UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"DISEÑO Y DESARROLLO DE UN SISTEMA BIOMÉTRICO POR HUELLA DIGITAL, PARA EL CONTROL DE ACCESOS A UNA INTRANET"

T E S I S

Que para obtener el título de:

INGENIERO EN COMPUTACIÓN

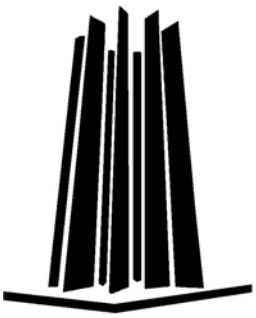
P R E S E N T A N:

ERIKA ORTEGA ARGÜELLES

Y

ALFONSO A. MARTÍNEZ NÚÑEZ

ASESOR: M. EN C. LEOBARDO HERNÁNDEZ AUDELO



MÉXICO 2006

Alfonso Alejandro Martínez Núñez
Erika Ortega Argüelles

DISEÑO Y DESARROLLO DE UN SISTEMA BIOMÉTRICO POR HUELLA DIGITAL, PARA EL CONTROL DE ACCESOS A UNA INTRANET.

Incluye CD-ROM
con código fuente

AGRADECIMIENTOS

A Dios:

Por enseñarme que los sueños sólo son realizables hasta que se intentan alcanzar; y aún si se falla, mantener la certeza de que si se mejora, entonces se podrán obtener.

A mi Madre:

Quien es y será por siempre, mi fuente de superación y ejemplo de trabajo. Por su Amor y apoyo incondicional.
Por ser mi Todo….

A mi Padre:

Por tu entrega y arduo esfuerzo por darnos el mejor legado de vida: La carrera Universitaria.
Tus manos son muestra de ello.

A mis hermanos y Tíos:

Porque espero ser y seguir siendo un ejemplo digno de ustedes.

A Leo:

Por su enorme apoyo y paciencia que nos brindó para la elaboración y mejora constante de este trabajo.
Nunca lo olvidaré.

A mi esposo:

Gracias por compartir el desarrollo de este trabajo hasta su finalización, y por ser testigo de este sueño personal.

A mis Maestros y la Universidad:

Que me dieron las bases del conocimiento, me inculcaron disciplina y valores humanos importantes para recorrer este camino.

Con todo mi amor, a todos ustedes.

Akire -<-<@

A mis Padres:

Por mostrarme que el camino del bien y el esfuerzo, es lo que me ha permitido lograr éste y mis demás objetivos personales.

A mi Esposa:

Por ser el motor y el motivo de todo lo que realizo en la vida y a quien debo todo el éxito de este logro.
Mil gracias y todo mi amor….

Con todo mi cariño y respeto.

Alfonso

ÍNDICE

RESUMEN

El presente trabajo pretende dar al lector, un acercamiento al área de la Biometría y muy particularmente, a los servicios de *Control de acceso y Autenticación.*

En concreto, está enfocado en el reconocimiento de huellas dactilares, presentando como caso práctico el desarrollo de un sistema que soportado por una base de datos y mediante la integración de un dispositivo lector de huellas dactilares, permite llevar la administración de las identidades de usuario para el acceso a una Intranet.

El sistema opera sobre una arquitectura cliente-servidor, y está orientado a un ambiente web.

Para el proceso de autenticación, se hace uso del algoritmo de comprobación de plantillas basado en la extracción de "minutiaes", donde cada usuario para acceder al sistema, es autenticado mediante la lectura de su huella dactilar.

PALABRAS CLAVE

Seguridad, Control de Acceso, Autenticación, Biometría, Criptografía, reconocimiento, huellas dactilares, plantilla, web, Tomcat, Java, MySQL.

NOTACIONES

- Se presentan en letras itálicas y negritas, los conceptos o términos nuevos que van siendo citados a lo largo del texto, y que son considerados importantes a resaltar. Por ejemplo:

  vulnerabilidad es cualquier debilidad que pueda explotarse para causar pérdida o daño a la información y/o sistema, ***riesgo*** cualquier posibilidad de causar daño sobre un activo; y ***daño***, el resultado de la amenaza y/o ataque tras explotar una vulnerabilidad.

- Se presentan entre paréntesis, ejemplos y/o significados textuales de alguna abreviatura en el idioma inglés o español. Por ejemplo:

  AFIS (Automated Fingerprint Identification System)
  TFR (Tasa de Falso Rechazo)
  MAD (Control de accesos discrecional)
  Característica física (huella, iris, pupila, etc.)

- Se presentan en letras itálicas, negritas y entre comillas, cuando se hace referencia a algún subcapítulo o anexo en particular, que puede ser consultado para mayores detalles. Por ejemplo:

  Los detalles respecto a este procesamiento de la huella, son tratados en el subcapítulo ***2.2 "El papel de la huella y su proceso de obtención de minutiaes".***

- Se presentan en letra regular e itálica, los nombres de los casos de uso y/o clases de la base de datos. Así mismo, cuando se hace referencia a alguna figura o tabla en particular a ser consultada. Por ejemplo:

  AutenAdmin, AutenBio, RegistraUser
  Ver Figura 3

- Se presentan entre dobles signos de mayor y menor << >>, sinónimos, términos o comentarios para puntualizar mejor la idea que se desea transmitir. Por ejemplo:

  patrón biométrico <<plantilla>>
  validando si <<es quién dice ser >>

- Se presentan entre comillas " ", conceptos o términos citados en modo literal o que son coloquiales. Por ejemplo:

  "lo que se tiene", "lo que se es" , "huella viva o huella actual", "cookies"
- Se presentan entre signos de mayor y menor < >, el significado del término antecesor. Por ejemplo:

  bio <vida> y metría < medida>

- Se presentan en letra regular, negritas y dentro de un recuadro, las fórmulas y ecuaciones. Por ejemplo:

  $$\mathbf{C = E_{Kpb}\ (M)}$$

- Se presentan entre corchetes [ ], con letras itálicas de tamaño 10, las referencias sobre libros o artículos consultados, en los cuáles se pueden obtener mayores detalles sobre el texto citado. Por ejemplo:

  Algunos otro algoritmos que integran esta clasificación, son: IRC5 y Rijdael (propuesta de nvo. estándar mundial) ***[RFC7,Mod2,p.37]***.

  En este ejemplo se hace referencia al libro 7 listado en el apartado de referencias, módulo 2, página 37.

- Se presentan con números superíndices de tamaño 10, las citas o notas aclaratorias. Los pies de página se denotan con letra regular de tamaño 10. Por ejemplo:

  Para entender los factores y requerimientos del sistema fue necesario identificar los ***actores***[17] y los escenarios involucrados en el desarrollo del sistema. Estos escenarios dan lugar a los ***casos de uso*** [18], los cuáles son la interacción generada por el usuario y el sistema de cómputo.

  [17] Actores del sistema son aquellos usuarios que interactúan con el sistema.
  [18] Los casos de uso son aquellas tareas en las cuáles están involucrados los actores.

- Se presentan en letras versales, negritas y de tamaño 13, los títulos de los subcapítulos. Por ejemplo:

  1.1 SEGURIDAD

- Se presentan en letras mayúsculas, negritas y de tamaño 26, los títulos de: capítulos, prólogo, referencias, resumen, anexos.

- Se presenta en letra regular y negritas, el texto para puntualizar una serie de pasos, etapas, clasificación o desglose de puntos. Por ejemplo:
  1. **Usuario o grupo de usuarios** (individuos que intentaran autenticarse ante el sistema)
  2. **Dueño o administrador del recurso** (quien decide los mecanismos necesarios de autenticación).

PRÓLOGO

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo hoy en día un nuevo campo llamado Seguridad Informática, como una de las áreas más demandadas de los últimos tiempos, que poco a poco ha ido cobrando relevancia en empresas de diversos sectores, preocupadas por mantener seguros sus activos informáticos que las integran. Lo anterior en gran parte, como resultado del proceso de concientización que se ha venido dando a través de diversos medios, en cuanto a Seguridad Informática y seguridad de la información se refiere, haciendo que muchas empresas se den a la búsqueda constante por garantizar su correcto funcionamiento y operación día a día, mediante el uso e implementación de mecanismos, modelos y medidas de seguridad, para otorgar niveles de protección mayores contra accesos no autorizados, ataques, robo, daño, fisgoneo o alteración en sus sistemas.

Debido a lo anterior, la evidente necesidad de contar con un control estricto sobre los accesos de usuarios a los recursos informáticos, ha conllevado a nuevos retos de autenticación para distinguir de manera efectiva entre los usuarios legítimos y los intrusos, y con ello, otorgar o denegar el acceso a los recursos; garantizando un cierto nivel de seguridad en los sistemas, mediante la correcta administración de identidades de usuario.

Considerando que los mecanismos de autenticación tradicionales se encuentran basados en el uso de contraseñas secretas e invariables, que necesariamente son compartidas entre usuario-sistema que por su propia naturaleza presentan serios problemas de seguridad, el surgimiento y desarrollo de nuevos mecanismos y tecnologías más avanzadas para la validación de identidades de usuario se ha visto impulsado de manera sorprendente en los últimos días, haciendo que el mercado de

la Seguridad Informática fije especial interés en los servicios de ***Control de acceso y Autenticación*** como piezas fundamentales para brindar un primer nivel de seguridad en los sistemas o áreas a proteger.

Dentro de las nuevas tecnologías aplicadas al proceso autenticación de usuarios, la industria biométrica es de las más relevantes en la actualidad, al resolver en gran medida los problemas comunes de compromiso, divulgación, desconfiguración, daño, robo y olvido, que los mecanismos de autenticación tradicionales presentan. Dando así, batalla a uno de los mayores huecos de seguridad actuales.

Si bien la tecnología biométrica hasta hace años era considera no muy confiable, lo cierto es que este tipo de tecnología ha venido madurando y desarrollándose a pasos agigantados, pasando hoy en día por un momento muy particular de su existencia debido en gran parte a circunstancias mundiales (ataques terroristas, necesidad de identificación de delincuentes, control de acceso en empresas, embajadas, etc.), que la han forzado hacia un desarrollo precipitado como resultado del grado de concientización y obsesión de los últimos tiempos por mantener la seguridad en los diversos sectores.

Dentro de la industria biométrica, la basada en huella digital es hoy por hoy una de las “consentidas”; principalmente por su facilidad de uso, no tan elevado costo en relación al universo de biométricos, y porque se trata de una de las tecnologías mayormente maduras que además no presenta tantos problemas técnicos.

Su relevancia radica en que a través de su uso, se elimina el uso de passwords o números de identificación complejos que el usuario normalmente tiene que recordar, permitiendo validar la identidad de los individuos de forma única y mayormente segura a través de la lectura de su huella. Lo anterior no solo hace del proceso algo más amigable, sino lo más importante: soluciona en gran parte, el problema de suplantación de identidades al aprovechar las propiedades de unicidad e intransferencia de la huella.

Bajo este contexto, y partiendo de la necesidad por mantener protegidos los recursos informáticos contra accesos no autorizados de enemigos reales, potenciales e imaginarios, sin descartar alguno de estos, el tema del presente trabajo representa un esfuerzo conjunto por transmitir el importante papel que juegan los servicios de Control de Acceso y Autenticación dentro del ámbito de la Seguridad Informática. Adicionalmente, se aprovecha el espacio para dar a conocer lo que es la tecnología biométrica por huella digital y sus ventajas, como tecnología de vanguardia para validar de forma mayormente confiable la identidad de los usuarios.

La parte medular del trabajo consiste en el diseño, desarrollo e implantación de un Sistema Biométrico para el control de accesos de una Intranet, integrando un lector de huella digital para llevar a cabo la autenticación de los usuarios de forma segura, única e intransferible.

El sistema opera bajo un ambiente cliente-servidor, soportado por una base de datos de tipo relacional que permite la posibilidad de autenticación de un usuario dado de alta previamente en el sistema, a través de la captura de su huella, y su comparación con el patrón biométrico almacenado en la BD.

La estructura del trabajo se encuentra diseñada de forma estratégica, iniciando con algunos antecedentes históricos que marcaron el surgimiento de los problemas de seguridad en el mundo informático hasta llegar a nuestros días en que se considera a la seguridad como una necesidad tal, dada la variedad de problemas a los que se debe enfrentar.

El Capítulo 1 inicia con algunas precisiones conceptuales en cuanto al ámbito de Seguridad Informática se refiere, proporcionando además, una introducción a lo que es la Criptografía dado el papel que ésta tendrá en el presente proyecto a través del protocolo SSL utilizado para cifrar toda la información que viaja a nivel cliente-servidor-cliente en el ambiente Web (Intranet). Así mismo, se analizan los principales modelos de Control de Acceso y Autenticación, finalizando con una introducción respecto a la tecnología biométrica por huella digital.

Adentrándose al tema central del proyecto, en el Capítulo 2 se aborda el papel de la huella digital enfocado al proceso de autenticación de usuarios, dando un panorama general sobre el procesamiento de la huella. Así mismo, se citan las principales ventajas y desventajas del utilizar tecnología biométrica aplicada en el proceso de autenticación de usuarios, detallando además, la tendencia en el ámbito.

En el Capítulo 3 se presenta el caso práctico, el cuál consiste en el desarrollo de un Sistema Biométrico por huella digital para el control de accesos a una Intranet. El capítulo se encuentra desglosado en las fases de análisis, diseño y desarrollo del sistema; detallando así mismo, las tecnologías utilizadas para llevar a cabo el desarrollo del mismo: lenguaje seleccionado, JAVA; Tomcat como contenedor de servlet's, Jsp's y servidor web; MySQL como manejador de base de datos.

Como Capítulo 4 se presenta la validación del sistema en términos de falsos rechazos y falsas aceptaciones.

Finalmente, en el Capítulo 5 se presentan los resultados, las conclusiones y trabajo a futuro.

Al término del trabajo se integran como anexos: manuales de usuario y Administrador del sistema; requerimientos técnicos para la operación del sistema, y las referencias utilizadas para el desarrollo del trabajo. Dichas referencias podrán ser consultadas para un mayor detalle de los conceptos analizados y como fundamento de lo plasmado a lo largo de los capítulos.

CAPÍTULO 1. INTRODUCCIÓN

"La Seguridad es una necesidad intrínseca que tiene sus orígenes desde tiempos ancestrales, que debido a su paralelismo con el desarrollo humano, es hoy en día una profesión compleja con funciones especializadas"[RFC1]

En el presente capítulo se analizan los principales elementos involucrados que fundamentan la temática del proyecto. Con la finalidad de dar una visión general al lector sobre el tema y facilitar así su comprensión, el capítulo inicia destacando los principales antecedentes y conceptos en torno a lo que es el área de Seguridad Informática y el impacto que ésta ha tenido a lo largo de los años.

Como elemento importante en el área de Seguridad, se describen las bases de Criptografía[1] y su aplicación, para la protección de datos; se analizan los principales tipos de ésta (simétrica, asimétrica y funciones hash), y sus características.

Analizado lo anterior, se dedica un subcapítulo para tratar lo que es el protocolo SSL[2] tras ser uno de los elementos utilizados en el caso práctico de este trabajo, para llevar a cabo la encripción de datos durante el intercambio de información a nivel cliente-servidor-cliente.

Adentrados en el tema, se aborda lo que es el Control de Acceso y Autenticación, servicios de seguridad considerados como vitales para poder brindar un nivel de seguridad básico en los sistemas informáticos, y así lograr distinguir entre los usuarios legítimos y los intrusos[3]. Aunado a ello, se detallan algunos de los factores de identificación más comunes y los elementos que deben ser considerados para seleccionar el método de autenticación idóneo, tomando en cuenta la necesidad específica que se tenga y el nivel de seguridad requerido.

---

[1] Criptografía es la ciencia que consiste en transformar un mensaje legible en otro que no lo es, mediante la utilización de claves, que solo el emisor y receptor conocen, con la finalidad de compartir y transmitir información de forma segura. Ver detalles en el subcapítulo ***"1.2 Criptografía"***

[2] Refiérase a protocolo, como el conjunto de normas (lenguaje de reglas, formatos de mensaje y símbolos) que rige cada tipo de comunicación entre dos o más equipos, para hacer posible el intercambio de información. Particularmente el protocolo SSL es un protocolo para proveer una conexión segura entre dos equipos. Ver detalles en el subcapítulo ***"1.3 SSL (Secure Sockets Layer)"***

3 Intruso es aquél ente, que con una variedad de acciones intenta comprometer un recurso, puede ser por hardware o software.

Finalmente al término del capítulo, se analiza detalladamente el tema central del trabajo: la tecnología biométrica por huella digital, su surgimiento, sus ventajas (y porqué no, también sus desventajas) y su campo de aplicación. Elementos que permitirán al lector, saber el porqué de la relevancia del tema seleccionado y tener en claro cuál es el propósito del proyecto aquí presentado.

1.1 SEGURIDAD

1.1.1 Antecedentes

Para conocer y adentrarse a lo que es el ámbito de la seguridad en el mundo informático, resulta conveniente hacer referencia a algunos acontecimientos históricos importantes que marcaron el surgimiento potencial de los problemas de seguridad que hoy en día no solo involucran problemas a nivel PC's de usuario, sino que debido al avance de la tecnología como el surgimiento de ambientes multitareas, multiusuarios, plataformas abiertas, equipos de propósito general y las redes[4], han llevado el problema a niveles caóticos de seguridad.

Como resultado de toda esta problemática en el mundo informático, el Control de Acceso como área, ha tomado especial interés en los últimos tiempos dada la importancia de mantener protegidos los activos informáticos, llámese software, hardware[5] y datos[6], contra accesos no autorizados, robos, daño u alteración.

Aunque los problemas de seguridad tienen su origen desde hace varios miles de años con el surgimiento de la información, la escritura, el lenguaje y la necesidad intrínseca de procesamiento, adquisición y transmisión a través de los diferentes medios que en aquél entonces existían, fue la Era Digital la que marcó la revolución en el área de Seguridad con el surgimiento de los primeros equipos de cómputo.

En 1943 en el Laboratorio Bletchley Park se enciende la primera computadora electrónica programable llamada Colossus, y en 1946 se construye la ENIAC

[4] Una Red es un conjunto de computadoras, impresoras, routers, switches y otros dispositivos, comunicados entre sí por algún medio de transmisión.

[5] Refiérase como hardware, a todos los componentes físicos y tangibles que conforman un sistema de cómputo como lo son: unidades de disco, tarjetas, microprocesador, memoria, etc.; y software, el conjunto de programas (o información) como lo son: archivos, directorios, programas ejecutables, bases de datos, utilerías, aplicaciones, controladores, etc; que son interpretados y ejecutados por el equipo de cómputo.

[6] Datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: texto (colección de palabras), campos de datos, registros, archivos y base de datos, hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

(Electronic Numerical Integrator and Computer) totalmente electrónica, de bulbos y digital. Su construcción en realidad se inicia en 1943 y se termina en 1946. Es construida por Mauchly y Eckert, pesaba 30 toneladas y contenía 18,000 bulbos. Fue la primera computadora universal y podía realizar 100,000 operaciones por segundo.

Pocos años después, se crea la UNIVAC (UNIVersal Automatic Computer) desarrollada por Presper Eckert y John Mauchly. Computadora programable, considerada la primera que se vendió comercialmente, costando más de 1 millón de dólares.

En 1960 la compañía Digital anunció la primera computadora pequeña, la PD-1 (Programmed data processor-1) diseñada por Ben Gurley.

En 1975 se inventa la Altair 8800, siendo la primer computadora personal (microcomputer) con un microprocesador intel 8080 y 256 bytes de memoria. En 1981 IBM introduce la computadora personal (PC), una micro computadora con arquitectura no propietaria desarrollada alrededor de la familia de procesadores Intel 8086, dando pauta a que la computadora pudiera llegar al hogar, escuelas y oficinas.

De allí hasta nuestra actualidad, el problema de seguridad se fue agrandando cada vez más al surgir nuevas formas y medios para manipular la información; siendo la segunda guerra mundial un factor importante que marcó la historia de la Seguridad Informática, donde las técnicas de ocultamiento ya no solo se utilizaban en el ámbito militar, sino en sectores gubernamentales, diplomáticos, científicos, técnicos e industriales.

En aquél entonces las computadoras eran de propósito específico y los equipos se encontraban centralizados. Después de la segunda guerra mundial éstas se volvieron multiusuario y multitarea, haciendo del problema de seguridad un verdadero dolor de cabeza. Adicional a ésto, surgen las redes de computadoras (1964 primer red LAN[7] y 1966 primera red WAN ARPAnet), haciendo de la situación un problema patológico debido a que ahora además de proteger la información era necesario cuidar de los canales públicos y abiertos.

Adicionalmente, se da el surgimiento de los sistemas operativos[8], la compartición de recursos (memoria, procesador, impresoras, etc.); interacción remota con las computadoras, diversidad de protocolos de comunicación, entre otros.

---

[7] LAN (Local Area Network - Red de Área Local), es una red de computadoras para dar servicio a un área geográfica pequeña, por ejemplo un edificio.

[8] El sistema operativo es un componente de tipo software, encargado de ejecutar, administrar, y controlar, los recursos físicos del sistema de cómputo (HW) y su interrelación con el software (SW), para hacer posible la operación del sistema. Se puede tener el mejor equipo de cómputo (el mejor hardware), pero si no se tiene instalado un sistema operativo, no funcionará (ni siquiera se podrá encender). Algunos ejemplos de sistemas operativos son: Windows98/2000/NT, MS/DOS, UNIX, Linux, etc.

Como puede apreciarse, el problema de seguridad se acrecienta, al llegar a nuestra actualidad donde muchas de las tareas se realizan a través de redes de todos tipos; desde comunicaciones y transferencia, proceso y acceso de información, hasta servicios bancarios, dinero y comercio electrónico. Es decir, se tiene ahora un universo no acotado de computadoras multiusuario heterogéneas, no seguras, intercomunicándose a través de dominios de seguridad sin políticas **[RFC7,p.30]**

Es así como el área de Seguridad Informática toma especial impulso, consolidándose hoy por hoy, como una de las áreas más demandadas en el mercado informático al tenerse la necesidad permanente de proteger la información, así como los recursos físicos y lógicos de las computadoras y redes, contra accesos no autorizados, virus informáticos, gusanos, etc; identificándose como factor común en todo esto, la necesidad e importancia del ***Control de Acceso***.

Éste último, considerado como elemento primario de defensa de los sistemas informáticos, para garantizar que solo los usuarios legítimos con privilegios definidos tengan acceso a los activos informáticos vía un proceso previo de autenticación (a través de una llave, password, token, característica física (huella, iris, pupila, etc), tarjeta inteligente, entre otros).

De acuerdo a hallazgos arqueológicos[9] que demuestran el uso de dispositivos tales como cerraduras, trampas, sistemas de alarmas y murallas, para mantener protegidos los recursos, el aspecto de la seguridad data desde épocas muy remotas. Épocas donde indudablemente la seguridad y mecanismos rudimentarios para restringir el acceso ya eran considerados, pero en donde el ser humano ni siquiera imaginaba la evolución y la relevancia que éstos tendrían, hasta llegar a nuestros días donde existen dispositivos bastantes sofisticados basados en tecnología de vanguardia como lo es la tecnología biométrica. Esta tecnología en los últimos años ha alcanzado un nivel de madurez importante, al permitir validar la identidad de los usuarios para otorgarles el acceso a los sistemas o áreas restringidas mediante la lectura de una o varias características físicas (huella digital, mano, pupila, iris, etc.); haciendo del proceso de autenticación, un proceso mayormente confiable y seguro.

[9] La más antigua cerradura conocida, data del 4000 a.c., y fue encontrada en el Palacio de Sargon, Khorsabad, cerca de Nineveh. En el mismo periodo, el dibujo de la cerradura fue realizado en el Templo de Karnak, en el valle del Nilo. En el 1000 a.c., el Dios egipcio fue representado con una llave en su mano derecha. **[RFC1]**

1.1.2 Fundamentos

"El conocimiento es el medio para dar batalla al problema de seguridad, lo cuál dará la visión para llevar a cabo un análisis sobre los riesgos, las vulnerabilidades, amenazas y contramedidas; evaluar las ventajas o desventajas de la situación y decidir sobre medidas técnicas, tácticas, metodológicas, físicas e informáticas más convenientes, en base a la necesidad específica que se tenga".

Teniendo un panorama mas claro sobre la evolución que se ha venido dando, los factores que han incrementado el problema de seguridad en el mundo informático, y la importancia que tiene el Control de Acceso como elemento primario para garantizar un nivel mínimo de seguridad, podrá comprenderse con mayor precisión particularidades del tema.

Con la finalidad de dejar en claro los conceptos principales de la Seguridad Informática y estandarizar términos para el mejor entendimiento del tema, en el presente subcapítulo se realizan algunas precisiones.

Para dar inicio, es preciso referirse a la ***Informática*** como área encargada del manejo de la información desde su creación, adquisición, sistematización, transmisión y almacenamiento; y como elementos básicos a proteger que conforman un sistema informático: ***hardware, software y datos.*** De estos 3 elementos, la información o datos representan los activos[10] más importantes debido a que son el resultado del trabajo realizado y del conocimiento adquirido a lo largo del tiempo, que a diferencia del software y/o hardware, su recuperación ante cualquier desastre o ataque informático es casi imposible, salvo que se tenga un buen mecanismo de backup's[11].

Tomando como referencia esto, la información presenta 4 estados principales (creación, adquisición, transmisión, y almacenamiento) y para cada uno de ellos, la Seguridad Informática busca brindar 5 ***servicios básicos de seguridad***:

> **Confidencialidad**: Que la información solo la conozcan o tengan acceso, quienes tengan autorización para ello. Para garantizar ésto, es común utilizar mecanismos de cifrado.
>
> **Disponibilidad**: Que la información o activo específico, se encuentre accesible para su uso en el momento que los usuarios legítimos lo requieran. Este servicio no puede garantizarse.

[10] Se denomina Activo, al elemento de cómputo o valor a proteger; pudiendo ser software, hardware y/o datos.

[11] Backup es una copia de seguridad o respaldo de información, que se realiza con el fin de mantener los datos en forma segura. Generalmente las copias son hechas en cintas, discos o algún otro dispositivo de almacenamiento.

Autenticidad: Que la información o activo específico provenga de fuentes válidas y autorizadas. Que los usuarios que accedan a la información sean quienes dicen ser.

Integridad: Que la información de los sistemas solo pueda ser creada o modificada por usuarios autorizados. Es decir, que no sea alterada sin autorización, o por errores de software o hardware.

No repudio: Se trata de obtener una evidencia contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje, u originado o haber sido el destinatario de una acción.

Partiendo de lo anterior, ***el objetivo principal de la Seguridad Informática es, proteger la información, procurando en la mayor medida posible mantener las propiedades citadas.***

Para ello un ***sistema informático*** se define como el conjunto conformado por hardware, software y datos, donde en términos generales el ***software*** son todos los elementos lógicos del sistema (sistema operativo, aplicaciones, etc.); el ***hardware*** todos los elementos físicos (CPU, impresoras, unidades de CD-ROM, equipos, cintas, cableado, componentes de comunicación, etc.). Los ***datos*** son el conjunto de información lógica que es manipulada a través del software y el hardware, tal como documentos, archivos, base de datos, etc.

Aunado a lo anterior, algo importante a saber es <<QUÉ>> se busca proteger, de <<QUIÉN>> y <<DE QUÉ>>.

Para ello, en el proceso de la Seguridad Informática se identifican 3 actores principales: activo-protector-atacante.

Activo es el valor a proteger (QUÉ), pudiendo ser software, hardware y/o datos; ***protector*** es el individuo o entidad dueña del activo; y ***atacante*** (de QUIÉN PROTEGERSE) es el individuo o entidad que aspira poseer un activo con fines de alterar algunos de los servicios de seguridad (disponibilidad, integridad, autenticidad y confidencialidad).

Siguiendo el contexto, una ***vulnerabilidad*** es cualquier debilidad que pueda explotarse para causar pérdida o daño a la información y/o sistema, ***riesgo*** es cualquier posibilidad de causar daño sobre un activo. ***Daño*** es el resultado de la amenaza y/o ataque tras explotar una vulnerabilidad.

Una ***amenaza*** es cualquier circunstancia con el potencial suficiente para causar pérdida, daño y/o compromiso, de alguno o todos los activos que conforman un sistema. Éstas pueden ser de tipo humanas o bien, debido a fenómenos naturales.

Las amenazas humanas se clasifican en: maliciosas (intencionales) o no maliciosas (ejecutadas por ignorancia o descuido del usuario). Las debido a fenómenos naturales, se refieren a las amenazas como consecuencia de inundaciones, terremotos, incendios, etc. Esta clasificación se muestra en la *Figura 1*

Un ***ataque*** es la acción (exitosa o no), que de manera intencional o accidental, atenta contra el buen funcionamiento del sistema informático.

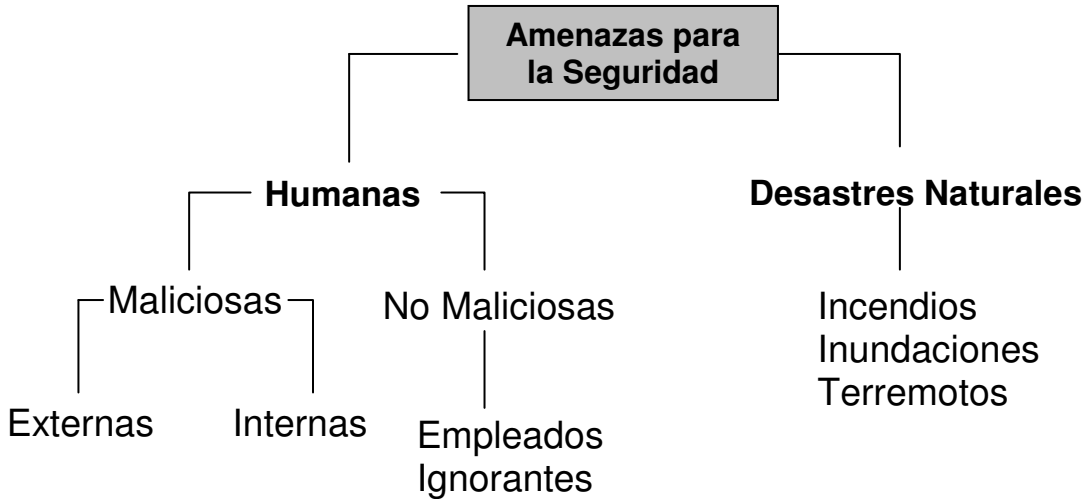


Figura 1. Tipos de amenazas informáticas.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. De acuerdo a la forma en que una amenaza explote las vulnerabilidades de los activos de un sistema informático, se identifican 4 tipos de amenazas principales:

Modificación: Se refiere a cuando una parte no autorizada logra el acceso del sistema y puede manipular algunos de sus activos. Es un ataque contra la integridad.

Intercepción: Se refiere a que alguna parte no autorizada (persona, proceso o sistema) logra el acceso a un activo del sistema. Es un ataque contra la confidencialidad.

Interrupción: Se refiere a cuando un activo se pierde, se hace no disponible, inutilizable o es destruido. Es un ataque contra la disponibilidad.

Fabricación: Se refiere a la inserción o creación de objetos falsos en un sistema. Es un ataque contra la autenticidad.

Los ataques se clasifican en pasivos y activos. Los ***ataques pasivos*** consisten solo en observar, leer y/o consultar la información sin llegar a alterarla o modificar el estado del sistema. Es decir, afectan únicamente la confidencialidad de la información y/o el sistema (p.e: lectura o fisgoneo de mensajes y análisis de tráfico).

Los ***ataques activos*** por el contrario, consisten en alterar y afectar el estado de la información, el sistema ó ambos. Es decir, afectan la confidencialidad, integridad y/o autenticidad (p.e: engaño, suplantación, replica o modificación de mensajes y/o negación de servicio).

Dado esto, es claro que cada uno de los activos estarán expuestos a ***amenazas y ataques*** (DE QUÉ protegerse) en base a las vulnerabilidades que éstos presenten.

La ***Seguridad Informática*** entonces, se puede definir como el "área que a través de acciones, métodos y mecanismos, busca reducir las vulnerabilidades, minimizar riesgos y garantizar los servicios de confidencialidad, disponibilidad, autenticidad, integridad y no repudio, de los activos que integran un sistema informático (software, hardware e información)".

De acuerdo a esto, dentro de la Seguridad Informática surgen dos grandes divisiones: ***Seguridad Física y Seguridad Lógica.*** La Seguridad Física se enfoca en la implantación de dispositivos, controles y mecanismos necesarios, a fin de prevenir y controlar los accesos físicos de personas no autorizadas a los sistemas de cómputo, así como ante posibles eventos de incendio, desastre natural o un corto circuito que pudieran ocurrir y afectar los activos informáticos. Algunos de estos mecanismos son por ejemplo: detectores de humo, puertas de seguridad, cámaras, entre otros.

La Seguridad Lógica por otro lado, es la encargada de proteger el activo más importante denominado "información", que consiste en la aplicación de controles y procesos para controlar los accesos a los sistemas, permitiendo el ingreso a los sistemas únicamente a personas autorizadas. Este tipo de seguridad se aplica al sistema operativo, bases de datos[12], sistemas de aplicación y cualquier otro software, para resguardarlos de modificaciones no autorizadas que puedan poner en riesgo su integridad.

Algunos de los mecanismos que la Seguridad Informática utiliza para implementar los servicios básicos de seguridad son: mecanismos de control de acceso,

[12] Una base de datos, es un conjunto de datos estructurados, organizados e interrelacionados entre sí, que se encuentran expresados en términos de tablas, campos y relaciones, para que el acceso a la información de interés pueda ser rápida.

algoritmos de cifrado, protocolos de autenticación, firmas digitales[13] y certificados digitales, protocolos de autenticación e intercambio de llaves, entre otros.

En el siguiente subcapítulo ***"1.2 Criptografía",*** se dan mayores detalles sobre algunos de estos mecanismos que la Seguridad Informática utiliza para implementar seguridad sobre servicios como: base de datos y transacciones, correo electrónico, redes seguras, servicios web, autenticación y control de acceso, etc; donde en gran parte de ellos hace uso de la Criptografía.

1.2 CRIPTOGRAFÍA

"Criptografía es el arte de crear y usar criptosistemas. Es el arte y la ciencia de desarrollar y usar mecanismos para transformar los datos en registros de información ilegibles para cualquiera, a excepción del destinatario quien los puede descifrar".

La palabra Criptografía proviene del griego Kryptos <oculta> y gráphein <escritura>, que conjuntándolas significan "escritura oculta".

La Criptografía junto con su oponente que es el Criptoanálisis, es una de las dos disciplinas que conforman la Criptología. La Criptografía se encarga de diseñar procedimientos particulares para cifrar la información con objeto de mantener su confidencialidad y el Criptoanálisis por lo contrario, se encarga de romper esos procedimientos de cifrado para recuperar la información en su forma original <<legible>>.***[RFC7, Mod.2, p.5]***

La Criptología como forma de proteger la información tiene sus orígenes desde épocas muy antiguas al surgir la necesidad de compartir, trasmitir y almacenar información manteniendo su confidencialidad con el propósito de que solo las personas autorizadas pudieran tener acceso a ésta. En sus inicios estuvo muy enfocada a sectores militares y diplomáticos debido a que éstos eran los únicos que tenían verdadera necesidad de hacer uso de ella; sin embargo, con el paso del tiempo, los avances en las comunicaciones y la tecnología de cómputo, su uso se vio incrementado llegando a ser una necesidad real entre los individuos para poder transferir y almacenar grandes flujos de información de manera más segura.

[13] Una firma digital es un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave de emisor y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del emisor y que el mensaje no ha sido modificado después de efectuada la transformación. Ver detalles en el apartado "***1.2.2 Criptografía asimétrica o de clave pública".***

Para ello se crean técnicas criptográficas que permitan “esconder” <<cifrar>> los mensajes que desean ser enviados vía un canal que se supone inseguro, permitiendo que sólo el receptor autorizado pueda leer el mensaje “escondido” <<descifrar>>.

Para hacer posible lo anterior, la Criptografía se basa en funciones matemáticas usadas para cifrar y descifrar mensajes; donde ***cifrado*** es el proceso de transformar un mensaje, para ocultar su contenido, en un mensaje ilegible (mensaje cifrado), y el ***descifrado*** es el proceso de regresar un mensaje cifrado, a texto en claro o mensaje original. Lo anterior se puede observar en las *Figuras 2 y 3*

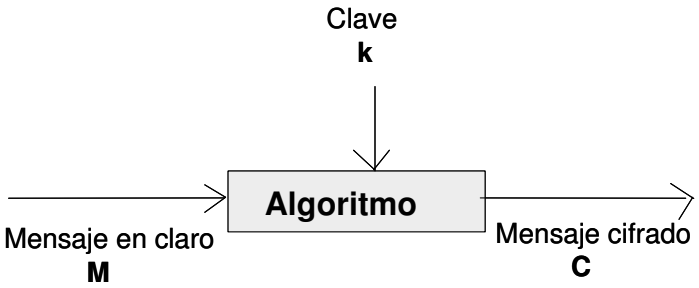


Figura 2. Proceso de cifrado de un mensaje.

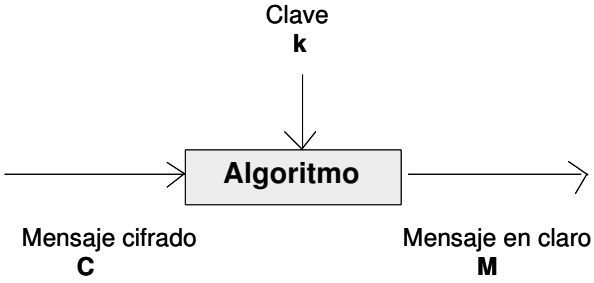


Figura 3. Proceso de descifrado de un mensaje.

Como técnicas de cifrado, dentro de la Criptografía se distinguen 3 rubros principales de acuerdo a la manera en que se realiza la transformación de los mensajes <<texto en claro>> y al manejo de las claves utilizadas: Criptografía simétrica, asimétrica y funciones hash.

1.2.1 Criptografía simétrica, de clave privada o convencional.

Este tipo de Criptografía maneja una sola clave que debe permanecer secreta, con la cuál se realiza tanto el cifrado como el descifrado; requiriendo por ello, de un acuerdo previo para su determinación o bien, de una tercera entidad confiable que funja como centro de distribución de claves y que además garantice el envío de las claves a ambos a través de un canal seguro.

Lo anterior está dado por un texto o mensaje en claro denominado **M**, el cuál a través de una clave **k**, es cifrado, dando como resultado C:

$$E_k(M) = C$$

El proceso inverso, o sea el descifrado, se lleva a cabo con la clave k para recuperar M, denotándose como:

$$D_k(C) = M$$

Nótese que $D_k (E_k(M)) = M$

La base de seguridad de la Criptografía simétrica está conformada por operaciones elementales (sustituciones y permutaciones). Los algoritmos estándar son DES (Data Encryption Standard-1977), IDEA (International Data Encryption Algorith-1990) y AES (Advanced Encryption Standard) de 128 bits. Algunos otros algoritmos que integran esta clasificación, son: IRC5 y Rijdael (propuesta de nvo. estándar mundial) ***[RFC7,Mod2,p,37]***.

Algunas características adicionales de la Criptografía simétrica, es que ésta es más sencilla y fácil de implementar en relación a la asimétrica; sin embargo, aunque sus algoritmos son más sencillos y generalmente más rápidos, tiene algunos problemas como el hecho de que requiere un "canal seguro" para transmitir o acordar la clave. Así mismo, aunque realiza eficientemente el cifrado de los datos en tiempo real y es segura contra ataques de fuerza bruta[14] cuando se usan claves lo suficientemente grandes, ésta solo otorga el servicio de confidencialidad.

[14] Refiérase a ataques basados en aprovechar diccionarios de palabras, para adivinar los passwords de usuario y así acceder a los sistemas informáticos. Lo que hace este tipo de ataques, es comparar las palabras almacenadas en el diccionario Vs. los passwords del sistema, hasta obtener el acceso al equipo.

1.2.2 Criptografía asimétrica ó de clave pública.

Este tipo de Criptografía no requiere acuerdo previo de secretos. Utiliza 2 claves: una clave pública para cifrar (que se da a conocer), y la otra privada para descifrar (que debe guardarse).

Lo anterior está dado por $\mathbf{(n-1)^n/2}$ como cantidad de claves requeridas, donde n es el número de destinatarios involucrados, lo cuál provoca que la distribución de tantas claves secretas sea complicada y costosa.

Como parte del proceso, todos los usuarios tienen una clave pública y una privada. Quien desea enviar un mensaje, emplea la clave pública para cifrar el mensaje que sólo podrá ser descifrado con la clave privada. Los mensajes cifrados con la clave pública no pueden descifrarse con la misma clave pública.

El cifrado de clave pública está basado en funciones matemáticas cuya complejidad hace poco posible que con un tiempo y potencia razonable, conociendo sólo el mensaje cifrado y la clave pública, pueda deducirse la clave privada y con ella obtener el mensaje original.

Los elementos principales de la Criptografía asimétrica está dado por **M= [M1, M2, M3,….Mm**] donde **M** es el mensaje de texto legible de longitud **m** elementos de un alfabeto finito. Ejemplo:

María genera un mensaje de texto legible **M**
Pedro genera un par de claves **Kpb** (clave pública) y **Ksb** (clave privada), donde **Kpb** es conocida por María.

Con el mensaje **M** y la clave pública Kpb, María genera el texto cifrado C:

$$\mathbf{C= [\ C1, C2, C3,….Cm]}$$

$$\mathbf{C = E_{Kpb}\ (M)}$$

Pedro el receptor, teniendo la clave privada correspondiente, puede invertir la transformación y descifrar el texto:

$$\mathbf{M= D_{ksb}(C)}$$

$$\mathbf{M = D_{Ksb}\ [\ E_{Kpb}(M)\ ]}$$

$C= E_{Kpb} [D_{Ksb}(C)]$	$M= D_{Ksb} [E_{Kpb}(M)]$
Cifrado (M)	**Descifrado (C)**

Como característica del cifrado de clave pública, para Pedro es computacionalmente fácil generar el par de claves **Kpb** (clave pública) y **Ksb** (clave privada) , y así mismo, para María cifrar el Mensaje **M** de longitud **m**, haciendo uso de la clave pública conocida (Kpb) para producir el texto cifrado **$C = E_{Kpb} (M)$**

Computacionalmente es fácil para Pedro como receptor, teniendo la clave privada correspondiente, descifrar el mensaje cifrado y recuperar el mensaje original **$M=D_{Ksb}(C)$**

De esta manera, no es computacionalmente factible para un atacante, conociendo la clave Kpb y el texto cifrado C, determinar la clave privada Ksb.

La seguridad en la Criptografía asimétrica se encuentra basada principalmente en la construcción de funciones matemáticas cuyo inverso es computacionalmente imposible de determinar.

La Criptografía asimétrica en comparación a la simétrica, es más potente (aunque computacionalmente más costosa y lenta) y no requiere transmitir una clave secreta (se da a conocer la clave pública, misma que puede ser transmitida por un canal inseguro pues no existe el problema de que pueda ser conocida). En ésta, tanto la clave pública como la privada guardan una relación estrecha, pues lo que una cifra, la otra lo descifra; logrando así, hacer “imposible obtener la una a través de la otra”. A diferencia de la Criptografía de clave simétrica, además del servicio de confidencialidad otorga los servicios de autenticidad e integridad.

Los algoritmos estándar son el Gamal (1978), el RSA (Rivest, Shamir y Adleman-1977) de 4096 bits, y el algoritmo de intercambio de llaves de Diffie y Hellman. Estos son la base de las firmas digitales y los certificados.

En lo que respecta a ***firmas digitales***, éstas hacen uso de Criptografía de clave pública para realizar el cifrado y descifrado, utilizando un par de claves intercambiables: una pública y una privada. La propiedad de las firmas digitales consiste en que si se utiliza una clave pública para cifrar un mensaje, sólo con la clave privada se puede descifrar. Y si se cifra el mensaje con la clave privada, sólo con su clave pública complementaria puede descifrarse el mensaje.

En la práctica, el remitente somete los datos por enviarse a una función que los resume digitalmente <<función hash>>. El resultado es cifrado con la clave privada y se agrega como firma al mensaje original. El receptor certifica que el mensaje

proviene del propietario de la clave pública con que descifra el mensaje hash, si el hash del mensaje descifrado concuerda con el hash del mensaje original. *Ver Figura 4.*

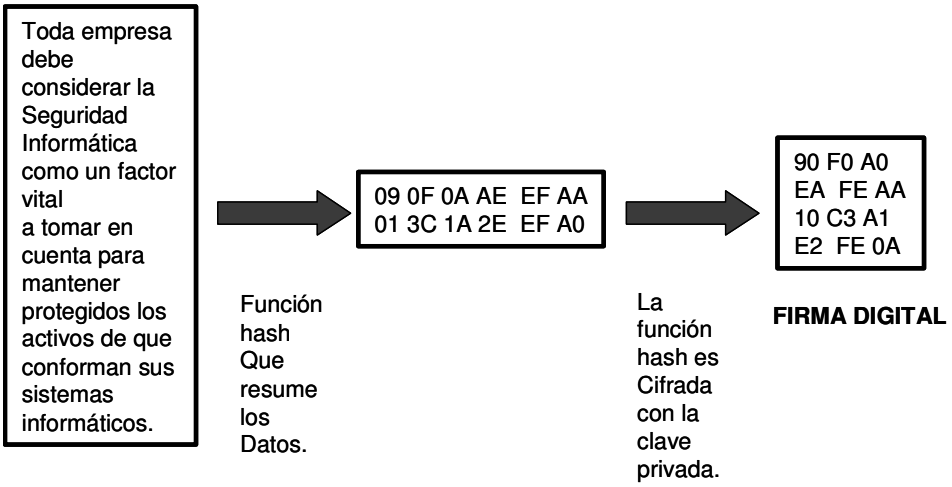


Figura 4. Proceso de firma digital.

