

**INDICE**

<b>AGRADECIMIENTOS:</b> .....	<b>2</b>
<b>INDICE DE FIGURAS</b> .....	<b>8</b>
<b>INTRODUCCION</b> .....	<b>11</b>
<b>ANTECEDENTES</b> .....	<b>11</b>
<b>DESCRIPCION DEL PROBLEMA</b> .....	<b>12</b>
<b>OBJETIVO DE LA INVESTIGACION</b> .....	<b>12</b>
<b>OBJETIVO GENERAL</b> .....	<b>12</b>
<b>OBJETIVO ESPECIFICO</b> .....	<b>13</b>
<b>ALCANCE</b> .....	<b>13</b>
<b>IMPLEMENTACION</b> .....	<b>13</b>
<b>CAPITULO 1: SEGURIDAD INFORMÁTICA</b> .....	<b>15</b>
<b>1.2.TERMINOS RELACIONADOS CON LA SEGURIDAD INFORMATICA</b> .....	<b>16</b>
1.2.1 <i>Confidencialidad, Disponibilidad e Integridad</i> .....	<b>16</b>
1.2.2 <i>Objetivos de la Seguridad Informática</i> .....	<b>17</b>
<b>1.3.Política de Seguridad</b> .....	<b>18</b>
1.3.1 <i>Generalidades</i> .....	<b>18</b>
1.3.2 <i>Definición de Políticas de Seguridad Informática</i> .....	<b>18</b>
1.3.3 <i>Elementos de una Política de Seguridad Informática</i> .....	<b>19</b>
1.3.4 <i>Parámetros para Establecer Políticas de Seguridad</i> .....	<b>20</b>
<b>1.4.Razones que Impiden la Aplicación de las Políticas de Seguridad Informática</b> .....	<b>20</b>
<b>1.5.Normas de las Políticas de Seguridad Informática</b> .....	<b>21</b>
1.6.OTRAS NORMAS Y ESTANDARES.....	<b>23</b>
<b>CAPITULO 2: SEGURIDAD FÍSICA Y LÓGICA</b> .....	<b>26</b>
<b>2.1.Vulnerabilidades de un sistema informático</b> .....	<b>26</b>
2.1.1 <i>Vulnerabilidad: definición y clasificación</i> .....	<b>27</b>
2.1.2 <i>Vulnerabilidades conocidas</i> .....	<b>27</b>
<b>2.2.Identificación de Amenazas potenciales a la Seguridad Física y Lógica</b> .....	<b>28</b>
<b>2.3.ANALISIS DE RIESGOS</b> .....	<b>29</b>
2.3.1 <i>RIESGOS</i> .....	<b>29</b>
2.4. <i>Medidas de Seguridad</i> .....	<b>30</b>
2.4.1 <i>Tipos de Medidas de Seguridad</i> .....	<b>30</b>
<b>2.5.Ciclo de Vida de la Seguridad Informática</b> .....	<b>31</b>
2.5.1 <i>Técnicas para asegurar el sistema</i> .....	<b>31</b>
<b>2.6.Estándar Australiano AS/NZ 4360:1999</b> .....	<b>33</b>
2.6.1 <i>Método lógico y sistemático</i> .....	<b>34</b>
<b>CAPITULO 3:DELITO INFORMATICO</b> .....	<b>35</b>

