



Universidad Autónoma del Estado de México

Centro Universitario UAEM Zumpango

Ingeniería en Computación

Control de acceso biométrico para empleados del centro especializado de atención primaria a la salud Miguel Ramos Arizpe

Memorias de trabajo

Que para obtener el título de
Ingeniero en Computación

Presenta:

Mauricio Román Ruiz Bárcenas

Asesor:

Ing. Diego Armando Ramírez Avelino

Dedicatoria

Mis más sinceros agradecimientos para mis padres, que siempre me apoyan en todo lo que realizo y gracias al esfuerzo de ellos alcance el grado profesional que hasta hoy tengo.

ÍNDICE

DEDICATORIA	2
ÍNDICE	3
LISTA DE FIGURAS	4
RESÚMEN	5
ABSTRACT	6
DESCRIPCIÓN DEL PROBLEMA	7
OBJETIVO GENERAL	8
OBJETIVOS ESPECÍFICOS	8
CAPÍTULO 1	9
1.1 HISTORIA DE LA BIOMETRÍA	10
1.2 HISTORIA DE LA HUELLA DIGITAL	14
1.3 QUÉ ES UNA HUELLA DIGITAL	19
1.4 ¿QUÉ ES EL RECONOCIMIENTO DE LA HUELLA DIGITAL?	20
1.5 DACTILOSCOPIA	21
1.5.1 LOFOSCOPIA	21
1.5.2 RECONOCIMIENTO DE LA HUELLA DIGITAL	21
1.6 CLASIFICACIÓN DE LOS DACTILOGRAMAS	22
CAPÍTULO 2	24
2.1 SISTEMAS BIOMÉTRICOS	25
2.2 BLOQUES Y ETAPAS DE UN SISTEMA BIOMÉTRICO	26
2.3 CARACTERÍSTICAS DE UN INDICADOR BIOMÉTRICO	27
2.4 ARQUITECTURA DE UN SISTEMA BIOMÉTRICO PARA IDENTIFICACIÓN PERSONAL	28
2.5 FASE OPERACIONAL DE UN SISTEMA DE IDENTIFICACIÓN PERSONAL	30
2.6 SISTEMAS BIOMÉTRICOS ACTUALES	31
2.7 TABLA COMPARATIVA DE SISTEMAS BIOMÉTRICOS	33
2.8 DISPOSITIVO U ARE U DE DIGITALPERSONA.....	34
CAPÍTULO 3	36
3.1 SISTEMA DESARROLLADO EN NETBEANS VERSIÓN 7.2	37
3.2 ALGORITMOS DEL SISTEMA	37
3.3 DIAGRAMA DE FLUJO	39
3.4 DIAGRAMA JERÁRQUICO	40
3.5 BASE DE DATOS.....	40
3.6 INTERFACES DE USUARIO Y DESCRIPCIÓN DEL SISTEMA	41
3.6.1 MÓDULO PRINCIPAL	41
3.6.2 MÓDULO DE REGISTRO.....	43
3.6.3 MÓDULO DE REGISTRO DE ENTRADA.....	44
3.6.4 MÓDULO DE REGISTRO DE SALIDA.....	45

CAPÍTULO 4	46
4.1 REPORTE MEDIANTE RED LOCAL	47
4.2 HTML	47
4.3 PHP	48
4.4 CARACTERÍSTICAS DE XAMPP	50
4.5 CÓDIGO HTML Y PHP	51
4.6 REPORTE POR TRABAJADOR	51
4.7 REPORTE POR RANGO DE FECHAS	52
4.8 COSTO E IMPACTO DE IMPLEMENTACIÓN	52
CAPÍTULO 5	53
5.1 CONCLUSIONES	54
5.2 OBLIGATORIO	55
5.3 RECOMENDACIONES	55
ANEXOS	56
ANEXO 6.1	57
ANEXO 6.2	58
ANEXO 6.3	59
ANEXO 6.4	61
ANEXO 6.5	65
ANEXO 6.6	69
ANEXO 6.7	72
ANEXO 6.8	73
ANEXO 6.9	74
BIBLIOGRAFÍA	79
GLOSARIO	80

Lista de figuras

Figura 2.1	26
Figura 2.2	29
Figura 2.3	34
Figura 2.4	35
Figura 3.1	40
Figura 3.2	42
Figura 3.3	43
Figura 3.4	44
Figura 3.5	45
Figura 4.1	50
Figura 4.2	51

RESÚMEN

Las huellas dactilares son un identificador biométrico ampliamente utilizado. Su uso se extiende desde aplicaciones policiales y forenses hasta aplicaciones civiles muy comunes, como el control de accesos, siendo esto sobre lo que se enfoca el presente trabajo, específicamente en el control de acceso para empleados del centro especializado de atención primaria a la salud, visto desde el punto de medida de seguridad. Con la aparición de los primeros sistemas automáticos de reconocimiento de huellas (AFIS, “Automatic Fingerprint Identification System”) se comenzó el desarrollo y utilización de algoritmos de comparación de huellas dactilares basados en minucias, que son puntos singulares dentro de la huella. Estos métodos se asemejan a la comparación visual realizada por un experto, identificando la posición de los puntos singulares para su posterior comparación.

ABSTRACT

For several years, the need for a unique way to identify humans has led humanity to apply several different methods, ranging from tattooing in its earliest form, to Modern biometric techniques.

Security systems based on biometrics are an effective and efficient for recognition of human beings. Among these, we highlight the face or facial recognition, voice recognition, analysis of the pattern of the iris, fingerprint recognition, analysis of the map of the retina of the eye, body odor analysis ear shape, analyzing the shape of the hand, finger geometry, the head shape, the map analysis hand veins.

This project builds one of the most used biometrics, fingerprint recognition. This system uses a capture device to generate a biometric code, which is programmed in netbeans, which is a very easy and quick to do. The storage system is based in MySQL free tool that allows us to create databases.

DESCRIPCIÓN DEL PROBLEMA

La importancia significativa que representa el cumplimiento por parte del personal respecto a la puntualidad y al respeto por las políticas o normativas establecidas por parte de la organización sobre este tema, implica poseer un método que regule de manera precisa, veraz y sobre todo eficiente. El control de asistencia que una organización realice de cada uno de sus miembros, deberá representar fielmente la verdadera incidencia del hecho, mostrando el tiempo real de ingreso y salida del lugar de trabajo.

Reportar estas incidencias de una manera adecuada, implicará adicionalmente de personal capacitado y con absoluta predisposición a corresponder a las bases administrativas de la organización, y no a imponer primero la amistad o inherencias personales para realizar registro de eventos correspondientes al control de asistencia y control de acceso. Este tipo de situación significará para la organización improductividad, y respeto por parte de sus empleados a las reglamentaciones impuestas, y por ende representar un problema de carácter financiero al no poder calcular de manera correcta las horas trabajadas, multas, descuentos y horas extras.

OBJETIVO GENERAL

Proporcionar a la Administración del instituto, información sobre el comportamiento de acceso de sus empleados, mediante el uso de tecnología biométrica, manteniendo de esa forma un control de Asistencia y mejorando la calidad de los servicios otorgados

OBJETIVOS ESPECÍFICOS

- Almacenar información de todo acceso del empleado mediante el uso del aplicativo.
- Proporcionar la seguridad mediante control biométrico, a través de la identificación de huellas dactilares.
- Brindar una solución eficiente, segura y accesible al problema de la identificación de las personas que ingresan al instituto.
- Generar reportes en base a la información recolectada en la base de datos, que representen con veracidad la eficiencia a las necesidades de la Administración.

CAPÍTULO 1

1.1 Historia de la Biometría

En la siguiente tabla, es posible apreciar un comparativo sobre la historia de la biometría, con la finalidad de generar un criterio verdaderamente objetivo sobre los trabajos existentes conforme a la lectura e interpretación de huellas dactilares.

	<p>1686 Marcello Malpighi En su tratado sobre las capas de la piel (llamada "Capa de Malpighi") señala las diferencias entre las crestas, espirales y lazos en las huellas dactilares.</p>
	<p>1823 Jan Evangelist Purkinje Profesor de la Universidad de Breslau, formula su tesis donde clasificaba en 9 los tipos de formas de huellas dactilares. 1856 Sr William Herschel Validación de contrato por impresión de la huella de la mano derecha, luego solo serían las huellas del dedo índice y medio.</p>
	<p>1889 D. Henry Faulds Estudió sobre las huellas dactilares halladas en antiguas cerámicas, propuso un método de clasificarlas, señalo la inmutabilidad de las mismas y destacó el valor de las huellas dactilares para su uso en la identificación de individuos. También fue quien propuso la impresión de las huellas dactilares a través de tintas y fue el primero en señalar el valor de reconocer las huellas latentes (rastros) en escenas de crímenes.</p>

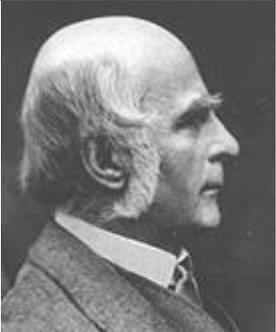
	<p>1891 Juan Vucetich Creación del primer método de clasificación de ficheros de huellas dactilares. También fue el primero en utilizar dicho método para esclarecer un crimen identificando a su autor por medio de las huellas dactilares encontradas en la escena del hecho. Este hecho marcó que ARGENTINA fuera el primer país a nivel mundial en reemplazar el uso de la antropometría por la clasificación de huellas dactilares.</p>
	<p>1892 Sr Francis Galton Primo de Charles Darwin, fue quién publicó en su libro "Fingerprints" que las huellas dactilares eran únicas y que no cambiaban a lo largo de la vida del individuo. Enunció las tres leyes fundamentales de la Dactiloscopia: perennidad, inmutabilidad y diversidad infinita. Establece su método de clasificación e identifica las características por lo que las huellas dactilares pueden ser clasificadas denominadas "minucias", en uso hoy en día. Su hijo, quien continuó su investigación, estableció el cálculo de probabilidad de que dos huellas sean iguales en 1:64.000.000.000.</p>
	<p>1896 Sr Richard Edward Henry Desarrolló en Scotland Yard e impuso el método de clasificación e identificación de huellas dactilares, en reemplazo de la antropometría, versión avanzada del método Galton, actualmente lo uso en Europa y Norteamérica. Publica "Clasificación y uso de las huellas dactilares".</p>

Tabla 1.1 Imágenes tomadas del libro *Biometrics*

El uso práctico de huellas dactilares como método de identificación de individuos ha sido utilizado desde finales del siglo 19 cuando Sr Francis Galton definió algunos de los puntos o características desde las cuales las huellas dactilares podían ser identificadas. Estos "puntos Galton" son la base para la ciencia de identificación por huella dactilar, la cual se ha expandido y efectuado una transición en el pasado siglo. La identificación por huella digital comienza su transición a la automatización a finales de los años 60 junto con la aparición de las tecnologías de computación. Con la llegada de las computadoras, un subconjunto de los puntos Galton, de aquí en más minucias (rasgos específicos), ha sido utilizado para desarrollar la tecnología de reconocimiento automatizado de huellas dactilares.

En 1969, hubo un empuje mayor por parte del Buró Federal de Investigaciones (FBI) para desarrollar un sistema para automatizar sus procesos de identificación por huellas dactilares, el cual rápidamente se había vuelto abrumador y requería de muchas horas hombre para el proceso manual. El FBI contrato al Buró Nacional de Estándares (NBS), ahora Instituto nacional de Estándares y Tecnología (NIST), para estudiar el proceso de automatización de la clasificación, búsqueda y concordancia de las huellas dactilares. El NIST identifico dos cambios clave: 1 escanear las tarjetas con huellas dactilares y extraer las minucias de cada huella y 2 buscar, comparar y combinar las listas de minucias contra grandes repositorios de huellas dactilares (1).

En 1975, El FBI fundo el desarrollo de escáneres de huella dactilar para clasificadores automatizados y tecnología de extracción de minucias, lo cual condujo al desarrollo de un lector prototipo. Este primer lector usaba técnicas capacitadas para recoger las minucias (2). En ese momento solo los datos biográficos de los individuos, la clasificación de los datos de huellas dactilares y las minucias eran almacenados a causa de que el costo de almacenamiento de las imágenes digitales de las huellas dactilares era prohibitivo. Durante las próximas décadas, el NIST se enfocó y condujo a desarrollos en los métodos

automáticos para digitalizar las huellas dactilares en tinta y los efectos de compresión y calidad de la imagen, la clasificación, extracción de minucias, y concordancia (3).

EL trabajo del NIST condujo el desarrollo del algoritmo M40, el primer algoritmo operacional utilizado en el FBI para estrechar la búsqueda de humanos. Los resultados producidos por el algoritmo M40 fueron provistos a técnicos humanos entrenados y especializados quienes evaluaron el significativamente el más pequeño grupo de imágenes candidatas. La tecnología de huellas dactilares disponible continuó mejorando y para el año 1981, cinco Sistemas automatizados de identificación por huella dactilar fueron desplegados. Varios sistemas estatales en los estados unidos y otros países habían implementado sus propios sistemas autónomos, desarrollados por un número de diferentes proveedores.

Durante esta evolución, la comunicación y el intercambio de información entre sistemas fueron pasados por alto, significando que una huella digital recogida con un sistema no podía ser buscado en otro sistema. Estos descuidos llevaron a la necesidad y al desarrollo de estándares para huellas digitales.

Conforme a la necesidad de un sistema de identificación integrado en la comunidad de la justicia criminal de los Estados Unidos se volvió rápidamente evidente, la próxima fase en la automatización de huellas dactilares ocurrió al finalizar la competencia de sistemas automatizados de identificación de huellas dactilares (Automated Fingerprint Identification System, IAFIS).

La competencia identificó e investigó tres desafíos principales:

- 1: Adquisición de huellas dactilares digitales,
- 2: Extracción de características de crestas locales, y
- 3: Concordancia de patrones de características de crestas (4).

Los sistemas modelo demostrados fueron evaluados en base a requerimientos de rendimiento específicos. Lockheed Martín fue seleccionado para construir el segmento AFIS del proyecto IAFIS del FBI y los componentes principales de IAFIS estuvieron operacionales para 1999. También en este plazo, los productos comerciales de verificación de huellas dactilares comenzaron a aparecer para varios controles de acceso, para logeo, y para beneficio de las funciones de verificación.

1.2 Historia de la huella digital

Las huellas digitales ofrecen medios infalibles de Identificación Personal. Ésa es la explicación esencial del porqué suplanta a otros métodos para establecer las identidades de los criminales. Otras características personales no cambian las huellas digitales.

En civilizaciones anteriores, fueron utilizados métodos para marcar al criminal. Le cortaban los dedos y/o mano.

En la Babilonia antigua, las huellas digitales fueron utilizadas en las tablas arcilla para las transacciones de negocios.

El romano empleó la aguja del tatuaje para identificar y para prevenir la desertión de soldados Mercenarios.

En China antigua, las impresiones del pulgar fueron encontradas en los sellos de arcilla.

En el siglo XIV en Persia, varios papeles oficiales del gobierno tenían las huellas digitales (impresiones), y un oficial del gobierno doctor, había observado que no hay dos huellas digitales exactamente semejantes.

Más recientemente, los oficiales con memorias visuales extraordinarias, "Con Memoria Fotográfica," identificaron a viejos delincuentes por la vista.