En cuanto a los ***certificados***, éstos tienen la función de autenticar a los clientes que desean acceder a los servidores de cómputo, en ambientes distribuidos. Los procedimientos de certificación informática fueron desarrollados originalmente por el MIT, a través del sistema conocido como Kerberos, el cuál fue adoptado como estándar internacional por la Unión internacional de telecomunicaciones (estándar ITU-T X.509)

El proceso de verificación se realiza por medio de una tercera entidad denominada servidor de certificación; de esta manera, el cliente, el servidor de certificación y el servidor de aplicación, entran a un proceso de certificación que consiste en el intercambio de mensajes cifrados para dar al usuario, acceso a los demás servidores. Las técnicas de autenticación determinan si la petición se generó de un usuario o aplicación autorizada. Una vez autenticada la petición, se determina el tipo de acceso y los recursos a los que el usuario tiene derecho a utilizar.
En la actualidad dos de los servicios mas destacados que proporcionan certificación lo representan Kerberos[15] como técnicas de autenticación, certificación y cifrado más populares; y RSA para el cifrado y descifrado.

Como puede observarse, existen diferencias importantes entre ambos tipos de Criptografía (simétrica y asimétrica), sin embargo, no es posible decir que una es mejor que la otra. Su elección deberá estar basada en la necesidad específica que

[15] Sistema de seguridad en el que el login y los passwords viajan encriptados a través de la red.

se tenga, resultando conveniente en algunas ocasiones utilizar Criptografía simétrica y en otras, asimétrica.

1.2.3 Funciones hash (dispersión, compendio).

También llamadas funciones de dispersión. No utilizan ninguna clave, operan sobre un mensaje de longitud arbitraria definida por una función matemática que acepta como entrada un conjunto de datos y genera como salida, un valor (valor hash) de longitud fija (casi siempre más pequeña que la del mensaje original).

Un hash **H** es una función *one-way* que opera sobre un mensaje **m** de longitud arbitraria, y regresa un valor de longitud fija **h**

$$H = H(m)$$

Esto es, dado un mensaje **m**, es fácil calcular **H(m)**

Dado **h**, es difícil calcular **m** tal que $H(m) = h$

Dado **m** específico es difícil hallar otro mensaje **m'**, tal que $H(m)=H(m')$

Dado un conjunto grande **M**, es difícil hallar cualquier pareja (mi,mj) con el mismo valor hash. Lo anterior confirma la dificultad de encontrar dos mensajes **M y M'** tales que **H(M)=H(M')**

El valor hash proporciona una huella digital de ***m***

Como premisa, a partir del resultado obtenido no debe ser posible reconstruir la fuente de datos original.

Las funciones hash deben ser fáciles de calcular, difícil de invertir y de encontrar 2 mensajes que den un mismo valor hash. El resultado compendiado es único para la fuente de datos original, dentro de las restricciones de longitud. Si la fuente de datos cambia ligeramente, el resultado que produce la función compendiada <<función hash>> será significativamente distinta. Su objetivo es producir un identificador único para un mensaje o documento de forma segura produciendo una especie de huella digital. El standard es MD5, aunque algunos otros algoritmos son: MD2, MD4, SHA.

Citado lo anterior, algo relevante a citar es que, de los 5 servicios que la Seguridad Informática busca otorgar (confidencialidad, autenticación, integridad, disponibilidad y no repudio), al menos en 4 de ellos se hace uso de la Criptografía.

Algunos de los mecanismos más comunes donde la Criptografía tiene uso, son: algoritmos de cifrado, mecanismos de control de acceso, protocolos de autenticación e intercambio de llaves, mecanismos de integridad, firmas y certificados digitales, entre otros.

La implementación de estos mecanismos se pueden identificar fácilmente en procesos y servicios tradicionales como:

- Autenticación y control de acceso (protocolo SSH, firmas y certificados digitales, etc).
- Verificación de integridad (cheksum criptográfico, funciones hash MD4, MD5)
- Correo electrónico seguro (PGP)
- Intercambio y almacenamiento de información (**SSL**, cifrado (DES, IDEA, 3DES, RC5, etc).
- Base de datos y transacciones electrónicas (SET[16], **SSL**, etc).
- Aplicaciones seguras (Java, Perl, etc).
- Redes seguras (Lan, Wan, intranet's)- (Kerberos, intranets seguras, etc).
- Web, comercio electrónico, etc. (**SSL**, SET, etc).

En lo que respecta al proyecto aquí presentado como sistema de control de accesos de usuario vía huella digital, el uso y la aplicación que tendrá la Criptografía, será exclusivamente a través del uso del protocolo SSL como elemento que utiliza Criptografía simétrica y asimétrica para otorgar seguridad en el ambiente Intranet [17]; y poder llevar a cabo el intercambio de información cliente- servidor en la web de forma segura.

Aunque la encripción de los patrones de las huellas pudiera implementarse para incrementar aún mas el nivel de seguridad del sistema, el alcance del presente proyecto de tesis no lo considera; pudiendo servir como antesala para que cualquier otro lector interesado en el tema, pueda desarrollar una segunda fase del proyecto y llevar a cabo dicha implementación a través de algún mecanismo de encripción particular.[18]

---

[16] SET (Secure Electronic Transaction- Transacción Electrónica Segura), es un protocolo creado y publicado por Visa y MasterCard con el fin de permitir la realización de transacciones electrónicas a través de la red.

[17] Intranet es una red privada de una compañía u organización, que utiliza el mismo software que se encuentra en internet, pero que es solo de uso interno.

18 Implementaciones interesantes para incrementar los niveles de seguridad en sistemas biométricos por huella digital han sido presentados por varios autores interesados en la materia. Tal es el caso del proyecto presentado por Yeung y Pankanti en el año 2000, consistente en la introducción de marcas de agua en las imágenes de las huellas para asegurar que todas las imágenes almacenadas en la BD sean auténticas y no hayan sido alteradas por algún intruso. [RFC3p.41]

Los detalles expuestos en este subcapítulo respecto a Criptografía, su campo de aplicación y características, han sido solo para efectos de conocimiento general, dada su importancia y papel en el área de Seguridad Informática.

1.3 SSL (SECURE SOCKETS LAYER)

"Implementar una correcta estrategia de seguridad en ambientes web, implica alcanzar un compromiso entre la universalidad en el acceso a la información y su seguridad, compromiso que proteja la confidencialidad e integridad tanto de los datos almacenados en el servidor, como de los que están siendo transportados hacia/desde el servidor."

La publicación de grandes volúmenes de información a través de ambientes web, constituye un medio conveniente para acceder a la información de una manera ágil y eficaz, pero a medida que crece la cantidad de información públicamente disponible y transportada a través de medios abiertos como lo es Internet o incluso ambientes intranets, surge la necesidad de asegurarla en parte o en su totalidad, protegiéndola de ojos indiscretos, modificaciones o daños, manteniendo la capacidad de acceso.

Debido a que en los últimos tiempos el uso de la red se ha incrementado de manera exorbitante, la necesidad de proteger los datos de las aplicaciones que vayan sobre TCP[19] como lo es la World Wide Web[20], se ha vuelto un elemento clave para evitar pérdidas o daños sobre alguno o varios de los activos informáticos que la integran.

Para lo anterior, se han desarrollado protocolos específicos con fines de implementar seguridad en diversidad de ambientes. En el caso de los servicios que se otorgan en ambiente web, los protocolos mas utilizados lo representan ***S-HTTP*** (secure HTTP) y ***SSL*** (secure sockets layer)[RFC2]. Ambos lanzados a mediados de los noventa y basados en técnicas similares, como las firmas y los certificados digitales. Adicionalmente existe otro protocolo llamado ***SET*** (secure electronic transanction), el cuál está enfocado a transacciones comerciales.

De estos 3 protocolos citados, en este apartado se analiza protocolo SSL, debido a que es uno de los elementos seleccionados que forma parte integral del proyecto de diseño, desarrollo e implementación del sistema de control de accesos para llevar a cabo el control de accesos de usuario de una Intranet realizando autenticación vía

[19] TCP (Transmission Control Protocol- Protocolo de control de transmisión), es uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte orientado a conexión, que tiene como función principal proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de éstos.

[20] World Wide Web (WWW). Estrictamente la web es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a browsers normalmente gráficos como Netscape o Internet Explorer.

huella digital. A través de este protocolo se pretende introducir una nueva capa entre los niveles TCP y de aplicación del modelo Internet para cifrar la comunicación a través de un puerto específico. Lo anterior se muestra en las *Figuras 5 y 6.*

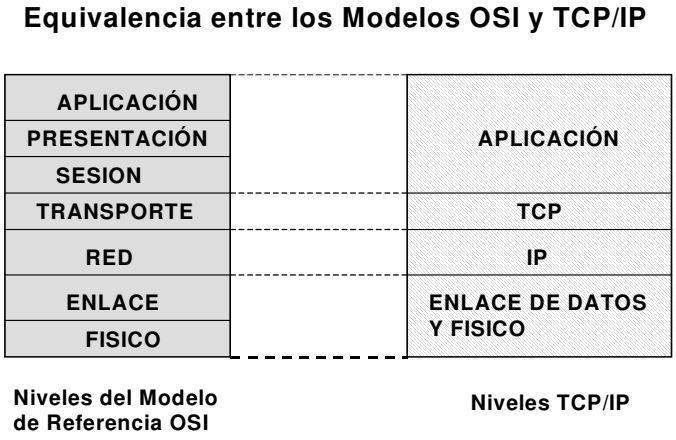


Figura 5. Equivalencia entre capas, de los modelos OSI y TCP/IP

Lo que hará el protocolo SSL, es autenticar un servidor ante un cliente y viceversa, cifrando toda la información en tránsito. Esto implica, que tanto los datos que viajan desde el servidor a la máquina del usuario, como en sentido inverso, resulten protegidos durante su transporte a través de la red. Lo anterior, haciendo uso de certificados digitales.

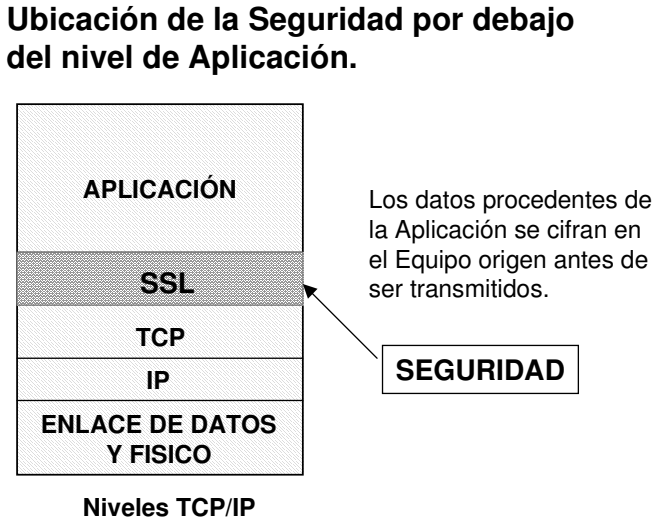


Figura 6. Protocolo SSL y su ubicación en las capas del modelo TCP/IP para otorgar seguridad.
* Conferencia "Seguridad en Internet" impartida por Jordi Forné, Universidad Politécnica de Catalunya. Mayo 2002.

El protocolo SSL fue introducido por Netscape. Es un protocolo de comunicación que proporciona principalmente 3 servicios básicos de seguridad: confidencialidad, autenticación e integridad para integrar seguridad a las comunicaciones sobre Internet.

Con el fin de garantizar dichos servicios, SSL hace uso tanto de Criptografía asimétrica (basada en la utilización de un par de claves, la pública y la privada) como de Criptografía simétrica (basada en la utilización de una única clave secreta). La justificación de dicha combinación viene dada por cuestiones de eficiencia, puesto que las transformaciones criptográficas (operaciones de cifrado y descifrado) realizadas mediante técnicas de Criptografía asimétrica son del orden de diez mil veces más lentas que las realizadas con Criptografía simétrica. SSL negocia en una primera fase utilizando Criptografía asimétrica (p.e. RSA), y cifra posteriormente la comunicación utilizando Criptografía simétrica (RC4, RC5, IDEA, etc).

En la actualidad existen tres versiones, la versión SSL-v3 es la última y la más utilizada. Los algoritmos en los que se basa son:

Funciones hash: MD5, SHA-1
Cifrado simétrico: DES-CBC, Triple DES-CBC, RC2, RC4.
Cifrado asimétrico: RSA, DSS.

La forma en que opera cuando existe una implementación mediante un protocolo SSL, es que cuando se inicia la comunicación entre un servidor y un cliente, primeramente se da un proceso de negociación de los algoritmos criptográficos a utilizar. Una vez establecidos los parámetros, el intercambio de información entre el cliente y el servidor se lleva a cabo de forma cifrada incluyendo el URL del documento solicitado, el contenido del documento, las “cookies” [21]enviadas por el servidor o por el cliente, etc.

Para realizar lo anterior, el protocolo SSL integra 2 subprotocolos particulares:

- SSL record protocol, encargado de definir el formato de los datos de sesión.
- SSL handshake protocol, encargado de negociar los algoritmos de cifrado a utilizar.

[21] Cookie es un pequeño trozo de información enviado por un servidor de web al sistema de un usuario. Se trata de un procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación. En la práctica la información es proporcionada desde el browser al servidor del world wide web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

Durante el protocolo SSL handshake, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes seis fases (de manera muy resumida):

- La fase hola, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación.
- La fase de intercambio de claves, en la que intercambia información sobre las claves, de modo que al final ambas partes comparten una clave maestra <<clave privada>>.
- La fase de producción de clave de sesión <<clave publica>>, que será la usada para cifrar los datos intercambiados.
- La fase de verificación del servidor, presente sólo cuando se usa RSA como algoritmo de intercambio de claves, y sirve para que el cliente autentique al servidor.
- La fase de autenticación del cliente, en la que el servidor solicita al cliente un certificado X.509 (si es necesaria la autenticación de cliente).
- Por último, la fase de fin, que indica que ya se puede comenzar la sesión segura.

Cabe mencionar que existe la posibilidad de elegir la longitud de clave en función del algoritmo elegido, existiendo una versión de exportación de baja seguridad que sólo permite la utilización de RC2, con clave de 40 bits, y RSA, con clave de 512 bits. La mayoría de los navegadores que se utilizan fuera de nuestro país por lo general incorporan esta versión de SSL ***[RFC2, p.215]***

La forma en que se puede identificar en un ambiente web cuando se está haciendo uso de SSL, es observando la línea URL[22], la cuál deberá iniciar como <<https://>>.

Como puede observarse, la seguridad en la infraestructura web puede ser tan variada como el tamaño de la inversión que se desee llevar a cabo. Es importante aclarar que el protocolo SSL representa uno de tantos mecanismos de protección, aunque no por sí solo, la protección integral.

[22] URL (Uniform Resourse Locator – Localizador Uniforme de recursos). Sistema de direccionamiento estándar para archivos y funciones de internet, especialmente en el world wide web. El URL está conformado por el servicio (p.e: http://) más el nombre de la computadora (p.e: www.inbursa.com.mx) más el directorio y el archivo referido.

1.4 MODELOS DE CONTROL DE ACCESO Y AUTENTICACIÓN.

"El Control de Acceso y la Autenticación son unos de los principales servicios de la Seguridad Informática. Una especie de pareja inseparable, donde el segundo valida la identidad de los usuarios, otorgándoles o denegándoles el acceso a los recursos según sea el caso; y el primero, de acuerdo a ello, identifica que perfil y de qué privilegios gozará en el sistema. Si alguno de ellos falta, entonces, no se puede hablar de seguridad".

1.4.1 Control de Acceso.

Sin lugar a dudas, para hablar de un sistema confiable hay que determinar cuáles pueden ser los caminos para llegar a la confiabilidad, los niveles que existen en los usuarios y los permisos o privilegios que dichos usuarios podrán tener en los sistemas. Hablar de una de las piezas fundamentales para garantizar la seguridad de los recursos, implica hablar de Control de Acceso como puerta primaria para otorgar o denegar el ingreso a los recursos. Es hablar de poder identificar los usuarios legítimos, de los intrusos, y en esa medida mantener protegidos cada uno de los activos que conforman el sistema informático, ante cualquier posibilidad de acceso no autorizado, fisgoneo, daño, robo, alteración o suplantación.

El Control de Acceso se define como el mecanismo para el control de los ingresos a un sistema o recinto en particular, que integra el establecimiento de perímetros y métodos de autenticación, con la capacidad de garantizar que dentro de la fortificación no exista enemigo.

La necesidad del control de acceso surge al presentarse 2 factores principales dentro de los sistemas o áreas críticas a proteger:

- Inexistencia de cota física (Perímetro) (p.e: la cantidad de equipos conectados en la red, distintas plataformas, acceso de diversos lugares, etc.).
- Grupo de usuarios no acotado.

Debido a su importancia, actualmente el control de acceso tiene un campo de aplicación muy extenso en cuanto a seguridad se refiere, cubriendo desde recursos tanto físicos como lógicos. Algunas de esas aplicaciones son:

- Acceso a PC's, redes y redes privadas virtuales (VPN's).
- Sistemas de pago y comercio.
- Acceso a bases de datos
- Servidores web
- Servicios de FTP, TELNET, etc.
- Sistemas de archivos

- Aplicaciones
- Sistemas operativos
- Otros.

El Control de Acceso es un de los servicios de seguridad que normalmente no utiliza técnicas criptográficas para su implementación, en cambio existe un gran número de técnicas y modelos propios de control de acceso para su implementación. Este servicio está cercanamente relacionado al de autenticación ya que un usuario debe ser autenticado antes de tener acceso a los activos del sistema, razón por la cuál en el subcapítulo ***"1.4.2 Autenticación"*** se analiza a detalle el aspecto de autenticación.

Como modelos de Control de Acceso, los primeros sistemas estaban basados principalmente en los modelos MAD (Modelo de Control de Acceso Discrecional) y MAO (Modelo de Control de Acceso Obligatorio), donde en el primero el usuario es quien decide como proteger el sistema mediante controles de acceso impuestos por el sistema; y en el segundo, es el sistema quien protege los recursos.

Debido a que cada uno de estos modelos tiene sus peculiaridades, surge un nuevo modelo llamado MBR (Modelo de Control de Acceso Basado en Roles), el cuál viene a mejorar algunos aspectos importantes puesto que contiene de cierta forma la flexibilidad para el control de accesos que tiene el MAD y la rigidez que presenta el MAO.

En resumen, hoy por hoy se estudian 3 modelos principales: MAD (Modelo de Control de Acceso Discrecional), MAO (Modelo de Control de Acceso Obligatorio) y MBR (Modelo de Control de Acceso Basado en Roles).

1.4.1.1 Modelo de Acceso Discrecional (MAD)

Este tipo de modelo decide y controla qué usuarios pueden acceder a qué información, basado en la identidad del usuario y las reglas que especifican cuáles usuarios tienen acceso a qué partes de información. Cuando algún usuario desea acceder a un conjunto de datos, el servidor busca una regla que especifique si ese usuario tiene permitido o no acceder a la información. Si esta regla es encontrada, el usuario puede acceder al recurso, de lo contrario el usuario no puede realizar ningún tipo de acceso.

Como parte de este modelo, se distinguen 2 conceptos principales: archivo y propiedad de los datos, y los permisos y derechos de acceso.

El archivo y propiedad de los datos se refiere a que cada objeto en un sistema debe estar protegido por un usuario, en este caso el dueño del recurso (p.e: persona que

creó el archivo, directorio, etc.). Este dueño es el encargado de definir las políticas de acceso a sus recursos.

Respecto a los permisos y derechos de acceso, el dueño del sistema se encarga de asignar a los usuarios o grupos de usuario, el acceso a los diferentes recursos, con privilegios y permisos específicos.

En este modelo el usuario propietario de un recurso asigna la manera de cómo debe de protegerse éste, estableciendo y limitando las operaciones que pueden realizarse sobre de él. Lo característico de este modelo es que el usuario a manera discrecional decide a quien compartirle el recurso.

Un ejemplo de este tipo de modelo es el de sistema de archivos de una PC, en donde el dueño del equipo es quien decide con quién compartir los recursos de la misma otorgándole el acceso a quien él designe, y a quien no, simplemente le niega el acceso.

1.4.1.2 Modelo de Acceso Obligatorio (MAO)

En este modelo, es el sistema quien protege los recursos, lo cuál representa una gran ventaja a diferencia del modelo MAD anterior, en donde el dueño es quien protege los recursos.

En el modelo MAO, el Administrador[23] es quien impone las reglas de forma segura, teniendo como premisa, que todo recurso del sistema y todo usuario tiene una etiqueta de seguridad.

Este tipo de control de acceso sigue el modelo de clasificación de información militar, en donde la confidencialidad de la información es lo más relevante, formando lo que se conoce como política de seguridad multinivel. En este tipo de sistemas, todas las decisiones de seguridad las maneja el sistema, comparando las etiquetas del usuario frente al recurso solicitado.

De esta manera, tal y como lo indica el nombre de este modelo, las políticas definidas deben aplicarse de manera obligatoria a todos los usuarios que intentan acceder a un recurso protegido por ésta.

Una de las desventajas de utilizar este modelo, es que es muy rígido y el usuario siempre tiene que recurrir al Administrador para realizar ajustes.

Un ejemplo de esta política es la que se aplica en los servicios de web-mail gratuito, en donde todos los usuarios sin distinción, tienen un espacio asignado en el servidor

[23] Refiérase a la persona que se encarga de todas las tareas de mantenimiento de un sistema informático, el cuál tiene acceso total y sin restricciones al mismo.

de correo el cuál no pueden sobrepasar. En este caso ni el remitente ni el destinatario de un mensaje pueden pedir al servidor del correo que ignore la política para un mensaje específico, sino que es el sistema quien aplica obligatoriamente dicha política a todos los mensajes y a todos los usuarios.

1.4.1.3 Modelo de Acceso Basado en Roles (MBR)

Partiendo del interés de determinar qué usuarios y qué grupos de usuarios pueden ejecutar qué tipo de operación sobre qué tipo de recurso, surge el modelo MBR.

El modelo surge de la necesidad de encontrar un modelo de acceso mas adecuado a las necesidades del día de hoy, tomando las principales bondades de los modelos MAD (modelo de acceso muy flexible) y el modelo de acceso MAO (modelo demasiado riguroso); e incorporando nuevos elementos en su estructura de control en términos de usuarios, roles, permisos, operaciones y objetos, así como las funciones y relaciones.

El modelo MBR parte del hecho de que la correcta administración de la seguridad, consiste en que los roles deben asignarse adecuadamente a los diferentes tipos de usuarios, según sus capacidades y puestos de cada uno de ellos. Dado esto, como parte de su estructura de control, el modelo MBR se enfoca en controlar los accesos de los usuarios a los recursos en términos de sus actividades y funciones de trabajo, representándose así, de forma natural la estructura de las organizaciones.

Dentro de su estructura, los permisos se encuentran asociados con los roles y los usuarios son miembros de los roles; de tal manera que cada usuario adquiere ciertos permisos en base al rol asignado.

Dada estas características traducidas en ventajas, el MBR es hoy en día uno de los modelos más utilizados debido principalmente a la forma jerárquica de funcionar, ya que es más fácil administrar un sistema asignando roles a los usuarios, y así llevar una administración confiable y de bajo costo.

Actualmente el uso del modelo MBR va desde los sistemas de base de datos relacionales, sistemas operativos de red, firewall[24], sistemas de sign-on y de seguridad web.

[24] Firewall es un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los firewalls pueden ser implementados en hardware y software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cuál examina cada mensaje y bloquea aquéllos que no cumplan con determinado criterio de seguridad.

Un ejemplo del modelo, son los accesos que se otorgan a los usuarios en un portal de comercio en donde cada usuario dependiendo del rol que desempeña (proveedores, clientes, distribuidores, etc.), accede a los diferentes micro sitios dependiendo de los privilegios que tenga su rol.

1.4.2 Autenticación.

La autenticación es uno de los pilares de seguridad. Este proceso es el que permite distinguir entre los usuarios validos y los que no lo son.

Un sistema de autenticación bien elaborado permite a los usuarios demostrar sus identidades y obtener acceso a los recursos o servicios de una organización, sin poner en riesgo la del mismo.

Como se puede observar en la *Figura 7*, dentro del proceso de control de acceso y autenticación, existen ciertos elementos que con facilidad se pueden identificar:

1. **Usuario o grupo de usuarios** (individuos que intentarán autenticarse ante el sistema)
2. **Dueño o Administrador del recurso** (es el dueño del recurso, quien decide los mecanismos necesarios de autenticación).
3. **Mecanismo de autenticación** (elemento que realizará el proceso de distinguir a un usuario o grupo de usuarios, de otros. Por ejemplo: password, huellas, smart card, etc).
4. **Privilegios de acceso** de usuarios (permisos que va a tener un usuario para acceder a los recursos solicitados, tras tener una autenticación exitosa; mismos que serán otorgados por el mecanismo de control de acceso. En caso de ser una autenticación fallida le negará el acceso al usuario).

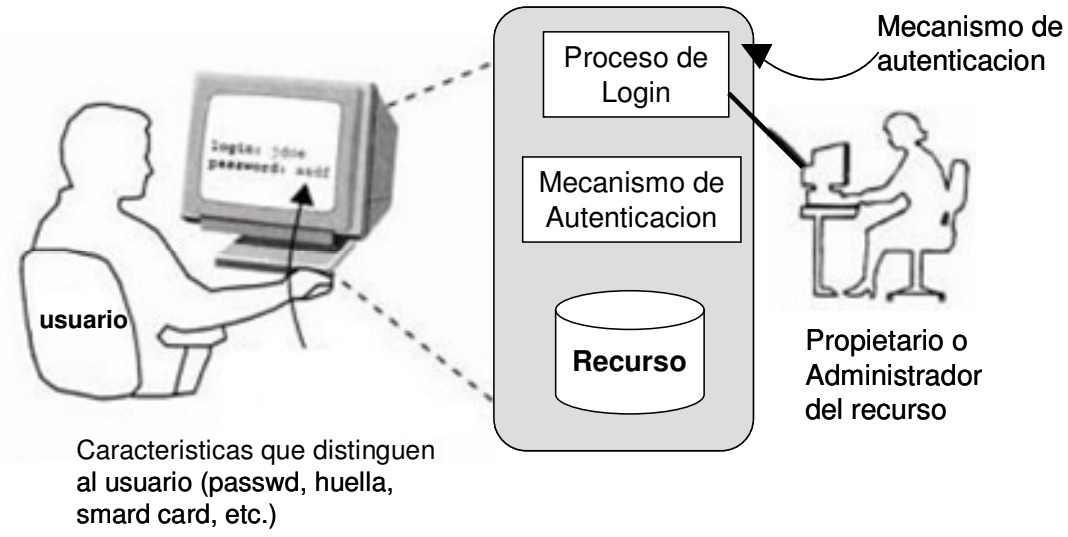


Figura 7. Elementos involucrados en los procesos
Control de Acceso y Autenticación.

Actualmente, todos los sistemas de la autenticación cuentan con uno o más de los siguientes ***factores de identificación***:

Lo que se sabe

La gran mayoría de los sistemas de autenticación emplean "lo que se sabe", es decir, contraseñas como la fecha de nacimiento del usuario o alguien importante para él; su color favorito, alguna combinación de fechas importante, el nombre de su pareja, etc.

Lo que se tiene

Sistemas basados en tarjetas inteligentes, generadores de semillas (p.e: token's), certificados digitales, etc.

Quien se es

Sistemas que detectan características físicas y/o biológicas del usuario como lo es la biometría de pupila, Iris, huella dactilar, fisonomía de las manos, timbre de voz, cinemática de la firma manuscrita, ADN, entre otros.

Donde se está

Se basan en sistemas de ubicación, no en el usuario. Analizan información como el número de teléfono originado desde una computadora, su IP de origen, su ubicación por medio de un celular, su ubicación geográfica, etc.

Como puede observarse, cada factor empleado presenta ventajas y desventajas particulares por sí solos. Por ejemplo, el nivel de seguridad proporcionado por "lo que se sabe" se relaciona con sistemas en los cuáles es difícil robar, pero es posible de olvidar, comprometer o divulgar.

El correspondiente a "lo que se tiene", son mejores para guardar y generar claves; sin embargo, son transferibles, pueden ser dañados, olvidados, extraviados o simplemente desconfigurados.

Respecto a lo "quien se es", son mejores, pero más costosos. Tienen la ventaja de que son únicos e intransferibles, además de que no pueden ser olvidados, prestados o desconfigurados. La tendencia en éstos, es que su uso se generalice cada vez más, sean más amigables y tiendan a abaratarse como ha venido sucediendo.

En algunos casos para lograr niveles más altos de seguridad, es posible combinar algunos de estos cuatro factores; haciendo que la redundancia agregue la confianza, pues la autenticación de dos factores es más segura que la de uno. Por ejemplo, una contraseña integrada en un entorno biométrico ofrece un nivel de confianza más alto. Una combinación de un mecanismo no biométrico basado en posesión (p.e: una smartcard), con un mecanismo de reconocimiento biométrico, puede elevar el nivel de seguridad del sistema, aunque quizás factores como el performance tengan que ser evaluados ya que podrían verse afectados.

Este tipo de sistemas son conocidos como de tipo multimodal. Actualmente, con el advenimiento del standard API (p.e: BioAPI; www.bioapi.org), se espera tener un incremento en las integraciones de huellas digitales con otros identificadores de tipo biométrico [25]

Lo anterior nos lleva a la conclusión de que todos los métodos de autenticación ya sea de tipo biométrico o tradicionales, presentan peculiaridades, pros y contras en relación a diversos factores que deben ser evaluados al momento de seleccionar alguno con fines de optar por la mejor técnica de autenticación segura, teniendo como base la situación o necesidad especifica que se tenga.

Algunos de estos factores por mencionar algunos, son:

[25] El Instituto Nacional de Estándares y Tecnología (NIST) y la Asociación Americana Motor Vehicle Administrators (AAMVA) introdujeron iniciativas sobre interoperabilidad para la normalización de los formatos de las huellas y su representación, con la finalidad de facilitar el intercambio de datos, procurando que los diferentes proveedores adopten un esquema común para el procesamiento, extracción, comparación y almacenamiento de los puntos característicos de las de las huellas (p.e. minutiaes). La expectativa es que a futuro se pueda lograr tener una especie de lenguaje que facilite el procesamiento, la compartición y el proceso de comparativo de huellas entre diferentes proveedores.

Facilidad de uso: El sistema debe ser amigable y no causar incomodidades, molestias o dudas para poder ser operado por los usuarios.

Factor de error: Umbral resultante de igualar los parámetros tasa de falsos rechazos y tasa de falsas aceptaciones, para asegurar el funcionamiento óptimo del sistema biométrico.

Precisión: Característica más crítica de los sistemas de autenticación, que se refiere a la capacidad de identificar de forma segura a los usuarios legítimos, de los impostores; que de no tenerse, la seguridad se vería comprometida. Este factor es generalmente configurable en los sistemas biométricos y es medido a través de los parámetros: tasa de falsos rechazos y tasa de falsas aceptaciones.

Aceptación: Refiérase al grado en que los usuarios están dispuestos a aceptar y utilizar el sistema biométrico. Este factor es el resultado del nivel de comprensión del funcionamiento, facilidad de uso, precisión, estabilidad y desempeño del sistema, que determinarán que los usuarios finalmente lo usen o no. El sistema no debe causar ningún tipo de complejidad en su operación, incomodidad física, frustración, "ansiedad por alta tecnología", ni generar dudas sobre su seguridad o compromiso de identidad.

Nivel de seguridad: Capacidad y fortaleza del sistema de resguardar la seguridad de los activos ante ataques de todo tipo.

Costo: Refiérase al precio por adquirir e implementar la solución integral (SW y HW) del sistema de autenticación biométrico para su operación y mtto.

Estabilidad a largo plazo: Refiérase al nivel de posible variabilidad con el tiempo, del patrón biométrico a identificar (afonías, catarros, barba, envejecimiento, etc.)

Velocidad y tasa de operación: Tiempo utilizado entre colocar la característica biométrica en el dispositivo lector, verificar la identidad del usuario y otorgar el acceso. La rapidez depende del sistema de cómputo y del sensor que indica el tiempo necesario para anunciar una decisión, donde un tiempo de 2 ó 5 segundos es considerado aceptable. Una tasa de operación de 6 a 10 usuarios por minuto (o sea de 10 a 6 segundos por usuario) es razonable.

Tamaño de almacenamiento. Refiérase al espacio requerido para el almacenamiento de datos específicos, registros y/o información en general. Por ejemplo, para un sistema de identificación, este factor afecta el tamaño global de la base de datos o disco duro del sistema, así como la velocidad de búsqueda.[26]

[26] De acuerdo a datos citados en la documentación del Verifinger 4.2 SDK.pdf, el tamaño de la plantilla de una huella digital generada (template) es de tan solo 150 a 300 bytes, característica que es vista como una de las ventajas de la biometría de huella digital. Es importante saber que el tamaño

Fiabilidad. Es el nivel de fortaleza y capacidad que presenta el sistema, ante ataques, intentos de burla ó intrusión. En la medida que un sistema sea capaz de distinguir con precisión a los usuarios legítimos, de los intrusos, su nivel de fiabilidad será mayor.

Desempeño: Refiérase a la exactitud, la rapidez y la robustez en la identificación; además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de evaluar el desempeño de un sistema, es comprobar que éste posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

No obstante a lo anterior, lo relevante a mencionar es que aunque en el proceso de autenticación la confiabilidad del proceso depende mucho de los algoritmos y métodos utilizados, la realidad es que en el sistema global de la aplicación, el factor conducta del usuario viene a ser uno de los aspectos mas críticos en la práctica, ya que éste a menudo es la fuente más grande de vulnerabilidades de seguridad en un sistema.

Queda claro que si existe corrupción, deshonestidad o conductas de ingeniería social[27] que comprometan la seguridad del Sistema, ni la mejor técnica, ni el método de autenticación más caro, ni la mejor combinación de técnicas, podrán librar el problema de compromiso de los activos.

Adicionalmente, otro factor importante es crear conciencia entre el personal involucrado sobre el sentido y la importancia de la seguridad; dando a conocer de qué manera se puede participar para incrementar los niveles de seguridad actuales, identificando claramente qué se busca proteger, cómo y el porqué. Así, en la medida que se tenga un mejor control de seguridad, en esa misma medida se estará asegurando la protección de los activos.

---

de la plantilla y la capacidad de almacenamiento están directamente relacionados, por lo cuál, estos tienen afectación directa a los costos de medios de almacenamiento, el ancho de banda y tiempo requerido para buscar y comparar una plantilla. Si bien las velocidades de búsqueda y comparación también dependen de la eficiencia de los algoritmos involucrados, mientras más pequeñas sean las plantillas, más cortos serán los tiempos de comparación.

[27] Refiérase a la habilidad de convencer a la gente, para que realice actos que puedan comprometer un sistema (p.e: convencer a un usuario que le preste su clave de acceso para navegar en el sistema cuando en realidad es para alterar una configuración u obtener información confidencial, etc.). Obtención de información por medios ajenos a la informática.

1.5 TECNOLOGÍA BIOMÉTRICA POR HUELLA DIGITAL.

1.5.1 Antecedentes.

Como bien se ha mencionado, en el ámbito de la Seguridad Informática uno de los principales problemas a enfrentar, es la necesidad de autenticar de forma segura la identidad de las personas que buscan acceder a los sistemas o recintos físicos; representando así, el Control de Acceso y la Autenticación, las áreas de mayor interés en lo que respecta a la seguridad.

Debido a que tradicionalmente se han venido utilizando métodos de autenticación comunes como lo son el uso de passwords, tarjetas inteligentes, token's, etc., con particularidades especificas y con problemas de seguridad inherentes a su naturaleza (pérdida, robo, daño, desconfiguración, etc), el surgimiento de la tecnología biométrica aplicada al proceso de autenticación, viene a resolver en gran parte estos problemas al realizar el proceso de forma mayormente segura.

De esta manera, tal y como lo indica el término, bio <vida> y metría <medida> **[RFC15]**, las técnicas de autenticación biométrica buscan hacer uso de las características fisiológicas o conductuales distintivas de una persona a otra, donde dichas características no sean fácilmente alterables y puedan ser expresadas matemáticamente en forma sintética con la finalidad de validar la identidad de los individuos. A estas características fisiológicas o conductuales, se les conoce como ***indicadores biométricos*** [28]

Dentro del área de la Biometría se puede identificar de forma genérica lo que es la ***Biometría Fisiológica*** basada en medidas o datos de partes del cuerpo humano (ojo, mano, rostro, dedeo, etc.) que realiza la comparación de éstas, contra un patrón que ha sido grabado previamente durante un proceso de registro; y la ***Biometría Conductual,*** basada en la medida o datos de acciones de una persona, e indirectamente en sus características físicas (voz, uso del teclado y la firma), la cuál realiza comparaciones de frecuencias y/o patrones vocales para validar la identidad de las personas.

Sin importar esta clasificación, la premisa del proceso, es llevar a cabo la autenticación biométrica con posibilidades de éxito, determinando los rasgos distintivos que identifiquen sin lugar a error a una persona; donde además de ser únicos, distintivos y puedan ser automatizados, dichos rasgos no sufran variaciones a lo largo del tiempo por causas como el envejecimiento o cambios en la masa corporal que pudiesen causar conflictos y/o malas decisiones en el sistema al momento de leer y comparar los patrones almacenados.

[28] Un indicador biométrico es alguna característica con la cuál se pueda realizar biometría, llámese iris, rostro, mano, huella, pupila, etc.

Dentro de las características que un indicador biométrico debe cumplir, se encuentran:

Universalidad: Que cualquier persona posea el indicador biométrico a ser utilizado.
Unicidad: Que la probabilidad de que 2 personas tengan un indicador biométrico idéntico sea muy bajo o irrepetible.
Permanencia: Que el indicador biométrico no cambie con el tiempo.
Cuantificación: Que el indicador biométrico sea medible, cuantificable.

Los criterios anteriores sirven como criterio para descartar o aprobar a alguna característica como indicador biométrico.

Lo anterior ha dado como resultado que algunos rasgos fisiológicos o conductuales sean mayormente utilizados hoy en la actualidad, como es el caso de la ***huella digital***; la cuál debido a su nivel de precisión, facilidad de uso, nivel de madurez de la tecnología y menor costo en relación con algunos otros dispositivos biométricos como son los lectores de retina, el iris, rostro, etc., le han permitido posicionarse en el mercado biométrico como una las características fisiológicas "consentidas", de mayor demanda entre empresas de diversos sectores. *Ver Tabla 1*

Características de la huella digital						
Facilidad de uso	**Tasa de error**	**Precisión**	**Aceptación**	**Nivel de seguridad**	**Estabilidad**	**Costo**
Alto	Bajo	Alto	Medio	Alto	Alto	Bajo

Tabla 1. Factores evaluados Vs. niveles alcanzados por la huella digital.
* Implementing Biometric Security. John Chirillo-Scott Blaul. Wiley Publishing, Inc.2003. Indianapolis, Indiana.

La principal ventaja de este tipo de tecnología es que es mucho más segura y cómoda que los sistemas tradicionales basados en los passwords o tarjetas. Mediante tecnología biométrica el acceso a una PC o una sala restringida, ya no depende de algo que se sepa, que se tenga o que se pueda robar, divulgar, transferir o copiar (como lo son los passwords); depende ahora de lo que se es, a través de la lectura de la característica física (huella dactilar).

La relevancia principal de la tecnología biométrica por huella digital (y en general la tecnología biométrica por iris, retina, voz, etc.) es que elimina el uso de passwords o números de identificación complejos que el usuario tenia que recordar, permitiendo hacer del proceso algo más amigable y seguro; además de solucionar en gran parte, el problema de suplantación de identidades tras aprovechar sus propiedades de unicidad e intransferencia, validando de forma segura la identidad de los usuarios.

De esta manera, dado que los patrones de las huellas son únicos e irrepetibles [29], los sistemas biométricos basados en el uso de la huella digital resultan mayormente confiables y difíciles de falsificar a diferencia del uso de mecanismos de autenticación tradicionales.

Debido a sus grandes propiedades, el uso de la huella dactilar como seña de identidad personal, aunque no parezca, es probablemente uno de los procedimientos más antiguos que existen. Hallazgos importantes demuestran cómo desde hace varios siglos los artesanos egipcios firmaban sus obras con sus huellas digitales para dejar evidencia de su autoría y autenticidad.

Hace miles de años, sus primeras aplicaciones se llevaban a cabo a modo de rúbrica en algunos países asiáticos como China y Corea. Posteriormente, pasó a emplearse en la actividad policial como prueba en casos de homicidio; y a partir de ese momento, comenzó a considerarse como uno de los métodos de identificación personal más seguros, y por tanto, más utilizados.

Como parte de la evolución de la tecnología, el proceso de autenticación por huella digital en sus inicios, trataba de una sencilla técnica basada en el revelado de las impresiones dactilares sobre una superficie, donde, gracias a los aminoácidos de los que se compone el sudor de la mano, era posible dibujar la huella dactilar al entrar en contacto con determinados reactivos químicos. Este método evolucionó hasta lo que hoy se conoce como AFIS (Automated Fingerprint Identification System-Sistema de Identificación Automática de Huellas Digitales), una tecnología que permite archivar las impresiones digitales de ciertos individuos en datos alfanuméricos, que se clasifican en función de las bifurcaciones, crestas y puntos característicos.

Siguiendo esta línea, NEC fue uno de los pioneros en el desarrollo de este tipo de sistemas, dando a conocer en 1983 AFIS21 y PID, dos procedimientos básicos de identificación de huellas dactilares (http://www.nectech.com/afis/index.htm)

Compaq también se subió al tren de la innovación, desarrollando un periférico que permite a los usuarios de PC ser identificados por su huella digital, simplificando así, el acceso a las redes corporativas y, al mismo tiempo, mejorando el nivel de seguridad.

Denominado FingerPrint, este lector de identificación es más pequeño que un ratón y permite asociar la huella dactilar del usuario con una contraseña ya existente.

---

[29] De acuerdo a estudios, la formación de las huellas dactilares se lleva a cabo aproximadamente a los 6 meses de vida en los fetos. Pequeñas líneas y bifurcaciones que identifican de manera única e irrepetible a los individuos, que además presentan la ventaja de no cambiar a lo largo de la vida a excepción debido a accidentes que pudieran resultar en cicatrices. Propiedades que hacen que las huellas dactilares sean una de las características fisiológicas más a tractivas de la industria biométrica, aplicado en el proceso de identificación de los individuos (Babler, 1991). **[RFC3, p.24]**

Por otra parte, Key Tronic presenta un nuevo teclado llamado Fingerprint scanner que integra un lector de huella digital. Para que el usuario sea admitido, en el servidor se debe crear previamente un archivo con sus datos, es decir, una plantilla codificada con información biométrica. Posteriormente, cada vez que éste pretenda entrar en el sistema, se comparará su huella con la almacenada en la base de datos y, si coincide, se le permitirá el acceso. La imagen obtenida de la huella, siempre explorada desde varios ámbitos o puntos clave, se realza de tal forma que se identifican los detalles, bordes y bifurcaciones característicos de la huella. Todos estos rasgos son guardados, en forma de valor numérico, en una plantilla que, correctamente comprimida, puede llegar a ocupar 700 bytes. (http://www.keytronic.com/secure)

En principio esta nueva tecnología estaba enfocada a sectores muy específicos en los que se necesita un elevado nivel de seguridad, tales como el médico o el de finanzas, así como a empresas con la necesidad de controlar más estrictamente el acceso a las redes corporativas.

Siguiendo esta línea, los dispositivos de reconocimiento de huella digital Fingerscan de la compañía Miros son usados en más de cincuenta países del mundo para el control de acceso a bases de datos en una corporación, o incluso, a la Red de redes.

En este sentido, TouchSafe Personal, es un dispositivo de verificación biométrica personal completamente portátil que permite la salvaguarda de datos y de aplicaciones. Por otro lado, TouchNet para Oracle es otra de las soluciones de la línea de productos biométricos FingerScan. Aprovecha la característica de irrepetibilidad de la huella digital para proveer una verificación de identidad segura y rápida en organizaciones que poseen bases de datos Oracle. En el momento en el que cada usuario autorizado se registra en el sistema, se crea un patrón biométrico de la huella digital, que se almacena en el servidor para ser consultado y comparado cada vez que el usuario intente acceder al sistema protegido. Durante la verificación, que se produce ante la solicitud de acceso, el usuario presenta su huella para ser comparada con el patrón anteriormente almacenado, con el que deberá coincidir para que la entrada pueda ser permitida.

Precise Biometrics es otra de las compañías que han orientado su actividad hacia la producción de soluciones y métodos de identificación personal.

Así, hasta nuestros días, una larga lista de empresas proveedoras de dispositivos lectores de huella dactilar conforman una importante cartera, donde cada una de ellas ofrecen dispositivos lectores con características particulares en cuanto a tipo de tecnología utilizada se refiere, niveles de resolución de imagen, modelo, número de píxeles, área de captura, contraste, nivel de distorsión, etc [30]. Normalmente un

[30] Para maximizar la compatibilidad entre las imágenes de huellas digitales y asegurar la buena calidad de la huellas capturadas, la US Criminal Justice Information Services (división del FBI) en el

scanner típico de huella digital, digitaliza la impresión de la huella a 500 dpi con 256 niveles de grises por píxel.

