



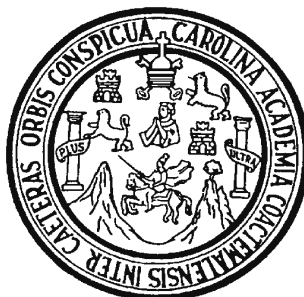
Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

TECNOLOGÍA BIOMÉTRICA

Blanca Cecilia Castillo Marroquín
Asesorada por: Inga. Floriza Ávila Pesquera

GUATEMALA, ABRIL DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA
TECNOLOGÍA BIOMÉTRICA

TRABAJO DE GRADUACIÓN
PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

BLANCA CECILIA CASTILLO MARROQUÍN

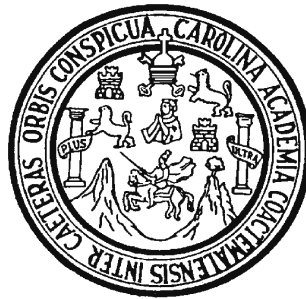
Asesorado por: Inga. Floriza Ávila Pesquera

AL CONFERÍRSELE EL TÍTULO DE
INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, ABRIL DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

| | |
|------------|--------------------------------------|
| DECANO | Ing. Sydney Alexander Samuels Milson |
| VOCAL I | Ing. Murphy Olympo Paiz Recinos |
| VOCAL II | Ing. Amahán Sánchez Álvarez |
| VOCAL III | Ing. Julio David Galicia Celada |
| VOCAL IV | Br. Kenneth Issur Estrada Ruiz |
| VOCAL V | Br. Elisa Yazminda Vides Leiva |
| SECRETARIO | Ing. Carlos Humberto Pérez Rodríguez |

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

| | |
|-------------|--------------------------------------|
| DECANO | Ing. Sydney Alexander Samuels Milson |
| EXAMINADOR | Ing. Ricardo Morales |
| EXAMINADORA | Inga. Elizabeth Domínguez |
| EXAMINADORA | Inga. Virginia Victoria Tala Ayerdi |
| SECRETARIO | Ing. Pedro Antonio Aguilar Polanco |

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

TECNOLOGÍA BIOMÉTRICA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha enero de 2003.

Blanca Cecilia Castillo Marroquín

Guatemala, noviembre de 2004

Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador de Privados y Revisión de Tesis
Escuela de Ciencias y Sistemas

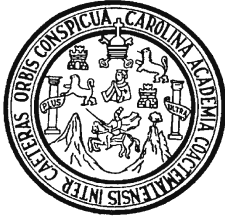
Estimado Ingeniero:

Por medio de la presente, me permito informarle que he asesorado el trabajo de graduación titulado: TECNOLOGÍA BIOMÉTRICA, elaborado por la estudiante Blanca Cecilia Castillo Marroquín, a mi juicio el mismo cumple con los objetivos propuestos para su desarrollo.

Agradeciéndole de antemano la atención que le preste a la presente, me suscribo de usted,

Atentamente,

Floriza Ávila Pesquera
Ingeniera en Ciencias y Sistemas
Asesora



El Director de la carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor, con el visto bueno del revisor de tesis y del licenciado en Letras, al trabajo de graduación titulado **TECNOLOGÍA BIOMÉTRICA**, presentado por la estudiante **Blanca Cecilia Castillo Marroquín**, aprueba el presente trabajo y solicita la autorización del mismo.

ID Y ENSEÑAD A TODOS

Ing. Luis Alberto Vettorazzi España
DIRECTOR
Ingeniería en Ciencias y Sistemas

Guatemala, marzo de 2005

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **TECNOLOGÍA BIOMÉTRICA**, presentado por la estudiante universitaria **Blanca Cecilia Castillo Marroquín** procede a la autorización para la impresión del mismo.

IMPRÍMASE:

Ing. Sydney Alexander Samuels Milsons
DECANO

Guatemala, abril de 2005

DEDICATORIA A

- Dios** Por la bendición que me da de poder cumplir la meta de graduarme.
- Mis padres** Ignacio Castillo Nova y Blanca Flor Marroquín de Castillo (Q.E.P.D), por el esfuerzo que hicieron para sacarnos siempre adelante.
- Mis abuelos** Tito de Jesús Castillo Guerra (Q.E.P.D) y Elvira Acevedo de Castillo, por su amor incondicional.
- Mis hermanos** José Ignacio Castillo Marroquín, Claudia Cecilia Castillo Marroquín (Q.E.P.D.), Nefi David Castillo Marroquín (Q.E.P.D), por su ejemplo.
- Mis amigos** Vicky Pérez, Luis Santizo, Mónica Dávila, Xiomara Vivar, Iván Reyes, Hervert de León, Betty Orozco y todos los demás con quienes he compartido y porque de cada uno de ellos he aprendido mucho.

AGRADECIMIENTOS

- A Dios** Por ser compañía constante e iluminarme siempre el camino.
- A mi padre** Por cuidar siempre de mí y por todas sus enseñanzas.
- A mi madre** Porque donde quiera que se encuentre sé que estará siempre a mi lado apoyándome.
- A mi asesora** Inga. Floriza Ávila Pesquera, por el apoyo y la confianza que puso en mí.
- A mis amigos** Por darme su sincera amistad y estar conmigo en tristezas y alegrías.
- A mis centros de estudio** Por la formación académica de mi persona.

ÍNDICE GENERAL

| | |
|---|------|
| ÍNDICE DE ILUSTRACIONES | V |
| GLOSARIO | VII |
| OBJETIVOS | IX |
| RESUMEN | X |
| INTRODUCCIÓN | XXII |
| | |
| 1. BIOMETRÍA | 1 |
| 1.1 Qué es biometría..... | 1 |
| 1.2 Tipos de tecnología biométrica..... | 3 |
| 1.2.1 Biometría estática..... | 3 |
| 1.2.2 Biometría dinámica..... | 4 |
| 1.3 Almacenamiento de un registro biométrico..... | 4 |
| 1.3.1 Sumisión..... | 4 |
| 1.3.2 Registro..... | 5 |
| 1.3.3 Dispositivo de captura..... | 5 |
| 1.4 Términos utilizados en tecnología biométrica..... | 6 |
| 1.4.1 Muestra biométrica..... | 6 |
| 1.4.2 Extracción de las características..... | 7 |
| 1.4.3 El patrón..... | 8 |
| 1.5 Proceso para la autenticación..... | 9 |
| 1.6 Arquitectura de los sistemas biométricos..... | 10 |
| | |
| 2. ALGUNOS TIPOS CONOCIDOS DE TECNOLOGÍA BIOMÉTRICA Y SUS APLICACIONES | 13 |
| 2.1 Biometría del tecleo..... | 13 |
| 2.1.1 El muestreo..... | 14 |
| 2.2 Verificación de la escritura..... | 15 |

| | |
|---|-----------|
| 2.2.1 Muestra..... | 15 |
| 2.3 Verificación de patrones oculares..... | 16 |
| 2.3.1 Iris..... | 16 |
| 2.3.2 Retina..... | 17 |
| 2.4 Geometría de la mano..... | 18 |
| 2.5 Reconocimiento de la voz..... | 19 |
| 2.5.1 Sensores para el reconocimiento de la voz..... | 20 |
| 2.6 Usos de la tecnología biométrica..... | 21 |
| | |
| 3. HUELLA DIGITAL..... | 23 |
| 3.1 Basadas en detalles..... | 24 |
| 3.2 Basadas en correlación..... | 25 |
| 3.3 Tipos de sensores para huellas dactilares..... | 26 |
| 3.3.1 Sensor de matriz capacitivo..... | 26 |
| 3.3.2 Sensor de matriz antena..... | 27 |
| | |
| 4. APLICACIÓN DE LA TECNOLOGÍA BIOMÉTRICA. SISTEMA DE CONTROL DE ACCESO A PERSONAL POR MEDIO DE LA HUELLA DIGITAL..... | 29 |
| 4.1 Descripción de la aplicación..... | 29 |
| 4.2 Requerimientos de <i>hardware</i> y <i>software</i> | 30 |
| 4.3 Análisis y diseño de la aplicación..... | 31 |
| 4.3.1 Modelo entidad-relación..... | 31 |
| 4.3.2 Descripción de las tablas utilizadas..... | 32 |
| 4.3.3 Codificación de las manos y los dedos..... | 34 |
| 4.3.4 Descripción de los algoritmos y diagramas de flujo..... | 35 |
| 4.3.4.1 Registro de empleados..... | 35 |
| 4.3.4.2 Modificación de datos de empleados..... | 36 |
| 4.3.4.3 Eliminación de empleados..... | 36 |

| | | |
|-----------|--|----|
| 4.3.4.4 | Consulta de empleados..... | 41 |
| 4.3.4.5 | Cambio de usuario administrador..... | 41 |
| 4.3.4.6 | Cambio de clave del administrador..... | 42 |
| 4.3.4.7 | Registro de huella..... | 47 |
| 4.3.4.8 | Comparación de huella..... | 48 |
| 4.3.4.9 | Eliminación de huella..... | 48 |
| 4.3.4.10 | Registro de acceso de los empleados..... | 54 |
| 4.3.4.11 | Reporte de empleados registrados..... | 56 |
| 4.3.4.12 | Reporte de huellas asociadas..... | 56 |
| 4.3.4.13 | Reporte de control de acceso de los empleados..... | 58 |
| 4.3.4.14 | Reporte de usuarios inválidos..... | 59 |
| 4.3.5 | Desarrollo de la aplicación..... | 62 |
| 4.3.5.1 | Arquitectura del reconocimiento de la huella digital..... | 64 |
| 4.3.5.2 | Descripción de los algoritmos para el dispositivo Biométrico..... | 65 |
| 4.4 | Funcionamiento del sistema..... | 70 |
| 4.4.1 | Registrar..... | 71 |
| 4.4.2 | El menú usuarios..... | 72 |
| 4.4.2.1 | Registro de usuarios..... | 72 |
| 4.4.2.2 | Modificación de usuarios..... | 73 |
| 4.4.2.3 | Eliminación de usuarios..... | 74 |
| 4.4.2.4 | Consulta de usuarios..... | 75 |
| 4.4.3 | El menú huellas..... | 75 |
| 4.4.3.1 | Registro de huella..... | 76 |
| 4.4.3.2 | Comparación de huella..... | 77 |
| 4.4.3.2 | Eliminación de huella..... | 78 |
| 4.4.4 | El menú administración..... | 78 |
| 4.4.4.1 | Cambio de usuario..... | 79 |
| 4.4.4.2 | Cambio de clave..... | 80 |
| 4.4.4.3 | Reportes..... | 80 |
| 4.4.4.3.1 | Usuarios registrados..... | 81 |

| | | |
|------------------------|--------------------------|-----------|
| 4.4.4.3.2 | Huellas asociadas..... | 81 |
| 4.4.4.3.3 | Control de acceso..... | 83 |
| 4.4.4.3.4 | Registros inválidos..... | 83 |
| CONCLUSIONES | | 85 |
| RECOMENDACIONES | | 87 |
| BIBLIOGRAFÍA | | 89 |

ÍNDICE DE ILUSTRACIONES

FIGURAS

| | | |
|-----|---|----|
| 1. | Arquitectura de un sistema biométrico..... | 11 |
| 2. | Lector biométrico para geometría de la mano..... | 19 |
| 3. | Micrófono óptico..... | 20 |
| 4. | Comparación entre dos plantillas de huella digital..... | 23 |
| 5. | Detalles de una huella digital..... | 24 |
| 6. | Sensor de matriz capacitivo..... | 26 |
| 7. | Sensor de matriz antena..... | 28 |
| 8. | Sensor biométrico de huella digital..... | 30 |
| 9. | Modelo entidad-relación de la aplicación..... | 31 |
| 10. | Diagrama de flujo de registro de empleados..... | 38 |
| 11. | Diagrama de flujo de modificación de empleados..... | 39 |
| 12. | Diagrama de flujo de eliminación de empleados..... | 40 |
| 13. | Diagrama de flujo de consulta de empleados..... | 44 |
| 14. | Diagrama de flujo de cambio de usuario administrador..... | 45 |
| 15. | Diagrama de flujo de cambio de usuario administrador..... | 46 |
| 16. | Diagrama de flujo de registro de huella..... | 50 |
| 17. | Diagrama de flujo de comparación de huella..... | 52 |
| 18. | Diagrama de flujo de eliminación de huella..... | 53 |
| 19. | Diagrama de flujo de registro de acceso de empleados..... | 55 |
| 20. | Diagrama de flujo de reporte de empleados..... | 57 |
| 21. | Diagrama de flujo de reporte de huellas asociadas..... | 58 |
| 22. | Diagrama de flujo de reporte de control de acceso..... | 60 |
| 23. | Diagrama de flujo de reporte de registros de inválidos..... | 61 |
| 24. | Arquitectura de un sistema de reconocimiento de huella digital..... | 64 |

| | | |
|-----|-----------------------------------|----|
| 25. | Menú principal..... | 70 |
| 26. | Registrar..... | 71 |
| 27. | Menú usuarios..... | 72 |
| 28. | Ingreso de datos..... | 73 |
| 29. | Modificación de usuarios..... | 74 |
| 30. | Eliminación de usuarios..... | 74 |
| 31. | Consulta de usuarios..... | 75 |
| 32. | Menú huellas..... | 76 |
| 33. | Registro de huella..... | 76 |
| 34. | Verificación de huella..... | 77 |
| 35. | Eliminación de huella..... | 78 |
| 36. | Menú de administración..... | 79 |
| 37. | Cambio de usuario..... | 79 |
| 38. | Cambio de clave..... | 80 |
| 39. | Menú de reportes..... | 81 |
| 40. | Usuarios registrados..... | 82 |
| 41. | Huellas asociadas..... | 82 |
| 42. | Control de acceso..... | 83 |
| 43. | Registros inválidos..... | 84 |
| 44. | Reporte de control de acceso..... | 84 |

TABLAS

| | | |
|------|---|----|
| I. | Tecnología biométrica y sus muestras..... | 6 |
| II. | Tabla de códigos para las manos..... | 34 |
| III. | Tabla de códigos para los dedos..... | 34 |

GLOSARIO

| | |
|----------------------|--|
| AC | Siglas de corriente alterna. Corriente que circula por y durante un tiempo en un sentido y después en sentido opuesto, volviéndose a repetir el mismo proceso en forma constante. |
| Algoritmo | Secuencia de pasos dados en la solución de un problema. |
| Amplificador | Son circuitos que se utilizan para aumentar el valor de la señal de entrada generalmente muy pequeña, y así obtener una señal a la salida con una forma mucho mayor a la señal de entrada. |
| Capacitancia | Valor de una tensión aplicada a un circuito electrónico y la intensidad que circula por el mismo. |
| Foto detector | Componente que convierte la luz en electricidad. |
| Minucia | Los puntos donde terminan o se bifurcan las líneas de una huella dactilar. |

| | |
|---------------------------|--|
| <i>Píxel</i> | Unidad de medida que expresa la capacidad de la pantalla de un monitor. El número de <i>píxeles</i> o puntos de una pantalla informa sobre su resolución. Cada imagen es el resultado de la luminiscencia de una determinada configuración y cantidad de estos puntos. |
| Periférico | Dispositivo conectado a la unidad central de proceso. Un teclado, un módem, un ratón, son periféricos. |
| Sistema biométrico | Sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal, que puede ser reconocida o verificada de manera automatizada. |
| USB | El llamado puerto USB (<i>Universal Serial Bus</i>) es un conector externo que llega a transferencias de 12 millones de <i>bits</i> por segundo. |

OBJETIVOS

◆ General

El objetivo general de esta investigación es dar a conocer algunas de las características y aplicaciones de la tecnología biométrica para que así más organizaciones puedan beneficiarse de las ventajas que brinda esta tecnología.

◆ Específicos

- 1) Proporcionar información que ayude a seleccionar y adquirir la tecnología que sea mas adecuada a las necesidades de una organización.
- 2) Describir conceptos y funcionalidades básicas de los diferentes tipos de tecnologías biométricas.
- 3) Diseño de una aplicación de acceso de control de personal utilizando la tecnología biométrica.

RESUMEN

La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento.

El siguiente trabajo contiene una descripción general de algunas técnicas biométricas así como el desarrollo de una aplicación de control de acceso de empleados mediante la huella digital.

El presente trabajo consta de cuatro capítulos. El primero de ellos describe conceptos fundamentales de la biometría. Dentro del mismo encontramos la definición de biometría y su clasificación. Asimismo, describimos los pasos a seguir para el almacenamiento de un registro biométrico y para la autenticación. También encontramos algunos términos utilizados dentro de esta tecnología, como lo son la muestra, el patrón y la extracción de características. Por último se describe la arquitectura de un sistema biométrico.

En el segundo capítulo se describen algunos tipos conocidos de tecnología biométrica como los son: biometría del tecleo, verificación de la escritura que se encuentra dentro de la biometría dinámica, verificación de patrones oculares, geometría de la mano, reconocimiento de voz dentro de la biometría estática. Adicionalmente encontramos los usos de esta tecnología.

En el tercer capítulo se analiza el tema de la huella digital, tecnología por la cual se desarrolló la aplicación también descrita en este trabajo. Se tratan temas como definición de la tecnología y los tipos de dispositivos que existen.

El último capítulo se enfoca en el desarrollo de una aplicación de control de acceso de empleados, utilizando como dispositivo biométrico un lector de huella digital. Se describe la aplicación, se realiza el análisis y diseño de la misma

incluyendo descripción de las estructuras, descripción de algoritmos y diagramas de flujo de los procedimientos utilizados en la aplicación, y se finaliza con la descripción del funcionamiento del sistema.

INTRODUCCIÓN

El concepto de biometría proviene de las palabras bio(vida) y metria (medida) por lo que con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona.

La biometría informática es la aplicación de técnicas biométricas en las cuales están involucradas técnicas matemáticas y estadísticas a las ciencias de los seres vivos, medicina, biología etc. El reconocimiento de formas, la inteligencia artificial, y el aprendizaje son ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométrica.

La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en la vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Este tipo de tecnología se basa en estas características para autenticar a la persona que requiere acceso.

Las técnicas biométricas se utilizan para la autenticación e identificación automática de personas en sistemas de seguridad informática, las cuales se basan en medir al usuario directa e indirectamente.

El presente trabajo describe algunos tipos de tecnologías biométricas, sus características, así como sus aplicaciones.

1. BIOMETRÍA

1.1 Qué es biometría

El concepto biometría proviene de las palabras bio y metria que significan vida y medida respectivamente, por lo que podemos definir la biometría como el estudio de identificación de personas mediante el uso de sus características físicas o su comportamiento.

Los seres humanos poseemos características propias que nos diferencian unos de otros. Por medio de un equipo biométrico podemos medir e identificar dichas características.

Un equipo biométrico posee capacidades para medir, codificar, comparar, almacenar y reconocer alguna característica propia de la persona, con un determinado grado de precisión y confiabilidad.

Los dispositivos biométricos tienen tres partes principales:

- Un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar.
- Una entidad para manejar aspectos como la comprensión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos.
- Una interfaz para las aplicaciones que los utilicen.

Los dispositivos biométricos no presentan riesgos en la salud o en la seguridad, no dejan marcas, no toman muestras físicas y requieren un mínimo contacto con el usuario. Tales dispositivos están diseñados pensando en la comodidad de éste, ya

que poseen una interfaz intuitiva para hacer fácil el uso de los mismos. En la mayoría de los casos los procesos biométricos son rápidos y simples.

Actualmente, muchas de las aplicaciones de autenticación personal hacen uso de tarjetas o números de identificación personal, los cuales no poseen un nivel de seguridad aceptable ya que pueden ser utilizados por otras personas al llegar a tener acceso a ellos.

Las técnicas de identificación biométrica tienen la ventaja que los patrones no pueden perderse o ser utilizados por otros individuos.

La identificación biométrica puede proveer un control eficiente y preciso de las personas, se puede saber con un alto grado de exactitud que la persona que utilizó un dispositivo biométrico es la persona a ser reconocida, a diferencia de una firma, código de barras, clave de acceso u otro medio similar.

La identificación biométrica provee un registro real de la identidad de una persona, eliminando así la posibilidad de que ésta tenga acceso a lugares a los que no tienen autorización o que sea suplantada, pudiendo así generar algún tipo de fraude con un falso registro.

La combinación de los últimos avances en biometría y en electrónica ha permitido el desarrollo de las más modernas soluciones de identificación biométrica.