La fotografía disminuyó la carga de la Memoria, pero no era la Solución al problema criminal de la identificación. El aspecto físico, era fácil de modificar.

Marcello Malpighi en 1686, profesor de anatomía, en la universidad de Bolonia, dio a conocer en su tesis, la diferencia entre los cantos, espirales y lazos de las huellas digitales. Él no hizo ninguna mención de su valor como herramienta para la identificación individual. Una capa de piel fue nombrada después de su presentación, capa de "Malpighi", que es aproximadamente 1.8 mm de espesor.

En 1823, Juan Evangelist Purkinji, profesor de anatomía, en la universidad de Breslau, publicó su tesis discutiendo 9 patrones de la huella digital, pero él también no hizo ninguna mención sobre el valor de las huellas digitales para la identificación personal.

El primer inglés que en julio de 1858 comenzó a usar huellas digitales, fue Sr Guillermo Herschel, principal magistrado del distrito de Jungipoor, en la India, las primeras huellas digitales usadas fueron en los contratos nativos. Por un capricho, y sin pensamiento, hacia la identificación personal, Herschel tenía a Rajyadhar Konai, hombre de negocios local, que utilizaba la impresión en su mano, en la parte posterior de un contrato.

Alrededor 1870 un antropólogo francés ideó un sistema para medir y registrar las dimensiones de ciertas partes huesudas del cuerpo. Estas medidas, integraron una fórmula que se aplicaría en teoría a una persona y que no cambiaría durante su vida del adulto.

Este sistema de Bertillon, nombrado después de su inventor, "Alphonse Bertillon", fue aceptado generalmente por treinta años. Pero nunca se recuperó de los acontecimientos ocurridos en 1903, cuando condenaron a un hombre inocente en los Estados Unidos, en la Penitenciaría de Leavenworth, Kansas.

La idea era simplemente "para asustar y dejar fuera de todo el pensamiento la posibilidad de negar su firma."

Herschel, hizo un hábito de requerir impresiones de la palma y más adelante, simplemente las impresiones del índice derecho y los dedos medios en cada contrato que hizo con los locales. Dándole un mayor valor a la firma de cada contrato.

Mientras tanto su colección de huellas digitales creció, sin embargo Herschel, comenzó a observar que las impresiones entintadas podrían, probar o refutar de hecho la identidad. Su experiencia con la huella dactilar era obviamente limitada, la convicción personal de Sr Herschel, era que todas las huellas digitales eran únicas al individuo, así fue como permaneció a través de su vida, ampliaría su uso.

Durante el 1870, el Dr. Henry Faulds, Cirujano-Superintendente Británico del hospital de Tsukiji en Tokio, Japón, tomó el estudio de "piel-surcos" después de notar marcas, en los dedos de las piezas de cerámica "prehistóricas".

El Dr. Faulds reconoció la importancia de huellas digitales como medios de la identificación, ideando un método de clasificación.

En 1880, el Dr. Faulds remitió una explicación de su sistema de clasificación y envió una muestra, de las formas que él había diseñado, para las impresiones entintadas, grabación de las huellas dactilares, al Sr Charles Darwin de edad avanzada y mala salud, informó al Dr. Faulds que él no podría brindarle ninguna ayuda, pero prometió pasar los materiales recibidos a su primo, Francis Galton.

También en 1880, el Dr. Faulds publicó un artículo en el diario científico, "Nautre" (naturaleza). Él explicó que las huellas digitales se podrían utilizar como "los medios de

identificación personal”, y el uso de la tinta de las impresoras, como método para obtener tales huellas digitales.

En 1882, Gilbert Thompson de la Universidad Geológica “ESTADOS UNIDOS” en nuevo México, utilizó sus propias huellas digitales en un documento para prevenir la falsificación. Éste es el primer uso sabido de huellas digitales en los Estados Unidos.

En el libro de Mark Twain en 1883, (Samuel L. Clemens) "vida en el Misissippi", el uso de la identificación de la huella digital permitió identificar a un asesino. En un libro posterior, "Pudd'n Wilson principal", habla de la identificación a través de la huella digital. Hay una película reciente, que fue basada en este libro.

Sr Francis Galton, Antropólogo Británico y primo de Charles Darwin, comenzó sus investigaciones, sobre las huellas digitales como medio de identificación en 1880. En 1892, publicó su libro, "huellas digitales", estableciendo la individualidad y personalidad, de huellas digitales. El libro incluyó el primer sistema de clasificación para las huellas digitales.

El mayor interés de Galton sobre las huellas digitales, estaba basado en la ayuda para la determinación de la herencia y orígenes de razas. Al poco tiempo descubrió, que las huellas digitales no ofrecían ninguna pista firme, para determinar la inteligencia o la historia genética de un individuo, si pudo afirmar, que las huellas digitales no cambian en el transcurso de la vida de un individuo, y que la posibilidad de encontrar dos huellas digitales exactamente iguales era imposible Según sus cálculos, las probabilidades de dos huellas digitales individuales iguales eran 1 en 64 mil millones.

Galton identificó las características por las cuales las huellas digitales pueden ser identificadas. Estas mismas características (minucias) básicamente todavía están en uso hoy, y se refieren a menudo como detalles de Galton.

En 1891, Juan Vucetich, funcionario de la Policía de Argentina, comenzó con los primeros archivos de huellas digitales, basados en los tipos del patrón de Galton. Al principio, Vucetich incluyó el sistema de Bertillon con los archivos.

En 1892, Juan Vucetich hizo la primera identificación criminal con la huella digital. Él pudo identificar a una mujer de Apellido Rojas, que había asesinado a sus dos hijos, y cortado su propia garganta en una tentativa de culpar en otra persona.

Su impresión digital sangrienta, fue dejada en el marco de la puerta, probando su identidad como la asesina.

En 1901 comenzaron a utilizar las huellas digitales para la identificación criminal en Inglaterra y el País de Gales, usando las observaciones de Galton, evaluadas por Sr Edward Richard Henry.

Así comenzó el sistema de clasificación de Sr Edward Richard Henry, usado hoy por los ingleses.

En 1902 comenzó el uso sistemático de huellas digitales en los ESTADOS UNIDOS por la Comisión de la función pública de New York.

El Dr. Henry P. De Forrest inicia el uso de la huella dactilar de los ESTADOS UNIDOS.

En 1903 el sistema Penitenciario del estado de Nueva York comenzó el primer uso sistemático de huellas digitales en los ESTADOS UNIDOS para los criminales.

En 1904 la identificación por huellas digitales, comenzó a utilizarse en la "Federal Penitentiary Leavenworth" en Kansas, en el departamento de Policía de Sr. Louis, asistidos por un Sargento de la Policía Británica.

En 1905 comienza el uso de las huellas digitales en el Ejército de los E.E.U.U. Dos años más tarde, la Marina de los ESTADOS UNIDOS comenzaba también el uso de las huellas dactilares y a partir de ese año, 1907, durante los próximos 25 años más Agencias de Seguridad y Estado fueron incorporando el uso de huellas digitales como medios de la identificación personal. Muchas de estas agencias comenzaron a enviar las copias de las huellas digitales a la oficina Nacional de Identificación Criminal, que fue establecida por la Asociación Internacional de Jefaturas de Policía.

En 1918 el Sr. Edmond Locard escribió que si 12 puntos (detalles de Galton - Minucias) fueran iguales, entre dos huellas digitales, sería suficiente como identificación positiva. De ahí nace el número requerido de puntos necesarios para una identificación positiva. Algunos países han fijado sus propios estándares, que incluyen un número mínimo de puntos, pero no en los Estados Unidos.

En 1924 en una Ley del Congreso, se aprobó la división de Identificación del F.B.I. a través de la huella digital, formando el primer archivo de huellas dactilares de los EEUU.

Antes de 1946, el F.B.I. había procesado 100 millones de tarjetas de huellas digitales en archivos manualmente mantenidos; y antes de 1971, 200 millones de tarjetas.

Con la introducción de la tecnología de AFIS, los archivos fueron clasificados en archivos criminales automatizados, de 25 a 30 millones de huellas dactilares y los archivos civiles eran mantenidos manualmente (5).

1.3 Qué es una Huella Digital

Las huellas dactilares son los relieves epidérmicos que se encuentran en las falangetas de cada uno de nuestros dedos que son también una característica física única que distingue a todos los seres humanos y son irrepetibles.

También los dibujos o figuras formadas por las crestas papilares reciben el nombre de dactilogramas. Se le llama dactilogramas papilares si se encuentran en los dedos de la mano, plantares si se encuentran en la planta del pie y palmares si provienen de la palma de la mano.

1.4 ¿Qué es el Reconocimiento de la Huella digital?

El problema de reconocimiento de huella digital puede agruparse en dos subdominios: uno es la verificación de la huella digital y el otro es la identificación de la huella digital. Además, a diferencia del método manual para el reconocimiento de la huella digital por expertos, el reconocimiento de la huella digital que aquí se hace referencia es el AFRS (Automatic Fingerprint Recognition System) que significa Sistema de Reconocimiento de Huella Digital Automático) que está basado en un programa.

Verificación vs. Identificación La comprobación de la huella digital es verificar la autenticidad de una persona por su huella digital. El usuario proporciona su huella digital junto con su información de identidad tal como su número de ID. El sistema de comprobación de huella digital recupera la plantilla de la huella digital según el número de ID y compara la plantilla con la huella digital del usuario adquirida en tiempo real. Normalmente es el principio fundamental del diseño de AFAS (Automatic Fingerprint Authentication System: Sistema de Autenticación de Huella digital Automático).

La identificación de la huella digital es especificar la identidad de una persona por su huella digital. Sin el conocimiento de la identidad de la persona, el sistema de identificación de huella digital intenta comparar su huella digital con aquéllas que están en la base de datos. Es especialmente útil para los casos de la investigación delictivos. Y es el principio de diseño de AFIS (Sistema de Identificación de Huella Digital Automático). Sin embargo, todos los problemas de reconocimiento de huella digital, comprobación o identificación, están finalmente basados en una representación bien definida de una huella digital. Mientras que en la representación de restos de las huellas digitales

permanece la singularidad y simplicidad, la comparación de huellas digitales, tanto para el caso de verificación como para el caso de la identificación, es directo y fácil (6).

1.5 Dactiloscopia

Ciencia que se encarga del estudio de las crestas papilares de las yemas de los dedos, a través de la cual se identifica a una persona. Etimológicamente, deriva su nombre del griego “**Daktilos**” que significa dedos y “**Skopein**” que significa estudio, observación o examen.

1.5.1 Lofoscopia

Ciencia que estudia las diferentes clases de dibujos papilares que aparecen en la yema de los dedos, en la palma de las manos y planta de los pies. La identidad es el conjunto de características y particularidades de origen congénito o adquirido que hacen a una persona única (7).

1.5.2 Reconocimiento de la Huella digital

El reconocimiento de huella dactilar es el método de identificación biométrica por excelencia debido a que es fácil de adquirir, fácil de usar y por ende goza de gran aceptación por parte de los usuarios. Tuvo su origen a mediados del siglo XIX, siendo pionero en esta área sr William Herschel.

La huella dactilar es una característica física única que distingue a todos los seres humanos y la ciencia que se encarga de su estudio se conoce como Dactiloscopia, Este nombre fue inventado por el doctor Francisco Latzina en sustitución al dedo en 1892 por Sr Francis Galtón (Icnofalangometría). Todos los sistemas dactiloscópicos se basan en tres principios fundamentales:

* Perennidad: Gracias al fisiólogo checo Juan Evangelista Purkinje se sabe que las huellas dactilares se manifiestan a partir del sexto mes del desarrollo del embrión y que están presentes a lo largo de toda la vida de los seres humanos y hasta la descomposición del cadáver.

* Inmutabilidad: Las huellas dactilares no se ven afectadas en sus características por el desarrollo físico de los individuos ni por enfermedades de ningún tipo y en caso de que llegase a presentarse un desgaste involuntario (por ejemplo una herida o quemadura), el tejido epidérmico que la conforma es capaz de regenerarse tomando su forma original en un periodo de 15 días.

* Diversidad Infinita: Las huellas dactilares son únicas e irrepetibles, cada ser humano posee huellas dactilares con características individuales. Es un error común pensar que los gemelos idénticos no cumplen con este principio, sin embargo las huellas dactilares no se desarrollan debido a un proceso genético sino a un proceso aleatorio por lo que no existe ningún tipo de correlación entre gemelos idénticos o individuos de una misma familia (8).

1.6 Clasificación de los dactilogramas

Los dibujos o figuras formadas por las crestas papilares reciben el nombre de dactilogramas. Se denominan dactilogramas papilares si provienen de los dedos de la mano, plantares si provienen de la planta del pie y palmares cuando provienen de la palma de la mano.

- Dactilograma natural: es el que está en la yema del dedo, formado por las crestas papilares de forma natural.
- Dactilograma artificial: es el dibujo que aparece como resultado al entintar un dactilograma natural e imprimirlo en una zona idónea.

- Dactilograma latente: es la huella dejada por cualquier dactilograma natural al tocar un objeto o superficie. Este dactilograma queda marcado, pero es invisible. Para su revelación requiere la aplicación de un reactivo adecuado.

De igual forma un dactilograma se puede dividir en tres partes que se conocen como: sistemas dactilares los cuales son el Sistema basilar, el Sistema marginal y el Sistema nuclear. Todos los dactilogramas coinciden en el hecho de que las crestas papilares no describen formas aleatorias, sino que se agrupan hasta llegar a constituir sistemas definidos por la uniformidad de su orientación y figura. Se pueden distinguir cuatro grupos o clases distintas de configuraciones dérmicas según la denominada Clasificación de Henry, pero antes debemos estudiar dos singularidades presentes en algunas huellas denominadas Núcleo (Core) y Delta (9).

CAPÍTULO 2

2.1 Sistemas Biométricos

La práctica tecnológica de identificar a un individuo por sus rasgos biológicos y conductuales recibe el nombre de biometría; cuando tiene lugar de manera automatizada, mediante técnicas matemáticas auxiliadas por computadora, se conoce como biometría informática. La identidad así construida se denomina identidad biométrica del individuo.

Un sistema biométrico es un sistema de identificación de personas que se sirve de la biometría informática para condicionar el acceso a un bien o servicio. Los mecanismos de control automático de acceso a bienes y servicios incluyen, además, bases de datos y sistemas físicos como puertas de acceso controladas electrónicamente. Los aparatos de lectura de huellas dactilares o de análisis de voz son ejemplos comunes de sistemas biométricos. Los torniquetes en las estaciones del Metro o del Metrobús de la Ciudad de México no son sistemas biométricos, pues no llevan a cabo ningún proceso de verificación de la identidad biométrica de los usuarios; los boletos dotados con cinta magnética o las tarjetas de prepago únicamente sirven para identificar a sus poseedores como usuarios autorizados, y lo mismo sucede con la mayoría de las tarjetas bancarias.

No todo rasgo físico o conductual es propicio para establecer la identidad biométrica. La elección del rasgo está condicionada por la rapidez y la confiabilidad requeridas, así como por el presupuesto y el equipo con que se cuenta. Por ejemplo, aunque la información genética de una persona es única, y serviría para identificarla con gran confiabilidad, difícilmente se hallarán en el mercado sistemas basados en el análisis del ADN. Los sistemas biométricos que se sirven de esta clase de información se utilizan en campos muy especializados, como la medicina forense o los vinculados a la verificación de relaciones de parentesco.