En la *Tabla 2* se muestran algunos ejemplos de empresas proveedoras y scanners de huella digital, agrupados por tecnología:

	Tecnology	Company	Model	Dpi	Area (h x w)	Pixeles
Optical	FTIR	Biometrika www.biometrika.it/eng/	FX2000	569	0.98" x.52"	560x296 (165,760)
	FTIR	Digital Persona www.digitalpersona.com	UareU2000	440	0.67" x 0.47"	316x228 (72,048)
	FTIR (sweep)	Kinetic Sciences www.kinetic.bc.ca	K-1000	Up to 1000	0.002"x0.6"	2x900 (Hx900)
	FTIR	Secugen www.secugen.com	Hamster	500	0.64"x0.54"	320x268 (85,760)
	Sheet Prism	Identix www.identix.com	DFR 200	380	0.67"x0.67"	256x256 (65,535)
	Fiber optic	Delsy www.delsy.com	CMOS module	508	0.71"x0.47"	360x240 (86,400)
	Electro-optical	Ethentica www.ethentica	TactilSEnse T-FPM	403	0.76"x0.56"	306x226 (69,156)
Solid-state	Capacitive (sweep)	Fujitsu www.fme.fujitsu.com	MBF300	500	0.06"x0.52"	32x256 (Hx256)
	Capacitive	Infineon www.inifineon.com	FingerTip	513	0.56"x0.44"	288x224 (64,512)
	Capacitive	ST-Microelectronics u.st.com	TochChip TCSIAD	508	0.71"x0.50"	360x256 (92,160)
	Capacitive	Veridicom www.veridicom.com	FPS110	500	0.60"x0.60"	300x300 (90,000)
	Thermal (sweep)	Atmel www.atmel.com	FingerChip AT77C101B	500	0.02"»x0.55"	8x280 (Hx280)
	Electric field	Authentec www.authentec.com	AES4000	250	0.38"x0.38"	96x96 (9,216)
	Piezoelectric	BMF www.bom-f.com	BLP-100	406	0.92"x0.63"	384x256 (98,304)

Tabla 2. Ejemplos de scanners de huella digital agrupados por tecnología.
* Fuente tomada del libro Handbook of Fingerprint Recognition Davide Maltoni. Pág. 70

Indistintamente del proveedor, los diferentes dispositivos reconocedores de huella digital, se basan en mecanismos especiales para llevar a cabo el análisis y obtención de los puntos característicos de las huellas dactilares. El elemento más importante de un scanner o lector de huella digital es el ***sensor***, el cuál es el componente donde la imagen de la huella digital es formada.

En términos generales existen sensores basados en principios ***ópticos, capacitivos, de ultrasonido y térmicos*** ***[RFC3p.59, RFC5p.28]***; donde éstos

---

año 1999 da a conocer una serie de especificaciones que regulan la calidad y el formato de las huellas obtenidas por medio de los diferentes dispositivos lectores biométricos. Sin embargo, muchos de los dispositivos fuera de la norma AFIS, no cumplen con dichas especificaciones pero a cambio son usualmente más amigables, compactos y significativamente más baratos.

producen una imagen digital de la huella, consistente en valores de 8 bits de escala de grises.

De esta clasificación, los ***sensores de huella digital de tipo ópticos*** son los más antiguos y los mayormente utilizados hoy en día. En la *Tabla 2* se muestra una lista de scanners[31] comerciales cuyo costo oscilan entre $200 dólares apróx., a excepción de los scanners por ultrasonido, los cuáles son mayormente caros y no están enfocados para aplicaciones de mercado masivo.

Algunos ejemplos sobre tipos de scanners de huella digital son:

- Universal (http:// www.mitretek.org)
- Scanner de DigitalPersona UareU (http://www.digitalpersona.com)
- Scanner Identix Touch View and DFR-2090 (http://www.identix.com)
- Scanner Cross Match Verifier 300 LC y classic (http://www.crossmatch.net)
- Scanner Biometrika FX 2000 (http://www.biometrika.it/eng/index.html) (www.neurotechnologija.com/scanners.html)
- Scanner Precise Biometrics 100 SC (http://www.biometricsdirect.com)
- Scanner KeyTronics Security Desktop (http:// www.networkcomputing.com) (http:// www.neutronet.com)
- Sensor ST Microelectronics TouchChip (www.neurotechnologija.com/scanners.html)
- Identicator Technology DF-90 (http:// www.neurotechnologija.com/verifinger.html) (http:// www.fulcrumspi.com/verifinger.htm)
- Scanner AuthenTec AES4000 y sensores AF-S2 (http://www.authentec.com)
- Sensores Atmel FingerChip (http://www.bergdata.com)
- Sensor BMF BLP-100 (http:// www.bm-f.com), (http:// www.ex-cle.com), (http:// www.biometricsys.ws)
- Scanner SecuGen Hamster (http:// www.access-logix.com) (http://www.kerrysecure.co.uk), (http:// www.eyenetwatch.com), (http:// www.uryou.com)
- TouchChip TCRU1C (http://www.st.com)
- AES4000 EntréPad (USB) (http://www.authentec.com)

[31] Los lectores de huella digital también son llamados scanners o dispositivos biométricos de huella digital.

El dispositivo lector de huella digital utilizado en el presente proyecto es el scanner de Digital Persona UareU 2000 de tipo óptico. Los detalles técnicos pueden consultarse en el ***"Anexo C"*** integrado al final del presente trabajo.

Respecto a los ***sensores basados en tecnología por ultrasonido,*** éstos encabezan el mercado biométrico como dispositivos de vanguardia. Lo anterior dada sus ventajas en relación a los de tipo óptico, evitando las fallas comunes que hasta ahora se llegan a tener con la lectura óptica, por suciedad en la piel o en el dispositivo de escaneo.

Se trata de una tecnología desarrollada en la última década, que ha demostrado una alta fiabilidad al extraer los rasgos más característicos e inequívocos de las personas para posteriores procesos de identificación.

Los sistemas biométricos por ultrasonido consisten en el envío de ondas de diferentes frecuencias que rebotan contra la base de la huella y el dispositivo de escaneo, penetrando cualquier tipo de suciedad encontrada en los dedos como grasa, polvo o manchas de tinta. De esta forma, se obtiene una imagen sin errores de las crestas y los valles del dedo escaneado, consiguiendo una gran precisión en la captura de la imagen que facilitará los procesos posteriores.

Dentro de las características sobresalientes de este tipo de dispositivos, es la insensibilidad del ultrasonido a los elementos externos que impiden una buena lectura de la huella en un sistema óptico (suciedad, luz, humedad, aire, etc); perturbaciones que los sistemas ópticos compensan por medio de software, perdiendo así los elementos fundamentales de la identificación (minutiaes y puntos característicos).

Los scanners por ultrasonido empiezan a desarrollarse hace 18 años atrás como resultado de algunos de los problemas y limitaciones que presentan los scanners de tipo óptico, llevando a los técnicos de la FBI a investigar y desarrollar una tecnología que solventa en gran parte éstos.

Considerando lo anterior, la principal razón de utilizar tecnología de ultrasonido es para mejorar la captura de la imagen de la huella y por tanto, poder realizar una validación de características de manera más precisa, sin errores, rápida y sobretodo, mayormente confiable.

Algunas de las ventajas más importantes de los scanners por ultrasonido Vs. scanners ópticos, son:

- La suciedad que del dedo no afecta la rápida, precisa y segura lectura de la huella.
- Los factores de grasa, humedad y temperatura, no influyen en la lectura e identificación de la huella.

- El scanner no es afectado por la luminosidad del ambiente, sol o luz directa.
- Una huella con estructura de surcos irregulares causa espacios de aire entre el dedo y la platina, hecho que dificulta la lectura óptica basada en la reflexión de la luz. El sistema por ultrasonido por actuar a profundidad, no se ve afectado por esta situación.
- La lectura de una huella por ultrasonido permite una identificación positiva aún a través de guantes de látex, lo que hace posible su uso en bloques quirúrgicos, salas blancas, etc.
- La estructura del lector ultrasónico ofrece una mayor solidez, durabilidad y estabilidad en su calibrado que la de un lector óptico.
- La lectura se hace sobre un cristal plano resistente a los rayones y los malos tratos.
- Menor tiempo requerido para realizar la verificación (demora solamente 1.7 segundos apróx.).
- Cuentan con sistema de auto-test para asegurar el perfecto funcionamiento de todos los componentes que lo conforman.
- No presentan limitaciones en cuanto a memoria para el registro de personas.
- El tamaño apróx. de los templates generados es de 40 y 45 bytes.
- Cumplimiento de las normas exigidas por el FBI de EEUU para la identificación criminal. (Safety certifications – EMC).
- Diferentes modos de búsqueda y comparación: 1:1 y 1:N
- Obtención de imágenes con una definición de hasta 1000 dpi con alto contraste, amplia gama de grises y libres de distorsión.

Cabe mencionar que aunque los scanners por ultrasonido presentan ciertas ventajas en relación a los de tipo óptico, en la actualidad la mayoría de los scanners son de éste último tipo. Lo anterior, debido en gran parte a que el costo de los scanners por ultrasonido resultan mayormente caros y a que estos se encuentran más bien enfocados a áreas donde se requiere un alto nivel de seguridad como: criminalística, médico-forense, FBI, aeropuertos, bancos, instalaciones militares, prisiones, entre otros. Donde evidentemente, la necesidad de identificar de manera precisa, es mayor.

La tecnología de ultrasonido aplicada a scanners de huellas dactilares, representa sin lugar a dudas, uno de los mayores avances en la técnica de identificación de personas y está considerada por los especialistas internacionales en la materia, como…."el salto tecnológico más importante de los últimos 18 años, en cuanto a dispositivos biométricos se refiere".

1.5.2 Campo de Aplicación.

Aunque el uso de la huella dactilar data desde tiempos muy antiguos de acuerdo a hallazgos encontrados, no ha sido hasta en los últimos 20 años que la tecnología biométrica ha llegado a desarrollarse lo suficiente para lograr tener una muy precisa tecnología de clasificación de los patrones de arrugas y los detalles de las huellas (minutiaes); aspecto que le ha permitido pasar de ser, de uso exclusivo para propósitos forenses, hasta llegar al día de hoy en que su campo de aplicación ha proliferado a tal grado de observar su uso en tareas comunes como: el control de acceso a sistemas críticos de varias empresas, acceso seguro a PC's y redes, control físico a instalaciones, control de asistencia, registro e identificación de los individuos en las embajadas, operaciones de comercio electrónico, transacciones bancarias, entre otros.

En la actualidad el campo de aplicación de la tecnología biométrica por huella digital no solo se encuentra enfocada al sector forense, sino que engloba 3 grandes categorías: forense, gubernamental y comercial. Tal y como se muestra en la *Tabla 3:*

Forense	Gubernamental	Comercial
Identificación de cadáveres, investigación criminal, identificación de terroristas. determinación de paternidad. personas extraviadas, etc.	Tarjeta de identificación nacional, servicio correccional, licencia de conductores, seguridad social, gastos de asistencia social, control fronterizo, control de pasaportes, etc.	Acceso a redes, seguridad de datos electrónicos, comercio electrónico, acceso a internet, ATM, tarjetas de crédito, control de acceso físico, teléfonos celulares, control de asistencia de personal, administración de registros médicos, aprendizaje a distancia, etc.

Tabla 3. Aplicaciones de reconocimiento por huella digital divididas en 3 categorías principales.
* Fuente tomada del Libro Handbook of Fingerprint Recognition Davide Maltoni. Pág. 43

Tradicionalmente las aplicaciones forenses han utilizado tecnología biométrica, las aplicaciones gubernamentales han utilizado sistemas basados en token's, y las aplicaciones comerciales han utilizado sistemas basados en conocimiento.

Lo importante a destacar es que en el reconocimiento por huella digital está siendo utilizado cada vez más en los distintos sectores, trayendo importantes beneficios. En relación al tipo de aplicaciones, se pueden dividir en 3 grandes grupos: bancarias, comercio electrónico y control de acceso (*Ver Figura 8*):

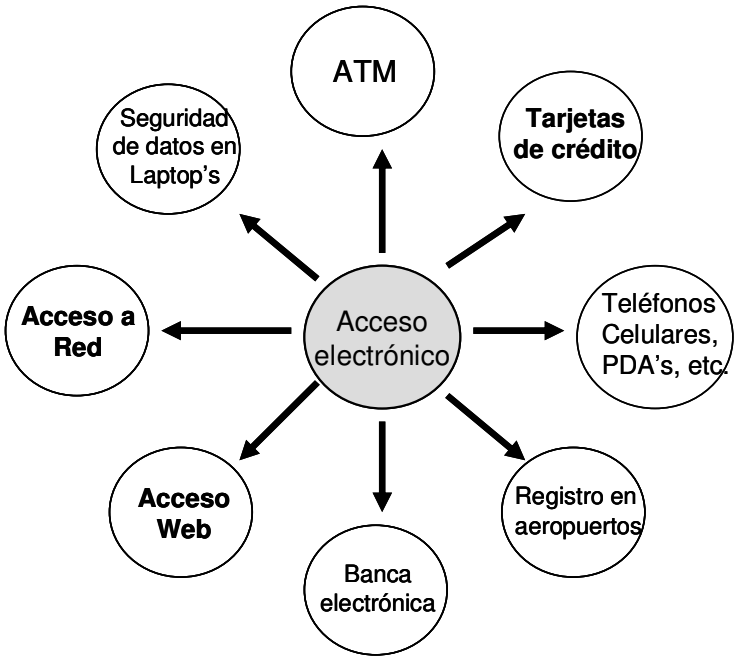


Figura 8. Ejemplos de aplicaciones de uso extendido,
que requieren reconocimiento automático.
* Fuente tomada del Libro Handbook of Fingerprint Recognition Davide Maltoni. Pág. 44

Algunas de las aplicaciones más comunes donde el uso de la huella digital tiene presencia en el proceso de autenticación, se presentan en la siguiente lista:

- Acceso seguro a PC's y redes (internet, extranet, intranet).
- Protección de archivos electrónicos y aplicaciones críticas.
- Acceso físico a edificios, oficinas y áreas restringidas.
- Control de horario y asistencia en empresas.
- Control de acceso físico a áreas restringidas.
- Control de acceso a aplicaciones de comercio electrónico, base de datos y de tipo bancarias.
- Protector de pantallas.
- Bloqueo de sesiones.
- Control de acceso a equipos portátiles.
- Uso en embajadas para control de identidad para entrega de pasaportes y visas.
- Uso en el sector de seguridad social y salud, para el control de padrones de usuarios.

- Uso en el área de criminalística para el análisis y comparación de rastros latentes.
- Uso en el área forense para la validación de identidades.
- Uso en prisiones para identificar guardias y prisioneros.
- Uso en fronteras para validar la identidad de los individuos.
- Uso en corporaciones policíacas y dependencias gubernamentales.
- Uso en cajeros automáticos.
- ……Otros.

Durante este capítulo se ha brindado un panorama general del tema central del proyecto, iniciando con los antecedentes y conceptos de la Seguridad Informática, pasando por lo que es la Criptografía y Modelos de Control de Acceso y Autenticación; hasta llegar a lo que es la tecnología biométrica por huella digital.

Ahora el lector tiene en claro cuál es el propósito del tema, su entorno y enfoque. En el capítulo siguiente se abordará a gran detalle el proceso de autenticación utilizando tecnología biométrica por huella digital, iniciando desde el procesamiento paso a paso al que es sometida la huella digital para la extracción de características (minutiaes), hasta finalizar con el proceso de comparación para decidir si la huella "viva" es igual a alguno de los patrones de huella (plantillas) que se encuentran almacenados en la BD previo a un proceso de registro.

CAPÍTULO 2. CONTROL DE ACCESO BASADO EN TECNOLOGÍA BIOMÉTRICA POR HUELLA DIGITAL.

"Proteger la seguridad de la información no solo equivale a implantar SW y HW para evitar ataques. Significa que en un mercado amplio conformado por entidades federadas, aplicaciones web, LAN, transacciones electrónicas, detección de intrusos y virus, ……, se tenga un común denominador: la correcta administración de identidades de usuario, con sus accesos y privilegios".

Este capítulo está enfocado a dar a conocer a detalle, cuáles son los elementos principales que conforman un sistema de autenticación biométrico haciendo uso de la huella digital; y así mismo, las fases y pasos que integran el proceso.

Con la finalidad de no dejar dudas, dentro del capítulo de manera clara y sencilla se hace la distinción entre lo que es un sistema de verificación y lo que es uno de identificación; sus características y diferencias, así como la relevancia de los parámetros TFR (Tasa de Falso Rechazo) y TFA (Tasa de Falsa Aceptación) para asegurar el correcto y óptimo funcionamiento del sistema biométrico, y con ello, determinar su capacidad de identificación.

Adentrados en el tema, en este mismo capítulo se dan a conocer las cualidades físicas de la huella y el porqué ésta ha resultado excelente patrón para determinar la identidad de las personas, de manera inequívoca en relación a otras características físicas humanas (iris, mano, etc). Teniendo un panorama más claro de las características de la huella digital, en el penúltimo subcapítulo se analiza todo el procesamiento integral que se le da a la huella desde la extracción de la imagen, su normalización, la selección del área de interés, eliminación de imperfecciones, extracción de puntos característicos <<minutiaes>>, etc., hasta llegar a la fase de comparación <<match>> para validar a través de un algoritmo de comparación de minutiaes, que la "huella actual o viva" corresponda a una de los patrones <<plantillas>> almacenadas en la B.D.

Finalmente, se listan algunos de los beneficios y desventajas de la tecnología biométrica en relación a los sistemas tradicionales de identificación de usuarios basados en el uso de passwords. Así mismo, se dan a conocer detalles sobre los kits disponibles para desarrolladores interesados en realizar integraciones y/o adaptaciones de aplicaciones de tipo biométrico de manera fácil y rápida, con la capacidad de operar en diversos ambientes y plataformas. Lo anterior, como parte de los esfuerzos de estandarización en la industria.

Citar las tendencias en el ámbito no podía faltar, así que al final del capítulo se dan a conocer cuáles son las expectativas del mercado biométrico y factores que se pretenden madurar.

2.1 PROCESO GENERAL DE AUTENTICACIÓN MEDIANTE HUELLA DIGITAL.

Una vez analizados los antecedentes sobre el uso de la huella digital y las características principales de la tecnología biométrica basada en el uso de esta característica física, queda claro que con el surgimiento de este tipo de tecnología se eliminan 2 elementos primordiales que hasta ahora han sido clave en todos los sistemas de seguridad informáticos: contraseñas y tarjetas.

Lo anterior viene a resolver en gran medida los problemas de seguridad ya citados (suplantación de identidades, extravío, robo, desconfiguración, compromiso y manejo de contraseñas simples y fáciles de averiguar o robar, etc), además de hacer del proceso algo mayormente seguro, sencillo y amigable hacia el usuario. Adicional a estas ventajas, permite disminuir significativamente la posibilidad de fraude debido a que el uso de la huella dactilar implica presencia física del usuario para realizar el proceso de autenticación.

Pero qué es lo que conforma un sistema de autenticación biométrico por huella digital? Y cuál es el proceso?

En realidad para poder llevar a cabo el proceso de identificación, los sistemas de autenticación por huella digital (al igual que el resto de tipo biométrico), incluyen tanto hardware (HW) como software (SW).

En términos generales, utiliza un dispositivo de captura <<lector de huella dactilar>> y un software biométrico, que de manera conjunta realizan la interpretación de la muestra física <<huella>> y su transformación en una secuencia numérica (a través de algoritmos matemáticos). Como resultado se obtiene lo que se denomina <<patrón de registro o plantilla>>.

Normalmente estos patrones de registro de huellas de usuario, serán almacenados en una base de datos.

Aunque en la actualidad existen diferentes métodos para llevar a cabo el proceso de reconocimiento por huella digital, de manera global el proceso se divide en ***2 grandes fases:*** Registro y Autenticación. Dentro de estas fases a su vez, se identifican ***4 pasos principales***: adquisición de los datos, pre-procesamiento, extracción de características y comparación de plantillas (match), ***[RFC4p.305]***:

Dado lo anterior, para poder entrar al detalle, es preciso indicar que se hará referencia a ***"huella actual, viva ó de entrada"***, a la huella situada en el lector de huella dactilar, o sea, la huella en vivo. Y se denominará ***"plantilla"*** al patrón que normalmente se encontrará almacenado en una BD previo a un proceso de registro. Esta plantilla es el conjunto de características extraídas de la huella transformada en una muestra numérica.

2.1.1 Procesos de Registro y Autenticación

Como grandes fases, el proceso de reconocimiento de patrones biométricos de huella digital, se encuentra dividido en ***Proceso de Registro (enrollment) y Proceso de Autenticación.*** *Ver Figura 9*

Para poder validar la identidad de un usuario a través de su huella, es necesario transformar y representar ésta en una plantilla, para posteriormente, realizar un comparativo entre los diferentes patrones de huellas de usuario y con ello, poder determinar si se trata de un usuario legítimo o no.

El proceso inicia con el registro (***enrollment***) de las huellas dactilares de los usuarios que van a hacer uso del sistema en el cuál requieren ser identificados.

El registro se realiza empleando un dispositivo biométrico <<lector de huella digital>> para examinar la huella.

El usuario puede registrar <<mapear>> una o varias de sus huellas dactilares de los diferentes dedos de sus manos. Para ello, el usuario posiciona su huella en el área de lectura del dispositivo biométrico <<lector de huella digital ó scanner>>, obteniendo éste, la imagen digital de la huella que posteriormente es normalizada mediante un proceso específico. De la imagen ya normalizada se extraen los puntos característicos también denominados ***minutiaes***[32] (crestas y bifurcaciones), los cuáles son cuantificados y traducidos en una plantilla <<secuencia matemática>>.

El sistema biométrico en concreto, no analiza la totalidad de la huella, sino únicamente el conjunto de minutiaes. Cada minutiae es representada con la finalidad de poder realizar el comparativo. La representación consiste en asignar a cada minutiae su posición relativa <<localización x,y respecto al sistema de coordenadas central de la imagen, y de su orientación (ángulo θ)>>. Para mayores detalles, referirse al subcapítulo ***"2.2 El papel de la huella y el proceso de obtención de minutiaes".***

[32] Esta demostrado que dos dedos nunca pueden poseer mas de ocho minutiaes comunes, y cada uno tiene al menos entre 30 y 40 de éstas, lo cuál hace de la huella una característica optima para ser utilizada en la autenticación de individuos.

La plantilla <<template>> obtenida y un dato asociado al usuario << su username[33] o ID >>, son guardados electrónicamente en una base de datos. Información que servirá para su identificación.

A esta primera fase del proceso, se le denomina ***Proceso de Registro*** <<enrollment o registro del usuario en el sistema >>.

Nótese que en ningún caso se extrae la imagen total de la huella, sino una muestra que es transformada en una secuencia de números que la representan como un patrón de registro <<plantilla>>. Es debido a esto, que reproducir la plantilla a partir de una plantilla de un miembro falso, resulta casi imposible

El proceso de registro en resumen, se encarga de adquirir y almacenar la información biométrica en forma de plantillas, para su posterior uso y comparativo, de los ingresos de usuario posteriores en el sistema.

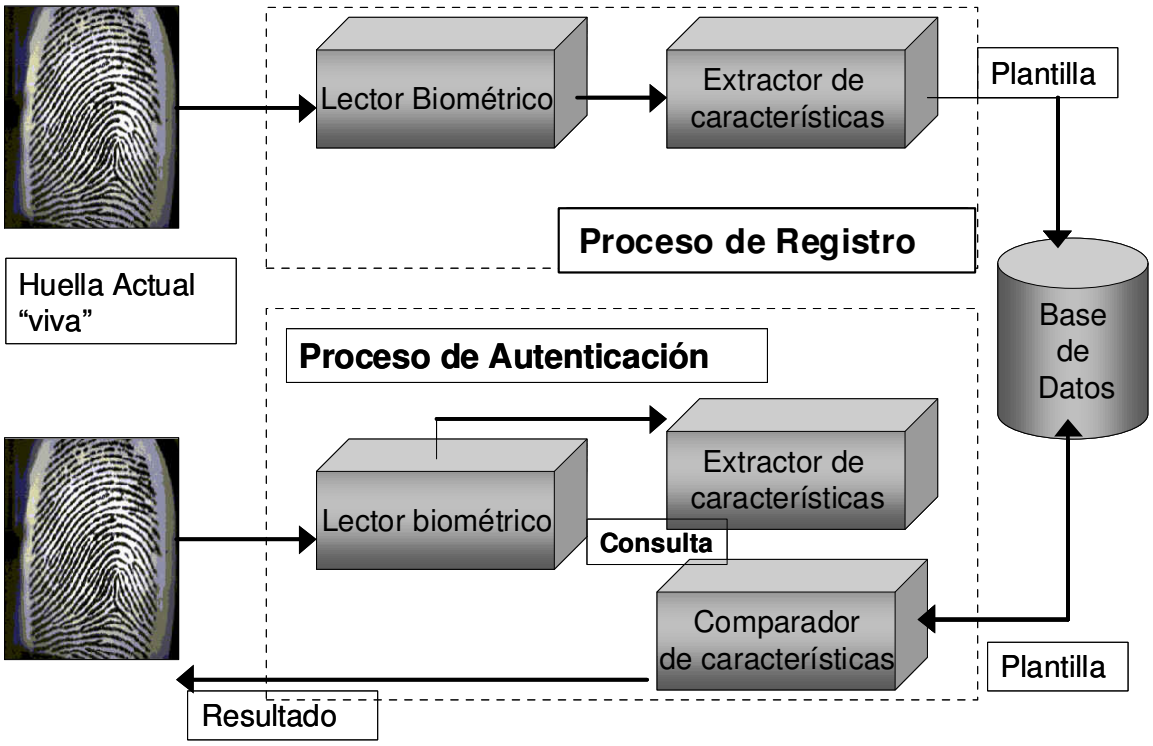


Figura 9. Proceso de reconocimiento de patrones de huella digital, y sus 2 grandes fases (registro y autenticación).

[33] Refiérase a username, al nombre único que identifica a un usuario, y que es utilizado como medio de identificación ante un sistema (p.e: username: eoarguel password:xxxxxx)

La segunda fase consiste en llevar a cabo la autenticación de los usuarios para otorgarles o denegarles el acceso a los recursos. Esto se logra a través de la identificación de su ID o username del usuario y su correspondiente asociación con la lectura de su huella digital para validar si se trata de un usuario legítimo o no.

A esta fase se le denomina ***Proceso de Autenticación***, el cuál necesariamente se da posterior al proceso de registro.

El proceso de autenticación inicia al momento en que un usuario desea autenticarse ante el sistema, debiendo ingresar vía el teclado su PIN, ID o username, y así mismo posicionar en el área de lectura del dispositivo, cualquiera de sus huellas registradas en el sistema biométrico.

El dispositivo biométrico en conjunto con el software biométrico, realizan el mismo proceso citado en la etapa de registro (obtención de la imagen de la huella y su normalización; extracción de los puntos característicos, transformación y obtención de la plantilla), solo que a diferencia de esta etapa, el sistema lleva a cabo un proceso de comparación <<match>>, entre la plantilla obtenida de la "huella en vivo ó huella de entrada" y la "plantilla" almacenada en la base de datos que tenga asociado el username, PIN ó ID ingresado por el usuario.

Dado esto, un usuario será autenticado exitosamente si las características extraídas de la "huella actual" coinciden con las de la <<plantilla>> dentro de un límite de tolerancia definido para el algoritmo de comparación de minutiaes. Es decir, para que el sistema certifique la identidad del usuario, la comparación no necesariamente debe resultar en una igualdad absoluta entre ambas plantillas.

Para realizar la certificación, las plantillas deben ser similares entre sí en cierto grado definido. Es decir, si la comparación de las posiciones relativas de las minutiaes leídas con las almacenadas en la base de datos cae dentro de los parámetros de tolerancia permitidos, se permite el acceso al usuario. En caso contrario, se le es denegado.

Con esto queda claro que los dispositivos biométricos no comparan directamente las huellas. Éstos utilizan algoritmos específicos para la creación de plantillas <<patrones ó templates>> que son representaciones electrónicas resultado de transformaciones matemáticas. Dichas plantillas por medio de un algoritmo de comparación, son utilizadas para comparar y validar la identidad de los usuarios durante el proceso de autenticación de huellas.

Para realizar todo el proceso desde la extracción hasta la validación de patrones de huella, los sistemas de identificación de tipo biométrico incluyen algoritmos específicos tanto para la generación, almacenamiento y comparación de éstas. Generalmente estos algoritmos son patentados por cada tipo de dispositivo biométrico.

Las técnicas de comparación <<match>> de huellas se encuentran clasificadas básicamente en 3 categorías**: *basado en minutiaes, basado en correlación y basado en patrones*** [34]. Donde, la técnica basada en minutiaes es una de las mayormente utilizadas, aunque una de las principales fuentes de problemas lo representan las imágenes de las huellas capturadas con baja calidad, al dificultar el proceso de extracción de minutiaes. La técnica basada en correlación por su parte, presenta problemas por las traslaciones y rotaciones de las imágenes.

Lo importante a destacar de todo esto, es que los procesos de extracción y comparación son pasos verdaderamente importantes en el proceso.

Ahora bien, como puede observarse, lo que el sistema hace como resultado del proceso, es "autenticar" al usuario a través de la asociación de su ID o username, y la lectura y comparación de su huella, validando si el usuario es legítimo o no. Todo esto, partiendo del hecho de que si la huella es encontrada en la BD segura, necesariamente corresponde a un usuario autorizado y donde su huella tendrá asociados los datos personales específicos que lo identifican. Es decir, el sistema verifica la identidad del usuario.

Como puede observarse, en un sistema biométrico la disyuntiva entre seguridad vs. conveniencia (hacer difícil la entrada a los no autorizados contra permitir el fácil acceso a los autorizados) no representa un problema, dado que la combinación de la identificación biométrica <<plantilla>> y un código de usuario <<PIN, ID ó username>> digitado en un teclado ofrece una seguridad virtualmente impenetrable.

[34] En la técnica basada en patrones, el dispositivo lector toma una imagen gráfica de la huella digital, típicamente capturándola como una imagen TIFF (Tagged image File format). El software de procesamiento examina la imagen de la huella digital y ubica el centro de la imagen, el cuál podría ser distinto al centro de la huella digital. Luego se corta la imagen a una distancia definida alrededor de ese centro de la imagen. La región recortada se comprime y se almacena para comparaciones posteriores. Los patrones de huella obtenidos miden entre 500 y 700 bytes comprimidos, y cerca de 1,024 bytes sin comprimir. El tamaño de la plantilla está directamente relacionado con la imagen y no puede controlarse fácilmente sin sacrificar detalle (y por consiguiente utilidad) de la imagen. Las plantillas basadas en patrones son más sensibles a los cambios físicos en la huella debido a que la comparación se hace usando una imagen recortada de la huella. Si una huella viva llega a sufrir cicatrices o manchas, se requerirá obtener una nueva imagen, extraer la plantilla y almacenarla. Debido a esto, la técnica basada en minutiaes es mayormente utilizada en relación a ésta otra.

2.1.2 Pasos generales involucrados en el proceso de reconocimiento por huella digital.

Ya se han analizado de manera general, las 2 grandes fases que conforman el proceso de reconocimiento de huellas digitales: Proceso de Registro y Autenticación.

Ahora corresponde entrar al detalle y analizar cuáles son los ***pasos principales*** que se llevan a cabo dentro de estas dos fases, desde la captura de la huella y su procesamiento, hasta la comparación de plantillas para determinar si se trata de una huella válida o no.

Tal y como se muestra en la *Figura 10*, estos pasos principales son: adquisición de los datos, pre-procesamiento, extracción de características y comparación de patrones (plantillas).

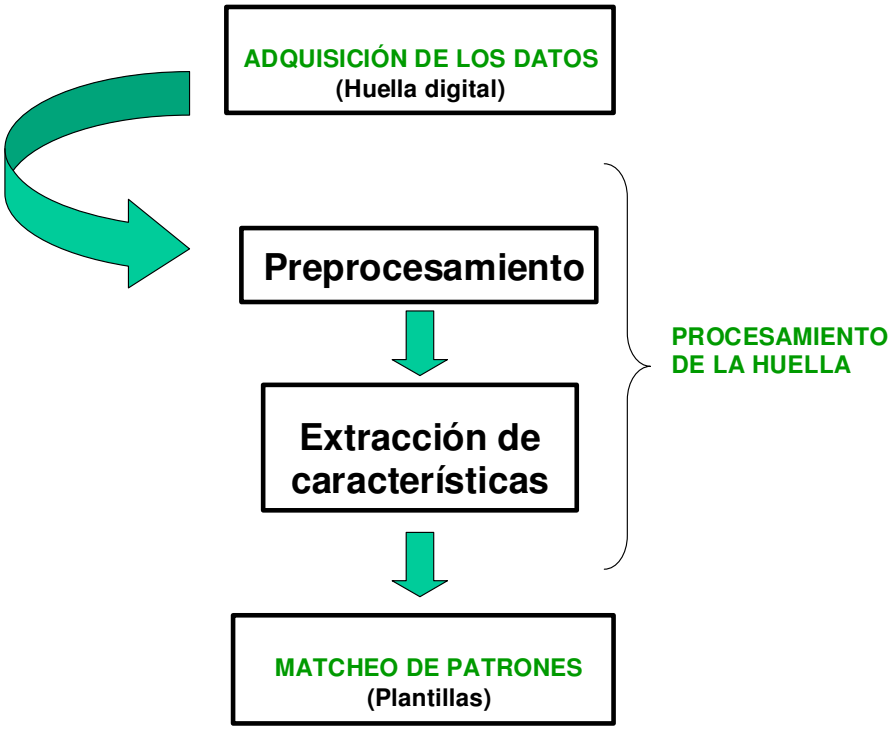


Figura 10. Pasos involucrados en el proceso de reconocimiento por huella digital

2.1.2.1 Adquisición de los datos.

El dispositivo biométrico (HW→ lector de huella digital) por medio de su scanner integrado, capta la huella dactilar del usuario y obtiene una imagen digital de ésta.

2.1.2.2 Preprocesamiento.

Debido a que la imagen digital obtenida de la huella puede tener imperfecciones, ruidos, etc; la huella digital previo al proceso de extracción de características, es sometida a un procesamiento integral para mejorar su calidad con la finalidad de facilitar la identificación de las minutiaes, su posicionamiento en relación a las coordenadas (x,y) y los ángulos de orientación. El procesamiento que se le da a la huella consiste básicamente en la aplicación de filtros para la eliminación de ruidos y normalización; segmentación <<descomposición de la imagen de la huella en foreground y background (ruido) para reducir el número de puntos falsos y seleccionar el área de interés>>, y cálculo del campo direccional (DF).

2.1.2.3 Extracción de características.

De la imagen digital mejorada, se extrae un conjunto de puntos característicos denominados **<<minutiaes>>**, mismos que a través de un algoritmo matemático que no tiene inversa, son transformados en una secuencia numérica, dando como resultado un ***patrón de registro o plantilla***.

Dicho patrón de registro o plantilla, es almacenado en una base de datos segura.

2.1.2.4 Comparación de patrones (plantillas)

Este paso consiste en comparar el patrón de registro obtenido de la huella de "entrada, actual ó viva" de un usuario vs. el patrón o patrones de huellas previamente registrados/almacenados en una base de datos. Es decir, es un comparativo entre plantillas para determinar si el usuario que está siendo autenticado en el momento <<huella de entrada>>, es un usuario legítimo del sistema o no. El resultado del proceso es <<match- no match>>

Los detalles respecto a todo el procesamiento que se le da a la huella, son tratados en el subcapítulo ***"2.2 El papel de la huella y el proceso de obtención de minutiaes".***

2.1.3 Identificación vs. Verificación.

Tal y como se detalla en la *Figura 11,* en términos generales existen 2 formas de validar la identidad del usuario: ***verificación e identificación.***

Saber diferenciar estos términos es algo realmente relevante, pues aunque éstos pudieran parecer equivalentes, la realidad es que existe una gran diferencia entre ellos; dando como resultado implicaciones sobre todo en cuestión de requerimientos de equipo de cómputo, procesamiento y tiempos de respuesta.

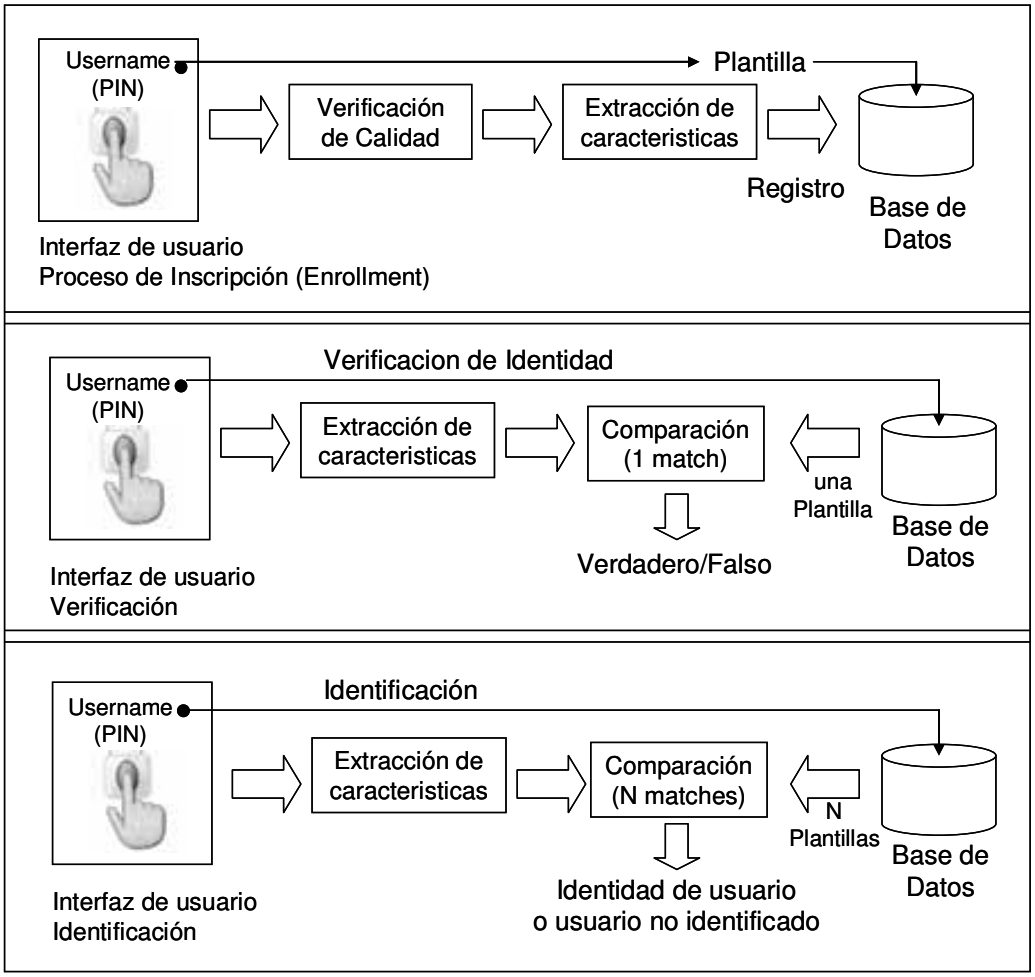


Figura 11. Diagrama a bloques de un sistema de reconocimiento de huellas, donde se muestran las actividades de registro (enrollment), verificación e identificación.
* Fuente tomada del libro Handbook of fingerprint recognition Davide Maltoni. Pág. 4

Un ***sistema de identificación*** realiza una búsqueda exhaustiva de la característica biométrica captada <<huella en vivo ó huella de entrada>>, entre TODOS los patrones de huellas de los usuarios registrados. Esto conduce a una comparación del tipo uno a muchos (1:N) para establecer la identidad del usuario <<quién es>>.

Esto sería por ejemplo el que un usuario expusiera su huella a través de un dispositivo lector, y el sistema biométrico fuera capaz de determinar si es un usuario válido y en ese caso, determinar de quién se trata. Esto hace del proceso una actividad compleja que necesariamente debe ser realizada por medios automatizados y que además, como consecuencia, tiene implicaciones técnicas importantes.

En un ***sistema de verificación*** sin embargo, lo que tradicionalmente se hace, es que se asocia un ID de usuario con el patrón de su huella digital. Esto conduce a una comparación uno a uno para determinar si la identidad reclamada por el usuario es verdadera o no. Es decir, el usuario introduce su identidad (su PIN, un numero ID ó username, etc.) y además posiciona su huella dactilar en el lector biométrico. El sistema biométrico realiza una consulta a la base de datos en busca del ID o username del usuario, y si éste es encontrado, toma el patrón de huella que tenga asociado <<plantilla>>. Este patrón de huella encontrado es comparado con el patrón de la “huella en vivo” que en ese momento se captó. Si coinciden, otorga el acceso., en caso contrario, se le es denegado.

En este caso, el sistema biométrico no identifica al usuario, tan solo lo autentica, validando si <<es quién dice ser>>. Como puede observarse, en este proceso el universo de usuarios se reduce, llevando a cabo una comparación de 1:1 en lugar de 1:N como es en el caso de la identificación. Ver *Figura 12*

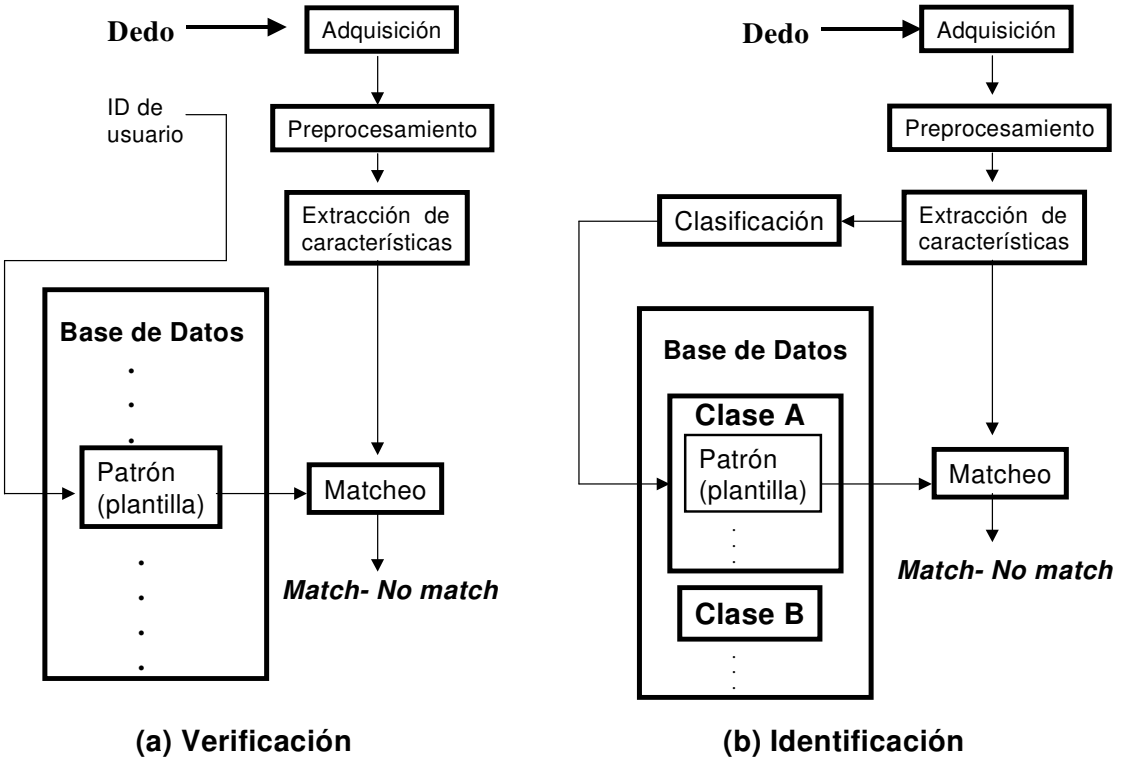


Figura 12. Diagrama de bloques de un sistema de reconocimiento por huella digital donde se hace distinción entre: (a) Verificación (b) Identificación.

2.1.4 Tasa de Falsos Rechazos (TFR) y Tasa de Falsas Aceptaciones (TFA).

Sin importar la distinción entre si se trata de un sistema de verificación ó identificación, lo importante a señalar, es que la coincidencia entre plantillas como resultado del proceso de comparación, no necesariamente debe arrojar una igualdad absoluta del 100%. Para ello, debe existir un umbral de tolerancia permisible.

Lo anterior no quiere decir que los sistemas biométricos no sean seguros, sino simplemente, que son sistemas probabilísticos, no absolutos y que como en todo, se debe permitir tener un porcentaje de variación, que por un lado asegure un nivel de precisión aceptable en los sistemas, y por otro, no se caiga en la paranoia de querer tener un 100% de exactitud porque entonces podrían presentarse problemas de denegación del servicio. Lo anterior resulta conveniente debido a la existencia de diversos factores como el sudor, la hinchazón de los dedos, las cortaduras, etc [35],

[35] Cuando un sistema basado en minutiaes procesa una huella digital, una cicatriz, arruga o mancha puede resultar en unas cuantas minutiaes, pero éstas sólo representarán un pequeño porcentaje del total de las minutiaes extraídas. Si 20% de las minutiaes que se extraen se deben a cambios fisiológicos de la huella desde que se tomó por primera vez, aún se cuenta con el 80% de las

que fácilmente pueden influir al momento de realizar la lectura de las huellas, y con ello, tener leves variaciones matemáticas de la muestra obtenida.

En relación a esta cuestión, estudios han demostrado que la exactitud de la medición varia de acuerdo a la tecnología y los diferentes dispositivos biométricos en valores desde 1/ 1,000 a 1/ 1078; y así mismo, que la probabilidad de que dos personas tengan la misma huella digital es de 1/ 67 millones, lo cuál confirma que la validación de identidades por huella digital es una de las tecnologías más seguras en términos de exactitud.

Aunado a lo anterior, el nivel de precisión generalmente es un parámetro ajustable en la mayoría de los dispositivos biométricos, lo cuál proporciona una mejor libertad de ajustar dicho parámetro, de acuerdo a la necesidad específica que se tenga.

En términos generales el proceso es común en todos los modelos de autenticación de tipo biométrico, representando la ***decisión***, el paso final del proceso y la característica más importante que determinará el nivel de fiabilidad y aceptación del sistema biométrico.

Una decisión tomada por un sistema biométrico distingue a los “usuarios legítimos” de los “impostores”. Para cada tipo de decisión, existen dos posibles salidas <<verdadero- match>> ó <<falso- no match>>. Es decir, se tiene un total de 4 posibles respuestas:

1. Un usuario legítimo es aceptado.
2. Un usuario legítimo es rechazado. (error tipo I)
3. Un impostor es rechazado.
4. Un impostor es aceptado. (error tipo II)

De estas posibles salidas, solo la 1 y la 3 son correctas, mientras que la 2 y 4 no lo son.