Muchos productos biométricos ya se han desplazado en la industria y han tenido resultados efectivos en la identificación y autenticación. La tecnología biométrica está comenzando a ser la fundación de un extenso conjunto de soluciones para verificación de personal y aplicaciones que requieren un alto grado de seguridad.

Diferentes aplicaciones de biometría están siendo utilizadas para proveer transacciones financieras confidenciales y proveen privacidad en los datos. La

necesidad de la utilización de tecnología biométrica puede ser encontrada en gobiernos, aplicaciones comerciales, etc.

1.2 Tipos de tecnología biométrica

Ya que la biometría se basa tanto en características físicas como en el comportamiento, podemos diferenciar dos tecnologías de este tipo:

1.2.1 Biometría estática

Mide la anatomía del usuario, se basa en medidas y datos derivados de la medición directa de una parte del ser humano.

Dentro de esta clasificación, podemos encontrar:

- Huellas digitales
- Geometría de la mano.
- Análisis del iris.
- Análisis de la retina
- Reconocimiento facial, etc.

1.2.2 Biometría dinámica

Mide el comportamiento del usuario. Son sistemas orientados al reconocimiento o autenticación del usuario basados en la utilización de factores asociados al comportamiento del usuario: cómo se mueve, cómo articula los sonidos y, lo que es mas importante, cómo interactúa con el sistema en sí que lo esta intentando reconocer.

Dentro de esta clasificación, encontramos:

- Patrón de voz.
- Firma manuscrita o verificación de escritura.
- Dinámica del tecleo.
- Análisis gestual, etc.

1.3 Almacenamiento de un registro biométrico

Los sistemas biométricos obtienen los datos por medio de un dispositivo, ya sea de características físicas o del comportamiento y convierten dichos datos en patrones que se utilizan posteriormente para identificar a los usuarios.

Dicho proceso puede dividirse en:

1.3.1 Sumisión

Es el proceso a través del cual se obtienen los datos necesarios del usuario. Dichos datos se obtienen dependiendo de la técnica biométrica que se esté utilizando. Si se trata de reconocimiento facial, se obtiene cuando el usuario mira en la dirección de la cámara, o si fuera por medio de huella digital, se obtiene colocando el dedo en la superficie del escáner.

1.3.2 Registro

Es el proceso a través del cual se extrae la muestra o muestras para ser valoradas y almacenadas siguiendo el proceso del sistema biométrico. Consiste en establecer una relación entre la muestra facilitada por el usuario, y los datos de identificación necesarios. Es decir, se asocia el patrón obtenido a una llave que identifique de quien es la muestra. Un ejemplo podría ser el patrón de la huella

digital reconocido por el dispositivo y el código único de la persona de quien se tomó la huella.

1.3.3 Dispositivo de captura

Es el *hardware* utilizado para capturar las muestras biométricas. Los siguientes dispositivos de captura están asociados a algunas tecnologías biométricas existentes:

Reconocimiento de la huella digital. Periférico de escritorio, ratón, *chip* o lector integrado en el teclado. Puede ser óptico o capacitivo.

Reconocimiento de la voz. Micrófono o teléfono.

Reconocimiento facial. Cámara de vídeo integrada en la computadora.

Lectura del iris. Cámara de vídeo de infrarrojos integrada en la computadora.

Lector de la firma. Bolígrafo sensible al movimiento. Tabla sensible al movimiento.

Reconocimiento de la forma de escribir en el teclado. Ubicado en la computadora o terminal móvil.

1.4 Términos utilizados en la tecnología biométrica

Definiremos a continuación algunos términos utilizados en la tecnología biométrica:

1.4.1 Muestra biométrica

Consiste en la característica física o del comportamiento captada durante la fase de sumisión que se utiliza para generar los patrones biométricos. El siguiente

cuadro ejemplifica los tipos de muestras asociados a algunas tecnologías biométricas existentes.

Tabla I. Tecnología biométrica y sus muestras

| Tecnología biométrica | Tipo de muestra |
|-------------------------------|---|
| Reconocimiento huella digital | Imagen de la huella digital |
| Reconocimiento de voz | Archivo de grabación de la voz |
| Reconocimiento facial | Imagen de la cara |
| Geometría de la mano | Imagen en 3D de la mano |
| Reconocimiento de firma | Imagen de la firma y grabación de los movimientos de la firma |
| Biometría del teclado | Grabación de caracteres utilizados y otras medidas relacionadas con la dinámica |

1.4.2 Extracción de las características

Es el proceso automático de codificación y almacenamiento de las características distintivas de la muestra biométrica, cuyo fin es generar el patrón de registro. El proceso de extracción de características puede incluir varios grados de imagen o de muestras procesadas para obtener una cantidad suficiente de datos precisos.

Por ejemplo, las tecnologías de reconocimiento de la voz pueden filtrar determinadas frecuencias y patrones, y las tecnologías de reconocimiento de la huella digital pueden comprimir las minucias presentes en la huella digital hasta el tamaño de un *píxel*.

Además, si la muestra es inadecuada para formar la extracción de la característica, el sistema biométrico ordenará al usuario que ofrezca otra muestra.

Las características físicas más comunes que se utilizan en el proceso de extracción son las siguientes:

- Reconocimiento de la huella digital. Localización y dirección del comienzo y fin de los arcos y bifurcaciones de la huella digital.
- Reconocimiento de la voz. Frecuencia, cadencia y duración del patrón de voz.
- Reconocimiento de la cara. Posición relativa y forma de la nariz, posición de las mejillas.
- Reconocimiento del iris. Forma del iris.
- Reconocimiento de la retina. Forma de los capilares de la retina
- Reconocimiento de la mano. Alto y ancho de los dedos y juntas entre los dedos y la mano.
- Reconocimiento de la firma. Rapidez, fuerza, presión y apariencia de la firma.
- Reconocimiento de la escritura en el teclado. Secuencia del tecleo, duración entre caracteres.

1.4.3 El patrón

Es un archivo comparativamente pequeño que se deriva de las características de una muestra o muestras del usuario, que se utiliza para obtener las correspondencias biométricas en el proceso de la comparación.

El patrón se crea por medio de un complejo proceso algorítmico que transforma las características diferenciales de la muestra. El concepto de patrón es uno de los elementos que definen la tecnología biométrica, a pesar de que no todos los sistemas biométricos utilizan patrones para realizar el proceso de comparación, puesto que algún sistema de reconocimiento de la voz utiliza la muestra original para realizar la comparación biométrica.

Dependiendo de cuándo hayan sido generados, los patrones pueden referirse a patrones de registro o de verificación.

- **Patrones de registro.** Se crean en la primera interacción del usuario con el sistema biométrico, y se almacenan para ser utilizados en futuras comparaciones.
- **Patrones de verificación.** Se generan durante los siguientes intentos de verificación, al comparar la característica con la almacenada en el patrón.

Se pueden utilizar múltiples muestras para generar el patrón de registro, el reconocimiento facial, por ejemplo, utilizará varias imágenes de la cara para generar el patrón de registro.

El patrón de verificación se deriva normalmente de una única muestra. Un patrón procedente de una única imagen facial se puede comparar con el patrón de registro para determinar el grado de similitud.

Los patrones biométricos no son interoperables, es decir, un patrón generado por un sistema del fabricante A no puede compararse con un fichero generado por un sistema B, aunque existen estándares para que se pueda realizar.

1.5 Proceso para la autenticación

Hemos definido ya el almacenamiento de un registro biométrico, ahora entraremos al proceso general de autenticación de los usuarios, es decir, la comparación de los datos almacenados en el registro con los datos obtenidos por los usuarios que se presentan al sistema.

Aunque cada tipo de tecnología biométrica lleva sus respectivos pasos, se puede definir algunos comunes a todos los modelos de autenticación biométrica:

- **Captura.** Lectura de los datos que el usuario a validar presenta.
- **Extracción.** Obtención de ciertas características de la muestra.
- **Comparación.** Se toman los datos almacenados en la base de datos y se comparan con los que el usuario esta presentando.
- **Decisión.** Se analiza si el usuario es válido o no.

1.6 Arquitectura de los sistemas biométricos

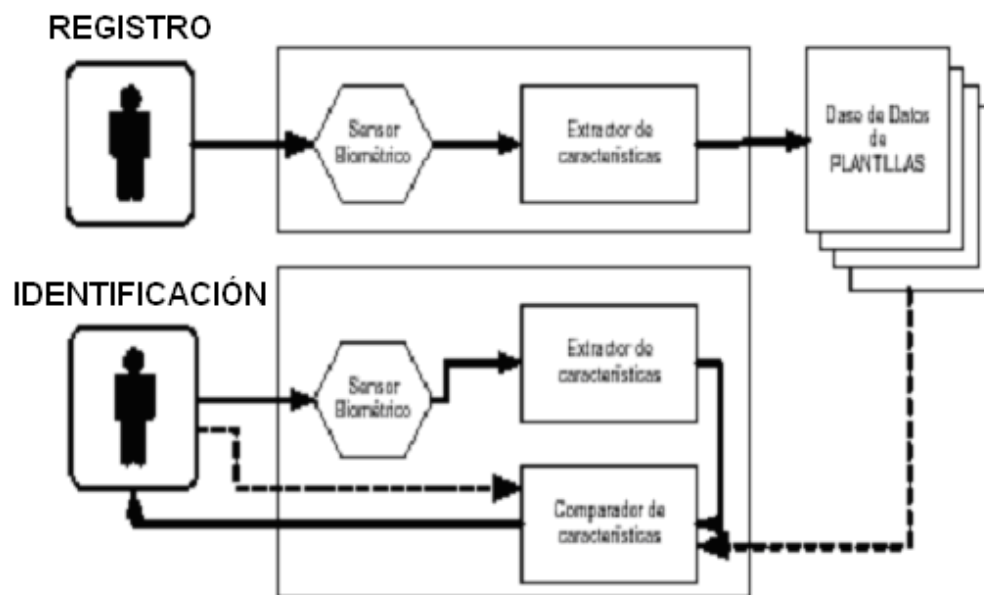
La arquitectura de un sistema biométrico típico refleja esencialmente la arquitectura de un sistema de reconocimiento de patrones:

- Se adquiere un patrón usando sensores.
- Se extrae una representación de la entrada adquirida usando un algoritmo de extracción de características.

- Se toma una decisión basada en la representación de entrada y la representación del patrón previamente almacenado en el sistema.

La figura a continuación muestra a grandes rasgos la arquitectura del sistema biométrico.

Figura 1. Arquitectura de un sistema biométrico



Fuente: Arquitectura general de un sistema biométrico

El sistema principalmente consiste de dos módulos:

- Registro
- Autenticación

La función del módulo de registro asocia la identidad de las personas registradas con representaciones de su medida biométrica. Cuando la señal biométrica y el nombre de la persona a ser registrada son alimentados al módulo de registro, un algoritmo de extracción de características (por ejemplo, minucias de

huellas dactilares) es aplicado al dato biométrica (por ejemplo, imagen de huella dactilar) y una representación de las características biométricas o patrones son extraídas y almacenadas en la base de datos del sistema.

El módulo de identificación autentifica la identidad de las personas que intentan acceder al sistema. La persona a ser autenticada indica su identidad y presenta su característica biométrica al sistema; el sensor biométrico captura el dato biométrico de entrada; se extraen las características biométricas capturadas y éstas son comparadas con la representación de la característica biométrica de la persona almacenada en la base de datos del sistema para verificar la identidad reclamada por la persona.

Un sistema de identificación determina la identidad asociada con la medida biométrica sin que la persona tenga que declarar su identidad.

2. ALGUNOS TIPOS CONOCIDOS DE TECNOLOGÍA BIOMÉTRICA Y SUS APLICACIONES

2.1 Biometría del tecleo

La biometría del tecleo se encuentra dentro del área de la biometría dinámica, sistemas basados en la utilización de factores no estáticos, y factores asociados al comportamiento del usuario.

El principal mecanismo de interacción de un humano con una computadora es el teclado, aunque existen otros medios de interacción con también muy comunes hoy día, como lo es ratón, o incluso el micrófono, pero a pesar de todo el mayor porcentaje de información del usuario a la computadora viene del teclado, y además es un elemento de *hardware* que viene de fábrica con todos los ordenadores. Esto, como veremos, es una ventaja fundamental para un sistema de seguridad sobre Internet.

Así pues, aparece una rama de la biometría dedicada al estudio del reconocimiento del patrón de tecleo de un usuario, la biometría del tecleo, la cual se centra en las técnicas necesarias para identificar en qué medida existe una cierta regularidad en el modo de teclear de un usuario de un sistema informático.

El proceso de tecleo es un proceso realmente complejo y que trasciende el aspecto meramente físico, en tanto es una capacidad emergente que surge de la propia dinámica cerebral en su origen. Desde el cerebro generamos los estímulos necesarios que se transmiten por el sistema nervioso periférico hasta nuestros músculos que efectúan complejas contracciones y distensiones para presionar un centenar de teclas de una computadora, plasmando la información verbal que el cerebro está procesando en un momento determinado.

En este tipo de tecnología no se hace necesario tener *hardware* adicional para el muestreo de patrones, y esto lo hace ideal para aplicaciones sobre Internet.

2.1.1 El muestreo

La clave del muestreo en el caso de la biometría del tecleo consiste en generar un proceso de medición de los tiempos entre diferentes pulsaciones de teclas del usuario, y que esta medición sea independiente de la frecuencia del microprocesador de la máquina.

Algunas formas diferentes de muestrear el tecleo:

- **Con tiempo.** Consiste simplemente en utilizar un reloj para medir el tiempo, marcar el tiempo de una pulsación y el de la siguiente y ver la distancia entre las dos. Normalmente, la mayor precisión que nos dará el lenguaje que estemos utilizando será como mucho de centésimas de segundo. Esto no es suficiente precisión para detectar adecuadamente el tecleo del usuario como se puede observar haciendo unos sencillos programas que intenten medirlo así.
- **Con ciclos máquina con chequeo constante.** Los ciclos máquina son la mayor frecuencia de muestreo que podemos conseguir en el ordenador, usando esta frecuencia se puede medir con suficiente precisión distancias entre dos pulsaciones de teclas en una situación normal de tecleo del usuario. Con el chequeo constante se suman ciclos mientras el *buffer* de teclado esté vacío, chequeándolo constantemente.
- **Con ciclos máquina con disparos de evento.** Típicamente esta técnica usa programación *multithread* para con una pulsación de tecla arrancar un *thread* contador que acumula ciclos máquina hasta que de forma

asíncrona, y sin chequear constantemente el *buffer* de teclado, se para cuando lo corta otro por haberse producido un evento de pulsación de tecla.

2.2 Verificación de escritura

Aunque la escritura generalmente la firma no es una característica estrictamente biométrica, se suele agrupar dentro de esta categoría. El objetivo aquí no es interpretar o entender lo que el usuario escribe en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica.

En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas: el tiempo utilizado para hacer la firma, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo, etc.

2.2.1 Muestra

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de *aprendizaje*, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente.

Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él, se les solicita tal firma, con un número limitado de intentos. La firma introducida es capturada por un lápiz óptico o por una lectora sensible, o por ambos, y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

2.3 Verificación de patrones oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: analizan patrones retinales, o bien analizan el iris.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos: por un lado, a los usuarios no les resulta cómodo que un haz de rayos analice su ojo, y por otro lado un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas.

Otra de las desventajas es que son sistemas demasiado caros para la mayoría de organizaciones, y el proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevadas. De esta forma, su uso se ve reducido casi sólo a la identificación en sistemas de alta seguridad, como el control de acceso a instalaciones militares.

2.3.1 Iris

La tecnología biométrica del iris se basa en el análisis de rasgos encontrados dentro del anillo colorido del tejido que rodea a la pupila. El análisis del iris indudablemente es menos accesible a las biométricas relacionadas con el ojo, usa poco el elemento de la convencional de la cámara y no requiere contacto entre usuario y el lector.

Una propiedad que el iris comparte con las huellas dactilares es la morfología aleatoria de su estructura. No existe alteración genética en la expresión de este

órgano más allá de su forma anatómica, fisiología, color y apariencia general. La textura del iris por sí misma es estocástica o posiblemente caótica.

El propósito del reconocimiento del iris es obtener en tiempo real, con alto grado de seguridad, la identidad de una persona; empleando análisis matemático del patrón aleatorio que es visible dentro del ojo a cierta distancia.

Debido a que el iris es un órgano interno protegido con textura aleatoria, es decir, inmune a influencias ambientales, estable, él puede ser usado como una clave viva que no necesita ser recordada pero que siempre estará ahí.

El iris se ve afectado por la pupila cuando ésta reacciona a la luz. Las deformaciones elásticas que ocurren con la dilatación y contracción son rápidamente corregidas empleando algoritmos matemáticos que se encargan de localizar los bordes interno y externo del iris.

2.3.2 Retina

La tecnología biométrica de la retina está basada en el análisis de la capa de los vasos de sangre situada en la parte posterior del ojo. Esta técnica involucra el usar una fuente de luz de baja intensidad a través de un dispositivo óptico para examinar los modelos únicos de la retina.

En los sistemas de autenticación basados en patrones retinales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado, y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis.

En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para

compararlos con los almacenados en una base de datos. Si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

2.4 Geometría de la mano

Esta geometría consiste en el análisis y medida de la forma de la mano. Esta técnica podría ser conveniente donde hay más usuarios o donde los usuarios acceden el sistema frecuentemente.

La geometría de la mano es un método de autenticación por el cual el usuario pone su mano en un lector que tiene cuatro palos tipo alfileres. El usuario coloca su mano en el lector de tal manera que los alfileres paran el movimiento delantero adicional de la mano. El método de autenticación mide el grosor y la longitud de los dedos y la distancia entre ellos. Crea un algoritmo único que se guarda normalmente en una banda magnética de una tarjeta tipo tarjeta de crédito.

El usuario tiene que poner su mano directamente sobre el metal del lector, como se muestra en la figura 2. Es relativamente fácil de usar, aunque es fácil también obtener una lectura errónea si los dedos no están colocados de la manera correcta.

Figura 2. Lector biométrico para geometría de la mano



www.ingenieria.com

El dispositivo biométrico toma medidas de la mano del usuario a identificar, entre ellas la longitud, ancho, grosor y características de la superficie.

Se almacena la forma tridimensional de la mano de la silueta, el dispositivo revisa únicamente la estructura de la mano, no los detalles de la superficie, ignorando así las uñas, las huellas, líneas y polvo, compara la forma de la mano que se está escaneando con una plantilla guardada en la memoria del sistema, si la imagen escaneada y la plantilla concuerdan, el lector produce una señal de salida y da acceso a la persona.

2.5 Reconocimiento de voz

Generalmente se tiende a confundir este tipo de sistema con el de reconocimiento de palabras o interpretador de comandos hablado, las cuales existen comercialmente para ser integradas a una computadora personal.

Este reconocimiento de palabras no es biometría, ya que sólo está diseñado para reconocer palabras del interlocutor.

En un sistema para el reconocimiento de voz, se emplea la biometría física y de conducta con el objetivo de analizar patrones de habla e identificar al interlocutor. Para llevar a cabo esta tarea, el patrón creado previamente por el interlocutor debe ser digitalizado y mantenido en una base de datos que generalmente es una cinta digital de audio.

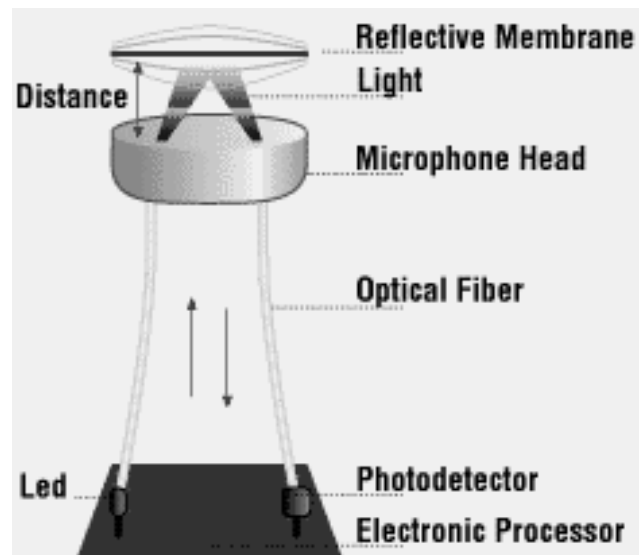
2.5.1 Sensores para el reconocimiento de voz

En algunos sistemas podemos encontrar los micrófonos ópticos unidireccionales, los cuales operan de la siguiente forma:

La luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra, cambiando así las características de la luz reflejada como lo indica en la figura 3.