<b>3.1.DELITO INFORMÁTICO</b> .....	<b>36</b>
<b>3.1.1.Crimenes específicos</b> .....	<b>36</b>
3.1.2.Sabotaje informático .....	36
3.1.3.Piratería informática .....	37
3.1.4.Hackeo.....	37
3.1.5.Crackeo .....	37
3.1.6..DDNS (Denegación de servicios de nombres de dominio) .....	38
3.1.7.Falsificación de documento electrónico.....	38
3.1.8.Cajeros automáticos y tarjetas de crédito .....	38
3.1.9.Robo de identidad.....	38
3.1.10.Phreaking .....	39
3.1.11.Fraudes electrónicos.....	39
3.1.12.Pornografía infantil .....	39
<b>3.2.DELITO INFORMÁTICO EN BOLIVIA.</b> .....	<b>39</b>
<b>3.3.DELITO INFORMÁTICO EN BRASIL “LEI CAROLINA DIECKMANN”</b> .....	<b>41</b>
<b>CAPITULO 4: ASFI</b> .....	<b>42</b>
<b>4.1.¿QUÉ ES ASFI ?</b> .....	<b>43</b>
<b>4.2.¿CUÁLES SON LOS OBJETIVOS DE ASFI?</b> .....	<b>43</b>
<b>4.3.¿CUÁL ES LA MISIÓN Y LA VISIÓN DE ASFI?</b> .....	<b>43</b>
<b>4.4.¿CÓMO REALIZA SU TRABAJO?</b> .....	<b>44</b>
<b>4.5.¿QUÉ CARÁCTER TIENEN LAS NORMAS QUE EMITE ASFI?</b> .....	<b>44</b>
<b>4.6.NUEVA CIRCULAR DE LA ASFI SOBRE SEGURIDAD INFORMÁTICA</b> .....	<b>44</b>
<b>CAPITULO 5: PROPIEDAD INTELECTUAL</b> .....	<b>46</b>
<b>5.1.PROPIEDAD INTELECTUAL</b> .....	<b>47</b>
5.1.1.¿Qué es la propiedad intelectual?.....	47
5.1.2.¿Qué son los derechos de propiedad intelectual? .....	47
<b>5.2.¿Por qué debe promoverse y protegerse la propiedad intelectual?</b> .....	<b>48</b>
<b>5.3.DERECHO DE AUTOR</b> .....	<b>48</b>
<b>5.4.PROPIEDAD INDUSTRIAL</b> .....	<b>49</b>
<b>5.5.¿Qué es la Organización Mundial de la Propiedad Intelectual?</b> .....	<b>49</b>
<b>5.6.SEGURIDAD INFORMATICA Y LA PROPIEDAD INTELECTUAL</b> .....	<b>50</b>
5.6.1.¿Cómo puede afectar la ley? .....	50
5.6.2.¿Cómo te afecta la LPI? Sobre todo en estos 4 puntos clave:.....	51
<b>CAPITULO 6 :SEGURIDAD BIOMÉTRICA</b> .....	<b>55</b>
<b>6.1.BIOMETRÍA</b> .....	<b>56</b>
<b>6.2.SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA</b> .....	<b>57</b>
<b>CAPITULO 7:..SEGURIDAD BIOMÉTRICA FACIAL</b> .....	<b>62</b>
<b>7.1. El presente de la biometría facial</b> .....	<b>63</b>
<b>7.2.Contra criminales</b> .....	<b>63</b>

<b>7.3.Detección y reconocimiento de rostro .....</b>	<b>64</b>
7.3.1Retos de la detección facial .....	64
<b>Figura 7.5 Rostros con diferente expresión.....</b>	<b>66</b>
<b>CAPITULO 8 :Reconocimiento de Patrones .....</b>	<b>68</b>
<b>8.1.Introducción.....</b>	<b>69</b>
<b>8.2.Aprendizaje .....</b>	<b>70</b>
<b>8.3.Enfoques de reconocimiento de patrones .....</b>	<b>70</b>
<b>8.4.Selección de variables.....</b>	<b>71</b>
8.4.1.Algoritmos del reconocimiento facial.....	71
8.4.2.Reducción de dimensionalidad.....	72
<b>8.5.Análisis de componentes principales (ACP).....</b>	<b>72</b>
<b>8.6.Análisis de componentes independientes (ACI) .....</b>	<b>73</b>
<b>8.7.Análisis Discriminatorio Lineal (ADL) .....</b>	<b>73</b>
<b>8.8.Técnicas de grafos: “Elastic Bunch Graph Matching” EBGM .....</b>	<b>74</b>
<b>CAPITULO 9: Reconocimiento Facial 3-D.....</b>	<b>75</b>
<b>9.1.El modelo de “morphing”.....</b>	<b>76</b>
9.1.1.Invariancia a la deformación.....	76
<b>9.2.Enfoque Bayesiano.....</b>	<b>76</b>
<b>9.3.Máquinas de soporte vectorial.....</b>	<b>77</b>
<b>9.4.Redes neuronales .....</b>	<b>77</b>
<b>9.5.Boosting y adaboost .....</b>	<b>78</b>
9.5.1.Marco Teórico de la detección de rostro.....	79
9.5.2.Descripción general .....	80
<b>9.6.Preprocesamiento .....</b>	<b>81</b>
9.6.1.Transformación a nivel de gris .....	81
9.6.2.Escalado por Interpolación .....	82
9.6.3.Ecualización del histograma .....	83
<b>9.7.Detección del Borde mediante el algoritmo de Canny.....</b>	<b>84</b>
9.7.1.Extracción de descriptores.....	85
9.7.2.Block de decisión .....	86
<b>9.9.Imagen Integral .....</b>	<b>89</b>
<b>9.10.Importancia de los descriptores de Harr-Like.....</b>	<b>91</b>
<b>9.10.11.Algoritmos de Aprendizaje .....</b>	<b>92</b>
<b>9.11.Evaluación del rendimiento de sistemas biométricos .....</b>	<b>94</b>
<b>CAPITULO 10 : ANATOMIA FACIAL.....</b>	<b>96</b>
<b>10.1.PARTES DE LA FACE.....</b>	<b>97</b>
<b>10.2.HUESOS DE LA CARA.....</b>	<b>98</b>
<b>10.3.LOS MÚSCULOS DE LA CARA Y CUELLO .....</b>	<b>99</b>
<b>CAPITULO 11 : NORMAS E POLITICAS.....</b>	<b>101</b>