El grado de decisiones correctas Vs. decisiones erróneas, puede ser asociado por la distribución estadística de usuarios legítimos e impostores. Para ello, existen 2 parámetros importantes a citar:

- **TFR (Tasa de Falsos Rechazos ó False Rejection Rate ó Error tipo I)**: Probabilidad de que el sistema de autenticación rechace a un usuario legitimo por su incapacidad de identificarlo correctamente. Este puede ocurrir cuando

---

minutiaes restantes para comparar. Puesto que una buena comparación se puede lograr con tan sólo el 30% de las minutiaes, la disponibilidad del 80% ofrece una margen de seguridad bastante amplio. Las plantillas de minutiaes, por lo tanto, son muy indulgentes a los cambios físicos de la huella, evitando tener que volver extraer una plantilla de la nueva imagen del dedo. **[RFC11]**

la información de la huella digital cae fuera de los límites de tolerancia aceptable debido a condiciones propias del dedo, colocación, presión, etc.

- **TFA (Tasa de Falsas Aceptaciones ó False Acceptance Rate ó Error tipo II)**: Probabilidad de que el sistema de autenticación autentique correctamente a un usuario ilegitimo.

Estos parámetros están íntimamente relacionados, de hecho son inversamente proporcionales uno de otro: una TFR bajo usualmente entregará un TFA alto, y viceversa.

Evidentemente un nivel elevado en algunos de estos tipos de tasa, tienen su inconveniente; si bien, una tasa alta de falsos rechazos traerá descontento entre los usuarios del sistema, por otro, una tasa alta de falsas aceptaciones dará como resultado serios problemas de seguridad al permitir el acceso a usuarios ilegítimos.

Con esto, el reto o recomendación, es identificar el nivel de seguridad que se requiere aplicar en el sistema dependiendo de la necesidad específica que se tenga.

Algunos sistemas pueden requerir un nivel de seguridad alto <<TFA bajo>>, mientras otros pueden requerir ser más amigables, otorgando fácil acceso <<TFR bajo>>, aunque no por ello, dejar de ser seguros.

Lo importante es definir el equilibrio más conveniente entre ambos parámetros, con la finalidad de tener una ***tasa de éxitos*** aceptable:

TE= 1- (TFA + TFR)

Para lograrlo, se debe fijar un umbral que permita igualar los 2 parámetros para asegurar el funcionamiento óptimo del sistema biométrico. Este umbral es llamado ***Tasa de Error Igual (TEI),*** y es el que determina la capacidad de identificación de un sistema y del cuál en gran parte, depende su éxito y aceptación por parte de los usuarios. En el capítulo ***"4. Validación del Sistema",*** se podrán obtener mayores detalles acerca los parámetros implicados para validar el nivel de fiabilidad del sistema biométrico.

Con lo anterior resulta conveniente destacar la importancia que tiene el hacer uso de tecnologías confiables para llevar a cabo la correcta administración de identidades, que permitan mantener protegidos los activos críticos que conforman los sistemas informáticos. Así mismo, dejar en claro que la elección de la tecnología idónea para llevar a cabo la validación de identidades a final de cuentas, debe estar basada en función a la necesidad específica que se tenga, bajo las condiciones y recursos que se dispongan, considerando los factores ya mencionados. Obviamente sin olvidar

que un sistema de identificación para que sea considerado viable, deberá ser al menos económicamente redituable para la organización, tener un nivel alto de fiabilidad y ser fuerte antes ataques informáticos.

2.2 EL PAPEL DE LA HUELLA Y EL PROCESO DE OBTENCIÓN DE MINUTAES.

2.2.1 La huella dactilar

La huella dactilar ha resultado un excelente patrón para determinar la identidad de las personas de forma inequívoca, tras comprobarse que debido a su estructura conformada por terminaciones, surcos y bifurcaciones, las huellas dactilares son únicas e irrepetibles en todos los seres humanos e incluso entre gemelos o entre los diferentes dedos de una misma persona: [36]

La huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. La huella dactilar tiene como característica principal, la presencia de un conjunto de partes donde la piel se eleva <<crestas>> sobre las partes más bajas <<valles existentes entre las crestas>>.

Dada esta estructura física, es como se han podido crear algoritmos específicos para llevar a cabo la extracción de puntos característicos para la identificación de los individuos.

Aunque de acuerdo a estudios en una huella dactilar humana se pueden distinguir hasta 18 tipos diferentes de puntos característicos, los principales que se pueden identificar en una huella dactilar son: terminaciones <<final de cresta>>, bifurcaciones, puntos de cresta y encerramientos, tal y como se muestra en la *Figura 13*:

[36] Después del ADN, la huellas dactilares constituyen la característica humana más singular. De acuerdo a estudios, la probabilidad de que 2 personas tengan una misma huella digital es 1/67 millones, lo cuál hace de la huella, una de las características más convenientes de utilizar en el proceso de autenticación de usuarios. La medición automatizada de la huella digital requiere un gran poder de procesamiento y alta capacidad de almacenamiento. Por eso, los productos biométricos basados en huella digital se basan en rasgos parciales, lo cuál aumenta la probabilidad de que dos personas resulten con plantillas similares a valores de 1/100,000 a 1/1,000,000, representando ser una de los dispositivos biométricos de mayor seguridad.

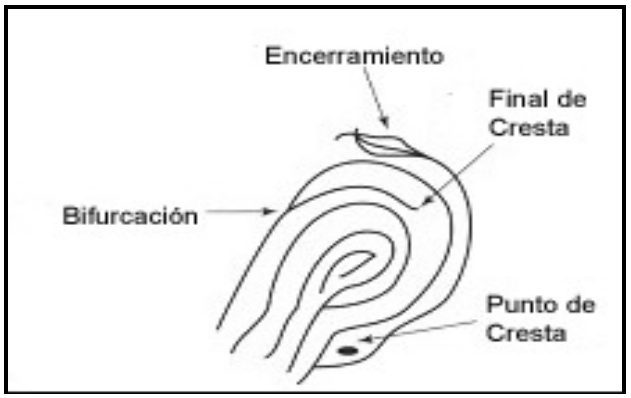


Figura 13. Minutiaes conformadas por encerramientos (enclosure), bifurcaciones (bifurcations), final de cresta (ridge ending) y puntos de crestas (ridge dot).
* Fuente tomada del libro Implementing Biometric Security John Chirillo- Scout Blaul. Edit. Wiley. Pág.15

Así mismo, las huellas dactilares se clasifican en 3 categorías en base a la forma que éstas presentan: curva (Loop), espiral (whorl) y arco (Arc). Lo anterior es de ayuda en sistemas de Identificación donde el comparativo es 1:N, pues a través de la clasificación de las huellas se logra reducir el número de comparaciones a realizar. En la *Figura 14* se muestra esta clasificación:

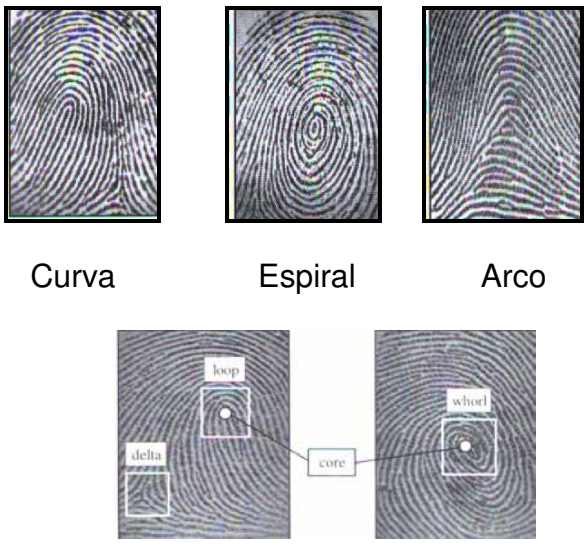


Figura 14. Clasificación de las huellas digitales. Estudios indican que alrededor del 65% son de tipo curva, 30% de tipo espiral y 5% de tipo arco.
Fuente tomada del libro Implementing Biometric Security John Chirillo- Scout Blaul Edit. Wiley. Pág. 15

2.2.2 Puntos característicos de la huella: bifurcaciones y terminaciones.

De acuerdo al área biométrica, la imagen digital obtenida de una huella se encuentra conformada por un conjunto de puntos con características únicas que pueden ser traducidos de forma general en términos de ***terminaciones*** <<líneas con terminación abrupta>> y ***bifurcaciones*** <<intersección de líneas>>; donde a la conformación de éstos, se le denominan ***minutiaes***. ***[RFC3]***

Adicional a estos puntos característicos de la huella dactilar, existen los denominados ***puntos singulares*** <<*cores y deltas>>,* donde la curvatura de las crestas es máxima. *Ver figura 14.*

La característica más interesante que presentan tanto las minutiaes como los puntos singulares, es que son únicos para cada individuo y permanecen inalterables a lo largo de su vida.

A pesar de esta variedad de minutiaes, las más importantes y las mayormente utilizadas por los algoritmos automatizados de comparación de huellas son: terminaciones y bifurcaciones; donde estas dos características quedan inequívocamente definidas a partir de su localización <<coordenadas x,y respecto al sistema de coordenadas central de la imagen>> y de su orientación <<ángulo θ>> [37]**:**

Terminación (ridge termination- ridge ending)[38]**:** Característica definida como el punto donde la cresta acaba de forma abrupta. Está dada por las coordinas [x0, y0], y el ángulo θ formado por la tangente que la minutiae forma con el eje horizontal.

Bifurcación (ridge bifurcation): Característica definida como el punto en el que la cresta se bifurca en dos o más crestas. Está dado por el ángulo de inclinación θ definido por la terminación de la minutiae y la bifurcación. Ver *Figura 15*.

---

[37] El término minutiae es denominado algunas veces como "Detalle Galton" en honor al Sr. Francis Galton, al ser la primera persona que utilizó el término minutiae en el año de 1892, tras realizar una análisis exhaustivo de las características de las huellas humanas y confirmar que éstas no cambian con el transcurso del tiempo de vida de las personas. **[RFC3p.85]**

[38] La American Nacional Standards Institute (ANSI, 1986), propuso que la taxonomía de las minutiaes se encontrara basada en 4 clases: terminaciones, bifurcaciones, trifurcaciones (o crossovers) e indeterminadas. El modelo de minutiaes adoptado por la FBI (Westeing, 1982) considera únicamente Terminaciones y Bifurcaciones. **[RFC3p.30y85]**

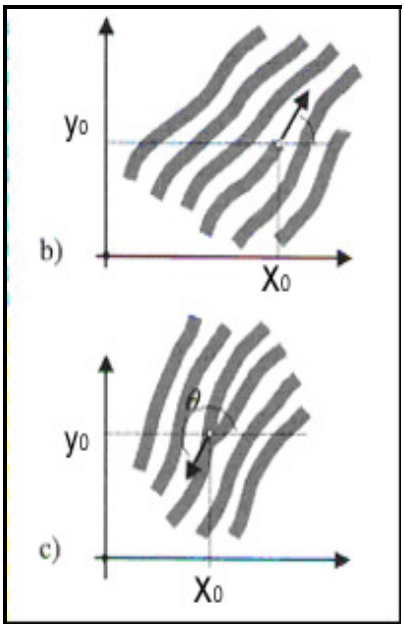


Figura 15. Minutiaes mayormente utilizadas en el proceso de comparación:
final de cresta y bifurcación.
b) Final de cresta dada por las coordenadas (Xo, Yo) y el ángulo θ formado por la tangente de la minutiae con respecto al eje horizontal. c) Bifurcación, donde θ está definido por el final de cresta y la bifurcación original que existe en la imagen negativa.
* Fuente tomada del libro Handbook of Fingerprint Recognition. Davide Maltoni 2003 Springer-Verlag New Cork. 2003 pág. 85

El motivo principal por el cuál se utilizan estos 2 tipos de minutiaes, es porque de acuerdo a estudios, las terminaciones representan aproximadamente el 60.6% de todas las minutiaes en una huella y las bifurcaciones el 17.9%. Además de que varias de las minutiaes menos típicas pueden ser expresadas en función de éstas dos señaladas.

Obviamente, para poder identificar a una persona mediante su huella, es necesario poder representar ésta última en forma de minutiaes para poder realizar el comparativo entre patrones biométricos. Para esto, la representación estándar consiste en asignar a cada minutiae una posición espacial (x,y) y su dirección θ, que es tomada con respecto al eje x en el sentido contrario a las manecillas del reloj. *Ver figuras 15 y 16*

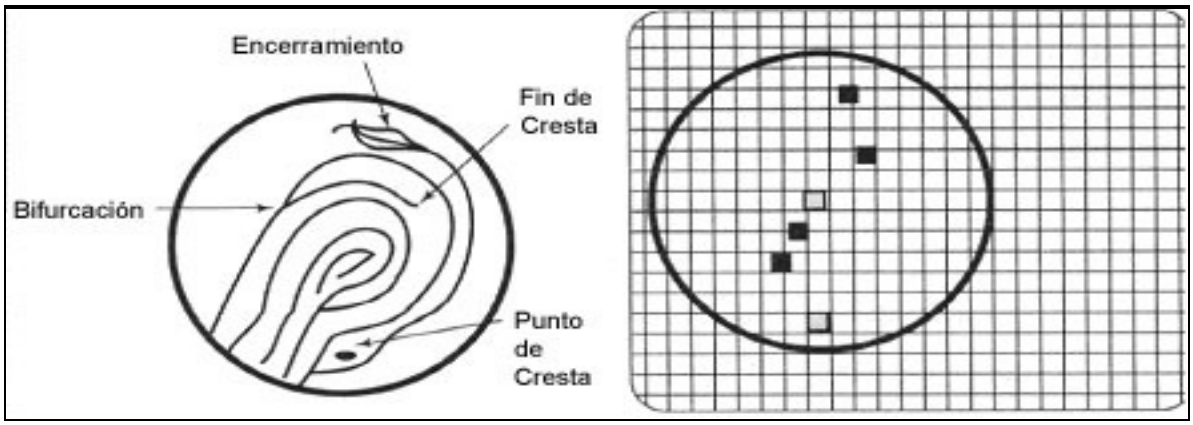


Figura 16. Ejemplo de una plantilla simple (template).
* Fuente tomada del libro Implementing Biometric Security
John Chirillo- Scout Blaul Edit. Wiley. Pág. 19

2.2.3 Procesamiento integral de la huella para la obtención del patrón biométrico.

Hasta el momento se han analizado en términos generales, las 2 principales fases que integran el proceso de reconocimiento por huella digital y los 4 pasos inmersos dentro de éstas. En este apartado muy particularmente nos enfocaremos a analizar de manera detallada el ***procesamiento integral que se le realiza a la huella, para obtener un patrón biométrico <<plantilla>>*** de buena calidad; donde al final del proceso, tiene lugar la comparación de patrones. Ver *Figura 17*

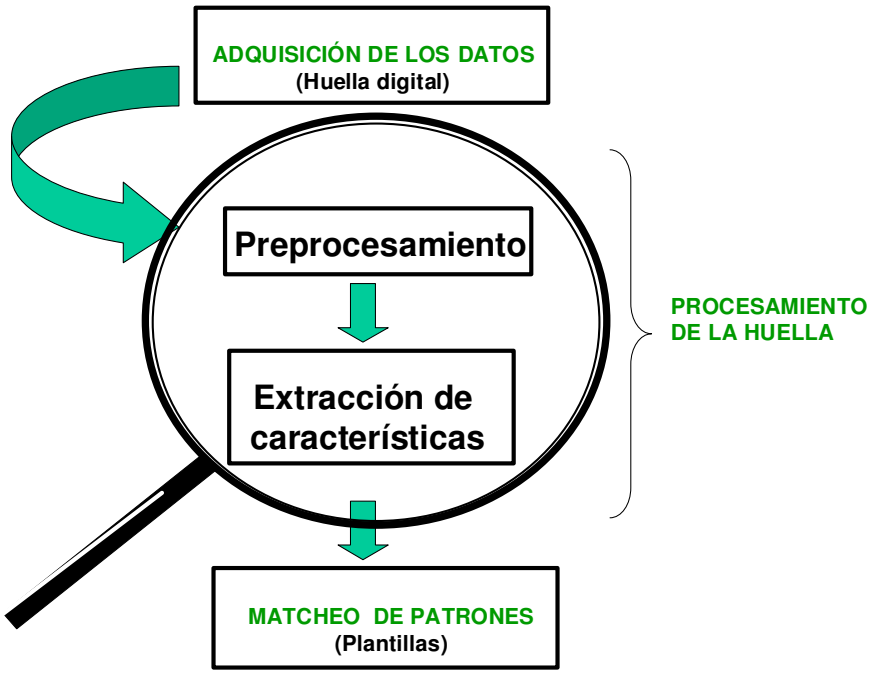


Figura 17. Pasos donde la huella digital es procesada para la extracción del patrón biométrico (plantilla).

Como se representa en la *Figura 18*, en el proceso intervienen lo que son: ***Algoritmo de extracción de minutiaes y Algoritmo de comparación de minutiaes.****[RFC3]*

Considerando lo anterior, en la primer etapa del proceso se tiene como objetivo el procesamiento de la huella, iniciando con su normalización, selección del área de interés, eliminación de imperfecciones, extracción de crestas, etc; hasta finalizar con la extracción de minutiaes que dan lugar a la <<plantilla ó patrón biométrico>>.

La segunda etapa es finalmente la comparación de las plantillas <<conjunto de minutiaes>>, para determinar si la huella del usuario es válida o no.

A continuación se analiza cada paso a detalle:

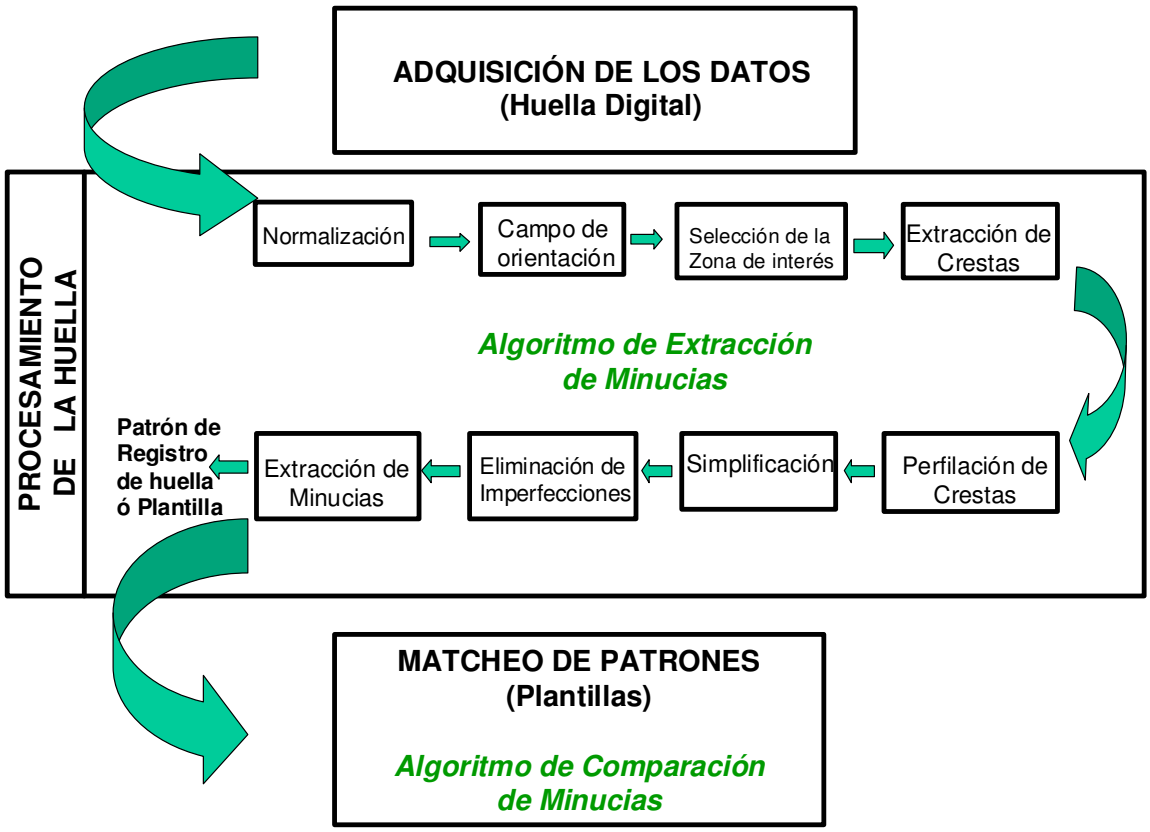


Figura 18. Procesamiento detallado que se le realiza a la huella, para la extracción del patrón biométrico (plantilla), iniciando con la captura hasta el proceso final de comparación.

2.2.3.1 Algoritmo de extracción de minutiaes.

Esta es una de las fases más importantes del proceso de reconocimiento de huellas, donde dependiendo de la calidad de la imagen capturada, algunos algoritmos de extracción de minutiaes podrán obviar algunas minutiaes, y en otros se pueden añadir minutiaes falsas. Las imperfecciones de la imagen pueden generar errores al determinar las coordenadas de cada minutiae y su orientación. La fiabilidad del sistema estará en relación a este conjunto de factores al momento de hacer la comparación entre la “huella actual” y la <<plantilla>>, de allí su importancia.

2.2.3.1.1 Normalización de la imagen.

En esta fase se busca disminuir los rangos de variación de grises entre las crestas y valles de la imagen capturada. Ver *Figura 19*

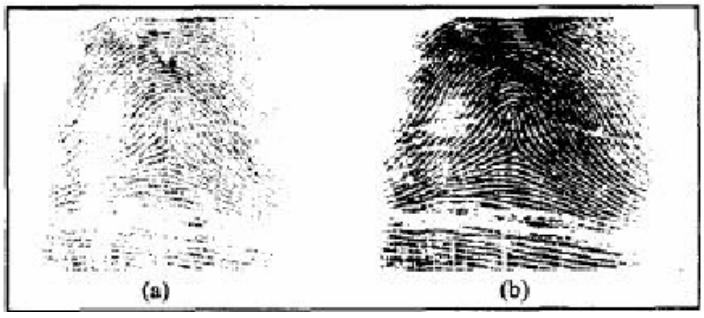


Figura 19. (a) Huella original (b) Huella normalizada

2.2.3.1.2 Cálculo del campo orientación (orientación local de las crestas de la huella).

En esta etapa tal y como se muestra en la *Figura 20*, la imagen se divide en bloques de 16 x 16 pixeles y se calcula la inclinación para cada píxel en coordenadas x, y.

Como pueden existir variaciones significativas del ángulo entre bloques adyacentes debido a factores como ruido y daños en los valles o crestas de la imagen, se aplica un filtro espacial de 5x5 pixeles al campo de orientación estimado para reordenar correctamente todos los segmentos.

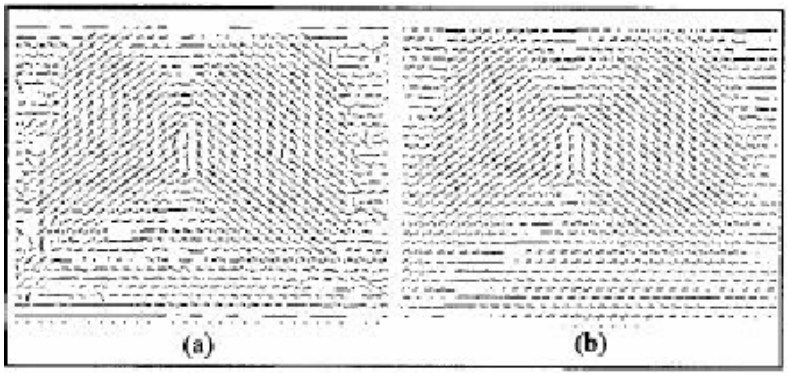


Figura 20. (a) Huella orientada (b) Campos realineados

2.2.3.1.3 Selección de la zona de interés.

En esta etapa se selecciona el área de la imagen definida por todos los bloques de 16x16 en la que existe una alta variación de nivel de grises en la dirección normal de las crestas existentes. Lo anterior debido, a que la imagen contiene ruido de fondo y los algoritmos podrían generar minutiaes fuera del área ocupada de la huella. *Ver Figura 21*

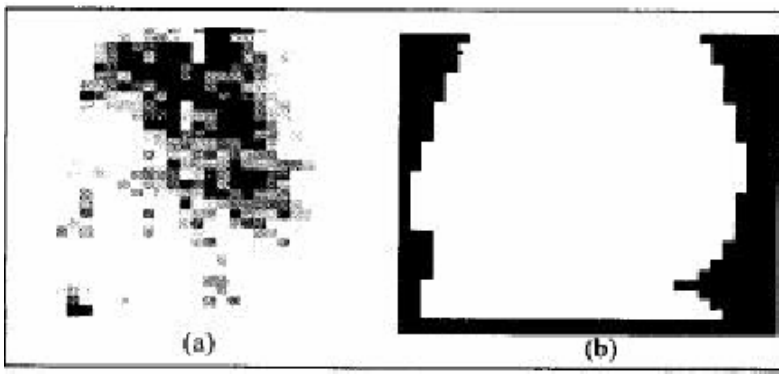


Figura 21. (a) Variaciones de la huella (b) Zona de interés

2.2.3.1.4 Extracción de crestas.

En esta etapa se realiza un filtrado de la imagen de la huella con la finalidad de incrementar el nivel de gris en la dirección normal de las crestas y con ello, decidir si un píxel pertenece o no a una cresta dada.

Si el nivel de gris de un píxel excede un umbral en las dos imágenes filtradas, se considera que el píxel pertenece a una cresta; de otra manera se determina que es un valle. Una vez realizado esto, se obtiene una imagen binaria de la huella, con bordes de crestas lisos. Ver *Figura 22*

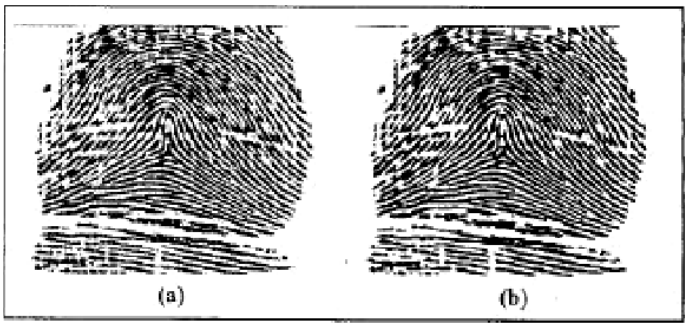


Figura 22. (a) Imagen filtrada (b) Imagen binaria obtenida

2.2.3.1.5 Perfilación de crestas.

En esta etapa se filtra la imagen para perfilar las crestas de la huella y eliminar las manchas de ciertas áreas. Para esto, se extraen los componentes de baja frecuencia y posteriormente se eliminan de la imagen original, proporcionando los componentes de alta frecuencia necesarios para perfilar las crestas. Se puede aplicar un nuevo filtro para eliminar las crestas falsas debido a manchas en la imagen utilizando una mascara espacial capaz de adaptar su orientación localmente a la orientación de la cresta. Ver *Figura 23*

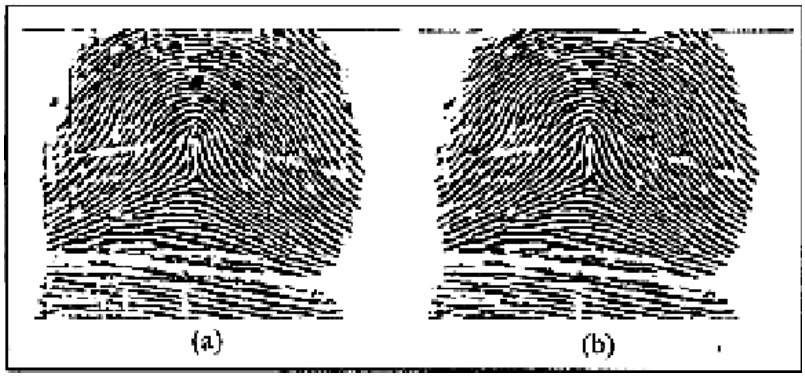


Figura 23. (a) Imagen después del 1er. filtro perfilador (b) Imagen después del segundo filtro perfilador.

2.2.3.1.6 Simplificación.

En este paso se aplican 2 algoritmos paralelos de simplificación con la finalidad de reducir a un único píxel el ancho de las crestas en la imagen. Este proceso se realiza sin modificar la estructura original de las crestas de la imagen, debiendo el algoritmo, calcular correctamente los comienzos, finales y bifurcaciones de las crestas.

2.2.3.1.7 Eliminación de imperfecciones.

Después del paso anterior llegado a este punto, dependiendo de la calidad de la imagen, ésta puede presentar crestas rotas, crestas falsas y huecos, para lo cuál se aplica un algoritmo para eliminar todas las líneas que no corresponden a crestas y otro algoritmo para unir crestas rotas. Ver *Figura 24*

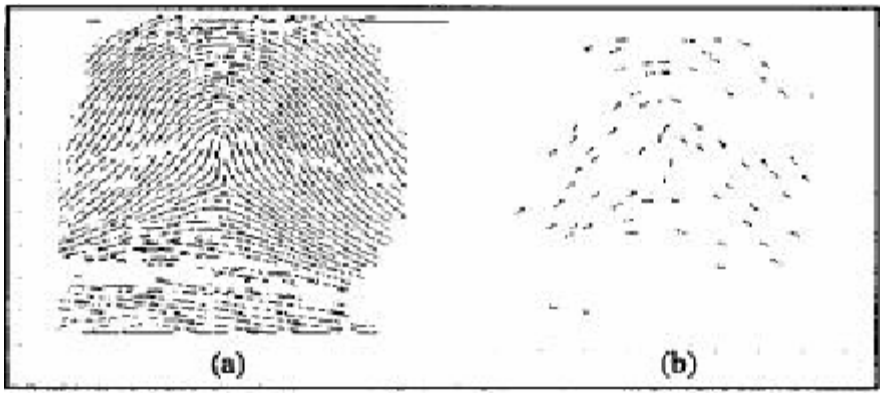


Figura 24. (a) Imagen después de la simplificación y eliminación de imperfecciones. (b) Patrón de minutiaes después del proceso de eliminación de conjuntos.

2.2.3.1.8 Extracción de minutiaes.

Como se puede observar en la *Figura 25*, en esta etapa se extraen las minutiaes de la imagen simplificada, obteniendo lo que se conoce como <<plantilla>> de la huella. En este proceso se realiza un conjunto de determinaciones: 1) si un píxel pertenece o no a una cresta 2) si es así, si es una bifurcación, comienzo o final de cresta, se obtiene un grupo de puntos candidatos a minutiaes. Posterior a esto, se procede a borrar todos los puntos en el borde de la zona de interés.

Debido a que la densidad de minutiaes por unidad de área no puede exceder un cierto valor, todos los conjuntos de puntos candidatos cuya densidad exceda este valor, son sustituidos por una simple minutiae localizada en el centro del conjunto, conformando el patrón de minutiaes final. La plantilla contendrá entre 70 y 80 minutiaes.

Figura 25. Patrón de minutiaes

2.2.3.2 Algoritmo de comparación de minutiaes.

En esta etapa se integra un proceso llamado de “emparejamiento” con la finalidad de determinar si dos huellas son del mismo dedo o no. Para llevar a cabo este proceso, se utilizan 2 características de las huellas: a) finales y b) bifurcaciones de las crestas (minutiaes). En la *Figura 26* se observan las minutiaes de una <<plantilla>> Vs. minutiaes de una huella digital “viva”, y su correlación entre éstas <<proceso de comparación>>.

Para cada minutiae detectada se almacenan los siguientes parámetros:

- Coordenadas x, y de la minutiae.
- Orientación definida como la orientación local de la cresta asociada.
- Tipo de minutiae, pudiendo ser terminación o bifurcación.
- Cresta asociada.

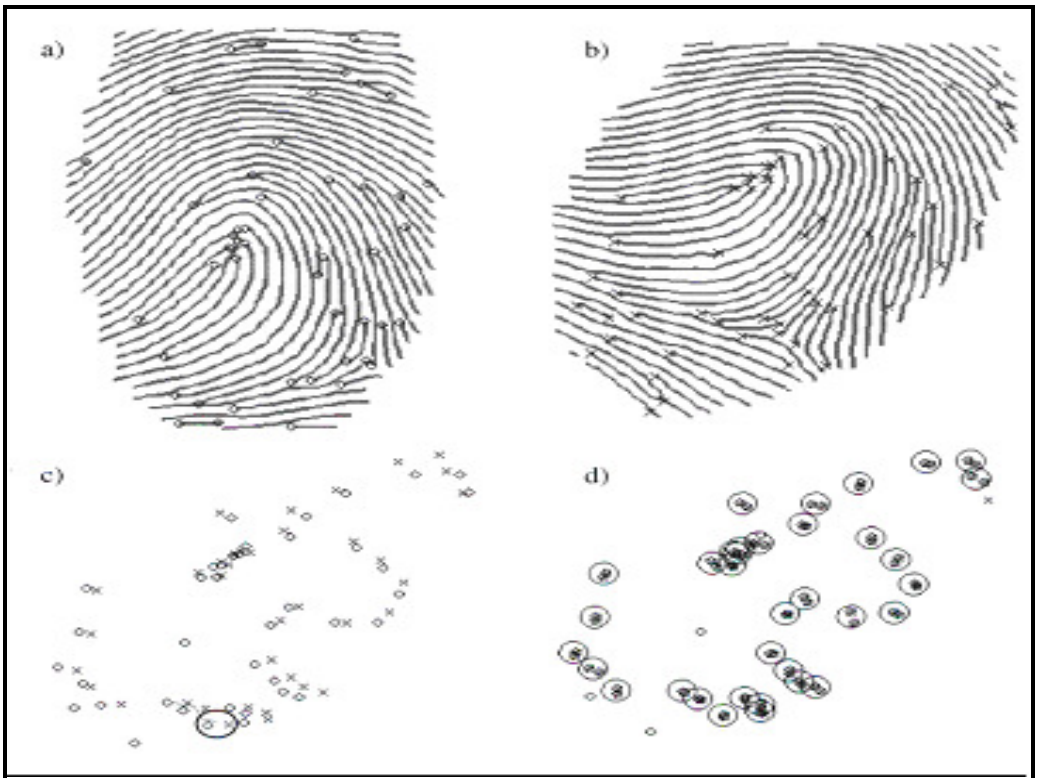


Figura 26. a) y b) Minutiaes extraídas de una plantilla (template) y una huella digital “viva” de entrada, respectivamente. c) y d) Proceso de correlación de minutiaes (comparación).
* Fuente tomada del libro Handbook of Fingerprint Recognition. Davide Maltoni 2003 Springer- Verlag New Cork. 2003 pág. 149

Como parte del proceso de comparación de minutiaes se realizan primeramente una ***alineación del conjunto de minutiaes***, para posteriormente llevar a cabo su ***comparativo,*** utilizando las coordenadas polares de éstas.

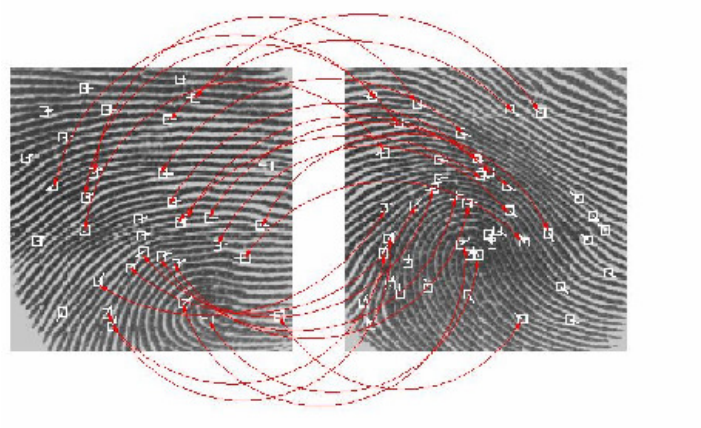


Figura 27. Proceso de comparación entre plantillas.

El proceso de comparación consiste en comprobar si el conjunto de minutiaes de una huella coincide con el de otra. Es decir, consiste en encontrar el grado de similitud entre dos vectores de características cuyas componentes representan a las minutiaes de cada huella. *Ver Figura 27*

Las principales dificultades en el proceso de comparación son:

1. En una imagen de buena calidad, hay alrededor de 70 a 80 minutiaes en promedio, cantidad que contrasta con las presentes en una imagen latente o parcial cuyo valor promedio es del orden de 20 a 30.
2. Hay traslaciones, rotaciones y deformaciones no lineales de las imágenes que se heredan a las minutiaes.
3. Aparecen minutiaes falsas, mientras otras verídicas desaparecen.
4. La base de datos puede ser muy grande.
5. No existe un método de comparación que entregue una coincidencia exacta entre las características de la imagen de entrada y las pertenecientes a la base de datos.

A la fecha, las técnicas propuestas que han obtenido mayor éxito en la labor de comparación <<matching>> se han basado en una comparación de índole geométrico de los vectores de características.

Como puede apreciarse, los procesos de extracción y comparación son pasos verdaderamente importantes del proceso.

2.3 BENEFICIOS, DESVENTAJAS Y TENDENCIAS DE LA TECNOLOGÍA BIOMÉTRICA.

"Si bien es cierto que la tecnología biométrica al igual que todo sistema de seguridad presenta desventajas, pros y contras, y para todas ellas se tienen soluciones; lo relevante del proceso es que a través de esta tecnología estamos dando un paso gigante para lograr el reconocimiento preciso de los individuos, y con ello, cubriendo uno de los principales huecos de seguridad en los sistemas. Estamos teniendo un mayor acercamiento al punto límite de la seguridad al 100%".

Analizados los principios primordiales de la tecnología biométrica por huella digital aplicada al proceso de autenticación de usuarios, resulta interesante conocer sus principales ventajas y desventajas; el saber porqué este tipo de tecnología no había sido utilizada de forma masiva sino hasta la última década de nuestros días en que la diversidad de áreas y empresas preocupadas por contar con un control estricto de autenticación de usuarios, la han adoptado con fines de llevar a cabo el proceso de validación de identidades, de forma más segura y eficiente.

Resulta que aunque la tecnología biométrica trae grandes beneficios, como todo mecanismo, también presenta peculiaridades específicas que le hacen tener desventajas en relación a ciertos factores; debido a lo cuál en definitiva su uso no garantiza tener un sistema 100% seguro <<recordemos que no existe ni existirá seguridad absoluta>>

Los métodos de autenticación biométrica entonces, deben ser considerados como una herramienta más dentro del repertorio de la seguridad, pues si bien trae grandes ventajas, ésta viene a complementar a otros métodos de autenticación, pero en ningún sentido por sí sola, a resolver todos los problemas y necesidades de validación de identidades de usuario y seguridad.

2.3.1 Beneficios

A manera de resumen, a continuación se citan las algunas de las principales ventajas de hacer uso de este tipo de tecnología:

- Elimina el uso del password vulnerable a olvido, divulgación, ingeniería social, robo, préstamo, ataques por fuerza bruta, etc.
- Dado que la huella digital es única, intransferible, no se desconfigura, no es vulnerable a robo, olvido y difícilmente es falsificada, la tecnología permite la identificación del individuo de forma segura.
- Automatiza el proceso de acceso a sistemas al no tener que teclear un password, y solo ingresar su huella.

- El proceso de autenticación es más amigable para el usuario al no tener que recordar passwords o números de identificación complejos.
- Reducción de hasta un 80% de las llamadas por problemas de uso y cambios de passwords[39], dando como resultado un ahorro en cuanto a recursos humanos y así mismo, elevación de la productividad.
- La combinación de un identificador y la exposición de la huella, hacen de la seguridad algo irrompible. (sistemas que combinan 2 ó más factores de autenticación de manera simultánea, elevando el nivel de seguridad en los sistemas). Ver detalles de sistemas multibiométricos o multifactor en (www.bionetrix.com, www.bioapi.org, www.saflink.com, www.identix.com).
- Facilidad de uso.
- Alto nivel de confiabilidad.
- Incremento del nivel de seguridad en los sistemas.
- La tasa de falsos rechazos y falsas aceptaciones es configurable en los dispositivos lectores biométricos.
- El patrón de la huella es más difícil de falsificar que una simple contraseña o tarjeta magnética.
- Elimina el problema de suplantación de identidad.
- Se le puede responsabilizar de manera directa al usuario, de toda acción que realice por medio con su huella en el sistema.
- Algunos dispositivos biométricos, tienen la facilidad de detectar mediante infrarrojos, el espesor de las capas subcutáneas para determinar si el dedo está vivo. Algunos más, tienen la capacidad de medir la temperatura, presión, pulso, conductividad, etc.
- Elimina las frustraciones de los usuarios al no poder ingresar a los sistemas aun siendo usuarios legítimos. Lo anterior dependerá del umbral llamado ***Tasa de Error Igual (TEI),*** que sea definido. Lo anterior es tratado en el subcapítulo ***"2.1. Proceso de autenticación mediante huella digital".***
- Debido a que la tecnología por huella digital es de las más maduras en el campo biométrico, se tiene la capacidad de elegir entre diversas compañías proveedoras y variedad de dispositivos con capacidades y características, especificas.

[39] Datos reportados por Gartner en el año del 2002 en Estados Unidos.

2.3.2 Desventajas

La tecnología biométrica al igual que cualquier otro tipo de tecnología ó método aplicada en la autenticación de usuarios, presenta ciertas desventajas.

Dentro de la lista de desventajas que ésta presenta, se encuentran principalmente tres aspectos: es el costo, mantenimiento y uso de estándares abiertos[40], donde este último es importante para poder llevar a cabo la integración de la tecnología biométrica hacia diferentes ambientes y aplicaciones, independientemente del proveedor, la tecnología y/o plataforma de operación; y así mismo, con la finalidad de asegurar la interoperabilidad e intercambio de datos entre aplicaciones de tipo biométrico.

Actualmente, existen varios grupos relacionados con la industria biométrica y organizaciones enfocadas a la creación de estándares biométricos ***[RFC4p.145]***

Dentro de las actividades de estandarización se encuentran: definición de formatos de datos biométricos (p.e: templates, formatos de imágenes, etc), técnicas para la protección de templates, formatos de archivos comunes, evaluación del performance, técnicas para mantener la confidencialidad e integridad de los datos, interfaces de programación de aplicaciones <<API's>>, perfiles de aplicación y metodologías para la imposición de puntos estándar a cumplirse, entre otros.

Algunos de los organismos principales enfocados en el establecimiento y definición de estándares biométricos se listan en la *Tabla 4*.

A continuación se detallan algunos de ellos:

- **Consorcio BioAPI**: Es un grupo fundado en 1998, conformado por 90 miembros con representación internacional <<Norte América 96%, Europa 25% y Asia 10%>> que tienen un interés común en promover el crecimiento del mercado biométrico. La especificación BioAPI define un estándar de sistema abierto API, que permite a las aplicaciones comunicarse con un amplio rango de tecnologías biométricas de manera común. Como una especificación de sistemas abiertos, BioAPI logra la integración e interoperabilidad de un amplio universo de ambientes y plataformas. Actualmente ***BioAPI*** (www.bioapi.org; Interfaz de programación de aplicaciones biométricas) es uno de los estándares biométricos mayormente

[40] Refiérase a la existencia de demasiados sistemas propietarios. Microsoft, uno de los fundadores del BioAPI, estándar propuesto en 1995 por el Biometric Consortium patrocinado por el gobierno de E.U., salió del grupo de 60 empresas y agencias para crear su propia tecnología. El Departamento de Defensa cuenta con una organización y un laboratorio de biométrica, donde se prueba la utilidad de los más de 600 productos existentes en el mercado. El Departamento de Energía desarrolla un escáner holográfico que analizará, a través de ondas de radio y en tres dimensiones, a los pasajeros para comprobar si esconden armas.

aceptado y generalizado, desarrollado en conjunción con otros estándares como el estándar X.9.84.
El BioAPI soporta un amplio rango de tecnologías biométricas, incluyendo huella digital, verificación del habla, reconocimiento de voz, scanneo de iris, firma dinámica y geometría de la mano. Actualmente, este tipo de estándar es compatible con estándares como: Common Biometric Exchange File Format (CBEFF), NIST 6529 que define la estructura de datos biométricos para asegurar a las compañías biométricas y clientes potenciales, que diferentes dispositivos biométricos y aplicaciones puedan intercambiar eficientemente información; y el ANSI X9.84 estándar para la gestión de biométricos y seguridad de servicios financieros.
El Instituto ANSI (American National Standards Institute) aprobó al BioAPI como un estándar ANSI oficial en Febrero del 2002, estándar americano.

- **ANSI X9F4** Aplicaciones criptográficas: Es el grupo de trabajo que desarrolló el ***estándar ANSI X9.84*** (Administración de la información biométrica y seguridad- www.x9.org, www.ansi.org), el cuál es uno de varios grupos de trabajo operando sobre el subcomité de X9F de datos y seguridad de la información. El estándar define los requerimientos mínimos para el manejo, distribución y procesamiento de la información biométrica promoviendo el uso de firma digital y encripción para proveer integridad y privacidad de los datos biométricos, teniendo su principal uso en la industria financiera, etc. Dentro de los puntos de seguridad que contempla se encuentra: a) Seguridad Física del HW utilizado en el proceso biométrico b) La manipulación de los datos biométricos y su procesamiento c) Uso de la tecnología biométrica para la verificación/identificación de clientes y empleados d) Aplicación de la tecnología biométrica en el control de acceso físico y lógico e) encripción de los datos biométricos f) técnicas para la transmisión y almacenamiento de datos biométricos.

- **IBIA** (Internacional Biometric Industry Association- www.ibia.org/formats.htm): Es una asociación fundada en septiembre de 1998 en Washington, DC, para la mejora, defensa, y apoyo de interés internacional colectivo de la industria biométrica. IBIA es dirigida por y para desarrolladores de aplicaciones biométricas, fabricantes e integradores. IBIA es el registro oficial para identificadores de objeto X9.84 e identificadores de BioAPI.

- **X.509** Estándar que especifica que las plantillas de minutiaes se almacenen en un certificado X.509 como un atributo de información dentro de un número fijo de bytes. Por definición, las plantillas basadas en patrones no pueden cumplir con este estándar. Por el contrario, la técnica basada en minutiaes, si.

