento facial en tiempo real usando Python*. Obtenido de <https://es.quish.tv/real-time-face-recognition-using-python>
- Raschka, S. (2014). *Linear Discriminant Analysis*. Obtenido de [http://sebastianraschka.com/Articles/2014\\_python\\_lda.html](http://sebastianraschka.com/Articles/2014_python_lda.html)

- Raspberry Pi. (15 de Noviembre de 2018). *Raspberry Pi 3 Model A+*. Obtenido de <https://www.raspberrypi.com/news/new-product-raspberry-pi-3-model-a/>
- Rubio, H. (5 de Marzo de 2021). *loop*. Obtenido de Enviando emails con Python. Guía completa.: <https://loopgk.com/2021/03/05/enviando-emails-con-python-guia-completa/>
- Ruiz, M., Rodriguez, J., & Olivares, J. (Septiembre de 2009). Una mirada a la biometría. *Avances en Sistemas e Informática, VI*, 29-33. Obtenido de <https://www.redalyc.org/pdf/1331/133113598005.pdf>
- Sánchez, R., Ávila, C., & Pereda, J. (1999). *Minimal Template Size for Iris-Recognition*. Atlanta, Estados Unidos: BMES/EMBS.
- Serengil, S., & Ozpinar, A. (2020). Deepface. *Innovations in Intelligent Systems and Applications Conference (ASYU)*, 23-27.
- Soukupová, & Čech. (2016). *Real-Time Eye Blink Detection using Facial Landmarks*.
- Suprema ID. (2021). *RealScan-G10*. Obtenido de <https://www.suprema-id.com/es/contents/detail.php?code=020102>
- Tecnopura. (2020). *Tecnopura*. Obtenido de Módulo sensor biométrico / Lector de huella digital ref. FPM10A: <https://www.tecnopura.com/producto/modulo-sensor-biometrico-lector-de-huella-digital-ref-fpm10a/>
- TOMTOP. (2020). *Full HD 1080P Webcam USB Mini Computer Camera*. Obtenido de [https://www.tomtop.com/p-h32504.html#flow\\_qa](https://www.tomtop.com/p-h32504.html#flow_qa)
- Valencia, Á., Maradei, M., & Espinel, F. (2016). Estudio sobre la influencia del diámetro de apertura en la fuerza ejercida por cada dedo. *Revista de Salud Pública*, 5. doi:<http://dx.doi.org/10.15446/rsap.v18n6.50424>



WAVESHARE. (2020). *5inch Capacitive IPS Touch Display*. Obtenido de

<https://www.waveshare.com/5inch-DSI-LCD-B.htm>

WAVESHARE. (2021). *7inch HDMI LCD (B) User Manual*. Obtenido de

[https://www.waveshare.com/w/upload/1/19/7inch\\_HDMI\\_LCD\\_%28B%29\\_User\\_Manual.pdf](https://www.waveshare.com/w/upload/1/19/7inch_HDMI_LCD_%28B%29_User_Manual.pdf)

WAVESHARE. (2021). *7inch HDMI LCD (H) User manual*. Obtenido de

[https://www.waveshare.com/w/upload/5/58/7inch\\_HDMI\\_LCD\\_%28H%29\\_User\\_Manual.pdf](https://www.waveshare.com/w/upload/5/58/7inch_HDMI_LCD_%28H%29_User_Manual.pdf)

ZKTECO. (2020). *Reloj Marcador Biométrico Zkteco MB10 Con Reconocimiento Facial Y*

*Huella Digital - Negro*. Obtenido de <https://nissei.com/py/reloj-marcador-biometrico-zkteco-mb10-con-reconocimiento-facial-y-huella-digital-negro>



---

# ANEXOS

---