Un foto-detector registra la luz reflejada que junto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido.

Figura 3. Micrófono óptico



Fuente: Sensores biométricos. http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIMETRICOS.html

2.6 Usos de la tecnología biométrica

Como todas las nuevas tecnologías, la investigación biométrica empezó por la necesidad de incrementar las herramientas de defensa del ejército, por ejemplo, el escáner de infrarrojos de diseño para detectar personas alrededor de un perímetro determinado.

Actualmente ya se han desarrollado algunas aplicaciones en el sector privado para el control de acceso de usuarios a computadoras personales, redes y terminales móviles, seguridad de acceso de trabajadores etc.

Algunas aplicaciones de los controles biométricos son:

- Control de accesos físicos
- Comercio electrónico
- Sistemas de salud
- Sistemas bancarios
- Control de horas laboradas por empleados
- Acceso a redes de computadores
- Sistemas electorales
- Acceso a datos de un archivo en una computadora personal
- Autorización a la utilización de datos personales.
- Aeropuertos
- Industria en general

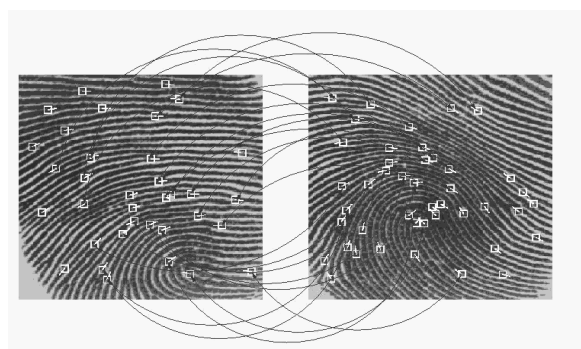
El acceso a los datos en una computadora personal es una de las aplicaciones más difundidas en el ámbito de la biometría. Casi todos los productores de sistemas biométricos proponen una solución para este acceso. Es suficiente conectar un lector biométrico y cargar un *software* adecuado, por lo que en el mercado hay una variedad de tipologías de lectores que generalmente tienden a parecerse a un *mouse* y a veces hasta están integrados en el teclado de la computadora.

3. HUELLA DIGITAL

Esta tecnología se encuentra dentro de la clasificación de la biometría estática. Se basa en identificar al individuo por medio de su huella dactilar, su funcionamiento se basa en tomar una imagen de la huella y por medio de algoritmos se reduce la imagen a una representación matemática llamada comúnmente plantilla. Ésta se almacena en una base de datos asociada a un número o clave de identificación personal.

Una huella dactilar es la representación de la epidermis de un dedo. Posee un conjunto de líneas que se intersectan y a veces terminan en forma abrupta. Los puntos donde éstas terminan o se bifurcan se conocen técnicamente como minucias. Si dos huellas dactilares corresponden o no a la misma persona, se lleva a cabo un procedimiento que comienza con la clasificación de la huella dactilar y termina con la comparación de las minucias de ambas huellas. La siguiente figura muestra el proceso de comparación entre dos patrones o plantillas de una huella digital.

Figura 4. Comparación entre plantillas



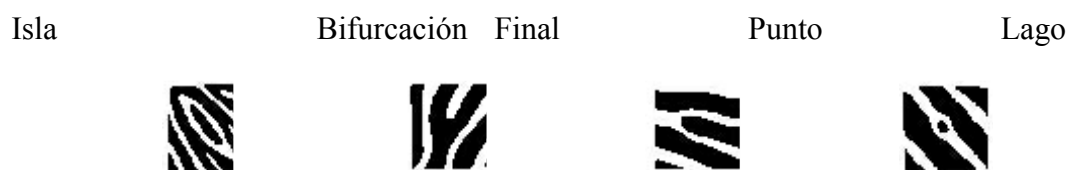
Fuente: Sensores Biométricos. http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIMETRICOS.html

Una huella puede ser determinada por dos tipos de patrones: el patrón de crestas y surcos, así como el de detalles.

3.1. Basadas en detalles

Esta técnica elabora un mapa con la ubicación relativa de detalles sobre la huella, los cuales permiten ubicar con certeza a un individuo. Sin embargo, existen algunas dificultades cuando se utiliza esta aproximación. Es muy difícil ubicar los detalles con precisión cuando la huella suministrada es de baja calidad. También este método no toma en cuenta el patrón global de las crestas y los surcos. En la figura 5 muestra algunos detalles que se pueden encontrar en una huella.

Figura 5. Detalles de una huella digital



Fuente: Sensores Biométricos. http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIMETRICOS.html

Cada individuo posee un solo arreglo de detalles, como se muestra en la figura, el cual puede ser descrito por un modelo de probabilidad:

$$P(C)=P(N).P(M).P(A)$$

Donde :

$P(C) = f(\text{Ley de Poisson})$

$P(M) = f(\text{frecuencia de aparición del detalle})$

$P(A) = f(\text{número de permutaciones posibles de detalles})$

3.2. Basadas en correlación

Esta técnica requiere de la localización precisa de un punto de registro, el cual se ve afectado por la rotación y traslación de la imagen.

Una vez obtenida la huella digital, es necesario clasificarla. Este proceso consiste en ubicar dicha huella dentro de los varios tipos existentes, los cuales proveen un mecanismo de indexado; esto se hace con la finalidad de reducir el tiempo de búsqueda. Los algoritmos existentes permiten clasificar la huella en cinco clases:

- Anillo de crestas.
- Lazo derecho.
- Lazo izquierdo.
- Arco.
- Arco de carpa.

Estos algoritmos separan el número de crestas presentes en cuatro direcciones (0° , 45° , 90° y 135°) mediante un proceso de filtrado de la parte central de la huella.

Dentro del proceso de reconocimiento es necesario emplear técnicas muy robustas que no se vean afectadas por algún ruido obtenido en la imagen, además de incrementar la precisión en tiempo real.

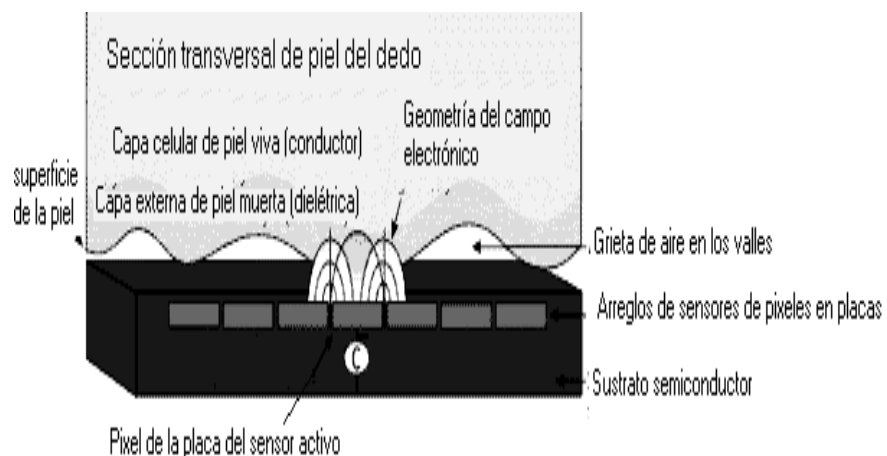
3.3 Tipos de sensores para huella dactilares

Existen dos tipos conocidos de sensores:

3.3.1 Sensor de matriz capacitivo

En la superficie de un circuito integrado de silicona se dispone un arreglo de placas de sensores capacitivos como lo muestra la figura 6. La capacitancia en cada *pixel* del sensor es medida individualmente, depositando una carga fija sobre ese *pixel*. El voltaje estático generado por esa carga es proporcional a la capacitancia del *pixel* y sus alrededores. Por la geometría del dedo, las líneas de flujo generadas desde el sensor energizado se inducen en la porción de piel inmediatamente adyacente a este sensor, terminando en sensores inactivos o en el sustrato.

Figura 6. Sensor de matriz capacitivo



Fuente: Sensores Biométricos. http://neutron.ing.ucv.ve/revista-No6/Olguin%20Patricio/SEN_BIMETRICOS.html

Una ventaja de este diseño es su simplicidad. Una desventaja es que debido a la geometría esférica del campo eléctrico generado por la placa del sensor, se puede tener un efecto de solapamiento sobre *pixel* vecinos, lo que producirá que el área sensora aumente en tamaño, trayendo como consecuencia un efecto de información cruzada entre los sensores adyacentes, reduciendo considerablemente la resolución de la imagen.

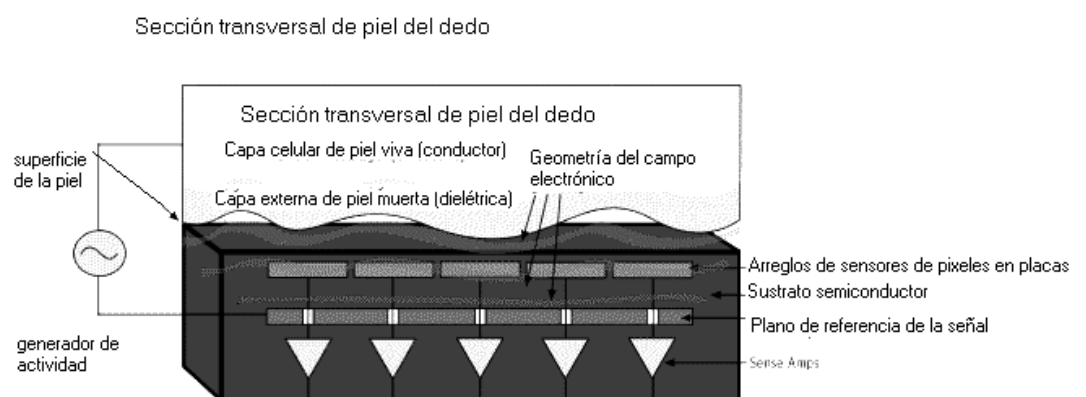
3.1.2 Sensor de matriz antena

Un pequeño campo RF (Radio Frecuencia) es aplicado entre dos capas conductoras, una oculta dentro de un *chip* de silicón llamado plano de referencia de la señal de excitación, y la otra localizada por debajo de la piel del dedo (ver figura 7.)

El campo formado entre estas capas reproduce la forma de la capa conductora de la piel en la amplitud del campo AC (Corriente Alterna). Diminutos sensores insertados por debajo de la superficie del semiconductor y sobre la capa conductora, miden el contorno del campo. Amplificadores conectados directamente a cada placa del sensor convierten estos potenciales a voltajes, representando el patrón de la huella.

Estas señales son acondicionadas en una etapa siguiente para luego ser multiplexadas fuera del sensor.

Figura 7. Sensor de matriz de antena



Fuente: Sensores Biométricos. http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIMETRICOS.html

4. APLICACIÓN DE LA TECNOLOGÍA BIOMETRICA: SISTEMA DE CONTROL DE ACCESO A PERSONAL POR MEDIO DE LA HUELLA DIGITAL

4.1 Descripción de la aplicación

La huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona.

El desarrollo de esta aplicación tiene como propósito llevar un control de acceso de empleados identificándolos por medio de la huella dactilar. Cada empleado tiene asociado un código que lo identifica al cual se le conoce como código de identificación personal.

Cuando un usuario desea autenticarse, ingresa su código de identificación personal en el sistema, colocando la yema del dedo en el sensor biométrico, el cual toma una imagen del dedo y extrae las minucias, las que posteriormente compara con el patrón almacenado en la base de datos cuyo registro esta identificado por el código de personal.

Si el patrón no corresponde, deniega el acceso al empleado ingresando un registro en la base de datos que se utiliza para tener un historial de usuarios que intentaron ingresar con un código y huella que no correspondía. Si coincide el patrón almacenado en la base de datos con el registro que se obtuvo, se autoriza la entrada almacenando un registro en la base de datos guardando el día y la hora de acceso, información que se utiliza para generación de reportes.

El proceso de almacenamiento del patrón de la huella de los empleados se realiza por medio de un algoritmo propio del fabricante del lector, solicitando la extracción de cuatro muestras de la huella y aplicando procesos matemáticos y estadísticos se genera dicho patrón el cual se asocia al código de identificación personal de cada usuario.

4.2 Requerimientos de *hardware* y *software*

- Sensor

El sensor utilizado para la captura de la huella digital es U.are.U de Digital Persona (véase figura 8). El sensor es un periférico ergonómico de computadora que es capaz de leer cualquier dedo, de la mano derecha o izquierda, en varios ángulos y grados de presión. El sensor incluye software para su instalación.

Figura 8. Sensor biométrico U.are.U 2000



- Procesador Pentium
- 64MB RAM
- Puerto USB
- Sistema operativo:

-Windows 98

-Windows Me

-Windows NT 4.0 (Service Pack 4.0 or menos)

-Windows 2000

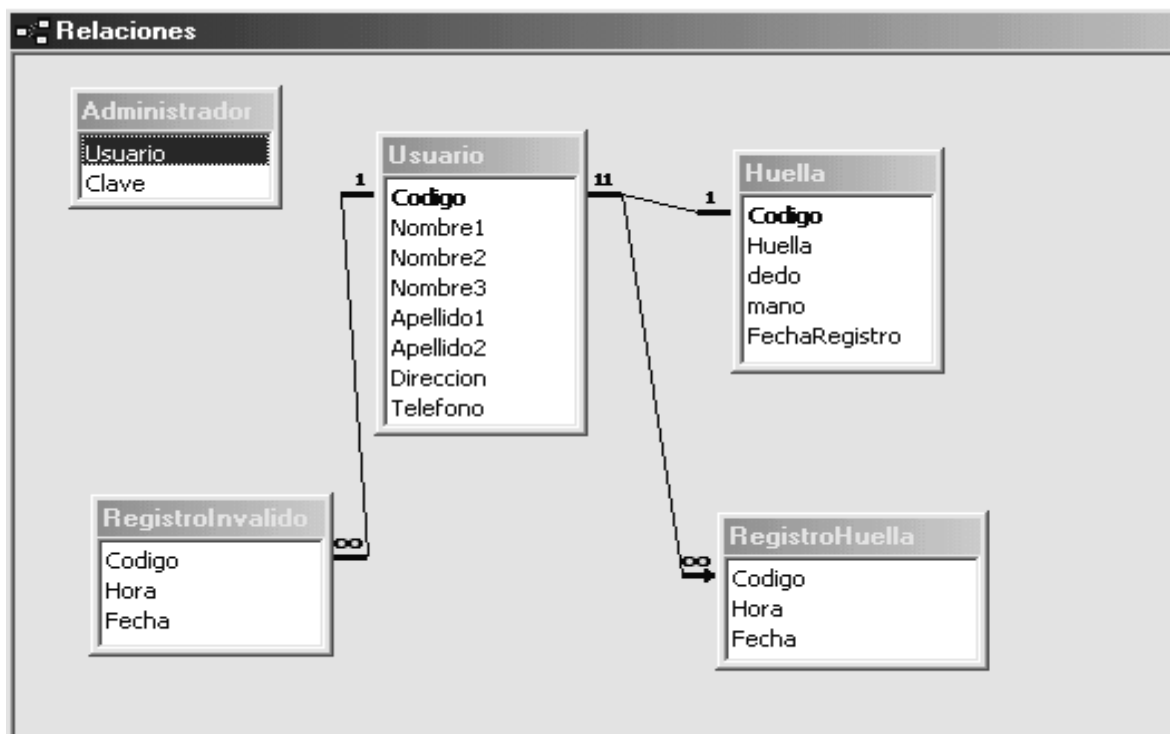
-Windows XP

4.3 Análisis y diseño de la aplicación

En esta sección describiremos el modelo entidad-relación, así como la descripción de cada una de las tablas y estructuras utilizadas.

4.3.1 Modelo entidad-relación

Figura 9. Modelo Entidad Relación de la aplicación



4.3.2 Descripción de las tablas utilizadas

Usuario. Se utiliza para almacenar los datos personales de los usuarios.

| CA MPO | DESCRIPCIÓN |
|-------------------|---|
| Código | Código de identificación personal de cada empleado. |
| Nombre1 | Almacena el primer nombre del empleado |
| Nombre2 | Almacena el segundo nombre del empleado. |
| Nombre3 | Almacena el tercer nombre del empleado. |
| Apellido1 | Almacena el primer apellido del empleado |
| Apellido2 | Almacena el segundo apellido del empleado |
| Dirección | Almacena la dirección del empleado |
| Teléfono | Almacena el número de teléfono del empleado. |

Huella. Almacena el registro de la huella del empleado asociada al código de identificación personal.

| CA MPO | DESCRIPCIÓN |
|-------------------|---|
| Código | Código de identificación personal de cada empleado. |
| Huella | Almacena el patrón de huella del empleado |
| Dedo | Almacena el código del dedo almacenado |
| Mano | Almacena el código de la mano almacenada. |
| “FechaRegistro” | Almacena la fecha en que fue almacenada la huella. |

“RegistroHuella”. Lleva el historial de acceso de los usuarios.

| CA MPO | DESCRIPCIÓN |
|-------------------------|---|
| Código | Código de identificación personal de cada empleado. |
| Hora | Almacena la hora de registro del usuario. |
| Fecha | Almacena la fecha de registro del usuario. |

“RegistroInvalido”. Lleva el historial de acceso de los usuarios que no estaban autorizados.

| CA MPO | DESCRIPCIÓN |
|-------------------------|---|
| Códi go | Código de identificación personal de cada empleado. |
| Hora | Almacena la hora de registro del usuario. |
| Fech a | Almacena la fecha de registro del usuario. |

Administrador. Almacena el usuario y la clave que se utiliza para registrar las huellas y emitir los reportes.

| CA MPO | DESCRIPCIÓN |
|-------------------------|--------------------------------------|
| <i>Login</i> | Usuario para acceder datos. |
| <i>Password</i> | Almacena la clave del administrador. |

4.3.3 Codificación de las manos y los dedos

Para la implementación de la aplicación se definieron ciertos códigos base especiales para el manejo de las huellas.

La mano y el dedo asociado a una huella que se almacena en la base de datos está codificado, como se muestra en las siguientes tablas:

Tabla II. Tabla de códigos para las manos

| DESCRIPCIÓN | CÓDIGO |
|--------------------|---------------|
| Derecha | 0 |
| Izquierda | 1 |

Tabla III. Tabla de códigos para los dedos

| DESCRIPCIÓN | CÓDIGO |
|--------------------|---------------|
| Pulgar | 0 |
| Índice | 1 |
| Medio | 2 |
| Anular | 3 |
| Meñique | 4 |

4.3.4 Descripción del los algoritmos y diagramas de flujo

A continuación describiremos los algoritmos utilizados en la aplicación.

4.3.4.1 Registro de empleados

Este algoritmo permite ingresar un empleado tomando como llave el código del mismo, y si dicho código no existe, se procede a ingresar los demás datos que posteriormente son almacenados en la base de datos. (Véase diagrama de flujo en la figura 10).

Procedimiento Registro_de_Empleado

Código ← Ingresar_Código

Busqueda_codigo(Código)

Si existe código:

Obtener(Primer nombre, segundo nombre, tercer nombre,

primer apellido, segundo apellido, dirección, teléfono)

Abrir_Tabla(Usuario)

Almacenar_Datos

Si no existe código: Mostrar_Mensaje_Error

Fin Procedimiento Registro_Usuario

4.3.4.2 Modificación de datos de empleados

Este algoritmo se utiliza para la modificación de los datos de un empleado tomando como llave el código del usuario. (Véase figura 11).

Procedimiento Modifica _ Empleado

Código ← Ingresar_Codigo

Abrir_Tabla(Usuario)

Busqueda_codigo(Código)

Si existe código :

Obtener(Primer Nombre,Segundo Nombre,Tercer Nombre,

Primer apellido,Segundo Apellido,Direccio,Telefono)

Actualizar_Datos

Si no existe código:

Mostrar_Mensaje_Error

Fin Procedimiento Modifica_Empleado

4.3.4.3 Eliminación de empleados

Un empleado se elimina tomando como llave el código de él. Si el empleado posee una huella asociada, se elimina. (Véase diagrama de flujo en figura 12).