- **Comité ANSI B10** para licencias de manejo e identificación: ANSI B10.8 Licencia de manejo/ Estándar de tarjeta de identificación (card ID- incluye

huella digital basado en minutiaes), acreditado por el comité de standards ANSI's en el año 2000.

El Comité Nacional para el estándar de Tecnología de Información (NCITS) es un comité dedicado a las tarjetas de identificación y todo lo relacionado al conocimiento de dispositivos como B10.

- **JCT1** (Joint Technology Commite) **SC17** (Subcomité 17) Tarjetas de identificación y dispositivos relacionados: Es la unión de ISSO y la organización IEC (International Electrotechnical Commission), enfocadas al ámbito de tarjetas de circuitos integrados, tarjetas de transacciones financieras, tarjetas de memoria óptica, licencia de manejo de vehículos y documentos relacionados. SC17 así mismo, ha iniciado un nuevo trabajo para el establecimiento de datos y estructura de archivos para el almacenamiento de datos biométricos en smart cards.

  Por otro lado, SC37 (Subcomité 37) se encuentra enfocado a la definición de estándares para la medición del performance de los sistemas biométricos, protección de templates biométricos y formatos de datos.

- **ANSI** (American National Standards Institute / **NIST** (Nacional Institute for Standard and Tecnology) /**ITL** (Information Tecnology Laboratory) Common Biometric Exchange File Format (***CBEFF-*** www.nist.gov/cbeff): Describe los elementos necesarios para soportar tecnologías biométricas de modo común, independientemente de la aplicación, del dominio y uso (p.e: dispositivos móviles, smart cards, protección de datos digitales, almacenamiento de datos biométricos, etc). El estándar especifica un formato común a ser utilizado para el intercambio patrones de huellas digitales, rostro, marcas, cicatrices, tatuajes o datos de identificación de diferentes fabricantes. CBEFF facilita el intercambio de datos biométricos entre diferentes componentes del sistema o entre diferentes aplicaciones, asegurando su interoperabilidad, compatibilidad e integración entre SW y HW.

  ANSI (American National Standards Institute) es el Instituto Administrador y Coordinador del sistema voluntario de estandarización del sector privado de Estados Unidos. El Instituto representa los intereses de sus casi 1.000 miembros entre compañías, organizaciones, fabricantes, agencias estatales y miembros institucionales e internacionales, a través de su oficina en Nueva York y de su sede central en Washington, D.C.

  Es el representante oficial de U.S. para el IAF (International Accreditation Forum), ISO (International Organization for Standardization), el comité Nacional de U.S., el IEC (International Electrotechnical Commission). Es además, miembro del PASC (Pacific Area Standards Congress) y el COPANT (Pan American Standards Commission).

- **Consorcio biométrico** (www.biometricfoundation.org): Sirve como punto de contacto del gobierno del E.U. para la investigación, desarrollo, prueba, evaluación y aplicación de la tecnología biométrica para la identificación/verificación de personal. Actualmente co-administrado por 2 agencias del Gobierno de los E.U: NIST y NSA (Nacional Security Agency).

- **Comité técnico 68 ISSO**, **Subcomité 2 (SC2)**: Enfocado a la administración de la seguridad y operaciones bancarias en general, incluyendo códigos, procedimientos y estándares de seguridad relacionados.

- **AAMVA** Fingerprint Minutiae Format /Nacional Estándar for the Driver License/Identification Card: Estándar que define los requerimientos mínimos para la presentación de los datos de identificación humana, incluyendo el formato, los datos de identificación en una cinta magnética, código de barras, tarjetas de circuitos integrados, memorias ópticas e imágenes digitales. También especifica un formato de minutiaes de las huellas digitales aplicado en licencias de manejo.

- Las mejores prácticas desarrolladas por **Common Criteria**[41] (www.commoncriteria.org). Enfocado a la evaluación de la seguridad, PP (Protection Profiles).

  El Common Criteria es un estándar internacionalmente reconocido y fundamentado en las normas ISO/IEC 15408:2005 e ISO/IEC 18405:2005.8.
  Para evaluar la seguridad de un producto y hacerlo merecedor de este certificado, se deben comprobar numerosos parámetros relacionados con la seguridad y propuestos previamente por el fabricante. Estos parámetros han sido consensuados y aceptados por 22 países de todo el mundo, hasta el punto de que algunos gobiernos (como el de Estados Unidos de América) exigen esta certificación para poder utilizar sus sistemas. El visto bueno de la Common Criteria Organtization permite que el producto sea usado en sistemas críticos de los gobiernos e instituciones de todo el mundo, ya sea pertenecientes a bancos, agencias secretas de inteligencia o el mismísimo Pentágono.
  Common Criteria exige a los fabricantes de los productos remitir una documentación exhaustiva sobre la seguridad de los mismos. Ésta es examinada y sometida a procesos de verificación por parte de laboratorios independientes para evaluar el nivel de adaptación a la norma. El aspirante a la certificación puede elegir la profundidad de estudio del sistema para que sea evaluado.

[41] Detalle obtenido del boletín “una-al-día” emitido por Hispasec el 28 de Enero del 2006.

Por su parte, Common Criteria otorga hasta siete niveles de seguridad EAL, aunque los requerimientos de los niveles EAL5 a EAL7 se orientan a productos con objetivos muy especializados.

Organization	Standard	Status
NIST/BC Working group/NSA	CBEFF – NISTIR 6529 Common Biometric Exchange File Format (CBEFF)	Publisher Jan 2001 as NISTIR 6529 Being augmented by the NIST/BC Biometric WG- INCITS Fast Track candidate.
BioAPI Consortium	BioAPI ANSI/INCITS 358 Applications Programming Interface	Released march 2001 Fast Track as ANSI/INCITS Stand
ANSI X9.F4	ANSI/ X9 X9.84 Financial Applications	Approved (ANSI) February 2001
Open Group	Human Recognition Services (HRS) Module of CDSA	Update to be consistent with BioAPI
ISO/IEC SC17 WG4	ISO/IEC SC17 7816-11 “Personal Verification Through Biometric Methods”.	Committee Draft NIST/BC WG Recommends CBEFF compliance
AAMVA	Nat Stand for Driver Lic/ID Card- Includes fingerprint Minutiae	AAMVA DL/ID 2000 Approved 2000
INCITS B10	INCITS 327	Draft based on AAAMVA DL/ID 2000
NIST	Data format for finger/facial/SMT	ANSI/NIST- ITL-2000 Approved 2000
DOD-BMO, BEMWG	Common criteria- Security Evaluations.	
U.K. BWG (Biometric Evaluation Methodology Working Group), FVC2002, FVRT2002, IBG	Performance Evaluation • U.K. Biometrics Working Group - “ Best Practices in Testings and Reporting Performance”. • FVC2002 - Fingerprint Algorithm Competition Standard Databases • FVRT2002 - Facial Recognition Competition - NIST • IBG - Comparative Testing	EAL Level 2 – Security Target (Nov. 1999- May 2001). Multi-National Representation: Canada, U.K., Germany, U.S., Finland, Italy.

Tabla 4. Principales estándares biométricos.
* Fuente tomada del trabajo final de Fernando Podio Brief (www.itl.nist.gov).

2.3.3 TEKS, SDKs, RDKs, EDKs

Como parte del esfuerzo de estandarización, muchas compañías proveedoras de dispositivos biométricos, ofrecen kits dirigidos a desarrolladores e integradores que les permiten realizar adaptaciones de aplicaciones biométricas de manera fácil y rápida, para que puedan operar en diferentes ambientes y plataformas. Algunos de estos kits por mencionar algunos son: TEKs (Technology Evaluation Kits), SDKs (Software Development Kits), RDKs (Reference Design Kits) y EDKs (Embedded Developer's Kits) **[RFC5p.280]**

Específicamente, los SDKs son kernels de programación que permiten a los programadores realizar desarrollos de aplicaciones para plataformas propietarias. Regularmente incluyen los API's, herramientas de programación y documentación; y dependiendo del proveedor, también pueden incluir los DLLs, código objeto, algoritmos, drivers, guías de desarrollo y herramientas/utilerías/debuggers.

Lo anterior representa una gran ayuda, sin embargo no lo es del todo, ya que la gran mayoría de los fabricantes manejan kit/SDK específicos para el tipo y modelo de dispositivo biométrico en particular, dificultando el trabajo de integración con otras aplicaciones o ambientes, dado que las API's son específicas para un grupo de dispositivos biométricos en específico.

Haciendo referencia al ***dispositivo biométrico de huella digital UareU 2000*** utilizado en el presente trabajo, del fabricante Digital Persona; con fines de realizar la integración del lector de huella digital al ambiente Intranet para llevar a cabo el control de los accesos de usuario vía autenticación de huella digital, se adquirió el ***SDK Standard*** de ***Verifinger 4.2. para Windows*** ***[RFC8].***

Para este modelo de dispositivo biométrico en particular, dependiendo de las necesidades del desarrollo que se requiera realizar, existen además, los siguientes tipos de SDKs disponibles en el mercado:

- **Verifinger 4.2 SDK Light**, dirigido a los desarrolladores que han obtenido una interfaz de scanner. Incluye una licencia para la de DLL Verifinger 4.2, VeriFinger DLL aplicaciones de ejemplo (con su código fuente) y documentación sobre el software.

- **Verifinger 4.2 SDK Standard**, dirigido a la mayoría de los desarrolladores de sistemas biométricos. Incluye todas las características del SDK Light e interfaces adicionales para los scanners: Digital Persona U.are.U, Ethenticator, STMicroelectronics TCRU1C, Biometrika FX 2000, AuthenTec AF-S2 y AES4000.

- **Verifinger 4.2 SDK Extendido,** dirigido a los desarrolladores que desean iniciar rápidamente un desarrollo que abarque un sistema biométrico utilizado

por medio de una red. Incluye todas las características del SDK Standard, también incluye 3 licencias para la DLLs de Verifinger, componentes ActiveX para el desarrollo de aplicaciones cliente/servidor y aplicaciones de ejemplo con su código fuente.

El paquete de distribución del SDK Standard de Verifinger por ejemplo, incluye:

- Una licencia para la DLL de Verifinger
- Interfaces para la adquisición de una imagen por medio de un archivo, para los scanners UareU, Ethenticator, DFR 2090, Verifier 300, FX 2000, TouchChip; y para los sensores EntréPad y FingerLoc.
- Códigos fuente de aplicaciones de ejemplo de uso de la DLL. Estos códigos fuente vienen en C/C++, Java, Visual Basic, Visual Basic .Net, Visual Basic para aplicaciones y Delphi 6.
- Motor de identificación de huella dactilares Verifinger 4.2
- Documentación

Este SDK contiene las interfaces para un grupo grande de scanners, lo cuál permite al desarrollador, obtener las imágenes de cualquier scanner sin la necesidad de ningún software adicional.

Requerimientos de Hardware para el SDK Standard de VeriFinger:

- PC Pentium con un procesador de 200MHz o mejor
- MS Windows 9x/ME/NT/2000/XP
- Interfaz del scanner, donde los usuarios pueden utilizar la interfaz incluida en el SDK Standard de VeriFinger u obtener la misma del fabricante del scanner.

El costo apróx. del VeriFinger 4.2 SDK Standard es de $399.00 dólares.

2.3.4 Tendencias

La tecnología biométrica por huella digital ha experimentado en los últimos años un importante auge dado su potencial aplicado en las áreas de reconocimiento y verificación de identidades de usuario para el control de accesos a sistemas o áreas criticas; representando durante la última década tras años de investigación, ser una de las tecnologías más prometedoras que ha logrado incursionar en variedad de sectores, pasando de ser una sorprendente tecnología de ciencia-ficción, a ser de los dispositivos más demandados en los últimos tiempos.

Hoy en día, los biométricos tienen un lugar importante en una sorprendente variedad de aplicaciones, más allá de controlar el acceso, inmigración, control de asistencia, asilos, guarderías y centros de atención médica, programas de beneficencia y puntos de venta son solo unas cuantas de las aplicaciones donde se utilizan biométricos.

De acuerdo a estadísticas de uso consultadas, el uso de la huella digital en el proceso de autenticación, representa una de las características mayormente utilizadas por los métodos de autenticación de tipo biométrico, destacando por su facilidad de uso, precisión, mayor seguridad, eficiencia, confiabilidad y no tan alto costo en relación al universo de biométricos. Lo anterior se puede observar en la *Tabla 5*

Biometric Identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Retina	H	H	M	L	H	L	L
Signatura	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Tabla 5. Comparativo de tecnologías biométricas.
H= Alto (High), L= Bajo (Low), M= Medio (Medium).
* Fuente tomada del libro Handbook of Fingerprint Recognition.
Davide Maltoni 2003 Springer- Verlag New Cork. 2003 pág. 12

Un reporte emitido por el Grupo Internacional Biometric en el año 2002, indicó que los sistemas biométricos basados en huella digital encabezan el mercado de la Biometría, acaparando mas del 50% del mercado, secundado por el reconocimiento basado en el rostro con el 12.4%. Ver *Figura 28* ***[RFC3p.12]***

Aunque la tecnología biométrica pudiera parecer un mercado aun muy virgen, la realidad es que existe una larga lista de empresas y sectores que han acudido a su uso, obteniendo resultados satisfactorios. Dentro de ellos se encuentran:

Master Card
IBM y American Express
Teléfonos de México S. A de C.V.
Radio Móvil Dipsa (Telcel)
Grupo – Elektra
Banco Azteca
TV Azteca
Universidad CNCI
El Palacio de Hierro
Reader's Digest, México
Pemex
Coca-Cola Centroamérica
Inbursa
Griaule, Brasil
Departamento de Seguridad Interna de E.U.
Oficina Federal de Investigaciones (FBI)
Agencia Central de Inteligencia (CIA)
Etc…

De acuerdo a un reporte de la Internacional Biometric Group, se estima que el mercado de la Biometría se vea incrementado considerablemente, consolidándose especialmente en los sectores de acceso a PC's y el mercado de e-commerce.

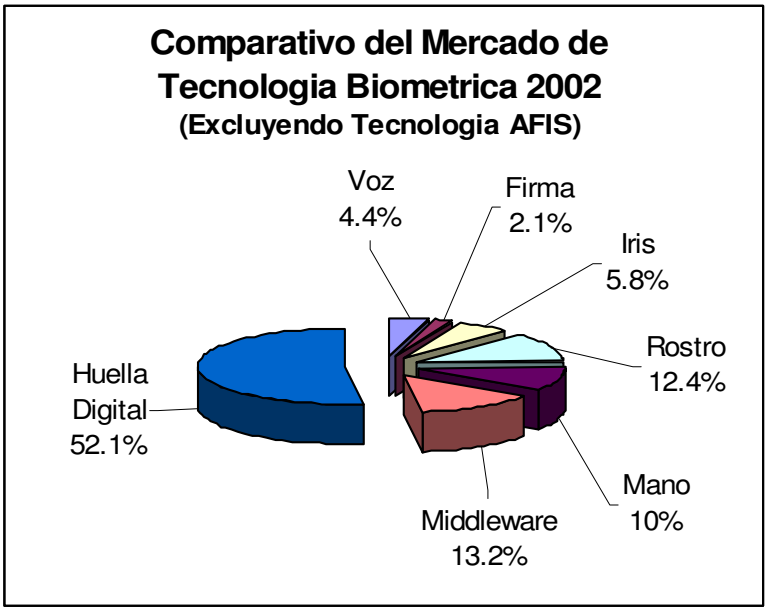


Figura 28. Comparativo de uso de las diferentes tecnologías biométricas.
Se puede apreciar como desde el 2002 la huella digital encabezaba la lista de las tecnologías mayormente utilizadas, lidereando el mercado biométrico hasta nuestros días.
* Fuente tomada del libro Implementing biometric security John Chirillo- Scout Blaul Edit. Wiley. Pág. 278

En la *Figura 29* se muestra el comportamiento del mercado biométrico de huella digital esperado para los próximos años[42]

Aunado a lo anterior, todo apunta a que cada vez más empresas dedicadas a la manufactura y venta de dispositivos biométricos se encuentren peleando en una guerra por imponer sus tecnologías e impulsando su uso no solo en áreas judiciales o forenses como era en un principio, sino incursionando en áreas de salud, informáticas, bancarias, etc.

Así mismo, el número de tecnologías y fabricantes se extenderá aún más.

Se piensa que científicos de diferentes partes del mundo continuarán trabajando en desarrollar algoritmos más eficientes, rápidos y seguros; así como mecanismos tecnológicos menos costosos capaces de reconocer las características fisiológicas que identifiquen a los individuos de manera única.

[42] Reporte presentado por la Internacional Biometric Group, referente al nivel de crecimiento estimado del mercado biométrico de huella digital y el elevado incremento de publicaciones científicas emitidas sobre el tema. **[RFC3p.49]**

De igual manera, algunas compañías proveedoras buscarán explorar nuevas tecnologías con nuevos atributos fisiológicos para identificación, mientras que otras se enfocarán a mejorar las tecnologías actualmente en uso.

El reconocimiento facial por ejemplo, ha recibido una buena cantidad de atención en estos últimos años. La gente identifica fácilmente a otras personas por su cara, pero automatizar esta tarea no es nada sencillo. Mucho del trabajo en esta área se ha dedicado a capturar la imagen facial. Una compañía está experimentando con una técnica única, el examinar el patrón térmico creado por los vasos sanguíneos en el rostro.

Otra tecnología nueva examina el patrón de las venas y arterias en la palma de la mano.

Respecto a los sistemas existentes, se están desarrollando nuevas tecnologías. Por ejemplo, como se mencionó anteriormente, los sensores para capturar huellas digitales utilizando tecnología de ultrasonido representan la vanguardia en el mercado biométrico de huella digital. Esta nueva tecnología permite minimizar problemas de polvo y ruido en la imagen que pueden confundir a los lectores ópticos actuales.

También se está experimentando con hologramas para almacenar las imágenes de las huellas digitales, lo que permite un almacenamiento de las huellas más compacto y comparaciones ópticas más rápidas.

Por otro lado, los parámetros de <<falsos rechazos>> y <<falsas aceptaciones>>, tomarán mayor relevancia.

Si bien en un principio cuando los biométricos hicieron su aparición en aplicaciones de alta seguridad su consideración principal era mantener afuera a los “impostores” y se prestó poca atención a dejar entrar a los “usuarios legítimos”; a medida que los biométricos se han integrado a aplicaciones comerciales, la tasa de falso rechazo ha venido tomando importancia.

Lo anterior es relevante, pues aunque muchos solo vean como requerimiento manejar una tasa baja de falsa aceptación en sus sistemas, para impulsar el uso extendido de los biométricos a nivel comercial es necesario contemplar ambas tasas procurando en lo posible, obtener un balance entre ellas hasta alcanzar un nivel de confiabilidad aceptable.

Por otra parte, los factores que se esperan abrirán aún más la puerta al mercado biométrico, es que en los próximos años con los avances de la tecnología, el costo de los dispositivos biométricos se vea decrementado, permitiendo llegar a más sectores y a mayor número de individuos hasta llegar a ser una tecnología de uso común. Así mismo, el uso extensivo de la Criptografía aplicada a la tecnología

biométrica con fines de mantener la privacidad de los patrones biométricos, identificación de huellas falsificadas, implementación de seguridad punto a punto mediante mecanismos de encripción, etc.

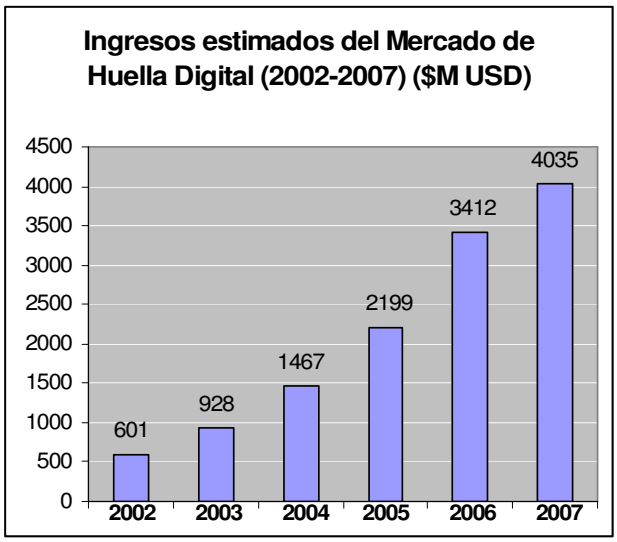


Figura 29. Crecimiento estimado del mercado biométrico.
Reporte del mercado biométrico (Internacional Biometric Group ©) estima que las ganancias en el mercado por huella digital crecerá rápidamente; mayormente en lo que respecta a las áreas de e-commerce, acceso a redes y PC's.
* Fuente tomada del libro Handbook of Fingerprint Recognition.
Davide Maltoni 2003 Springer- Verlag New York. 2003. pág. 49

Adicional a lo anterior, el estado actual de la investigación en el campo de la autenticación biométrica, augura un futuro bastante prometedor a mediano plazo en el que ésta tomará un papel relevante especialmente aportando grandes ventajas al área de control de acceso y autenticación. Muy probablemente la generalización de hardware de autenticación biométrica en los equipos informáticos o la utilización de autenticación biométrica en los cajeros automáticos son fenómenos que no tardarán en ser una realidad común en nuestra vida cotidiana.

Lo cierto de esto, es que finalmente aunque estas tecnologías se ven muy prometedoras, su utilidad la determinará lo hábil que sea cada una para ofrecer soluciones de buen desempeño y bajo costo que cumplan con las necesidades del mercado. Donde de igual manera, aquéllas empresas que opten por estas soluciones desde este momento, estarán en una clara situación de ventaja competitiva con respecto a las que se limiten a actuar como meros espectadores.

En este capítulo el lector ha conocido ya, el detalle del procesamiento que le es realizado a la huella digital hasta obtener una imagen de buena calidad que permita extraer los puntos característicos <<minutiaes>> de manera confiable.

Como se ha mencionado, los algoritmos de extracción y comparación son piezas fundamentales en el proceso, pues estos determinan de manera efectiva el nivel de confiabilidad del sistema biométrico al momento de validar los patrones de huellas y determinar si se trata de una huella válida o no.

Se consideró importante incluir todo este detalle sobre el procesamiento de la huella digital dado que sin él, todo usuario final pensaría que el proceso es verdaderamente sencillo, cuando en realidad no lo es.

El siguiente capítulo está enfocado a tratar a detalle el caso práctico en cada uno de sus fases: Análisis, diseño y desarrollo.

El caso práctico trata sobre el diseño y desarrollo de un sistema para el control de accesos de usuario de una Intranet, integrando un lector biométrico para llevar a cabo la autenticación de cada usuario mediante la lectura de su huella.

CAPÍTULO 3. CASO PRÁCTICO DE DESARROLLO DE UN SISTEMA BIOMÉTRICO

En este capítulo se describe el análisis, diseño y desarrollo de un sistema biométrico que llevará el control de accesos de usuario realizando autenticación biométrica por huella digital, para acceder a la Intranet de una empresa.

Este capítulo constituye la parte medular del trabajo. En él se detalla el caso práctico seleccionado como parte integral del alcance de este proyecto.

El caso práctico trata sobre el desarrollo de un sistema para controlar los accesos de usuario a una Intranet, integrando un lector biométrico de huella dactilar para realizar la autenticación de cada uno de los usuarios, de manera mayormente confiable.

Con la finalidad de ir analizando paso a paso el caso práctico expuesto, el capítulo se encuentra dividido en los subcapítulos de análisis, diseño y desarrollo.

Como parte del análisis se expone cuál es la situación actual <<necesidades>> y cómo se pretende resolver <<solución propuesta>>. Es decir, se detalla cuál es la arquitectura actual en que opera la Intranet haciendo uso de autenticación tradicional (uso de passwords), y se plantea la propuesta de una nueva arquitectura de operación integrando autenticación biométrica por huella digital, para llevar un control sobre los accesos de usuario de manera más efectiva.

Dentro del análisis y adentrándose un tanto a la parte de diseño, se definen cuáles son los actores y escenarios involucrados en el desarrollo del sistema; dando lugar a la conformación de los casos de uso. Adicional a esto, se definen las tablas y campos que integran la base de datos, así como el modelo relacional, diccionario de datos y diagramas de secuencia que conforman el sistema.

En el apartado de desarrollo, se listan las diferentes pantallas del sistema que integran lo que es propiamente la interfaz gráfica hacia el usuario, para el acceso, alta, registro y despliegue, de usuarios, Administrador General y Administrador Maestro.

En el ***"Anexo D"*****,** se citan los requerimientos de HW y SW, tanto del servidor como a nivel cliente.

3.1 ANÁLISIS

El caso práctico se encuentra enfocado a resolver la necesidad de mejorar el proceso de control de accesos de usuario a la Intranet de una empresa, con la finalidad de proteger la confidencialidad de cierta información que es publicada y que no debe ser conocida/divulgada por personas no autorizadas, debido a la relevancia que ésta tiene.

El método de autenticación de usuarios que actualmente se utiliza para el acceso a la Intranet, es de tipo tradicional. Cada empleado proporciona su usuario y password, mismos que son enviados en texto plano para ser consultados en la tabla de usuarios de un servidor web, para corroborar que sea un usuario válido y de esa manera, otorgarle el acceso.

Con la finalidad de resolver las vulnerabilidades que sabemos presenta el método tradicional de autenticación de usuarios haciendo uso de passwords (divulgación, olvido, transferencia, etc), la propuesta técnica que se describe, trata sobre el desarrollo de un sistema para controlar los accesos de usuario a una Intranet, integrando un lector biométrico de huella dactilar. Lo anterior, permitirá realizar la autenticación de cada uno de los usuarios de manera mayormente confiable, única e intransferible, a través de la lectura de su huella.

El sistema desarrollado utiliza una arquitectura cliente servidor que se basa en la implementación de estándares abiertos en la parte del servidor, lo que permite una fácil portabilidad. La parte del cliente se encuentra basada en sistema Windows ya que es la plataforma más ampliamente usada en estaciones de trabajo.

La funcionalidad del sistema se encuentra enfocada a cubrir básicamente 2 objetivos:

- Controlar los accesos de usuario a la Intranet de una empresa, realizando autenticación biométrica para validar la identidad de los mismos, por medio de un lector de huella dactilar.

- Permitir administrar las huellas y datos personales de los usuarios registrados, para poder efectuar altas, activaciones, desactivaciones y cambios.

Para cumplir con los objetivos citados, se seleccionó el uso de la tecnología Java en sus modalidades de jsp, applets y javabeans para el desarrollo del sistema. Lo anterior, considerando las ventajas interesantes que esta tecnología presenta en relación a otras como Visual Basic, C++ o C al ser implementadas en un ambiente web.

Entre las ventajas que presenta el lenguaje Java se encuentran:

- **Orientado a objetos*:*** Trabaja con objetos y con interfaces a éstos, soportando encapsulamiento, herencia y polimorfismo.
- **Distribuido:** Sus librerías y herramientas le proporcionan gran libertad para acceder a recursos distribuidos en la red.
- **Estándar abierto de programación*:*** La generación de su código ejecutable es independiente de la arquitectura del equipo sobre el que se ejecuta.
- **Seguro*:*** No accede a zonas restringidas de memoria, tiene un verificador de código para detectar segmentos de éste, que afecten al equipo en el cuál se ejecuta.
- **Multihilo:** Permite procesos simultáneos, lo cuál mejora la ejecución del programa.
- **Multiplataforma*:*** Los programas java pueden ser ejecutados en cualquier plataforma que contenga el Java Runtime Enviroment.

Adicional a esto, se seleccionaron además**:**

- ***Tomcat*** como contenedor de servlets, Jsp's y servidor web.
- ***MySQ*** como Sistema Manejador de Base de Datos
- Verifinger como engine de reconocimiento de huellas, el cuál nos proporciona las API's necesarias para el manejo del lector y procesamiento de la huella.
- ***SSL*** como protocolo para cifrar toda la información que viaje entre cliente-servidor-cliente en el ambiente web. Ver detalles en el subcapítulo "***1.4 SSL (Secure Sockets Layer)"***

La metodología empleada en el análisis y diseño del sistema está basado en el ***Modelo orientado a objetos UML (Unified Modeling Language: Lenguaje Unificado de Construcción de Modelos).[RFC6]***

Las fases comprendidas para lograr el desarrollo del sistema se detallan a continuación.

3.1.1 Análisis de requerimientos.

En esta parte del análisis se exponen las necesidades del usuario y la manera cómo éstas van a ser resueltas.

Función	Descripción
Administrador Maestro	▪ Es el encargado de inicializar el sistema. ▪ Este tipo de usuario accede al sistema, autenticándose con usuario y password. No utiliza autenticación biométrica.

	▪ Es el encargado de dar de alta a uno o varios Administradores Generales (según sean las necesidades que se tengan), modificar sus datos o realizar desactivaciones. Serán los Administradores Generales quienes se encargarán de dar de alta a los usuarios. ▪ No puede modificar, dar de alta o baja a usuarios del sistema. ▪ No puede dar de alta a usuarios normales. Serán los Administradores Generales quienes se encargarán de esa actividad.
Administrador General	▪ Es el encargado de dar de alta a los usuarios normales, y registrar sus huellas. ▪ Podrá realizar altas, activaciones, desativaciones y modificación de datos, de cuentas de usuario. ▪ Este tipo de usuario accede al sistema, mediante su huella dactilar (autenticación biométrica).
Acceso a usuarios (pantalla de acceso)	▪ Debe detectar la presencia de huella en el lector biométrico, para realizar la autenticación del usuario. ▪ Debe permitir el acceso al sitio restringido (Intranet) si la autenticación es exitosa, en caso contrario, deberá indicar el error y regresar a la pantalla de acceso.
Usuario	▪ Este tipo de usuario tendrá la obligación de acudir con el Administrador General del sistema para realizar el mapeo de su huella, y proporcionar los datos para su registro en el sistema. Los datos solicitados son: nombre, apellido paterno, apellido materno, región, ubicación y teléfono. ▪ Para obtener acceso a la Intranet, este usuario deberá ser autenticado biométricamente, posicionando su huella en el lector y obteniendo una autenticación exitosa.

Tabla 6. Requerimientos de usuario

3.1.2 Proceso de negocio.

3.1.2.1 Situación actual (diagrama de arquitectura).

El proceso de autenticación y acceso a la Intranet actualmente se realiza proporcionando usuario y password. Dichos datos son enviados en texto plano y son consultados en la tabla de usuarios del servidor web, para corroborar si se trata de un usuario legítimo o no; dependiendo de ello, se le otorga/niega el acceso a la Intranet de la empresa. Ver *Figura 30*

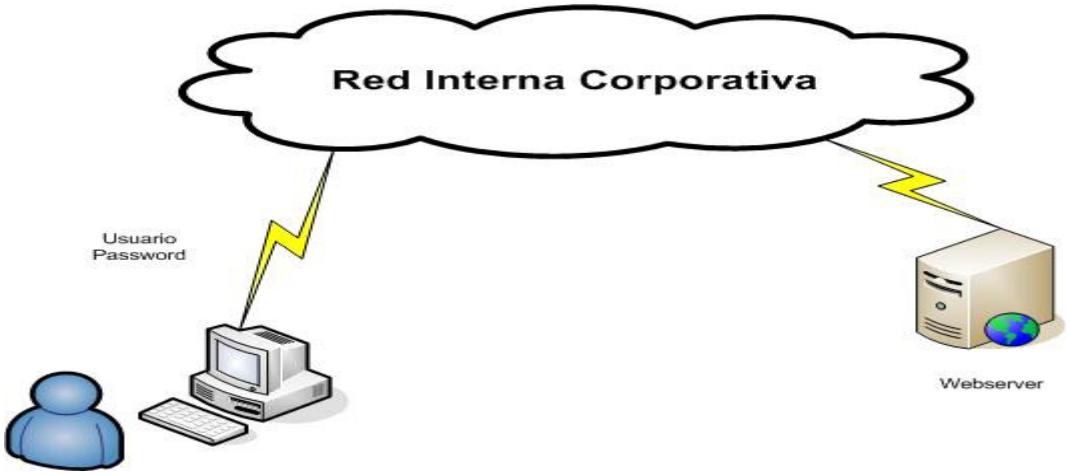


Figura 30. Diagrama de arquitectura actual, utilizando autenticación tradicional mediante el uso de passwords.

3.1.2.2 Solución propuesta (diagrama de arquitectura)

La nueva arquitectura tiene como objetivo, la implantación de un sistema de autenticación biométrico, por medio de un lector de huella digital basado en una arquitectura cliente –servidor.

Los datos de registro de los usuarios (nombre, apellido paterno, apellido materno, región, ubicación física, teléfono, id usuario y tipo de usuario), residirán en una base de datos relacional, al igual que los patrones de sus huellas <<plantillas>>.

El canal de comunicación entre el browser[43] (p.e: Netscape o Mozilla FireFox) y el servidor web, estará encriptado mediante la habilitación del protocolo SSL en el servidor web (https://). Los diagramas donde se puede apreciar lo anterior, se observan en las *Figuras 31 y 32*:

[43] Browser ó navegador, es el término aplicado normalmente a los programas usados para conectarse al servicio www. Algunos ejemplos de browsers son Internet Explorer y Netscape.

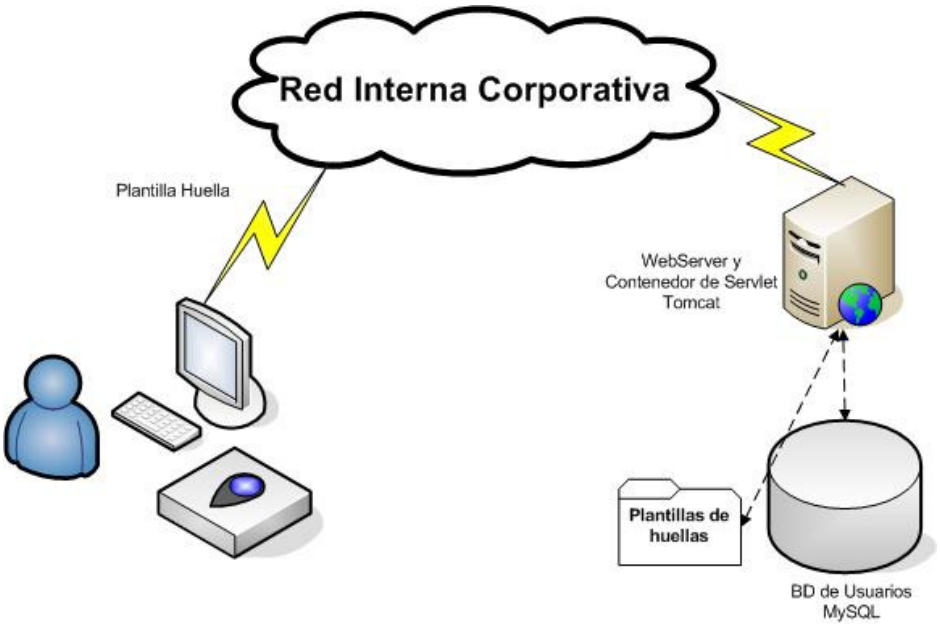


Figura 31. Diagrama de arquitectura propuesto, integrando autenticación biométrica por huella digital.

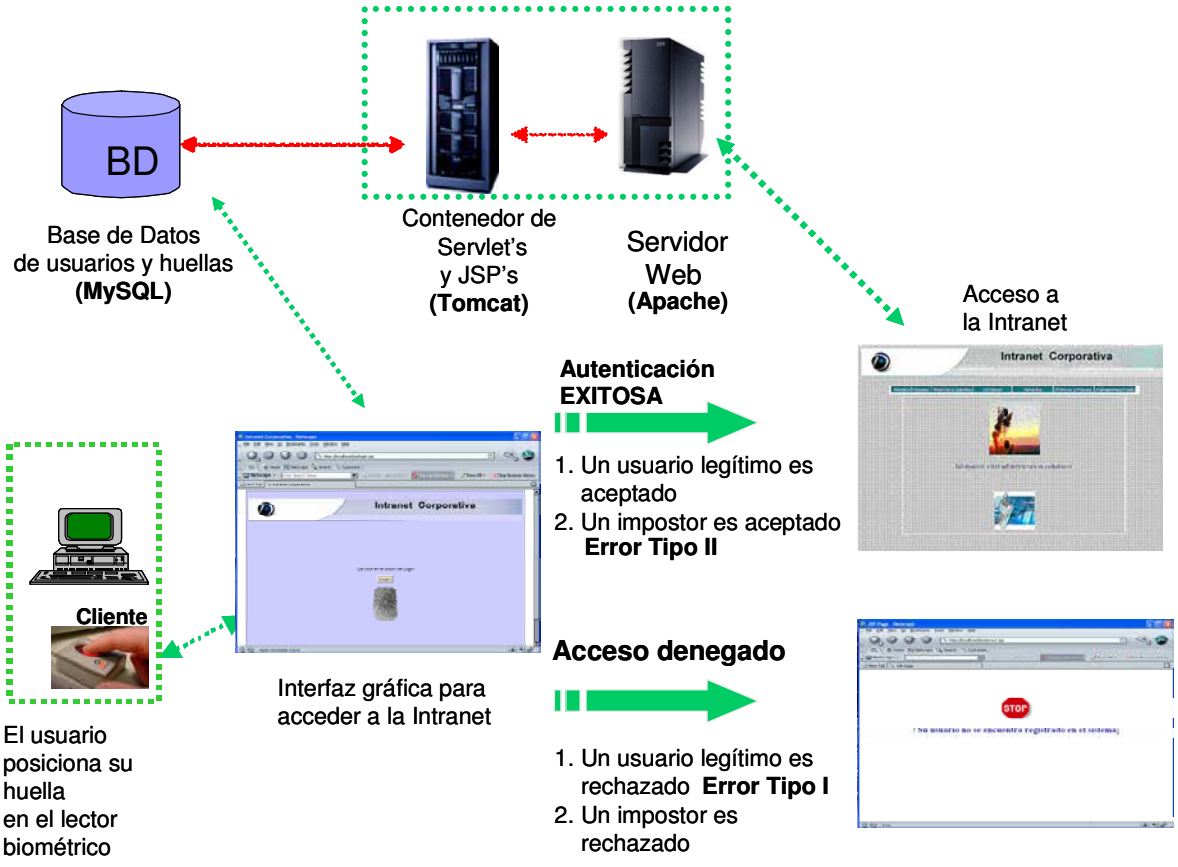


Figura 32. Flujo del proceso, integrando autenticación biométrica por huella digital.

3.1.3 Análisis de casos de uso

Para entender los factores y requerimientos del sistema fue necesario identificar los ***actores***[44] y los escenarios involucrados en el desarrollo del sistema. Estos escenarios dan lugar a los ***casos de uso***[45], los cuáles son la interacción generada por el usuario y el sistema de cómputo.

En el sistema se presentan los siguientes actores y casos de uso.

3.1.3.1 Actores

Existen tres usuarios o actores en el sistema a desarrollar: Administrador Maestro, Administrador General y usuario.

> **Administrador Maestro**: Es el usuario encargado de inicializar el sistema y dar de alta a los Administradores Generales. Es el único usuario que no requiere autenticación biométrica para acceder al sistema. Todas estas operaciones son realizadas a través de un ambiente web.
>
> **Administrador General**: Es el usuario encargado del mantenimiento del sistema, cuya función principal es efectuar modificaciones a la base de datos de usuarios (activaciones, desactivaciones, altas y cambios). Este tipo de usuario requiere autenticarse biométricamente para acceder al sistema. Todas estas operaciones son realizadas a través de un ambiente web.
>
> **Usuario**: Es el individuo, que va hacer uso del sistema para obtener el acceso a la Intranet. Para ello, debe ser registrado de manera previa por el Administrador General del sistema, con la finalidad de que su acceso se encuentre creado y activado.

[44] Actores del sistema son aquéllos usuarios que interactúan con el sistema.
[45] Los casos de uso son aquéllas tareas en las cuáles están involucrados los actores.

3.1.3.2 Casos de uso

3.1.3.2.1 Administrador Maestro

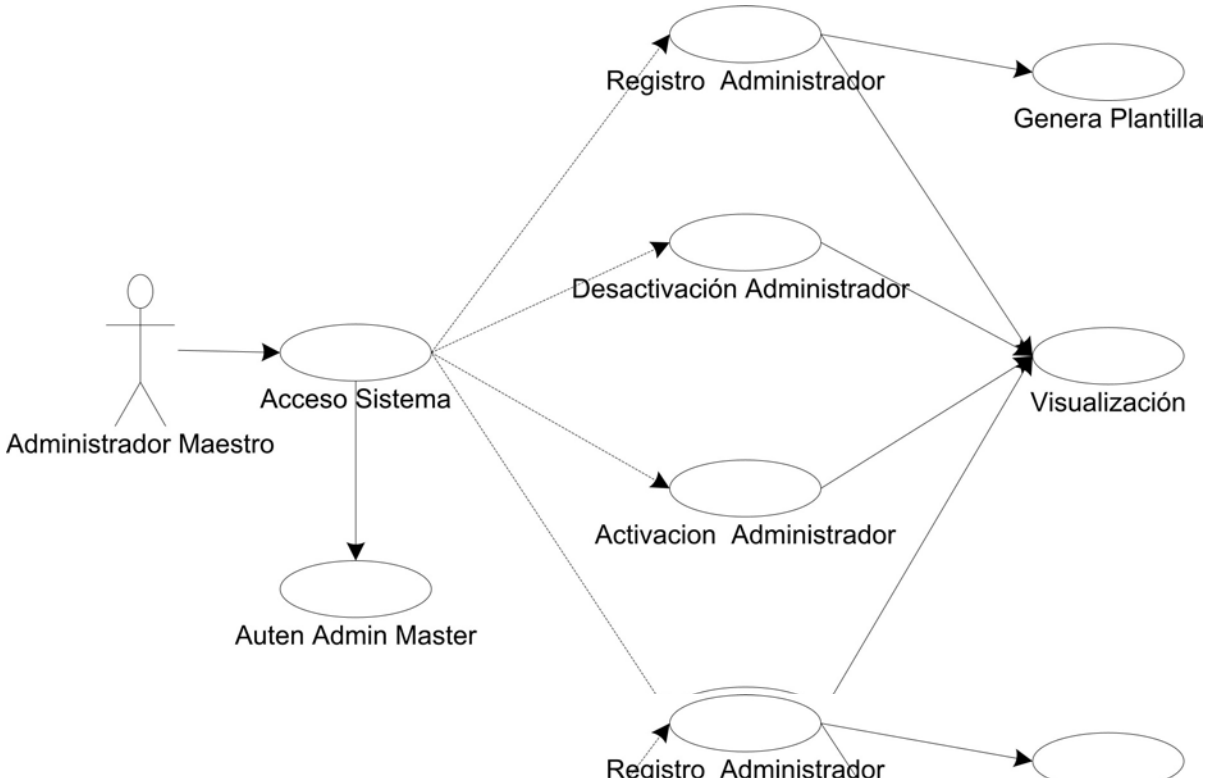


Figura 33. Diagrama donde se muestran los casos de uso del usuario Administrador Maestro.

Acceso_sistema: Este caso de uso se emplea en todos los procesos. Este caso de uso, permitirá a los usuarios obtener el acceso al sistema; así como al Administrador Maestro para que pueda interactuar con el caso *Auten_Admin_Master.*

Auten_Admin_Master: Este caso de uso permite autenticar al Administrador Maestro por medio de un usuario y password, y así obtener acceso al sistema.

Alta_Administrador: Este caso de uso permite dar de alta al Administrador General del sistema y registrarlo en la base de datos.

Genera plantilla: Este caso de uso permite generar el patrón de registro <<plantilla>> en base a la extracción de minutiaes de la huella digital. El patrón obtenido es un archivo pequeño de aproximadamente 150 a 300 bytes, el cuál contiene la información necesaria que será de utilidad para el proceso de autenticación.

Activación usuario: Este caso de uso permite activar las cuentas de usuario, para poder hacer uso del sistema. Para realizar esto, se cambiará la bandera de acceso de 0 a 1 en el registro del usuario.

Desactivación usuario: Este caso de uso permite desactivar las cuentas de usuario del sistema. Para realizar esto, se cambiará la bandera de acceso de 1 a 0 en el registro del usuario.

Modifica_Administrador: Este caso de uso permite modificar los datos personales del Administrador General: nombre, apellido paterno, apellido materno, región, ubicación y teléfono.

Visualización: Este caso de uso permite consultar los datos del Administrador General

3.1.3.2.2 Administrador General.

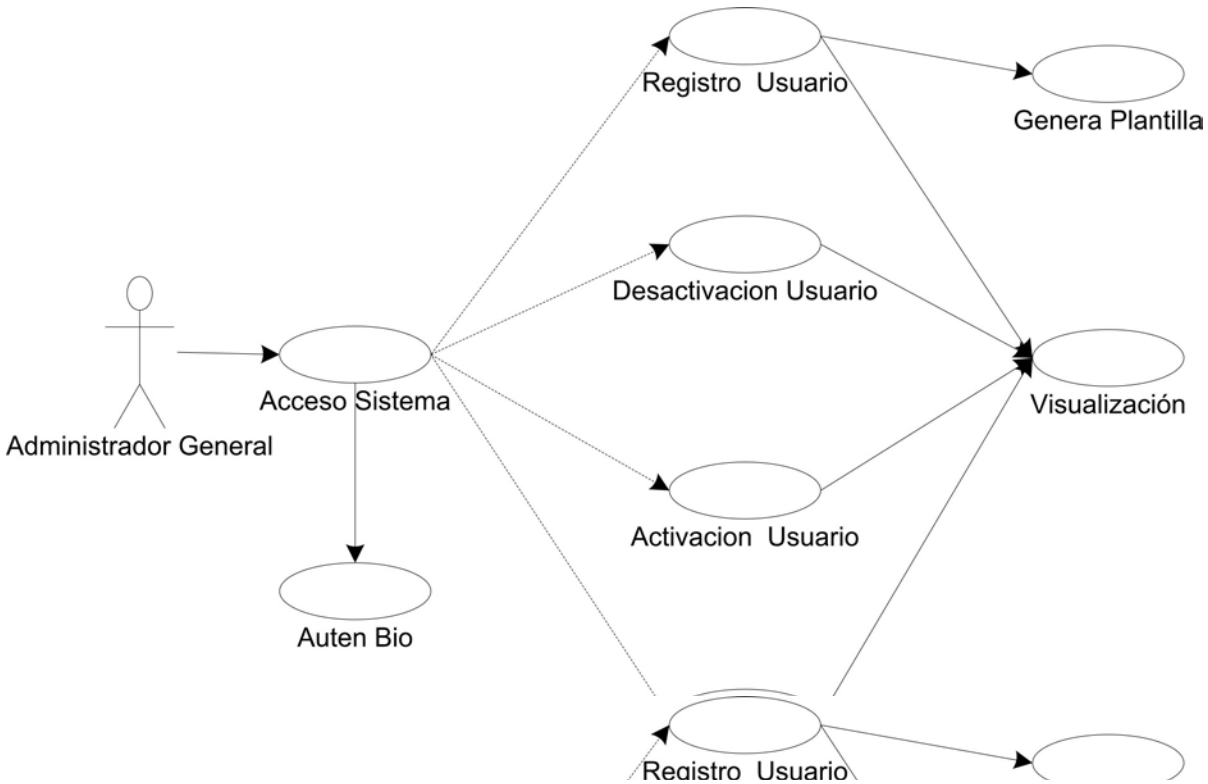


Figura 34. Diagrama donde se muestran los casos de uso del Administrador General del sistema.