Un Sistema Biométrico por definición, es un sistema automático capaz de:

- Obtener la muestra biométrica del usuario final.
- Extraer los datos de la muestra.
- Comparar los datos obtenidos con los existentes en la base de datos.
- Decidir la correspondencia de datos.
- Indicar el resultado de la verificación.

2.2 Bloques y etapas de un sistema biométrico

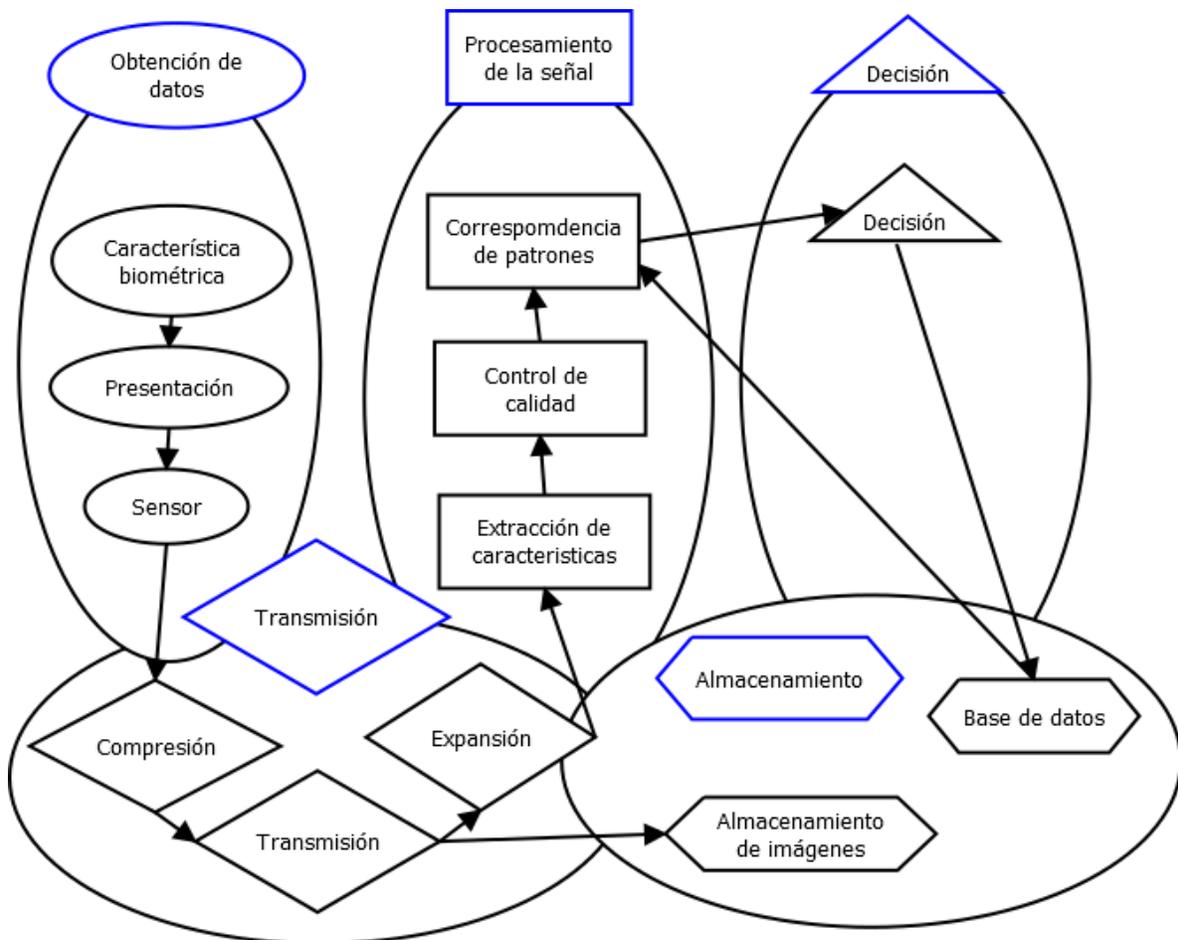


Figura 2.1 Imagen tomada del libro *Biometric Systems Technology*.

La evolución tan vertiginosa de la tecnología ha llevado a estos sistemas desde el plano de la ciencia-ficción a la realidad. Tanto así que podemos encontrar sistemas que procesan las siguientes variables biométricas:

- Reconocimiento de Rostro.
- Reconocimiento de la Voz.
- Patrón de Iris.
- Huellas Dactilares.
- Mapa de la Retina.
- Olor Corporal
- Forma del Oído
- Forma de la Mano
- Geometría de los dedos
- Forma de la Cabeza
- Mapa de Venas de la Mano

2.3 Características de un Indicador Biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera que sea el indicador, debe cumplir los siguientes requerimientos:

1. Universalidad: cualquier persona posee esa característica;
2. Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña;
3. Permanencia: la característica no cambia en el tiempo;
4. Cuantificación: la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como indicador biométrico. Luego de seleccionar algún indicador que

satisfaga los requerimientos antes señalados, es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores (10).

2.4 Arquitectura de un Sistema Biométrico para Identificación Personal

Los Dispositivos Biométricos poseen tres Componentes Básicos:

- El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner.
- El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos, Con los datos almacenados.
- El tercer componente establece un interfaz con aplicaciones ubicadas en el mismo u otro sistema.

Esta puede entenderse conceptualmente como dos módulos: Módulo de inscripción (enrollment module) y Módulo de identificación (identification module).

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El módulo de identificación es el responsable del reconocimiento de individuos. En la siguiente figura se muestra un esquema típico de un sistema de comparación automática de huellas dactilares (6).

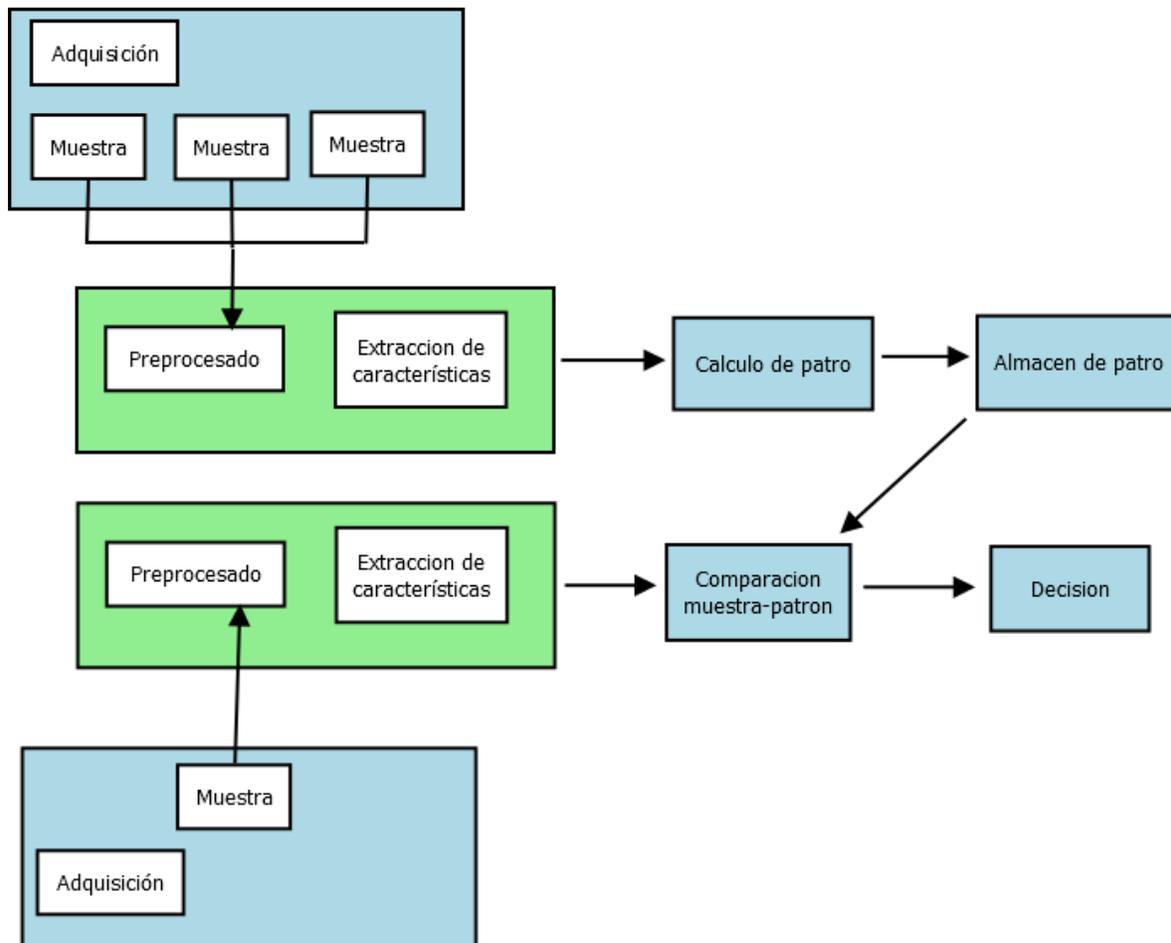


Figura 2.2

Adquisición: En esta etapa se toma una muestra de la huella dactilar de un sujeto. Dependiendo del sensor utilizado, la calidad y la resolución de la imagen obtenida varían enormemente. Los parámetros más relevantes que se utilizan para caracterizar los sensores son la resolución, el área de captura, el número de píxeles, la precisión geométrica, el contraste y la distorsión geométrica.

Preprocesado: La imagen obtenida en la etapa de adquisición se trata en función de las necesidades de los algoritmos de extracción y comparación que se vayan a utilizar. Normalmente siempre es necesario algún ajuste de la imagen para aumentar la calidad de la misma, como pueden ser ajuste de contraste, ecualización del histograma y una eliminación de las partes de la imagen que no contienen a la huella dactilar, lo que se denomina segmentación. Normalmente el preprocesado requerido para los algoritmos de comparación de huellas dactilares es bastante complejo y requiere una alta capacidad computacional.

Extracción de características: En esta etapa se extrae la información relevante de las huellas para su posterior comparación. La mayor parte de los algoritmos de comparación de huellas dactilares utilizan como característica las minucias. Uno de los algoritmos de extracción de minucias más destacados es el algoritmo de seguimiento de crestas de Mano, que consiste en el seguimiento de todas las crestas de la huella, determinando como minucias las bifurcaciones (desdoblamiento de una cresta en dos crestas) y terminaciones (fin de una cresta).

Comparación: En esta etapa se comparan las características extraídas para determinar si las dos muestras pertenecen al mismo individuo. Existen algoritmos que no necesitan extracción de características y por tanto realizan directamente la comparación.

2.5 Fase Operacional de un Sistema de Identificación Personal

Un sistema biométrico en su fase operacional puede operar en dos modos:

- Modo de verificación
- Modo de identificación

Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con los templates del individuo. Por ejemplo, si una persona ingresa su nombre de usuario entonces no será necesario revisar toda la base de datos buscando el template que más se asemeje al de él, sino que bastará para comparar la información de entrada sólo con el template que está asociado al usuario.

Esto conduce a una comparación uno a uno para determinar si la identidad reclamada por el individuo es verdadera o no. De manera más sencilla el modo de verificación responde a la pregunta: ¿eres tú quién dices ser?

Un sistema biométrico operando en el modo de identificación descubre a un individuo mediante una búsqueda exhaustiva en la base de datos con los templates, Esto conduce a una comparación del tipo uno-a-muchos para establecer la identidad del individuo. En términos sencillos el sistema responde la pregunta: ¿quién eres tú? Generalmente es más difícil diseñar un sistema de identificación que uno de verificación.

En ambos casos es importante la exactitud de la respuesta. Sin embargo, para un sistema de identificación la rapidez también es un factor crítico. Un sistema de identificación necesita explorar toda la base de datos donde se almacenan los templates, a diferencia de un sistema verificador.

De la discusión anterior resulta obvio notar que la exigencia sobre el extractor y el comparador de características es mucho mayor en el primer caso (11).

2.6 Sistemas Biométricos Actuales

En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características, Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

- 1.-Reconocimiento facial
- 2.-Termograma del rostro
- 3.-Huella dactilar
- 4.-Geometría de la mano
- 5.-Venas de las manos
- 6.-Iris
- 7.-Patrones de la retina
- 8.-Voz
- 9.-Firma Biométrica

Cada una de las técnicas anteriores posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir que técnica utilizar para una aplicación específica. En particular deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento. Una huella dactilar, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales.

También las máquinas que miden características físicas tienden a ser más grandes y costosas que las que detectan comportamientos. Debido a diferencias como las señaladas, no existe un único sistema biométrico que sea capaz de satisfacer todas las necesidades. Una compañía puede incluso decidir el uso de distintas técnicas en distintos ámbitos. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la identificación.

Se integran el Reconocimiento de Rostros y Huellas Dactilares. La razón es que el reconocimiento de Rostros es rápido pero no extremadamente confiable, mientras que la

Identificación mediante Huellas Dactilares es confiable pero no eficiente en consultas a bases de datos. Lo anterior sugiere el utilizar el reconocimiento de rostros para particional la base de datos. Luego de esto comienza la identificación de la huella. Los resultados alcanzados por el sistema conjunto son mejores que los obtenidos por sus partes por separado (12).

2.7 Tabla comparativa de sistemas biométricos

En la siguiente tabla, es posible apreciar las ventajas que se ofrecen sobre la viabilidad, facilidad y aceptación que se tiene conforme a los diversos dispositivos biométricos empleados para la lectura de los diferentes medios de interpretación persona.

	Fiabilidad	Facilidad De uso	Prevención De ataques	Aceptación	Estabilidad
Ojo (iris)	Muy alta	Media	Muy alta	Media	Alta
Ojo (retina)	Muy alta	Baja	Muy Alta	Baja	Alta
Huellas Dactilares	Muy alta	Alta	Alta	Alta	Alta
Vascular Dedo	Muy alta	Muy alta	Muy Alta	Alta	Alta
Vascular Mano	Muy alta	Muy alta	Alta	Alta	Alta
Geometría De la Mano	Alta	Alta	Alta	Alta	Media
Escritura Y firma	Media	Alta	Media	Muy alta	Baja
Voz	Alta	Alta	Media	Alta	Media
Cara 2D	Media	Alta	Media	Muy alta	Media
Cara 3D	Alta	Alta	Alta	Muy alta	Alta

Tabla 2.1

2.8 Dispositivo U Are U de DigitalPersona

El dispositivo usado en este proyecto fue desarrollado a la compañía DigitalPersona, la cual se dedica exclusivamente a producir dispositivos para reconocimiento biométrico, exclusivamente de huella digital. Entre los diversos productos que ofrece se encuentran: Sistemas Software-Hardware ya diseñados para un uso exclusivo, como lo es para el control de accesos a una red, control de uso de dispositivos, etc.

Sistema para diseño de aplicaciones con el dispositivo de huella digital, el cual incluye el dispositivo hardware para conexión por USB, y el driver, así como el ocx para el diseño de sistemas en lenguajes visuales (13).

En este caso del dispositivo usado para el proyecto es el mostrado en la figura Siguiente.



Figura 2.3

El funcionamiento interno del dispositivo no es el objetivo de este proyecto, razón por lo cual se omite su descripción; centrándonos en el uso del mismo solamente.