Procedimiento Eliminar _Empleado

Código ← Ingresar_Codigo

Abrir_Tablas(Usuario,Huella)

Busqueda_codigo(Código)

Si existe código :

Buscar_huella(codigo)

Si existe_huella

Eliminar_huella

Eliminar_Empleado

Si no existe código:

Mostrar_Mensaje_Error

Fin Procedimiento Eliminar_Empleado

Figura 10. Diagrama de flujo de registro de empleados

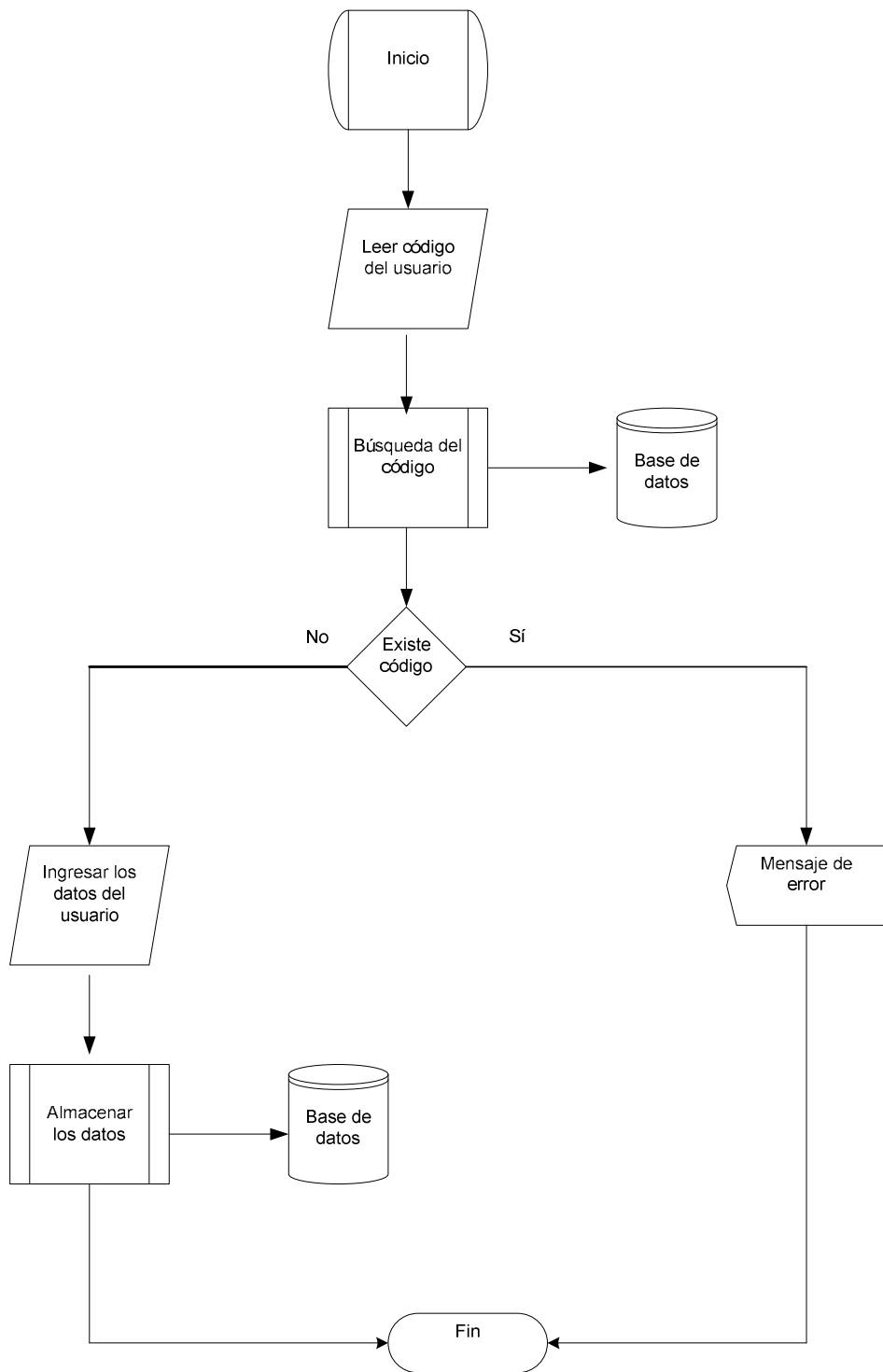


Figura 11. Diagrama de flujo de modificación de empleados

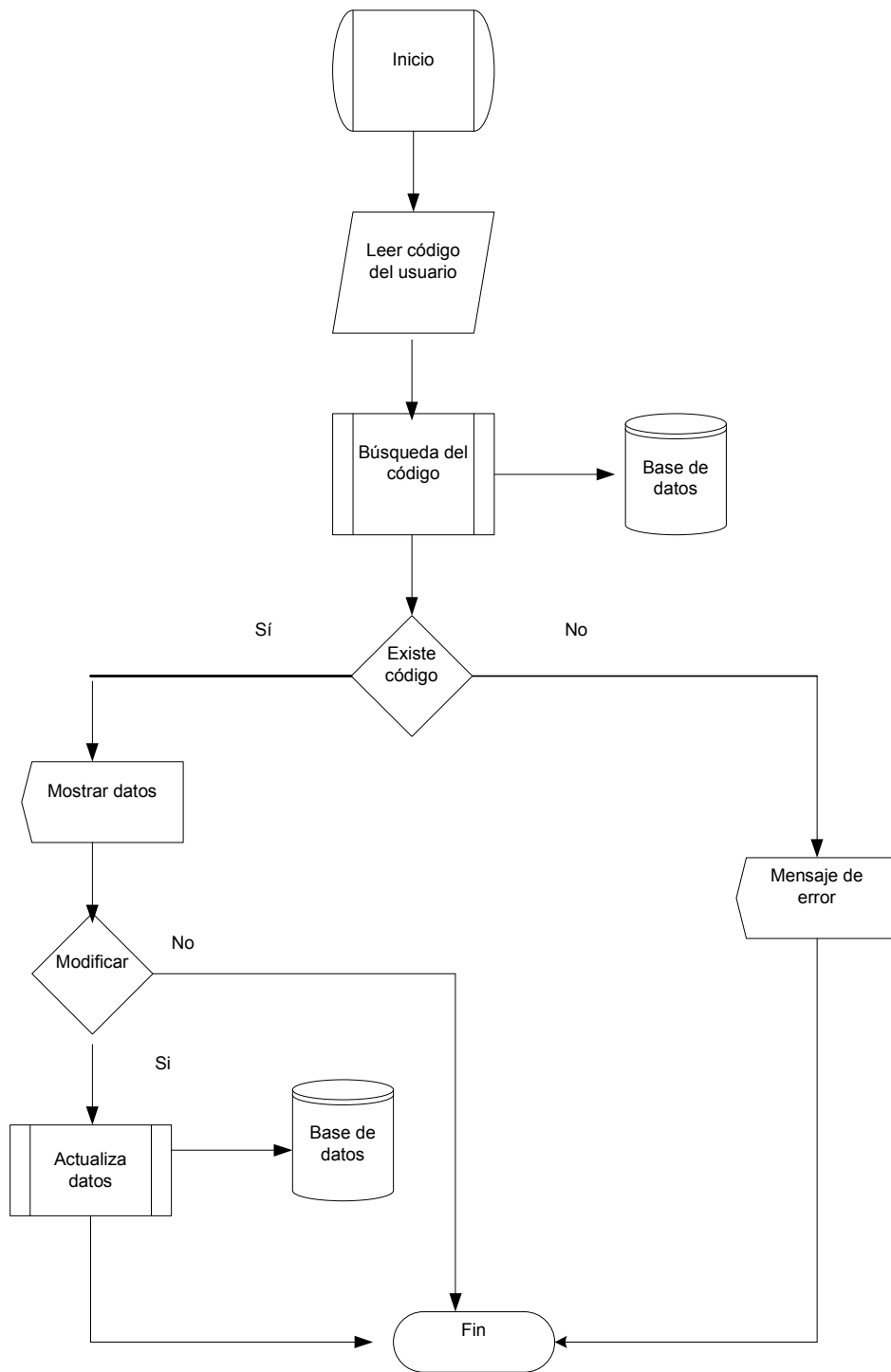
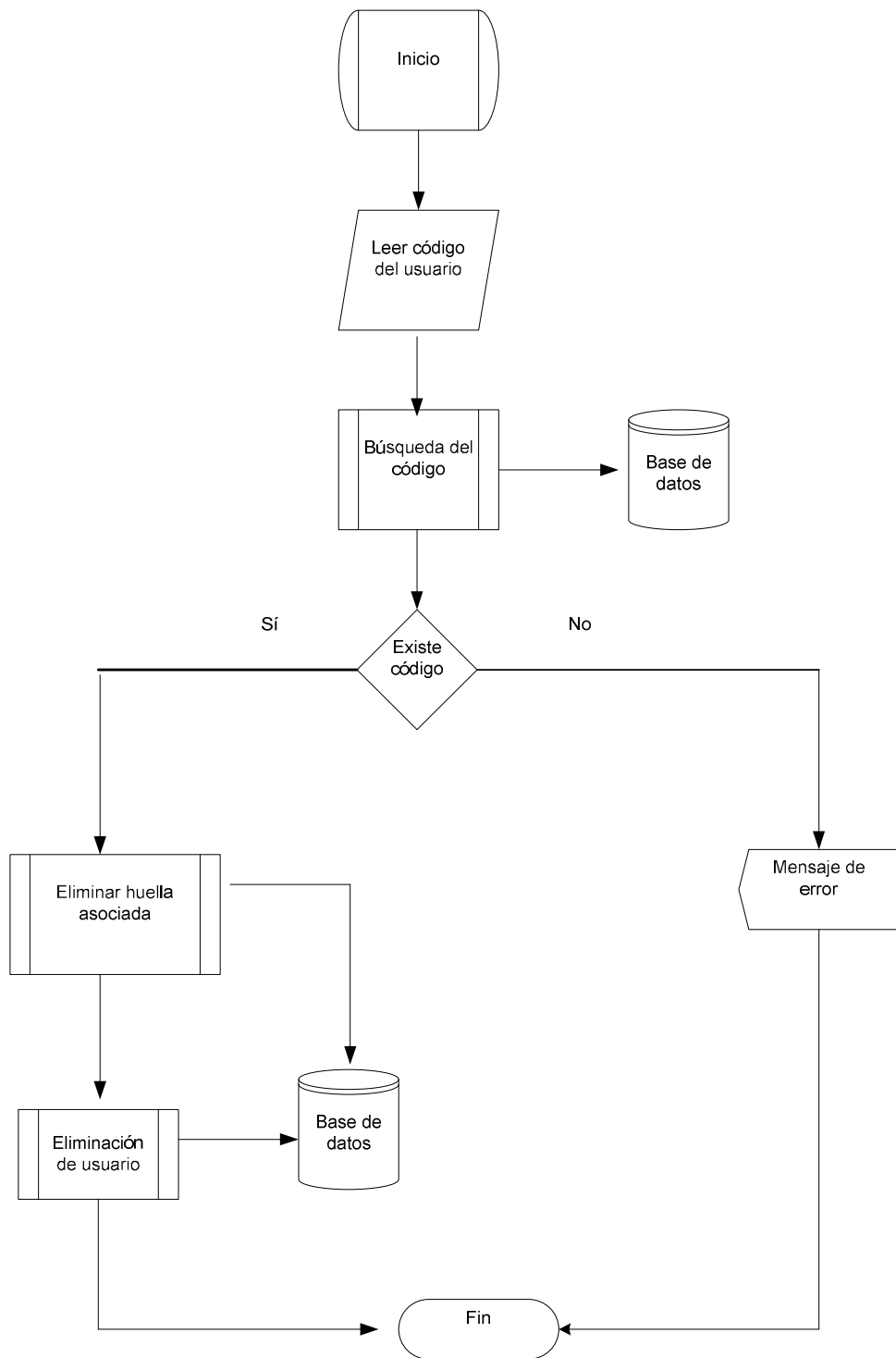


Figura 12. Diagrama de flujo de eliminación de empleados



4.3.4.4 Consulta de empleados

Este algoritmo permite obtener los datos almacenados de los empleados. Los criterios de búsqueda de los datos son: búsqueda de todos los empleados, búsqueda

por código, búsqueda por nombres y búsquedas por apellidos. (Véase diagrama de flujo en figura 13).

Procedimiento Consulta_Empleados

Criterio ← Ingresar_Criterio_de_búsqueda

Busqueda_de_datos(Criterio)

Si existen datos:

Mostrar_Datos

Si no existen datos:

Mostrar_Mensaje_Error

Fin Procedimiento Consulta_Empleados

4.3.4.5 Cambio de usuario administrador

Con el siguiente algoritmo se modifica el nombre del usuario con el cual se accede al mantenimiento de huellas de los empleados. (Véase diagrama de flujo en figura 14).

Procedimiento Cambio_Usuario_Administrador

Ingresar_Usuario

Ingresar_Clave

Si Clave_correcta

Obtener (Usuario_Actual, Usuario_Nuevo, Confirmación)

Si Usuario_Actual es distinto a Usuario_Nuevo:

Y Usuario_Nuevo es igual a Confirmación

Abrir_Tabla(Administrador)

Actualizar_Usuario_Administrador

Si no es distinto:

Mostrar_Mensaje_Error

Si no es Clave_correcta:

Mostrar_Mensaje_Error

Fin Procedimiento Cambio_Usuario_Administrador

4.3.4.6 Cambio de clave del administrador

Se modifica el nombre del usuario con el cual se accede al mantenimiento de huellas de los empleados. (Véase diagrama de flujo en figura 15).

Procedimiento Cambio_Usuario_Administrador

Ingresar_Usuario

Ingresar_Clave

Si Clave_correcta:

Obtener (Clave_Actual, Clave_Nueva, Confirmación)

Si Clave_Actual es distinta a Clave_Nueva

Y Clave_Nueva es igual a Confirmación:

Abrir_Tabla (Administrador)

Actualizar_Clave_Administrador

Si no es distinta:

Mostrar_Mensaje_Error

Si no es Clave_correcta:

Mostrar_Mensaje_Error

Fin Procedimiento Cambio_Clave_Administrador

Figura 13. Diagrama de flujo de consulta de empleados

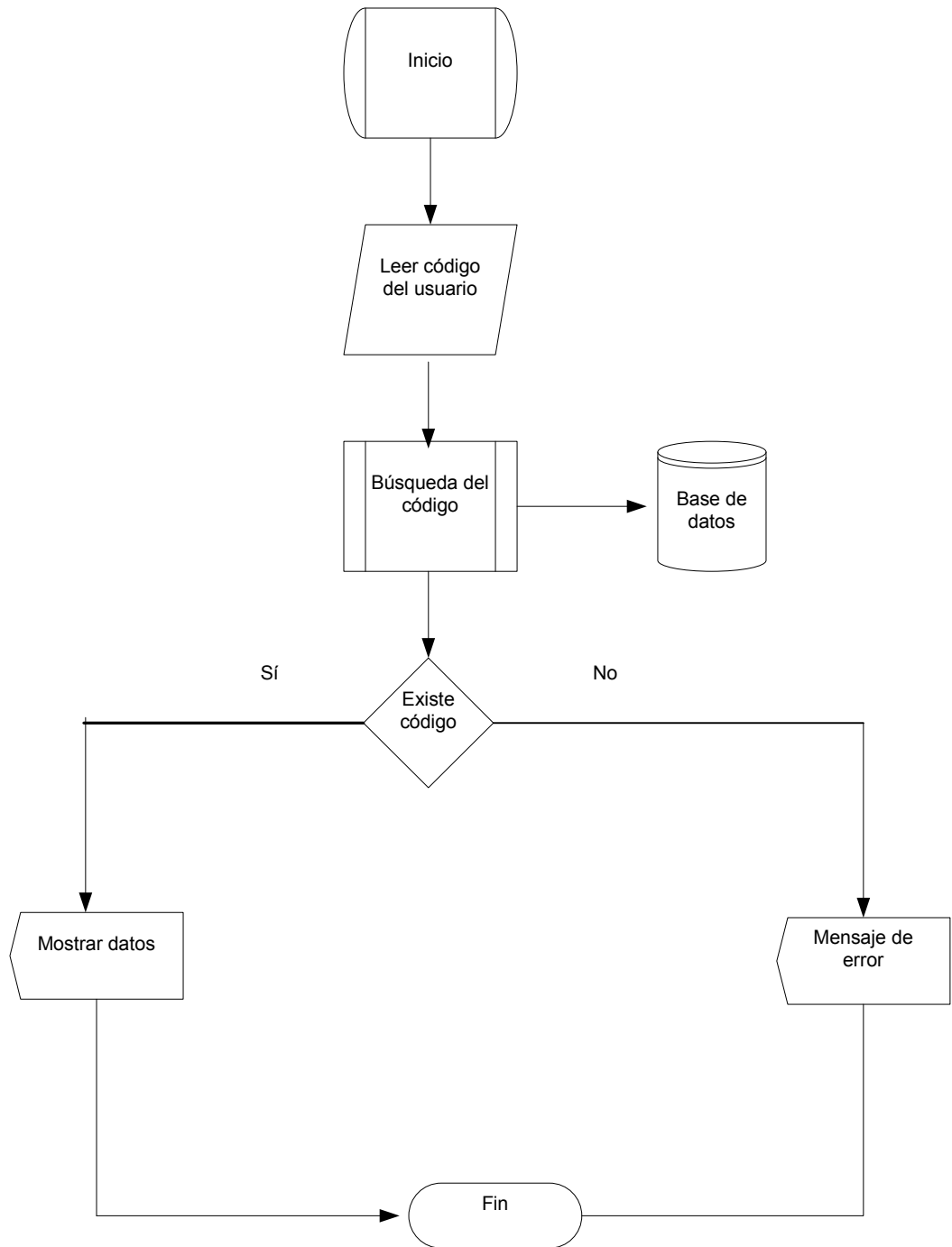


Figura 14. Diagrama de flujo de cambio de usuario administrador

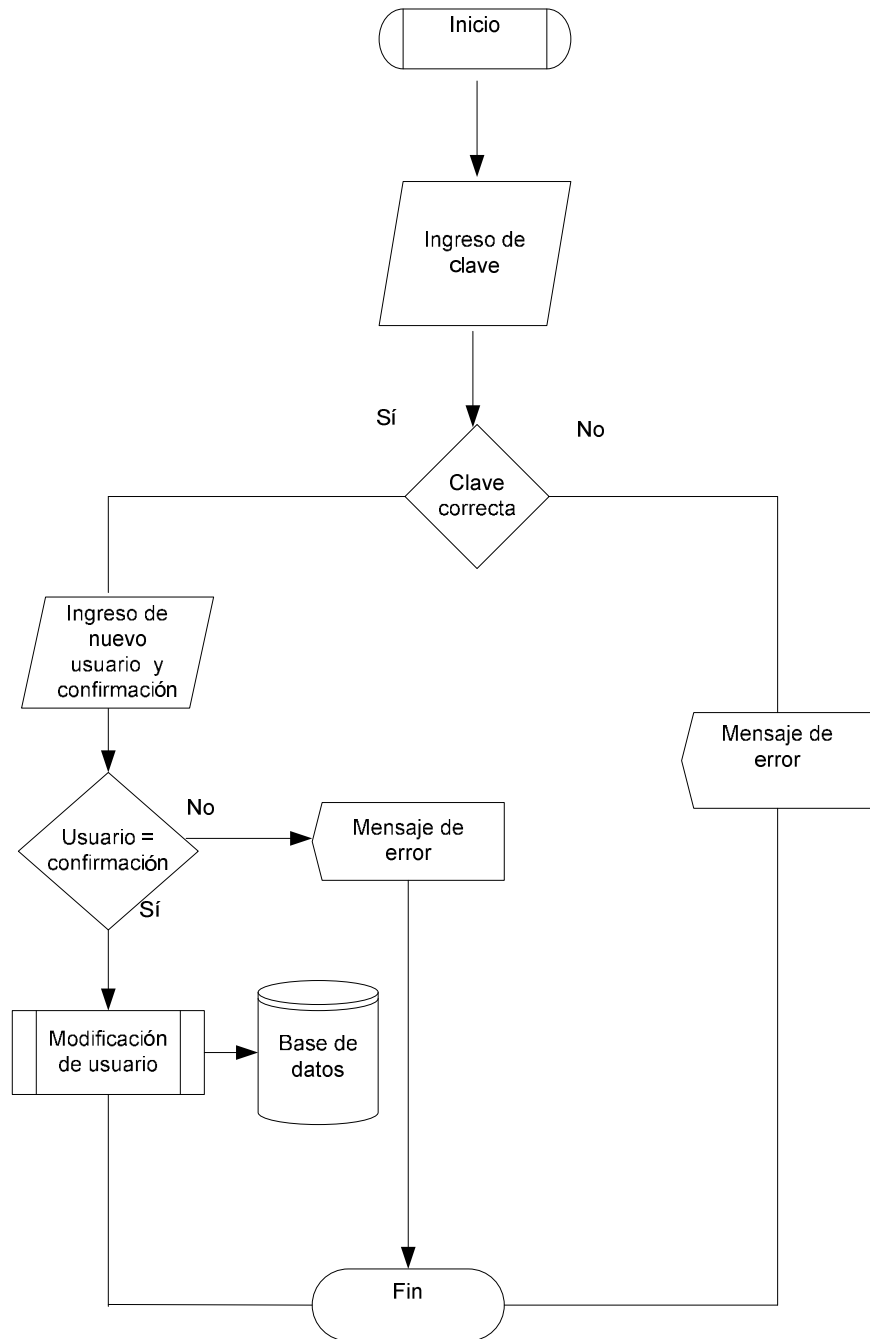
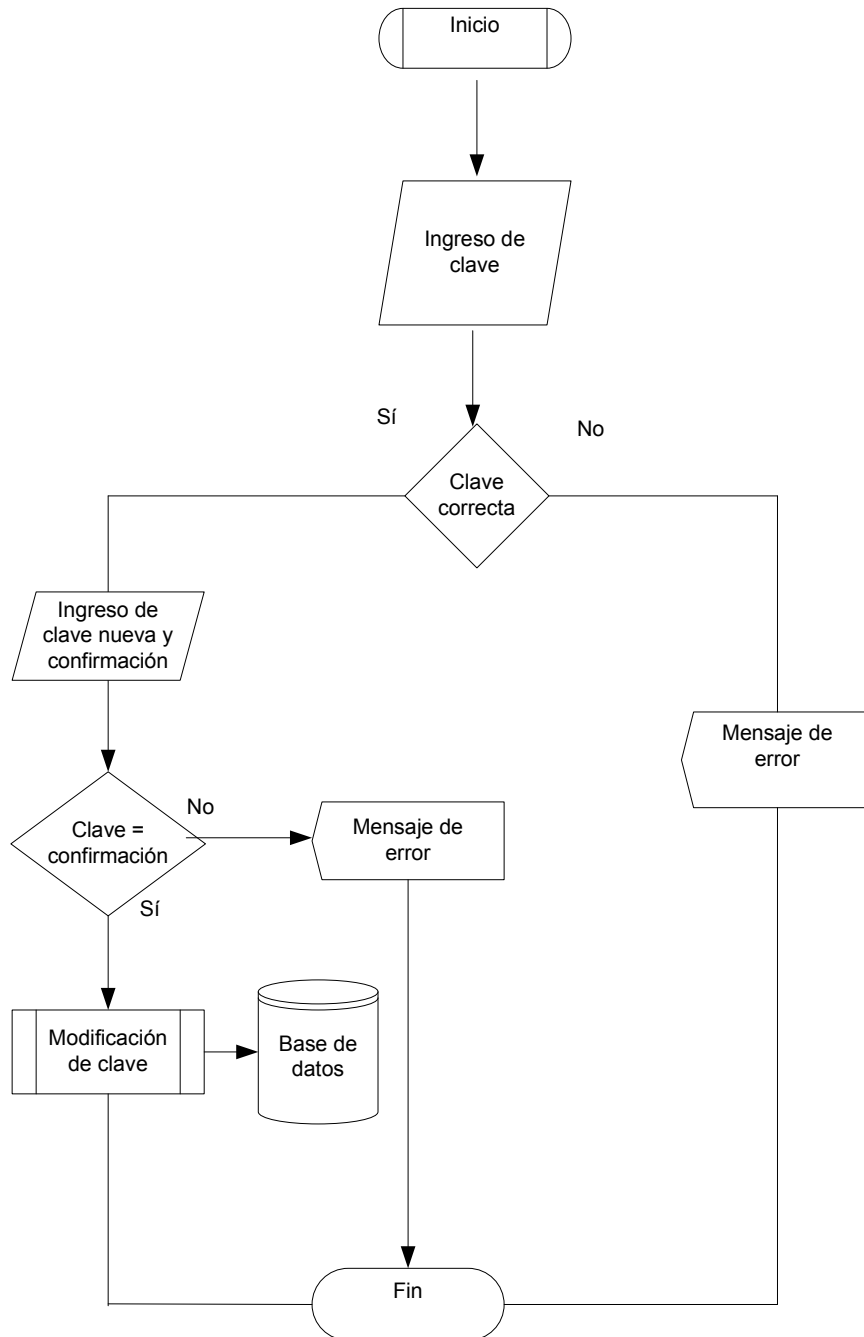


Figura 15. Diagrama de flujo de cambio de clave del administrador



4.3.4.7 Registro de huella

El siguiente algoritmo se utiliza para el registro de la huella de los empleados. (Véase diagrama de flujo en figura 16).

Procedimiento Registrar _ Huella

Código ← Ingresar_Código

Abrir_Tabla(Usuario,Huella)

Busqueda_código(Código)

Si existe código:

Busqueda_Huella(Código)

Si Existe_huella:

Mostrar_Mensaje_Error

Si no Existe_huella:

Obtener_muestras_de_huella

Generar_patron

Almacenar_Huella

Si no existe código:

Mostrar_Mensaje_Error

Fin Procedimiento Registrar_Huella

4.3.4.8 Comparación de huella

Luego de ingresar la huella, el empleado puede comparar si ésta se ha almacenado correctamente. El siguiente algoritmo descubre dicha comparación. (Véase diagrama de flujo en figura 17).

Procedimiento Comparar _ Huella

Código ← Ingresar_Código

Abrir_Tabla(Huella)

Busqueda_Huella(Código)

Si existe código:

Obtener_Patron

Comparar_Huella

Mostrar_Resultado

Si no existe código:

Mostrar_Mensaje_Error

Fin Procedimiento Comparar _ Huella

4.3.4.9 Eliminación de huella

Con el siguiente algoritmo eliminamos una huella de la base de datos asociada al código del empleado ingresado. (Véase diagrama de flujo en figura 18).

Procedimiento Eliminar _ Huella

Código ← Ingresar_Código

Abrir_Tabla(Huella)

Busqueda_Huella(Código)

Si existe código :

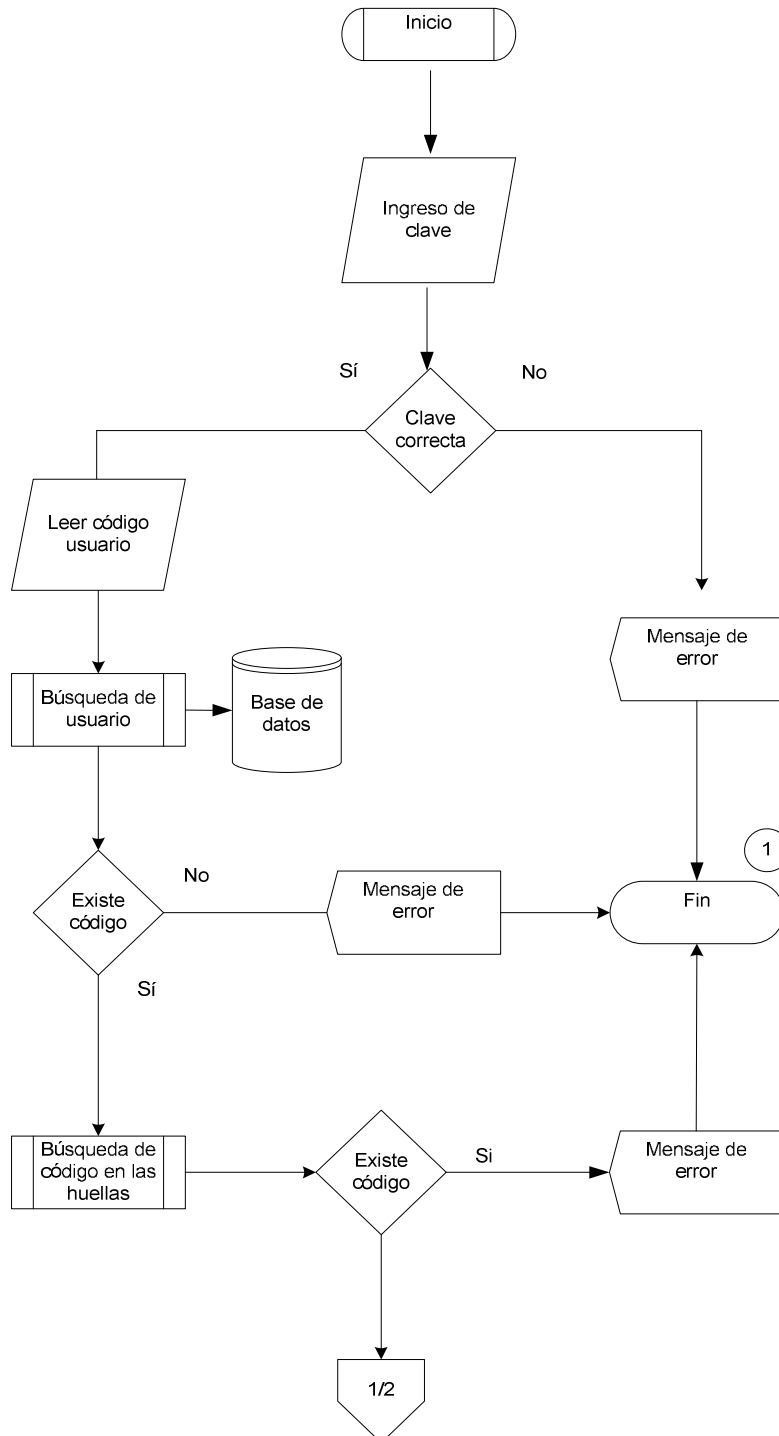
Elimina_Huella(Código)

Si no existe código:

Mostrar_Mensaje_Error

Fin Procedimiento Eliminar_Huella

Figura 16. Diagrama de flujo de registro de huella



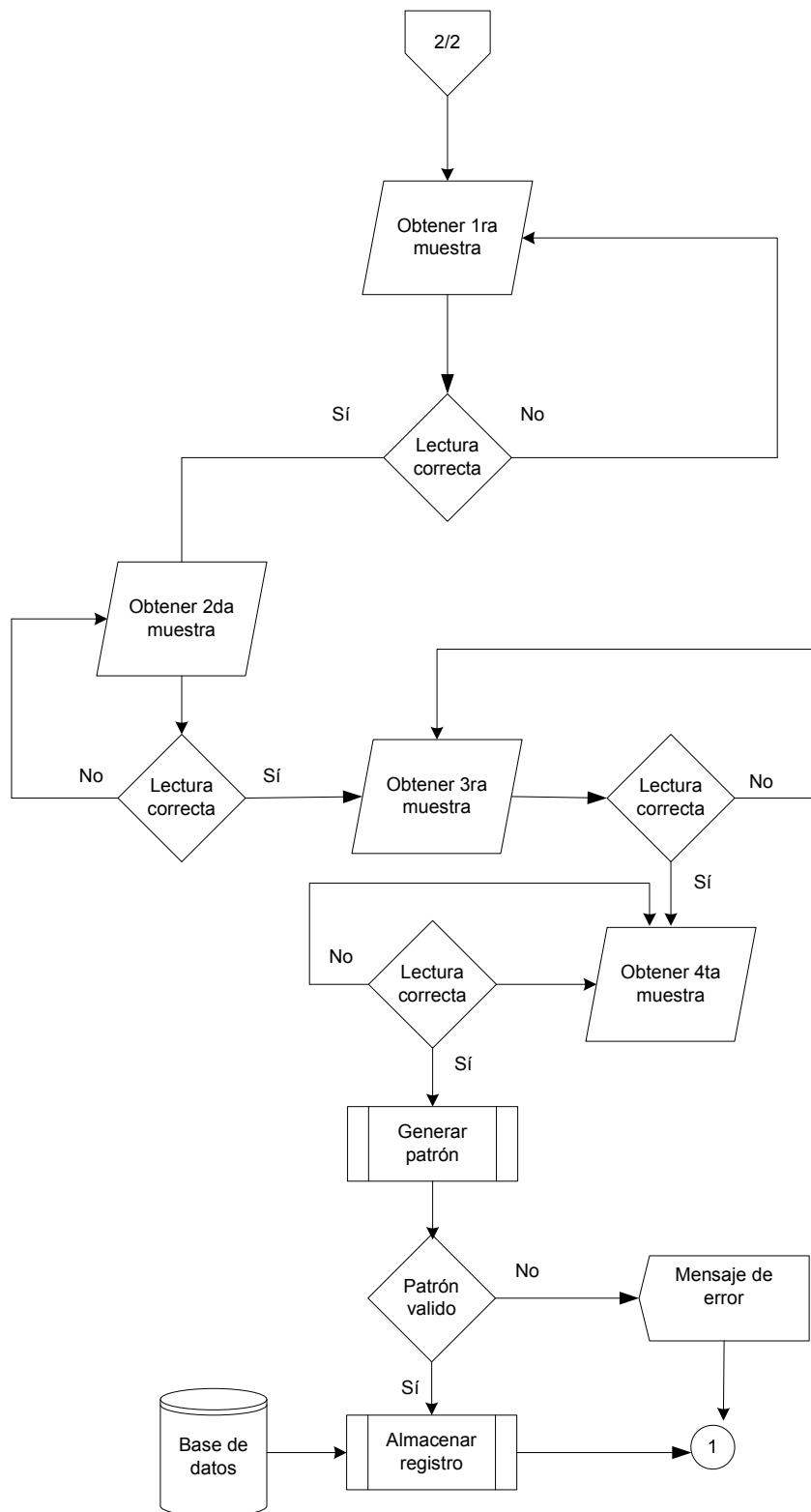


Figura 17. Diagrama de flujo de comparación de huella

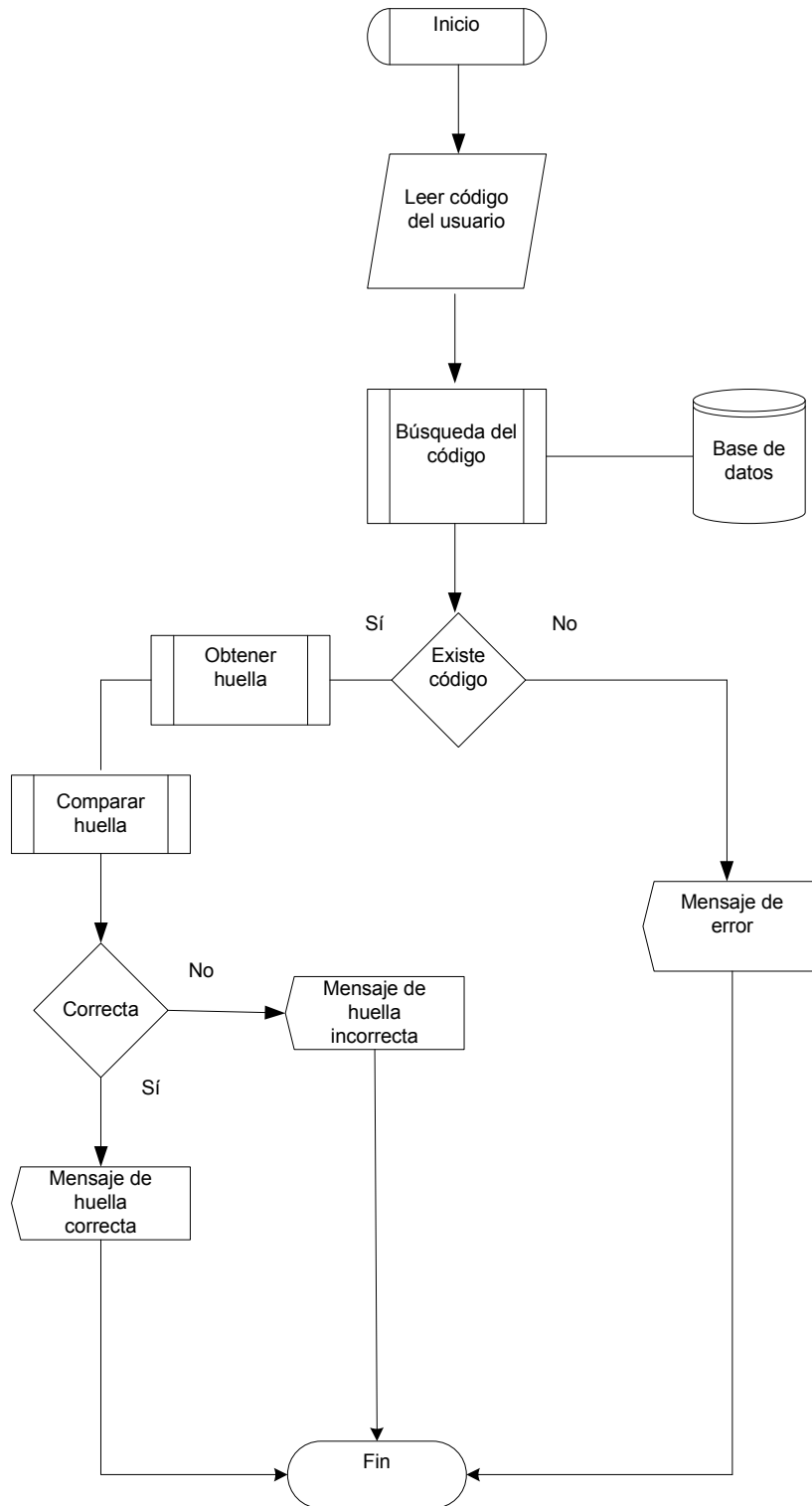
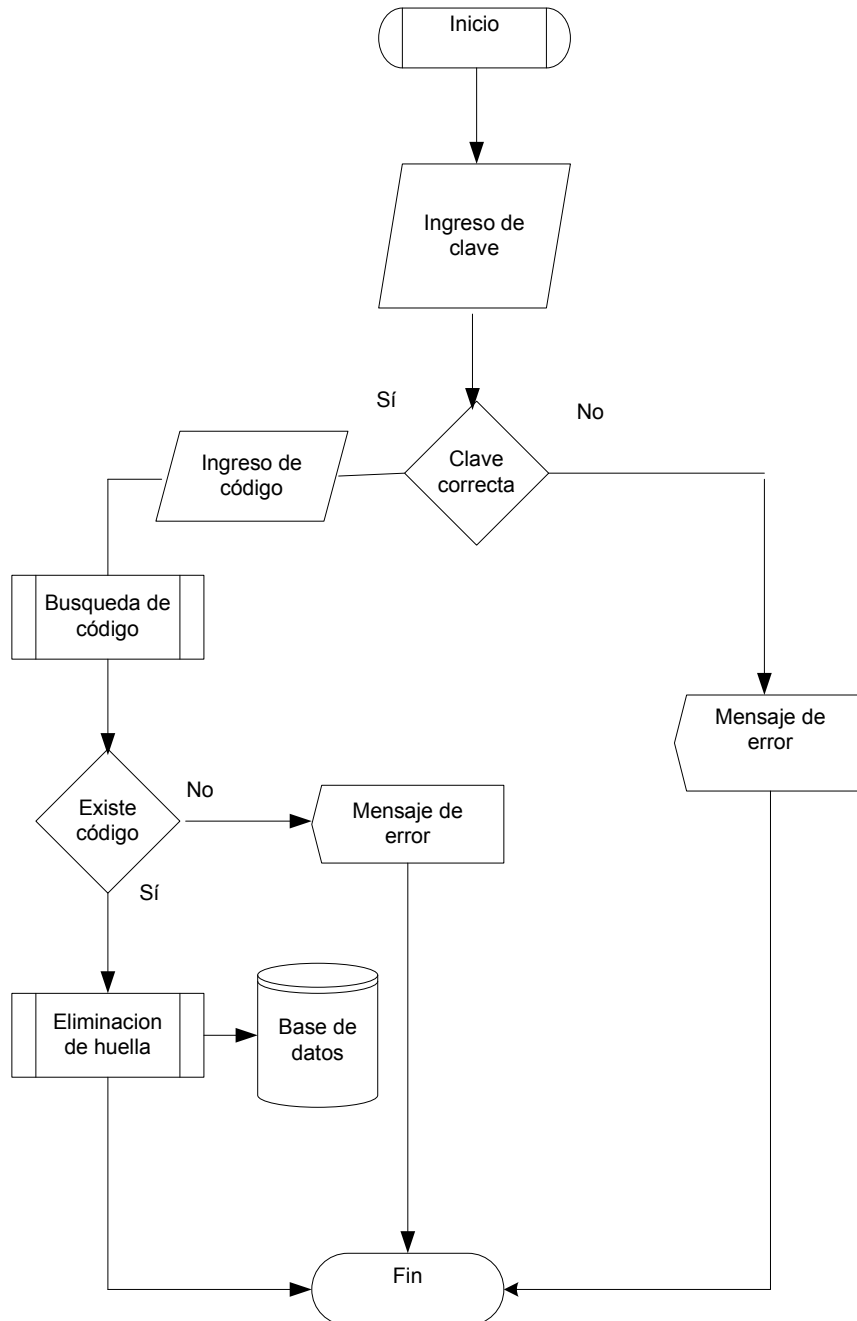


Figura 18. Diagrama de flujo de eliminación de huella



4.3.4.10 Registro de acceso de los empleados

El siguiente algoritmo permite llevar el control del acceso de los empleados. El empleado ingresa su código y luego su huella, la cual es comparada con la almacenada en la base de datos. Si la huella es correcta, se almacena un registro de control, si no, se lleva un historial de accesos denegados. (Véase diagrama de flujo en figura 19).