Acceso_sistema: Este caso de uso le permite el acceso al Administrador General del sistema, e interactuar con el caso *Auten_Bio* para obtener el acceso.

Auten_Bio: Este caso de uso permite autenticar biométricamente al Administrador General, y así obtener acceso al sistema, para realizar altas, activaciones, desactivaciones, consultas y cambios.

Registro de usuario: Este caso de uso permite al Administrador General del sistema, realizar el registro de los usuarios. Los datos que debe de ingresar para cada usuario a dar de alta son: nombre, apellidos, número de empleado, región y ubicación. Este caso de uso permite la interacción con el caso generar plantilla para completar el registro del usuario.

Genera plantilla: Este caso de uso permite generar el patrón de registro <<plantilla>> en base a la extracción de minutiaes de la huella digital. El patrón obtenido, es un archivo pequeño de aproximadamente 150 a 300 bytes, el cuál contiene la información necesaria que será de utilidad para el proceso de autenticación.

Activación usuario: Este caso de uso permite activar usuarios del sistema. Para realizar esto, se cambiará la bandera de acceso de 0 a 1 en el registro del usuario.

Desactivación usuario: Este caso de uso permite desactivar las cuentas de usuario del sistema, sin necesidad de eliminar los datos de registro de la base de datos. Para realizar esto, se cambiará la bandera de acceso de 1 a 0 en el registro del usuario.

Modifica usuario: Este caso de uso permite modificar los datos del usuario a excepción de su ID de usuario y su patrón de registro de huella <<plantilla>>. Los datos actuales son presentados en modo de edición para que puedan ser modificados y posteriormente actualizados en la base de datos.

Visualización: Este caso de uso permite visualizar todos los usuarios en el sistema y así mismo, seleccionar individualmente un usuario para visualizar sus datos de registro.

3.1.3.2.3 Usuario del sistema

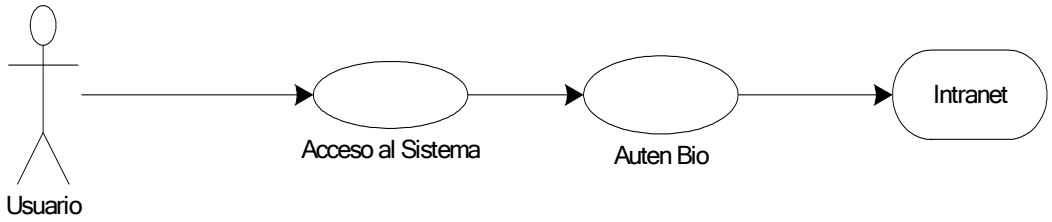


Figura 35. Diagrama donde se muestran los casos de uso del usuario del sistema.

Acceso_sistema: Este caso de uso le permite, el acceso e interacción con el caso *Auten_Bio* para obtener acceso a la Intranet.

Auten_Bio: Este caso de uso permite autenticar biométricamente al usuario, para obtener el acceso a la Intranet. Para lo anterior, el Administrador General de manera previa, debió haber dado de alta al usuario en el Sistema, con sus datos personales y sus huellas, para así obtener el acceso.

Intranet: Este caso de uso representa la Intranet.

3.2 DISEÑO

En este apartado se da inicio al diseño del sistema, después de haber recopilado y analizado la información necesaria respecto a las necesidades del usuario y la manera de cómo darles solución.

3.2.1 Diagrama de clases

Para el diseño del sistema se identifica el siguiente esquema de paquetes, el cuál se visualiza en la *Figura 36*:

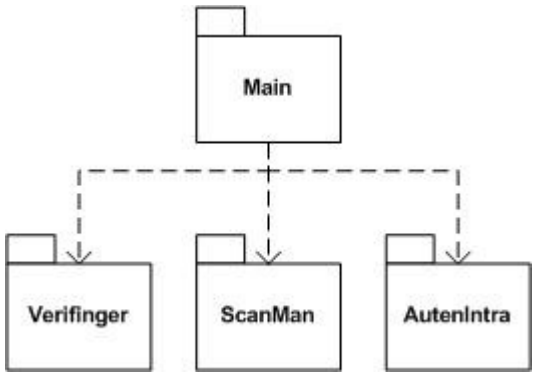


Figura 36. Diagrama de clases y paquetes.

3.2.1.1 Clases manejo de lector biométrico ScanMan

El paquete de clases *scanman* está compuesto por cuatro clases: *ScanMan, scannerEvenListener, ScanManException y ScannersMonitor.*

Estas clases son las encargadas del monitoreo, extracción y manejo de excepciones del lector biométrico de huella digital.

La *Figura 37* muestra las clases contenidas en el paquete y sus referencias:

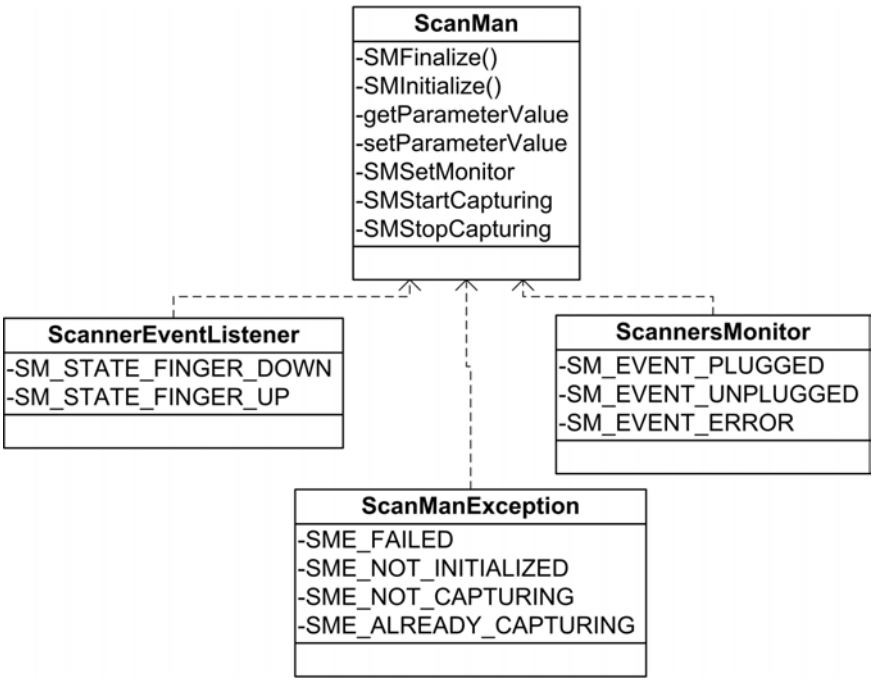


Figura 37. Diagrama donde se muestran las clases contenidas en el paquete scanman y sus referencias.

3.2.1.2 Clases manejo de huella digital VeriFinger

El paquete de clases V*eriFinger* está compuesto por siete clases: *VeriFingerExtractionResult, VeriFingerWrapper, VeriFingerFeature, VeriFingerMatchDetails, VeriFingerException, FigerprintData, VeriFingerGeneralizationResult y FingerDatabase*.

Estas clases son las encargadas de la extracción de minutiaes y generación de patrones de huella <<plantillas>>. Así mismo, del manejo de excepciones, búsqueda, identificación y almacenamiento de las mismas, en la base de datos de huellas.

En la *Figura 38* se muestran las clases contenidas en el paquete y sus referencias:

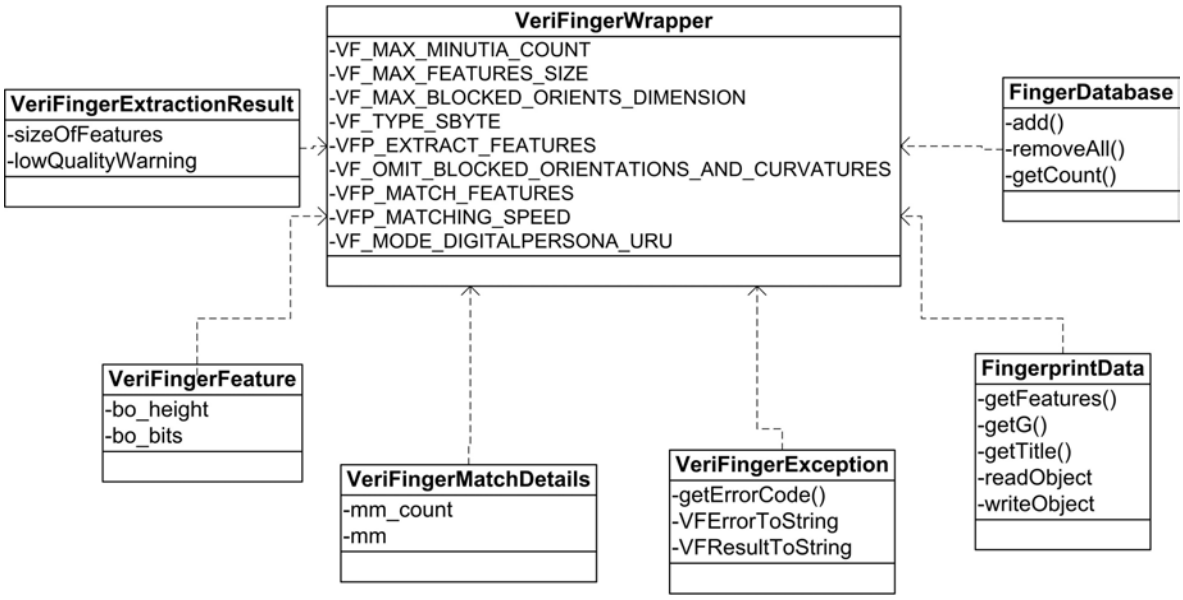


Figura 38. Diagrama donde se muestran las clases contenidas en el paquete VeriFingerWrapper y sus referencias.

3.2.1.3 Clases manejo de usuarios AutenIntra

El paquete de clases AutenIntra está compuesto por cinco clases: UpdateDatosUser, InsertaDatosUser, Conecta, CargaDatos y BuscaDatosUser.

Estas clases son las encargadas del manejo de usuarios, altas, desactivaciones, desactivaciones, modificaciones, búsquedas y conexiones a la base de datos. La *Figura 39* muestra las clases contenidas en el paquete AutenIntra:

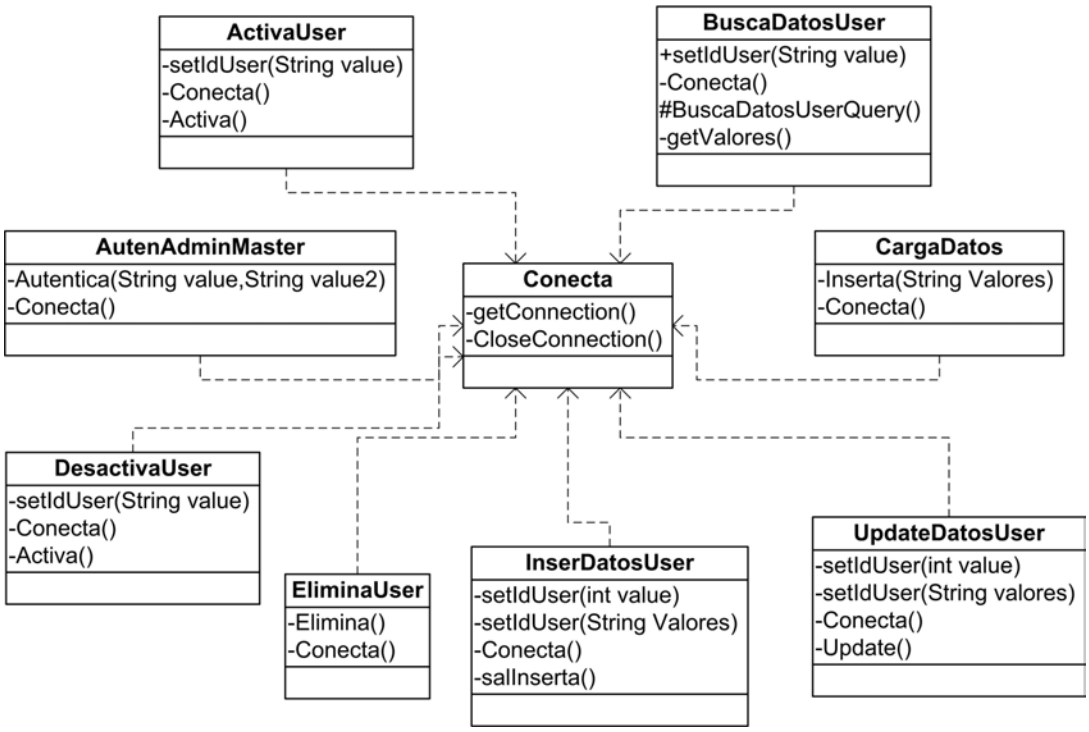


Figura 39. Diagrama donde se muestran las clases contenidas en el paquete de clases AutenIntra.

3.2.1.4 Clases principales Main

El paquete de clases Main está compuesto por siete clases: ValidaHuellaGrafico, EditApplet, InicioApplet, GrabaHuellaGrafico, DialogoCaptura, AltaApplet y CargaBaseDatos.

Estas clases son las encargadas de la parte de la interfaz gráfica, para el manejo de usuarios, altas, desactivaciones, modificaciones, búsquedas y conexiones a la base de datos.

La *Figura 40* se muestran las clases contenidas en el paquete Main:

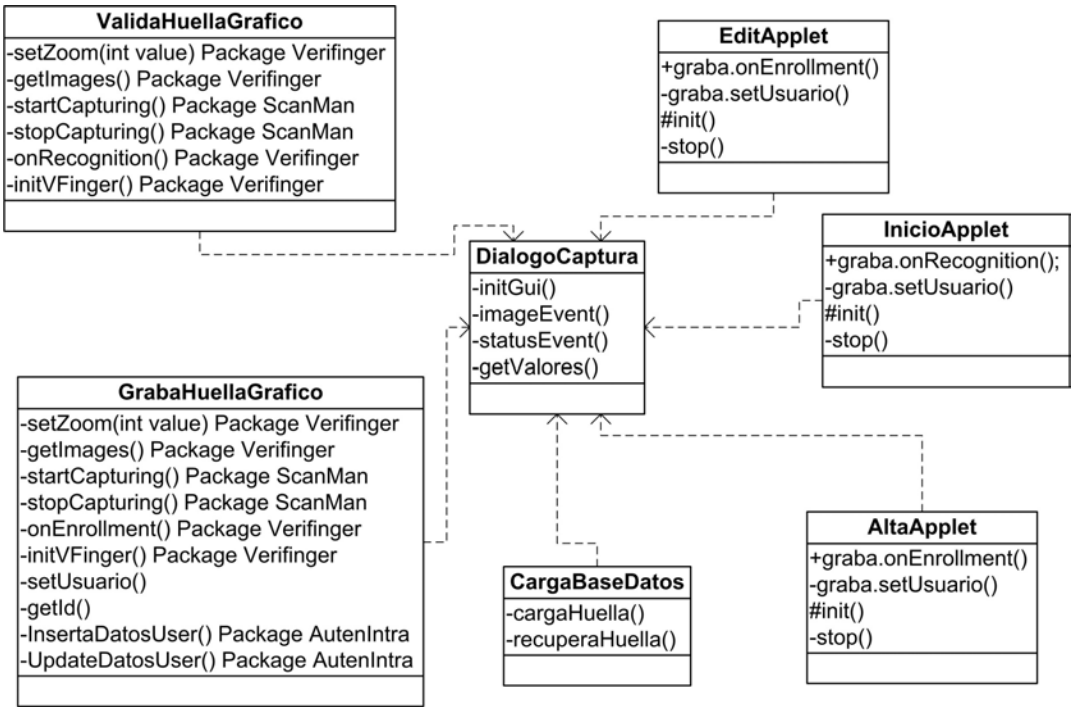


Figura 40. Diagrama donde se muestran las clases contenidas en el paquete de clases Main.

3.2.2 Base de datos y tablas

Para el desarrollo de la aplicación fue necesario generar una base de datos en la cuál se almacena y administra toda la información referente a datos de usuarios y sus huellas.

3.2.2.1 Campos y tablas.

La información almacenada en la base de datos es la siguiente:

- **Usuario:** nombre, apellido paterno, apellido materno, región, ubicación física, teléfono, id usuario y tipo de usuario.
- **Plantillas:** id y huella.
- **AdminMaster:** id_admin y pwdadmin

Adicionalmente es necesaria la generación de un archivo binario, el cuál contiene las huellas y será el medio para cargar en memoria ésta información

De acuerdo a lo anterior, se identifican dos tablas principales y una auxiliar: tabla de usuarios, tabla de plantillas y tabla de usuario Administrador Maestro. Ver *Figura 41:*

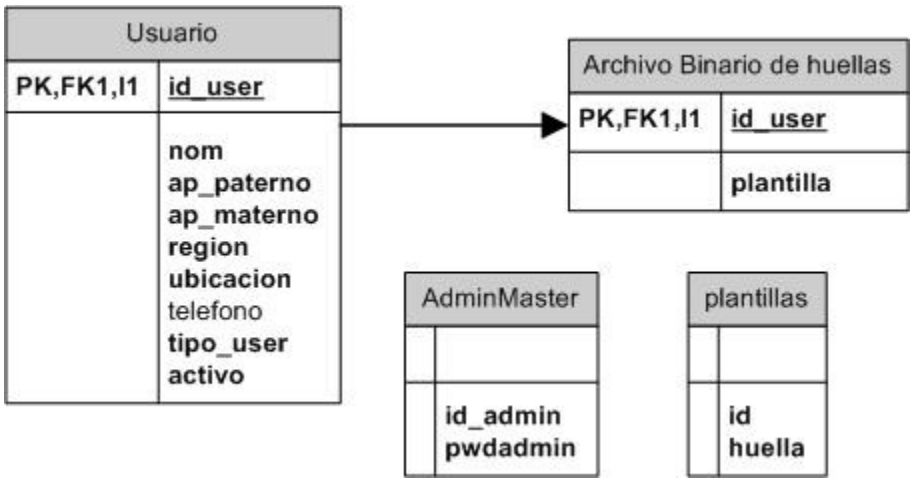


Figura 41. Tabla de usuarios, tabla de plantillas, archivo binario de huellas y tabla AdminMaster

3.2.3 Modelo relacional y diccionario de datos

A continuación en la *Figura 42* se muestra el modelo relacional de cada tabla, así como su ***diccionario de datos****:*

Physical Name	Data Type	Req'd	PK	Notes
id_user	INTEGER	☑	☑	identificador del usuario (Ejemplo de datos: 9867)
plantilla	BYTE	☑	☐	arreglo de bytes que representan la huella del usuario (Ejemplo de datos: gsdsrenhcdhe843474hsb)

Physical Name	Data Type	Req'd	PK	Notes
id_admin	INTEGER	☑	☐	identificador del administrador (Ejemplo de datos: 9867)
pwdadmin	CHAR(10)	☑	☐	password del administrador

	Physical Name	Data Type	Req'd	PK	Notes
▶	id_user	INTEGER	☑	☑	Identificador del usuario (Ejemplo de datos: 123)
	nom	VARCHAR(30)	☑	☐	Nombre del usuario (Ejemplo de datos: Ricardo)
	ap_paterno	VARCHAR(30)	☑	☐	Apellido Paterno del usuario (Ejemplo de datos: Castro)
	ap_materno	VARCHAR(30)	☑	☐	Apellido Materno del usuario (Ejemplo de datos: Gonzalez)
	region	VARCHAR(10)	☑	☐	Region del usuario (Ejemplo de datos: Corporativo)
	ubicacion	VARCHAR(80)	☑	☐	Ubicacion fisica del usuario (Ejemplo de datos: Ejercito Nacional 1234 Polanco Mexico D.F.)
	telefono	VARCHAR(10)	☐	☐	Telefono del usuario (Ejemplo de datos: 5551234567)
	tipo_user	VARCHAR(5)	☑	☐	Tipo de usuario (Ejemplo de datos: Admin Master, Admin, User)
	activo	INTEGER	☑	☐	Usuario activo (Ejemplo de datos: 0 o 1)
			☐	☐	

Figura 42. Modelo relacional de tablas y su diccionario de datos.

3.2.4 Diagramas de secuencia del sistema

Los siguientes diagramas expresan los escenarios[46] en los cuáles se ven involucrados los casos de uso.

[46] El escenario de un caso de uso es una instancia o trayectoria realizada por medio del uso: un ejemplo real de ejecución. **[RFC6,p.137]**

3.2.4.1 Diagrama de secuencia autentica Administrador Maestro

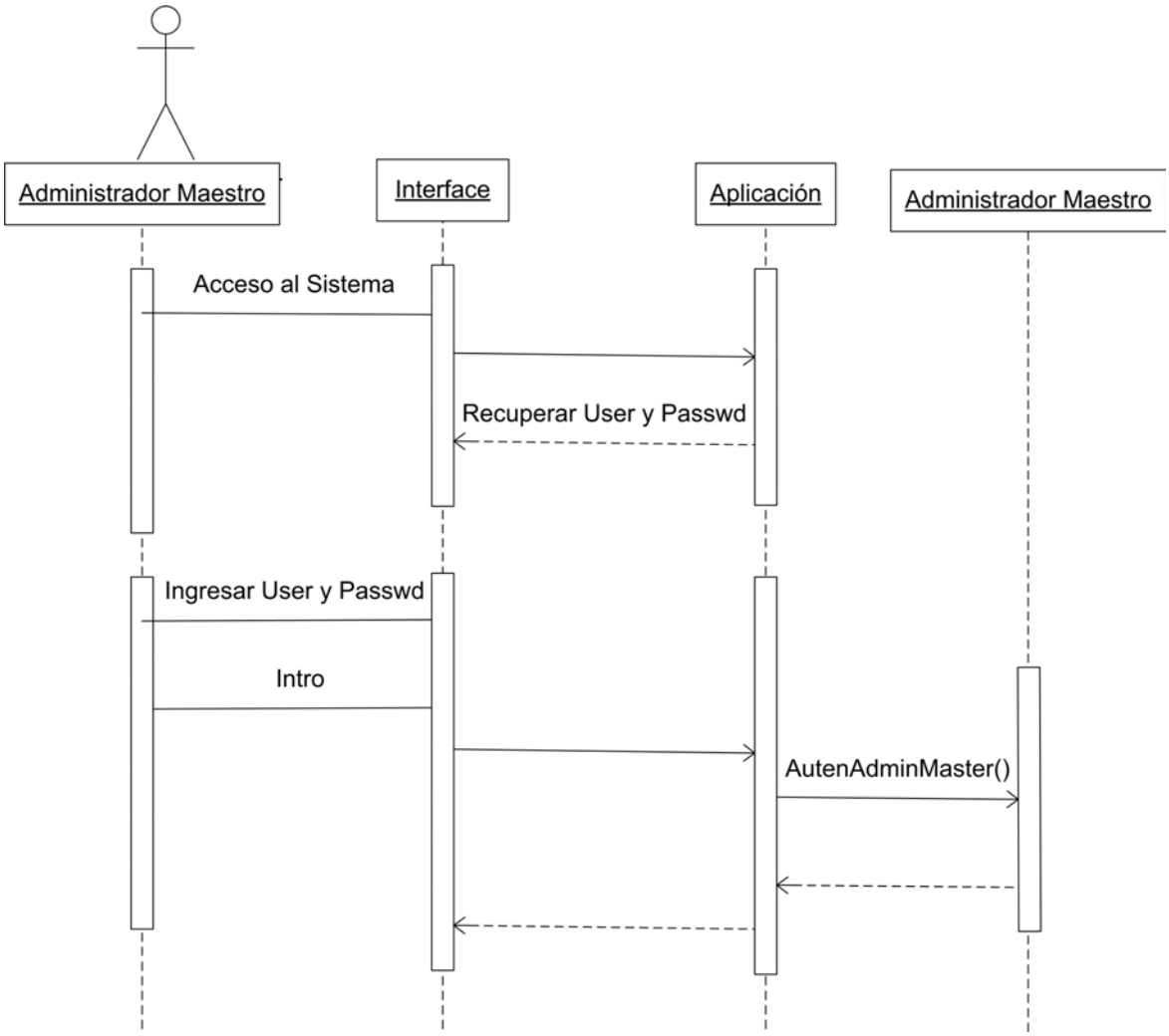


Figura 43. Diagrama de secuencia autentica Administrador Maestro.

3.2.4.2 Diagrama de secuencia alta Administrador General

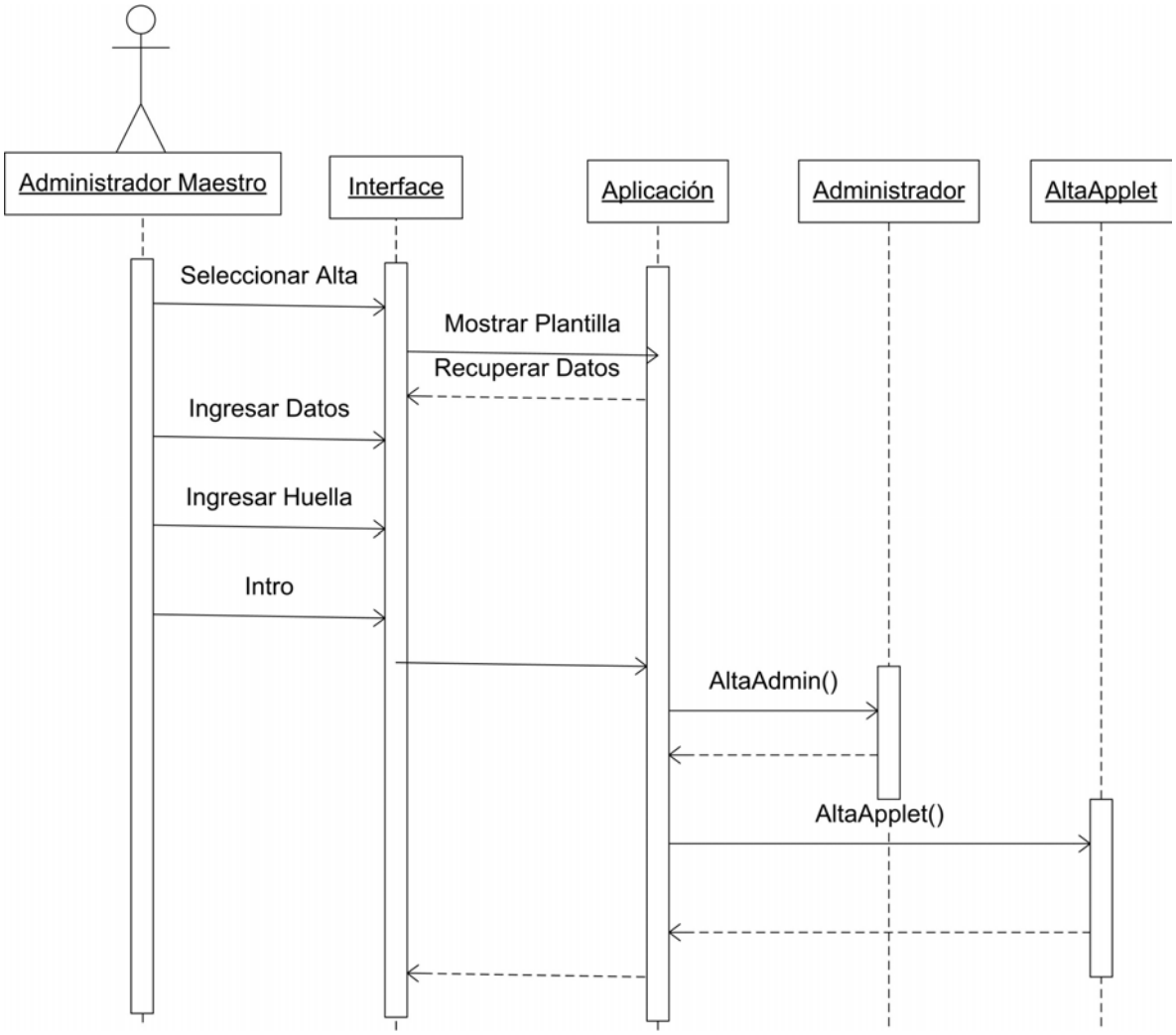


Figura 44. Diagrama de secuencia alta Administrador General

3.2.4.3 Diagrama de secuencia modifica Administrador General

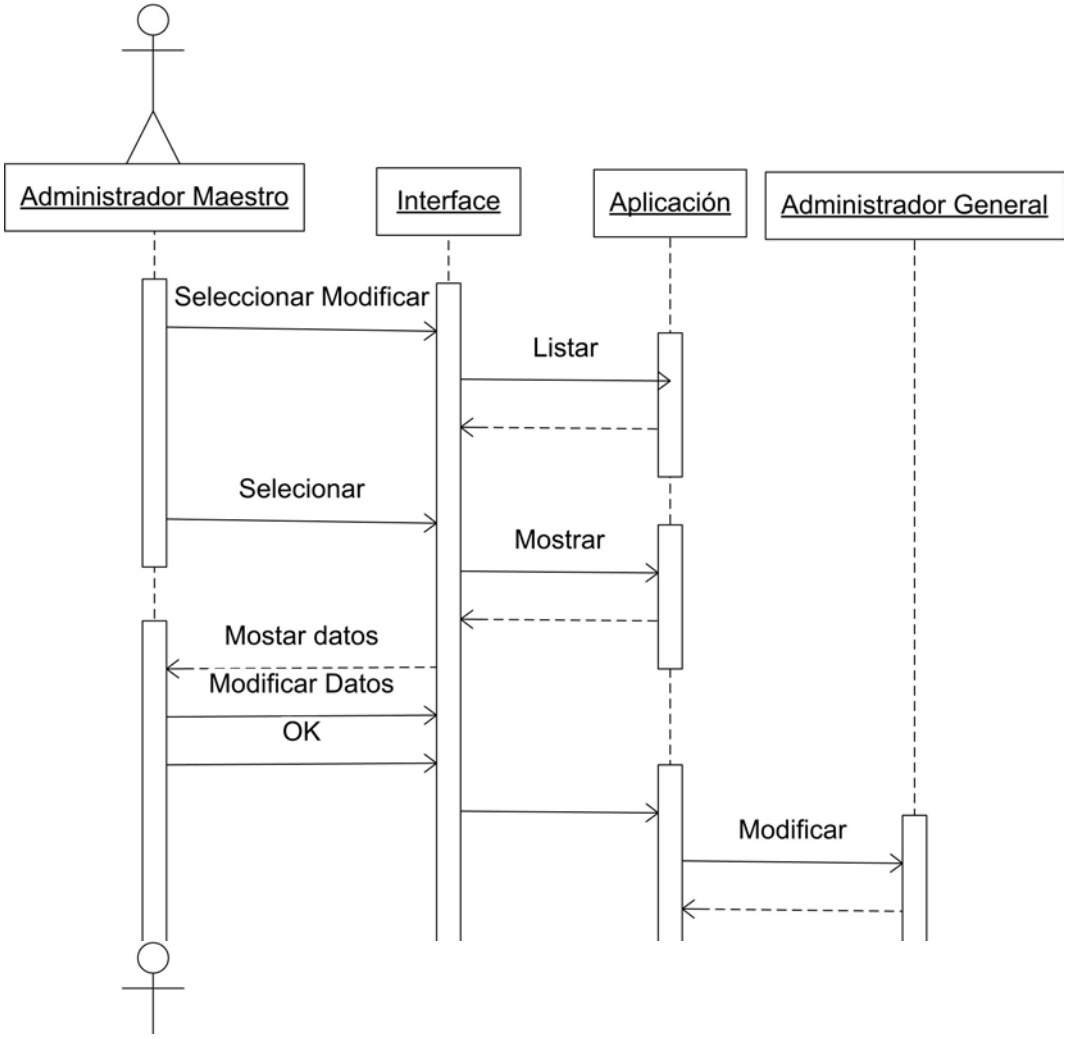


Figura 45. Diagrama de secuencia modifica Administrador General

3.2.4.4 Diagrama de secuencia visualiza

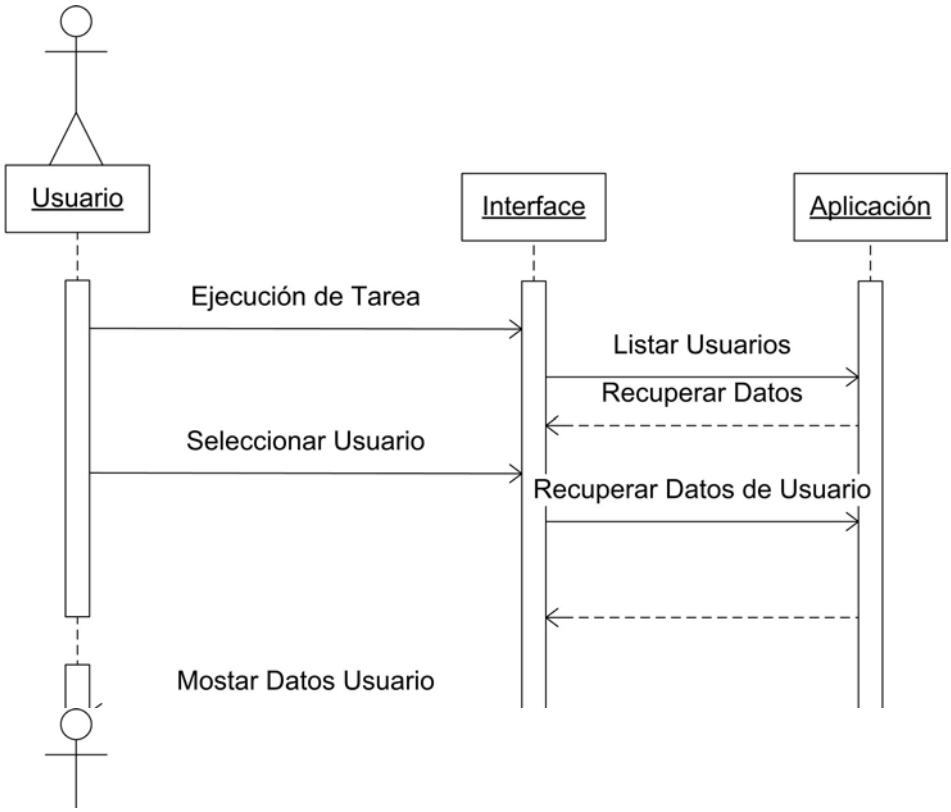


Figura 46. Diagrama de secuencia visualiza.

3.2.4.5 Diagrama de secuencia registra usuario

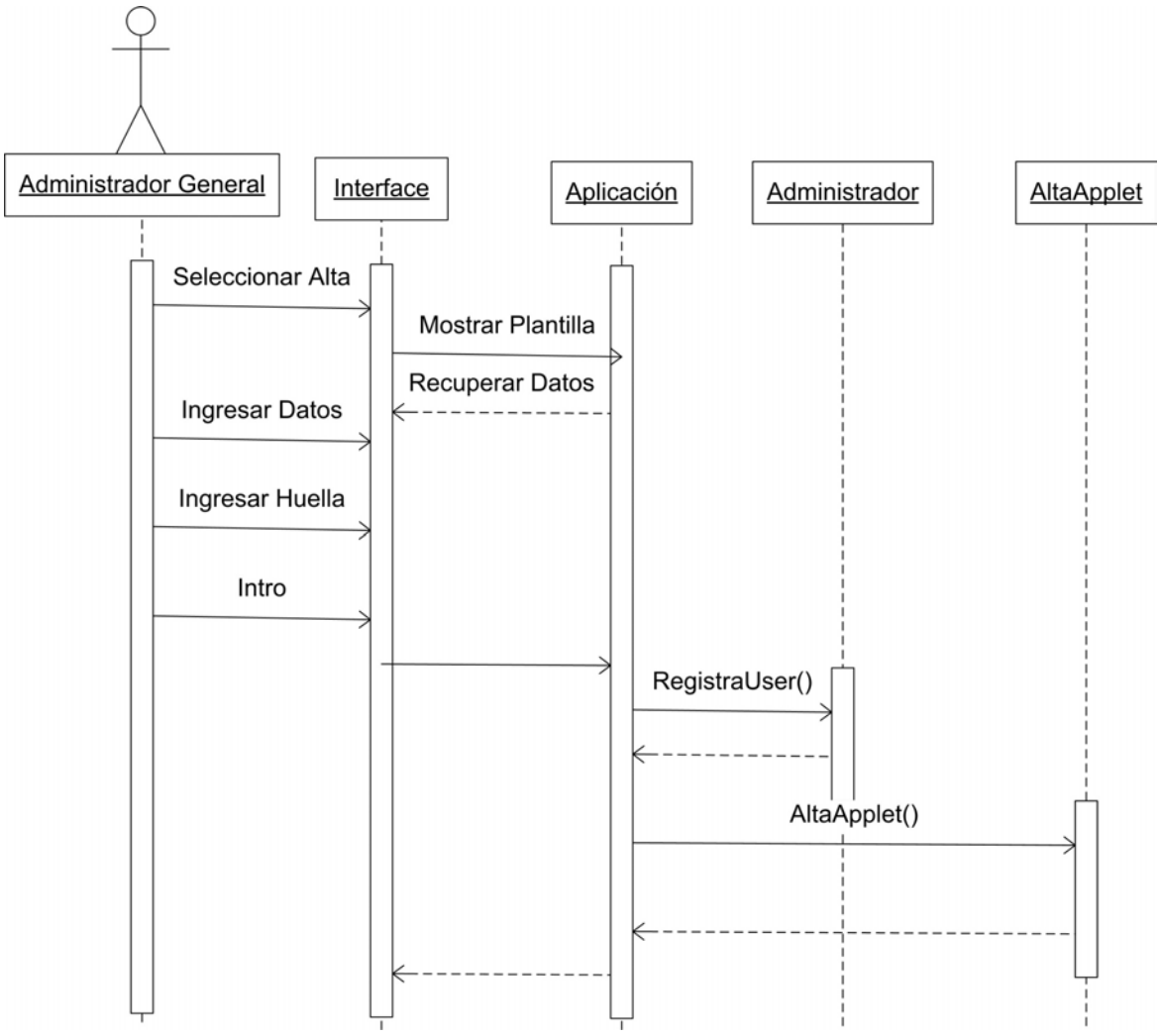


Figura 47. Diagrama de secuencia registra usuario.

3.2.4.6 Diagrama de secuencia modifica usuario

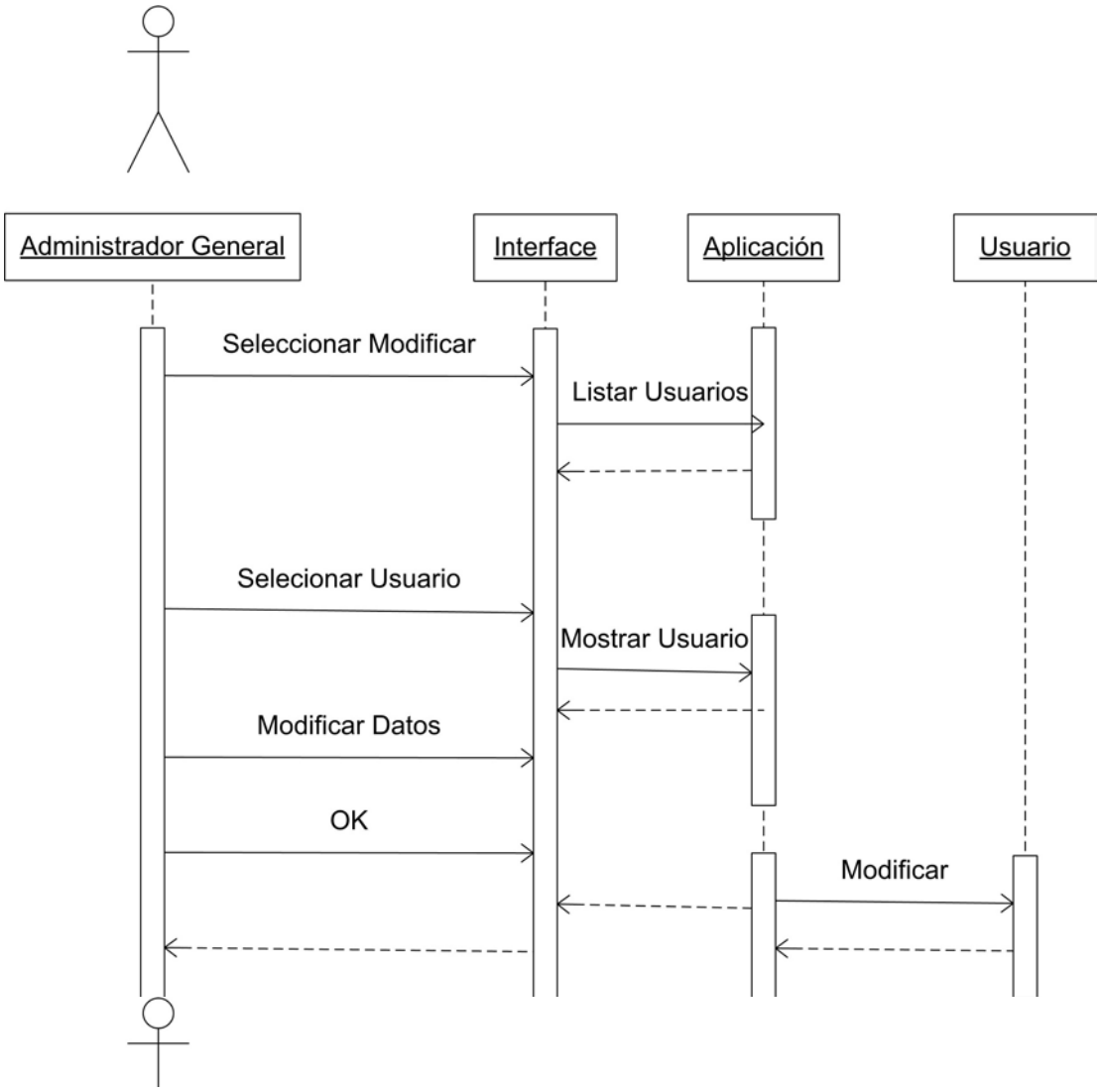


Figura 48. Diagrama de secuencia modifica usuario.

3.2.4.7 Diagrama de secuencia Autenticación Biométrica

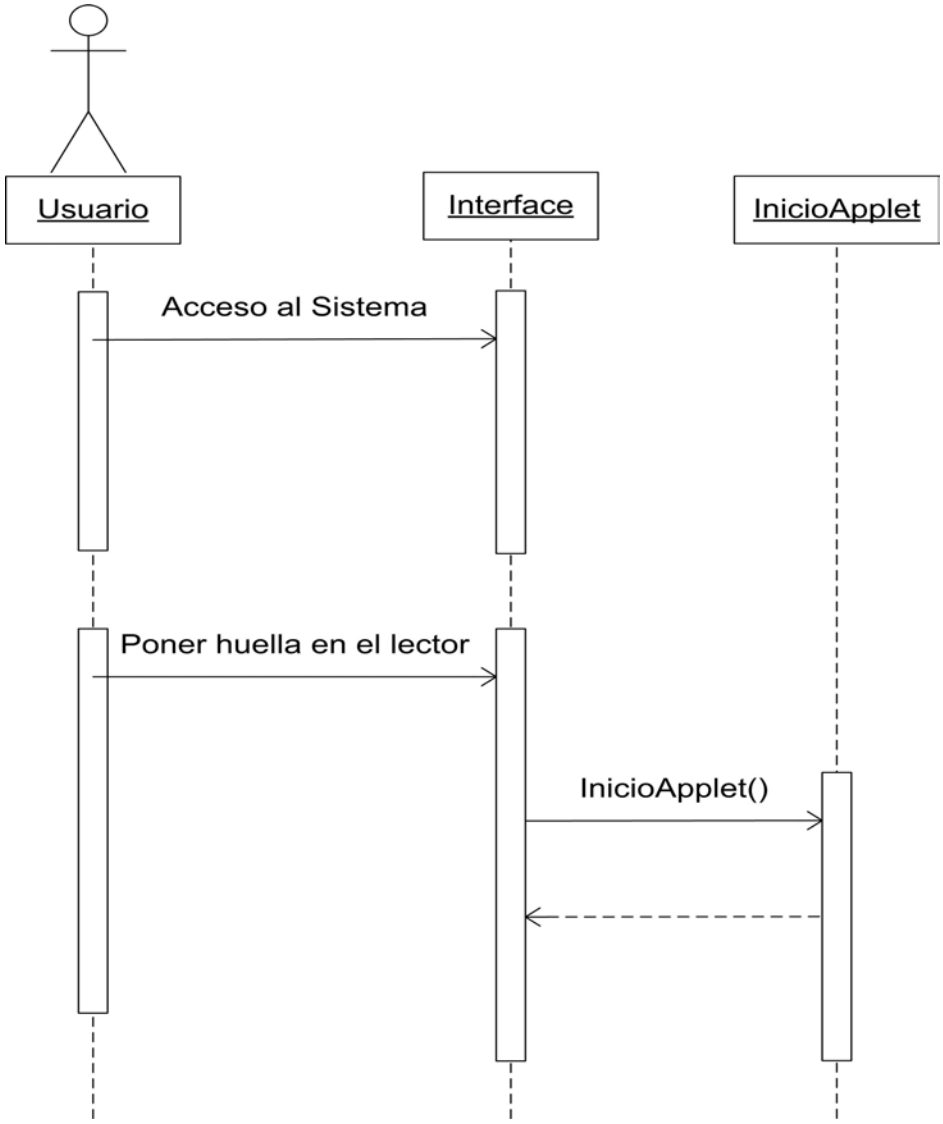


Figura 49. Diagrama de secuencia Autenticación Biométrica.