<b>11.1.NORMAS</b> .....	<b>102</b>
11.1.1.ISO/IEC 19794.....	102
<b>11.2. ISO/IEC 27002</b> .....	<b>103</b>
11.2.1.CONTROL DE ACCESO.....	103
<b>11.3.POLITICA APLICADA</b> .....	<b>106</b>
11.3.1.Acceso a las instalaciones utilizando VF300 .....	106
11.3.2.ESPECIFICACIONES DE LA POLITICA APLICADA .....	107
<b>CAPITULO 12 : APLICACIONES COMERCIALES DESARROLLADAS</b> .....	<b>109</b>
<b>12.1.APPS FORNECIDOS DE RECONOCIMIENTO FACIAL</b> .....	<b>110</b>
<b>12.2.CASOS DE IMPLEMENTACIONES DE SISTEMAS DE RECONOCIMIENTO FACIAL</b> .....	<b>111</b>
<b>CAPITULO 13:SISTEMA DE CONTROL DE ACCESO DESARROLLADO COM ZKTECO VF-300</b> .....	<b>113</b>
<b>13.1.VENTAJAS Y DESVENTAJAS</b> .....	<b>114</b>
<b>13.2. ZKTECO Y EL DESARROLLO DE LA BIOMETRIA</b> .....	<b>115</b>
<b>13.3.PATENTE DEL ALGORITMO DE RECONOCIMIENTO FACIAL ZKFACE</b> .....	<b>115</b>
13.3.1.PATENTE DEL SOFTWARE .....	115
13.3.2.PATENTE CHINA ALGORITMO ZKFACE 7.0 .....	116
<b>13.4.AUTENTICACION DE SEGURIDAD</b> .....	<b>117</b>
<b>13.4.1.Autenticación</b> .....	<b>117</b>
13.4.2.AUTENTICACION DE DOBLE FACTOR .....	118
13.4.3.Autenticación de factores múltiples.....	118
<b>13.5.DESARROLLO DEL SISTEMA DE CONTROL DE ACCESO</b> .....	<b>119</b>
13.5.1. PROGRAMA Y LENGUAJE UTILIZADO.....	119
13.5.2. SDK DEL ZKSOFTWARE.....	120
13.5.2. CÓDIGO DEL PROGRAMA .....	121
<b>13.6. ZKTECO VF-300</b> .....	<b>129</b>
<b>13.7.FUNCIONAMIENTO DEL SISTEMA DE "CONTROL DE ACCESO"</b> .....	<b>131</b>
<b>CONCLUSIONES</b> .....	<b>137</b>
<b>RECOMENDACIONES</b> .....	<b>138</b>
<b>BIBLIOGRAFIA</b> .....	<b>138</b>
<b>ANEXOS</b> .....	<b>146</b>