Procedimiento Registro_de_Acceso

Código ← Ingresar_Código

Busqueda_Huella(Código)

Si existe código:

Obtener_Patron

Comparar_Huella

Si huella_correcta

Abrir_Tabla (RegistroHuella)

Ingresar_Datos_Acceso

Si no es huella_correcta:

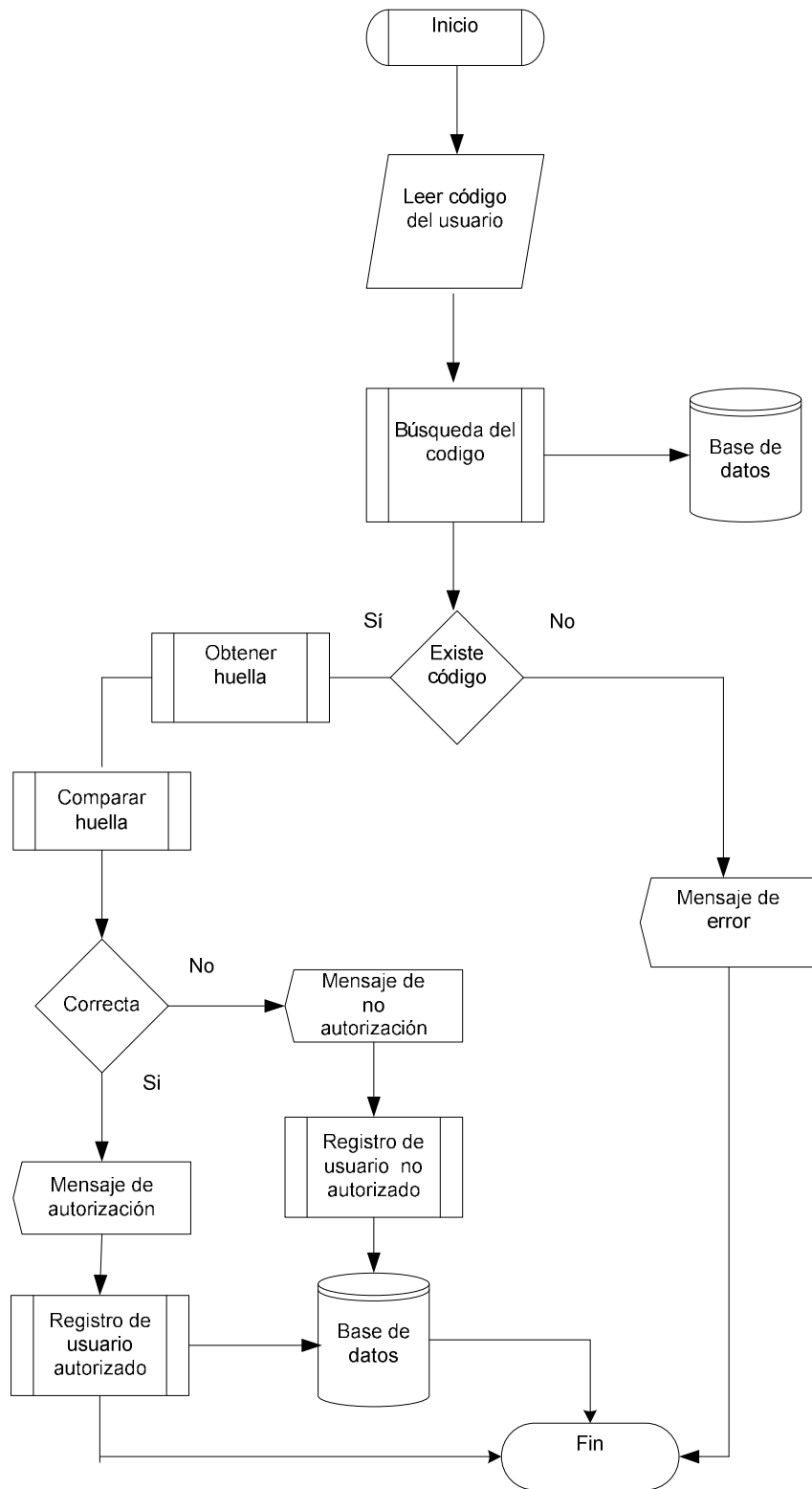
Abrir_Tabla(RegistroInvalido)

Ingresar_Datos_Acceso

Si no existe código: Mostrar_Mensaje_Error

Fin Procedimiento Registro_de_Acceso

Figura 19. Diagrama de flujo de registro de acceso de empleados



4.3.4.11 Reporte de empleados registrados

El siguiente algoritmo muestra la generación del reporte de empleados registrados en la base de datos. (Véase diagrama de flujo en figura 20).

Procedimiento Reporte_de_Empleados

Abrir_Tabla(Usuario)

Obtener_Datos

Si existen datos:

Generar_Reporte

Si no existen datos:

Mostrar_Mensaje

Fin Procedimiento Reporte_Empleados

4.3.4.12 Reporte de huellas asociadas

El siguiente algoritmo muestra el reporte de las huellas que están registradas dentro de la base de datos. (Véase diagrama de flujo en figura 21).

Procedimiento Reporte_de_Huellas

Abrir_Tabla(Usuario)

Obtener_Datos

Si existen datos:

Generar_Reporte

Si no existen datos:

Mostrar_Mensaje

Fin Procedimiento Reporte_de_Huellas

Figura 20. Diagrama de flujo de reporte de empleados

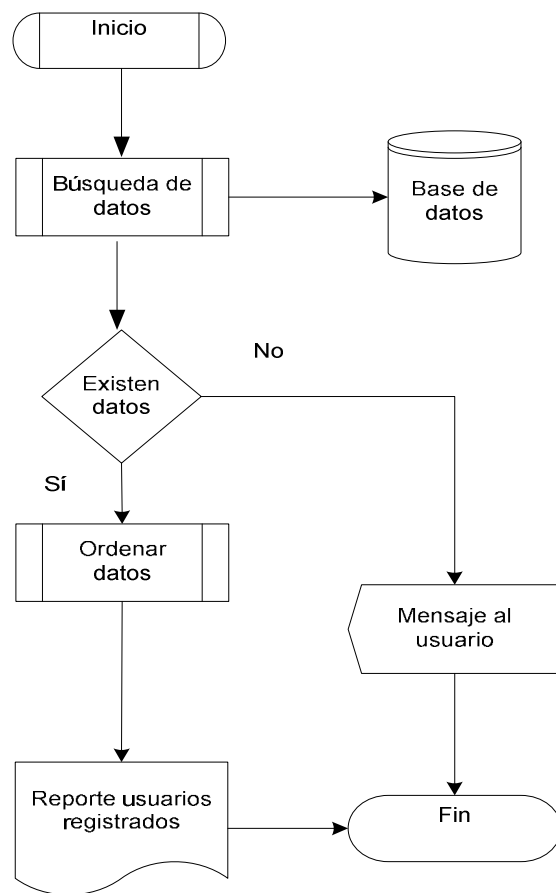
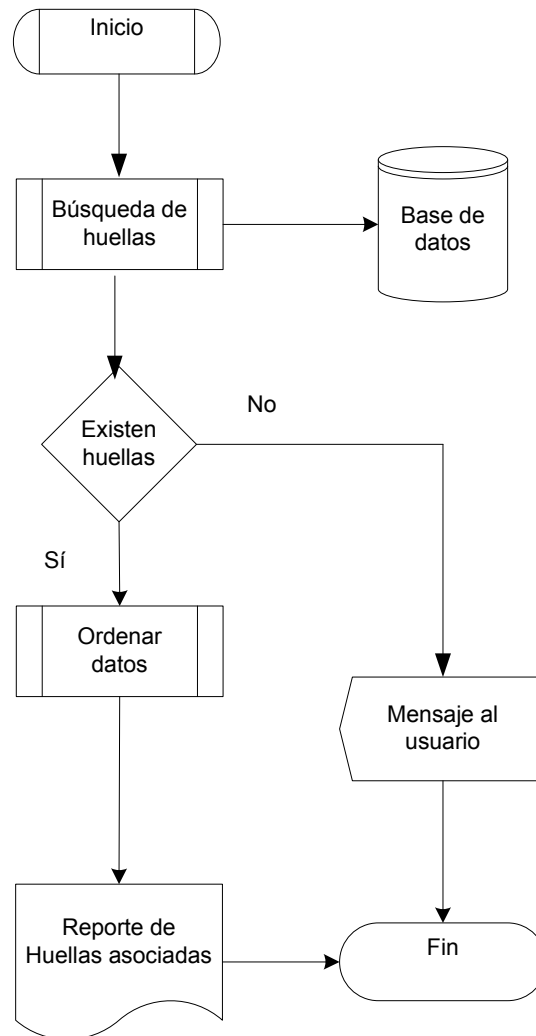


Figura 21. Diagrama de flujo de reporte de huellas asociadas



4.3.4.13 Reporte de control de acceso de los empleados

El siguiente algoritmo muestra el reporte del control de acceso de los empleados. Puede obtenerse un reporte por todos los empleados o uno en particular. (Véase diagrama de flujo en figura 22).

Procedimiento Reporte_de_Control_de_acceso

Abrir_Tabla(Usuario, RegistroHuella)

Obtener_Datos_Según_criterio

Si existen datos:

Generar_Reporte

Si no existen datos:

Mostrar_Mensaje

Fin Procedimiento Reporte_Control_de_acceso

4.3.4.14 Reporte de usuarios inválidos

El siguiente algoritmo muestra el reporte de rechazos de ingreso de los empleados. Al igual que el anterior, puede ser de un empleado o de todos. (Véase diagrama de flujo en figura 23).

Procedimiento Reporte_de_Control_de_acceso

Abrir_Tabla(Usuario, RegistroHuella)

Obtener_Datos_Según_criterio

Si existen datos:

Generar_Reporte

Si no existen datos:

Mostrar_Mensaje

Fin Procedimiento Reporte_Control_de_acceso

Figura 22. Diagrama de flujo de reporte de control de acceso

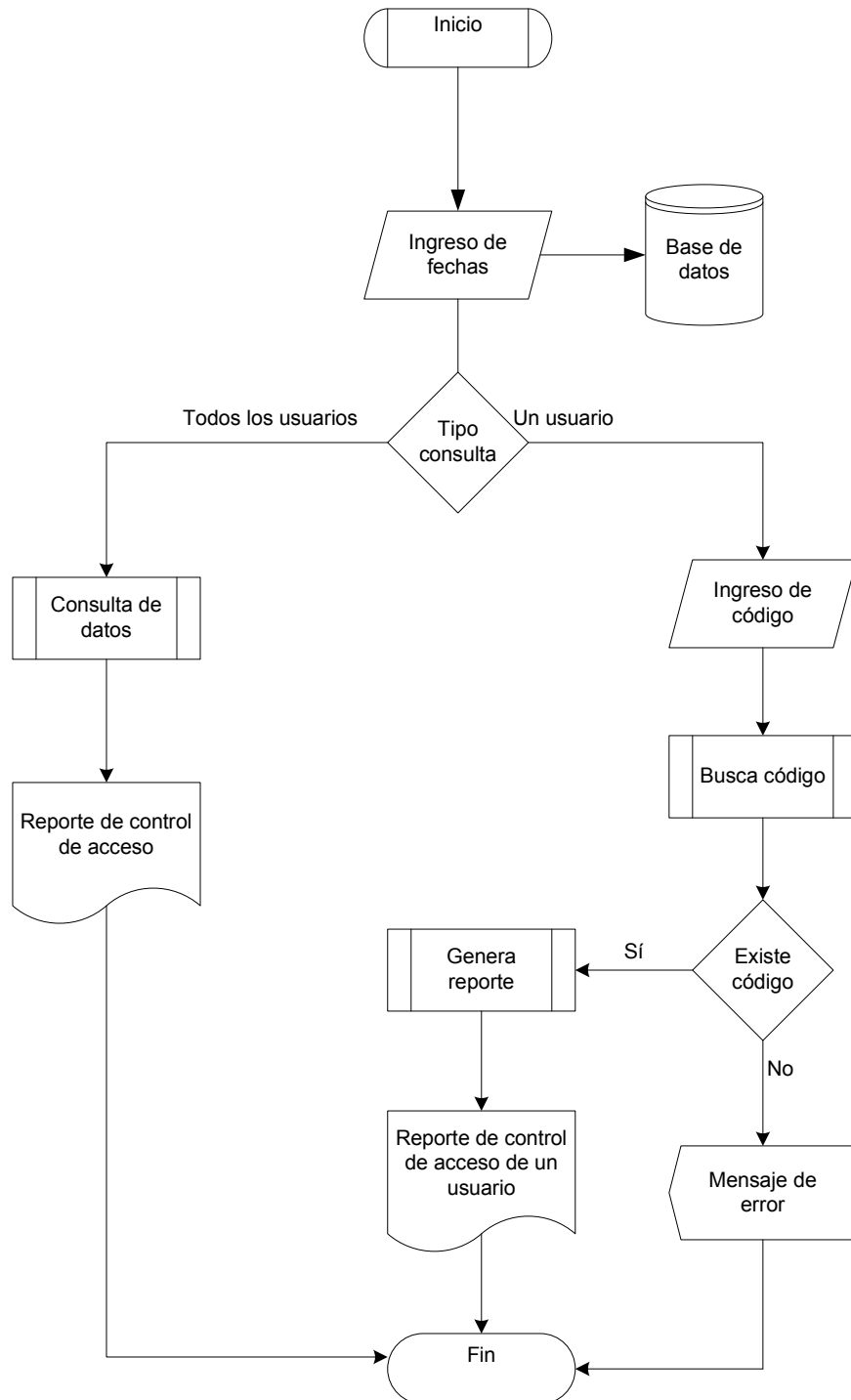
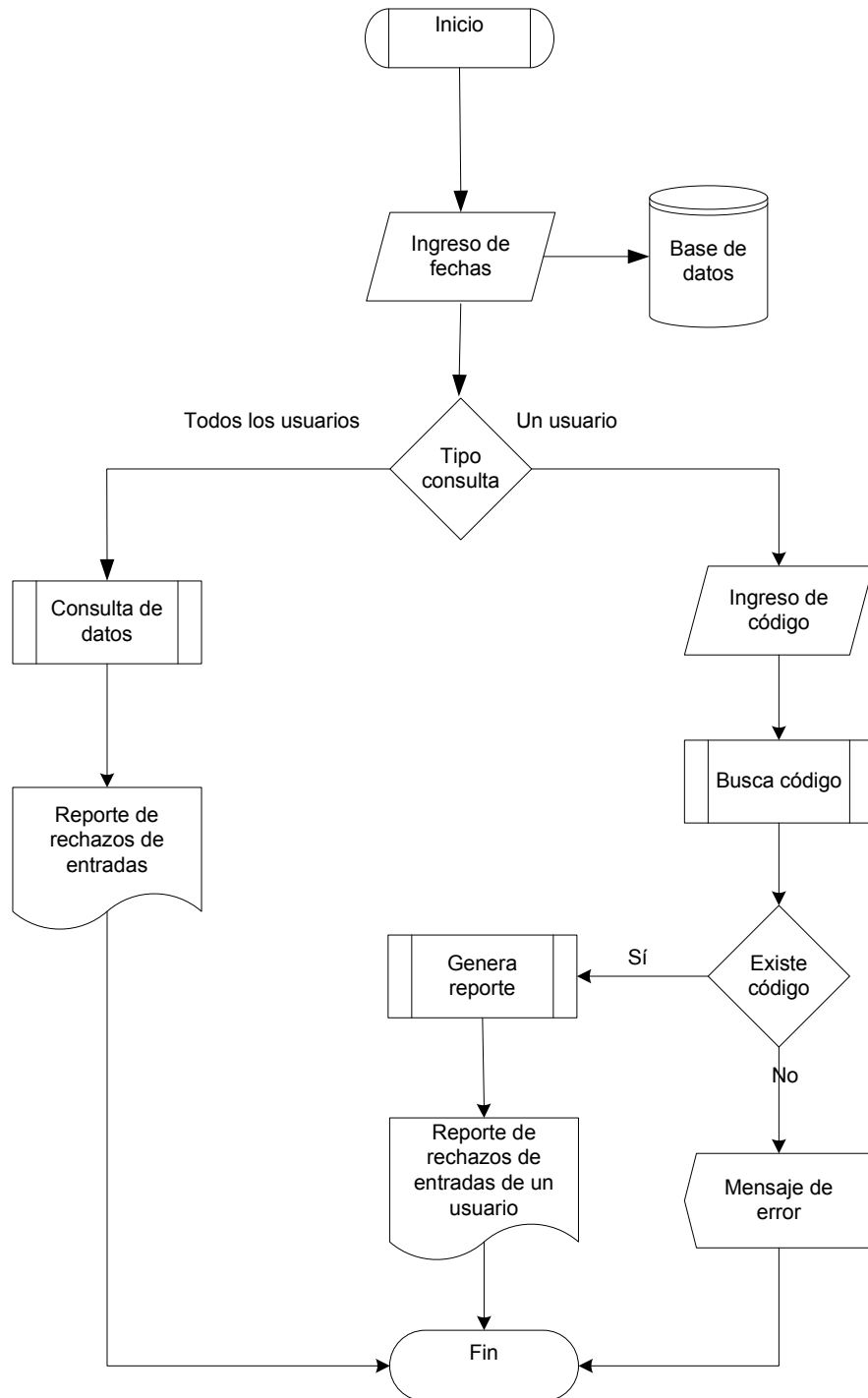


Figura 23. Diagrama de flujo de reporte de registros de Inválidos



4.3.5 Desarrollo de la aplicación

La aplicación se desarrolló en el lenguaje de programación *visual basic* utilizando una base de datos en *Access*. Para la comunicación del lector de huella digital con la computadora, se utilizaron los algoritmos que están incluidos en el *kit* de desarrollo del *software* del fabricante del lector (*U. Are U. Platinum Software Developer's kit o SDK*)

Dentro de los algoritmos para el reconocimiento de la huella digital utilizamos dos términos llamados tasas de error:

- Tasa de falsa aceptación (FAR, por sus siglas en inglés, *False Acceptance Rate*).

Se define como la probabilidad de que un individuo no autorizado sea aceptado por el sistema.

- Tasa de falso rechazo (FRR, por sus siglas en inglés, *False Rejection Rate*).

Definida como la probabilidad de que un individuo autorizado es rechazado por el sistema.

La tasa de falsa aceptación y la tasa de falso rechazo son funciones del grado de seguridad deseado. Usualmente, el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo $[0, 1]$, que indicará la correlación entre la característica biométrica proporcionada por el usuario y la almacenada en la base de datos.

Actualmente, los algoritmos de “DigitalPersona” que son los utilizados para esta aplicación proveen una tasa de falsa aceptación de 0.01% y una tasa de falso rechazo de 1.4%.

Los siguientes procesos comprenden el reconocimiento de la huella digital dentro de la aplicación.

- **Obtener la imagen de la huella**

El primer paso en el reconocimiento de la huella consiste en adquirir una imagen de la misma. Cuando el usuario toca el sensor, una imagen de la huella llamada muestra es comprimida y encriptada por el sensor y es enviada a la computadora

- **Descompresión de la muestra**

Cuando la muestra es recibida por el sensor, es descomprimida y descriptada en una muestra cuyas características pueden ser extraídas y con ello crear una plantilla.

- **Creación de la plantilla**

Después de determinar la operación ya sea registro o verificación se crea la plantilla apropiada. Una plantilla es una descripción matemática de las características de la huella digital y es asignado uno de los dos tipos: pre-registro o verificación de la plantilla.

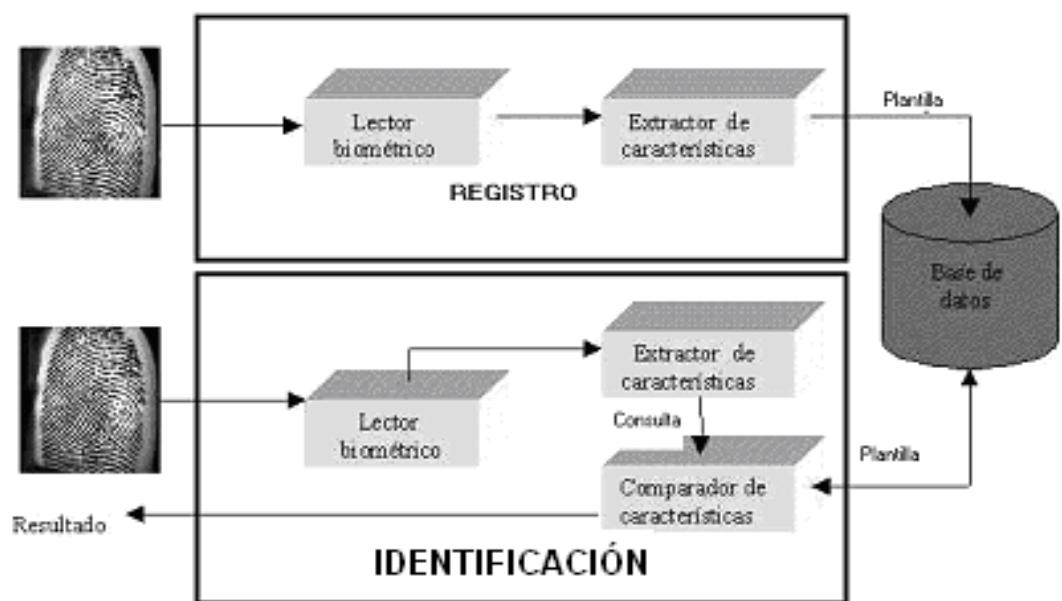
- **Ejecutar la operación de registro o verificación**

En el registro, si una huella nueva está siendo registrada, se deben tomar cuatro muestras o plantillas que son usadas para crear una sola plantilla, la cual puede ser almacenada en una base de datos para utilizarla posteriormente. En la verificación, una plantilla es requerida y comparada con la almacenada en la base de datos.

4.3.5.1 Arquitectura del sistema de reconocimiento de la huella digital

La siguiente figura muestra la arquitectura del sistema de reconocimiento de la huella digital.

Figura 24. Arquitectura de un sistema de reconocimiento de huella digital



En el proceso de registro, un usuario brinda al sistema muestras de su huella digital, con las cuales el extractor de características genera una plantilla que es almacenada en la base de datos.

El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de las plantillas. La representación resultante se denomina, se consulta, y es enviada al comparador de características que confronta a éste la plantilla almacenada en la base de datos para establecer la identidad.

4.3.5.2 Descripción de los algoritmos para el dispositivo biométrico

Los siguientes algoritmos fueron adaptados para efectos de la aplicación del código original que está incluido en el *kit* de desarrollo del dispositivo.

- **Registro de la huella digital**

Como primer paso, creamos una instancia del objeto *FPTemplate* y una del objeto *FPRegisterTemplate*, que se utilizarán para el registro de la huella digital.

```
Dim WithEvents op As FPRegisterTemplate
Dim cursample As Integer
Dim regtemplate As FPTemplate
```

Como segundo paso, tomamos las cuatro muestras para generar una plantilla. Esto lo hacemos con el siguiente algoritmo el cual contiene la sentencia *op.run* con la cual hacemos la llamada a un método del objeto *FPRegisterTemplate* anteriormente definido, y el cual procede al proceso de registro.

```
Sub TomaHuella()
```

```
    Dim i As Integer
```

```
    cursample = 0
```

```
    For i = 0 To 3
```

```
        picSample(i).Picture = Nothing
```

```
        dot(i).Visible = False
```

```
    Next i
```

```
    dot(cursample).Visible = True
```

op.Run

LblMensajes.Caption = "Mensajes:"

Mensajes.Caption = "Coloque el dedo en el sensor"

lblQuality.Caption = ""

lblTemplateID.Caption = ""

lblEvents.Caption = ""

End Sub

El tercer paso consiste en verificar la calidad de la muestra. Con el siguiente código verificamos la calidad de la muestra tomada del sensor, si la muestra fue tomada correctamente, si fue muy borrosa, si no se logró tomar una región central, etc.

*Private Sub op_SampleQuality(ByVal Quality As
DpSdkEngLib.AISampleQuality)*

Dim Error As Integer

Select Case Quality

Case AISampleQuality.Sq_Good

lblQuality.Caption = "OK"

cursample = cursample + 1

dot(cursample - 1).Visible = False

If cursample <> 4 Then

dot(cursample).Visible = True

End If

Case AISampleQuality.Sq_LowContrast

lblQuality.Caption = "Muestra incorrecta"

Error = 1

Case AISampleQuality.Sq_NoCentralRegion

lblQuality.Caption = "Muestra incompleta" Error = 1

Case AISampleQuality.Sq_None

lblQuality.Caption = "Muestra incorrecta"

Error = 1

Case AISampleQuality.Sq_NotEnoughFtr

lblQuality.Caption = "Muestra incorrecta"

Error = 1

Case AISampleQuality.Sq_TooDark

lblQuality.Caption = "Muestra incorrecta"

Error = 1

Case AISampleQuality.Sq_TooLight

lblQuality.Caption = "Muestra incorrecta"

Error = 1

Case AISampleQuality.Sq_TooNoisy

```

        lblQuality.Caption = "Muestra incorrecta"

        Error = 1

    End Select

    If Error = 0 Then

        lblEvents.Caption = "Muestra correcta"

        LblMensajes.Caption = "Mensajes:"

        Mensajes = "Coloque el dedo en el sensor"

    Else

        lblEvents.Caption = "Coloque nuevamente el dedo"

        Mensajes = "Coloque nuevamente el dedo"

    End If

End Sub

```

Si ocurre cualquiera de los errores anteriores en la toma de una muestra, se solicita nuevamente hasta que se ingrese una apropiada para generar la plantilla.

El cuarto paso es mostrar una imagen de la muestra obtenida por el sensor. Cuando la muestra es requerida por el sensor, un evento es activado y se muestra al usuario la imagen de la huella ingresada. Utilizamos el siguiente código para desplegar dicha imagen.

```

Private Sub op_SampleReady(ByVal pSample As Object)

    pSample.PictureOrientation = Or_Portrait

```

*pSample.PictureWidth = picSample(cursample).Width /
Screen.TwipsPerPixelX*

*pSample.PictureHeight = picSample(cursample).Height /
Screen.TwipsPerPixelY*

picSample(cursample).Picture = pSample.Picture

lblEvents.Caption = "Listo"

End Sub

Como último paso se procede a almacenar el patrón generado. Si se logró generar un patrón válido, se exporta el valor almacenado en la plantilla a una variable global, la cual es enviada posteriormente a la base de datos.

Dim blob() As Byte

regtemplate.Export bvariant

blob = bvariant

- **Proceso de verificación de la huella digital**

Al igual que en el proceso de registro de la huella, en la verificación, como primer paso definimos una instancia del objeto, pero en este caso para verificación.

*Dim WithEvents op As FPVerifyTemplate
Dim regtemplate As FPTemplate*

Como segundo paso, extraemos de la base de datos la plantilla generada del usuario que se presenta a verificar la huella, la cual está asociada al código de identificación del usuario. Creamos una nueva instancia *FPTemplate* a la cual le importamos el valor obtenido de la base de datos, con las siguientes sentencias de código:

```
Set regtemplate = New FPTemplate
```

```
res = regtemplate.Import(blob)
```

Como tercer paso, activamos el evento del objeto que toma la huella del sensor la codifica y la compara con la almacenada en la plantilla.

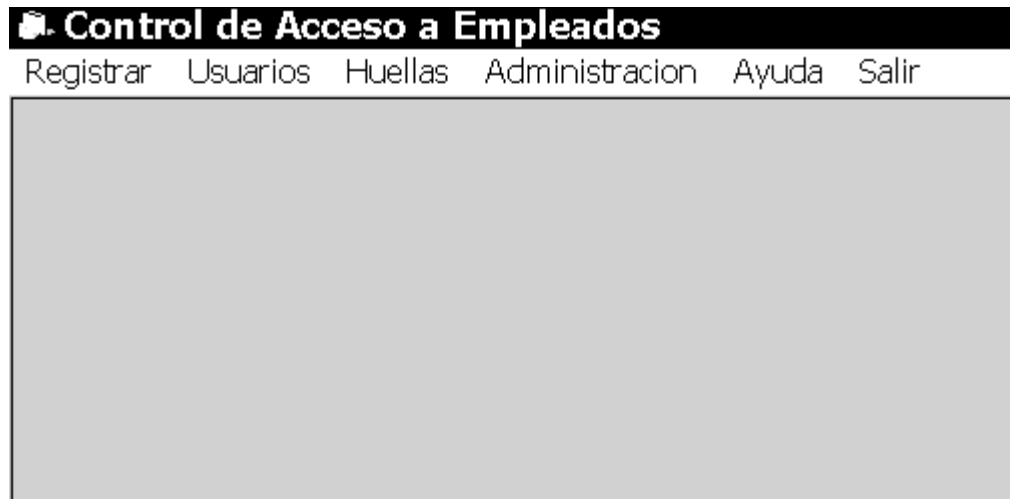
```
op.Run regtemplate
```

Se activan los eventos que se mencionaron en el registro de huella, los cuales determinan la calidad de la muestra obtenida y se procede a comparar las dos muestras, determinando así si se acepta la huella como correcta o no.

4.4 Funcionamiento del sistema

El menú principal de la aplicación tiene las opciones: registrar, usuarios, huellas y administración, como se muestra en la siguiente figura.

Figura 25. Menú principal



A continuación se describirá cada una de las opciones.

4.4.1 Registrar

Un usuario con un patrón previamente almacenado, se presenta al sistema para ingresar su registro de entrada. El usuario ingresa su código de identificación personal el cual es validado, coloca el dedo en el sensor biométrico y se genera un patrón o plantilla que se compara con el almacenado en la base de datos asociado a ese código.

Si coinciden los patrones, se registra la fecha y la hora de acceso al sistema y se le da la bienvenida al usuario. Si no coinciden, se almacena un registro con el código, la fecha y la hora en que un usuario intentó ingresar al sistema con una huella que no era la almacenada en la base de datos. Esta opción se muestra en la figura 26.

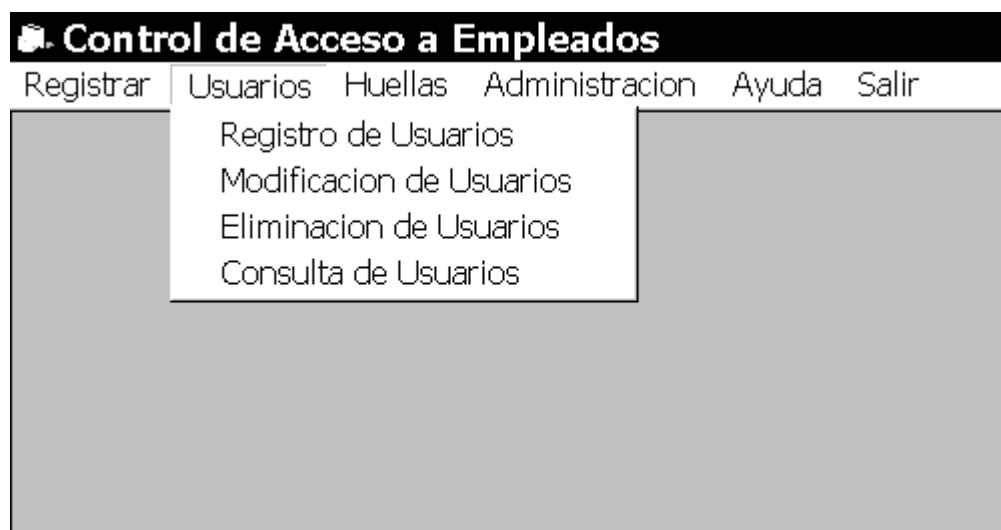
Figura 26. Registrar



4.4.2 El Menú usuarios

Este menú se muestra en la siguiente figura.

Figura 27. Menú usuarios

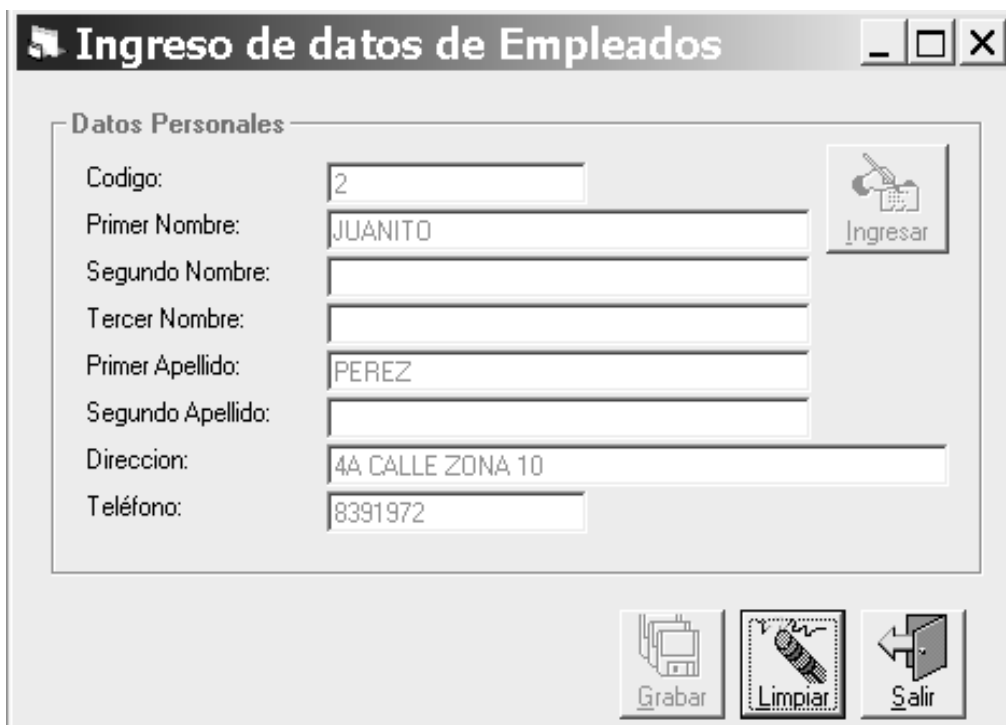


Tiene las opciones:

4.4.2.1 Registro de usuarios

Se solicita al usuario que ingrese su código de identificación personal, el cual se valida si existe en la base de datos, si ya existiera se despliega un error en esa operación. Si no existe, se solicita al usuario que ingrese sus datos personales: nombres, apellidos, dirección, teléfono y se ingresan a la base de datos. Esta opción se muestra en la siguiente figura.

Figura 28. Ingreso de datos



The screenshot shows a software window titled "Ingreso de datos de Empleados". The window contains a form with the following fields and values:

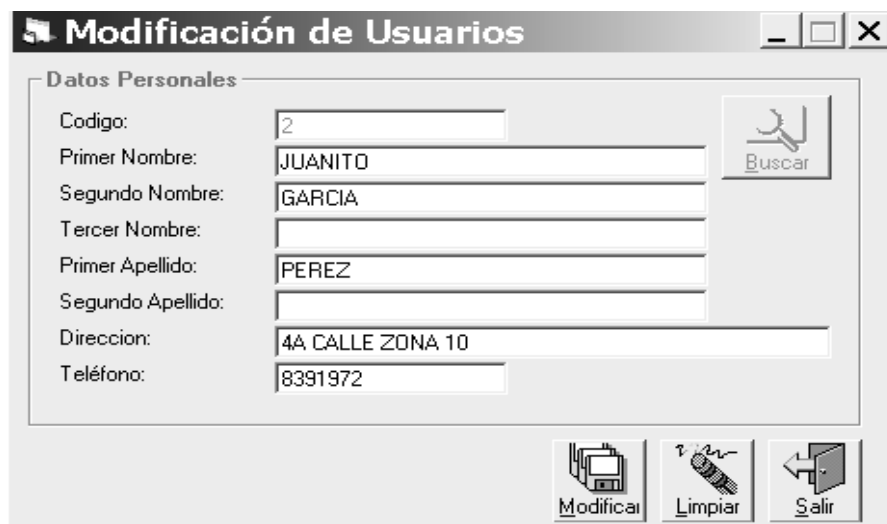
| Datos Personales | |
|-------------------|------------------|
| Codigo: | 2 |
| Primer Nombre: | JUANITO |
| Segundo Nombre: | |
| Tercer Nombre: | |
| Primer Apellido: | PEREZ |
| Segundo Apellido: | |
| Direccion: | 4A CALLE ZONA 10 |
| Teléfono: | 8391972 |

At the bottom of the window, there are three buttons: "Grabar", "Limpiar", and "Salir".

4.4.2.2 Modificación de usuarios

Se solicita al usuario que ingrese su código de identificación personal, el cual es validado en la base de datos, si existe se muestran los datos almacenados de ese usuario y se habilitan para modificarlos, luego, esos datos modificados se actualizan. Esta opción se representa en la siguiente figura.

Figura 29. Modificación de usuarios



The screenshot shows a window titled "Modificación de Usuarios" with a standard Windows-style title bar (minimize, maximize, close). The window contains a form with the following fields and values:

| Datos Personales | |
|-------------------|------------------|
| Código: | 2 |
| Primer Nombre: | JUANITO |
| Segundo Nombre: | GARCIA |
| Tercer Nombre: | |
| Primer Apellido: | PEREZ |
| Segundo Apellido: | |
| Dirección: | 4A CALLE ZONA 10 |
| Teléfono: | 8391972 |

At the bottom of the form, there are three buttons: "Modificar" (with a floppy disk icon), "Limpiar" (with a trash can icon), and "Salir" (with a door icon). A "Buscar" button with a magnifying glass icon is located to the right of the "Codigo" field.

4.4.2.3 Eliminación de usuarios

Se solicita al usuario que ingrese su código de identificación personal, el cual se valida en la base de datos, si existe se muestran los datos. Al escoger el botón de eliminar e ingresar confirmación, automáticamente se elimina el usuario y la huella asociada a ese código. La siguiente figura representa esta opción.

Figura 30. Eliminación de usuarios

Eliminación de Usuarios

Datos del Usuario

Código: 2

Primer Nombre: JUANITO

Segundo Nombre: GARCIA

Tercer Nombre:

Primer Apellido: PEREZ

Segundo Apellido:

Dirección: 4A CALLE ZONA 10

Teléfono: 8391972

Eliminar Limpiar Salir

4.4.2.4 Consulta de usuarios

Esta consulta muestra los datos de un usuario y si tiene huella asociada. Puede ser por el código o por los nombres del usuario y se representa en la siguiente figura.

Figura 31. Consulta de usuarios

Consulta de Usuarios

Todos

Código: 2

Primer Nombre: JUANITO

Segundo Nombre: GARCIA

Tercer Nombre:

Primer Apellido: PEREZ

Segundo Apellido:

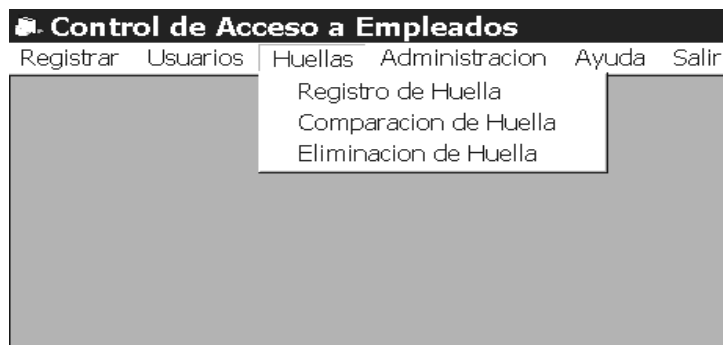
Buscar Limpiar Salir

| CODIGO | NOMBRE 1 | NOMBRE 2 | NOMBRE 3 | APELLIDO | APELLIDO 2 | DIRECC |
|--------|----------|----------|----------|----------|------------|--------|
| 1 | BLANCA | CECILIA | | CASTILLO | MARROQUI | 25 ZON |
| 2 | JUANITO | GARCIA | | PEREZ | | E ZON |
| 3 | MARIA | GABRIELA | | ARTEAGA | GUTIERREZ | 25 ZON |

4.4.3 El menú huellas

La figura siguiente representa el menú para el mantenimiento de huellas de los usuarios. Para el acceso a cualquier opción de este menú se solicita la clave del administrador. Tiene las siguientes opciones:

Figura 32. Menú huellas



4.4.3.1 Registro de huella

Se solicita al usuario que ingrese su código de identificación personal, el cual se valida que exista en la base de datos. Se solicita al usuario que coloque su dedo en el sensor cuatro veces para generar un patrón válido, el cual se asocia al código y se almacena en la base de datos. Esta opción está representada en la siguiente figura.

Figura 33. Registro de huella



4.4.3.2 Comparación de huella

Se utiliza para verificar que si se registró correctamente la huella de un usuario. Esta opción se muestra en la figura 34. Se ingresa el código de identificación personal y se valida que exista, se coloca el dedo en el sensor y se compara con el almacenado en la base de datos. A diferencia de la verificación, esta opción no almacena registro, sólo se muestra si la huella es correcta o no.

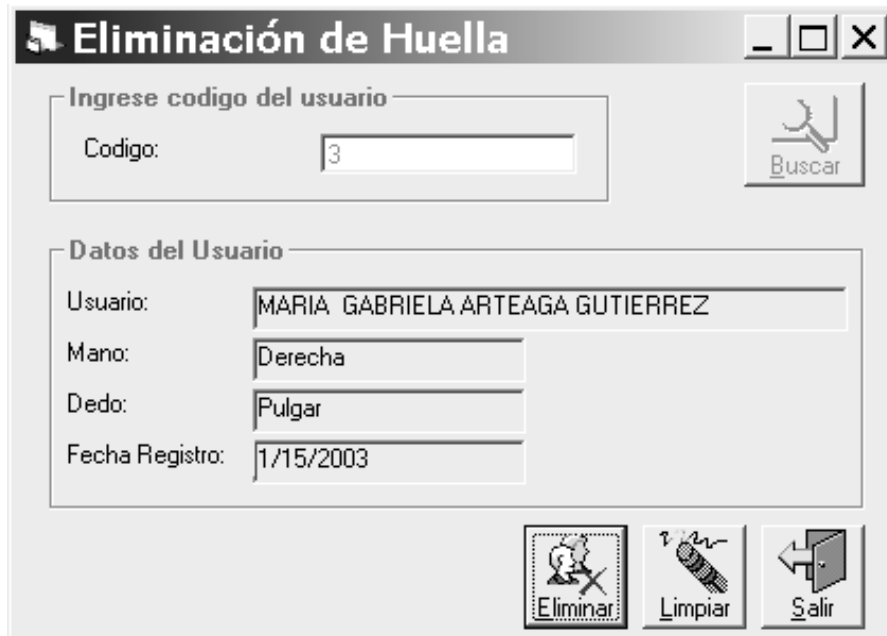
Figura 34. Verificación de huella



4.4.3.3 Eliminación de huella

En esta opción se elimina un plantilla asociada al código de identificación personal que el usuario ingrese, el cual es verificado previamente en la base de datos. La figura que se muestra a continuación representa esta opción.

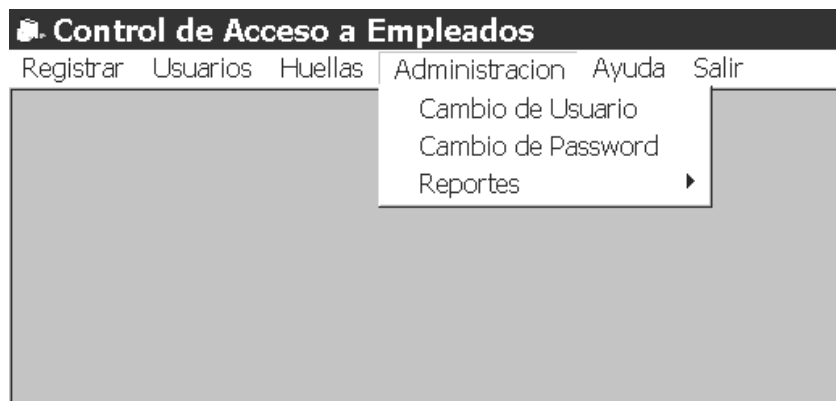
Figura 35. Eliminación de huella



4.4.4 El menú administración

Este menú permite llevar reportes de los usuarios. Al igual que el menú huellas, para poder ingresar a cualquier opción se debe ingresar la clave del administrador.

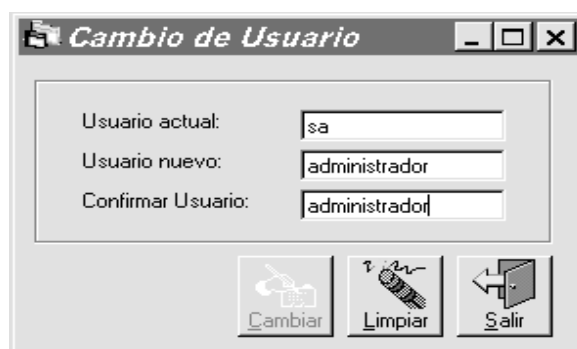
Figura 36. Menú administración



4.4.4.1 Cambio de usuario

En esta opción se puede cambiar el usuario administrador ingresando el nombre del usuario actual y un nuevo nombre solicitando una confirmación, y si es válida, se actualiza el registro en la base de datos. A continuación se muestra la figura.

Figura 37. Cambio de usuario



The screenshot shows a window titled "Cambio de Usuario". Inside, there are three text input fields. The first is labeled "Usuario actual:" and contains the text "sa". The second is labeled "Usuario nuevo:" and contains "administrador". The third is labeled "Confirmar Usuario:" and contains "administrador". Below these fields are three buttons: "Cambiar" (with a keyboard icon), "Limpiar" (with a trash can icon), and "Salir" (with a door icon).

4.4.4.2 Cambio de clave

En esta opción se puede cambiar la clave del supervisor, ingresando la clave actual y la nueva solicitando una confirmación.

Si es válida, se actualiza el registro en la base de datos. A continuación se muestra la figura.

Figura 38. Cambio de clave

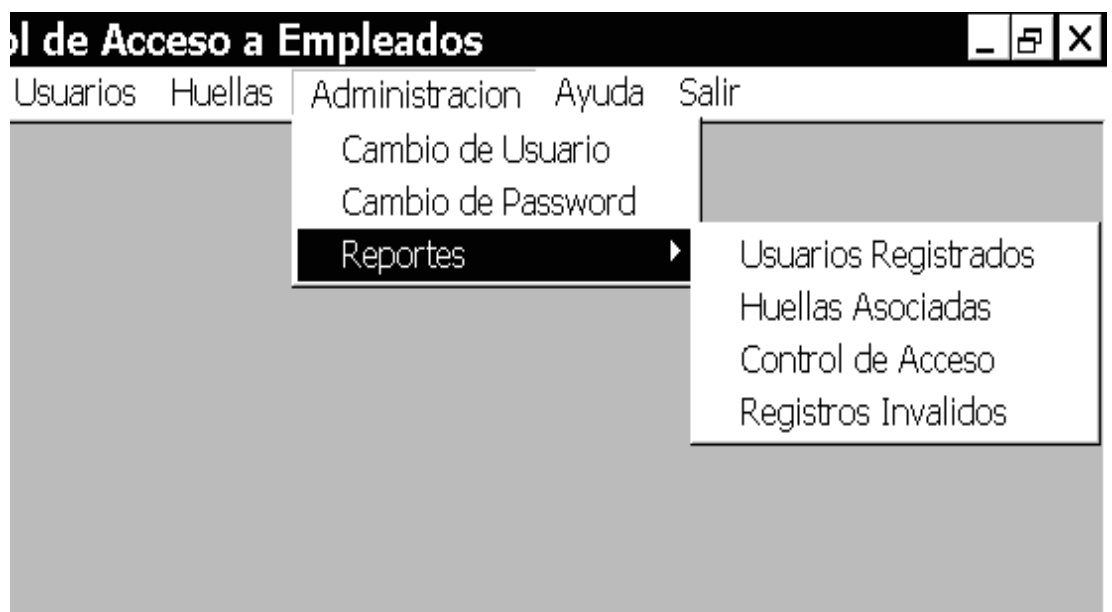


The screenshot shows a window titled "Cambio de Clave". Inside, there are three text input fields. The first is labeled "Password actual:" and contains three asterisks "***". The second is labeled "Password nuevo:" and contains four asterisks "****". The third is labeled "Confirmar Password:" and contains four asterisks "****". Below these fields are three buttons: "Cambiar" (with a keyboard icon), "Limpiar" (with a trash can icon), and "Salir" (with a door icon).

4.4.4.3 Reportes

Este menú permite llevar el control de las entradas y salidas de los usuarios y sus datos, generando reportes que pueden ser impresos o almacenados en archivos de *Excel*. Estas opciones se muestran en la siguiente figura.

Figura 39. Menú de reportes



4.4.4.3.1 Usuarios registrados

Reporte de los datos de los usuarios registrados en el sistema. Se muestra en la figura 40.

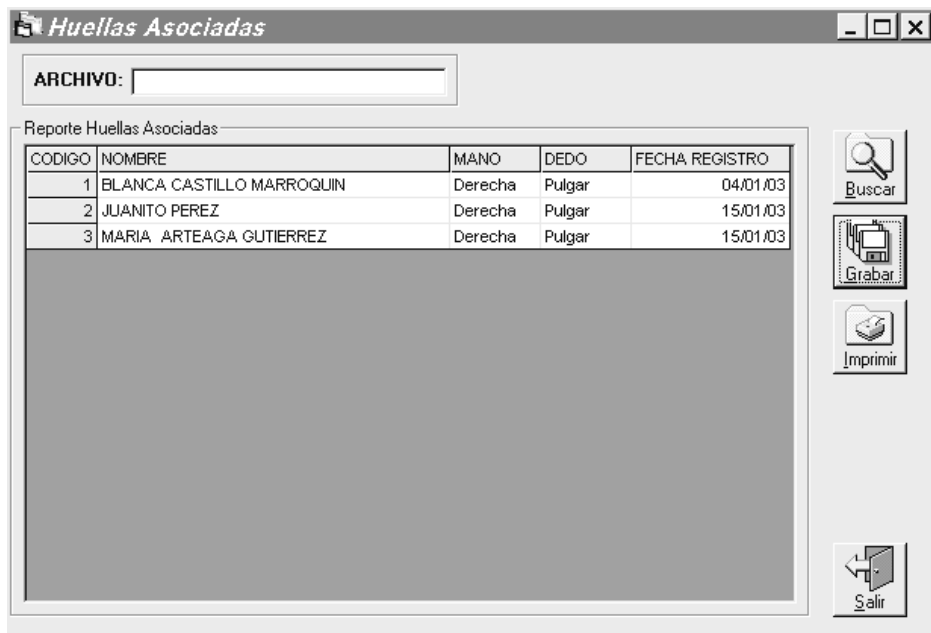
4.4.4.3.2 Huellas asociadas

Reporte de usuarios que tienen huella registrada en el sistema y la fecha de registro de la misma. Esta opción se muestra en la figura 41.

Figura 40. Usuarios registrados



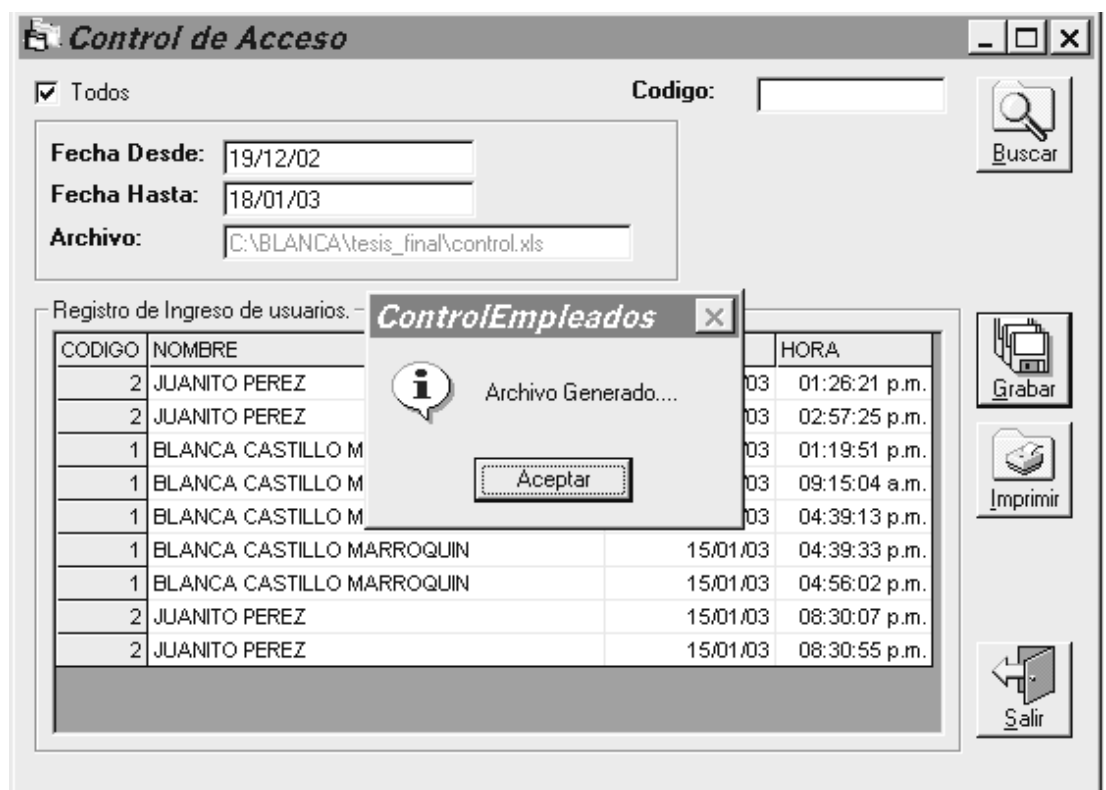
Figura 41. Huellas asociadas



4.4.4.3 Control de acceso

Muestra un listado por fechas de todos los ingresos al sistema, en este se incluye el código del usuario, nombre, fecha y hora de acceso. Véase figura a continuación.

Figura 42 Control de acceso



4.4.4.3.4 Registros inválidos

Muestra un listado por fechas de todos los intentos de ingresar al sistema con una huella que no es la correcta. Véase figura 43.

Luego de generar un reporte, puede ser almacenado como un archivo de *Excel*. La figura 44 muestra un ejemplo de un archivo de control de acceso generado en *Excel*.

Figura 43. Registros inválidos



Figura 44. Reportes de control de acceso

Microsoft Excel - control

Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

B8 = 2

| | A | B | C | D | E | F |
|----|---|-------------------------------|------------------------------|--------------|---------------|---|
| 1 | | | | | | |
| 2 | | | CONTROL DE ACCESO A USUARIOS | | | |
| 3 | | | | | | |
| 4 | | REPORTE: Control de Acceso | | | | |
| 5 | | FECHA: 18/01/03 10:03:04 a.m. | | | | |
| 6 | | | | | | |
| 7 | | CODIGO | NOMBRE | FECHA | HORA | |
| 8 | | 2 | JUANITO PEREZ | 01/01/03 | 01:26:21 p.m. | |
| 9 | | 2 | JUANITO PEREZ | 01/01/03 | 02:57:25 p.m. | |
| 10 | | 1 | BLANCA CASTILLO MARROQUIN | 02/01/03 | 01:19:51 p.m. | |
| 11 | | 1 | BLANCA CASTILLO MARROQUIN | 11/01/03 | 09:15:04 a.m. | |
| 12 | | 1 | BLANCA CASTILLO MARROQUIN | 15/01/03 | 04:39:13 p.m. | |
| 13 | | 1 | BLANCA CASTILLO MARROQUIN | 15/01/03 | 04:39:33 p.m. | |
| 14 | | 1 | BLANCA CASTILLO MARROQUIN | 15/01/03 | 04:56:02 p.m. | |
| 15 | | 2 | JUANITO PEREZ | 15/01/03 | 08:30:07 p.m. | |
| 16 | | 2 | JUANITO PEREZ | 15/01/03 | 08:30:55 p.m. | |
| 17 | | | | | | |
| 18 | | | | | | |

CONCLUSIONES

1. Como todas las nuevas tecnologías, la investigación biométrica empezó por la necesidad de incrementar las herramientas de defensa del ejército estadounidense, pero actualmente ya se han desarrollado algunas aplicaciones en el sector privado para el control de acceso de usuarios.
2. La biometría busca la automatización de tareas que involucran el reconocimiento del individuo y puede proveer un control eficiente y preciso de las personas, en el cual se puede saber con un alto grado de exactitud que la persona que utilizó un dispositivo biométrico es la persona a ser reconocida.
3. En general, todos los sistemas biométricos se basan en un proceso que se inicia con el suministro de una muestra o característica, ya sea física o del comportamiento, con la cual se genera un patrón de registro que servirá para buscar correlaciones con el patrón de verificación.
4. Existe una variedad de características de medición en la tecnología biométrica que se pueden utilizar en diferentes aplicaciones, entre ellas las más comunes son la huella digital, el reconocimiento de voz, la geometría de la mano, la firma digital y el reconocimiento de los patrones oculares.

5. La tecnología biométrica puede utilizarse en múltiples aplicaciones, entre ellas se puede mencionar aplicaciones de comercio electrónico, control de acceso, sistemas de salud, sistemas bancarios, aeropuertos etc.

6. Mientras menos intimidante sea el dispositivo biométrico que se utilice en una aplicación, más rápidamente será aceptado. Una de las desventajas de los lectores de los métodos basados en el análisis de patrones oculares es su escasa aceptación, ya que el usuario tiene que mirar a través de un binocular, algo que no es cómodo ni aceptable para muchos de ellos.

RECOMENDACIONES

1. No es posible aseverar que una tecnología biométrica es mejor que otra, ya que cada una de las tecnologías tiene su aplicabilidad dentro de los sistemas de seguridad. Al momento de elegir dispositivos biométricos, deben considerarse varios factores entre los que se puede mencionar: facilidad de uso, precisión, costo, aceptación por el usuario, estabilidad, etc.
2. Cada una de las técnicas de la tecnología biométrica posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir qué técnica utilizar para una aplicación específica. Una compañía que va a utilizar alguna de estas técnicas debe evaluar las características de cada una, y de acuerdo a ello elegir la más adecuada, incluso puede decidir el uso de distintas técnicas en distintos ámbitos.

BIBLIOGRAFÍA

1. ABIE Agrupación de biometría informática española. <http://www.ii.uam.es/~abie> España: (2002).
2. Aplicaciones en biometría. <http://www.ast-afis.com/es/es-ID3.htm>.
3. Biometría. www.ast-afis.com/biometria.htm.
4. Biométrica. <http://www.aunmas.com/guias/criptologia/biometrica.htm>.
5. Ictnet comunidades. www.ictnet.es/ictnet/cv/comunidad.jsp.
6. Identificación biométrica. <http://www.iec.csic.es/criptonomicon/articulos/expertos73.html>.
7. Identificación biométrica. [http://www.uagro.mx/dependencias/Guadalupe/automatizacion %20 y%20nuevas%20tecnologias/sld011.htm](http://www.uagro.mx/dependencias/Guadalupe/automatizacion%20y%20nuevas%20tecnologias/sld011.htm).
8. Insys soluciones biométricas. [http://www.insys.com.mx/biometria/ biometría.htm](http://www.insys.com.mx/biometria/biometria.htm).
9. La biometría. <http://www.imcyc.com/cyt/enero02/biometria.htm>.

10. La biométrica y la seguridad. <http://www.almargen.com.ar/sitio/seccion/tecnologia/biometrica/>.
11. Qué es biométrica. <http://www.saltillonet.com/articulos/biometrica/>.
12. ¿Qué es la biometría? <http://www.nrtec.com.mx/biometria.htm> México: (2001).
13. Qué es la biometría. <http://www.e-printing.com.ar/Bio.htm>.
14. Reconocimiento de voz. <http://acceso.uv.es>. España: (2001). México: (2002).
15. Soluciones bancarias. <http://www.homini.com/bancaria.htm>.
16. Tecnología biométrica. [http://www.securynet.com/rubros/rev/julio_2001/32\(ts7+ts15+ts2+ts3\).htm](http://www.securynet.com/rubros/rev/julio_2001/32(ts7+ts15+ts2+ts3).htm).