3.2.4.8 Diagrama de secuencia desactiva usuario.

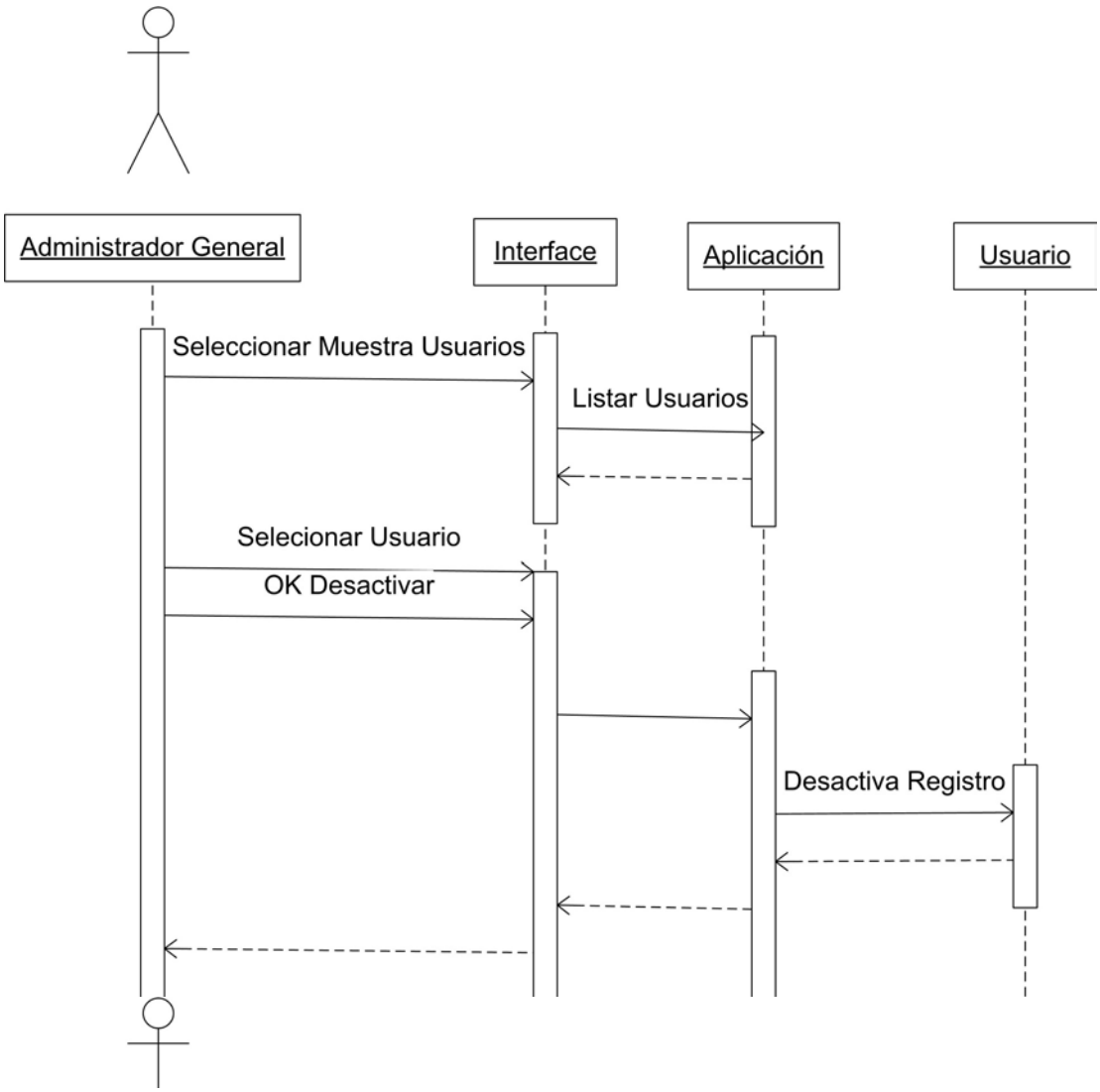


Figura 50. Diagrama de secuencia desactiva usuario

3.3 DESARROLLO

En este apartado se muestran las ***interfaces gráficas*** *<<front end>>* hacia el usuario y Administradores, que permitirán interactuar con la aplicación de manera fácil y amigable.

Dichas interfaces gráficas son el resultado del análisis y diseño realizado en las fases anteriores, mismas que se detallan a continuación.

El código fuente se proporciona para su consulta, en el "***Anexo E. Código Fuente"*** de este trabajo.

3.3.1 Pantalla de acceso Administrador Maestro

Para inicializar el sistema y poder empezar a utilizarlo, es necesario crear una cuenta de usuario de tipo Administrador Maestro por medio de una sentencia de sql:

```
    INSERT INTO administrador ( id_admin, pwdadmin )
VALUES ( 54245,'123sdfe456 )
```

Este usuario servirá para crear a los Administradores Generales, los cuáles a su vez, serán los encargados de dar de alta a los usuarios normales y registrar sus huellas para que puedan acceder al sistema.

El usuario Administrador Maestro será el único usuario que accederá al sistema a través de login y password, y lo realizará por una única ocasión, mientras se crean las cuentas de los Administradores Generales.

La interfaz de acceso para el Administrador Maestro se muestra en la *Figura 51*, donde en ella debe de ingresar su <<username>> y <<password>> para acceder al sistema.

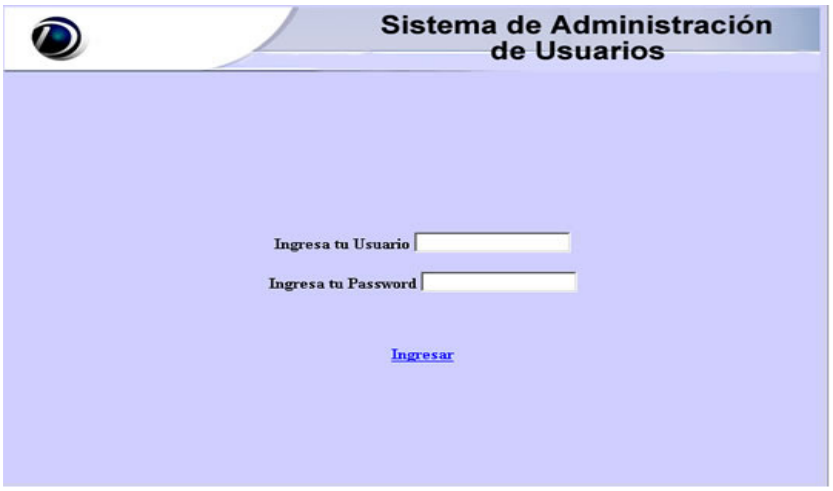


Figura 51. Pantalla de acceso, del Administrador Maestro.

3.3.2 Pantalla menú Administrador Maestro

Esta interfaz muestra las opciones a las cuáles, tiene acceso el Administrador Maestro: a) alta de administrador y b) muestra administrador. Lo anterior se muestra en la *Figura 52*:

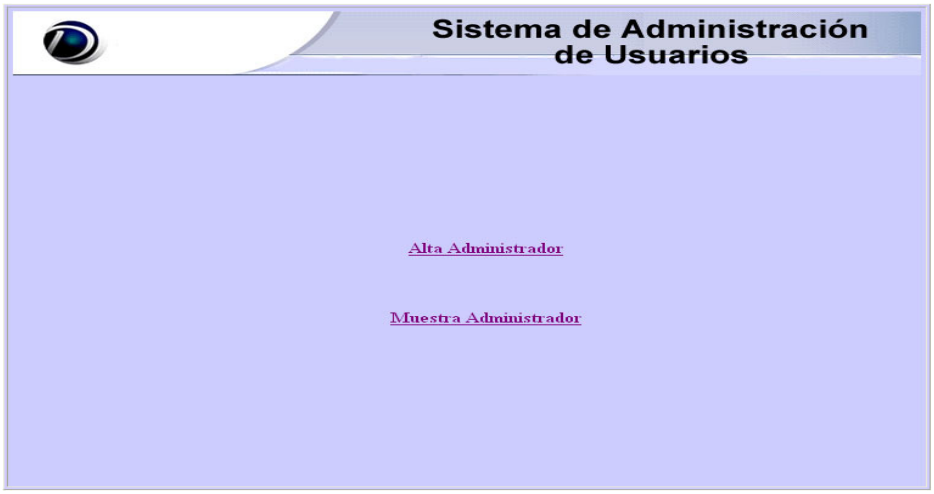


Figura 52. Pantalla de menú del Administrador Maestro.

3.3.3 Pantalla alta Administrador General

Esta interfaz muestra la plantilla que debe de llenarse para dar de alta al Administrador General. La información de registro que se debe proporcionar es: usuario, nombre, apellidos, región, ubicación, teléfono y la huella del dedo pulgar o cualquier otra que se defina como norma dentro del proceso. Ver *Figura 53*

Realizado lo anterior, deberá posicionar su dedo en el lector biométrico, con la finalidad de que el sistema efectúe el registro de su huella dactilar en la base de datos. Al término del registro, el usuario Administrador General creado, podrá comenzar a dar de alta a los usuarios comunes del sistema.

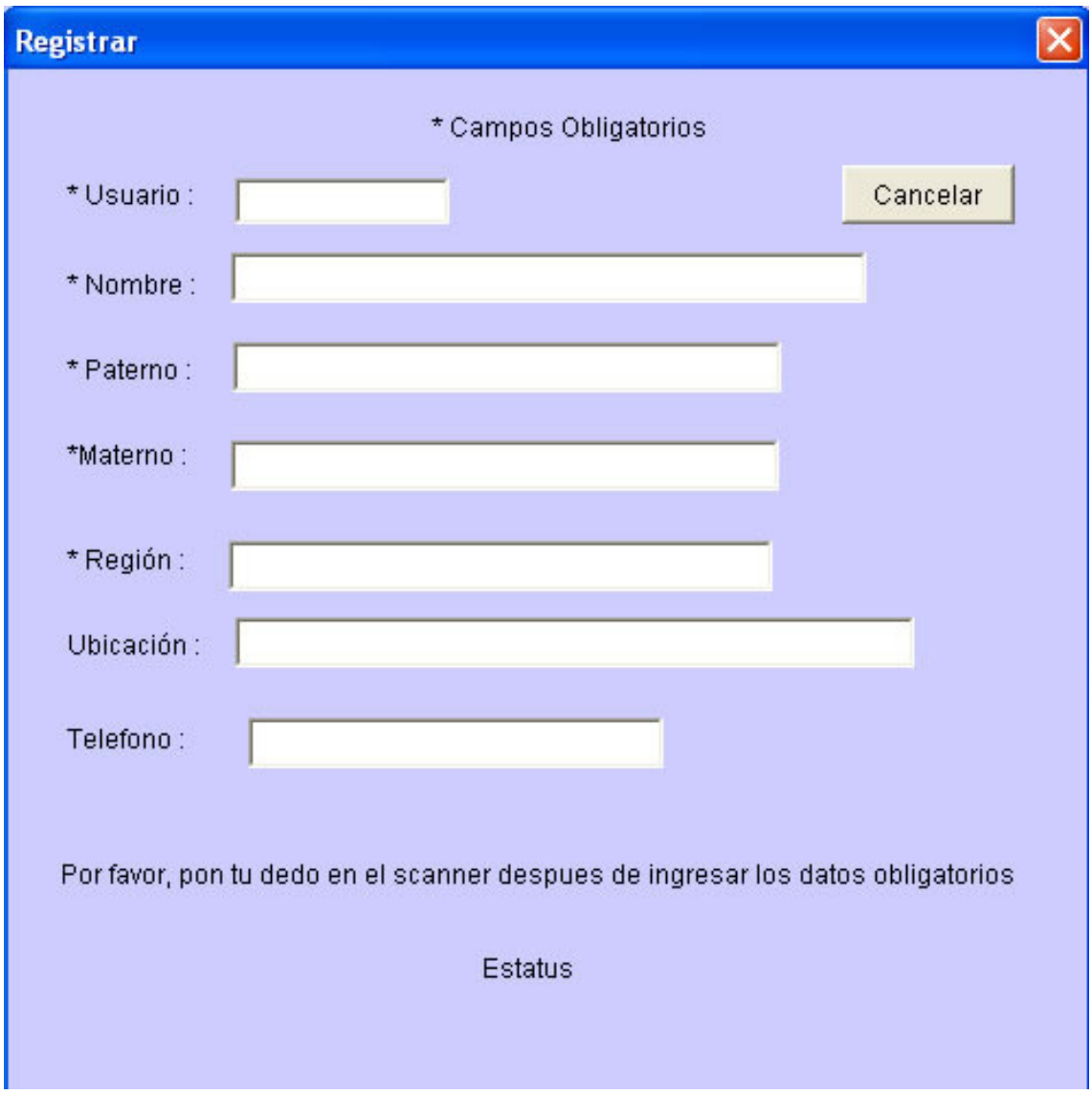


Figura 53. Pantalla de registro para el alta del Administrador General.

3.3.4 Pantalla muestra Administrador General

Esta interfaz lista la relación de Administradores Generales existentes, y muestra las opciones: a) Activar/desactivar Administrador y b) Modificar Administrador. Al pulsar los botones respectivos se accede a las opciones que se muestran en la *Figura 54*:

Figura 54. Pantalla con las opciones para realizar la baja del Administrador General y/o modificaciones.

3.3.5 Pantalla de acceso Administrador General

Esta es la interfaz de acceso para el Administrador General. Es a través de ésta interfaz, donde el Administrador General debe ingresar. Esta interfaz se muestra en la *Figura 55*:

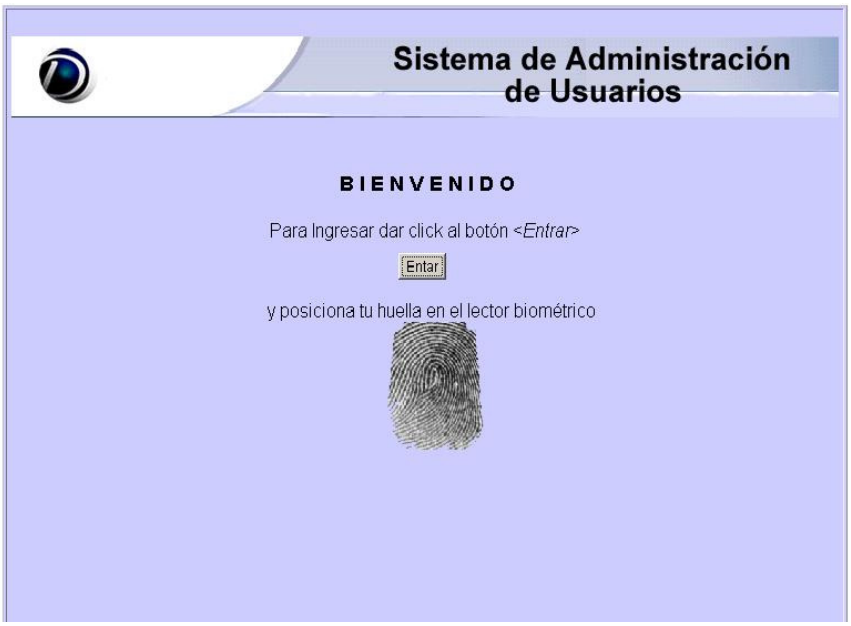


Figura 55. Pantalla de acceso del Administrador General.

3.3.6 Pantalla menú del Administrador General

Esta interfaz muestra las opciones a las cuáles tiene acceso el Administrador General: a) alta usuarios y b) modifica usuarios. Ver *Figura 56:*

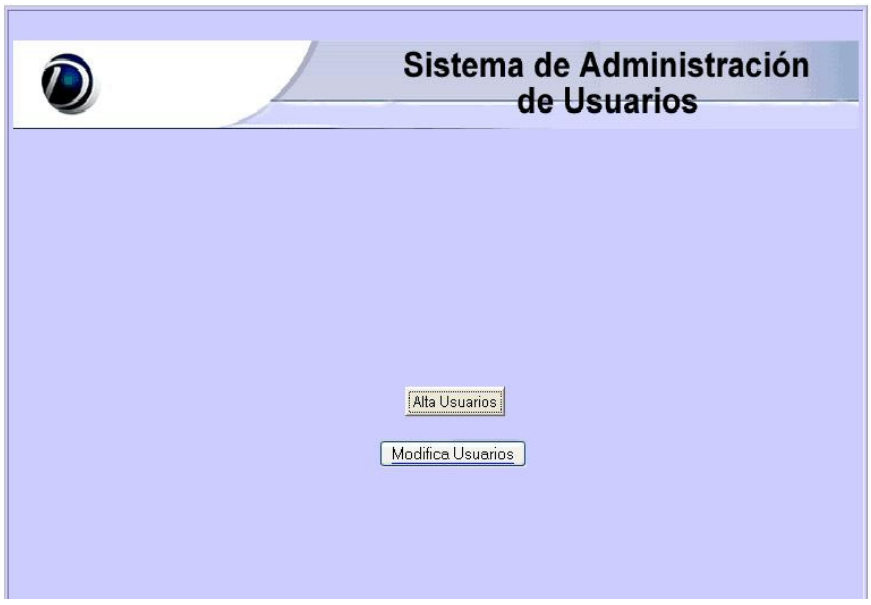


Figura 56. Pantalla de menú del Administrador General.

3.3.7 Pantalla registra usuario

Como se observa en la *Figura 57,* esta interfaz muestra la plantilla que debe de llenarse para dar de alta a un usuario. La información de registro que debe proporcionarse de manera obligatoria es: usuario, nombre, apellido paterno, apellido materno, región y la huella del dedo elegido. Los datos opcionales son: teléfono y ubicación.

Después de posicionar el dedo definido en el lector biométrico, el dispositivo capturará la huella del usuario y efectuará el registro en la base de datos, con lo cuál el usuario podrá acceder a la Intranet.

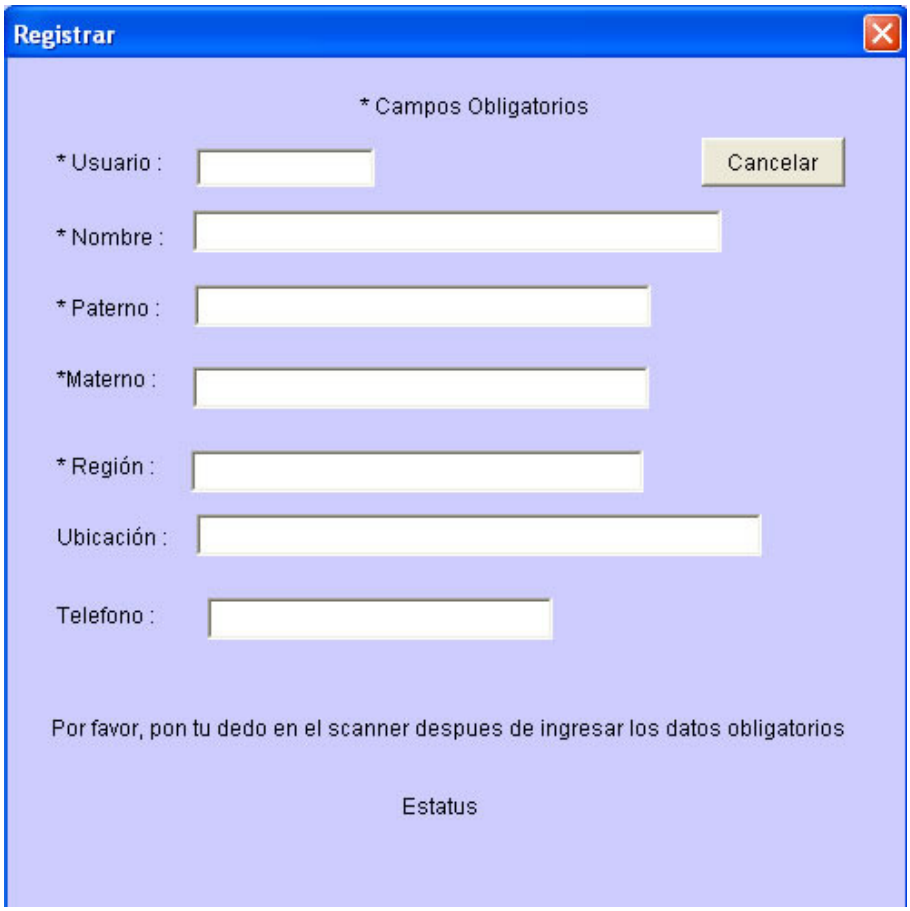


Figura 57. Pantalla de registro para el alta de usuarios y sus huellas.

3.3.8 Pantalla muestra usuarios

Esta interfaz muestra las opciones para llevar a cabo la activación, desactivación y modificación de usuarios, así como mostrar en qué estado se encuentra la cuenta de cada usuario (activada/desactivada). Al pulsar los botones respectivos se accede a las opciones que se muestran en la *Figura 58*:

Figura 58. Pantalla donde se muestra la lista de usuarios, y las opciones para su activación, desactivación y/o modificación.

3.3.9 Pantalla acceso usuario

En la *Figura 59* se muestra la interfaz de acceso para los usuarios. Es a través de esta interfaz, donde los usuarios deberán ingresar su huella en el lector biométrico, con la finalidad de ser autentificados biométricamente para acceder a la Intranet.

Figura 59. Pantalla de acceso de usuarios, donde se les solicita su huella dactilar para su autenticación ante el sistema.

En este capítulo se ha dado a conocer el detalle del caso práctico planteado para llevar a cabo la autenticación de usuarios mediante la lectura de su huella digital, para otorgar/denegar el acceso a la Intranet de una empresa. El objetivo de este apartado ha sido dar a conocer al lector, una de tantas aplicaciones donde la tecnología biométrica puede ser utilizada e integrada de manera eficiente como método alternativo de autenticación, adicional a los tradicionales que hacen uso de passwords y que presentan vulnerabilidades importantes que mantienen en riesgo la seguridad de los sistemas.

El caso práctico desarrollado es factible de ser mejorado en varios aspectos, pero consideramos que es un buen ejemplo para mostrar a grandes rasgos el análisis que debe realizarse y los elementos a considerar.

Gran parte de la expectativa de incluir un caso práctico como parte integral del proyecto, ha sido porque consideramos realmente importante pasar de la teoría a la práctica. Porque al pasar esta frontera, siempre implica enfrentar detalles técnicos, problemas, nuevos planteamientos, soluciones, etc, y por consecuencia, obtener nuevos conocimientos.

CAPÍTULO 4.
VALIDACIÓN DEL SISTEMA

Para la validación del sistema, se utilizó una base de datos que contiene 100 imágenes de huellas dactilares, pertenecientes a 10 personas diferentes de las que se capturó una imagen por cada dedo.

Debido a que la base de datos es pequeña, la forma de operación seleccionada para realizar el comparativo fue 1:N; donde cada imagen en la base da datos es comparada con su propia <<plantilla>> y con las otras 99 <<plantillas>>.

La forma de validar la operación del sistema, fue en términos de falso rechazo y falsa aceptación. Es decir, si se realiza la comparación de una "huella viva o de entrada" Vs. la plantilla de ese mismo dedo (ésta última obtenida durante el proceso de registro del usuario y almacenada en la BD) y el resultado es exitoso, se considera una autenticación correcta. En caso contrario, se trata de un *falso rechazo.*

Si se obtiene una autenticación exitosa al comparar una huella con otra que no pertenece al mismo dedo, estamos ante lo que se denomina una *falsa aceptación.* Mayores detalles se puede consultar el subcapítulo ***2.1.7 "Tasa de falsos rechazos (TFR) y Tasa de falsas aceptaciones (TFA)".***

Para obtener un estimado del nivel de fiabilidad del sistema, se utilizaron los valores del porcentaje de autenticación y porcentaje de rechazo; donde se denota a falsos rechazos como *num_falsos_rechaz, num_correctas* al número de autenticaciones correctas y *num_falsas_acept* al número de falsas aceptaciones.

Considerando lo anterior, el porcentaje de autenticación y el porcentaje de rechazo, es calculado de la siguiente manera:

$$\%\ \text{Autenticación} = \frac{num\_correctas + num\_falsas\_acept}{num\_total\_huellas\_BD} \times 100$$

$$\%\ \text{Rechazo} = \frac{num\_falsos\_rechaz}{num\_total\_huellas\_BD} \times 100$$

La *Tabla 7* muestra los valores obtenidos respecto al sistema desarrollado:

	Nombre Usuario	falsos rechaz	falsas acept	correctas	% rechazo	TE
1	Alfonso Mtz Núñez	1	0	49	1%	99%
2	Darío Rodríguez Pérez	0	0	50	0%	100%
3	Guadalupe González López	2	0	48	2%	98%
4	David Pérez de León	0	0	50	0%	100%
5	Miriam Reyes Rodríguez	0	0	50	0%	100%
6	Erika Ortega Argüelles	0	0	50	0%	100%
7	Marco Antonio Díaz Mendoza	0	0	50	0%	100%
8	Alejandro Hernández Badillo	1	0	49	1%	99%
9	Manuel Arroyo Bautista	0	0	50	0%	100%
10	Alfonso Lizárraga Ramírez	0	0	50	0%	100%

Tabla 7. Resultados en términos de % Rechazo y Tasa de Éxitos

De lo anterior se concluye que los valores obtenidos son óptimos, obteniendo un 99.6% de media de autenticación exitosa.

CAPÍTULO 5. RESULTADOS, CONCLUSIONES Y TRABAJO A FUTURO

El desarrollo de este proyecto representa un esfuerzo conjunto por transmitir la importancia que tiene la correcta administración de identidades de usuario y el proceso de autenticación, haciendo uso de tecnologías mayormente efectivas como lo es la Biometría por huella dactilar, con la finalidad de validar la identidad de los usuarios de manera eficiente y segura, e incrementar el nivel de seguridad y confiabilidad de los sistemas informáticos.

Como resultado del trabajo desarrollado (teoría y caso práctico), se confirma el cumplimiento de los objetivos planteados desde el inicio del proyecto, en cuanto al desarrollo de un sistema que permitiera llevar el control de accesos de usuario a una intranet, integrando un dispositivo biométrico por huella dactilar para validar la identidad de los usuarios de manera mayormente efectiva. Es decir, mejorando la seguridad de una intranet corporativa de una empresa, con la finalidad de que solo los usuarios autorizados, tengan acceso a la información respectiva.

Por otro lado, la integración realizada como caso práctico, nos permitió tomar lo mejor de las tecnologías existentes: biometría por huella dactilar como tecnología de autenticación y validación de identidades de usuario, y java en su modalidad cliente/servidor vía web, para realizar la integración del motor de búsqueda y reconocimiento; lo cuál consideramos, permite una fácil portabilidad entre diferentes sistemas operativos y una fácil actualización de la aplicación.

De acuerdo a los resultados obtenidos en el caso práctico, podemos decir que la tecnología biométrica por huella digital es sin lugar a dudas, una de las tecnologías de vanguardia con un nivel de confiabilidad alto (98%); que debido a las ventajas que presenta, viene a resolver gran parte de las vulnerabilidades de los métodos de autenticación tradicionales, aunque no por ello capaz de brindar seguridad al 100%.

Lo anterior nos lleva a señalar algo importante, y es que aunque la protección pura no existe, si se toman en cuenta las mejores prácticas en materia de seguridad, con certeza se podrá garantizar que los riesgos sean menores. Esto nos lleva a dejar en claro algo, y es que, la seguridad de los sistemas y activos informativos en general, no recae en un solo factor (en este caso los mecanismos de autenticación utilizados), sino de una serie de factores como lo son los antivirus, firewalls, mecanismos para el control de acceso físico y lógico, personal técnico de la empresa, los usuarios, grado de concientización sobre la importancia de seguridad,

etc. Es decir, una serie de buenas prácticas de seguridad, donde necesariamente se involucren a las tecnologías, los procesos y las personas.

Como parte de lo anterior, los mecanismos para el control de acceso y autenticación de usuarios, representan uno de tantos factores a considerar, al ser la puerta primaria de entrada a los sistemas. Como resultado de esto, la tecnología biométrica por huella digital aplicada a este proceso, conforma una de tantas opciones del mercado, que debido a las ventajas que otorga, ha logrado posicionarse de manera rápida en diversas empresas.

Si bien es cierto que la tecnología biométrica no es de uso masivo aún, opinamos que por lo menos para el para el sector gobierno y empresas grandes o medianas, ya es muy importante, debido a que no solo les permite mejorar la Seguridad Informática (como el acceso a sus sistemas); sino que además, es de gran utilidad como elemento de identificación de usuarios, empleados o ciudadanos, y para mejorar sus sistemas administrativos, servicios públicos, reducir costos, eliminar fraudes, evitar corrupción, entre otros.

Considerando lo anterior y de acuerdo a la experiencia obtenida, opinamos que aunque la inversión requerida para implantar un sistema biométrico pudiera parecer costosa, los beneficios obtenidos como: incremento de la seguridad, mejora en la protección de los activos, mitigación de riesgos, etc; justifican sin duda alguna, el gasto realizado.

De esta manera, sin pretender ser un tanto tendenciosos o futuristas (tomando en cuenta los cambios importantes que se han venido dando en los últimos tiempos como lo es la apertura del uso de Internet), consideramos que la tecnología biométrica por huella digital continuará cautivando mercado en gran variedad de áreas; pudiéndola encontrar operando a corto plazo, en situaciones de uso común o cotidiano como en bancos, computadoras de acceso restringido, padrón electoral, etc.

Por otro lado, el factor humano sin lugar a dudas, continuará siendo la parte más delicada; así que algunas de las tareas que deben ser asumidas por las empresas donde se decida integrar una cultura de seguridad y/o se implanten mecanismos sofisticados haciendo uso de tecnologías de punta que necesariamente impliquen un cambio en la forma de operar, deberán ser: involucrar a todas las áreas de la organización en los aspectos-misión de seguridad que se establezcan (desde directivos hasta operativos); concientizar a todos los involucrados dando a conocer los riesgos y sus consecuencias; brindar capacitación en el área; y con la finalidad de erradicar el miedo y la resistencia al cambio (asegurar la aceptación), persuadir al personal sobre las ventajas de las nuevas tecnologías que se pretenden implantar, entre otras cosas.

Respecto a las mejoras a realizar en el área de la Biometría por huella digital, consideramos que uno de los retos es el promover e impulsar el uso de estándares abiertos, con la finalidad de facilitar a las empresas, el acceso a este tipo de soluciones; permitiéndoles encontrar el verdadero sentido de su uso, y compartir de manera fácil y amigable las múltiples aplicaciones de software existentes.

Opinamos que el presente proyecto será del interés de la comunidad universitaria y lectores en general, pudiendo servir de incentivo para que cualquier otra persona continúe investigando sobre el tema; y así mismo, para el planteamiento de mejoras al desarrollo presentado, y quizás, muy particularmente a la creación de algoritmos más sofisticados para la extracción y comparación de puntos característicos de las huellas. La propuesta de utilizar nuevas tecnologías para llevar a cabo el proceso de autenticación biométrica como lo es hoy por hoy el ultrasonido, es otro aspecto que bien puede ser fuente de investigación y desarrollo.

Para finalizar, creemos que la Seguridad Informática incluyendo los servicios de Control de Acceso y Autenticación, deben ser considerados como elementos integrales inherentes al proceso de negocio de cada empresa; y no como elementos aislados. Lo anterior, si es que realmente se desea tener éxito en la misión.

ANEXOS

A. Manual de Usuario
B. Manual de Administrador
C. Detalle técnico del dispositivo lector de huella digital.
D. Requerimientos técnicos
E. Código fuente

ANEXO A.

Manual de usuario

El presente manual muestra la manera de acceder a la Intranet corporativa de la empresa. Para que los usuarios pueden obtener el acceso, el Administrador General del sistema, debió haber realizado de manera previa el proceso de registro de los datos de usuario y sus huellas, en el sistema. Si lo anterior se cumple, los pasos a seguir son:

1. Abrir el navegador Mozilla Nestcape o Mozilla FireFox.

Para acceder a la Intranet es necesario abrir un navegador, los cuáles pueden ser Mozilla Nestcape o Mozilla FireFox y teclear la siguiente dirección http://localhosts/bio/login.jsp , localhosts es la dirección ip o hostname del servidor web que tiene instalada la aplicación *Figura 1*

2. Autenticación en el sistema

Después de haber tecleado la dirección electrónica del paso anterior, se mostrará una pantalla como se muestra en la *Figura* 1,

El usuario debe seguir los siguientes pasos:

1. Dar click al botón <<*Entrar*>>

Después de lo cuál se mostrará la pantalla de la *Figura* 2

2. Colocar en el lector biométrico, el dedo de la huella que fue registrado por el Administrador General del sistema:

Figura 1. Pantalla de acceso de usuarios, donde se les solicita su huella dactilar para su autenticación ante el sistema.

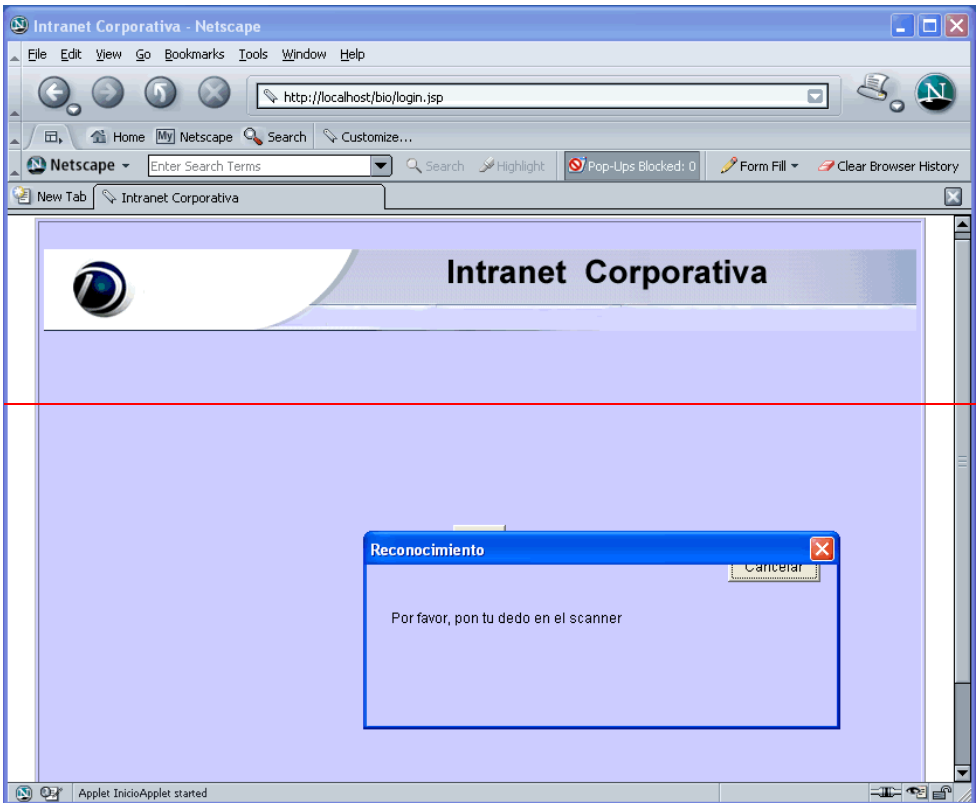


Figura 2. Pantalla donde el usuario posiciona su huella en el lector biométrico para acceder a la Intranet

3. Acceso a la Intranet

Si la autenticación del usuario fue exitosa, se mostrará la pantalla que se muestra en la *Figura* 3; en caso contrario, se mostrara la pantalla que se muestra en la *Figura 4*, después de lo cuál será enviado a la pantalla inicial de acceso.

Figura 3. Pantalla principal de la Intranet donde se muestra el nombre del usuario autenticado exitosamente, en el sistema.

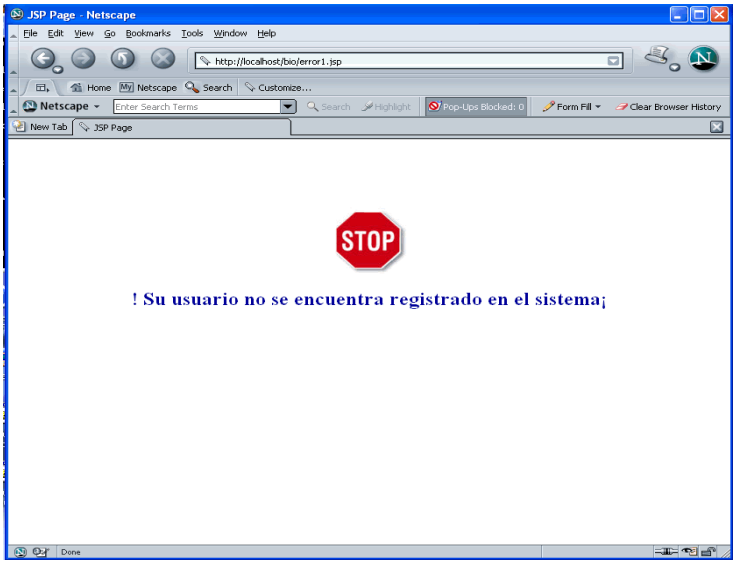


Figura 4. Pantalla de error, que es desplegada cuando la autenticación no es exitosa. El usuario que se está intentando acceder al sistema, no se encuentra registrado.

En caso de tener problemas para acceder a la Intranet, aún siguiendo los pasos citados en este manual, deberá dirigirse con el Administrador General del sistema para su solución.

ANEXO B.

Manual de Administrador

El presente manual muestra al Administrador General del sistema de autenticación biométrica vía web, la manera cómo debe de operar y configurar el sistema.

Prerrequisitos

El ambiente donde va a ser instalado el sistema debe de cumplir con los siguientes prerrequisitos.

Servidor web

- Apache 1.3.x en adelante
- Sunone Web Server 5.x en adelante

Contenedor de servlets y jsp's

- Tomcat 4.x en adelante
- WebSphere 5.1.x en adelante
- Weblogic 7.x en adelante
- SunOne Aplication Server

Sistema operativo

- Linux
- Windows
- AIX
- Solaris

Versión de Java

- JRE Versión 1.4 en adelante

Base de datos

- Informix
- MySql
- Oracle
- Db2

El servidor web, contenedor de servlets, la base de datos y configuración SSL deben estar configurados y funcionando. Dentro del paquete de instalación se proporciona el WAR de la aplicación, los scripts para la creación de la base de datos y las tablas y las librerías que se ejecutan en el cliente.

1. Configuración del sistema

a) **Creación de base de datos y tablas.**

A continuación se presentan los scripts para la creación de la base de datos y las tablas necesarias para el sistema. Estos scripts deben de ser ejecutados desde el ambiente de base de datos configurado.

En este manual se presentan los scripts de sql para la creación de base de datos y tablas.

Creación de base de datos:

```
Create database biometría
```

Creación de tablas:

Tabla de usuarios

```
create table usuario(
id_user int(11) NOT NULL DEFAULT 0 ,
nom varchar(30) ,
ap_paterno varchar(30) ,
ap_matreno varchar(30) ,
region varchar(10) ,
ubicacion varchar(80) ,
telefono varchar(10) ,
tipo_user varchar(15) DEFAULT "user" ,
activo int(11) ,
PRIMARY KEY (id_user),
KEY nombre(nom),
KEY activo(activo)
)
```

Tabla de plantillas

```
create table plantillas(
id varchar(32) ,
huella longblob ,
KEY id_huella(id)
)
```

Tabla de Administrador Maestro

```
create table adminmaster(
id_admin varchar(15) ,
password varchar(10) NOT NULL
)
```

b) Instalación del archivo WAR (web Archive) en el contenedor de servlets:

El WAR de la aplicación es un archivo comprimido tipo zip, el cuál contiene todos los jsp, servlets, bean's , jar's , imágenes y html's necesarios para que la aplicación web se ejecute. Dicho archivo debe ser instalado en el contenedor de servlets o servidor de aplicaciones, siguiendo los procedimientos correspondientes aplicables en cada uno de ellos.

A continuación se presenta el procedimiento de instalación del archivo war, en el contenedor tomcat 4.1.3.1.

Se teclea la dirección http://localhost/manager/html, después de lo cuál, el sistema solicitará la autenticación del usuario admin, mismo que fue previamente configurado durante la instalación. Posterior a esto, la pantalla que se muestra, es la interfaz de administración del Tomcat y es aquí desde donde se instalará el WAR que contiene la aplicación como lo muestra la *Figura 1.*

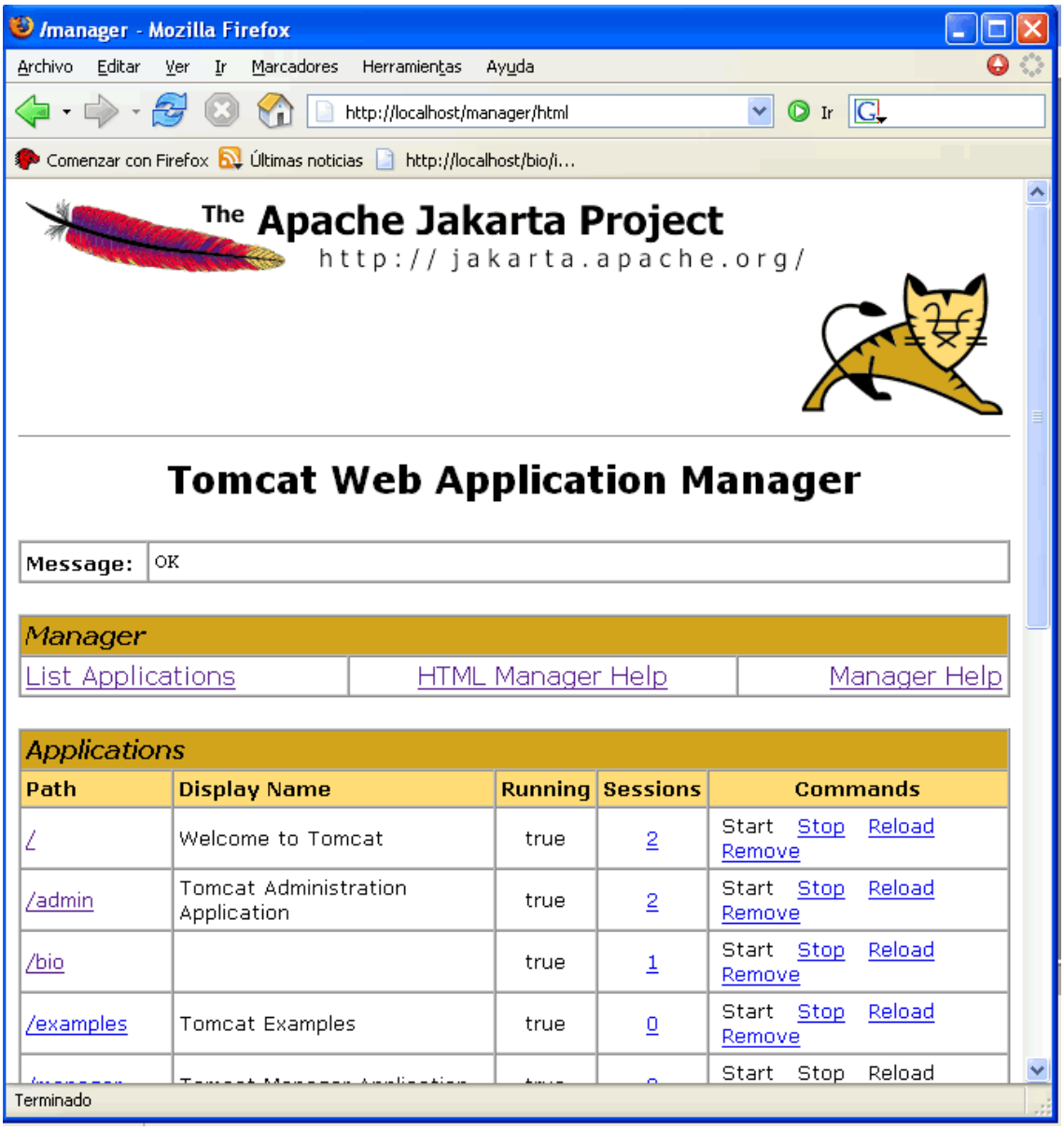


Figura 1. Pantalla de administración de aplicaciones del Tomcat.

Estando en la pantalla de administración, se posiciona en la opción "**upload a WAR file to install**" y se da click al botón "**Examinar**" para buscar el archivo WAR que contiene la aplicación. Después de seleccionado el archivo, se da click al botón "**Install**" para instalar la aplicación como se muestra en la *Figura* 2.

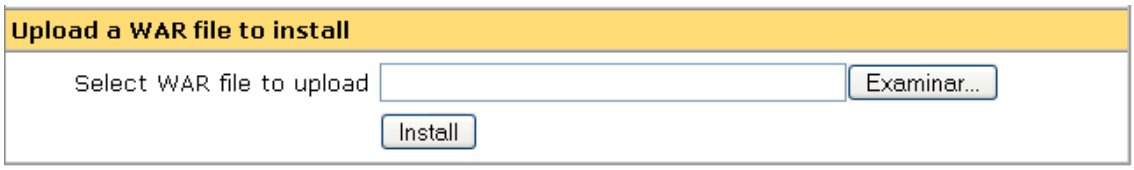


Figura 2. Interfaz de carga de archivos WAR.

c) Creación del usuario Administrador Maestro

Para inicializar nuestro sistema y poder empezar a utilizarlo, es necesario crear la cuenta de usuario Administrador Maestro, por medio de una sentencia de SQL. Dicha sentencia es la siguiente:

INSERT INTO administrador (id_admin., pwdadmin)
VALUES (54245,'123sdfe456)

Este usuario servirá para crear a los Administradores Generales que se requieran. Así mismo, los Administradores Generales serán los encargados de dar de alta a los usuarios comunes, y realizar el registro de sus huellas en el sistema, por medio de la interfaz de administración que en el transcurso de este manual se explica.