La forma en que se captura la imagen para posteriormente vectorizarla y generar su código, se genera internamente en conjunción con el driver del dispositivo, la captura se

realiza al presionar el dedo sobre la parte sensible y una vez detectada la presión sobre él se realiza el escaneo.

Una vez realizada la operación completa se genera un código de 901 caracteres que Sera de hoy en adelante el código para el reconocimiento de la huella digital que se capturó.

Estos 901 caracteres representan la interpretación de todos y cada uno de los elementos que integran a la huella digital capturada, que la representan diversos elementos los cuales están dispuestos en forma única en cada ser humano



Figura 2.4 Imagen tomada del libro *Criminalística tomo 2*

Una vez obtenido este código, se puede almacenar en una base de datos para su posterior uso para la identificación de personas. La forma en que se realiza la captura de dicho código es como sigue: para obtener un código que sea real, se deben tomar cuatro muestras de la huella dactilar, de estas cuatro muestras se obtiene un código que es el más aproximado posible al de la huella escaneada. Una vez obtenido dicho código, solo resta hacer la verificación y para esto solo se toma la muestra a comparar contra el código capturado. Se hace la observación que para realizar el escaneo de la huella, el dedo debe estar alineado correctamente en el escáner.

CAPÍTULO 3

3.1 Sistema desarrollado en netbeans versión 7.2

Se utilizó Netbeans porque permite integrar el código de programación del lector u are u digital person y puede ser ejecutado tanto en Windows como en sistemas basados en Unix.

3.2 Algoritmos del sistema

Para el desarrollo de este sistema, se partió de una base de datos limpia que almacene los registros de las huellas, en este caso preparamos una tablas sencilla que contenga los datos principales de los trabajadores, ID, nombre completo de la persona y la huella registrada, estos datos se almacenan por el código generado por el dispositivo de almacenamiento.

Módulo de registro

- 1.- Toma la muestra de su huella dactilar
- 2.- Capturar las cuatro muestras de su huella dactilar
- 3.- Verificar que la imagen tenga una calidad excelente
- 4.- Pide nombre del trabajador
- 5.- Almacenar los datos.

Módulo de registro de entrada

- 1.- Toma la muestra de su huella dactilar
- 2.- Obtiene las huellas de la base de datos
- 3.- Compara las características de la huella recientemente capturada con las plantillas guardadas en la base de datos
- 4.- Muestra los datos del trabajador y la hora de entrada

5.- Actualiza la base de datos con los nuevos valores

Módulo de registro de salida

1.- Toma la muestra de su huella dactilar

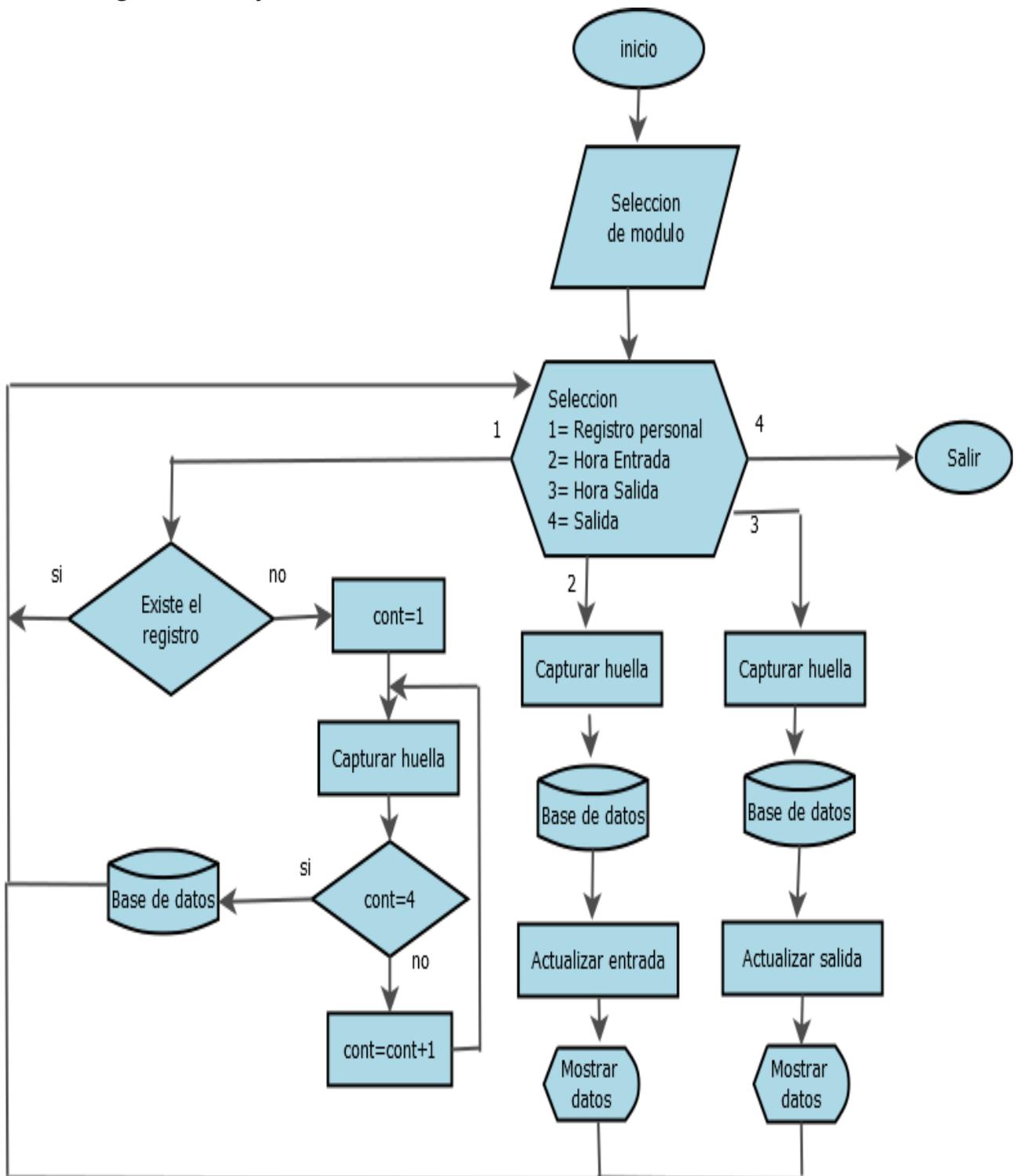
2.- Obtiene las huellas de la base de datos

3.- Compara las características de la huella recientemente capturada con las plantillas guardadas en la base de datos

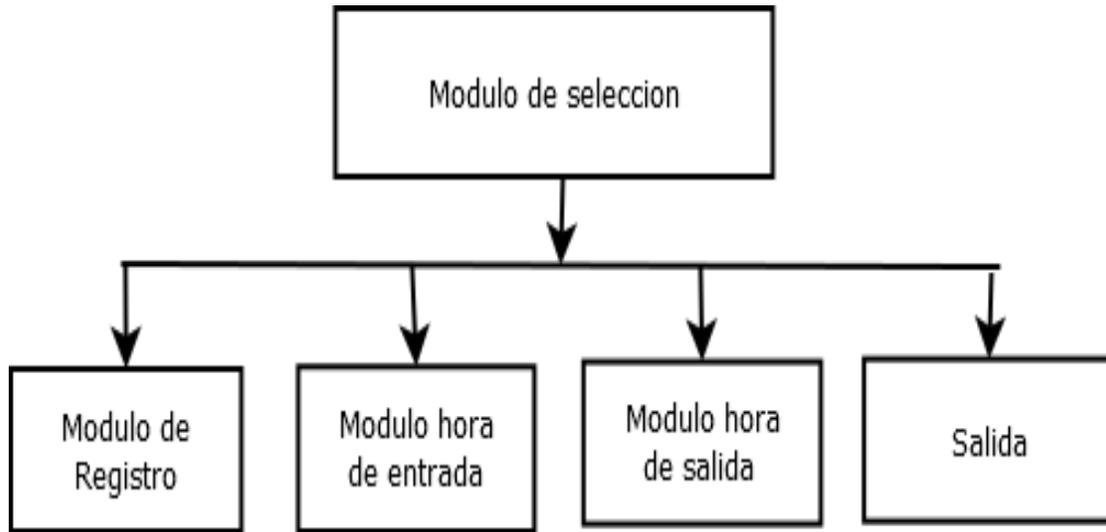
4.- Muestra los datos del trabajador y la hora de salida

5.- Actualiza la base de datos con los nuevos valores

3.3 Diagrama de flujo



3.4 Diagrama jerárquico



3.5 Base de datos

El sistema de almacenamiento, que se utiliza para el sistema se generó con MySQL consta de 2 tablas, las cuales están relacionadas por medio del campo que representa la clave del trabajador las tablas tienen el siguiente diseño:

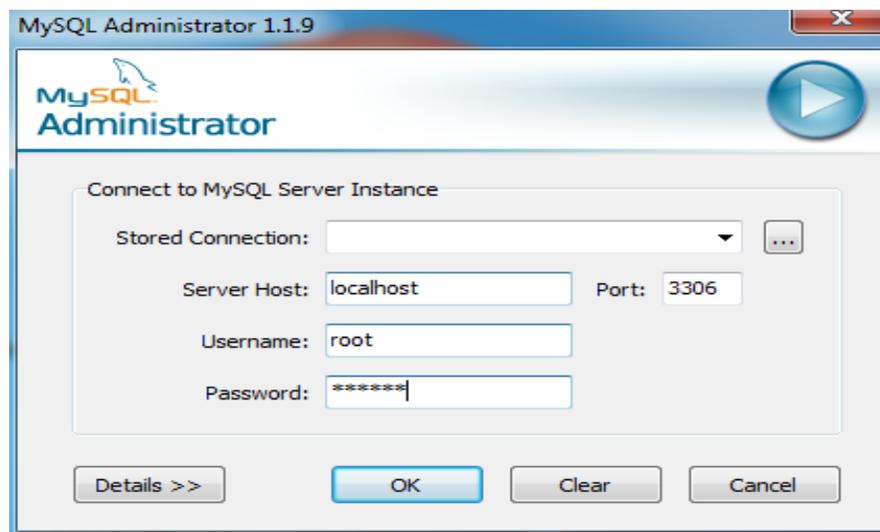


Figura 3.1

Tabla trabajadores

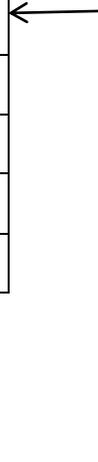
Nombre del Campo Tipo de Dato

ID	Integer
Nombres	Varchar
Apellido Paterno	Varchar
Apellido Materno	Varchar
Huella	Blob

Tabla Registros

Nombre del Campo Tipo de Dato

ID	Integer
Fecha	Date
Entrada	Time
Salida	Time



3.6 Interfaces de usuario y Descripción del Sistema

El sistema consta de 4 módulos principales:

- Módulo principal
- Módulo de registro
- Módulo de registro de entrada
- Módulo de registro de salida

3.6.1 Módulo principal

En este módulo se tiene el menú de inicio través del cual se tendrá acceso a los otros módulos. Véase figura E



Figura 3.2

Al iniciar el sistema se tienen 4 opciones, las cuales se pueden acceder por medio de botones, en este módulo solo se tiene acceso a los módulos principales del sistema, por lo cual aquí solo existen declaración de algunos objetos.

```
Captura Huella obj= new Captura Huella();
```

```
obj.setVisible(true);
```

```
this.setVisible(false);
```

```
registro_entrada obj= new registro_entrada();
```

```
obj.setVisible(true);
```

```
this.setVisible(false);
```

```
registro_salida obj=new registro_salida();
```

```
obj.setVisible(true);  
this.setVisible(false);  
System.exit(0);
```

3.6.2 Módulo de registro

En este módulo se lleva a cabo la captura de la huella digital, el control para realizar una cosa u otra se lleva a cabo por medio de programación, esta se realiza través del SDK (13) proporcionado por el fabricante. Véase figura F

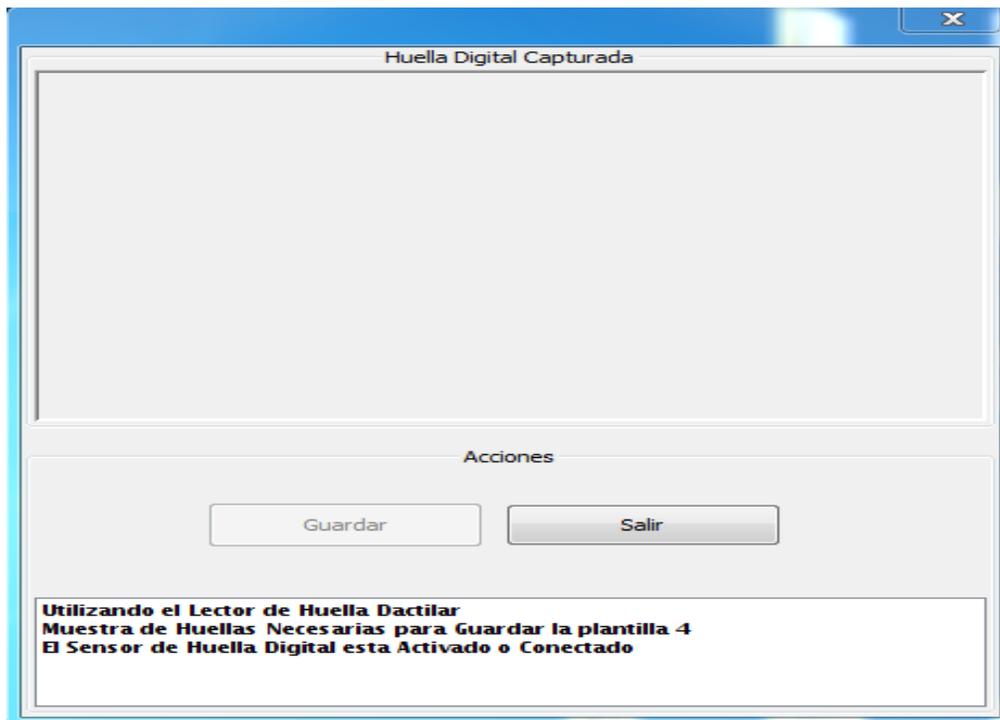


Figura 3.3

En esta modulo se realiza la conexión con la base de datos así como la creación de los métodos abstractos que se implementan para el correcto funcionamiento del lector y la toma de las 4 muestras para formar la plantilla ya tomadas se pide el nombre del trabajador para posteriormente guardarlo en la base de datos (Anexo 6.1).

Creamos los métodos abstractos, para la variable Lector, creando un Nuevo método que podemos llamar Iniciar, en el cual vamos a colocar los distintos métodos programable del lector, bien sea cuando ocurre la captura de la huella, cuando el lector se conecta o desconecta, cuando se coloca el dedo o se retira y cuando se presenta algún error, estos suelen ser los más importantes (anexo 6.2).

Ya definido los métodos creamos el método para procesar la captura de la huella y guardar huella (anexo 6.3).

3.6.3 Módulo de registro de entrada

En esta modulo se realiza la conexión con la base de datos y se vuelven a utilizar los métodos abstractos para el correcto funcionamiento de del lector y la toma de la huella digital para su proceso e identificación en la base de datos así como el registro de entrada (anexo 6.4). véase figura G

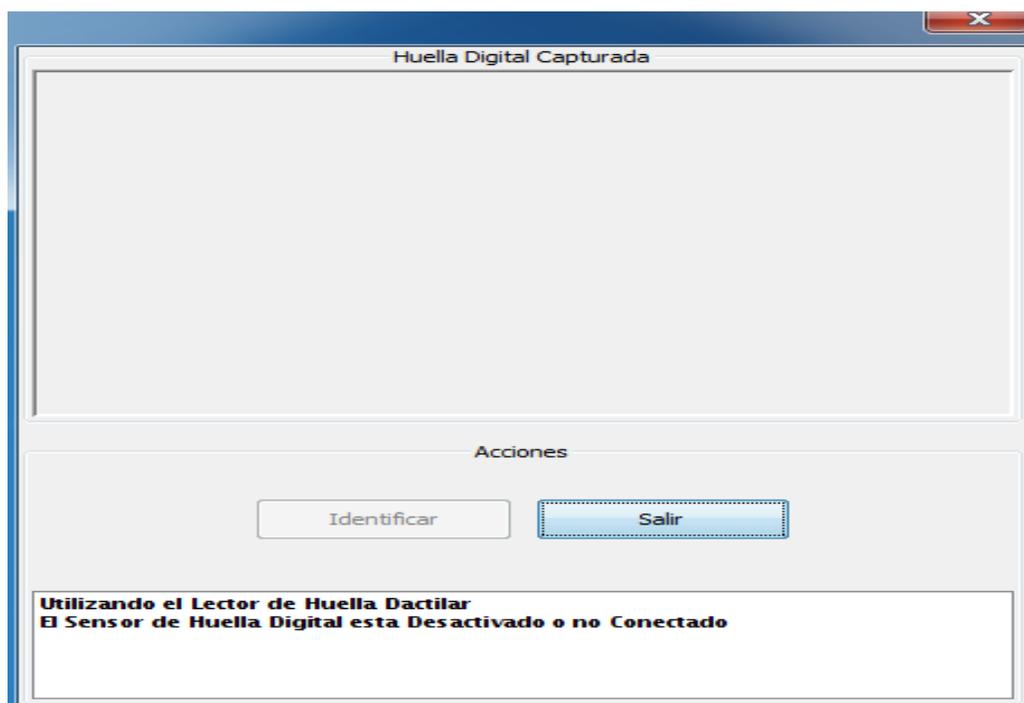


Figura 3.4

3.6.4 Módulo de registro de salida

En esta modulo se realiza la conexión con la base de datos y se vuelven a utilizar los métodos abstractos para el correcto funcionamiento de del lector y la toma de la huella digital para su proceso e identificación en la base de datos Este módulo es similar al anterior solo se modifican algunos campos para que tome el registro de la hora de salida (anexo 6.5). Véase figura h

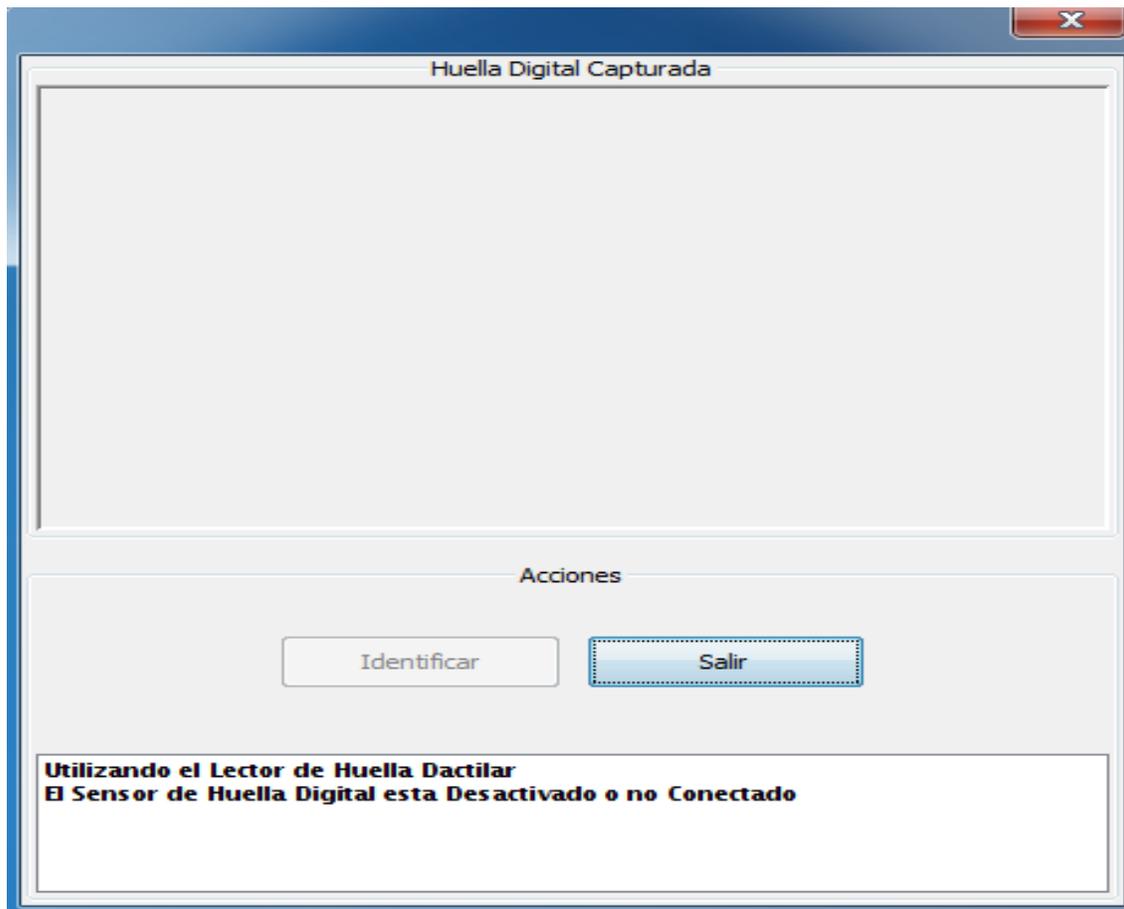


Figura 3.5

CAPÍTULO 4

4.1 Reporte mediante red local

En esta parte del proyecto el administrador del CEAPS realiza la verificación de los registros mediante un servidor web que hace una conexión a la base de datos en red, se utilizó código HTML y PHP para generar la página web y permitir la conexión a la base de datos.

4.2 HTML

El HTML, Hyper Text Markup Language (Lenguaje de marcación de Hipertexto) es el lenguaje de marcas de texto utilizado normalmente en la www (World Wide Web). Fue creado en 1986 por el físico nuclear Tim Berners-Lee; el cual tomo dos herramientas preexistentes: El concepto de Hipertexto (Conocido también como link o ancla) el cual permite conectar dos elementos entre si y el SGML (Lenguaje Estándar de Marcación General) el cual sirve para colocar etiquetas o marcas en un texto que indique como debe verse. HTML no es propiamente un lenguaje de programación como C++, Visual Basic, etc., sino un sistema de etiquetas. HTML no presenta ningún compilador, por lo tanto algún error de sintaxis que se presente éste no lo detectará y se visualizara en la forma como éste lo entienda.

El entorno para trabajar HTML es simplemente un procesador de texto, como el que ofrecen los sistemas operativos Windows (Bloc de notas), UNIX (el editor vi o nano) o el que ofrece MS Office (Word). El conjunto de etiquetas que se creen, se deben guardar con la extensión html Estos documentos pueden ser mostrados por los visores o "navegadores" de páginas Web en Internet, como Firefox, Chrome, Opera y Microsoft Internet Explorer. También existe el HTML Dinámico (DHTML), que es una mejora de Microsoft de la versión 4.0 de HTML que le permite crear efectos especiales como, por ejemplo, texto que vuela desde la página palabra por palabra o efectos de transición al estilo de anuncio publicitario giratorio entre página y página (14)

4.3 PHP

PHP es un acrónimo recursivo que significa PHP Hypertext Pre-processor (inicialmente PHP Tools, o, Personal Home Page Tools). Fue creado originalmente por Rasmus Lerdorf; sin embargo la implementación principal de PHP es producida ahora por The PHP Group y sirve como el estándar de facto para PHP al no haber una especificación formal. Publicado bajo la PHP License, la Free Software Foundation considera esta licencia como software libre.

Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos y plataformas sin costo alguno. El lenguaje PHP se encuentra instalado en más de 20 millones de sitios web y en un millón de servidores, el número de sitios en PHP ha compartido algo de su preponderante dominio con otros nuevos lenguajes no tan poderosos desde agosto de 2005.

El gran parecido que posee PHP con los lenguajes más comunes de programación estructurada, como C y Perl, permiten a la mayoría de los programadores crear aplicaciones complejas con una curva de aprendizaje muy corta. También les permite involucrarse con aplicaciones de contenido dinámico sin tener que aprender todo un nuevo grupo de funciones.

Aunque todo en su diseño está orientado a facilitar la creación de sitios webs, es posible crear aplicaciones con una interfaz gráfica para el usuario, utilizando la extensión PHP-Qt o PHP-GTK. También puede ser usado desde la línea de órdenes, de la misma manera como Perl o Python pueden hacerlo; a esta versión de PHP se la llama PHP-CLI (Command Line Interface).

Cuando el cliente hace una petición al servidor para que le envíe una página web, el servidor ejecuta el intérprete de PHP. Éste procesa el script solicitado que generará el contenido de manera dinámica (por ejemplo obteniendo información de una base de

datos). El resultado es enviado por el intérprete al servidor, quien a su vez se lo envía al cliente. Mediante extensiones es también posible la generación de archivos PDF, Flash, así como imágenes en diferentes formatos.

Permite la conexión a diferentes tipos de servidores de bases de datos tales como MySQL, PostgreSQL, Oracle, ODBC, DB2, Microsoft SQL Server, Firebird y SQLite.

PHP también tiene la capacidad de ser ejecutado en la mayoría de los sistemas operativos, tales como Unix (y de ese tipo, como Linux o Mac OS X) y Microsoft Windows, y puede interactuar con los servidores de web más populares ya que existe en versión CGI, módulo para Apache, e ISAPI.

PHP es una alternativa a las tecnologías de Microsoft ASP y ASP.NET (que utiliza C# y Visual Basic .NET como lenguajes), a ColdFusion de la empresa Adobe, a JSP/Java y a CGI/Perl. Aunque su creación y desarrollo se da en el ámbito de los sistemas libres, bajo la licencia GNU, existe además un entorno de desarrollo integrado comercial llamado Zend Studio. CodeGear (la división de lenguajes de programación de Borland) ha sacado al mercado un entorno de desarrollo integrado para PHP, denominado 'Delphi for PHP. También existen al menos un par de módulos para Eclipse, uno de los entornos más populares (15).

Para este proyecto se utilizó XAMPP es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl. El nombre proviene del acrónimo de X (para cualquiera de los diferentes sistemas operativos), Apache, MySQL, PHP, Perl.

El programa está liberado bajo la licencia GNU y actúa como un servidor web libre, fácil de usar y capaz de interpretar páginas dinámicas. Actualmente XAMPP está disponible para Microsoft Windows, GNU/Linux, Solaris y MacOS X.

4.4 Características de XAMPP

XAMPP solamente requiere descargar y ejecutar un archivo zip, tar , exe o fkl, con unas pequeñas configuraciones en alguno de sus componentes que el servidor Web necesitará. XAMPP se actualiza regularmente para incorporar las últimas versiones de Apache/MySQL/PHP y Perl. Véase figura I. También incluye otros módulos como OpenSSL y phpMyAdmin. Para instalar XAMPP se requiere solamente una pequeña fracción del tiempo necesario para descargar y configurar los programas por separado. Puede encontrarse tanto en versión completa, así como en una versión más ligera que es portátil.

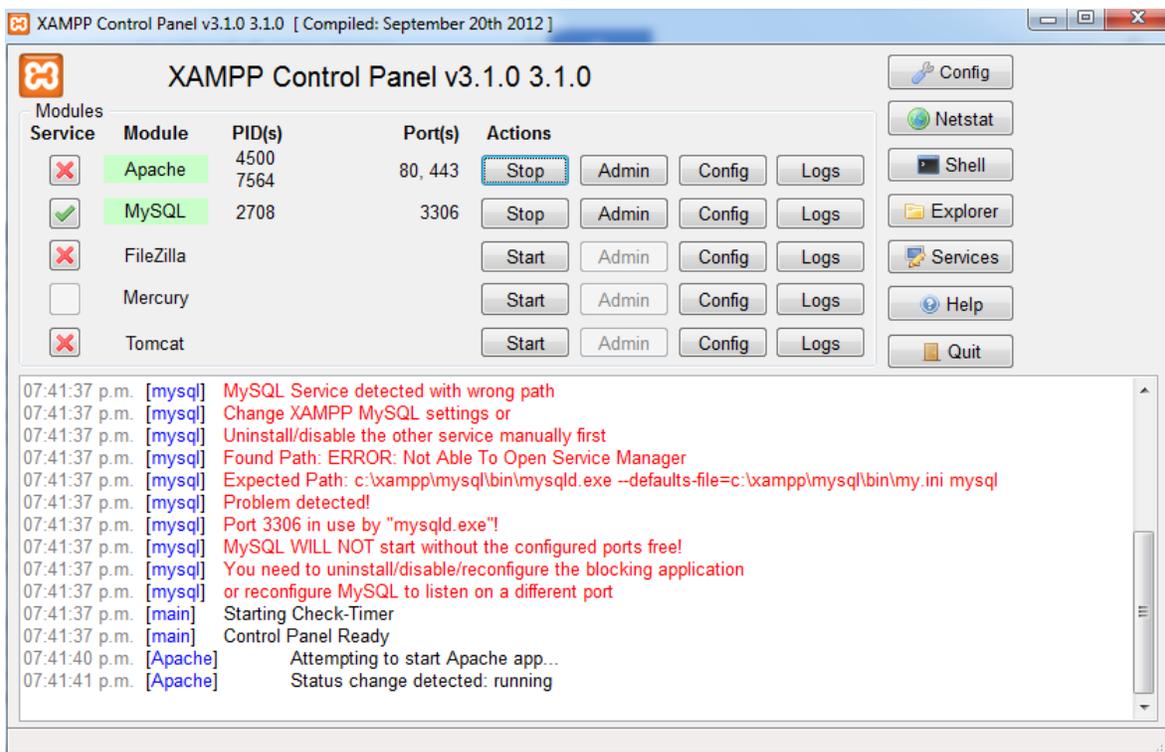


Figura 4.1

4.5 Código HTML y PHP

Se crearon 3 páginas web para generar el reporte, la principal tiene 2 métodos de búsqueda por fecha exacta o rango de fechas (anexo 6.6). Véase figura J



Figura 4.2

4.6 Reporte por trabajador

En este reporte pasamos los valores de nombre del trabajador y fecha específica mediante el método post (anexo 6.7).

4.7 Reporte por rango de fechas

En este reporte pasamos el rango de fechas que se desee revisar en la cual incluya a todos los trabajadores (anexo 6.8).

4.8 Costo e Impacto de implementación

El impacto registrado en el CEAPS durante el tiempo en que se implementó a la fecha actual es positivo, se ve reflejado en la asistencia y puntualidad del personal en todos los turnos anteriormente el 40% del personal se retiraba 2 o 3 horas antes de su salida ya que solo se debía registrar en una libreta logrando colocar datos falsos e incorrectos sin alguna tipo de supervisión.

Desde que se implementó el registro por huella digital el personal cumple con su horario establecido en su contrato ya que el salir con anticipación se verá reflejado en su remuneración económica y perdería muchos beneficios que del instituto así mismo se incrementó la calidad de los servicios otorgados en el CEAPS.

El costo del sistema fue mínimo el equipo que se utilizo es el mismo que está en el área de archivo, el lector tuvo un costo aproximada de 1000 pesos, el centro de salud cuenta con una red inalámbrica la cual es ocupada para que el administrador pueda revisar los horarios.

En conclusión se utilizaron las herramientas que se tenían a la mano para disminuir costos y hacer más eficiente el servicio.

CAPÍTULO 5

5.1 Conclusiones

El campo de la biometría con huellas digitales puede ser trabajado en muchas áreas de la sociedad, optimizando procesos que involucren tiempo y espacios. Así mismo los desarrolladores cuentan en la actualidad con novedosas y útiles herramientas libres para la creación, codificación y depuración de los programas que se realicen. Por las anteriores razones es un campo que ofrece muchas posibilidades y está siendo acogido por la sociedad.

En la práctica como tal, este sistema puede llegar a ser vulnerable en aspectos como: la inexperiencia de los usuarios en el momento de poner el dedo en el escáner hace que el registro o verificación se haga menos eficiente, las condiciones en que el usuario puede tener el dedo hace que el sistema pierda efectividad. Por ejemplo, un dedo muy sucio o engrasado pierde características de reconocimiento a la hora de hacer el escaneo.

A la fecha, las técnicas propuestas que han obtenido mayor éxito, se han basado en una comparación de índole geométrica de los vectores de características. El sistema de identificación biométrica con huellas digitales es uno de los sistemas actualmente más rápidos y su seguridad depende del grado de aceptación que se le dé al mismo.

El proyecto elaborado ofrece como ventaja la de permitir a las instituciones mantener un control de las asistencias de sus empleados, eliminando el uso de reportes manuales y por ende del tiempo para el procesamiento de registros.

La biometría está entrando con fuerza en sectores y destinados al control de recursos humanos. El control de presencia, control de puntualidad, control de horario, y control de productividad, es esencial en la gestión de los recursos humanos en una empresa. Una empresa que desee hacer una gestión de personal eficiente debe tener herramientas que acaten unas reglas de juego objetivas para todos los trabajadores.

Este sistema en el momento de su creación suele ser extenso con los registros de empleados, ya que se encarga de verificar el cumplimiento de los empleados en una empresa registrando de esta forma si cumple con las políticas de entrada y salida que una empresa dispuso. Tiene como objetivo mantener el registro e información sobre el personal

5.2 Obligatorio.

Las empresas están gradualmente reconociendo la necesidad de mantener controles de asistencia de forma automática mediante el uso de sistemas biométricos, haciendo uso de los mismos, sin embargo se requiere de una visión que determine qué tipo de tecnología biométrica es la más adecuado para la empresa.

La implementación de sistemas de control de asistencias a prevenir y controlar problemas habituales referentes al cumplimiento de las jornadas laborales, control de acceso a ciertos lugares restringidos por la organización, aunque no sea una garantía de administrar la seguridad.

5.3 Recomendaciones

El sistema desarrollado se limita a proveer la información de las asistencias de los empleados de una entidad, proporcionando un soporte de toma de decisión a la empresa con el fin de evaluar la productividad de los mismos.

El sistema implementado está diseñado para funcionar dentro de una red local.

Para mantener un respaldo de la información es necesario realizar los backup correspondiente a fin de proveer información actualizable en caso de algún percance que motive la pérdida de los datos.

Realizar el mantenimiento del dispositivo biométrico, con el propósito de mantener su correcto desempeño y obtener resultados veraces en la identificación.

ANEXOS

Anexo 6.1

Conexión a la base de datos

```
public class ConexionBD {
public String puerto="3306";
public String nomservidor="localhost";
public String db="huellas?zeroDateTimeBehavior=convertToNull";
public String user="root";
public String pass="*****";
Connection conn=null;
public Connection conectar(){
    try{
        String ruta="jdbc:mysql://";
        String servidor=nomservidor+": "+puerto+"/";
        Class.forName("com.mysql.jdbc.Driver");
        conn = DriverManager.getConnection(ruta+servidor+db,user,pass);
        if (conn!=null){
            System.out.println("Conección a base de datos listo...");
        }
        else if (conn==null)
        {
            throw new SQLException();
        }
    }catch(SQLException e){
        JOptionPane.showMessageDialog(null, e.getMessage());
    } catch (ClassNotFoundException e) {
        JOptionPane.showMessageDialog(null, "Se produjo el siguiente error: "+e.getMessage());
    }catch (NullPointerException e){
        JOptionPane.showMessageDialog(null, "Se produjo el siguiente error: "+e.getMessage());
    }finally{
        return conn;
    }
}
public void desconectar(){
    conn = null;
    System.out.println("Desconexión a base de datos listo...");
}
```

```
}  
}
```

Anexo 6.2

```
protected void Iniciar(){  
    Lector.addDataListener(new DPFPDataAdapter() {  
        @Override public void dataAcquired(final DPFPDataEvent e) {  
            SwingUtilities.invokeLater(new Runnable() { public void run() {  
                EnviarTexto("La Huella Digital ha sido Capturada");  
                ProcesarCaptura(e.getSample());  
            }});  
        });  
    };  
    Lector.addReaderStatusListener(new DPFPReaderStatusAdapter() {  
        @Override public void readerConnected(final DPFPReaderStatusEvent e) {  
            SwingUtilities.invokeLater(new Runnable() { public void run() {  
                EnviarTexto("El Sensor de Huella Digital esta Activado o Conectado");  
            }});  
        }  
        @Override public void readerDisconnected(final DPFPReaderStatusEvent e) {  
            SwingUtilities.invokeLater(new Runnable() { public void run() {  
                EnviarTexto("El Sensor de Huella Digital esta Desactivado o no Conecatado");  
            }});  
        }  
    });  
    Lector.addSensorListener(new DPFPSensorAdapter() {  
        @Override public void fingerTouched(final DPFPSensorEvent e) {  
            SwingUtilities.invokeLater(new Runnable() { public void run() {  
                EnviarTexto("El dedo ha sido colocado sobre el Lector de Huella");  
            }});  
        }  
        @Override public void fingerGone(final DPFPSensorEvent e) {  
            SwingUtilities.invokeLater(new Runnable() { public void run() {  
                EnviarTexto("El dedo ha sido quitado del Lector de Huella");  
            }});  
        }  
    });  
    Lector.addErrorListener(new DPFPErrorAdapter(){  
        public void errorReader(final DPFPErrorEvent e){
```

```

SwingUtilities.invokeLater(new Runnable() { public void run() {
    EnviarTexto("Error: "+e.getError());
    }});}
};
}

```

Anexo 6.3

```

public void ProcesarCaptura(DPFPSample sample)
{
    // Procesar la muestra de la huella y crear un conjunto de características con el propósito de inscripción.
    featuresinscripcion = extraerCaracteristicas(sample, DPFPSamplePurpose.DATA_PURPOSE_ENROLLMENT);
    // Procesar la muestra de la huella y crear un conjunto de características con el propósito de verificación.
    featuresverificacion = extraerCaracteristicas(sample, DPFPSamplePurpose.DATA_PURPOSE_VERIFICATION);
    // Comprobar la calidad de la muestra de la huella y lo añade a su reclutador si es bueno
    if (featuresinscripcion != null)
        try{
            System.out.println("Las Caracteristicas de la Huella han sido creada");
            Reclutador.addFeatures(featuresinscripcion);// Agregar las características de la huella a la plantilla a
crear
            // Dibuja la huella dactilar capturada.
            Image image=CrearImagenHuella(sample);
            DibujarHuella(image);
        }catch (DPFPImageQualityException ex) {
            System.err.println("Error: "+ex.getMessage());
        }
        finally {
            EstadoHuellas();
            // Comprueba si la plantilla se ha creado.
            switch(Reclutador.getTemplateStatus())
            {
                case TEMPLATE_STATUS_READY: // informe de éxito y detiene la captura de huellas
                    stop();
                    setTemplate(Reclutador.getTemplate());
                    EnviarTexto("La Plantilla de la Huella ha Sido Creada, ya puede Verificarla o Identificarla");
            }
        }
    }
}

```



```

JOptionPane.showMessageDialog(null,"Huella Guardada Correctamente");
con.desconectar();
btnGuardar.setEnabled(false);
} catch (SQLException ex) {
//Si ocurre un error lo indica en la consola
System.err.println("Error al guardar los datos de la huella.");
}finally{
con.desconectar();
}
}
}

```

Anexo 6.4

```

protected void Iniciar(){
Lector.addDataListener(new DPFPDataAdapter() {
@Override public void dataAcquired(final DPFPDataEvent e) {
SwingUtilities.invokeLater(new Runnable() {    public void run() {
EnviarTexto("La Huella Digital ha sido Capturada");
ProcesarCaptura(e.getSample());
}}});
});
Lector.addReaderStatusListener(new DPFPReaderStatusAdapter() {
@Override public void readerConnected(final DPFPReaderStatusEvent e) {
SwingUtilities.invokeLater(new Runnable() {    public void run() {
EnviarTexto("El Sensor de Huella Digital esta Activado o Conectado");
}}});
@Override public void readerDisconnected(final DPFPReaderStatusEvent e) {
SwingUtilities.invokeLater(new Runnable() {    public void run() {
EnviarTexto("El Sensor de Huella Digital esta Desactivado o no Conectado");
}}});
});
Lector.addSensorListener(new DPFPSensorAdapter() {
@Override public void fingerTouched(final DPFPSensorEvent e) {
SwingUtilities.invokeLater(new Runnable() {    public void run() {
EnviarTexto("El dedo ha sido colocado sobre el Lector de Huella");
}
}
}
}
}

```

```

    });}
    @Override public void fingerGone(final DPFPSensorEvent e) {
    SwingUtilities.invokeLater(new Runnable() {    public void run() {
    EnviarTexto("El dedo ha sido quitado del Lector de Huella");
    });}
    });
    Lector.addErrorListener(new DPFPErroAdapter(){
    public void errorReader(final DPFPErroEvent e){
    SwingUtilities.invokeLater(new Runnable() { public void run() {
    EnviarTexto("Error: "+e.getError());
    });}
    });
    }
}
ya definido los métodos creamos el método para procesar la captura de la huella e identificar huella
public void ProcesarCaptura(DPFPSample sample)
{
// Procesar la muestra de la huella y crear un conjunto de características con el propósito de inscripción.
featuresinscripcion = extraerCaracteristicas(sample, DPFDataPurpose.DATA_PURPOSE_ENROLLMENT);
// Procesar la muestra de la huella y crear un conjunto de características con el propósito de verificación.
featuresverificacion = extraerCaracteristicas(sample, DPFDataPurpose.DATA_PURPOSE_VERIFICATION);
// Comprobar la calidad de la muestra de la huella y lo añade a su reclutador si es bueno
if (featuresinscripcion != null)
    try{
        System.out.println("Las Caracteristicas de la Huella han sido creada");
        Reclutador.addFeatures(featuresinscripcion);// Agregar las características de la huella a la plantilla a
crear
        // Dibuja la huella dactilar capturada.
        Image image=CrearImagenHuella(sample);
        DibujarHuella(image);
        btnIdentificar.setEnabled(true);
    }catch (DPFPImageQualityException ex) {
        System.err.println("Error: "+ex.getMessage());
    }
    finally {
        EstadoHuellas();

```

```

// Comprueba si la plantilla se ha creado.
    switch(Reclutador.getTemplateStatus())
    {
    case TEMPLATE_STATUS_READY: // informe de éxito y detiene la captura de huellas
        stop();
        setTemplate(Reclutador.getTemplate());
        EnviarTexto("La Plantilla de la Huella ha Sido Creada, ya puede Verificarla o Identificarla");
        btnIdentificar.setEnabled(false);
        break;
    case TEMPLATE_STATUS_FAILED: // informe de fallas y reiniciar la captura de huellas
        Reclutador.clear();
        stop();
        EstadoHuellas();
        setTemplate(null);
        JOptionPane.showMessageDialog(registro_entrada.this, "La Plantilla de la Huella no pudo ser
creada, Repita el Proceso", "Inscripcion de Huellas Dactilares", JOptionPane.ERROR_MESSAGE);
        start();
        break;
    }
    }
}

public void identificarHuella() throws IOException{
    try {
        //Establece los valores para la sentencia SQL
        Connection c=con.conectar();
        //Obtiene todas las huellas de la bd
        PreparedStatement identificarStmt = c.prepareStatement("SELECT * FROM somhue");
        ResultSet rs = identificarStmt.executeQuery();
        //Si se encuentra el nombre en la base de datos
        while(rs.next()){
            //Lee la plantilla de la base de datos
            byte templateBuffer[] = rs.getBytes("huehuella");
            //String id=rs.getString("ID");
            int id=rs.getInt("ID");
            String nombre=rs.getString("huenombre");

```

```

//Crea una nueva plantilla a partir de la guardada en la base de datos
DPFPTemplate referenceTemplate =
DPFPGlobal.getTemplateFactory().createTemplate(templateBuffer);
//Envia la plantilla creada al objeto contenedor de Template del componente de huella digital
setTemplate(referenceTemplate);
// Compara las caracteristicas de la huella recientemente capturda con la
// alguna plantilla guardada en la base de datos que coincide con ese tipo
DPFPVerificationResult result = Verificador.verify(featuresverificacion, getTemplate());
//compara las plantilas (actual vs bd)
//Si encuentra correspondencia dibuja el mapa
//e indica el nombre de la persona que coincidió.
if (result.isVerified()){
// obtener fecha
java.util.Date utilDate = new java.util.Date(); //fecha actual
long lnMilisegundos = utilDate.getTime();
java.sql.Date sqlDate = new java.sql.Date(lnMilisegundos);
java.sql.Time sqlTime = new java.sql.Time(lnMilisegundos);
java.sql.Timestamp sqlTimestamp = new java.sql.Timestamp(lnMilisegundos);
//crea la imagen de los datos guardado de las huellas guardadas en la base de datos
JOptionPane.showMessageDialog(null, "La huella capturada es de "+nombre,"Verificacion de Huella",
JOptionPane.INFORMATION_MESSAGE);
JOptionPane.showMessageDialog(null, "La fecha es: " +sqlDate);
JOptionPane.showMessageDialog(null, "La hora es: " +sqlTime);
//-----
//actualizar datos
PreparedStatement insertStmt = c.prepareStatement("INSERT INTO registros(fecha,entrada,id)
values(?,?,?);
System.out.println(insertStmt);
insertStmt.setDate(1, sqlDate);
insertStmt.setTime(2, sqlTime);
insertStmt.setInt(3, id);
//Ejecuta la sentencia
insertStmt.execute();
insertStmt.close();
return;

```

```

        }
    }
    //Si no encuentra alguna huella correspondiente al nombre lo indica con un mensaje
    JOptionPane.showMessageDialog(null, "No existe ningún registro que coincida con la huella",
"Verificacion de Huella", JOptionPane.ERROR_MESSAGE);
    setTemplate(null);
    } catch (SQLException e) {
    //Si ocurre un error lo indica en la consola
    System.err.println("Error al identificar huella dactilar."+e.getMessage());
    }finally{
    con.desconectar();
    }
}

```

Anexo 6.5

```

protected void Iniciar(){
    Lector.addDataListener(new DPFPDataAdapter() {
        @Override public void dataAcquired(final DPFPDataEvent e) {
            SwingUtilities.invokeLater(new Runnable() {      public void run() {
                EnviarTexto("La Huella Digital ha sido Capturada");
                ProcesarCaptura(e.getSample());
            }});
        });
    Lector.addReaderStatusListener(new DPFPReaderStatusAdapter() {
        @Override public void readerConnected(final DPFPReaderStatusEvent e) {
            SwingUtilities.invokeLater(new Runnable() {      public void run() {
                EnviarTexto("El Sensor de Huella Digital esta Activado o Conectado");
            }});
        @Override public void readerDisconnected(final DPFPReaderStatusEvent e) {
            SwingUtilities.invokeLater(new Runnable() {      public void run() {
                EnviarTexto("El Sensor de Huella Digital esta Desactivado o no Conectado");
            }});
        });
    Lector.addSensorListener(new DPFPSensorAdapter() {

```

```

@Override public void fingerTouched(final DPFPSensorEvent e) {
    SwingUtilities.invokeLater(new Runnable() {      public void run() {
        EnviarTexto("El dedo ha sido colocado sobre el Lector de Huella");
    }});}

@Override public void fingerGone(final DPFPSensorEvent e) {
    SwingUtilities.invokeLater(new Runnable() {      public void run() {
        EnviarTexto("El dedo ha sido quitado del Lector de Huella");
    }});}

});

Lector.addErrorListener(new DPFPErroAdapter(){
    public void errorReader(final DPFPErroEvent e){
        SwingUtilities.invokeLater(new Runnable() { public void run() {
            EnviarTexto("Error: "+e.getError());
        }});}
});

}

public void ProcesarCaptura(DPFPSample sample)
{
    // Procesar la muestra de la huella y crear un conjunto de características con el propósito de inscripción.
    featuresinscripcion = extraerCaracteristicas(sample, DPFPSDataPurpose.DATA_PURPOSE_ENROLLMENT);
    // Procesar la muestra de la huella y crear un conjunto de características con el propósito de verificación.
    featuresverificacion = extraerCaracteristicas(sample, DPFPSDataPurpose.DATA_PURPOSE_VERIFICATION);

    // Comprobar la calidad de la muestra de la huella y lo añada a su reclutador si es bueno
    if (featuresinscripcion != null)
        try{
            System.out.println("Las Caracteristicas de la Huella han sido creada");
            Reclutador.addFeatures(featuresinscripcion);// Agregar las características de la huella a la plantilla a
crear
            // Dibuja la huella dactilar capturada.
            Image image=CrearImagenHuella(sample);
            DibujarHuella(image);
            btnIdentificar.setEnabled(true);
        }catch (DPFPImageQualityException ex) {
            System.err.println("Error: "+ex.getMessage());
        }
    }
}

```

```

}
finally {
    EstadoHuellas();
    // Comprueba si la plantilla se ha creado.
    switch(Reclutador.getTemplateStatus())
    {
        case TEMPLATE_STATUS_READY: // informe de éxito y detiene la captura de huellas
            stop();
            setTemplate(Reclutador.getTemplate());
            EnviarTexto("La Plantilla de la Huella ha Sido Creada, ya puede Verificarla o Identificarla");
            btnIdentificar.setEnabled(false);
            break;
        case TEMPLATE_STATUS_FAILED: // informe de fallas y reiniciar la captura de huellas
            Reclutador.clear();
            stop();
            EstadoHuellas();
            setTemplate(null);
            JOptionPane.showMessageDialog(registro_salida.this, "La Plantilla de la Huella no pudo ser
creada, Repita el Proceso", "Inscripcion de Huellas Dactilares", JOptionPane.ERROR_MESSAGE);
            start();
            break;
    }
}
}

public DPFPPFeatureSet extraerCaracteristicas(DPFPSample sample, DPFPPDataPurpose purpose){
    DPFPPFeatureExtraction extractor = DPFPPGlobal.getFeatureExtractionFactory().createFeatureExtraction();
    try {
        return extractor.createFeatureSet(sample, purpose);
    } catch (DPFPImageQualityException e) {
        return null;
    }
}

public void identificarHuella() throws IOException{
    try {
        //Establece los valores para la sentencia SQL

```

```

Connection c=con.conectar();

//Obtiene todas las huellas de la bd
PreparedStatement identificarStmt = c.prepareStatement("SELECT * FROM somhue");
ResultSet rs = identificarStmt.executeQuery();

//Si se encuentra el nombre en la base de datos
while(rs.next()){
//Lee la plantilla de la base de datos
byte templateBuffer[] = rs.getBytes("huehuella");
//String id=rs.getString("ID");
int id=rs.getInt("ID");
String nombre=rs.getString("huenombre");
//Crea una nueva plantilla a partir de la guardada en la base de datos
DPFPTemplate referenceTemplate =
DPFPGlobal.getTemplateFactory().createTemplate(templateBuffer);
//Envia la plantilla creada al objeto contendor de Template del componente de huella digital
setTemplate(referenceTemplate);
// Compara las caracteriticas de la huella recientemente capturda con la
// alguna plantilla guardada en la base de datos que coincide con ese tipo
DPFPVerificationResult result = Verificador.verify(featuresverificacion, getTemplate());
//compara las plantilas (actual vs bd)
//Si encuentra correspondencia dibuja el mapa
//e indica el nombre de la persona que coincidió.
if (result.isVerified()){
// obtener fecha
java.util.Date utilDate = new java.util.Date(); //fecha actual
long lnMilisegundos = utilDate.getTime();
java.sql.Date sqlDate = new java.sql.Date(lnMilisegundos);
java.sql.Time sqlTime = new java.sql.Time(lnMilisegundos);
java.sql.Timestamp sqlTimestamp = new java.sql.Timestamp(lnMilisegundos);
//crea la imagen de los datos guardado de las huellas guardadas en la base de datos
JOptionPane.showMessageDialog(null, "La huella capturada es de "+nombre,"Verificacion de Huella",
JOptionPane.INFORMATION_MESSAGE);
JOptionPane.showMessageDialog(null, "La fecha es: " +sqlDate);

```

```

JOptionPane.showMessageDialog(null, "La hora es: " +sqlTime);
//actualizar datos
identificarStmt.executeUpdate("UPDATE registros SET salida='"+sqlTime+"' WHERE
fecha='"+sqlDate+"'");
//-----
return;
    }
}
//Si no encuentra alguna huella correspondiente al nombre lo indica con un mensaje
JOptionPane.showMessageDialog(null, "No existe ningún registro que coincida con la huella",
"Verificacion de Huella", JOptionPane.ERROR_MESSAGE);
setTemplate(null);
} catch (SQLException e) {
//Si ocurre un error lo indica en la consola
System.err.println("Error al identificar huella dactilar."+e.getMessage());
}finally{
con.desconectar();
}
}

```

Anexo 6.6

```

principal
//definimos el inicio del documento HTML
<html>
//colocamos el fondo indicando la dirección de la imagen y definimos el cuerpo de la //pagina
<body background="images/fondos_linux_20120121_2052451166.jpg" bgProperties="fixed">
//esto permite colocar el título a la pestaña del navegador web
<title>Control de asistencia</title>
//colocamos etiquetas para dar forma a la página web con algunas configuraciones //como tamaño,
posición y color.
<div id="text1" style="position:absolute; overflow:hidden; left:420px; top:137px; width:385px; height:41px;
z-index:0"><div class="wpmid">
<div><font class="ws28" color="#000000"><B><I>Control de asistencia</I></B></font></div>

```

```

</div></div>
//esto nos permite colocar imagines y configurarlas con tamaño y posición.
<div id="image2" style="position:absolute; overflow:hidden; left:879px; top:37px; width:223px;
height:87px; z-index:1">
</div>
//esto nos permite colocar imagines y configurarlas con tamaño y posición.
<div id="image1" style="position:absolute; overflow:hidden; left:116px; top:38px; width:219px;
height:95px; z-index:14">
</div>
//colocamos etiquetas para dar forma a la página web con algunas configuraciones //como tamaño,
posición y color.
<div id="text2" style="position:absolute; overflow:hidden; left:192px; top:245px; width:290px; height:35px;
z-index:2"><div class="wpmd">
<div><font class="ws14">Revisar asistencia por trabajador:</font></div>
</div></div>
//colocamos un cuadro de texto donde el administrador colocara los datos //correspondientes para hacer
la consulta.
<div id="text3" style="position:absolute; overflow:hidden; left:192px; top:311px; width:75px; height:26px;
z-index:3"><div class="wpmd">
<div><font class="ws14">Nombre:</font></div>
</div></div>

//colocamos un cuadro de texto donde el administrador colocara los datos //correspondientes para hacer
la consulta.
<div id="text4" style="position:absolute; overflow:hidden; left:191px; top:421px; width:42px; height:25px;
z-index:4"><div class="wpmd">
<div><font class="ws14">De:</font></div>
</div></div>
//colocamos un cuadro de texto donde el administrador colocara los datos //correspondientes para hacer
la consulta.
<div id="text5" style="position:absolute; overflow:hidden; left:511px; top:420px; width:53px; height:27px;
z-index:5"><div class="wpmd">
<div><font class="ws14">Hasta:</font></div>
</div></div>
//colocamos etiquetas para dar forma a la página web con algunas configuraciones //como tamaño,

```

posición y color.

```
<div id="text6" style="position:absolute; overflow:hidden; left:193px; top:372px; width:249px; height:30px; z-index:6"><div class="wpmd">
```

```
<div><font class="ws14">Revisar asistencia por fecha:</font></div>
```

```
</div></div>
```

//colocamos un cuadro de texto donde el administrador colocara los datos //correspondientes para hacer la consulta.

```
<div id="text7" style="position:absolute; overflow:hidden; left:504px; top:313px; width:63px; height:25px; z-index:7"><div class="wpmd">
```

```
<div><font class="ws14">Fecha:</font></div>
```

```
</div></div>
```

//este método nos permite crear un botón indicándole los datos que se van a tomar //y transferirlos a una nueva página web donde se utilizaran para realizar la //consulta a la base de datos y mostrar el reporte correspondiente.

```
<FORM action="uno.php" method="post">
```

```
<input name="defecha" type="text" style="position:absolute;width:200px;left:279px;top:419px;z-index:10" />
```

```
<input name="hastafecha" type="text" style="position:absolute;width:200px;left:568px;top:418px;z-index:11" />
```

```
<input type="submit" value="consultar" style="position:absolute;left:796px;top:418px;z-index:13" />
```

```
</FORM>
```

//este método nos permite crear un botón indicándole los datos que se van a tomar //y transferirlos a una nueva página web donde se utilizaran para realizar la //consulta a la base de datos y mostrar el reporte correspondiente.

```
<FORM action="trabajador.php" method="post">
```

```
<input name="nombre" type="text" style="position:absolute;width:200px;left:285px;top:313px;z-index:8" />
```

```
<input name="fechanombre" type="text" style="position:absolute;width:200px;left:567px;top:312px;z-index:9" />
```

```
<input type="submit" value="consultar" style="position:absolute;left:797px;top:311px;z-index:12">
```

```
</FORM>
```

//definimos el final del cuerpo de la pagina

```
</body>
```

//definimos el final del documento HTML

```
</html>
```

Anexo 6.7

```
<?php
//Conexion con mysql
$con = mysql_connect("localhost", "root", "*****");
if(!$con){die('ERROR DE CONEXION CON MYSQL: '.mysql_error());}
//Conexión con la base de datos
$db = mysql_select_db("huellas",$con);
if(!$db){die('ERROR DE CONEXION CON DB: '.mysql_error());}

//Ejecutamos la consulta que soliciata el nombre y la fecha
$sql = "SELECT huenombre, entrada, salida FROM somhue INNER JOIN registros ON registros.id=somhue.ID
WHERE fecha = ".$_POST['fechanombre']."' AND huenombre = ".$_POST['nombre']."'";
$resultado = mysql_query($sql);
//verificamos que no haya error
if(!$resultado){
echo "la consulta SQL contiene errores.".mysql_error();
exit();
}
else{
if($row=mysql_fetch_array($resultado)){
print "<table border=1>";
print "<tr><td>Nombre</td><td>Entrada</td><td>Salida</td></tr>";
do {
print"<tr><td>".$row["0"]."</td><td>".$row["1"]."</td><td>".$row["2"]."</td><td>";
}
while($row=mysql_fetch_array($resultado));
print"</table>";
}
else {
print "No hay registros en la base de datos";
}
}
?>
```

Anexo 6.8

```
<?php
//CONEXION CON MYSQL
$con = mysql_connect("localhost", "root", "*****");
if(!$con){die('ERROR DE CONEXION CON MYSQL: '.mysql_error());}
//CONEXION CON LA BASE DE DATOS
$db = mysql_select_db("huellas",$con);
if(!$db){die('ERROR DE CONEXION CON DB: '.mysql_error());}
//EJECUTAMOS LA CONSULTA QUE SOLICITA EL NOMBRE Y FECHA
//$sql = "SELECT huenombre, entrada, salida FROM somhue INNER JOIN registros ON
registros.id=somhue.ID WHERE fecha =".$_POST['fechanombre']."' AND huenombre
=".$_POST['nombre']."";
$sql = "SELECT huenombre, entrada, salida FROM somhue INNER JOIN registros ON registros.id=somhue.ID
WHERE fecha BETWEEN '".$_POST['defecha']."' AND '".$_POST['hastafecha']."";
$resultado = mysql_query($sql);
//verificamos que no haya error
if(!$resultado){
echo "la consulta SQL contiene errores.".mysql_error();
exit();
}
else{
if($row=mysql_fetch_array($resultado)){
print "<table border=1>";
print "<tr><td>Nombre</td><td>Entrada</td><td>Salida</td></tr>";
do {
print"<tr><td>".$row["0"]."</td><td>".$row["1"]."</td><td>".$row["2"]."</td><td>";
}
while($row=mysql_fetch_array($resultado));
print"</table>";
}
else {
print "No hay registros en la base de datos";
}
}
```

```
}  
?>
```

Anexo 6.9

Manual de usuario

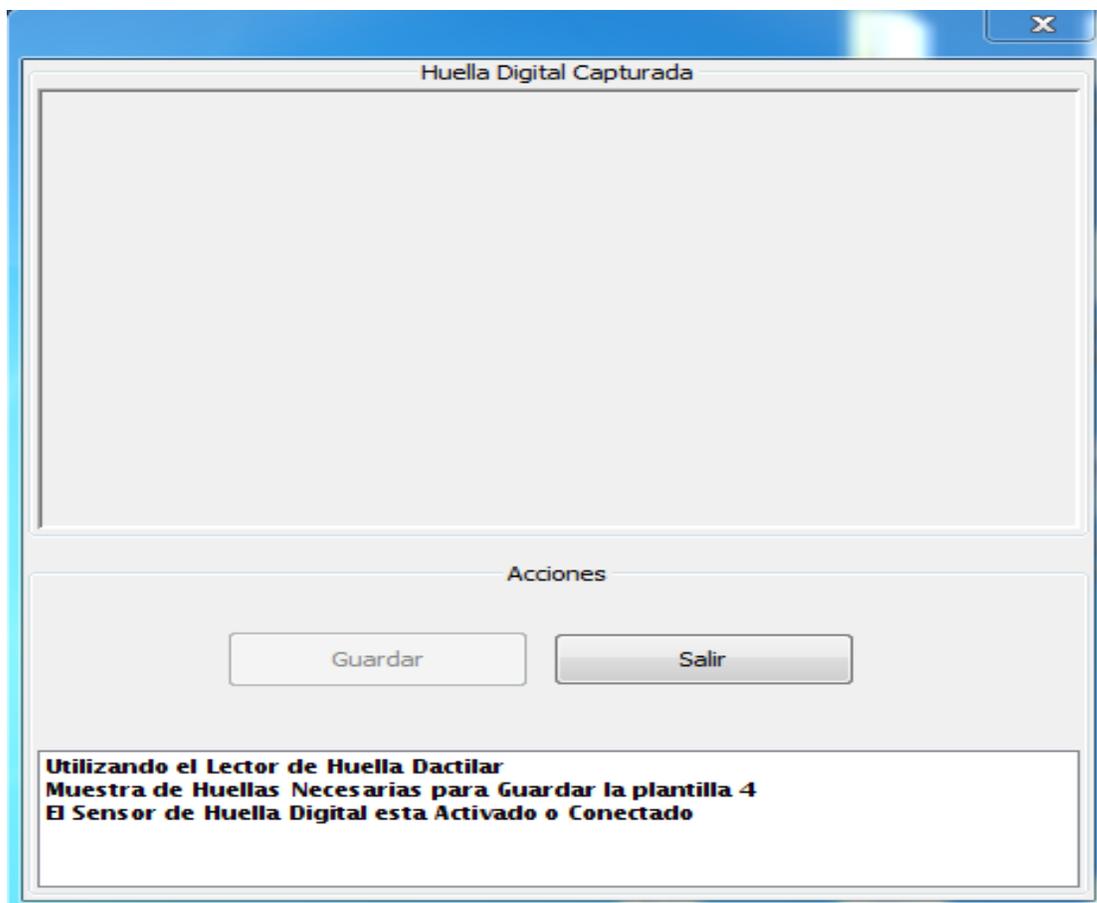
Comenzaremos abriendo la aplicación desde el escritorio con el siguiente icono



Con esto se abrirá la aplicación la cual nos permitirá elegir varias opciones

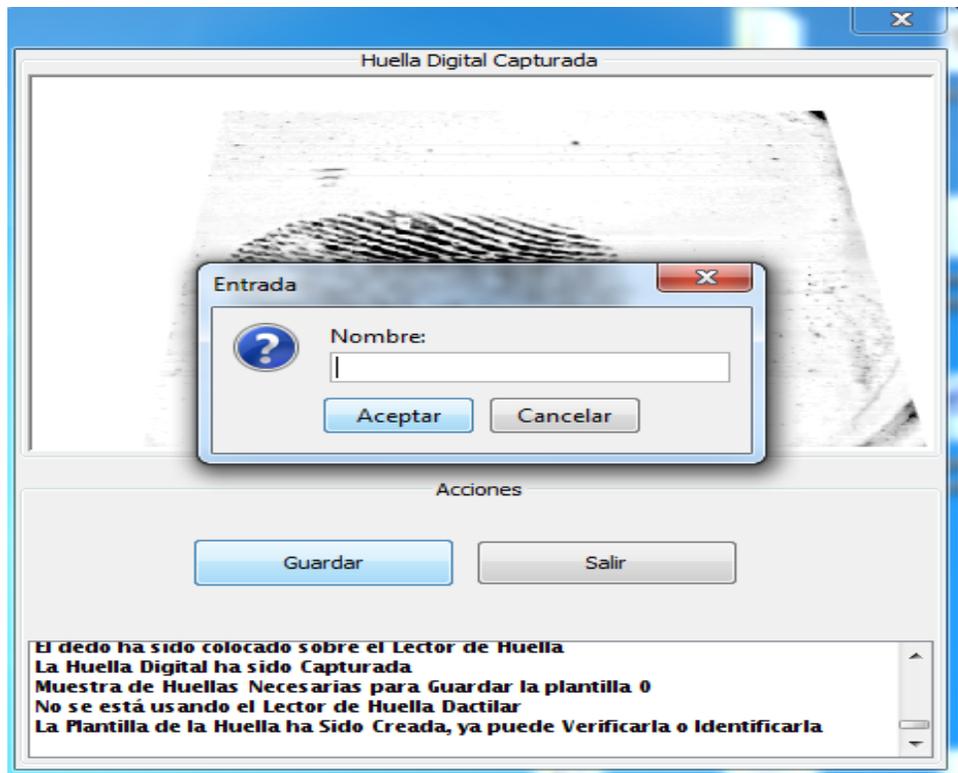


Para poder realizar el registro de los trabajadores se accede a la opción Nuevo registro la cual nos llevara a la siguiente pantalla

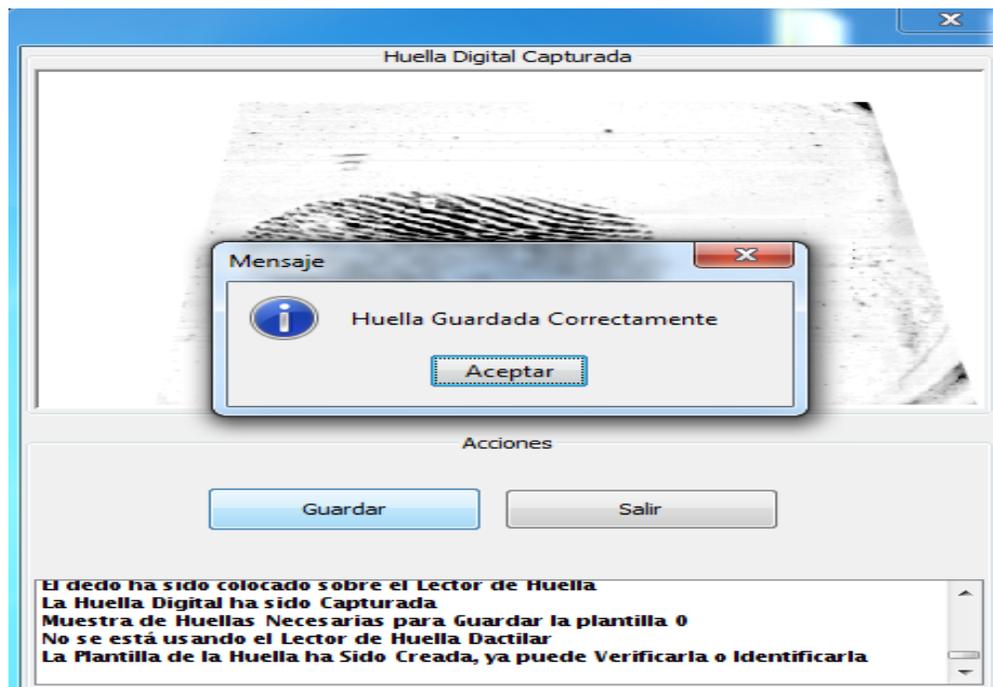


Esta pantalla nos indicara cuantas capturas de huellas se necesitan para generar la plantilla y guardarla en la base de datos

Una vez generada la plantilla nos pedirá el nombre del trabajador para asignarla a la plantilla

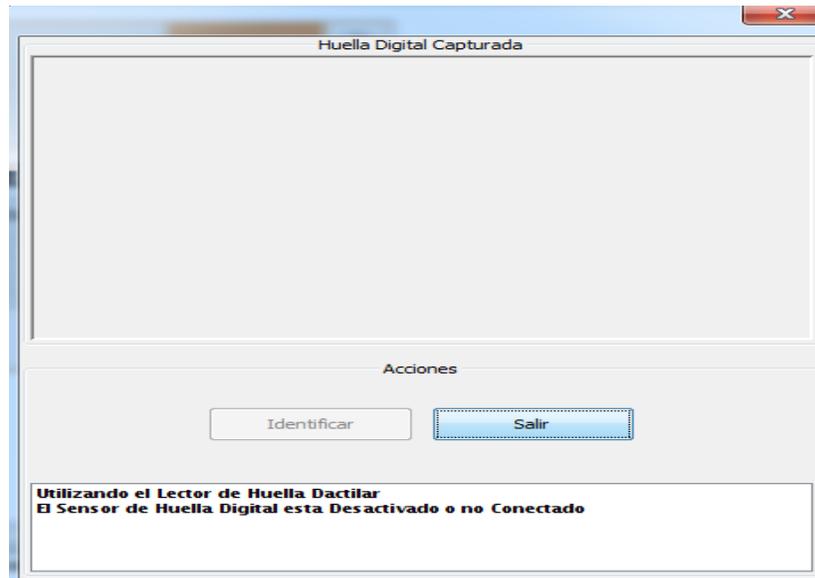


Ya realizado esto nos mandara una notificación que la huella fue guardada exitosamente

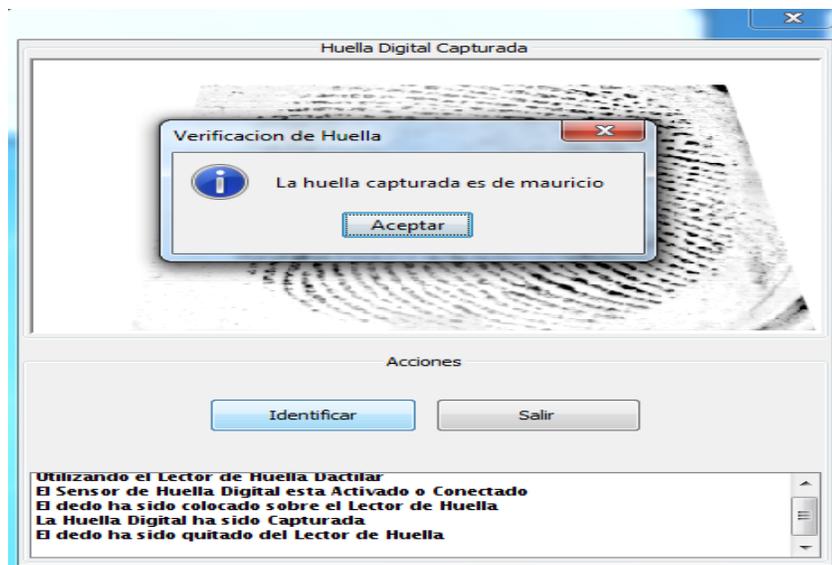


Después se procede a presionar el botón salir para regresar al menú principal.

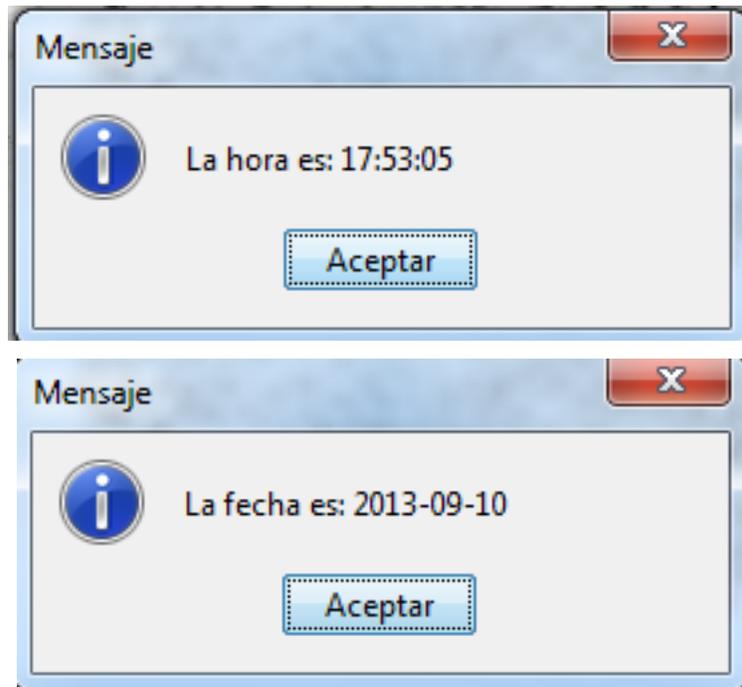
Para el registro de entrada y salida en el menú principal tenemos la opción de cada una en estos apartados el procedimiento es el mismo nos aparecerá la siguiente pantalla:



En la cual pondremos nuestro dedo sobre el lector tomara la imagen y la comparara con la de las bases de datos para obtener el registro



El siguiente paso nos manda una notificación de la fecha y hora las cuales quedaran guardadas en el registro



Después se procede a presionar el botón ACEPTAR para regresar al menú principal

BIBLIOGRAFÍA

1. **John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins.** *Biometrics*. new york : McGraw Hill Osborne, 2003.
2. **Bolle, Nalini Ratha and Ruud.** *Automatic Fingerprint Recognition Systems* . New York : Springer, 2004.
3. **Wayman, James.** *Biometric Systems Technology, Design and Performance Evaluation*. London : Springer, 2005.
4. **Maltoni, Davide, Maio, Jain, and Prabhakar.** *Handbook of Fingerprint Recognition*. New York : Springer, 2005.
5. **Agustín Alvarez, Vicente López.** <http://www.tekhnosur.com>. [En línea] 2013. http://www.tekhnosur.com/index.php?option=com_content&view=article&id=118&Itemid=11.
6. **López, Luis Eduardo Morán.** Sistema de Detección de Huella Digital. *Sistema de Detección de Huella Digital*. Coquimatlan : s.n., 2002.
7. **Sosa, Juventino Montiel.** *Criminalística tomo 2*. México, D.F : Limusa, 2001.
8. **UNAM.** *UNAM - Facultad de Ingeniería*. [En línea] 11 de marzo de 2011. <http://redyseguridad.fi-p.unam.mx/proyectos/biometria/bibliografia.html>.
9. **Martinez, Arminda Reyes.** Dactiloscopia y otras tecnicas de identificacion. Argentina : porrua.
10. **Leticia, Estrada Brenda.** *Autenticacion Biometrica Como Sistema De Seguridad*. 2013.
11. **Ecured.** Sistemas Biométricos. [En línea] julio de 2013. <http://www.ecured.cu/index.php/Biometr%C3%ADa>.
13. **digitalPerson.** [En línea] 2012. <http://devportal.digitalpersona.com/portal.php>.
14. **Intoducción a xhtml.** [aut. libro] Javier Eguluz. *Intoducción a xhtml*. 2013.
15. **PHP.** php. [En línea] 2013. <http://php.net/manual/es/history.php.php>.

GLOSARIO

FingerPrint.- Huella digital

Templates.- Plantillas

Query.- Consulta, Pregunta, averiguación

Driver.- Software utilizado en el sistema operativo Windows para crear la interfaz de control de algún dispositivo hardware conectado a la computadora.

OCX.- Un objeto que se expone a otras aplicaciones o herramientas de programación mediante interfaces de Automatización.

Biometría.- La biometría analiza y mide ciertas características unívocas de un individuo para crear un identificador biométrico el cual puede ser almacenado en una base de datos y recuperado para su comparación con un ejemplo vivo con las mismas características.

AFIS.- Sistema automatizado de identificación de huellas digitales

DPI.- Puntos por pulgada

Enrollment.- Matricula

Integer.- Tipo de dato entero

Varchar.-Código de longitud variable

Blob.- Objetos binarios grandes

HTML.- Lenguaje de marcado hipertextual

Php.- Pre-procesador de hipertexto

Www.- World Wide Web

Command.- Patrón de comportamiento