2. Función del Administrador Maestro

El Administrador Maestro es el encargado de crear al Administrador General del sistema. El Administrador Maestro no podrá crear usuarios normales ni registrar las huellas, pues esa será función exclusiva del Administrador General del sistema.

En la *Figura 3* se muestra la interfaz de acceso para el Administrador Maestro, donde debe de ingresar su <<username>> y <<password>>. Recordemos que este usuario fue creado previamente en el apartado de configuración del sistema. El URL a acceder, es el siguiente: http://localhost/bio/loginMaster.jsp

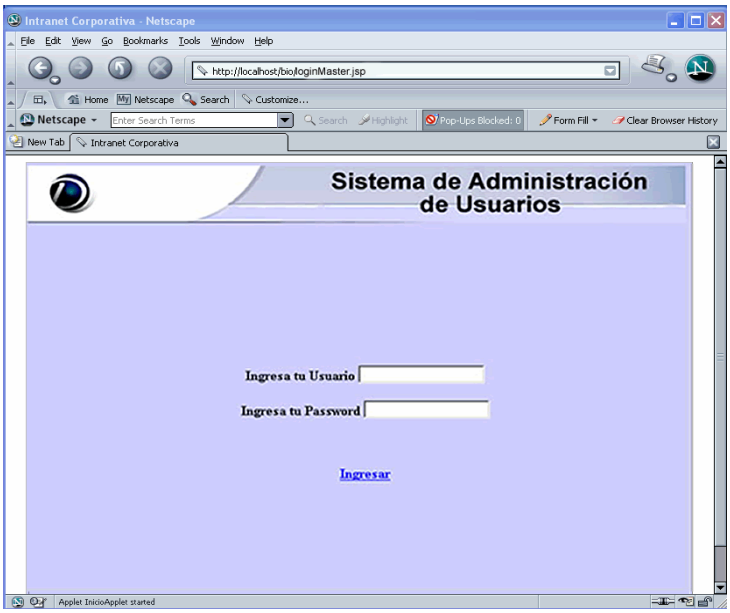


Figura 3. Pantalla de acceso del Administrador Maestro.

Al entrar al sistema se muestran las opciones a las cuáles tiene acceso el Administrador Maestro (*Figura 4*):

a) Alta administrador
b) Muestra administrador.

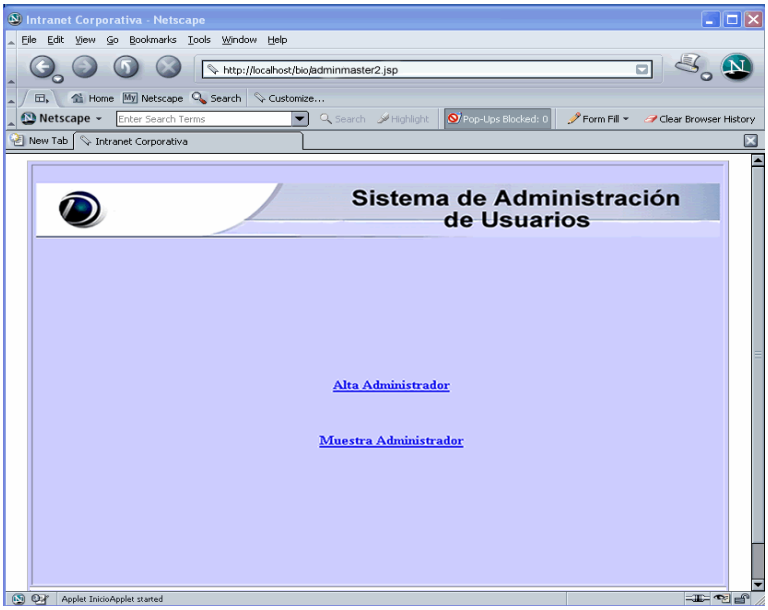


Figura 4. Pantalla de menú del Administrador Maestro.

a) Alta Administrador General

Esta interfaz muestra la plantilla que debe de llenarse para dar de alta al Administrador General. La información de registro que debe proporcionarse es:

Usuario: campo de tipo numérico que representa él numero de empleado.
Nombre: campo de tipo texto donde se debe de ingresar el nombre completo.
Paterno: campo de tipo texto donde se debe de ingresar el apellido paterno.
Materno: campo de tipo texto donde se debe de ingresar el apellido materno.
Región: campo de tipo texto donde se debe de ingresar la región a la cuál está adscrito el empleado.

Los campos que son opcionales a ser llenados, son los siguientes:

Ubicación: campo de tipo texto donde se debe de ingresar la dirección física del usuario.
Teléfono: campo de tipo texto donde se debe de ingresar el número de teléfono o extensión asignados.

Después de haber llenado los campos anteriores, el Administrador General deberá posicionar su huella en el lector biométrico para realizar el registro de ésta. Los datos y la huella del Administrador General, quedarán registrados en la base de datos, después de lo cuál podrá comenzar a dar de alta a los usuarios comunes del sistema. Lo anterior se muestra en la *Figura 5:*

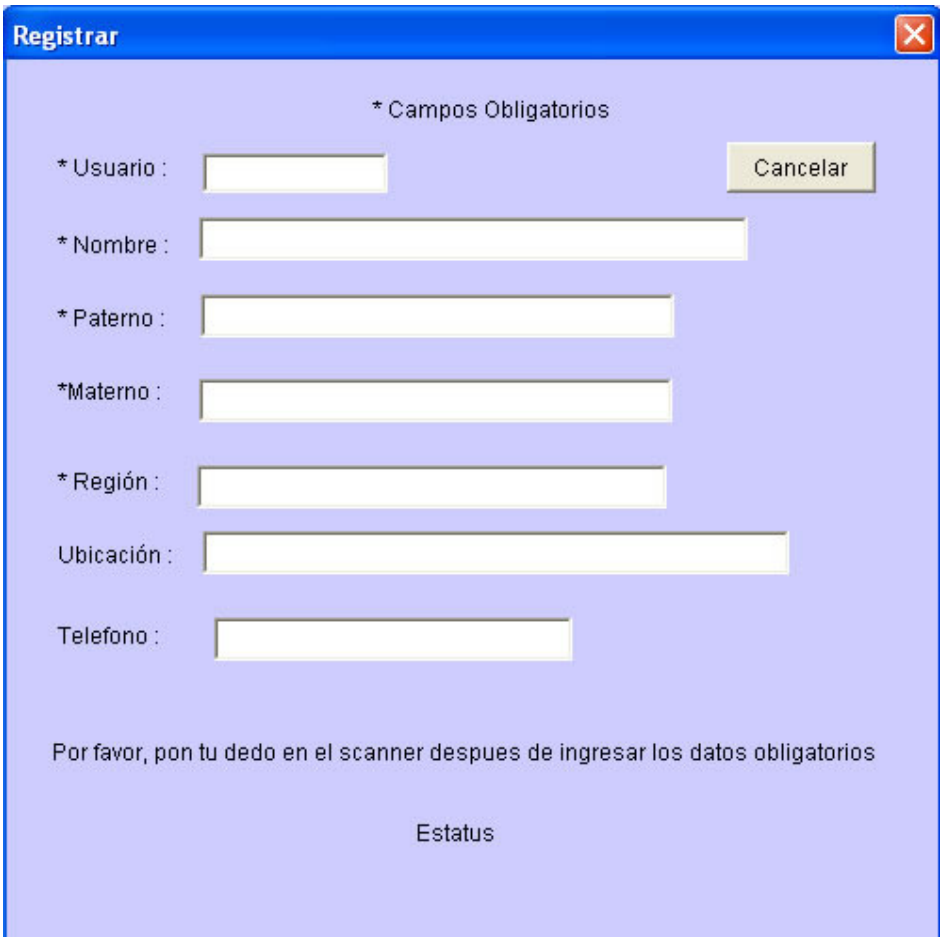


Figura 5. Pantalla de registro para el alta del Administrador General.

b) Muestra Administrador General

Esta interfaz muestra las opciones:

a) Baja administrador
b) Modificar administrador

Al pulsar los botones respectivos se accede a las opciones y se puede dar de baja al Administrador General o modificar los campos de su registro. Esto se muestra en la *Figura 6*:

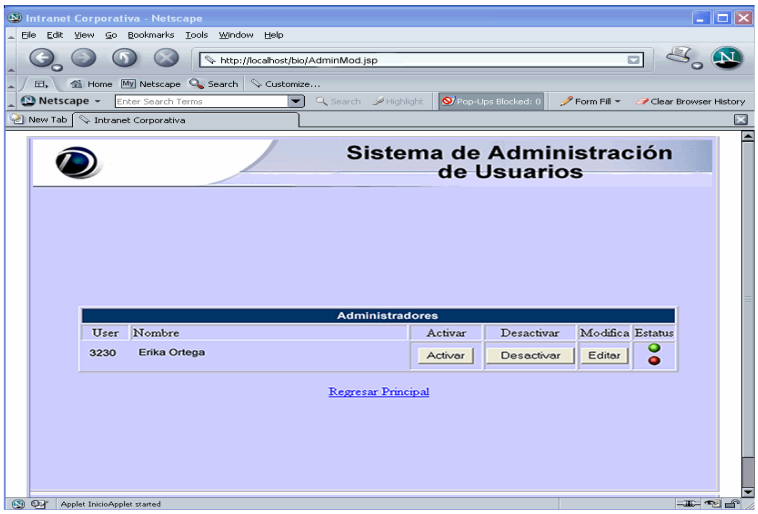


Figura 6. Pantalla de consulta de Administrador General

3. Función de Administrador General

El Administrador General es el encargado del manejo de los usuarios, registro de sus datos y sus huellas, modificación y eliminación de los mismos.

La interfaz de acceso para el Administrador General se muestra en las *Figuras 7 y 8.* El URL a acceder, es el siguiente: http://localhost/bio/loginAdmin.jsp

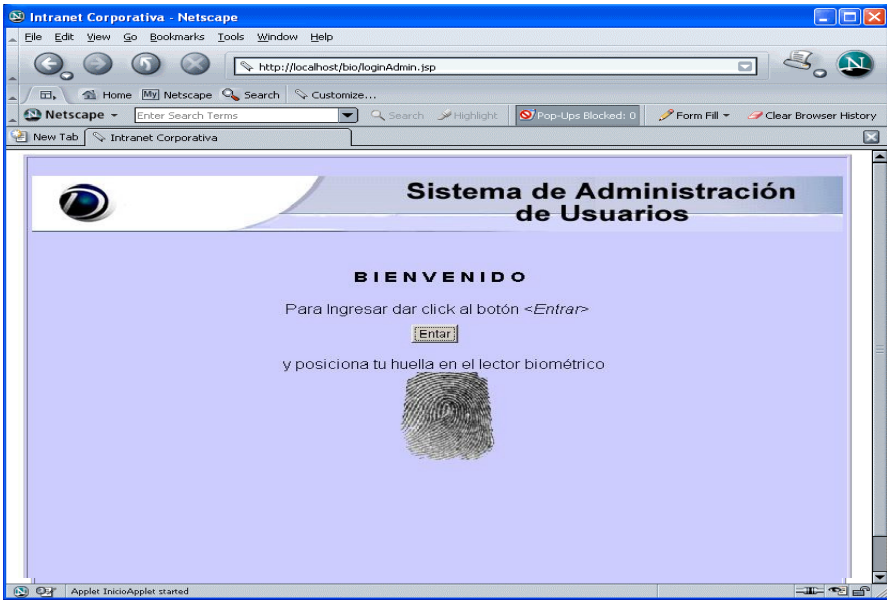


Figura 7. Pantalla de acceso del Administrador General, donde se solicita su huella dactilar para su autenticación ante el sistema.

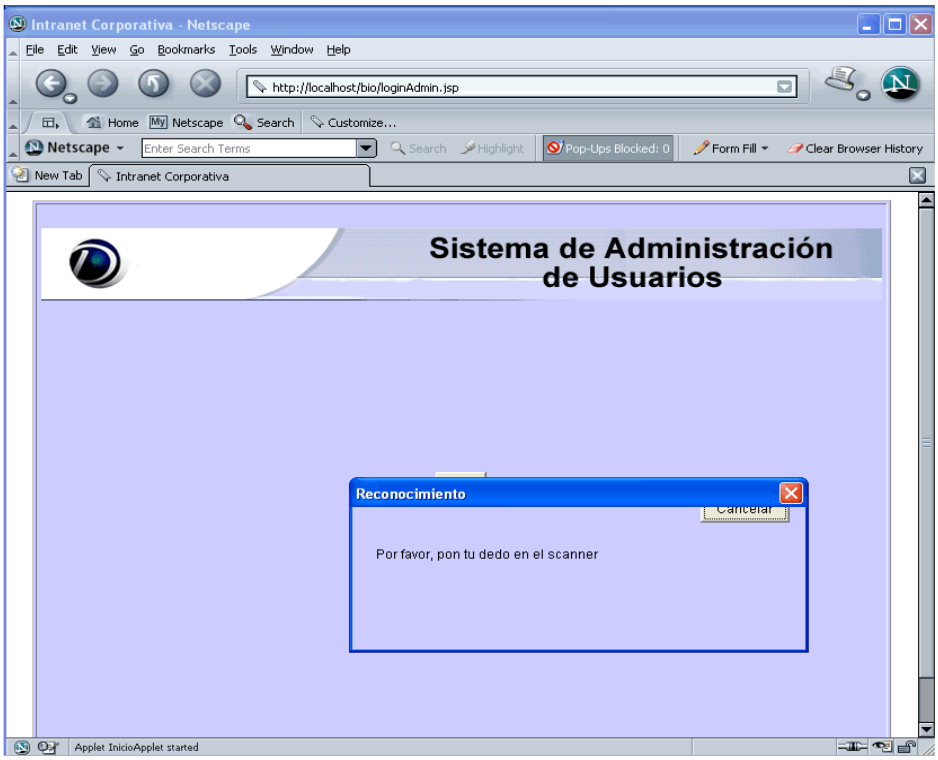


Figura 8. Pantalla donde el Administrador General, posiciona su huella dactilar para su autenticación ante el sistema

Al ingresar al sistema, el Administrador General tendrá 2 opciones (Ver *Figura 9*):

a) Alta usuarios
b) Modifica usuarios

Figura 9. Pantalla de menú del Administrador General.

a) Alta de usuarios

Esta interfaz tal y como se observa en la *Figura 10*, muestra la plantilla que debe llenarse para dar de alta a un usuario.

Al ingresar a la opción Alta Usuario, se deben llenar todos los campos marcados como obligatorios, mismos que se citan a continuación:

Usuario: campo de tipo numérico que representa él numero de empleado.
Nombre: campo de tipo texto donde se debe de ingresar el nombre completo.
Paterno: campo de tipo texto donde se debe de ingresar el apellido paterno.
Materno: campo de tipo texto donde se debe de ingresar el apellido materno.
Región: campo de tipo texto donde se debe de ingresar la región a la cuál está adscrito el empleado.

Los campos que son opcionales a ser llenados son los siguientes:

Ubicación: campo de tipo texto donde se debe de ingresar la dirección física del usuario.
Teléfono: campo de tipo texto donde se debe de ingresar el número de teléfono o extensión asignados.

Después de haber llenado los campos anteriores, el usuario deberá posicionar su dedo en el lector biométrico, para realizar el registro de su huella en el sistema. Los datos y su huella quedan registrados en la base de datos, los cuáles serán de utilidad, al momento que el usuario desee autenticarse en el sistema, para acceder a la Intranet.

Figura 10. Pantalla de alta de usuarios.

b) Modifica usuarios

En esta interfaz muestra las siguientes opciones:

Muestra usuarios
Activación usuarios.
Desactivación usuarios.
Modificación usuarios.

Lo expuesto anteriormente se muestra en la *Figura 11*:

Figura 11. Pantalla lista de usuarios, y las opciones para activación, desactivación y/o modificación.

Muestra usuarios

Muestra usuarios como se muestra en la *Figura 12*, es la interfaz que despliega la información contenida en el registro del usuario. Para acceder a esta opción es necesario dar click al link del usuario.

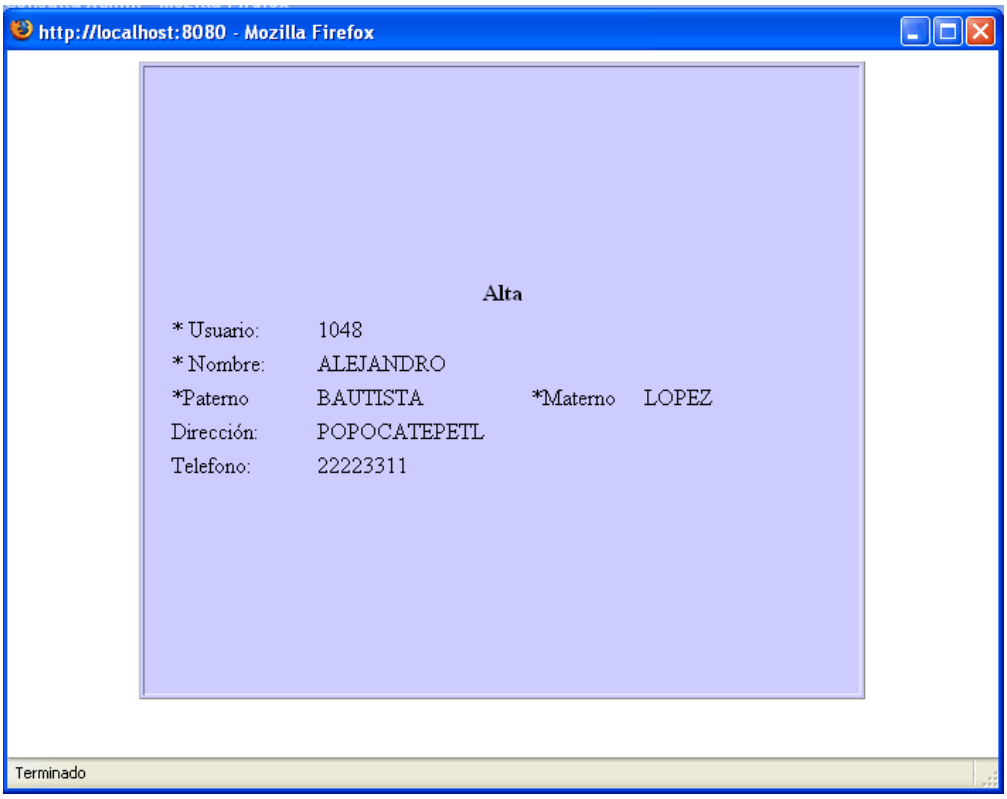


Figura 12. Pantalla muestra usuarios.

Activación usuarios

El botón de activación de usuario, solo se mostrará en los usuarios que aún no han sido activados. En los usuarios que ya se encuentran activos, dicha opción no se muestra.

Al pulsar el botón *Activar*, se activará al usuario para que tenga acceso a la Intranet y se desplegará una ventana como se muestra en la *Figura 13,* indicando el estado de la operación.

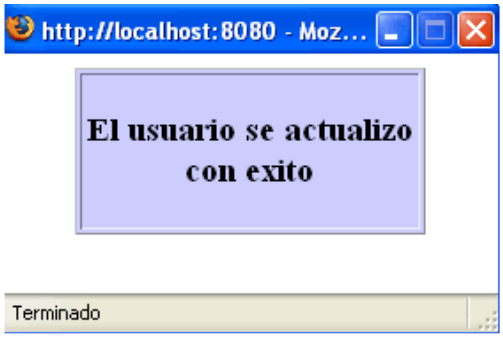


Figura 13. Pantalla de estado de la operación.

Desactivación usuarios

El botón de desactivación de usuario, solo se mostrará en los usuarios que se encuentran activos. Las cuentas de usuario que ya se encuentran en estado desactivo, no se muestra dicho botón.

Al pulsar el botón *desactivar*, el registro del usuario seleccionado quedará bloqueado; dejando de tener por lo tanto, acceso a la Intranet.

La *Figura 14* indica el estado de la operación.

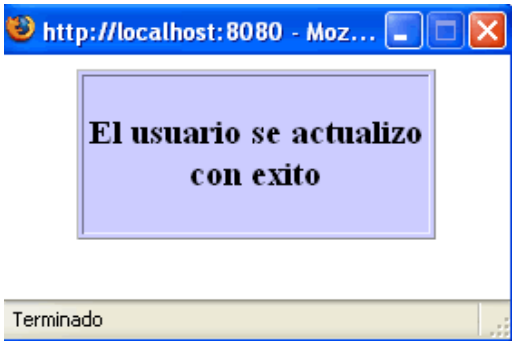


Figura 14. Pantalla de estado de la operación

Modificación usuarios

Al pulsar este botón se puede acceder a la plantilla de registro y efectuar las modificaciones requeridas a los datos del usuario y su huella. La interfaz se muestra en la *Figura* 15.

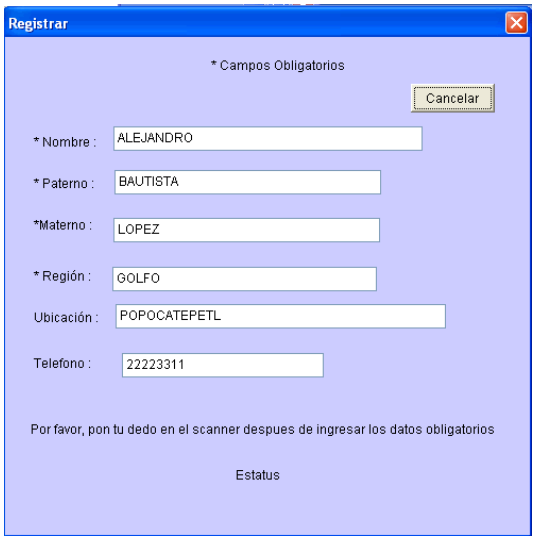


Figura 15. Pantalla de modificación de datos de los usuarios

ANEXO C.

Descripción técnica del Dispositivo Biométrico de Huella Digital

Figura 60. Scanner UareU 2000 Standard

Nombre del dispositivo lector de huella digital: Scanner UareU 2000 Standard
Fabricante: Digital Persona Inc. (http://www.digitalpersona.com)
Resolución: 500 dpi
Tamaño: 54x65x27 mm.
Área de captura de imagen: 13x18 mm
Temperatura operación: +5ºC..+35ºC (+40ºF..+95ºF)
Sistemas operativos soportados: MS Windows (Win95, Win98, WinME, WinNT 4.x, WinXP, Windows2000).
Tipo de conexión: Vía Puerto USB
Motor de identificación de huella dactilares utilizado: Verifinger 4.2 [1](http://www.ex-cle.com/ESSdkVf.htm)
Requerimientos de PC para su operación: Pentium 500MHz o superior.
Motor de identificación de huellas dactilares: Verifinger 4.2
Modo de comparación: 1:1 y 1:N
Velocidad de comparación de hasta 30000 huellas por segundo.
Requerimientos de memoria: 512 Kb
Compañía proveedora del motor de identificación de huellas: Neurotechnologija Ltd. (Lithuania)

---

[1] Verifinger se encuentra disponible como SDK (software Development Kit) y como código fuente para MS Windows, Windows CE 3.0 y Linux, para aquéllos que deseen obtener información acerca del algoritmo de reconocimiento.

El código fuente de VeriFinger está escrito en ANSI C bien estructurado y documentado. La documentación del código fuente principal se encuentra en “código fuente y descripción del algoritmo” con la descripción del código, las técnicas de optimización, la representación matemática de la función y los ejemplos de operaciones, etc.

El scanner U.are.U 2000 contiene un sensor que captura automáticamente la imagen y la envía a la PC por una interfaz USB (Ver *Figura 61*). Los componentes electrónicos del scanner controlan la captura de la imagen, la calibración y la interfaz Plug-n-Play USB.

Este dispositivo puede operar con el motor de identificación de huellas dactilares VeriFinger 4.2 (requiere el SDK Standard o SDK Extendido), desarrollado por Neurotechnologija Ltd., el cuál está destinado a desarrolladores e implementadores de sistemas biométricos concretos.

VeriFinger es uno de los más poderosos motores de reconocimiento de huellas dactilares. Este asegura alta confiabilidad en el registro <<enrollment>> e identificación de huellas dactilares, pudiendo operar en los modos de comparación 1:1 y 1:N, a una velocidad de comparación de hasta 30000 huellas por segundo, requiriendo sólo 512 Kb de memoria.

Dentro de sus características más sobresalientes se tienen:

Confiabilidad:

Considerando que usualmente la calidad de reconocimiento de los algoritmos es expresada por las curvas de recepción operativa (Receiver Operating Curves- ROC), que muestran la relación del falso rechazo con la falsa aceptación; de acuerdo a la competencia internacional de verificación de huellas dactilares celebrada en el año 2002[2], los resultados obtenidos en términos de Receiver Operating Curves (ROC) a partir de cuatro bases de datos estándar, indican que la confiabilidad de VeriFinger para diferentes bases de datos es igual o mejor a los resultados obtenidos por otros participantes en la competencia.

VeriFinger 4.2 fue probado con conjuntos de huellas dactilares de muchos Scanners. Los resultados más interesantes son los obtenidos a partir de bases de datos estándar.

A continuación, en la *Figura 62* se presentan las ROC obtenidas de las bases de datos utilizadas en la competencia de verificación de huellas dactilares (FVC):

[2] FVC 2000 fue la primera competencia internacional de algoritmos de verificación de huellas dactilares. La última sesión de evaluación tuvo lugar en abril de 2002 y los resultados de los 31 participantes fueron presentados en la 16ava ICPR (Conferencia Internacional de Reconocimiento de Patrones). Esta iniciativa es organizada por D. Maio, D. Maltoni, R. Cappelli de Biometric Systems Lab (Universidad de Bologna), J. L. Wayman del U.S. National Biometric Test Center (Universidad del estado de San Jose) y A. K. Jain del the Pattern Recognition and Image Processing Laboratory de la Universidad del Estado de Michigan.

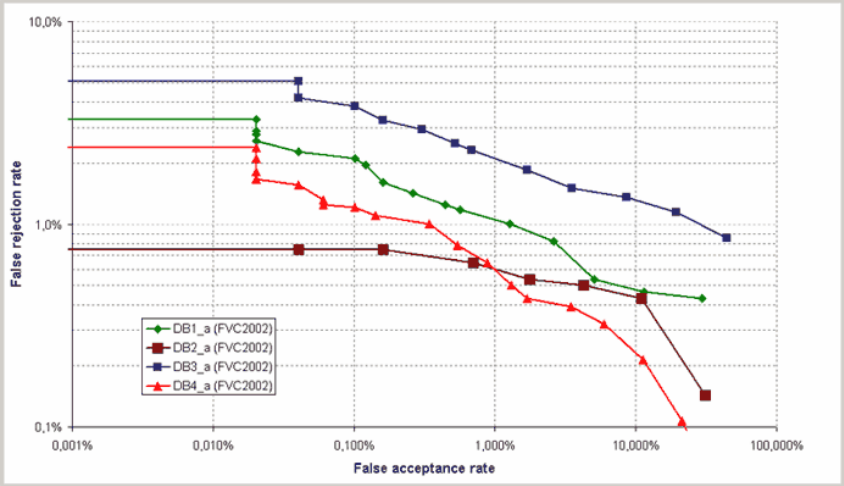


Figura 61. Tasas de Falso Rechazo y Falsa Aceptación obtenidos por Verifinger.

En la gráfica se puede observar que el falso rechazo de VeriFinger es sólo del 1,5 al 6 %, con una falsa aceptación de 0,001%.

Para las diferentes bases de datos de la FVC los resultados obtenidos por VeriFinger son iguales o superiores a los del resto de los participantes. En aplicaciones reales los resultados son aún mejores ya que en la FVC no se permitió incluir la generalización de características. Estos parámetros fueron obtenidos con el sistema corriendo bajo un procesador Pentium IV a 1.8 Ghz.

Velocidad: El tiempo de enrolamiento o carga de las huellas es entre 0,2 y 0,5 segundos; VeriFinger puede comparar 30000 huellas por segundo en modo de identificación 1:N.

Memoria Requerida: El tamaño del código de Verifinger es cercano a los 180kb (dependiendo de la plataforma y las opciones de cada compilador). Los vectores de datos utilizados por VeriFinger solo utilizan 280kb de memoria haciéndolo así, fácilmente implementable en sistemas con poca memoria y hardware de bajo costo.

Características del algoritmo:

Como se ha mencionado, un factor importante en el proceso de reconocimiento de huellas, lo representan los algoritmos para el procesamiento confiable de la imagen de la huella, eliminación del ruido, extracción de minutiaes, tolerancia a rotación y traslación, etc. Para lo cuál, estos algoritmos deben correr tan rápido como sea posible para garantizar su uso confortable en aplicaciones con alta demanda.

El algoritmo de reconocimiento de huellas VeriFinger utiliza un esquema de identificación a partir de un conjunto de puntos específicos de la huella <<minutiaes>>, empleando una serie de soluciones algorítmicas originales para la mejora del rendimiento y la confiabilidad de la metodología. Para ello, entre otros recursos utiliza:

Utiliza un algoritmo de filtrado de imagen que permite la eliminación de ruidos, ruptura de crestas y crestas cortadas, y extrae minutiaes confiables aún desde imágenes de baja calidad, con un tiempo de procesamiento de entre 0,2 y 0,5 <<tiempos tomados con el sistema corriendo bajo un procesador Pentium III a 733 Mhz.>>

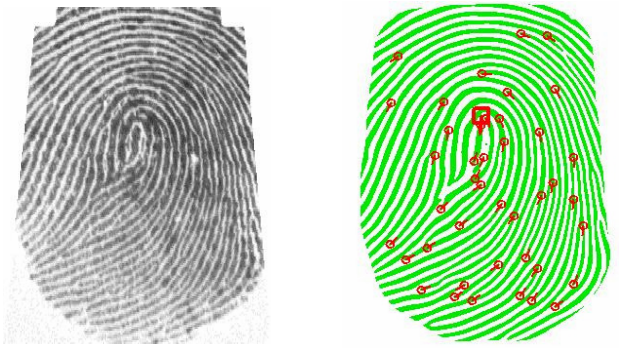


Figura 62. Imagen original de la huella Vs. Imagen luego del filtrado y procesamiento por VeriFinger. Se puede observar la posición y dirección de la minutiae marcada por círculos rojos y líneas.

VeriFinger puede ser utilizado en verificación 1:1 o reconocimiento 1:N
VeriFinger es ampliamente tolerante a traslación y rotación de las imágenes de huellas. Esta tolerancia es alcanzada usualmente utilizando un algoritmo basado en transformación Hough, pero este método es bastante lento y poco confiable. VeriFinger utiliza un algoritmo original que permite comparar 30000 huellas por segundo e identificar huellas aún si están rotadas o trasladadas aún con sólo 5 a 7 minutiaes similares. Usualmente dos huellas del mismo dedo contienen 20 a 40 minutiaes similares.

VeriFinger no requiere la presencia del centro o delta de la huella en la imagen, y puede reconocer una huella a partir de cualquier parte de la misma. De todas maneras si estas características están presentes, la utiliza para un reconocimiento más confiable.

En VeriFinger toda la base de datos está preordenada utilizando ciertas características globales. La comparación es realizada primero contra las huellas almacenadas que contienen similares características globales a la que se está evaluando. Si la comparación contra este grupo no arroja resultados positivos, el próximo registro con características globales similares es seleccionado, y así continúa hasta que el reconocimiento es positivo o hasta que se llega al final de la base de datos. En la mayoría de los casos hay una alta probabilidad de que el reconocimiento exitoso se alcance al comienzo de la búsqueda. Como resultado, la cantidad de comparaciones requeridas para alcanzar un reconocimiento exitoso decrece drásticamente, y consecuentemente, la velocidad de respuesta efectiva es mayor.

VeriFinger registra <<enrola>> tres imágenes de la misma huella. Cada imagen es procesada y sus características son extraídas. Luego las tres colecciones de características son analizadas y combinadas en una sola colección de características combinadas, que es la que se escribe en la base de datos. De esta manera la minutiae enrolada es más confiable, y la calidad y confiabilidad del reconocimiento es mayor.

ANEXO D.

Requerimientos Técnicos

REQUERIMIENTOS TÉCNICOS DE HARDWARE Y SISTEMA OPERATIVO DEL SERVIDOR.

La parte del servidor del sistema desarrollado puede operar con el hardware y software que a continuación se cita:

Servidor web

- Apache
- Sunone web server

Contenedor de servlets y Jsp's

- Tomcat
- WebSphere
- Weblogic
- SunOne Aplication Server

Sistema operativo

- Linux
- Windows
- AIX
- Solaris
- JRE Versión 1.4 en adelante

REQUERIMIENTOS TÉCNICOS DE HARDWARE Y SISTEMA OPERATIVO DEL CLIENTE.

La parte del cliente del sistema desarrollado, puede operar con el hardware y software que a continuación se cita:

Sistema operativo de usuario

- Windows 98, Windows 2000 o Windows XP
- JRE Versión 1.3.1_02

Browsers

- Netscape 7 en adelante

ANEXO E.

Código Fuente

REFERENCIAS

LIBROS

[1] Dr. Giovanni Manunta. ***Seguridad: Una Introducción.*** Consultor y profesor de Seguridad de Cranfield University. Revista virtual Seguridad Corporativa. http://seguridadcorporativa.org

[2] Ampara Fúster Sabater. ***Técnicas Criptográficas de Protección de datos***. Edit. Alfaomega 2ª. Edic. 2001. Traducido al Español.

[3] Davide Maltoni. D. Maio, A.K. Jain, S. Prabhakar. ***Handbook of Fingerprint Recognition.*** New York, 2003

[4] David Zhang. ***Biometric Solutions for Authentication in an E-world***. Universidad Politécnica de Hong Kong. Kluwer Academic Publishers. 2002.

[5] John Chirillo-Scott Blaud. ***Implementing Biometric Security CISSP***. Wiley Publishing, Inc. Indianapolis, Indiana. 2003

[6] Craig Larman. ***Uml y Patrones*****.** Prentice Hall**.** México. 2003

[7] UNAM. ***Diplomado de Seguridad Informática.*** Documentación. México. 2003.

[8] Neurotechnologija Ltd. ***Documentación técnico-funcional del Verifinger 4.2 SDK.*** 1998-2003 (http://www.ex-cle.com/ESSdkVf.htm)

[9] Francisco Javier Ceballos. ***Interfaces gráficas y aplicaciones para Internet***. Edit. Alfaomega. 3ª. Edic. Méx. 2003

[10] Chavarría Olarte, Marcela. ***Orientaciones para la Elaboración y Presentación de Tesis***. Edit. Trillas. México. 1993.

ARTÍCULOS, REVISTAS Y PUBLICACIONES

- Netmedia Publishing. ***En la Línea Enemiga.*** Revista B:Secure. Empowering Busines Continuity**.** Febrero 2006:26 **http://www.bsecure.com.mx**

- Netmedia Publishing. ***Bajo Acecho.*** Revista B:Secure. Empowering Busines Continuity**.** Marzo 2006:27**: http://www.bsecure.com.mx.**

- Arturo García Hernández. ***Seguridad Informática***. Presentación. Grupo de Seguridad Informática del Banco de México. 2002

- Hyldeé M. Ibarra Naranjo, José A. Mañas Argemí. ***RBAC: Alternativa actual para la realización de control de accesos a gran escala***. Presentación. Universidad Politécnica de Madrid España. Dep. Ingeniería en sistemas Telemáticos. 2003

- Jose Anibal Barahona ***Comparación de plantillas de huella digital basadas en minutiaes Vs. basadas en Patrones***. Neo Tec. Mayo 2002.

- Cristina Muñoz. ***Sistema de Reconocimiento Digital***. PC Plus. Marzo 2000

- Manuel A. Delgado Tenorio. ***Introducción a la autenticación biométrica.*** http:// www.imarketing.es/. México. 2003

- Miguel Glz. ***El precio de la Seguridad***. La Opinión. 14 Sep. 2003.

- Joaquín Glz. Rdz. ***Identificación Biométrica***. CSIC (Consejo Superior de Investigaciones Superiores). Profesor titular del Área de tratamiento de Voz y señales del Dpto. Ing. Audiovisual y Comunicaciones de la EUIT telecomunicación de la Universidad Politécnica de Madrid. 1997-2000

- Oscar Cánovas Reverte. ***Las Claves criptográficas.*** CSIC (Consejo Superior de Investigaciones Superiores). 2002

- Jordi Herrera Joancomarti. ***Criptografía de Clave pública***. CSIC (Consejo Superior de Investigaciones Superiores). Licenciado en Matemáticas por la UAB (Universidad Autónoma de Barcelona). 1997-2000.

- Gonzálo Álvarez Marañón. ***Secure Socket Layer (SSL)***.CSIC (Consejo Superior de Investigaciones Superiores). 1997-1998

- Gonzálo Álvarez Marañón. ***Seguridad en Java.*** CSIC (Consejo Superior de Investigaciones Superiores). 1997-1999

- Gonzálo Álvarez Marañón. ***Acceso a Base de Datos***. CSIC (Consejo Superior de Investigaciones Superiores).1997-2002

- José Aníbal Barahona. Neo Tec***. Los Biométricos y la exactitud de la plantilla***. Abril 2002. “Payroll Accuracy: Biometrics Make the Dream A Reality”.

- José Aníbal Barahona. ***Conveniencia Vs. Seguridad.*** Neo Tec. Abril 2002.

- José Aníbal Barahona. ***Comparación de plantillas de huella digital basadas en minutiaes Vs. basadas en patrones.*** Neo Tec. Mayo 2002.

- Guido Gabriel Gómez Medina. ***Introducción a los biométricos***. Neo Tec. May.2002.

- Virginia Espinosa Duró. ***Evaluación de Sistemas de Reconocimiento Biométrico***. Departamento de Electrónica y Automática Escuela Universitaria Politécnica de Mataró. Adscrita a la UPC. Mataró (Barcelona). Marzo 2001.

- Roberto Gómez. ***Engañando a los Sistemas Biométricos***. Agosto 2003.

- Sreekanth Malladi, Jim Alves-Foss. Center For Secure and Dependable Systems. University of Idaho. Moscow.
  Sreenivas Malladi Satyam Computers Private Ltd. Hyderabad. ***Preventing Guessing Attacks Using Fingerprint Biometrics.*** India 2002.

- Saul Prabhakar (Digital Persona), Sharath Pankanti (IBM T.J. Watson Reserch center), Anil K. Jain (Michigan State University). ***Biometric Recognition: Security and privacy Concerns.*** Abril 2003. IEEE Security & privacy.

- James L. Wayman. ***National Biometric Test Center Collected Works***.. San José State University, CA. August 1997-2000.

- Sharath Pankanti (IBM T.J.) NY, Salil Prabhakar + (Digital Persona Inc.) CA., Anil K. Jain. (Michigan State University, MI). ***On the Individuality of Fingerprints.*** E.U. 2002

  Nota: An earlier version of this paper apperead in the proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), pp. 805-812, hawaii, December 11-13, 2001. + Corresponding Author.

- Salil Prabhakar, Anil K. Jain, Sharath Pankanti. ***Learning Fingerprint Minutiae Location and Type.*** * Nota: An earlier version of this papre was presented at the 15th International Conference on Pattern Recognition (ICPR), Barcelona, September. 3-8, 2000.

- A.K. Jain, Salil. Prabhakar, A. Ross. ***Biometrics_Bases Web Access.*** Department of Computer Science and Engineering Michigan State University, [jain, prabhakar, rossrun]@cse.msu.edu

- Manuel José Lucena López. ***Criptografía y Seguridad en Computadores***. Dpto. de Informática Universidad de Jaén. 3ª. Edic. (Versión 2.10). España. Mayo 2003. Mlucena@ujaeh.es

- Colin Soutar Bioscrypt. ***Biometric Standards***. Presentación. CTO Bioscrypt Inc. Canadian National Summit on Biometrics Technology. Julio del 2002.

- Fernando Podio. ***Accelerating the Development of Biometric Standards.*** Presentación. NIST/ITL, CISD Co-chair, Biometric Consortium. 2003.

- M. Paul Collier. ***Biometrics_Standards Activities***. Presentación. National Defense Industrial Association 19th Annual Security Symposium. Reston, Virginia. June 19, 2003. Executive Director. The Biometric Fundation. Washington, DC.

- Ruy Campos Dugone. ***El impacto de la Seguridad Estratégica en el cuadro de resultados***. Presentación. A4E- Defense Corporation. Jun 2003.

- Organización Vertix Telemática. ***Seguridad Informática.*** Presentación. WALC Sep. 2003.

ORGANISMOS

- www.ibia.org/formats.htm. IBIA (Internacional Biometric Industry Association).

- www.bioapi.org BioAPI™ Consortium

- www.biometricfoundation.org The Biometric Foundation. Washington, D.C.

- www.ansi.org ANSI (American National Standards Institute). Instituto administrador y coordinador del sistema voluntario de estandarización del sector privado de Estados Unidos.

- http://www.nist.gov NIST (National Institute of Standards and Technology).

- http://www.nsa.gov:8080 NSA (National Security Agency).

- http://www.ncsa.uiuc.edu NCSA (National Computer Security Association).

- http://www.ii.uam.es/~abie/ Asociación de Biometría Informática Española
- http://www.ictnet.es/ICTnet/cv/comunidad.jsp?area=engInf&cv=biometrica Comunidad de Biometría

EMPRESAS

- http://www.necsam.com/idsolutions/products/Identification.cfm Nec Solutions America

- http://www.mitretek.org) Mitretek Systems y el scanner de huella digital Universal.

- http://ww.digitalpersona.com DigitalPersona y su Motor de Identificación de huellas dactilares Verifinger (Software UareU)

- http://ww.neurotechnologija.com/scanners.html NeoroTecnologija, Lithuania. Compañía enfocada principalmente al desarrollo de algoritmos y software identificación de tipo biométrico, tales como Kits de desarrollo (SDK's, EDKs, etc), y su compatibilidad con los Scanners biométricos: UareU, UareU 4000, UareU Keyboard, UareU Module, Verifier 300 Classic, Verifier 300 LC, FM 200, Tacoma CMOS, MBF 200, DFR-2090, TCRU1C, FX 2000, AES4000, AF-S2, LTT-C500, FirgerChip.

- http://www.biometriaplicada.com Biometría Aplicada. Empresa proveedora de software y HW de Identificación, librerías y código fuente para reconocimiento de huella digital y rostro. Único distribuidor autorizado de Neurotechnologija para México, y la única Premier Partner de Digital Persona fuera de Estados Unidos y Canadá.

- http://www.identix.com Identix - Fingerprint and Facial recognition.

- http://www.crossmatch.net Cross MATCH Tecnologies Inc. y el scanner Cross Match Verifier 300 LC

- http://www.biometrika.it/eng/index.html Biometrika srl y los scanners de huella digital FxLock, Fx2000, Fx3000 y Fx Integrator. Italia.

- http://www.biometricsdirect.com Biometrics Direct y el Scanner Precise Biometrics 100

- http://ww.fulcrumspi.com/verifinger.htm Fulcrum Strategic Partners, Inc. Fairfield, CA. Compañía enfocada a la consultoría, selección, integración y desarrollo de soluciones biométricas para operaciones de misión crítica.

- http://www.authentec.com AuthenTec, Inc. Empresa líder proveedora de sensores de huella digital para PC's, redes, PDA, control de acceso. Detalles sobre los Scanners AuthenTec AES4000 EntréPad (USB) y sensores AF-S2 .

- http://www.bergdata.com Bergdata. Empresa enfocada en el desarrollo y venta de dispositivos basados en huella digital. Creadora de la engine de identificación de huella digital **bdfis**- (Bergdata Firgerprint Indentification System) que soporta sensores de diferentes vendedores.

- http://www.biometricsys.ws Biometric Systems. Compañía establecida en Berlín, Alemania. Proveedora de productos de alta tecnología y soluciones en el área biométrica de huella digital para el control de acceso físico, sistemas de seguridad de TI, venta, consultoría, personalización, integración, capacitación soporte y servicios. Propietaria del engine BioUPI (Biometry Unit of Person Identification) para el reconocimiento de huella digital, y así mismo, de la aplicación FingerGina Login que permite proteger computadoras personales, workstation, notebook utilizando vía autenticación por huella digital.

- http://www.bioscrypt.com Bioscrypt Inc. Empresa líder en proveer avanzada tecnología de huella digital. Ofrece un rango amplio de opciones biométricas para el control de acceso a equipos, información, redes, etc., así como soluciones para la integración de aplicaciones biométricas en diferentes ambientes y plataformas, y algoritmos para la identificación de huellas.

DIRECCIONES WEB VARIAS

Nota: Por el continuo movimiento de las direcciones de Internet es posible que alguna de las enumeradas a continuación, no se encuentren disponibles.

- http://www.javahispano.org Java en Castellano
- http://www.mysql.com MySQL
- http://jakarta.apache.org Tomcat
- http://www.openssl.org Open SSL
- http://www.nist.gov/cbeff Página de información técnica sobre el standard CBEFF (Common Biometric Exchange File Format).
- http://www.Kriptopolis.com Sitio sobre Criptografía, noticias, artículos y foros de seguridad.
- http://www.iec.cisc.es/criptomicon Servicio ofrecido libremente desde el Instituto de Física Aplicada del CSIC (Consejo Superior de Investigaciones Superiores), donde se publican artículos sobre seguridad, Autenticación, Control de Acceso, Criptografía, Java, acceso a BD, etc.

- http://www.ex-cle.com/ESSdkVf.htm Detalle sobre el Motor de Reconocimiento de Huellas dactilares Verifinger 4.2. disponible como SDK y como código fuente para MS Windows, Windows CE 3.0 y Linux. Ex - Clé s.a. Paraguay

- http://cda.dummies.com/WileyCDA/DummiesArticle/id-1725.html Exploring access control for security + certification. Wiley, J. and Sons, Inc.;

- http://www.sesamo-arg.com/huellas.htm La tecnología del ultrasonido aplicada a scanners de huellas dactilares.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS