ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO PARA AUTENTICACIÓN, AUTORIZACIÓN, Y CONTEO (AAA) PARA EL CONTROL DE ASISTENCIA DE LOS EMPLEADOS DE LA ESCUELA POLITÉCNICA NACIONAL POR MEDIO DE HUELLAS DACTILARES

TOMO I

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

XAVIER EDUARDO ZURITA FRÍAS

DIRECTOR: ING. PABLO HIDALGO

Quito, Agosto 2004

DECLARACIÓN

Yo, Xavier Eduardo Zurita Frías, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Xavier Eduardo Zurita Frías

AGRADECIMIENTO

En primer lugar quiero dar gracias a mi Dios, por darme la oportunidad de culminar mi carrera y darme la fuerza para lograrlo.

A mis padres, Edgar Zurita y Nancy Frías por estar siempre pendientes de mi, ayudarme en mis estudios incondicionalmente y ser mis mejores amigos.

A mis abuelitos, por ser como mis padres, cuidarme y enseñarme a vivir.

A mis tíos: Wider, Vinicio y Miguel Frías por ser mis hermanos y compañeros en mi niñez y apoyarme en todo momento.

A mi tía Rita y a la familia Córdova Frías por recibirme como un miembro más de su hogar y darme la oportunidad de superarme en esta ciudad.

A todos mis hermanos y primos por ser mis fieles amigos, en especial a mi hermano Alejandro (Alex) y a mi primo Mauricio.

A mis amigos y compañeros de la poli: Washington, Fernando, Juan Carlos, Fabián, Patricio, Nancy, Adriana, Tannia y Nubia por ser el grupo más unido tanto para estudiar como para divertirse, de corazón gracias por estar estos años junto a mi.

A los ingenieros, Fernando Flores y Myriam Bautista por la inmensa ayuda prestada para la culminación de este proyecto y por ser además unos buenos amigos.

Al Ing. Pablo Hidalgo, por ser a más de un buen director un excelente amigo que me ayudado a formarme tanto personal como profesionalmente, mil gracias Inge.

A todos los amigos de mi Rosario querido, en especial a Cristian y Don César por estar siempre en las buenas y en las malas.

DEDICATORIA

A mis abuelitos, Fáber Frías y Elina Córdova por ser el pilar de mi ser y darme la oportunidad de surgir en la vida, y en especial a ti abuelito por ser la persona a la cual sigo de ejemplo, por enseñarme a vivir y a seguir mis ideales; gracias, porque por ustedes he llegado a ser lo que soy ahora.

A mi madre, Nancy por ser mi mejor amiga y confiar en mi en todo momento y ser la luz que guía mi camino.

A mi amor Blanca López, por ser el apoyo incansable de todos mis días, por quererme y amarme con esa fuerza que me da las ganas para esquivar los obstáculos que la vida me pone en delante.

Xavier

ÍNDICE

TOMO I

TOMO II

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación está destinado a implementar un Sistema de Control de Asistencia de los empleados de la Escuela Politécnica Nacional por medio de huellas dactilares.

Este trabajo contiene dos tomos: el primero abarca los cuatro capítulos de teoría, diseño e implementación del sistema, en tanto que el segundo presenta los seis anexos relacionados a este trabajo.

En el primer capítulo se describen los conceptos relacionados con la seguridad de redes y sistemas, se analizan las diferentes técnicas de acceso mediante parámetros biométricos comúnmente empleados en el mercado, en un enfoque práctico y de aplicación.

El segundo capítulo concentra un estudio exhaustivo del identificador biométrico de la huella dactilar y cómo se debería desarrollar un sistema de este tipo así como también se presenta un análisis de las ventajas y desventajas de usar este identificador como elemento de autenticación de personas.

En el tercer capítulo se detalla el desarrollo del Sistema de Control de Asistencia (SCA) para la Escuela Politécnica Nacional en base a un diseño en diagrama de bloques, se detalla sus partes y funcionamiento de acuerdo a la técnica biométrica utilizada, así como la programación del software en lenguaje de alto nivel que servirá como interfaz del usuario. Se evalúa el prototipo para analizar la viabilidad de su implantación en la Escuela Politécnica Nacional

El cuarto capítulo contiene conclusiones y recomendaciones del presente proyecto.

Los anexos contienen tópicos que ayudan a comprender la lectura del documento, además de incluirse el código fuente del *software* del sistema y una estimación de costos.

PRESENTACIÓN

La seguridad es un tema que ha tomado importancia relevante, por lo que cada día los sistemas de seguridad computacionales buscan técnicas de autenticación más fiables, una de ellas y hasta el momento la más confiable es el uso de la Autenticación Biométrica, técnica que analiza y mide ciertas características físicas y del comportamiento de un individuo para crear un identificador biométrico que garantiza la identificación y autenticación de un individuo que desee acceder a cierto lugar o información clasificada.

Estos sistemas se están difundiendo con rapidez y cada día son más las empresas que optan por esta solución a la seguridad, es por eso, se desea que en nuestro medio también se aplique estas técnicas, para ello se implementa un sistema seguro de control de asistencia para la Escuela Politécnica Nacional mediante el análisis de un parámetro biométrico tan común como lo es la huella dactilar.

La Escuela Politécnica Nacional se ha venido manejando con sistemas de control de asistencia electromecánicos y poco flexibles al momento de realizar reportes de asistencia y puntualidad, a más de no haber un control estricto de la persona que "timbra" para justificar su asistencia, es por ello que se automatiza este sistema con una sólida autenticación al momento de controlar la asistencia utilizando las ventajas que presenta la autenticación biométrica, mediante el registro de las huellas dactilares.

Para ello se analiza en detalle los pasos y herramientas que se necesita para implementar un sistema de autenticación de personas utilizando huellas dactilares; se implementa el prototipo basado en un lector de huellas dactilares y un *software* que facilita la administración de la información de la asistencia de los empleados de la Institución.

CAPÍTULO

1

DE AUTENTICACIÓN, AUTORIZACIÓN CONTEO BIOMÉTRICOS

CAPÍTULO 1

SISTEMAS DE AUTENTICACIÓN, AUTORIZACIÓN Y CONTEO BIOMÉTRICOS

1.1. GENERALIDADES DE SEGURIDAD [1] [3] [6]

1.1.1. ¿Qué es seguridad?

Un diccionario define seguridad como "la cualidad o el estado de estar libre de daño" y como "las medidas de protección tomadas contra espionaje, el sabotaje, el crimen, el ataque o la fuga", claro que esta definición es generalizada, pero da una visión de lo que debe evitarse en cualquier sistema seguro. Este concepto es aplicable a un sistema informático y de cierta manera se debe buscar que este sistema sea infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

En términos generales se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

¿Qué implica cada uno de estos tres aspectos?

1.1.1.1. La confidencialidad o Privacidad

Dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; es decir, la información debe ser vista y manipulada únicamente por quienes tienen el

derecho o la autoridad de hacerlo. Un ejemplo de ataque a la Privacidad es la Divulgación de Información Confidencial.

1.1.1.2. La integridad

Significa que los objetos solo pueden ser modificados (por modificar se entiende escribir, cambiar el estado, borrar y crear) por elementos autorizados, y de una manera controlada; es decir, la información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

1.1.1.3. La disponibilidad

Indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados, es decir, la información debe estar en el momento que el usuario la requiera. Un ataque a la disponibilidad es la negación de servicio (*Denial of Service* o DOS) o "indisponer" el servidor.

1.1.2. ¿Qué queremos proteger? [6] [7]

Los tres elementos principales a proteger en cualquier sistema informático son:

- *Software*
- *Hardware* y
- Los datos

Por *hardware* se entiende el conjunto formado por todos los elementos físicos (todo aquello que se puede tocar) de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, *diskettes*, etc.) o tarjetas de red. *Software* es el conjunto de programas lógicos que hacen funcional al *hardware*; todo el *hardware* que hay, no puede funcionar si no hay un programa o programas que hacen que opere de manera adecuada

tanto sistemas operativos como aplicaciones. En tanto que los datos corresponden al conjunto de información lógica que la maneja el *software* y el *hardware*, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorías de seguridad se habla de un cuarto elemento a proteger, los fungibles (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, cintas magnéticas, *diskettes*, etc), aquí no se considera la seguridad de estos elementos por ser externos al sistema de seguridad.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

Para hablar con propiedad contra cualquiera de los tres elementos descritos anteriormente (pero principalmente sobre los datos) se pueden realizar una multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Para una mejor comprensión se explicarán algunos conceptos básicos sobre el tema.

Amenaza se entiende por amenaza una condición del entorno del sistema de información (persona, entidad, evento o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad o disponibilidad).

Un Ataque es la realización de una amenaza. Una Protección son los controles físicos, mecanismos, políticas y procedimientos que protegen los activos o recursos del sistema.

Una Vulnerabilidad es el debilitamiento o ausencia de una protección en un recurso o activo.

Un Riesgo es una medida del costo de una realización de una vulnerabilidad que incorpora la probabilidad de éxito de un ataque. El riesgo es alto si el valor del activo vulnerable es alto y la probabilidad de éxito de un ataque es alta.

Las amenazas conllevan a un ataque y en general estos ataques se dividen en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación.

Interrupción.- Un ataque se clasifica como interrupción si hace que un recurso u objeto del sistema se pierda, quede inutilizable o no disponible. Éste es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento *hardware*, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

Intercepción.- Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto o recurso del sistema. Éste es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son interceptar una línea para hacerse de los datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

Modificación.- Si además de conseguir el acceso se consigue modificar o manipular el objeto o recurso, se dice que este ataque es del tipo modificación; algunos autores consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Éste es un ataque contra la integridad. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

Fabricación.- Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el `fabricado'.

En la figura 1.1 se muestran estos tipos de ataque de una forma gráfica.

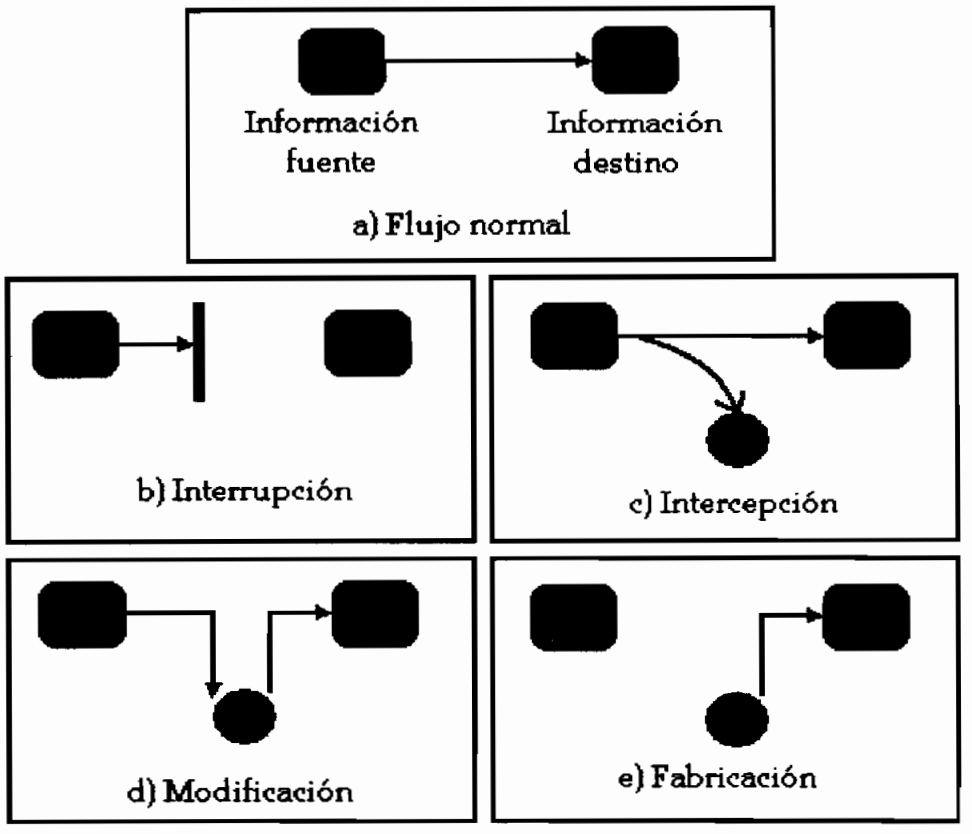


Figura 1.1: Tipos de ataques a un sistema informático. [7]

1.1.3. ¿De qué nos queremos proteger?

En la gran mayoría de publicaciones relativas a seguridad informática en general tarde o temprano se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. En general los atacantes pueden ser personas o elementos dependiendo de la orientación del tema; en este trabajo se hablará mucho sobre el acceso de las personas, siendo ésta una amenaza latente para un sistema informático sin dejar de lado que el sistema pueda verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas, catástrofes naturales, fenómenos naturales, etc.

A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a un sistema. No pretende ser exhaustiva, ni por supuesto una taxonomía formal; simplemente trata de proporcionar una idea acerca de qué o quién es una amenaza para un sistema.

1.1.3.1. Personas

La mayoría de ataques a un sistema van a provenir en última instancia de personas que, con o sin intención, pueden causar enormes daños, lo que a su vez provoca pérdidas tanto materiales como de información.

Generalmente se trataría de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno o algunos, de los riesgos lógicos de los que se hablará a continuación, especialmente de debilidades del *software* o del lugar donde se encuentra la información. Pero con demasiada frecuencia se suele olvidar que los piratas 'clásicos' no son los únicos que amenazan los equipos: es preocupante que mientras hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su *software*, restringiendo servicios, utilizando cifrado de datos, etc.), pocos administradores tienen en cuenta factores como la ingeniería social o el "basureo" a la hora de diseñar una política de seguridad.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para los sistemas; generalmente se dividen en dos grandes grupos: los atacantes **pasivos**, aquellos que fisgonean por el sistema pero no lo modifican (o destruyen), y los **activos**, aquellos que dañan el objetivo atacado, o lo modifican en su favor.

De esta forma se puede hablar de otra clasificación de los Ataques:

Ataques pasivos

Un ataque pasivo es aquel que no causa modificación o cambio en la información o recurso, son los más peligrosos ya que los fines que se alcanzan son más letales y beneficiosos para el que los comete. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitorea, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitoreados.

- **Control del volumen de tráfico** intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.

- **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos cuyo análisis se escapa del alcance de este estudio.

Ataques activos

Los ataques activos, son aquellos que producen cambios en la información o en el comportamiento del sistema.

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque pasivo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de dólares en la cuenta A" podría ser modificado para decir "Ingresa un millón de dólares en la cuenta B".

- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Generalmente los curiosos y los *crackers* realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si la red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

Entre los tipos de personas que pueden realizar estos ataques se tiene:

1.1.3.1.1. El personal de una empresa

Muchas de las veces no se toma en cuenta que el propio personal de una empresa viene a convertirse en una amenaza latente contra la seguridad de la propia organización; se supone un entorno de confianza, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, etc.) puede comprometer la seguridad de los equipos.

Los ataques pueden ser intencionados, en cuyo caso sus efectos son extremadamente dañinos ya que nadie mejor que el propio personal a cargo del sistema de la organización conoce mejor las debilidades del mismo, y no intencionados o accidentes causados por un error o por desconocimiento de las normas básicas de seguridad. Este último pudiera ser más común en una empresa en la que se interrelaciona confianza mutua, por ejemplo un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros.

1.1.3.1.2. Ex-empleados

Cuando una persona que ha trabajado en una empresa y abandona el entorno no por su propia voluntad y ésta no ha estado de acuerdo con la decisión, puede considerarse como un elemento potencialmente interesado en atacar algún sistema de dicha empresa. Generalmente, se trata de personas descontentas con la organización que pueden aprovechar las debilidades de un sistema, las cuales conocen perfectamente, para dañarlo como venganza por algún hecho que no consideran justo.

1.1.3.1.3. *Crackers*

Antes de tratar con este grupo de personas, se va a señalar la diferencia entre un *Hacker* y un *Cracker*:

> ***Hacker***.-Individuo que disfruta explorando los sistemas y programas, y que sabe cómo sacar el máximo provecho. Experto o que es especialmente hábil en el manejo de un sistema.
>
> ***Cracker***.-Individuo que rompe la seguridad de un sistema, se adentra en el terreno de lo ilegal. Individuo que se aprovecha de los conocimientos para hacer daño; *hacker* que responde al llamado del lado oscuro de lo ilegal.

Este tipo de personas tienen como objetivo típico los entornos de seguridad media, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor que se tiene muy en cuenta en ellas.

1.1.3.1.4. Curiosos

El instinto natural de las personas hace que deseen conseguir mayor privilegio que el que tienen referente a una red o sistema de información, intentando acceder a sistemas a los que oficialmente no tienen acceso, haciendo de este grupo de personas una amenaza inminente grande en cualquier organización.

1.1.3.1.5. Terroristas

Por `terroristas' no se debe entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de ficheros de un servidor que alberga páginas *web* de algún grupo religioso, entre otros.

1.1.3.1.6. Intrusos remunerados

En este caso los terroristas buscan hacer daño para su propia satisfacción. Imagínese este tipo de personas, a las cuales a cambio de destruir, robar, adulterar información se las paga, es el grupo de atacantes de un sistema más peligroso, aunque el menos habitual en redes normales; suele afectar más a las grandes empresas o a organismos de defensa. Podría decirse que son delincuentes informáticos con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, generalmente son pagados por terceras personas. Estas terceras personas suelen ser de una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los

mejores en su especialidad, y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance.

Aunque como se ha dicho los intrusos remunerados son los menos comunes en la mayoría de situaciones, en ciertas circunstancias pueden aprovechar las redes como plataforma para atacar otros organismos, que vendría a ser una situación aún más grave para la seguridad.

1.1.3.2. Amenazas lógicas [13]

En las 'amenazas lógicas' en la mayoría de las ocasiones se engloba el concepto de virus informático, pero en realidad existen varios tipos de programas que de una forma u otra pueden dañar a un sistema; para tener una idea de este tipo de amenazas no solo se debe referir a los virus informáticos ya que sólo son una parte de este tipo de amenazas.

Éstos pueden ser creados de forma intencionada como lo es el *software* malicioso, también conocido como *malware* o simplemente por error: *bugs* o agujeros.

1.1.3.2.1. *Software* incorrecto

Las amenazas más habituales en un sistema informático provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.

A estos errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema son los *exploits*. Como se ha dicho, representan la amenaza más común, ya que cualquiera puede conseguir un *exploit* [1] y utilizarlo contra una máquina sin ni siquiera saber cómo funciona y sin conocimientos mínimos del sistema.

[1] *Exploit*, viene de *to exploit* - aprovechar, código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios.

1.1.3.2.2. Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

1.1.3.2.3. Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar 'atajos' en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras o falsas (*trap doors* o *back doors*), son un mecanismo establecido en el sistema por su diseñador o por alguien que ha modificado el funcionamiento del mismo, su objetivo es ofrecer un modo de acceder al sistema esquivando todas las medidas de seguridad establecidas cuando se usa el procedimiento normal. Se trata pues de proporcionar una ruta directa y oculta de acceso al sistema.

El peligro corre cuando los programadores dejan estos atajos en las versiones definitivas de su *software* para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad del sistema.

1.1.3.2.4. Caballos de Troya

Un caballo de Troya es un fragmento de código que se esconde en el interior de un programa aparentemente inofensivo, y que desarrolla actividades distintas del propósito aparente del programa que le sirve de anfitrión.

Por ejemplo, un caballo de Troya sería un código escondido en el interior de un juego, o de una versión de demostración de un *software* muy llamativo. El usuario

se trae el *software* con intención de probarlo y en principio no tiene porque notar la diferencia con un programa correcto. Si embargo al ejecutar el programa, éste, de modo oculto al usuario, estaría realizando otro tipo de acciones, tales como borrar código, enviar copias de información por la red, instalar un virus informático, etc. A diferencia de los gusanos o los virus, un caballo de Troya es incapaz de replicarse, y su funcionamiento se basa en la ejecución del programa original que lo contiene. Obviamente el nombre de este tipo de amenazas es muy adecuado y proviene de la técnica ideada por Ulises en "la Iliada" de Homero para vencer a los Troyanos.

El éxito de un caballo de Troya se basa en hacer que el usuario ejecute el programa que lo contiene. De este modo, suelen esconderse en programas aparentemente inofensivos, muy llamativos y distribuidos en gran medida como *software shareware* o *freeware*. Los típicos programas anfitriones de los caballos de Troya son los juegos, editores de texto, hojas de cálculo, e incluso hay algunos casos muy curiosos en los que se esconden en supuestas nuevas versiones de conocidas herramientas antivirus.

Un ejemplo interesante de caballo de Troya es aquel que puede esconderse en el sistema UNIX dentro del programa *login*, y cuya finalidad es obtener las contraseñas de los usuarios. De hecho, uno de los creadores del UNIX, Ken Thompson, escribió un maravilloso artículo donde describía cómo introducir un caballo de Troya en el código del programa *login* de modo que éste fuese indetectable.

1.1.3.2.5. Bombas Lógicas

Pueden considerarse como un tipo de caballo de Troya que se usa para lanzar un virus, un gusano u otro tipo de ataque directo contra el sistema. Puede tratarse de una pieza de código o de un programa independiente que permanece sin realizar ninguna función, preparado para atacar el sistema cuando se cumplan ciertas condiciones; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los activadores más

comunes de estas bombas lógicas pueden ser: la ausencia o presencia de ciertos ficheros, una fecha determinada, cuando se haya arrancado el sistema un número dado de veces o se pulse una secuencia definida de teclas. Cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa, causando graves daños al sistema.

1.1.3.2.6. Canales cubiertos

Los canales cubiertos o canales ocultos, son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

1.1.3.2.7. Virus

Una definición muy general de virus informático sería la siguiente: Secuencia de instrucciones ejecutable en un entorno informático, capaz de autoreplicarse de forma autónoma, parasitando a otras secuencias. [8]

Existen varios aspectos de esta definición que es necesario matizar. En primer lugar hay que decir que un virus NO es un programa independiente. No funciona por sí solo, sino que debe parasitar otros programas para poder funcionar. En este sentido es muy adecuado el uso del término virus, puesto que los virus biológicos también poseen esta característica. Tan sólo son capaces de reproducirse utilizando la maquinaria ofrecida por las células de un organismo.

Por otro lado, un virus tan sólo se ejecuta cuando lo hace la secuencia de instrucciones que ha infectado. Existe mucha confusión a este respecto, el hecho de editar el texto de un virus o de listar el nombre del fichero que lo contiene no permite la actuación del virus. Incluso el hecho de copiar el código que contiene el virus, no supone ningún tipo de problema, a no ser que posteriormente se ejecute el código copiado.

Cuando se dice que un virus es una secuencia de instrucciones, se está ampliando su ámbito. Aunque la inmensa mayoría de los virus son secuencias escritas en código máquina, es perfectamente imaginable que un virus consista en una secuencia de instrucciones incluida en cualquier programa. Existen varios tipos de virus, y su funcionamiento normal pasa por una serie de etapas que se denominará ciclo de vida del virus. Por último, es necesario resaltar que el objetivo inicial (y en ocasiones el único) de un virus informático es autoreplicarse. El objetivo posterior del virus depende de su sistema de ataque, y éste puede ser tan variado como permita la imaginación y el sistema utilizado para su creación.

1.1.3.2.8. Gusanos

Los gusanos, o *worms*, son programas independientes capaces de autoreplicarse. Al contrario de lo que ocurre con los virus informáticos, los gusanos son programas completos que pueden funcionar por sí solos, y que por tanto no necesitan parasitar otros programas para replicarse.

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, de ahí su nombre que probablemente provenga del hecho de que "se arrastran" por la red viajando de una máquina a otra; en ocasiones éstos portan virus o aprovechan *bugs* de los sistemas a los que se conecta para dañarlos.

Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fue precisamente el *Internet Worm*, un gusano que en 1988 causó pérdidas millonarias al infectar y detener más de 6000 máquinas conectadas a la red.

Se debe considerar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder al sistema, mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar la red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

1.1.3.2.9. Programas conejo o bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la "caída" total de la máquina.

1.1.3.3. Catástrofes

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas. Un subgrupo de las catástrofes es el denominado de riesgos poco probables. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja (menor incluso que la del resto de catástrofes) que nadie puede tomar, medidas contra ellos. Ejemplos habituales de riesgos poco probables son un ataque nuclear contra el sistema, el impacto de un satélite contra la sala de operaciones, etc. Nada nos asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas.

Como ejemplos de catástrofes se hablará de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que se pueda pensar); obviamente los riesgos poco probables se los tratará como algo anecdótico. A continuación una breve descripción de algunos de ellos.

1.1.3.3.1. Incendios

Pocos desastres son tan devastadores como el fuego. La destrucción de los recursos por el calor es sólo el principio. El daño producido por el humo, el agua,

y el resto de residuos resultantes, pueden hacer imposible recuperar algo después del fuego. Los contratos de licencias de *software* que demuestran las compras no pueden utilizarse después de haberse convertido en cenizas; ni siquiera son facturas de compra.

1.1.3.3.2. Inundaciones

Las inundaciones son los desastres más comunes. Ciertamente, se suelen leer noticias que informan de inundaciones ocurridas en alguna parte del mundo, así como en nuestro país, cuyo clima cambia tan dramáticamente sin importar el tiempo en el que se esté y con un sistema de alcantarillado que deja mucho que desear.

1.1.3.3.3. Accidentes Industriales

Uno de ellos puede ser el sobrevoltaje que se produce por mala manipulación de los cables de energía. Un cortocircuito puede acabar en un incendio o quemar todo lo que encuentre a su paso.

Nadie sabe cuando ni cómo ocurrirán estos desastres accidentales, intencionales o que la naturaleza ponga en nuestro camino, pero dependiendo del medio externo que nos rodea, aunque no podamos impedirlos, se debe estar preparados para una contingencia de esta magnitud.

1.1.4. ¿Cómo nos podemos proteger?

Para completar esta visión global de seguridad se hablará del ¿cómo? proteger los elementos principales de un sistema informático; para ello primero se realizará un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrán generar, y la probabilidad de su ocurrencia. A partir de este análisis se diseñará una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan.

A los mecanismos utilizados para implementar esta política de seguridad se les denomina mecanismos de seguridad, los cuales son la parte más visible del sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación.

- Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las comunicaciones hacia o desde un sistema.

- Por mecanismos de detección se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría como *Tripwire*.

- Finalmente, los mecanismos de recuperación son aquellos que se aplican cuando una violación del sistema se ha detectado, y se desea retornar éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el *hardware* adicional.
  Dentro de este último grupo de mecanismos de seguridad se encuentra un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

1.1.5. Áreas de Administración de la Seguridad

Si se quiere que un sistema sea seguro, se debe desarrollar sistemas AAA (Autenticación, Autorización y Auditoría o Conteo). Para simplificar, es posible dividir las tareas de administración de seguridad en tres grandes grupos, los cuales son:

1.1.5.1. Autenticación

Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio puede ofrecer.

Provee la capacidad de verificar la identificación del usuario o recurso. Esto se puede realizar comparando algo que este individuo sabe, tiene, es o puede hacer a una referencia registrada. Por ejemplo:

Algo que sabe: Una palabra paso o *password*.- es algo que el usuario conoce y el resto de personas no.
Algo que tiene: Una tarjeta de identidad.- es algo que el usuario lleva consigo
Algo que es: La huella dactilar.- es una característica física del usuario.
Algo que puede hacer: La firma.- es única y es un acto reproducible propio por el interesado en su forma de escribirla.

Además, la autenticación de una fuente de datos en un sistema de información es la clave de la seguridad de los datos. Ayuda a determinar cuánta credibilidad se puede establecer, en la exactitud, formalidad e integridad de la información presentada por este sistema.

En lo que se refiere a este proyecto de titulación, se profundizará en la autenticación biométrica, que resume a la frase "algo que es"; más adelante se mencionarán algunas de estas técnicas de autenticación.

1.1.5.2. Autorización

Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan efectivamente acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

El único propósito de la función de autorización es permitir quién puede hacer con un recurso dado.

Esta función generalmente relaciona a un usuario con un recurso del sistema por medio de reglas determinadas de autorización. Esto es, la autorización establece reglas que limitan a los usuarios a ejercer sólo las acciones predeterminadas al recurso del sistema. Cada individuo debe primero tener la autorización explícita de la administración para el acceso al recurso del sistema.

1.1.5.3. Auditoría

Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Un sistema que es auditable permite a un inspector independiente verificar su actividad con relativa facilidad en cualquier momento. El sistema debe demostrar que está ejecutándose para las especificaciones autorizadas, obedeciendo a las respuestas de control, siendo utilizado como se lo ha pensado y conforme con las normas de buena práctica. Para obtener este criterio, el sistema debería ser construido totalmente con componentes auditables.

Para ejemplificar lo anterior, se tomará el ejemplo de una compañía ficticia a la que se la llamará "Servicios de Cómputo". Esta compañía dispone de un servidor donde se ejecuta el *software* encargado del procesamiento de las nóminas y el control de recursos humanos (ambos muy relacionados).

Autenticación se refiere a que sólo las personas de esos departamentos tengan cuentas de acceso a dichos equipos, puesto que sería peligroso que algún otro departamento lo tuviera. El responsable de los equipos de cómputo llevaría a cabo la labor de Autorización, al no permitir que todas las personas responsables de recursos humanos tengan acceso a las Bases de Datos de Nóminas, si no lo necesitan.

La Auditoría se lleva a cabo al establecer políticas de uso y acceso a los recursos, así como reglamentos que rijan la no-divulgación de información confidencial. También aquí se debe llevar un registro de los recursos utilizados para prevenir, por ejemplo, que un uso del 100% en un disco provoque que el sistema deje de funcionar. Debe vigilarse también los intentos de acceso legal e ilegal al mismo.

1.1.6. Seguridad Física y Lógica

Todo esto conduce a plantear soluciones para contrarrestar estas amenazas y ataques, pero estas soluciones deberán ir en su respectivo campo.

1.1.6.1. Seguridad Física

La Seguridad física comprende el aspecto del *hardware*, la manipulación del mismo, así como también el ambiente en el cual se van a instalar los equipos.

Es muy importante ser consciente que por más que el sistema sea el más seguro desde el punto de vista de ataques externos (*hackers*, virus, ataques de DOS, etc.), la seguridad de la misma será nula si no se ha previsto cómo combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras del personal que accede a una área del sistema que se encuentra restringida.

La seguridad física es una de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física

existir técnicas, más allá de la seguridad física que la asegure. Estas técnicas la brinda la Seguridad Lógica.

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo". La seguridad lógica comprenderá el aspecto de los sistemas, tanto operativos como de información.

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.1.7. Control de entrada al sistema

El presente tema se enfocará principalmente al acceso a un sistema o lugar donde deba haber una alta seguridad. Cuando una persona intenta acceder a un equipo por medios normales, la seguridad del medio informático exige que el sistema pueda enfrentarse a la eventualidad de que se trate de un intruso que haya aprovechado fallos o tolerancias en la seguridad física. En ese caso es claro que deben existir medios para impedir que acceda al sistema. Pero incluso si se trata de un usuario autorizado, se ha de canalizar su entrada de forma que opere en el entorno que tiene asignado (es decir, con las cuentas, ficheros, máquinas, periféricos, procesos o prioridades que le correspondan). Para hacer frente a ambas situaciones, el sistema debe cerciorarse de la identidad del usuario antes de dejarlo acceder. A lo largo de este capítulo se tomará muy en cuenta este aspecto, estudiando los mecanismos biométricos que se utilizan con carácter general para controlar la entrada a un sistema informático.

1.1.7.1. Mecanismos de autenticación

Ahora que se tiene claro el panorama de los sistemas AAA, se debe concentrar la atención en el primer elemento de este sistema, la Autenticación.

Para acceder a un sistema se sigue un proceso de dos pasos: primero, el usuario dice al sistema quién es (identificación), y segundo, el sistema comprueba que el usuario es efectivamente quién dice ser (autenticación).

Evidentemente la dificultad está en el segundo paso, pues los ordenadores no disponen de mecanismos sensoriales ni cognitivos, y los sistemas sólo pueden reconocer al usuario mediante una clave que lo distingue del resto de personas para evitar al impostor. Las claves que se utilizan en este proceso de autenticación se suelen dividir en tres grupos: claves informativas, claves físicas y claves biométricas.

A continuación se describirá cada una de ellas.

alguna unas personas de otras, y al mismo tiempo lo suficientemente flexible como para admitir las variaciones puntuales que los datos biométricos de cada persona experimentan con el tiempo.

También es importante que los sensores sean capaces de detectar los intentos de falsificación.

Los distintos tipos de claves de autenticación no son excluyentes entre sí. Por ejemplo, es muy frecuente la combinación de tarjetas magnéticas con contraseñas, que pueden estar almacenadas en el sistema o en la propia tarjeta. Asimismo, muchas veces se utilizan claves de autenticación para acceder no al sistema, sino a su entorno (edificio, planta, habitación, etc.), por lo que resuelven problemas propios de seguridad física. Sin embargo, se suele preferir tratarlos como mecanismos de seguridad interna por el hecho de que son implementados siempre con medios informáticos; en última instancia estarán bajo el control de un ordenador especializado que puede considerarse como parte del sistema.

1.2. LA BIOMETRÍA APLICADA A LA SEGURIDAD

El concepto tradicional de Biometría se refiere a la aplicación de las técnicas matemáticas y estadísticas a las ciencias de los seres vivos, medicina, biología, etc. Un concepto bastante amplio para el presente estudio. [9]

En el tema de seguridad, la Biometría analiza y mide ciertas características unívocas de un individuo para crear un identificador biométrico el cual puede ser almacenado en una base de datos y recuperado para su comparación con un ejemplo vivo con las mismas características. En este entorno la Biometría se resumiría en los siguientes postulados: [10]

- Conjunto de métodos automatizados de identificación y verificación de la identidad de una persona viva, basados en una característica fisiológica.

- Analiza y mide ciertos rasgos unívocos de un individuo para crear un identificador biométrico.

- Este identificador puede ser almacenado en una base de datos y recuperado para su comprobación posterior.

La Biometría es fácil de usar, nada que recordar nada que cambiar nada que perder. La Biometría se deriva del análisis estadístico de observaciones biológicas. Es una ciencia emergente que compara electrónicamente características biológicas de un individuo (rostro, huella dactilar, voz, etc.) contra una población de una o más de tales características; para este estudio, se denominará al tratamiento de cada característica biológica del individuo como técnica biométrica.

La Identificación y Autenticación biométricas (I&A) explota el hecho de que ciertas características biológicas son singulares e inalterables y son además, imposibles de perder, transferir u olvidar. Esto las hace más confiables, amigables y seguras que los *passwords*.

1.2.1. La Biometría Informática [11]

La "Biometría Informática" es la aplicación de técnicas biométricas a la autentificación e identificación automática de personas en sistemas de seguridad informática.

Como se puede observar en la figura 1.2, algunos expertos, dividen a la Biometría en dos ramales:

Biometría Estática:

- Huellas Digitales.
- Geometría de la mano o de los dedos. (Geometría manual)
- Termografía.

- Análisis del iris
- Dibujo del sistema venoso de la retina o fondo del ojo. (Análisis de retina)
- Venas del dorso de la mano.
- Formas o rasgos de la cara.
- Informaciones genéticas.
- Etc.

Biometría Dinámica: Mide el comportamiento del usuario.

- Patrón de Voz.
- Firma manuscrita.
- Dinámica de tecleo.
- Cadencia del paso.
- Análisis gestual.
- Etc.

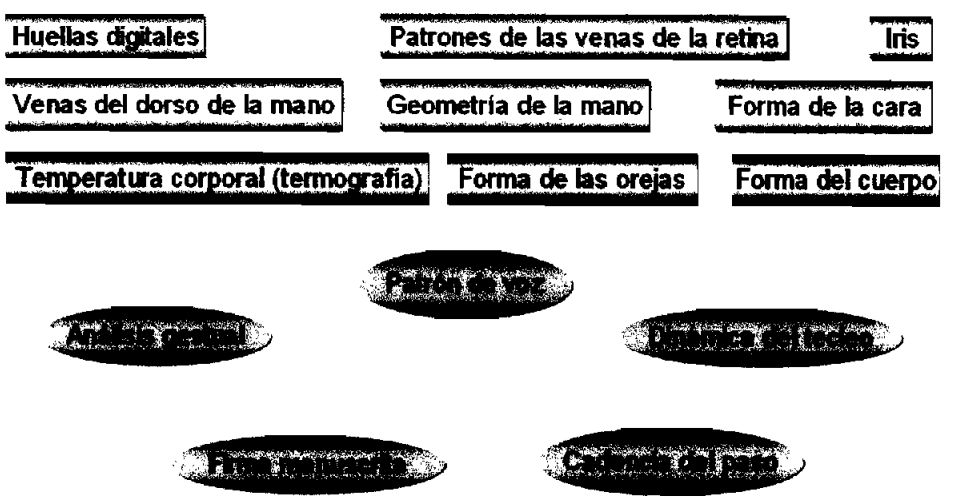


Figura 1.2: División básica de la Biometría. [11]

En el presente proyecto se analizarán las técnicas más importantes y comunes que se usan en la actualidad como son: huellas dactilares, forma de la cara,

geometría de la mano, reconocimiento de iris y retina, patrón de voz y reconocimiento de firma.

1.2.2. Área de Acción

El entorno tecnológico y empresarial actual demanda niveles de seguridad que, por el momento, están lejos de haberse conseguido. En tono jocoso, se puede decir que la seguridad de muchos sistemas informáticos está basada únicamente en fechas de nacimiento, nombres de mascotas y una fe ciega en todo lo que llega por el correo electrónico. El alcance de las aplicaciones biométricas no cubre solamente a los especialistas en computación y seguridad, sino también a los propios gerentes de negocios y administradores que deben conocer las nuevas tecnologías para así tomar decisiones relacionadas con la seguridad de sus empresas.

La seguridad biométrica, la nueva tecnología de seguridad basada en el reconocimiento de una característica física de las personas y cuya principal ventaja es su intransferibilidad, se está volviendo muy común en nuestro alrededor, ya no solo las grandes potencias poseen sistemas de seguridad basados en el reconocimiento biométrico.

La Biometría también ofrece una solución efectiva a un tipo de fraude muchas veces infravalorado por las empresas, el fraude interno, provocado en la mayoría de los casos por usuarios autorizados, conscientes o no de lo que están haciendo. Un ejemplo de usuario inconsciente sería aquel que abandona su puesto de trabajo con el PC encendido; en cambio, el consciente podría ser un empleado despedido o descontento con la empresa. En ambos casos, la biometría impide que información confidencial de la empresa se utilice para fines poco éticos o perjudiciales para la misma, como el espionaje industrial.

Además del alto nivel de seguridad intrínseco del propio sistema, basado en el proceso algorítmico de creación de los "patrones", las tecnologías biométricas son altamente flexibles y se pueden adaptar a los distintos niveles de seguridad

requeridos por la empresa. En este sentido, la Biometría se puede complementar con tarjetas inteligentes y encriptación de datos a través del sistema PKI[2]. Por ejemplo, en un edificio con áreas restringidas, el personal autorizado deberá introducir una tarjeta donde está registrado el patrón de registro de su huella digital y su *password*. Además, deberá introducir su nombre y colocar su dedo para realizar la verificación de identidad.

En conclusión, la creciente necesidad de sentirse seguros está dando un gran impulso a esta nueva tecnología de seguridad que mejora la calidad de vida de todos los agentes de la sociedad: empresas, gobiernos y ciudadanos. Sin embargo, la tecnología biométrica aún no ha despegado del todo y la mayoría de los ejemplos se los encuentra en el entorno del control de la criminalidad y de las altas finanzas.

Existen muchas tecnologías biométricas y no todas son lo que sus fabricantes predican. La Biometría es un mercado enorme y se analizará muy bien cada producto para estar seguro de que puede cumplir las expectativas demandadas por el cliente.

La mayoría de consultoras coinciden en que la tecnología biométrica con mayor potencial de difusión, es la basada en el reconocimiento de la huella dactilar. Uno de los principales motivos es que es la menos intrusiva y la de mayor costo-beneficio.

Por otro lado, la basada en el reconocimiento del iris es considerada una de las más fiables pero también una de las más caras.

Una de las barreras comunes a todas ellas y que está frenando la difusión masiva de este tipo de tecnología es la falta de un estándar de programación así como la dificultad de integración de estos sistemas con los sistemas de seguridad existentes en las empresas.

[2] PKI : Public Key Infrastructure – Infraestructura o Arquitectura de Clave Pública.

Sin embargo, se está avanzando mucho en este campo y esto lo demuestran los casos de implementación en los ámbitos del acceso a PC´s y de las redes informáticas que se multiplican cada año. En conjunto, se prevé un crecimiento de los ingresos derivados de la biometría de un 30% de media anual del 2002 al 2005 llegando a una cifra de 1,9 billones de dólares[3] .

El desarrollo de la Autenticación Biométrica (AB) puede ayudar a solucionar muchos de los problemas de seguridad que afectan actualmente. En esta línea, existen ya aplicaciones comerciales de la AB en forma de lectores de huellas dactilares incorporados a ordenadores portátiles que sustituyen o complementan la tradicional protección por contraseña. Controles de huellas o de iris se están usando también en sistemas de control de acceso a instalaciones. Los lectores de huellas o los reconocedores de voz pueden, a mediano plazo, sustituir a los PIN de los teléfonos móviles o a las llaves de los autos.

1.2.3. Una tecnología no aislada [12]

No obstante lo anterior, la AB por sí sola no puede resolver todas las necesidades de autentificación y seguridad, sino que se le ha de considerar como una herramienta más. El ejemplo más claro es la firma digital o la encriptación dentro de una PKI. Un sistema de AB puede ser el sustituto perfecto para la contraseña de una clave privada dentro de una PKI, pero sin el resto de elementos que forman la PKI la AB no podría cumplir ninguno de los objetivos de irrefutabilidad, autentificación e integridad. Por tanto, se debe recordar que la AB es una herramienta más en todo sistema de seguridad informática y que su uso ideal es como complemento de otros sistemas de autentificación o criptografía. De hecho, la autenticación con un sistema biométrico puede ser el primer paso para autorizar el acceso a recursos de una red.

Como todas las tecnologías de seguridad existentes, la Biometría no es invulnerable. Un matemático japonés (no un ingeniero, ni programador o experto

[3] Fuente: *International Biometric Group*, año 2001

en falsificaciones, sino un matemático) ha conseguido engañar once lectores de huellas dactilares invirtiendo menos de 10 dólares en material de fácil obtención. Tsutomu Matsumoto duplicó una huella dactilar resaltando su impresión sobre un cristal (por ejemplo, un vaso o una ventana) mediante adhesivo de cianoacrilato (comercialmente distribuido con marcas tan conocidas como "Super Glue") y fotografiando el resultado mediante una cámara digital. La imagen resultante se mejoró mediante *PhotoShop* y se imprimió en una hoja de papel transparente.

Matsumoto utilizó dicho papel como máscara para generar un circuito impreso con la imagen de la huella dactilar (para proporcionar "relieve"). Dicho circuito impreso, el material para el fijado y revelado y las instrucciones detalladas del proceso, se pueden conseguir en cualquier tienda de electrónica por menos de 3 euros. Seguidamente se obtuvo un dedo de "gelatina" empleando el circuito impreso para proporcionarle el relieve que emula la huella dactilar original. En total, menos de 10 dólares en gastos y una hora de trabajo. El resultado: un "dedo" que pasa la prueba de un escáner digital con una efectividad del 80%.

"La biometría no es un elemento aislado, su eficacia depende del entorno"

Se debe entender la seguridad biométrica como un elemento complementario en un entorno seguro que añade un nivel más de seguridad al sistema. La Biometría por sí sola no es la panacea de la seguridad.

Que la Biometría cumpla con su función depende de tres factores fundamentales:

El producto: como se ha indicado antes, el mercado de la Biometría es muy amplio y se analizará y probará el producto a fondo antes de integrarlo en el portafolio de soluciones de seguridad. Nunca se deberá confiar en lo que dice el fabricante ya que la mayoría de las pruebas se realizan bajo condiciones ideales de laboratorio; siempre se deberán comprobar las características técnicas del producto en el campo de acción.

convencional no ofrece una forma totalmente segura, o al menos un elevado nivel de seguridad, que permita reconocer al usuario legítimo y distinguirlo del intruso.

En cambio, las características propias y distintivas de una persona, especialmente las referidas al aspecto físico, permiten realizar sistemas de mayor seguridad compitiendo en eficiencia y servicio con los sistemas tradicionales comentados anteriormente.

De esta manera, por ejemplo, se puede asegurar que quien se quiere registrar en un sistema es realmente la persona que dice que es y no otra que quizás se enteró de la contraseña porque la encontró escrita en la parte inferior del teclado de la PC del usuario legítimo, o encontró la tarjeta del mismo.

Las soluciones biométricas mantienen la privacidad de los usuarios puesto que no almacenan los elementos mismos de caracterización de una persona; no guardan una foto de las huellas dactilares, de las caras, manos u ojos, como tampoco una grabación de la voz, etc. En general, todos los sistemas biométricos se basan en un proceso que se inicia con el suministro de una muestra de la característica física o de comportamiento por parte del usuario, como por ejemplo, colocar la yema del dedo sobre la superficie del *scanner* o pronunciar una frase delante de un micrófono. A partir de la información capturada, se conforma una representación digital que involucra los atributos correspondientes a un modelo matemático. Esta información que se guarda encriptada, constituye el **perfil o plantilla**, como también se la llama, que define las características correspondientes de cada usuario; es decir se genera el "patrón de registro", que servirá para buscar correlaciones con el patrón de verificación. Esta última se crea cada vez que el usuario intenta acceder al sistema, como, por ejemplo, a la red local de su empresa. Esta fase se denomina "**correspondencia**".

Para buscar correspondencias se pueden utilizar dos procesos distintos: la **identificación** o reconocimiento (1:N) y la **autenticación o verificación** (1:1). Ambas tienen sus ventajas e inconvenientes. Decidirse por un proceso u otro

depende de las necesidades y preferencias de la empresa o institución donde se implementará.

En el caso de la identificación, el proceso de correspondencia es más lento, ya que el sistema buscará entre N patrones dentro de la base de datos de los registros. Sin embargo, es más conveniente para el usuario ya que sólo utilizará su característica física. Un ejemplo de aplicación sería en un programa de control del terrorismo en los aeropuertos, donde se ha instalado un *scanner* de reconocimiento del iris.

La identificación responde a buscar y reconocer una determinada persona entre todas las demás. Se trata entonces de responder a la pregunta **¿Quién es?.**

Para establecer la identidad de una persona se trabaja con las características biométricas que se capturan para compararlas con las correspondientes de una base de datos en línea que guarda los perfiles de un conjunto de personas. El proceso de búsqueda y equiparación es escalonado, de forma tal que al ir reduciendo en aproximaciones sucesivas, el conjunto seleccionado conduzca a un único elemento (persona) más algún posible grado de ambigüedad en cuanto a la determinación de dicho elemento.

La **verificación**, por su parte, busca autenticar una determinada persona en base a ciertas características biométricas, es decir, basándose en ciertos elementos morfológicos que le son inherentes y que sólo se dan en ese sujeto o que le son propias. Es un proceso de reconocimiento de uno contra uno mismo basado en la comparación con muestras biométricas previas.

Como se puede deducir, la verificación es una forma explícita de autenticación tal como se conoce generalmente en el ambiente de computación. Se trata entonces de responder a la pregunta **¿Es quién dice ser?.**

La verificación, en cambio, es más fácil de procesar, ya que la comparación es 1:1, de forma directa. Para ello, el usuario debe introducir un identificador propio como, por ejemplo, su nombre, para que el sistema busque directamente su patrón de

registro y lo compare con el de verificación. En este sentido, la autenticación contiene un elemento más, el identificador del usuario, para poder realizar una correlación 1:1. Se propone el caso: para realizar una transferencia electrónica, el sistema verificará que la persona está autorizada a través de su nombre: ¿Es José Marcos, el Director de compras?, y luego realizará la verificación: ¿es quien dice ser?, a través de la comparación de su patrón de registro con el de verificación.

A pesar de las diferencias, ambos sistemas ofrecen el mismo nivel de seguridad si se aplican en el entorno adecuado.

Uno de los aspectos distintivos pero comunes a todas las tecnologías de seguridad biométrica es que no puede existir una coincidencia del 100% entre patrones de registro y de verificación; si existiera, se estaría produciendo algún tipo de fraude. Y es que las tecnologías biométricas permiten obtener correlaciones con un margen de error casi nulo debido a que dos patrones sucesivos nunca pueden ser idénticos. Gracias al complicado proceso algorítmico que procesan los patrones, se puede saber si existe correlación o no entre patrones similares. Paradójicamente, el residual, pero existente margen de error de estas tecnologías, las convierte en uno de los sistemas más seguros y fiables de nuestros días. En la figura1.3 se tiene un esquema del procedimiento explicado.

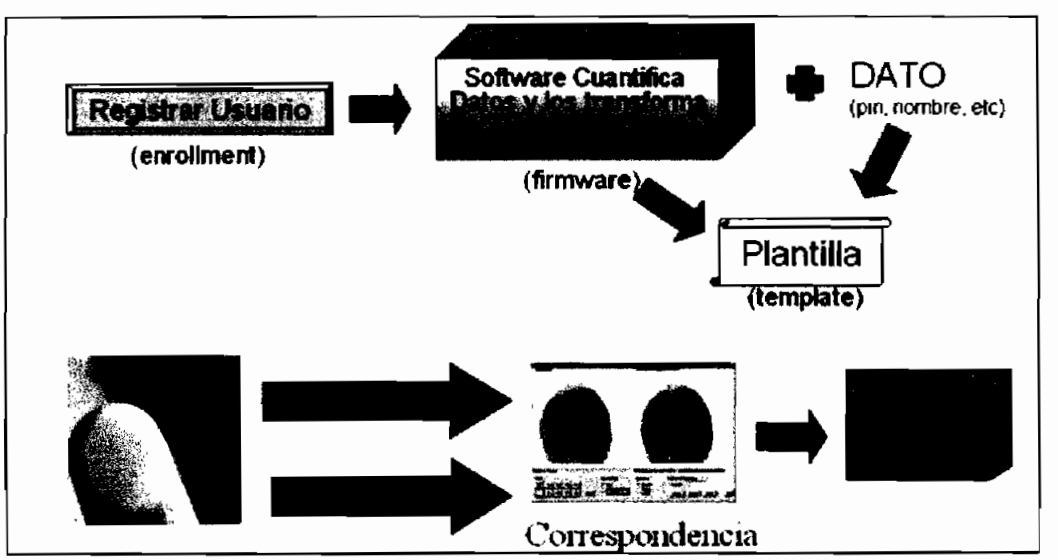


Figura 1.3: Procedimiento para la obtención de un patrón biométrico basado en la huella dactilar. [11]

1.2.5. Sistema Biométrico

En el pasado el procesamiento de Identificación y Autenticación (I&A) biométrica era hecho manualmente por gente que física y mentalmente comparaba huellas dactilares contra tarjetas, rostros contra fotos de pasaportes y voces contra cintas grabadas. Hoy en día, dispositivos tales como *scanners*, videocámaras, y micrófonos pueden electrónicamente capturar y entregar estas mismas características biométricas para automatizar procesos y comparaciones. Cada tecnología biométrica (huella dactilar, rostro, voz, etc,) tiene sus propias características, variedades y certezas. Sin embargo el proceso de captura y extracción de esas características y variedades, el almacenamiento y la comparación es universalmente similar. En la mayoría de los casos, un individuo presenta su característica biometría en un dispositivo de captura que colecta los datos y los envía a un algoritmo que extracta las características únicas de la misma y crea un identificador, este identificador puede entonces ser almacenado o comparado contra otros identificadores previamente almacenados.

En la captura del identificador biométrico no hay dos tomas iguales aún del mismo individuo a causa de diferencias ambientales y otras condiciones en el momento de la captura. Normalmente la mayoría de los algoritmos de comparación generan un ámbito para cada ensayo de comparación el cual es cotejado dentro de determinados umbrales antes de ser aceptado o rechazado; si el umbral es demasiado bajo, se vuelve demasiado fácil para una persona no autorizada ser aceptada por el sistema, en cambio si el umbral está demasiado alto, personas autorizadas pueden llegar a ser rechazadas. Cada proveedor de tecnología biométrica configura la aceptación o falso rechazo de forma diferente. Los niveles de precisión biométricos pueden variar pero son siempre más confiables que el 100% de falsas aceptaciones experimentadas con los *passwords* prestados o robados.

1.2.5.1. Arquitectura de un sistema biométrico para identificación personal [16]

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún identificador biométrico de

una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un *scanner*. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos (en el ejemplo de la figura 1.4 una imagen) con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema. La arquitectura típica de un sistema biométrico se presenta en la figura 1.4. Ésta puede entenderse conceptualmente como dos módulos:

1. Módulo de inscripción (*enrollment module*) y
2. Módulo de identificación (*identification module*).

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

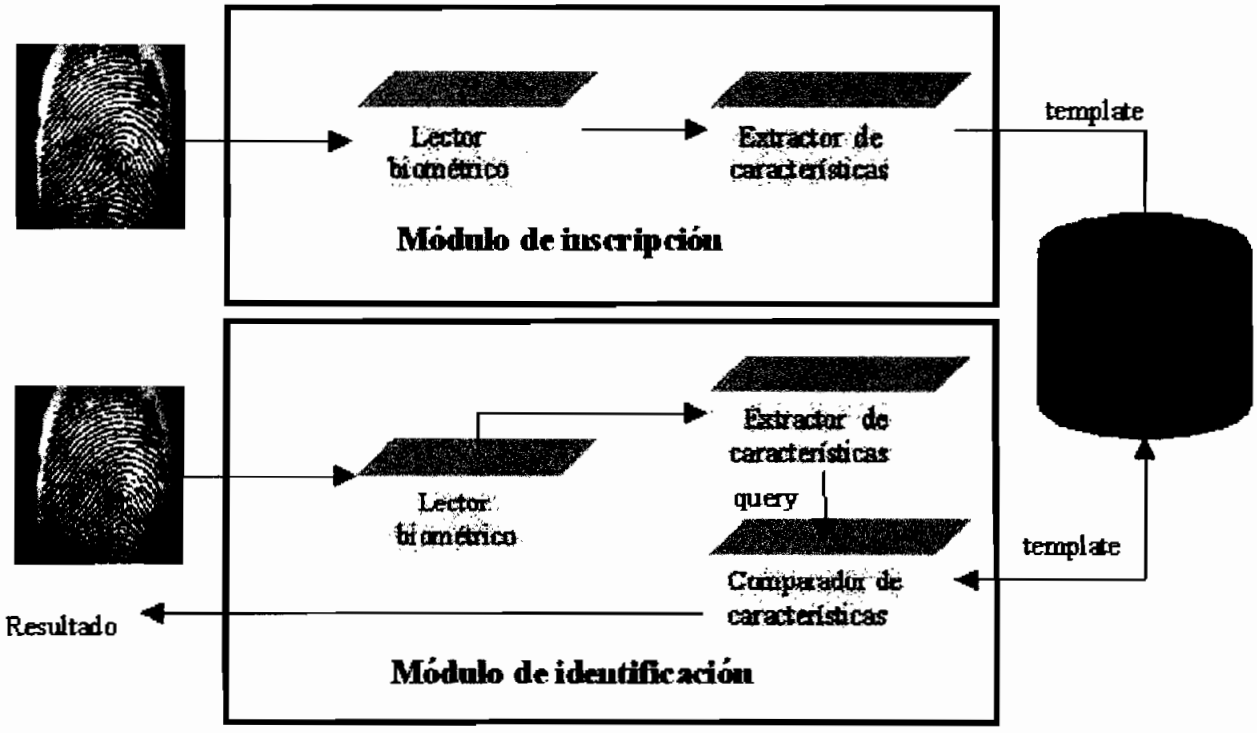


Figura 1.4: Arquitectura de un sistema biométrico para identificación personal, aquí ejemplificado con huellas dactilares. [16]

El primero se encarga de adquirir datos relativos al identificador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del identificador. El conjunto de características, que será almacenado en una base de datos central u otro medio como una tarjeta magnética, recibirá el nombre de *template*. En otras palabras un *template* es la información representativa del identificador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del identificador biométrico en el punto de acceso.

El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo en una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de los *templates*. La representación resultante se denomina *query* y es enviada al comparador de características que confronta a éste con uno o varios *templates* para establecer la identidad.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de fase de inscripción, mientras que los procesos realizados por el módulo de identificación reciben la denominación de fase operacional. Un sistema biométrico en su fase operacional puede operar en dos modos, anteriormente estudiados: verificación e identificación.

1.2.5.2. Características de un Sistema Biométrico

Un sistema biométrico ideal reúne algunas condiciones especiales: debe ser automático, fácil de usar, de elevada precisión en las mediciones, alta velocidad de respuesta, mínimo contacto con el usuario y la mayor aceptación posible; todo claro está al menor costo. Adicionalmente puede interesar el espacio ocupado en disco por la base de datos.

Además, hay cuestiones relacionadas con las características de los usuarios que se van alterando con el tiempo.

Por sus raíces, los sistemas biométricos pueden ser más exactos que los demás sistemas de seguridad de autenticación, lo que se pone de manifiesto en las mediciones de **aceptaciones equivocadas** (o falsas), es decir reconocimiento de usuarios ilegítimos. Su vulnerabilidad al fraude está en principio relacionado con el sistema biométrico específico, que luego se analizará, la implementación de cada producto y el umbral de sensibilidad o ajuste de cada dispositivo. En este último punto se vuelve importante la cuestión de los **rechazos equivocados** (o falsos), es decir no reconocimiento de usuarios legítimos.

Tanto los rechazos equivocados como las aceptaciones equivocadas se miden, calculan y establecen en forma de tasas porcentuales. Por lo tanto la tasa de **aceptaciones equivocadas** es el porcentaje de usuarios no autorizados que igualmente logran pasar el control, mientras que la tasa de **rechazos equivocados** es precisamente lo opuesto, es decir, el porcentaje de usuarios autorizados que no logran pasar el control. Mientras una tasa baja de aceptaciones equivocadas es fundamental en cuanto a seguridad, valores no tan bajos en la tasa de rechazos equivocados podrían ser aceptables. Sin embargo si bien el valor de esta última variable no afecta la seguridad misma, puede resultar intolerable por las molestias innecesarias causadas a usuarios legítimos que por un motivo u otro no se reconocen.

Mientras la relación intrínseca con los usuarios constituye el punto más importante a favor de las soluciones biométricas, en algunos casos también se arrastran ciertas desventajas principalmente en cuanto al propio factor humano.

Efectivamente, algunos métodos provocan connotaciones negativas por lo que presentan resistencia natural por parte de los usuarios. Un caso es el de las huellas dactilares, que se asocia con procedimientos policíacos. Otro es el escaneado de la retina por medio de un haz de luz, que puede generar temores.

Los productos biométricos también pueden catalogarse en dos grandes categorías en cuanto a la fase operacional para el que están previstos: **verificación** e **identificación**, tal como se comentara antes. En el primer caso se trata de saber quién es la persona, es decir ubicarla dentro de un conjunto de usuarios; en el segundo, en cambio se busca verificar que un usuario sea realmente quien dice ser.

Otra forma de clasificación parte de las características personales. En este sentido hay características **fisicas** (estáticas) y **del comportamiento** (dinámicas) ya mencionadas. Entre las primeras se puede mencionar las más importantes, como el sistema de huellas dactilares, reconocimiento facial, geometría de las manos, y reconocimiento de iris y retina. Los métodos referidos al comportamiento incluyen la verificación de firmas y el reconocimiento de la voz.

Como resumen, en todos estos casos se capturan las características principales de cada usuario según el método, se las transforma en una representación digital que constituye el perfil o plantilla de dicho usuario, se encripta y se guarda en una base de datos. Cuando posteriormente el usuario intenta registrarse o acceder al sistema protegido, se repiten los tres primeros pasos y el resultado se chequea contra toda la información existente en la base de datos si se trata de una identificación, o bien contra su supuesta plantilla en caso de una verificación. Estos procesos se realizan en tiempo real evitando así la existencia de duplicados en el sistema.

1.2.5.3. Partes del Sistema

Los sistemas biométricos incluyen *hardware* y *software*; el primero es el encargado de capturar las características humanas para las que está preparado, mientras que el *software* interpreta y elabora los datos resultantes para luego compararlos con el perfil existente para así determinar su aceptación o rechazo. Surge entonces que un punto fundamental del sistema es la construcción de la base de datos de registro inicial. Para ello cada usuario deberá proveer una o varias muestras de los componentes biométricos que lo caractericen efectivamente.

En los casos de verificación, la operación incluye alguna identificación del tipo PIN o bien una contraseña, que en la práctica obra también como un índice para la búsqueda de la información pertinente en la base de datos de perfiles o plantillas.

La metodología de implementación básica de un sistema de reconocimiento biométrico está conformada por tres fases:

1. La fase de entrenamiento o modelado, donde se extraen las características significativas de la señal de entrada,
2. La fase de almacenamiento del modelo obtenido en la fase anterior, y
3. La fase de prueba, donde se realiza el reconocimiento propiamente dicho.

Es evidente la necesidad de una gran base de datos que contenga los patrones necesarios para el tipo de autentificación descrita.

1.2.6. Tipos de Identificadores biométricos

El reconocimiento biométrico responde a un sistema automático basado en la inteligencia artificial y el reconocimiento de patrones, que permite la identificación y/o verificación de la identidad de personas a partir de características morfológicas o de comportamiento, propias y únicas del individuo, conocidas como identificadores biométricos. Como principales identificadores biométricos se puede mencionar las huellas dactilares, la geometría de la mano, la cara, el iris, la retina, la voz, el estilo de escritura...etc.

1.2.6.1. Características de un identificador biométrico

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

1. Universalidad: cualquier persona posee esa característica;

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

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como identificador biométrico.

1.2.6.2. Terminología [2]

Para determinar las prestaciones de un sistema biométrico, habrá que remitirse al análisis y valoración de los siguientes parámetros estándares:

- **FAR (*False Acceptance Rate*):** Porcentaje de personas no autorizadas aceptadas por el sistema.

- **FRR (*False Reject Rate*):** Porcentaje de personas autorizadas no aceptadas por el sistema.

- **SR (*Success Rate*):** Responde a una combinación de los dos factores anteriores que se utiliza como indicador de la resolución total del sistema.

  SR= 1 - (FAR + FRR)

- **ERR (*Equal Error Rate*):** El FAR y el FRR responden a parámetros inversamente proporcionales, por tanto, variarán en función de las condiciones prefijadas por el programa de identificación biométrica. Por ejemplo si se debe utilizar el programa en un entorno de máxima seguridad, se intentará que el FAR sea el más pequeño posible, aunque esta acción signifique de forma implícita, el incremento drástico del factor FRR. Se deberá fijar un parámetro o umbral que permita igualar los dos factores, asegurando de esta manera el óptimo funcionamiento del sistema. Este umbral se denomina *Equal Error Rate* (ERR), y es el que determinará,

finalmente, el poder de identificación del sistema. En la figura 1.5, se muestra gráficamente la relación descrita.

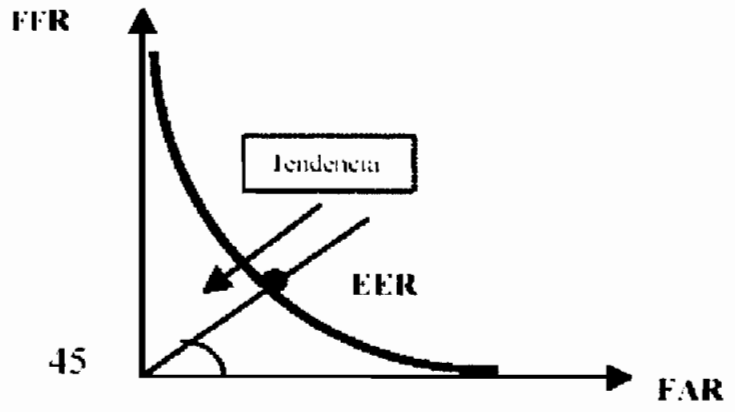


Figura 1.5: Relación entre FAR, FRR y ERR. [30]

En razón de la amplitud de la temática, el estudio se limitará a los sistemas de mayor popularidad mencionados anteriormente.

1.2.6.3. Reconocimiento de Huellas Dactilares

La identificación única por medio de las huellas dactilares nos ha acompañado durante muchas décadas. Quizás por esta razón, las aplicaciones biométricas en computación tienen también su tiempo; fue a principios de los 80 en que aparecieron los primeros sistemas de este tipo.

Figura 1.6: Huella dactilar. [11]

El sistema parte de un proceso similar al conocido, esto es, trata de tomar las huellas dactilares. El escaneado o lectura electrónica de la huella se convierte a un código digital que se compara con los existentes en la base de datos.

Pese a la gran exactitud de este método, las lecturas pueden complicarse por suciedad, grasa, quemaduras, lastimaduras, cicatrices, etc. que deformen la imagen como para verse representada de manera lo suficientemente diferente de la original y provocar un rechazo equivocado.

Entre los usos de este sistema se pueden mencionar el acceso a aplicaciones financieras, autorización de transacciones de alto valor en bancos, acceso a redes, estaciones de trabajo y recursos de red, verificaciones del horario de trabajo, y hasta registro de votación.

La operación de un sistema de este tipo puede incluir el escaneado de los dedos desde diferentes ángulos para tener una información más completa.

1.2.6.3.1. Características del Autentificador[17]

Se trata de una característica de tipo morfológico que presenta como característica principal, la presencia de un conjunto de crestas (líneas) o partes donde la piel se eleva sobre las partes más bajas o valles existentes entre las crestas.

La información en sí misma consiste en establecer dos componentes: un patrón formado por crestas y surcos y el formado por detalles menudos.

El patrón propiamente dicho se refiere a las líneas y surcos o valles (espacio entre líneas) que conforman la huella dactilar.

Los patrones básicos son tres*: **lazo, arco y espiral.***

- En un patrón tipo lazo, las líneas comienzan de un lado del dedo, llegan hasta un tope aproximadamente en el centro de la yema del dedo y regresan hacia el mismo lado.

- Se tiene un patrón en forma de arco cuando las líneas también comienzan al costado del dedo y llegan al centro de la yema pero ahora siguen hacia

el otro lado del dedo, formando precisamente un arco que pasa por la zona central de la yema.

- Finalmente, en un patrón en forma de espiral las líneas forman círculos aproximadamente concéntricos al centro de la yema.

En muchos casos, las huellas dactilares muestran una combinación de estos patrones.

El otro componente se refiere a los detalles menudos o minucias; en la práctica son tan importantes como los patrones, tales como los lugares en que las líneas se cortan o bifurcan, etc.

Aquí se trata de determinar dónde aparecen puntos singulares en las líneas, es decir detalles como la terminación, ruptura, formación de un gancho, y cambios en general de las líneas. En este aspecto se puede distinguir:

- **Bifurcación de la cresta (*rigde bifurcation*)**: El punto donde una línea se divide en varias líneas llamadas ramas.

- **Divergencia:** El punto donde se separan varias líneas prácticamente paralelas.

- **Punto:**

- **Cercado o Lago:** Punto en que una línea que se divide en dos ramas que más adelante se vuelven a juntar.

Estas dos características quedan unívocamente definidas a partir de su localización (coordenadas espaciales x,y respecto al sistema de coordenadas central de la imagen) y de su orientación (ángulo θ). Las primeras responden al 60.6 % del total de detalles presentes en una huella, mientras que las segundas responden al 17.9%. [16]

Se debe notar que las huellas dactilares nacen como resultado de un proceso aleatorio, por lo que se puede afirmar la no existencia de ningún tipo de correlación entre mellizos idénticos o individuos de una misma familia. Asimismo, se debe puntualizar que las personas de raza asiática presentan crestas muy pequeñas y finas, hecho que dificulta en gran medida, la aplicación del sistema de reconocimiento dactilar a dicho colectivo.

Las huellas dactilares son un caso en que se dan sistemas de identificación y de verificación.

Los sistemas de identificación, es decir, de reconocimiento de uno entre muchos, son conocidos como **AFIS** (Sistemas de Identificación Automática de Huellas dactilares).

A su vez hay dos tipos de aplicaciones AFIS: forense y civil. En el primer caso se capturan múltiples imágenes de cada dedo desde diferentes ángulos. Las aplicaciones civiles, en cambio, trabajan generalmente con una única imagen plana de algunos dedos solamente.

Por su parte, los sistemas de verificación, también trabajan con imágenes planas pero de un único dedo, haciendo en pocos segundos el reconocimiento de uno contra uno mismo.

En la figura 1.9 se muestra el diagrama de bloques de un sistema utilizado para la verificación de huellas dactilares. En el mismo se describe en forma general las operaciones lógicas necesarias para llevar a cabo la identificación.

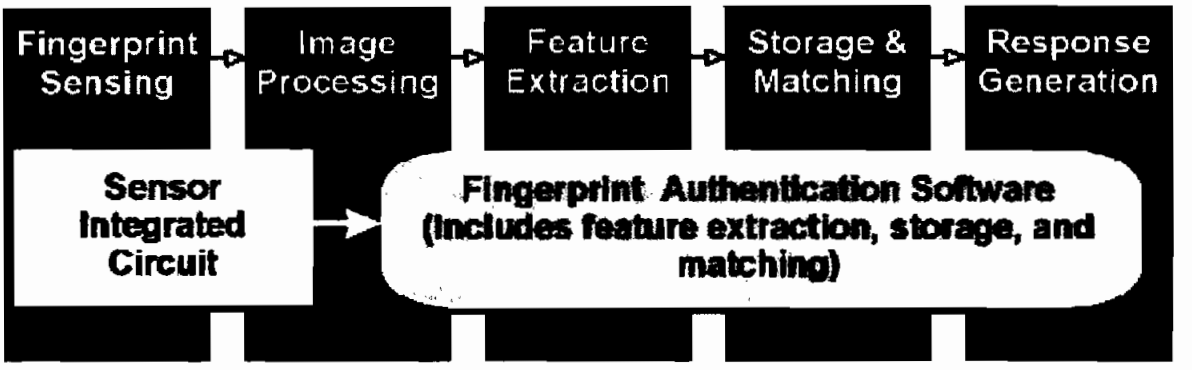


Figura 1.9: Diagrama de bloques de un sistema reconocimiento de huellas dactilares. [17]

1.2.6.3.2. Sistema de Reconocimiento

La mayoría de los sistemas de reconocimiento de huellas dactilares, se hallan englobados dentro de los sistemas AFIS, constituyendo un elemento indispensable dentro de las investigaciones policiales.

Las técnicas de reconocimiento de huellas se dividen en dos categorías: locales basadas en las minucias ya mencionadas y globales basadas en la correlación. El principal inconveniente de la primera aproximación radica en la difícil tarea de extracción de las minucias en imágenes de baja calidad, mientras que la segunda viene a mejorar algunas dificultades presentadas por la aproximación creada por los el patrón de detalles (minucias), pero presenta sus propias fallas, esta técnica requiere de la localización precisa de un punto de registro el cual se ve afectado por la rotación y traslación de la imagen.

1.2.6.3.3. Características del Sistema [11]

- Probabilidad de igualdad = 1/67 billones.
- Se necesita gran poder de procesamiento y alta capacidad de almacenamiento.
- Se basa en rasgos parciales.
- Más utilizado, mejor precio, mayor cantidad de fabricantes y mayores ventas.
- Lectores ópticos de silicón vs. *scanner* ultrasónico.
- Sistema de difícil falsificación.

de los huesos, asimetrías de puntos notables, etc. Estos sistemas están diseñados para compensar el efecto de barbas, lentes o anteojos, y sombreros.

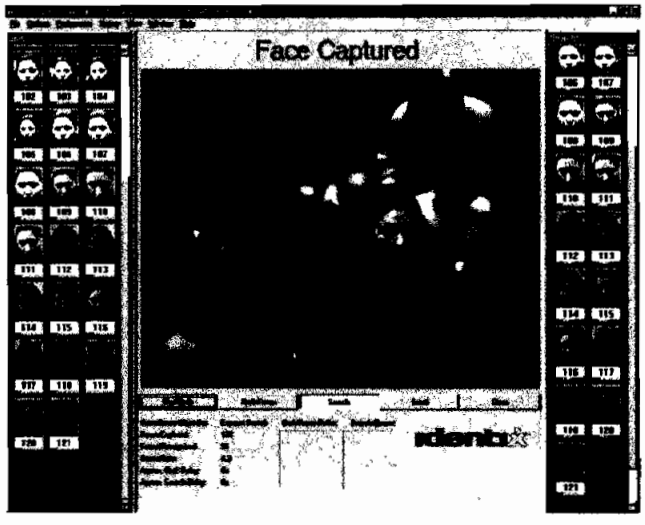


Figura 1.10: Reconocimiento facial. [11]

Como siempre, los datos resultantes se convierten a un código digital que puede resultar que ocupe bastante espacio de almacenamiento. Si bien el sistema es muy exacto, su uso principal se orienta a la verificación de una persona determinada y no precisamente a la identificación de una entre muchas.

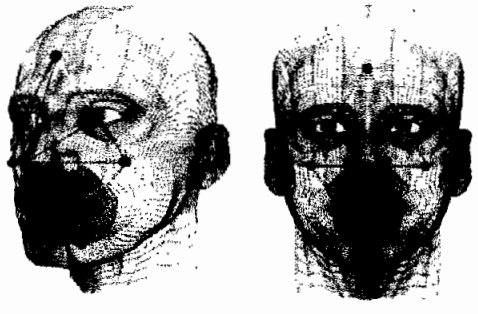


Figura 1.11: Extracción de parámetros geométricos de la cara. [18]

Los sistemas de reconocimiento de caras se usan en aplicaciones de ventas por menor, pago de cheques, operaciones financieras en general incluyendo operaciones de bolsa en línea, atención de salud de sistemas de seguridad social, control de fronteras (junto con reconocimiento de la voz), acceso a VPNs y seguridad en general.

1.2.6.4.1. Etapas de detección

La primera etapa consiste en la detección de la imagen capturada de la cual se separan los elementos faciales eliminando información extraña (como la barba y anteojos).

El *software* ahora analiza la imagen buscando determinar las estructuras típicas de los elementos más importantes (como ojos y nariz) con las que calcula la cara completa recortando el fondo original y ubicándola dentro de un recuadro rectangular llamado máscara binaria.

La segunda etapa es la del reconocimiento o comparación de la imagen resultante con las de la base de datos.

En los últimos años se han realizado progresos considerables en la detección y reconocimiento de caras, especialmente en el proceso denominado "*mug shots*", que son fotografías donde solo se ve la vista frontal de la cabeza del sujeto a reconocer tomadas con iluminación controlada y siempre con la misma escala. Los mejores resultados han sido obtenidos en 2D (dos dimensiones) utilizando técnicas basadas en el análisis de características, técnicas basadas en las *eigenfaces*[6] o eigenimágenes, o bien combinando ambas técnicas.

El análisis de las características faciales se realiza por medio de operaciones matemáticas recursivas para encontrar los componentes únicos o propios de la muestra, concepto que a veces se refiere con el término alemán "*eigen*". De esta manera la imagen se descompone en un conjunto de áreas de luz y sombras dentro de un determinado patrón. El resultado es entonces que una cara resulta ser la combinación de dichas áreas únicas de esa cara.

Algunos productos trabajan con imágenes térmicas logradas con cámaras infrarrojas que permiten crear mapas de venas subcutáneas. Estos sistemas

[6] El término alemán 'eigen' se refiere a la matemática recursiva usada para analizar características faciales únicas.

resultan más precisos especialmente al no depender de cambios en la superficie de la piel y, por supuesto, pueden llegar a operar en la oscuridad.

La fase final del reconocimiento comparará las características únicas encontradas con las características correspondientes de la base de datos.

Pero como no hay seguridad invulnerable en el mundo, el reconocimiento facial tiene sus errores; la revista alemana "C't" siguió sus pasos, con una prueba más amplia en once dispositivos comerciales presentados en la feria CEBIT. La mayor parte del mercado biométrico se centra en la huella dactilar, seguida del reconocimiento facial y de iris. Todos fueron derrotados. Los sistemas faciales fallaron al dar por buena la foto o el vídeo de la cara de una persona. [19]

En nuestro mundo la tecnología no se estanca, y si los críticos echan de menos el método de reconocimiento facial, alguien trata de demostrar lo contrario. En un artículo del 12-03-2003 señala que unos gemelos muy idénticos de 22 años, casi imposible de diferenciar, han aplicado una nueva tecnología para el reconocimiento de rostros de una manera que podría revolucionar la seguridad internacional. "Se lo dije como un chiste: si consiguen desarrollar un sistema que los pueda distinguir entre sí, tendrán una nota de 100", dijo el profesor de los gemelos, Roin Kimmel, del Instituto Technion, de Haifa. "Lo lograron y tuvieron un 100. Son brillantes", agregó.

1.2.6.4.2. Características de una nueva tecnología [20]

La tecnología que han desarrollado estos dos jóvenes, escanea y hace un mapa del rostro humano como una superficie tridimensional, suministrando una referencia mucho más precisa para identificar a una persona que los sistemas actuales, la mayoría de los cuales se basa en imágenes de dos dimensiones, dijo Kimmel.

El producto potencialmente puede cubrir un amplio rango de necesidades de seguridad, en un mundo sacudido por los atentados del 11-Septiembre. Kimmel y uno de sus ex alumnos, Assi Eld, ya habían desarrollado el algoritmo usado como bloques de construcción para el sistema de identificación de rostros. Los gemelos

Bronstein construyeron un *scanner* de tres dimensiones, junto con el ingeniero Eyal Gordon, y aplicaron las ideas al reconocimiento de caras.

Los gemelos y Kimmel dijeron que querían hacer de la tecnología -registrada por una patente en Estados Unidos- un producto comercial, con un espectro de aplicaciones desde aeropuertos y zonas de seguridad fronterizas, a cajeros automáticos. "Tenemos un prototipo y vemos que la idea funciona", dijo Michael Bronstein. "Hay una esperanza de que esto se convierta en un producto comercial y nos permita a todos sentirnos más seguros".

1.2.6.4.3. Características del Autentificador

- Responde a una característica de tipo morfológico variable con el tiempo.
- En particular, la estructura facial responde a dos tipos de cambios temporales: La variación no agresiva, característica del crecimiento y del envejecimiento del individuo (variación caracterizada por aparecer de forma relativamente lenta), y la variación agresiva, debida principalmente a factores como operaciones de cirugía estética, accidentes...etc, de acción prácticamente inmediata.
- Analiza las características faciales.
- Una cámara digital captura una imagen de la cara, a partir de la cual se crea la plantilla.
- Extendido en Europa.
- Complejos comerciales y edificios lo utilizan para identificar delincuentes.

1.2.6.4.4. Sistema de Reconocimiento y Métodos utilizados [21] [22][23]

Lo sistemas de reconocimiento facial están englobados dentro de las técnicas FRT (*Face Recognition Techniques*). Estas técnicas de aproximación al reconocimiento facial, pueden clasificarse en dos categorías según el tipo de aproximación: holística o analítica.

La aproximación holística (método de las *eigenfaces*,) considera las propiedades globales del patrón, mientras que la segunda considera un conjunto de

características geométricas de la cara. Existen dos divisiones de este segundo tipo de aproximación: la basada en los vectores característicos extraidos del perfil, y la basada en los vectores característicos extraidos a partir de una vista frontal de la cara.

Una división más general y conocida es la siguiente: Métodos basados en detección de características y métodos basados en la imagen propiamente dicha.

a. Métodos basados en detección de características

También llamados "*featured-based*" o "eigenfeature", son los métodos tradicionales basados en detección de características, es decir que utilizan datos explícitos como modelos colorimétricos o geométricos de caras, es decir se enfocan en los rasgos faciales; estos métodos se basan en buscar determinados elementos que componen una cara, como pueden ser los ojos, líneas de contorno, distancias entre las características faciales como la nariz, ojos, estructura ósea, boca y pestañas.

Hacen uso de características de bajo nivel como son los bordes, los niveles de gris, el color y el movimiento. La distribución de mínimos locales de niveles de gris puede señalar la presencia de cejas, pupilas y labios y por lo tanto marcar la presencia de una cara en la imagen, a esta técnica se la llama "información de grises". En un espacio de crominancia normalizado, el color de la piel, sea cual sea el grupo étnico al que pertenezca la cara a detectar, puede ser modelado mediante una distribución gaussiana sencilla. Características faciales de mayor resolución pueden ser buscadas secuencialmente, comenzando con los ojos, o por grupos mayores de características. La mayoría de las técnicas anteriores se utilizan sólo para detección de cabezas y hombros y en escenas frontales.

Los métodos basados en características son apropiados para procesamiento de imágenes en tiempo real cuando el color y el movimiento son posibles. Para imágenes en niveles de gris estáticas, los métodos basados en reconocimiento de patrones son más adecuados.

Dentro de esta clasificación se puede realizar tres tipos de análisis: A bajo nivel, de rasgos y de silueta activa los mismos que se encuentran detallados en el **ANEXO A**.

b. Métodos basados en la imagen

También llamados "*image-base*", son los más recientes y se basan en métodos de reconocimiento de patrones, en los que se incluye la técnica basada en los *eigenfaces*, que obtienen la información de manera implícita mediante el aprendizaje desde ejemplos o patrones.

En seguridad se puede tener necesidad de reconocer automáticamente a individuos en una escena; para resolver este problema como la detección de múltiples caras en fondos no controlados, se utilizan los detectores basados en reconocimiento de patrones o aprendizaje de ejemplos, sin utilizar una formulación explícita para la cara. La mayoría de estos métodos requieren como paso preliminar un costoso proceso de búsqueda por ventanas a diferentes resoluciones (diferentes escalas y posiciones). Estos detectores se basan en redes neuronales artificiales que distinguen entre entradas que son rostros de los que no lo son.

En este tipo se puede mencionar dos métodos: El de los *eigenfaces* y Redes Neuronales.

b.1. Método de los Eigenfaces

En el análisis de características se pretende reconocer al sujeto a partir de ciertas características extraídas de la imagen, como la distancia entre los ojos, la longitud de la boca, etc. En las técnicas basadas en *eigenfaces* se cambia el espacio original de la imagen por otro espacio generado a partir de las imágenes originales, esto se realiza haciendo uso de la transformada de Karhunen-Loeve y también se conoce como la técnica estadística PCA (Análisis de Componentes Principales) donde las imágenes faciales se expresan como un subconjunto de sus vectores propios o eigenvalores, de ahí su nombre "*eigenfaces*". Existen otros

5) Se repite desde el paso 2, aumentando en cada iteración el tamaño de la ventana, hasta que la ventana alcance el tamaño de la imagen original.

Este algoritmo se caracteriza por ser lento, pero compensa por su alto porcentaje de aciertos.

1.2.6.4.5. Características del Sistema

- No existe contacto del autentificador con el sistema de reconocimiento.
- Permite la identificación de personas en movimiento.
- Sistema con posibilidad de camuflaje (las personas no pueden conocer que son objeto de un proceso de reconocimiento).
- Reconocimiento de sujetos no dispuestos a cooperar.
- El sistema de captura necesita de una fuente de luz auxiliar.
- Susceptible a problemas de iluminación.
- Sistema vulnerable al reconocimiento de sujetos que se han sometido a operaciones de cirugía plástica (estéticas y de cirugía en general).

1.2.6.5. Geometría de la mano

Desde las pinturas rupestres, la huella de la mano siempre ha sido un signo identificador de la humanidad. Ya en el 600 a. c. chinos y japoneses la utilizaban para firmar contratos, y más de mil trescientos años después, en 1859, un gobernador inglés de un distrito de Bengala incorporó esta aplicación a documentos oficiales.

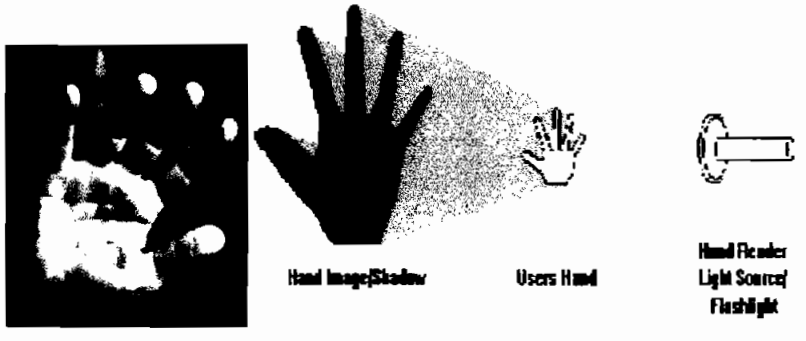


Figura 1.12: Sombra geométrica de la mano. [24]

Ésta es otra forma biométrica con una historia de dos décadas. En una operación de poco más de un segundo, un sistema de este tipo permite obtener un registro tridimensional de las principales características de la mano y/o los dedos tales como longitud, ancho y altura, algunas áreas particulares, etc. así como posiciones relativas de dedos y nudillos. Con esa información, existen sistemas que crean un mapa tridimensional del contorno de la mano que luego vuelca a un código de 9 bytes (72 bits). Se podría pensar que son más que suficientes los casi 40.000 trillones de números diferentes (las claves más comunes son de 56 y 64 bits). En la práctica, sin embargo y con los productos actuales, no se alcanza el nivel de eficiencia logrado con otros sistemas biométricos. Además, el análisis puede verse afectado por heridas, desgarros e hinchazones.

Uno de los primeros usos del mecanismo de geometría de manos fue en el sistema de seguridad de los juegos Olímpicos de 1996. De hecho el bajo costo y facilidad de uso de estos sistemas está facilitando su difusión en aplicaciones muy diferentes. Se lo está usando, por ejemplo, para identificación personal en operaciones con cajeros automáticos y tarjetas de crédito.

Mientras en combinación con un PIN algunas grandes compañías realizan el chequeo de asistencia del personal, en el otro extremo se lo implementa para control de las personas que retiran niños de guarderías e instituciones educativas. Se lo encuentra también en centros de datos así como para el acceso a dormitorios de universidades.

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura (ver figura 1.13). Una vez que la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (ancho, longitud, área, determinadas distancias...) en un formato de tres dimensiones.

corazón.

En esta categoría también es usual incluir el reconocimiento de la palma de la mano por medio del escaneado correspondiente que se analiza luego de manera similar al reconocimiento de huellas dactilares ya comentado. Los principales inconvenientes de estos sistemas son el mantenimiento que requieren debido al

Estos novedosos sistemas introducen este nuevo tipo de características de la disposición natural de la mano, propio de cada individuo, las mismas que son definidas al considerar un sistema de referencia propio para cada mano en vez de una estrategia de sistema de coordenadas universal. Consecuentemente, todas las medidas son referenciadas sobre cada sistema propio, esperando una invarianza en la imagen para todos los registros de un mismo individuo. Esto hace que no sea necesario delimitar la mano por medio de pivotes ni obligar al usuario a adoptar un posicionamiento determinado. El único requisito exigible es que el usuario extienda su mano de modo natural antes de tomar una muestra. Esto implica que el prototipo desarrollado sea flexible, fácil de mantener y fácil de utilizar.

Para obtener estos datos es necesario un procesamiento más complejo de la imagen para detección de las articulaciones y segmentación de cada dedo, que se describirá en el siguiente apartado.

Se obtiene así un total de 70 medidas geométricas sobre una colocación libre de la mano basándose en medidas físicas (longitudes, anchos de dedos y falanges etc...) y en datos referentes a la posición natural de la mano (posiciones, plantillas de borde, etc...). Además se puede obtener medidas de la mano derecha e izquierda, por lo que se tienen el doble de datos e incluso se pueden estudiar la correlación existente entre ambas manos de un individuo, ya que como se sabe no existe simetría exacta entre el lado izquierdo y el derecho del cuerpo humano.

Figura 1.15: Prototipo para obtención de las características basado en la disposición natural de las manos. [25]

a. Proceso de extracción de características invariantes de la mano

El proceso de extracción de características comienza con la obtención del sistema de referencia de la mano. Para ello se necesita una alineación previa de la imagen de la mano respecto al eje Y de la imagen, de forma que la mano sea posicionada dentro de la imagen con una orientación concreta, ya que la mano ha sido capturada en la disposición libre con la que el usuario la colocó en la plataforma.

Ya alineada la mano con los ejes de la imagen, se procede a extraer el sistema de referencia. Este sistema de referencia se basa en dos puntos invariantes en la mano: la posición del extremo del dedo corazón y la posición del extremo del dedo pulgar. Estas posiciones corresponden con los puntos más alejados en los ejes de coordenadas X e Y, respectivamente, de la imagen. Esto se puede observar en la figura 1.16.

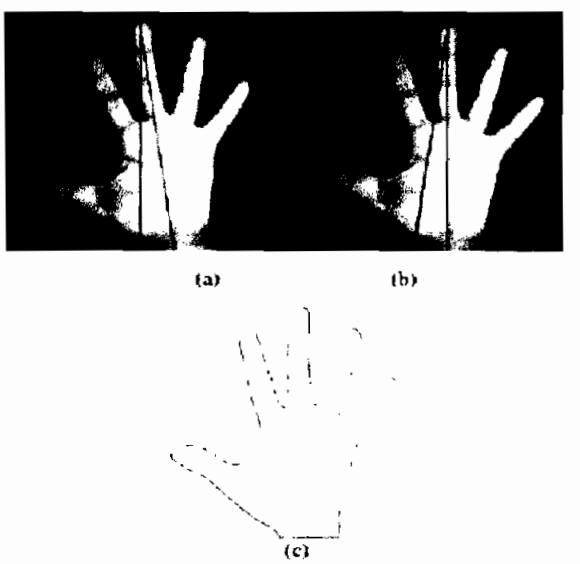


Figura 1.16: (a) Imagen original en posición libre, (b) la imagen después de realizar la alineación junto con el sistema de referencia, (c) situación del sistema de referencia. [25]

Definido el sistema de referencia propio, la imagen de la mano es trasladada, figura 1.16 (b), y se procede a la extracción de características. En el presente caso, se han distinguido dos tipos de características invariantes:

1) La geometría de la mano.
2) La disposición natural de la mano.

a.1. Características invariantes basadas en la Geometría de la mano

El proceso comienza con la extracción del contorno y tamaño de la mano. Posteriormente se obtienen los puntos característicos como son, los máximos correspondientes a las 5 extremidades de los dedos y los 4 valles. Este proceso es crucial para la segmentación de los dedos, para ello se implementa un proceso robusto de obtención de estos puntos mediante interpolación por β-*splines*[7].

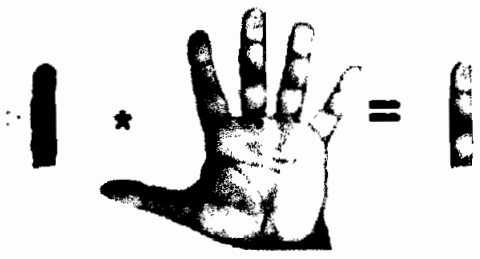
Con estos puntos, además de almacenar su posición relativa al sistema y obtener distancias y ángulos relativos al origen, se pueden hallar medidas de distancias entre valles y crestas de los dedos, como muestra la figura 1.17 (b).

Figura 1.17: (a) Mano centrada en el nuevo sistema y posiciones de los valles y las crestas, (b) Medidas calculadas a partir de los puntos de los valles y las crestas. [25]

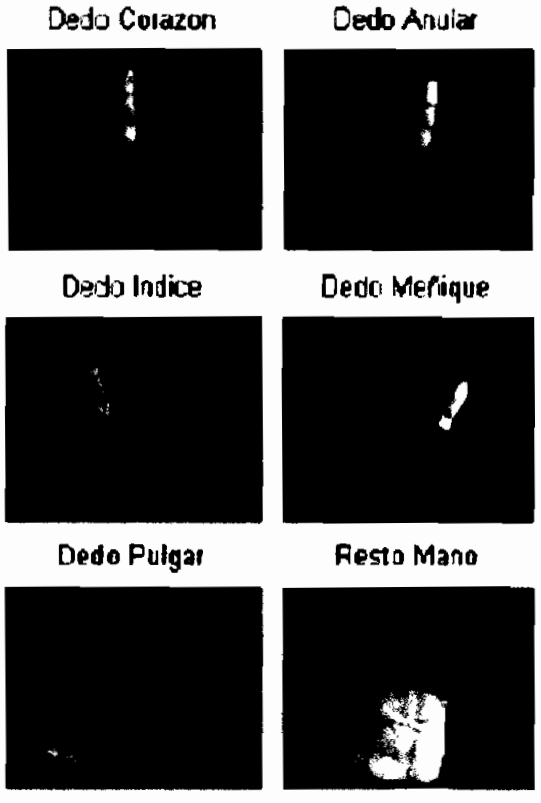
El siguiente proceso que se realiza es la segmentación de los dedos, figura 1.18. De forma que se puede trabajar de manera independiente con cada dedo y la palma de la mano. Este proceso de segmentación es el siguiente:

[7] La interpolación mediante *splines*, es una variedad de la interpolación de una función mediante funciones que son polinomios por partes. Lo que distingue a las *splines* del resto de las interpolaciones con polinomios por partes, es que éstas tienen una cantidad determinada (dependiendo del grado de la *spline*) de derivadas continuas. Dicho en forma poco rigurosa, se le impone a la función interpoladora una cierta suavidad en la unión de los polinomios que la componen.

1) Corte del dedo respecto el resto de la mano.
2) Obtención del contorno cerrado del dedo.
3) Generación de una máscara del dedo.
4) Operación AND de la imagen original y la máscara.
5) Almacenamiento del resultado.



(a)



(b)

Figura 1.18: (a) Proceso de segmentación de un dedo, (b) Salida del proceso de segmentación de la mano. [25]

Tras este proceso es posible calcular medidas referentes al tamaño y longitud de cada dedo y de la palma de la mano.

El siguiente procesamiento se realiza sobre cada dedo para obtener la división en falanges del mismo. Esto lleva un procesamiento de la imagen más complejo, ya que se basa en las líneas marcadas por los pliegues de los dedos en las articulaciones de cada falange. Existen problemas de ruido en la imagen procedente de reflejos o sombras que dificultan el proceso de imagen. Para solventarlo, se realiza el proceso siguiente:

1) Aumento del contraste de la imagen.
2) Cálculo del esqueleto del dedo para detectar su eje medio, y posteriormente el ángulo de inclinación.
3) Obtención de líneas paralelas al eje del dedo. Se obtienen puntos referentes a los máximos locales de intensidad de la imagen en esas líneas.
4) Agrupación de los puntos característicos respecto el ángulo mínimo de inclinación.

Por ponderación de intensidad y distancia al centro, se eligen las dos líneas de corte que representan las articulaciones de las falanges. Este proceso está ilustrado en la figura 1.19 (a). Con los dedos ya divididos en falanges se obtienen medidas referentes a las longitudes y tamaños de cada falange, así como el ancho del dedo en el corte o articulación de la falange figura 1.19 (b).

a.2. Características invariantes basadas en la Disposición Natural de la mano

El uso de una disposición natural de la mano tiene dos objetivos: evitar los problemas derivados del aprendizaje en la colocación de la mano y proporcionar nuevas invariantes personales. Teóricamente la disposición de los dedos de una mano completamente extendida es casi invariable y es, además, propia de cada individuo. La figura 1.20 ilustra la disposición natural en tres muestras tomadas para un usuario donde la disposición cercana de los dedos índice y anular se mantiene. Por otra parte, la posición natural de los dedos permite definir sistemas de referencia distintos para manos aparentemente semejantes.

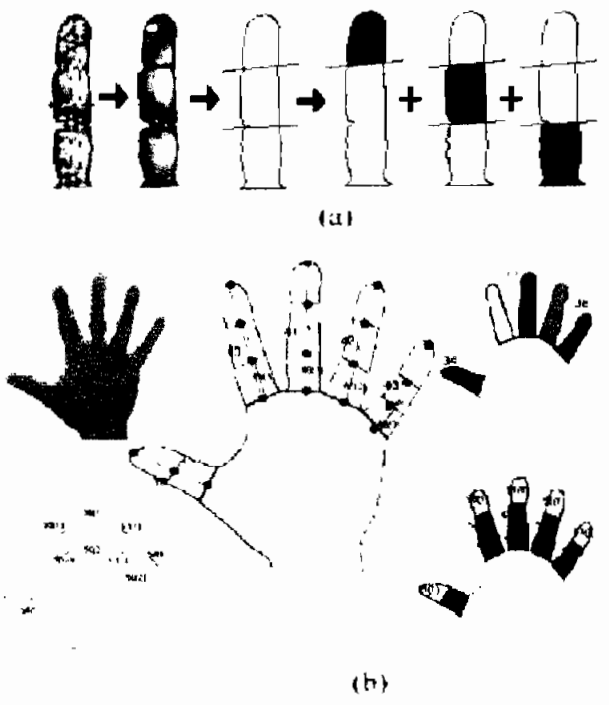


Figura 1.19: (a) Proceso de detección de las falanges; (b) Resto de medidas obtenidas. [25]

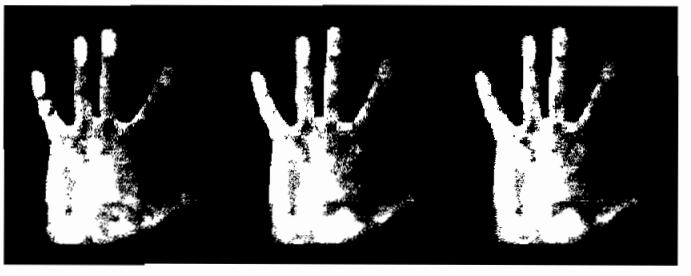


Figura 1.20: Invarianza de la disposición de los dedos. [25]

La figura 1.21 muestra dos manos de parámetros geométricos muy parecidos pero donde los sistemas de coordenadas propios son diferentes (se marca el origen para cada mano). Cuando se consideran ambas imágenes referenciadas a sistemas de referencia propios, la disparidad de las manos es evidente. Igualmente en la figura 1.21 se muestra el aumento de disparidad entre ambas.

obtienen las funciones de módulos *f* y argumentos *g*. La figura 1.22 (c) y (d) muestran las funciones *f* y *g* respectivamente para un ejemplo dado.

2) Características geométricas: Longitud de borde en **E** y área de mano en I_N. Estas medidas geométricas son sensibles a la colocación natural de la mano para cada persona.

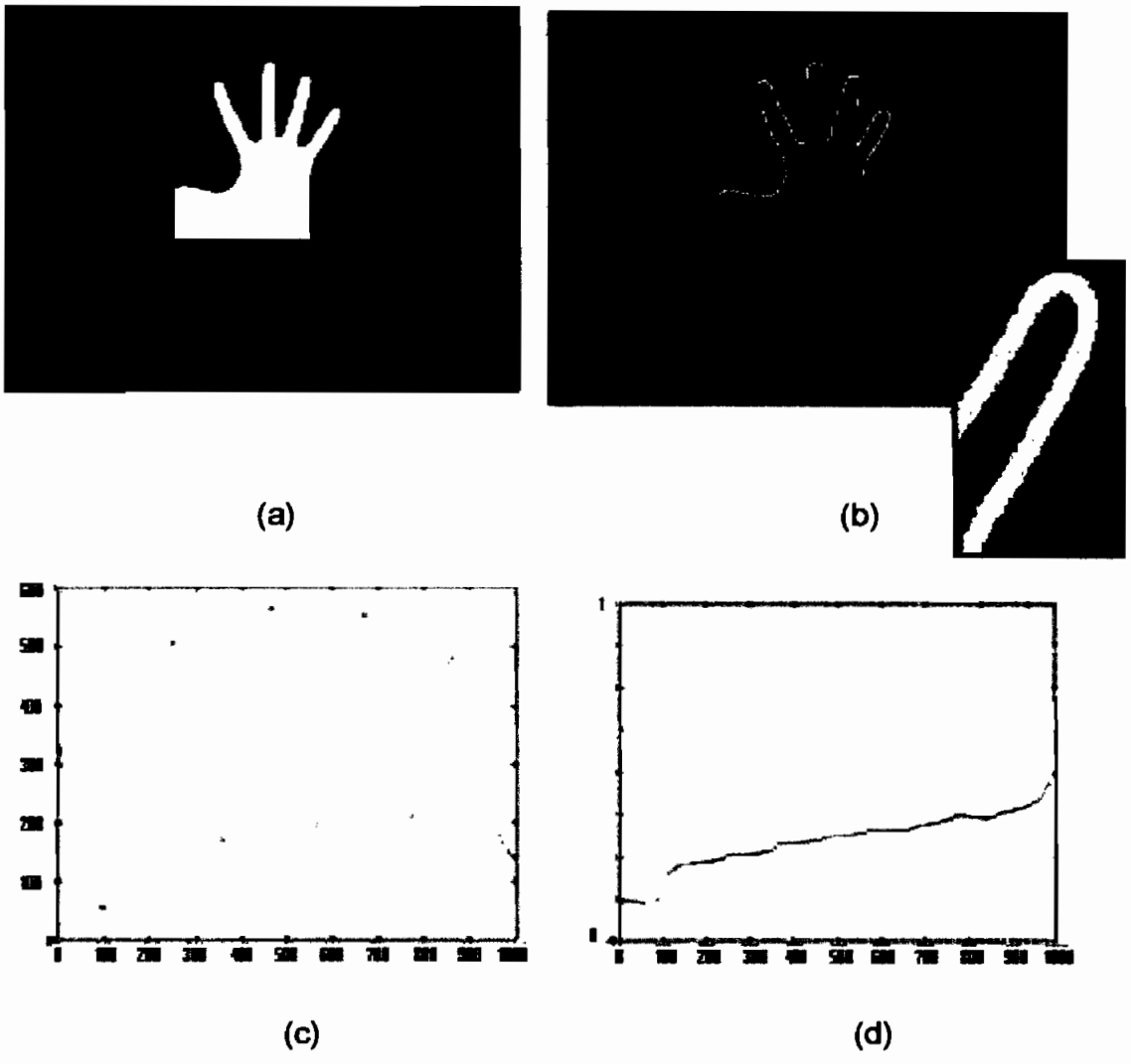


Figura 1.22: (a) Plantilla I_N, (b) Imagen de borde extendido E, (c) Función de módulo, (d) Función de fase del contorno. [25]

Un producto que ya está en el mercado es el de la empresa norteamericana *Recognition Systems*, la serie *Handkey*.

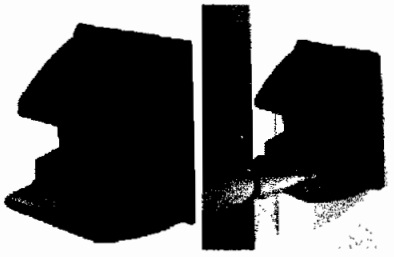


Figura 1.23: Equipos lectores de la geométrica de la mano serie *Handkey*

Estos equipos son fabricados desde 1986 y fueron introducidos en el mercado mexicano en 1990 por DICSA. A la fecha existen más de 1,700 unidades instaladas a lo largo y ancho de México en empresas e Instituciones de todos los tamaños cubriendo aplicaciones de Control de Puntualidad y Asistencia, Acceso, Firma Digital, Acceso a Comedores, etc. Están basados en el reconocimiento tridimensional de la mano; largo, ancho y espesor, son algunas de las más de 90 medidas que se toman en cuenta para conformar la identidad biométrica de la persona. Esta tecnología es la más utilizada mundialmente, siendo líder del mercado con una participación del 36% según la publicación inglesa *Biometric Technology Today* (1998). [27]

En la tabla1.2 se ve una comparación entre algunos productos existentes en el mercado.

Empresa	**BioMet Partners**	**Recognition Systems, Inc.**
Producto	**Digi-2**	**HandKey ID3D**
Tasa Falso rechazo	0.1%	0.1%
Tasa Falsa Aceptación	0.1%	0.1%
Tasa de igual error	0.1%	0.1%
Tiempo verificación	1 segundo	1 segundo
Autónomo	Sí	———
Red	Sí	Sí
Emulación de lector de tarjetas	Sí	No disponible

Tabla 1.2: Productos biométricos basados en la Geometría de la mano.

1.2.6.6. Reconocimiento de Iris y de la Retina

Los sistemas basados en los ojos de las personas generalmente son los que ofrecen mayor seguridad entre los métodos biométricos, gracias a la unicidad de los patrones individuales y la calidad de los dispositivos de captura. Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: análisis de patrones retinales o análisis del iris.

Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de potenciales usuarios, la probabilidad de coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

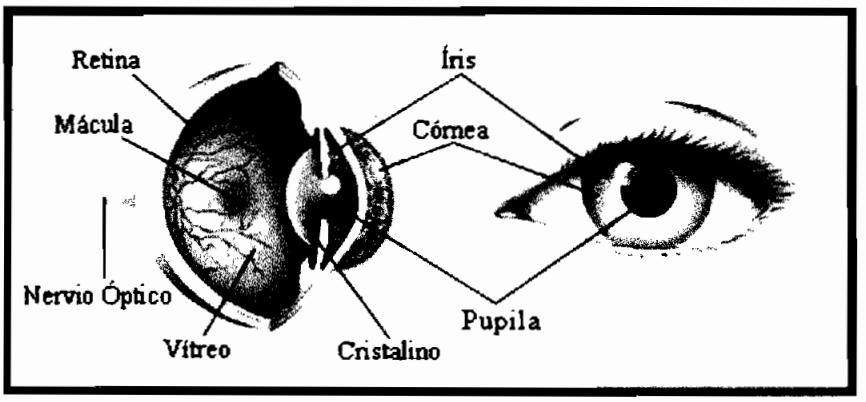


Figura 1.24: Partes del ojo humano. [11]

1.2.6.6.1. Reconocimiento de Iris

El iris es la franja de tejido que rodea la pupila del ojo que a simple vista diferencia el color de ojos de cada persona. Tiene una estructura compleja de estrías, anillos, surcos, coronas y flecos que ofrece prácticamente infinitas variaciones incluso entre ambos ojos de la misma persona, y que además, permanece constante con el tiempo. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

Es necesario notar que el iris y la pupila no responden a circunferencias concéntricas (no presentan el mismo centro).

Un sistema de reconocimiento por medio del iris, está basado en la gran cantidad de detalles que posee su textura. Entre las características visibles más importantes en un iris están: Criptas, pecas, grietas, coloraciones, anillos, coronas, estrías y huecos.

Todas estas características y otras que son determinadas por diferentes tejidos que conforman el iris lo hace un órgano distintivo, que puede ser utilizado como elemento de identificación al ser fotografiado a cierta distancia y bajo ciertas condiciones externas de iluminación. Otras propiedades que lo hacen adecuado para identificación son:

- Es un órgano protegido y aislado del ambiente externo ya que se encuentra en el interior del ojo detrás de la córnea y del humor acuoso.
- Clínicamente es imposible modificarlo sin riesgos de perder la visión.
- Su respuesta fisiológica a la luz, permite experimentos naturales en contra de cualquier intento de trampa.

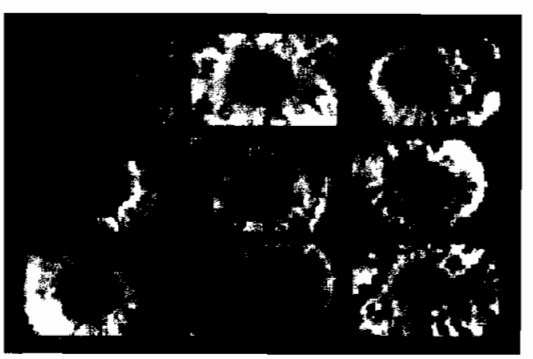


Figura 1.26: Características visibles en un iris.[28]

b. Sistema de Reconocimiento [28]

Mediante un proceso de adquisición riguroso, el sistema captura la imagen a nivel de grises mediante *scanners* que captan la superficie del ojo (no se realiza, por tanto, ningún tipo de reconocimiento a nivel cromático); este tipo de adquisición

dota al sistema de invarianza a escalados, desplazamientos y rotaciones presentes en la imagen original. Posteriormente se realiza una etapa de preprocesado de la imagen, de la cual, se detallarán sus pasos de forma rigurosa, por considerar éstos, de vital importancia dentro de todo el proceso de reconocimiento para asegurar un óptimo resultado (figura 1.27):

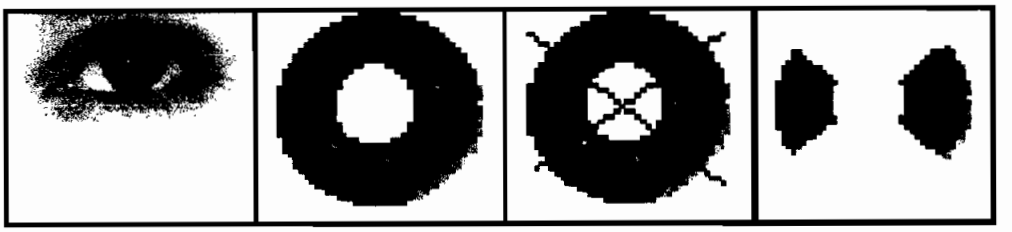


Figura 1.27: Preprocesado sobre la imagen adquirida. [30]

Un sistema de estas características está conformado por tres etapas: Adquisición, análisis, y codificación.

Adquisición

Localización y aislamiento de la estructura del iris a partir de la detección de los contornos exterior e interior del mismo (frontera con la esclerótica y la pupila respectivamente), mediante un algoritmo iterativo de búsqueda del máximo gradiente de intensidad a lo largo de una circunferencia (aprovechando la geometría circular del iris y de la pupila).

La etapa de adquisición se encarga de la captura de las imágenes, las cuales son almacenadas generalmente en formato JPG de 640x480 y a color. Es de vital importancia que con el sistema de adquisición se logre obtener imágenes de características que varíen dentro de un intervalo razonable (iluminación constante y uniforme, distancia focal, nitidez), debido a la necesidad de establecer criterios comunes a todas las imágenes, que permitan el correcto funcionamiento de las siguientes etapas.

El análisis del iris comienza con la determinación de los límites que lo conforman. Estos límites se pueden denotar como: Frontera límbica o exterior y frontera

diferencia del resto de objetos presenta la mayor área, característica que se aprovecha para ubicarla. Para optimizar este paso, antes se aplica en forma local, un filtro que disminuye la cantidad de objetos en la imagen (figura 1.31).

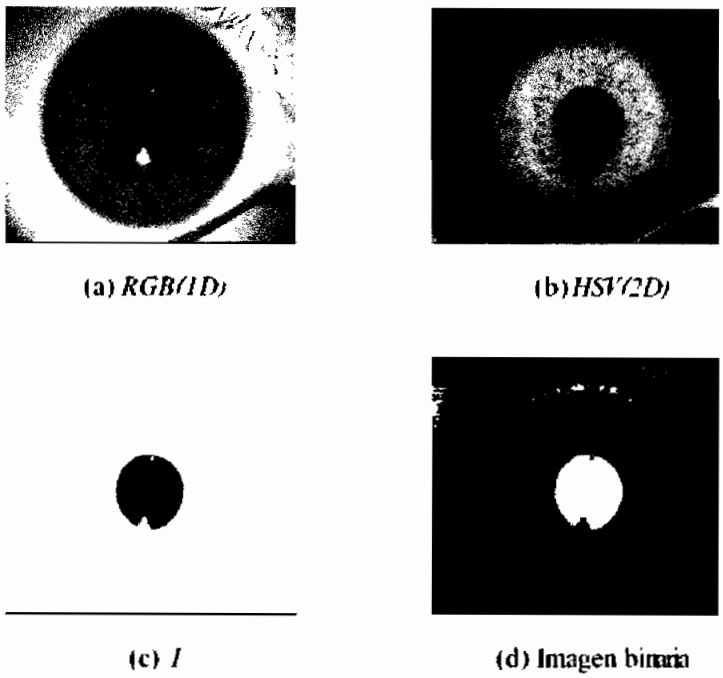


Figura 1.30: Pasos para obtener la imagen binaria en iris miel, café o verde. [28]

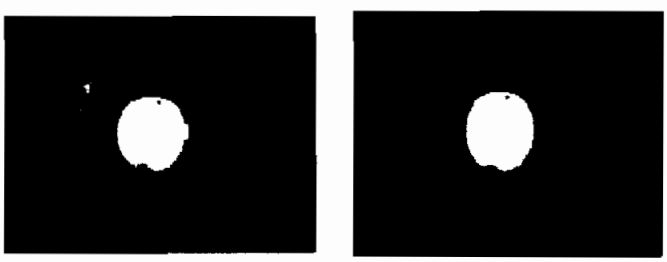


Figura 1.31: (a) Imagen binaria después de aplicarle el filtro de mediana, (b) pupila ubicada. [28]

Para un caso en particular se puede trabajar con una ventana de 10 x 10 pixels ya que es la que mejores resultados presenta en cuanto a tiempo de procesamiento y eliminación de ruido. Luego de ubicar la pupila a nivel de objeto, se localiza de una forma más detallada determinando, por su forma aproximadamente circular,

su radio y su centro. Para obtener mayor exactitud en los valores de radio y centro, es conveniente eliminar huecos existentes en el área de la pupila (figura 1.32).

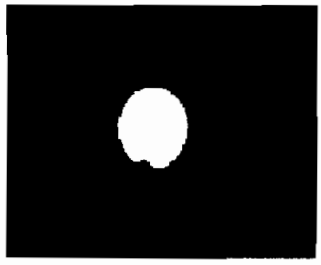


Figura 1.32: Pupila rellena. [28]

La forma de la pupila no es netamente circular, sin embargo, es aproximado.

Para localizar el centro de la pupila, se obtienen las filas y columnas que corresponden a cada uno de los píxeles que la conforman (figura 1.33).

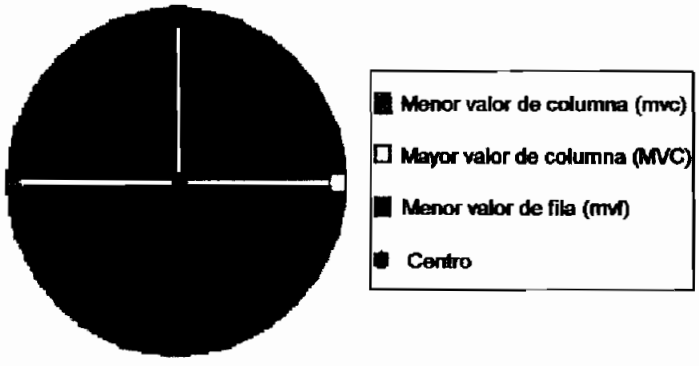


Figura 1.33: Localización del centro de la pupila. [28]

Se resta el mayor y el menor valor de columna (*MVC* y *mvc* respectivamente). A partir de esta distancia dividida en dos, se obtiene el valor de columna del píxel del centro *PC*.

$$PC = \frac{(MVC - mvc)}{2} \tag{1.4}$$

Este procedimiento se podría aplicar para ubicar la fila del píxel del centro *PF*, pero por la ubicación del reflejo de la luz dentro de la imagen, es más acertado tomar el menor píxel de fila *mvf* y sumarle el valor de *PC*.

$$PF = mvf + PC \tag{1.5}$$

A partir de este centro se determina el radio pupilar. Para esto se utilizará un modelo elíptico (figura 1.34) ya que es el que mejor se adapta a la forma aproximadamente circular de la pupila. Con este modelo, se podrá establecer dos radios, uno a partir de la longitud del eje menor de la elipse contenida dentro de la pupila y otro con el eje mayor. Como la idea es no perder información, se toma el eje menor.

Figura 1.34: Modelo elíptico. [28]

Para obtener la frontera límbica no hay necesidad de hacer ningún procedimiento ya que, en el momento de adquirir la imagen se puede utilizar una plantilla para la cámara que permiten mantener un tamaño estándar para el limbo; para el caso de la pupila esto no es aplicable ya que ella está sujeta a cambios de tamaño por la dilatación y contracción. En aplicaciones reales, es ideal encontrar la forma de ubicar este límite. Esto podría hacer aprovechando la forma aproximadamente circular del iris. Los radios tanto límbico ***rl*** como pupilar ***rp*** determinarán el área de análisis para el procesamiento (figura 1.35).

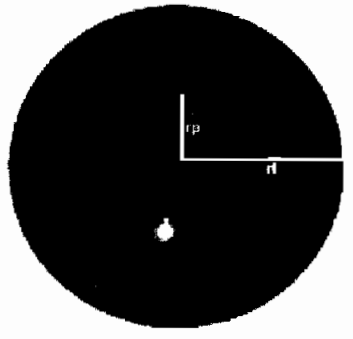


Figura 1.35: Radios límbico (rl) y pupilar (rp). [28]

Debido a la imposibilidad de fijar a priori el grado de abertura/cierre del párpado en el momento de la adquisición, se dividirá la imagen en cuatro sectores (sectores izquierdo, derecho, superior e inferior), eliminándose posteriormente los sectores

superior e inferior. La extracción de características se realizará, por tanto, a partir de la información relativa a los sectores L (izquierdo) y R (derecho). (figura 1.27: Preprocesado sobre la imagen adquirida).

Figura 1.36: Área de análisis. [28]

Finalmente se realizará una reordenación de la información resultante mediante un muestreo tanto en radio como en ángulo de la misma, obteniendo una imagen cuadrada o en forma de cinta (figura 1.38 (a)). (Las columnas indican fracciones de radio, mientras que las filas responderán a incrementos de ángulo).

Para esto, primero se toma como centro de coordenadas el centro pupilar ya determinado. Luego, se ubican todos los puntos del área de análisis en coordenadas polares (figura 1.37), ya que estas coordenadas son las más apropiadas por la forma aproximadamente circular del iris. Con un muestreo punto a punto del radio *r* y de 0.017° φ del ángulo se obtienen dichas coordenadas. El máximo y el mínimo radio son el límbico y el radio pupilar respectivamente.

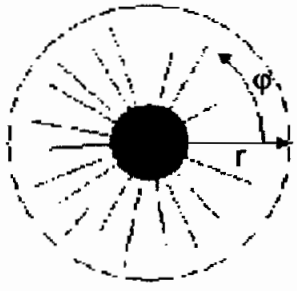


Figura 1.37: Coordenadas polares. [28]

Inmediatamente después de obtener todas las coordenadas polares, éstas son convertidas a coordenadas cartesianas. Con estos valores de $y_{r,\varphi}$ y $x_{r,\varphi}$ se interpola el anillo obteniéndose finalmente una cinta rectangular de fácil manipulación. Estos valores de muestreo se fijan por el tamaño de la imagen buscando contener la mayor cantidad de información, y por tiempos de procesamiento. Se toma la cinta en tonos de rojos (figura 1.38 (a)) ya que es la que la que mejor contraste tiene.

(a) (b)

Figura 1.38: (a) Cinta de análisis, (b) Cinta contrastada. [28]

Las dimensiones de las cintas generadas con el procedimiento anterior pueden ser diferentes debido a que el iris se comporta como una membrana elástica en la cual los detalles se desplazan proporcionalmente en dirección radial a la dilatación o contracción de la pupila en el momento de la adquisición. Esto hace necesario la aplicación de una transformación que asegure que los detalles para un mismo ojo se encuentren en, aproximadamente, el mismo lugar. Esta transformación se hace interpolando linealmente las cintas a un tamaño aproximado de 60 píxeles de ancho (figura 1.39).

Figura 1.39: Cinta interpolada. [28]

Análisis y Codificación

El análisis matemático o procesamiento de la cinta se hace por medio de filtros de Gabor en 2D que tienen la particularidad de ser localizados en frecuencia y además de ser muy utilizados para caracterización de texturas. Los coeficientes generados por la convolución de la cinta con los filtros, se codifican de la siguiente forma: 1 para los coeficientes mayores o iguales a cero y 0 para los coeficientes

menores a cero. Es muy importante que los códigos tengan el mismo formato y longitud constante (número de coeficientes estándar), a pesar de la cantidad de detalles que un iris pueda tener. Si esto no se tiene en cuenta, podría presentarse el caso en el que se comparen dos códigos de tamaños distintos dando lugar a parciales correlaciones y no correlaciones. Esto facilita la etapa de comparación, y mejora la velocidad y la confiabilidad en el reconocimiento de un iris. Tanto el análisis como la codificación encierran una matemática que se escapa al entorno analizado en este documento.

Posteriormente se procederá a la extracción de características para generar el vector patrón utilizando para ello un proceso de filtrado mediante *wavelets*[8]. El sistema de reconocimiento finalizará, tras aplicar el algoritmo de *matching* basado en la mínima distancia entre el patrón de prueba y todos los modelos.

c. Características del Sistema

- Una de las tecnologías biométricas más exactas.
- El usuario puede usar los lentes al momento de la lectura.
- Sistema de difícil falsificación.
- La resolución del sistema será función de la calidad de la imagen de la estructura del iris.
- El sistema es invariable al uso de lentes de contacto o gafas ya que la estructura del ojo no se ve alterada según dichos elementos. Así mismo, se tratará de un sistema invariante a lentes de contacto de colores o gafas de sol ya que el color no responde a ningún grado de libertad dentro del sistema de reconocimiento evaluado.
- La detección del fraude (por presentación, por ejemplo, de una foto del iris a reconocer), se puede realizar de forma sencilla capturando dos imágenes consecutivas y comprobando mediante técnicas de correlación, la diferencia de tamaño de la pupila. Se pueden forzar también, cambios controlados de la iluminación para analizar la respuesta de la pupila a estos cambios.

[8] Las *wavelets* son familias de funciones que se encuentran en el espacio y se emplean como funciones de análisis, examinan la señal de interés para obtener sus características de espacio, tamaño y dirección. Analogía con las series de Fourier que se basan en funciones sinusoidales.

- Elevadas tasas de reconocimiento. A continuación se detallará las tasas conseguidas a nivel comercial: FAR= 0.0006% y FRR=0.0007%. [29]
- Elevado tiempo de captura de la imagen (proceso de escaneado del ojo): entre 30 y 60.
- Baja aceptación popular.
- Elevado coste.

En la tabla 1.3 se ven algunas características de los productos existentes en el mercado.

Empresa	Iriscan
Producto	**Sistema 2000EAC**
Tasa Falso rechazo	0.00066%
Tasa Falsa Aceptación	0.00078%
Tasa de igual error	0.00076%
Tiempo verificación	2 segundos (10,000 usuarios)
Autónomo	Sí
Red	Sí
Emulación de lector de tarjetas	Sí

Tabla 1.3: Productos biométricos basados en el iris.

1.2.6.6.2. Reconocimiento de la Retina

La retina es la capa más interna (llena de vénulas o venillas) de la pared posterior del globo ocular. La vasculatura retinal (forma de los vasos sanguíneos de la retina humana); es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura (figura 1.40). También permanece bastante estable con el tiempo salvo cuando resulta afectada por algunas enfermedades.

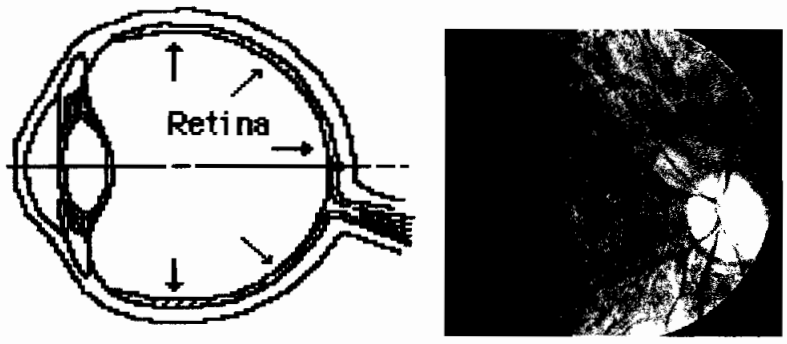


Figura 1.40: Retina Humana. [11]

Con una imagen adecuada se puede establecer un mapa muy preciso y único del patrón de conductos venosos.

En los sistemas de autenticación basados en patrones retinales el usuario a identificar debe mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se capta la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

Para un resultado adecuado la imagen debe estar bien enfocada y mantenerse quieto el usuario, lo que agrega más complejidad además del temor, y consiguiente rechazo, que puede causar el haz de luz sobre el ojo.

a. Características del Sistema

- Se comparan capilares que están situados en el fondo del globo ocular.
- Se examinan los patrones con luz de baja intensidad.
- Procedimiento intimidante.
- Más impopular.
- No debe haber lentes puestos.

La compañía EyeDentify posee la patente mundial para analizadores de vasculatura retinal, por lo que es la principal desarrolladora de esta tecnología; su página *web* se puede encontrar en http://www.eyedentify.com/.

Figura 1.41: Lector de retina de EyeDentify.

En la tabla 1.4 se observan algunas características de los productos existentes en el mercado de esta empresa.

Empresa	EyeDentify
Producto	**Icam 2001**
Tasa Falso rechazo	0.4%
Tasa Falsa Aceptación	0.001%
Tasa de igual error	———
Tiempo verificación	1.5 a 4 segundos
Autónomo	Sí
Red	Sí
Emulación de lector de tarjetas	Sí

Tabla 1.4: Producto biométrico basado en la Retina-EyeDentify.

1.2.6.7. Reconocimiento de la Voz

Si bien este sistema es menos seguro que el de las huellas dactilares y el escaneado de iris o retina, en cambio su costo lo hace más accesible.

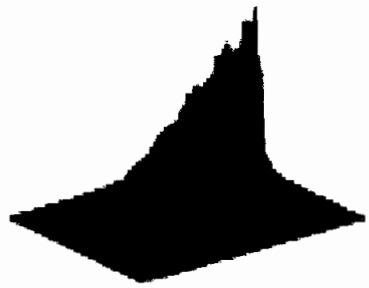


Figura 1.42: Imagen tridimensional del espectro de la voz. [11]

Su principal uso se encuentra en aplicaciones de seguridad en el acceso telefónico, para verificación de acceso a correo de voz, activación de tarjetas de crédito y hasta para constatar la identidad de personas en libertad condicional con reclusión domiciliaria. En la voz que se registra se analizan principalmente el tono (intensidad o fuerza) y la altura (frecuencia) de los sonidos; generalmente por medio del análisis eléctrico de la densidad de energía y formas de onda (por componentes armónicos), así como las inflexiones o cadencia en el hablar y el propio comportamiento lingüístico se llega a identificar a una persona.

Para el registro inicial generalmente se repite varias veces una misma frase y/o una serie de frases. De esta manera se establece el patrón individual contra el cual se compara cada vez que se recurra al sistema para verificación del usuario.

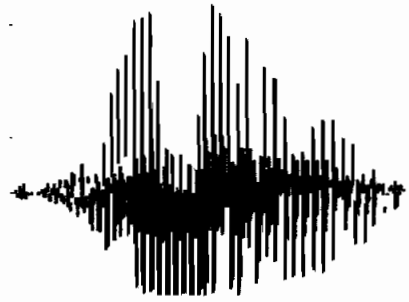


Figura 1.43: Espectro de voz. [11]

Así, cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, pronunciar el

nombre del usuario, de forma que el reconocedor lo entienda y lo autentique. Estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va 'proponiendo' a la persona la pronunciación de ciertas palabras extraidas de un conjunto bastante grande. Lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales, etc.).

La exactitud del sistema puede verse afectada principalmente por el ruido de fondo y las características del elemento que capta el sonido (teléfono por ejemplo o un micrófono), así como por variaciones naturales entre las que se puede mencionar cambios de humor, fatiga, transcurso del tiempo, etc. Es importante indicar que este sistema ocupa bastante espacio en disco.

El principal problema del reconocimiento de voz es la inmunidad frente a *replay attacks*, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos; volviendo al ejemplo anterior, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autenticador y luego reproducir ese sonido para conseguir el acceso. Prácticamente la única solución consistiría en utilizar otro sistema de autenticación junto al de reconocimiento de voz.

Por el contrario, en modelos de texto independiente, más interactivos, este ataque no es tan sencillo porque la autenticación se produce realmente por una especie de desafío-respuesta entre el usuario y la máquina, de forma que la cantidad de texto grabado debería ser mucho mayor y la velocidad para localizar la parte del texto que el sistema propone tendría que ser elevada. Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que éste necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase, es habitual que

el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión nasal hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso será autorizado o no, incluso el estado anímico de una persona hace variar su timbre). A su favor, el reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

Existen varios métodos para analizar la voz. Compañías como *Domain Dynamics*, manejan los patrones de la voz y verifican su validez a través de su información biométrica. Muchos de los sistemas de reconocimiento de voz utilizan la serie de Fourier para cuantificar los cambios de frecuencias por unidad de tiempo. Este método presenta un problema ya que no se adapta a la manera como se tiende a hablar normalmente (algunas veces más lento que otras). Para compensar este problema se necesita emplear mecanismos, como la alineación dinámica del tiempo, que requiere aún mayor retardo de procesamiento. Otros métodos representan la voz como ondas sonoras a tiempo real, así simplificando el análisis del mismo.

1.2.6.7.1. Características del Sistema

- Verificación del patrón de voz (los tonos bajos y agudos, vibración de la laringe y tonos nasales y de la garganta).
- *Hardware* necesario: micrófonos y bocinas.
- Implementación económica (un computador).
- Debilidades: factores ambientales, como el ruido, pueden afectar la verificación y los archivos utilizan mucho espacio (1 Mb).
- La tecnología está siendo mejorada.

En tabla 1.5 se presentan algunas características de los productos existentes en el mercado.

Empresa	Voice Strategies
Producto	VACS: Sistema de Control de Acceso por Voz.
Tasa Falso rechazo	———
Tasa Falsa Aceptación	———
Tasa de igual error	———
Tiempo verificación	1.5 segundos
Autónomo	No
Red	Sí
Emulación de lector de tarjetas	No

Tabla 1.5: Producto biométrico basado en el reconocimiento de la voz.

1.2.6.8. Reconocimiento de Firma

En esta sección se analizará algo que nada tiene que ver con el sistema de Firma Digital para autenticar la autoría de un mensaje por medio de claves públicas y privadas. La verificación tradicional de firmas es ampliamente conocida especialmente en el medio bancario. El sistema biométrico correspondiente, por su parte, goza precisamente de una aceptación similar en este caso como medio de verificación. Este sistema ha encontrado uso en empresas de seguro y hospitales así como en general para autenticar documentos electrónicos.

Figura 1.44: Firma. [11]

Sin embargo, ahora no se trata de observar manualmente con mayor o menor precisión la forma de una firma en comparación con la imagen de una firma registrada anteriormente. Un sistema DSV (Verificación Dinámica de Firmas) pondera y mide características de la firma, especialmente las relacionadas con el modo como se firma. Para ello se suelen usar lápices o estilos especiales sobre tabletas gráficas digitalizadoras o simples *palmtops*. Algunas de las características analizadas son la presión que se ejerce sobre el lápiz a en las diferentes partes, puntos en los que el lápiz se separa del papel, orden, velocidad y aceleración de los trazos, y agudeza de los lazos.

Para medir características como la aceleración se necesita identificar los trazos en planos de ejes coordenados con una resolución de fracción de milímetro que se muestrean periódica y sincrónicamente. La representación matemática de todas las características se guarda adecuadamente codificada para ser tomada como base cada vez que se recurra al sistema.

Algunas limitaciones de este sistema se refieren a que los cambios naturales que se producen en las firmas con el tiempo, pueden aumentar el nivel de rechazos equivocados, a lo que se suma el mayor costo respecto de otras soluciones.

Generalmente el sistema capta hora, fecha, identificación de la PC, información de chequeo del contenido del documento y alguna otra información procurando acotar el evento en sí de la firma. Sin embargo esto no demuestra que la firma realmente es auténtica. Lo mencionado en este párrafo simplemente señala un grupo de productos que procuran incorporar la firma a un documento para dar a éste validez respecto de su autor. Son formas más simples pero no seguras de suplir las conocidas firmas digitales ya mencionadas.

1.2.6.8.1. Características del Sistema

- Analiza la manera que el usuario realiza su firma personal (rapidez, presión y la forma de la firma).
- Tiene uno de los niveles más bajos de exactitud entre los lectores biométricos.

- Una de las técnicas más fáciles de introducir al usuario.

1.2.6.9. Otros Sistemas

Especialmente para los que tipean más o menos al tacto, el sistema de dinámica del tipeado también puede servirles de identificación.

Esta solución trabaja con dos métricas: por un lado capturan el tiempo de residencia, es decir el tiempo que dura apretada cada tecla, y por el otro el tiempo de vuelo, es decir el tiempo invertido en pasar de una tecla a otra. De esta manera puede obtenerse una medida del ritmo de cada usuario. Generalmente se trabaja con una palabra o frase corta que el usuario repite varias veces al momento del registro inicial, muestras que servirán para hacer comparaciones posteriores.

Otras soluciones no han salido del laboratorio o están en las primeras etapas de desarrollo. Se puede mencionar la medición de venas del cuerpo por medio de luz infrarroja, el mapeado de los poros de la piel y el análisis de la composición del olor corporal. Estas nuevas posibilidades parecen estar todavía en ambiente de ficción o películas... como alguna vez estuvieron prácticamente todos los sistemas reales y actuales comentados antes.

1.2.7. Criterios para elegir una tecnología biométrica

- Facilidad de Uso.
- Factores que inciden en la lectura: factores ambientales y condición de miembros corporales.
- Precisión: la tasa de falsa aceptación (FAR) y la tasa de falso rechazo (FRR).
- Costo: lector biométrico, capacidad de procesamiento necesaria para mantener la base de datos, instalación, implementación y entrenamiento, concientización del usuario y mantenimiento del sistema.
- Aceptación por parte del usuario.
- Estabilidad.

1.2.8. Ventajas y desventajas de los Sistemas Analizados

Puestos los sistemas juntos se puede mencionar las ventajas y desventajas más concretas que caracterizan a las diferentes soluciones.

Ventajas:

- Huellas dactilares: seguro y disponible especialmente para identificación. No acepta ni aún una cinta donde se haya levantado una impresión no visible a partir de una huella espolvoreada.
- Reconocimiento de Caras: Apto para aplicaciones de identificación de uno contra muchos.
- Geometría de las manos: Fácil de usar.
- Escaneado de iris: Muy seguro para aplicaciones de identificación de uno contra muchos.
- Escaneado de retina: Muy seguro para aplicaciones de identificación.
- Análisis de la voz: Para aplicaciones de verificación local o remota siendo de bajo costo.
- Verificación de Firma: Alto nivel de aceptación para verificación de un usuario determinado.

Desventajas:

- Huellas dactilares: Resistencia al uso por connotaciones criminales.
- Reconocimiento de Caras: Costoso y sujeto a engaños con fotos montadas sobre narices semejantes.
- Geometría de las manos: Sujeta a cambios físicos, no muy adecuada para grandes bases de datos de sistemas de identificación y verificación.
- Escaneado de iris: Costoso, sensible a los movimientos del usuario y ocupa mucho espacio.
- Escaneado de retina: Costoso, no puede usarse con algunos usuarios por su sensibilidad a un escaneado infrarrojo o láser en los ojos.
- Análisis de la voz: Sujeto a cambios físicos y cierta facilidad de engaño con voces semejantes incluso con grabaciones en algunos casos.
- Verificación de Firma: Sujeta a cambios físicos.

1.2.9. La configuración por defecto

Un factor que afecta el comportamiento especialmente de algunas soluciones es el relacionado con la configuración por defecto, es decir la configuración de fábrica.

La cuestión que interesa en este momento radica en que los productos en general pueden hacerse más seguros si se los vuelve más "estrictos" en sus comparaciones con el perfil almacenado. Pero al mismo tiempo que se gana bajando la tasa o porcentaje de aceptaciones equivocadas, también subirá la tasa de rechazos equivocados (ver Tabla 1.6). Aunque la relación no sea necesariamente inversamente proporcional, la relación inversa es real. Además, un aumento de la sensibilidad del sistema acarrea mayor procesamiento y retardo en el reconocimiento.

Entonces hay que plantearse hasta qué punto se puede aceptar una cierta cantidad de rechazos equivocados con las consiguientes molestias para los usuarios y administradores, con tal de asegurar un mayor grado de seguridad al reducir consecuentemente la tasa de aceptaciones equivocadas.

El hecho concreto es que prácticamente todos los fabricantes ofrecen una configuración por defecto que trabaja con un umbral relativamente bajo de rechazos equivocados y de hecho baja sensibilidad también a las aceptaciones equivocadas. Esta situación se nota más en los productos de reconocimiento facial y de voz.

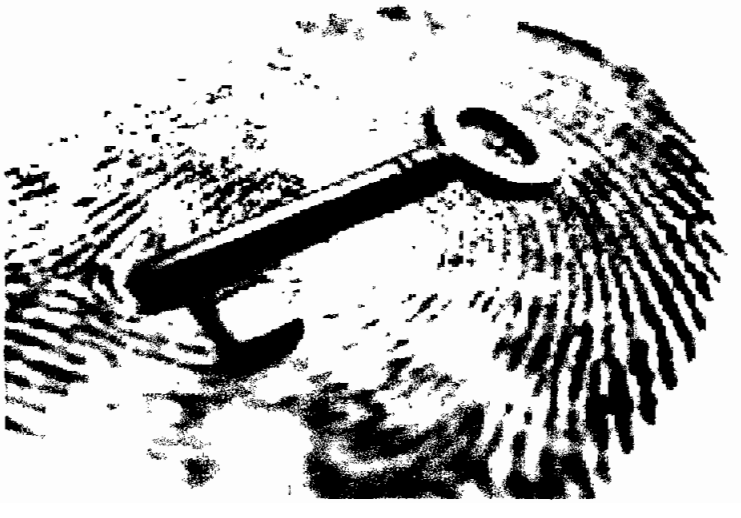
El administrador puede levantar esta sensibilidad para lograr un aumento de la seguridad del sistema, pero a costa de aumentar también el nivel de rechazos equivocados, con las molestias ya comentadas.

Adicionalmente, si las necesidades de seguridad imponen ciertas exigencias mayores se puede combinar el uso de algunas de las soluciones biométricas junto con tarjetas inteligentes.

CAPÍTULO

2

A DACTILAR, ESTUDIO Y ANÁLISIS
IDENTIFICADOR BIOMÉTRICO



CAPÍTULO 2

LA HUELLA DACTILAR, ESTUDIO Y ANÁLISIS COMO UN IDENTIFICADOR BIOMÉTRICO

2.1. RAZONES E HISTORIA

2.1.1. ¿Porqué Identificar la Huella Dactilar? [31]

Es bien conocido que los seres humanos poseemos una fina capa de la piel en las yemas de los dedos, capa que forma una superficie rugosa constituida por pequeñas líneas, algunas continuas otras interrumpidas, y que forman aparentemente caprichosos patrones como espirales y curvas. Estas huellas dactilares son únicas e irrepetibles para cada individuo y lo que es más extraordinario es que, si esta pequeña capa es dañada o inclusive hasta quemada, la nueva piel crecerá siguiendo el mismo patrón por lo que pueden ser utilizadas como un certificado de identidad.

Sin embargo, se tienen registrados extraños casos en los que las huellas dactilares del individuo están casi borradas en su totalidad, ya sea por el paso del tiempo o por que nacieron con esta condición, pues sólo unas cuantas franjas son visibles. Además, como dato curioso, se puede mencionar que, contrariamente a la creencia popular de que sólo los seres humanos contamos con huellas dactilares, los primates también cuentan con ellas, y hasta incluso los koalas. La formación de huellas dactilares es un fenómeno que no está explicado totalmente, aunque se sospecha que detrás de este fenómeno está una rama poco explotada de la ciencia y que se podría asociar a la física no lineal: la morfogénesis matemática, y que ha permitido entender patrones no solamente como los de las huellas dactilares, sino el de los dibujos de la piel de algunos peces tropicales. El hecho de que cada individuo posea un patrón de huellas dactilares característico que lo diferencie de todos los demás, ha conducido a que actualmente éstas sean utilizadas para identificar individuos en registros criminales, natales e incluso hasta legales, ya que cada individuo poseerá las mismas huellas dactilares durante toda su vida, desde los 3 meses de gestación en el vientre de la madre

hasta que muera y no serán iguales a las de nadie más. En la lectura de este documento, se referirá como huella digital aquella que es capturada por un explorador de huellas.

2.1.2. Un poco de Historia [32]

Las huellas digitales ofrecen medios infalibles de identificación personal, esa es la explicación esencial para que este método sea el más usado desde la antigüedad para las identidades de los criminales. Otras características personales cambian, las huellas digitales no.

Los romanos empleaban la aguja para hacer un tatuaje con el propósito de identificar y prevenir la deserción de los soldados. Posteriormente hubo los oficiales con memorias visuales extraordinarias, que identificaban a viejos delincuentes por medio de la vista. La fotografía disminuyó la carga de la memoria pero no era la respuesta al problema criminal de la identificación. Los aspectos personales cambian.

Alrededor de 1870 un antropólogo francés ideó un sistema para medir y registrar las dimensiones de ciertas partes huesudas del cuerpo. Estas medidas fueron reducidas a una fórmula que, se aplicaría teóricamente solo a una persona y no cambiaría durante su vida de adulto. Este sistema de "Bertillon", nombrado por su inventor, Alphonse Bertillon, fue aceptado generalmente por treinta años. Pero nunca se recuperó de los acontecimientos de 1903, cuando condenaron a un hombre llamado Will del Oeste en la penitenciaría en Leavenworth, Kansas de Estados Unidos, no se percataron que el hombre tenía las mismas medidas de Bertillon (eran casi exactas) de las del verdadero culpable, Guillermo del Oeste. Sobre una investigación que se había hecho a los dos hombres, que parecían exactamente iguales, sus nombres eran Will y Guillermo del Oeste, sus medidas de Bertillon estaban bastante cercanas identificándolos como la misma persona; sin embargo, una comparación de la huella dactilar dio como resultado que se trataba de dos personas distintas. Los hombres del Oeste eran al parecer

hermanos gemelos idénticos por expedientes descubiertos en los últimos años de la prisión citada.

Prehistoria

El dibujo de una mano con los patrones de las huellas de sus dedos fue descubierto en Nueva Escocia. En la Babilonia Antigua, las huellas dactilares fueron utilizadas en las tablas de arcilla para las transacciones de negocios. En China antigua, las impresiones del pulgar fueron encontradas en los sellos de arcilla. En el siglo XIV, en Persia, varios papeles oficiales del gobierno tenían las huellas dactilares impresas.

Marcello Malpighi – 1686

En 1686, Marcello Malpighi, profesor de Anatomía en la Universidad de Bolonia, realizó un tratado. "Cretas, espirales y lazos en huellas dactilares". Él no hizo ninguna mención de su valor como herramienta para la identificación individual. La capa de piel del dedo, la huella en sí, fue nombrada como: capa de "Malpighi", que tiene aproximadamente 1.8 mm. de grueso.

John Evangelist Purkinji - 1823

En 1823, John Evangelist Purkinji, profesor de anatomía de la Universidad de Breslau, publicó su tesis discutiendo 9 patrones de huellas dactilares; de la misma forma no hizo ninguna mención del valor de las huellas dactilares para la identificación personal.

Sir Guillermo Hershel - 1856

En julio de 1858, este inglés fue el primero que comenzó a usar huellas dactilares para registros legales, cuando Sir Guillermo Herschel, principal magistrado del distrito Hooghly en Jungipoor, India, usó las primeras huellas dactilares para contratos nativos. Por un capricho, y sin pensamiento hacia la identificación personal, Herschel ordena a Rajyadhar Konai, hombre de negocios local, a poner la impresión de su mano en la parte posterior de un contrato.

dactilar con una encontrada en una botella de alcohol.

Gilbert Thompson - 1882

En 1882, Gilbert Thompson en el encuentro U.S Geological Survey en Nuevo México, utilizó sus propias huellas dactilares en un documento para prevenir la falsificación. Es el primer documento que se conoce en utilizar huellas dactilares en los Estados Unidos.

Marca Twain (Samuel L. Clemens) - 1883

En el libro de Twain, "Vida en el Mississippi", usó la identificación de la huella dactilar para reconocer a un asesino. En su último libro "Pudd'n Head Wilson ", había un ensayo dramático en una corte con la identificación de una huella dactilar. Una película más reciente fue hecha del mismo.

Sir Francis Galton - 1888

Francis Galton, antropólogo británico y primo de Charles Darwin, comenzó sus observaciones de huellas dactilares como medio de identificación en los 1880's. En 1892, publicó su libro, "Huellas Dactilares", estableciendo la individualidad y la permanencia de huellas dactilares. El libro incluyó el primer sistema de clasificación para las mismas.

El interés primario de Galton en las huellas dactilares estaba centrado en la determinación de herencia y del fondo racial. Pronto descubrió que las huellas dactilares no ofrecían ninguna pista firme sobre la historia genética de un individuo, pero podría probar lo que los científicos Herschel y Faulds sospechaban de las huellas dactilares, éstas no cambiaban en el curso de la vida de un individuo, y no podrían haber dos huellas dactilares exactamente iguales. Según sus cálculos, las probabilidades que dos huellas dactilares individuales fuesen iguales eran de 1 en 64 mil millones.

Galton identificó las características por las cuales las huellas dactilares se pueden identificar. Estas mismas características, las minucias, básicamente están hoy en uso y se refieren a menudo como detalles de Galton.

Juan Vucetich

En 1891, Juan Vucetich, funcionario de la policía de Argentina, comenzó a realizar los primeros archivos de la huella dactilar basados en tipos de patrones de Galton. Al principio, Vucetich incluyó el sistema de Bertillon con los archivos.

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

Su impresión sangrienta fue dejada en un peldaño de la puerta, probando su identidad como el asesino.

1901

Ese año se caracteriza por la introducción de las huellas dactilares para la identificación criminal en Inglaterra y Países de Gales, usando las observaciones de Galton y las revisiones de Edward Richard Henry; se comenzó el sistema de clasificación de Henry, usado hoy en los países de habla inglesa.

1902

Primer uso sistemático de huellas dactilares en los Estados Unidos, por la Comisión Civil de Nueva Cork. De acuerdo a la historia el Dr. Henry y DeForrest son los pioneros del uso de la huella dactilar para identificación en los Estados Unidos.

1903

El sistema penitenciario del estado de Nueva York comenzó el primer uso sistemático de huellas dactilares en Estados Unidos para los criminales.

1904

El uso de huellas dactilares comenzó en la penitenciaría federal de Leavenworth en Kansas, y el departamento de policía de San Louis.

1905

El ejército de los Estados Unidos empieza usar las huellas dactilares. Dos años más tarde la marina siguió los pasos de la armada y comenzó a usar también las huellas dactilares para el registro de los enlistados; durante los siguientes 25 años muchas agencias relacionadas con la ley empezaron hacer uso de las huellas dactilares como medios de identificación personal.

En 1918 Edmond Locard escribió que si 12 puntos (detalles de Galton) fueran iguales entre dos huellas dactilares, entonces sería suficiente para dar como positiva una identificación. Algunos países han fijado sus propios estándares que incluyen un número mínimo de puntos, pero no en los Estados Unidos.

1924

En 1924, el Congreso estableció la división de identificación del F.B.I. El *National Bureau* y *Leavenworth* se consolidaron para formar la oficina central de huellas dactilares del F.B.I.

1946

Antes de 1946, el F.B.I. había procesado 100 millones de tarjetas de huellas dactilares, archivados manualmente; y antes de 1971, 200 millones de tarjetas.

Con la introducción de la tecnología de AFIS (Sistemas de Identificación Automática de Huellas Dactilares), los archivos estuvieron divididos en archivos criminales automatizados y archivos manuales civiles. Muchos de los archivos manuales eran duplicados, los expedientes representaban realmente una cantidad de 25 a 30 millones de criminales, y un número desconocido de individuos en los archivos civiles.

En un futuro no muy lejano, las esperanzas del FBI se podrán ser realidad, de pasar de un sistema de tarjetas impresas de la huella dactilar a un nuevo sistema: AFIS Integrado (IAFIS) en Clarksburg, W V. El IAFIS tendrá inicialmente expedientes automatizados individuales de huellas para aproximadamente 33 millones de criminales. Las viejas tarjetas para los archivos civiles todavía se mantienen, pero con una mayor facilidad para archivarlas en Fairmont, W V. Desde la guerra del Golfo, la mayoría de las tarjetas militares de alistamiento basadas en la huella dactilar han sido solamente archivadas alfabéticamente por nombre. El FBI tiene la esperanza de clasificar y archivar estas tarjetas, tal que se pueda identificar con mayor facilidad a los enlistados.

2.2. ERRORES Y EVALUACIÓN DE UN SISTEMA BIOMÉTRICO BASADO EN LA HUELLA DACTILAR

2.2.1. Terminología [2]

2.2.1.1. *Template*

El *"template"* o plantilla es un elemento que define la tecnología de los sistemas biométricos. Una plantilla es un archivo pequeño derivado de las características distintivas de los datos biométricos de un usuario, usadas para realizar comparaciones o emparejamientos biométricos. Los sistemas biométricos almacenan y comparan plantillas biométricas. La mayoría de las plantillas ocupan menos de 1 kilobyte, y las plantillas de algunas tecnologías pueden ser tan pequeñas como de 9 bytes; los tamaños de la plantilla también se diferencian de acuerdo al fabricante del sistema biométrico.

Los tamaños de archivos pequeños permiten emparejar o comparar muy rápidamente, pueden ser almacenados en dispositivos pequeños tales como tarjetas inteligentes, y facilitar la transmisión y cifrado rápidos. Ver figura 2.1.

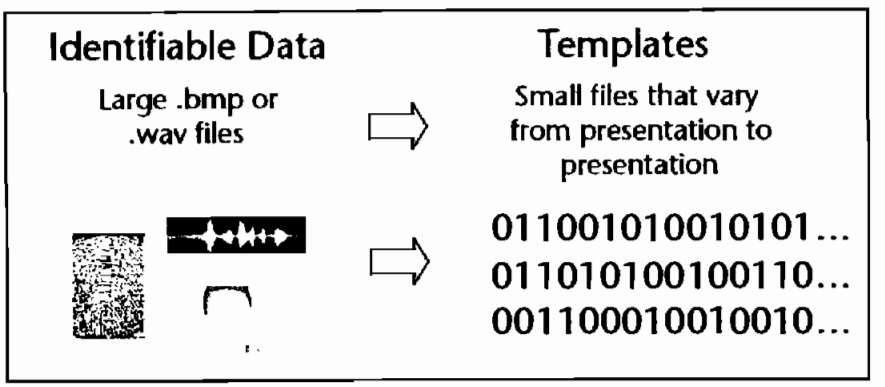


Figura 2.1: Plantillas biométricas versus datos biométricos identificables [2]

2.2.1.2. *Biometric Matching*

La comparación de las plantillas biométricas para determinar el grado de correlación de similitud se llama "*matching*" o emparejar. El proceso de *matching* de las plantillas biométricas da lugar a un *score* o marcador, que, en la mayoría de los sistemas, se compara en relación a un umbral. Si el *score* excede el umbral, el resultado es un "*match*", si el *score* cae debajo del umbral, el resultado es un *nonmatch*. El proceso de *matching* implica la comparación de un *template* o plantilla de verificación, creada cuando el usuario proporciona datos biométricos denominada lectura en vivo (*live scan*) con la(s) plantillas(s) de la inscripción almacenadas en un sistema biométrico. El sistema realiza la verificación utilizando la plantilla de verificación emparejando con la plantilla de inscripción de un usuario, la plantilla de verificación se puede emparejar contra las docenas, millares, incluso millones de plantillas de inscripción.

Los siguientes pasos y términos se utilizan en el *Biometric Matching*

El ***score***.- Las decisiones biométricas de *match/no-match*[9] se basan en un resultado que es un número que indica el grado de semejanza o de correlación resultante de la comparación de las plantillas de inscripción y de verificación. Los sistemas biométricos utilizan algoritmos propietarios para el proceso de plantillas y/o generación de *scores*. No hay escala estándar para los *scores* biométricos: algunos sistemas biométricos emplean una escala de 1 a 100; otros utilizan una

[9] *Match*, término inglés para indicar como positivo algún evento.

escala de -1 a 1, o de 0 a 1. Estos *scores* pueden ser generados con métodos logarítmicos o lineales; para el caso particular de las huellas digitales, éste se encontraría por la cantidad de minucias emparejadas iguales.

Umbral.- Una vez que se genere un *score*, se compara con el umbral de la tentativa de la verificación. Un umbral es un número predefinido, elegido generalmente por un administrador de sistema, que establece el grado de correlación necesario para que una comparación pueda ser juzgada como un *match*, como por ejemplo, la cantidad de minucias mínimas para la identificación de la huella dactilar. Los umbrales pueden variar de usuario a usuario, de transacción a transacción, y de tentativa de identificación a la tentativa de verificación. Los sistemas pueden ser altamente seguros o inseguros dependiendo de los ajustes del umbral. La flexibilidad ofrecida por la combinación de *scores* y de umbrales permite que la biometría desplace a los métodos tradiciones de autenticación.

Decisión.- El resultado de la comparación entre el *score* y el umbral es una decisión. Las decisiones que un sistema biométrico puede incluir son: *match*, *nonmatch*, y poco concluyente. Dependiendo del tipo de sistema biométrico desplegado, un *match* puede conceder el acceso a los recursos, un *nonmatch* puede limitar el acceso a los recursos, mientras que poco concluyente, puede incitar al usuario a proporcionar otra muestra. Por lo tanto, para la mayoría de las tecnologías, no hay un *match* del 100%. Esto no debe implicar que los sistemas no son sistemas totalmente seguros, éstos pueden verificar identidad con índices de error de menos de 1 en 100.000 o 1 en 1 millón. Sin embargo, las demandas de 100 por ciento de exactitud son engañosas y no son reflexivas de la operación básica de la tecnología.

2.2.2. Evaluación del Sistema Biométrico [2]

Como ya se ha mencionado, la respuesta de un *match* en un reconocimiento de la huella dactilar dará como válido una verificación de cualquier individuo. Esta respuesta dependerá del *score* que informe el sistema para evaluarlo con un umbral. La decisión del sistema es regulada por un umbral **t**; pares de las huellas

digitales que generan *scores* más arriba o igual a **t** se deducen como *match*, es decir pertenece al mismo dedo; los pares de huellas digitales que generen *scores* más bajos que **t** se deducen como pares *no-match*, es decir, pertenecen a diversos dedos.

Un sistema biométrico típico de verificación confía dos tipos de errores llamados los *"mistaking biometrics"* (confusiones biométricas), la primera es la que las medidas de dos dedos diversos son aparentemente iguales, a esto se lo llama un *match* falso y la segunda confusión es cuando dos medidas biométricas del mismo dedo da como que son de dos dedos diversos, a esto se le llama un falso *non-match*. Observe que estos dos tipos de errores también están denotados a menudo como falsa aceptación (FAR) y falso rechazo (FRR), estudiados en el capítulo I. En el mercado, los sistemas y dispositivos utilizan más los términos de FAR y FRR como una medida de la confiabilidad del equipo.

2.2.2.1. Errores en la verificación

Desde la perspectiva del diseño, el problema de la verificación de la huella dactilar y en general para cualquier sistema biométrico, se puede formular como sigue:
Sea la plantilla almacenada de una persona representada como **T** y la entrada adquirida (lectura en vivo) representada como **I**. Las hipótesis posibles que se pueden dar son:

H_0: $I \neq T$, la entrada no viene de la misma persona de la plantilla almacenada
H_1: $I = T$, la entrada viene de la misma persona de la plantilla almacenada.

Las decisiones asociadas serían:

D_0: la persona no es quien dice ser.
D_1: la persona es quien dice ser.

La verificación implica emparejar **T** e **I** usando una medida de semejanza. Si el *score* resultante es menor que el umbral **t** del sistema, se decide por D_0, caso contrario se decide por D_1. La terminología mencionada anteriormente puede

relacionarse con la teoría de las comunicaciones, donde el objetivo está en detectar un mensaje en presencia del ruido. H_0 sería la hipótesis de que la señal recibida es solamente ruido, y H_1 sería la hipótesis que la señal recibida es el mensaje más el ruido.

Una formulación de prueba de la hipótesis, intrínsecamente contendría dos tipos de errores:

Tipo I : *match* falso (se dice D_1 cuando H_0 es verdad);
Tipo II : *non-match* falso (se dice D_0 cuando H_1es verdad).

El *False Match Rate* (FMR) es la probabilidad del error tipo I (también llamado nivel de prueba de la hipótesis) y el *False Non-Match Rate* (FNMR) es la probabilidad del error tipo II:

$$FMR = P\left(D_1 \middle| H_0 = verdad\right) \tag{2.1}$$

$$FNMR = P\left(D_0 \middle| H_1 = verdad\right) \tag{2.2}$$

Observe que: (1 - FNMR) también es llamado energía de la prueba de la hipótesis. Evaluar la exactitud de un sistema biométrico como el de la huella dactilar significa que uno debe recoger los *scores* generados por pares de huellas digitales del mismo dedo (la distribución $p\ (s \mid H_1 = verdad)$ normalmente se llama distribución genuina) y los *scores* generados por pares de huellas digitales de diversos dedos (la distribución $p\ (s \mid H_0 = verdad)$ normalmente se llama distribución del impostor).

La figura 2.2 ilustra gráficamente FMR y FNMR sobre las distribuciones genuinas y del impostor:

$$FNMR = \int_0^t p\left(s \middle| H_1 = verdad\right) ds \ , \tag{2.3}$$

$$FMR = \int_{t}^{1} p(s|H_0 = verdad)ds \quad . \tag{2.4}$$

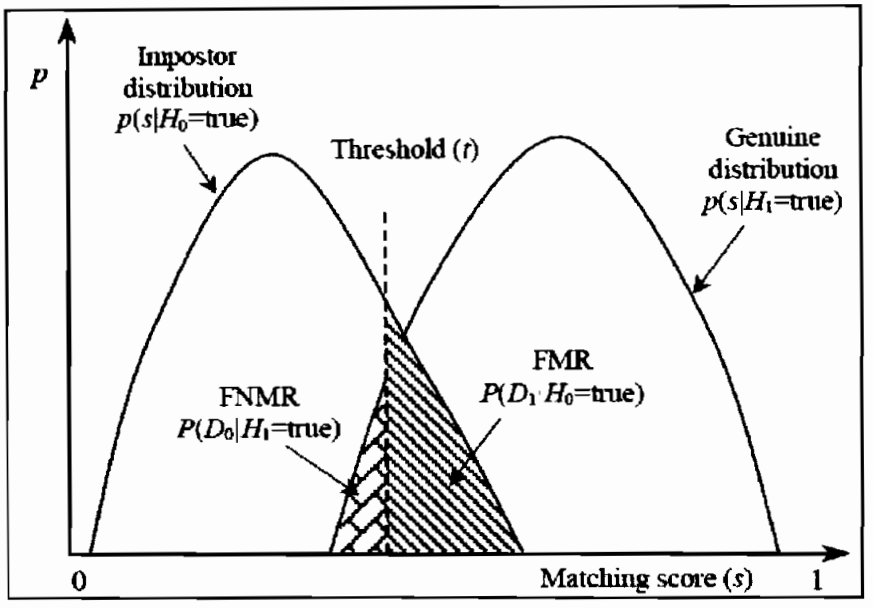


Figura 2.2: FMR y FNMR para un umbral dado t se grafican sobre las distribuciones genuinas y del impostor de la distribución del *score*. [2]

Del dibujo, es evidente que FMR es el porcentaje de los pares del impostor con *scores* que son mayores o iguales a t, y FNMR es el porcentaje de los pares genuinos con *scores* que son menores que t.

Hay una compensación determinante entre FMR y FNMR en cada sistema biométrico (Golfarelli, Maio, y Maltoni, 1997). De hecho FMR y FNMR son funciones del umbral **t** del sistema, y se debe, por lo tanto referirlos como FMR(t) y FNMR(t) respectivamente. Si **t** disminuye para hacer al sistema más tolerante con respecto a variaciones y ruido en la entrada, entonces FMR(t) aumenta; y viceversa, si **t** se eleva para hacer el sistema más seguro, FNMR (t) por consiguiente se aumenta. Un diseñador puede no saber por adelantado el uso particular para el cual el sistema se puede utilizar (o un solo sistema se puede diseñar para una variedad de aplicaciones). Es recomendable presentar el funcionamiento del sistema en todos los puntos (umbral, **t**). Esto da como resultado la traza de una curva de la característica de funcionamiento del receptor

ROC. Una curva de ROC es un diagrama de *FMR* versus *(1- FNMR)* para los varios umbrales de decisión (FNMR a menudo se grafica a lo largo del eje vertical en vez de (1 - FNMR)).Ver figura 2.3.

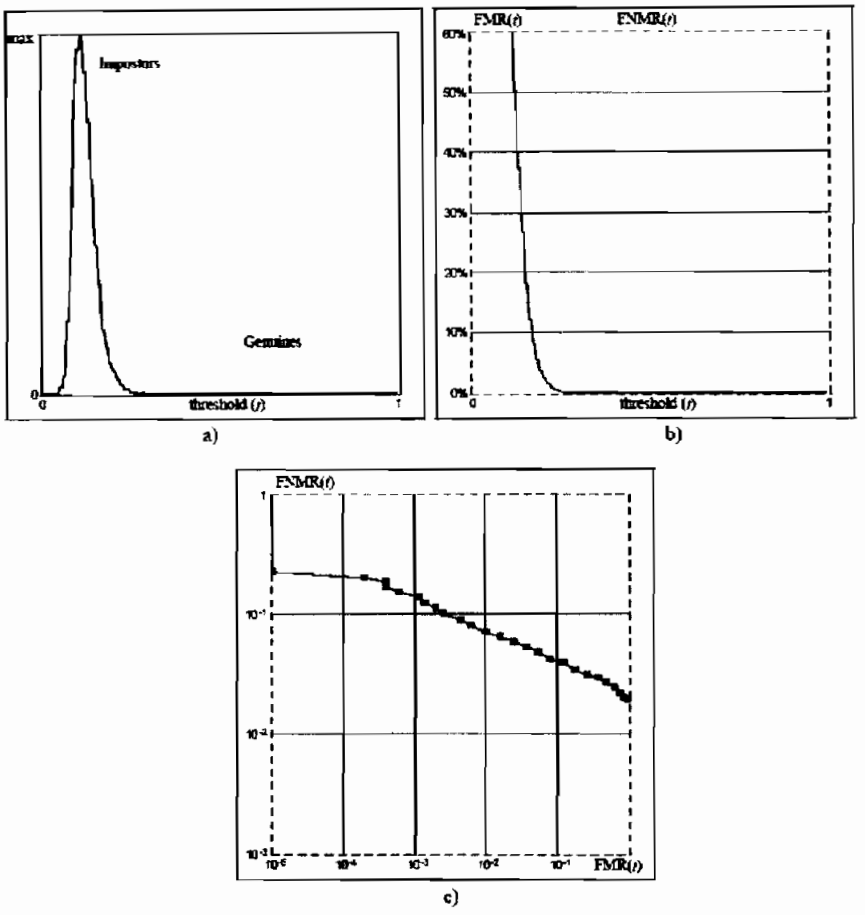


Figura 2.3: Evaluación del sistemas FVC2002 para verificación de la huella digital (Maio et al., 2002b) utilizando la base de datos DB1: (a) Las distribuciones genuinas y del impostor a partir de 2800 pares genuinos y de 4950 pares del impostor, respectivamente; (b) FMR(t) y FNMR(t) se derivan de las distribuciones del *score* en a); (c) La curva de ROC se deriva de las curvas de FMR(t) y de FNMR(t) en b). [2]

Además de las distribuciones y de las curvas antes mencionadas, algunos autores también manejan los siguientes términos:

Equal Error Rate (EER), denota el error en el umbral **t** para el cual FMR y FNMR son idénticos: FMR (t) = FNMR (t) (ver figura 2.4). En la práctica, no puede existir un punto exacto de EER, como alternativa se debe graficar un intervalo. Aunque EER es un indicador importante, en la realidad, un sistema

biométrico basado en la huella raramente utiliza este punto para evaluar su funcionamiento.

ZeroFNMR, es el FMR más bajo en el cual FNMR es casi nulo.

ZeroFMR, es el FNMR más bajo en el cual FMR es casi nulo.

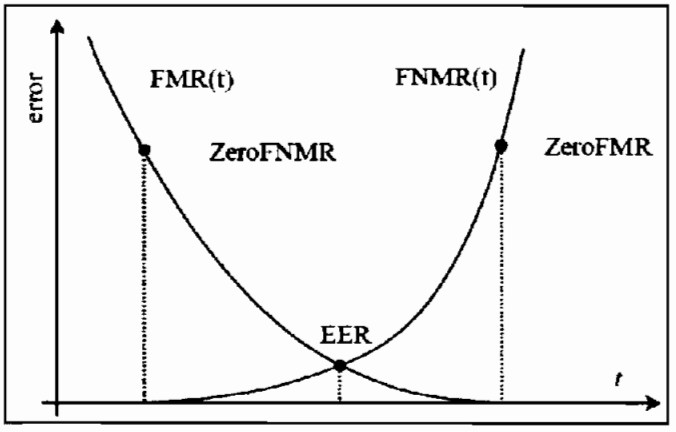


Figura 2.4: Ejemplo de las curvas de FMR(t) y de FNMR(t), donde se destacan los puntos que corresponden a EER, ZeroFNMR y a ZeroFMR. [2]

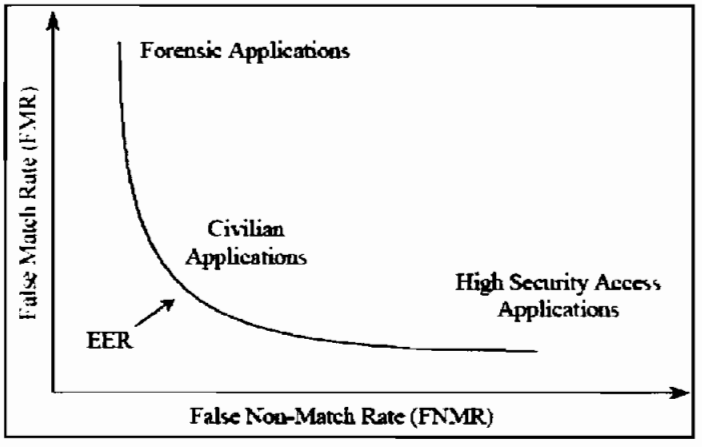


Figura 2.5: Los puntos de funcionamiento típicos de diversos usos exhibidos en una curva ROC. [2]

Ahora, ¿cómo hacer que las definiciones de los errores introducidos para la verificación de la huella digital se extiendan a la identificación de la huella digital? Bajo algunas premisas de simplificación, una valoración del funcionamiento en el

modo de la identificación se puede deducir por las estimaciones del error en el modo de la verificación.

2.2.2.2. Errores en la Identificación

Se asume que no hay mecanismo de indexación/recuperación disponible (es decir, la base de datos entera que contiene **N** plantillas tiene que ser buscada), y que una sola plantilla para cada usuario está presente en la base de datos. $FNMR_N$ y FMR_N se denotan para la identificación como *false non-match rate* y *false match rate*, respectivamente, entonces:

- $FNMR_N = FNMR$; quiere decir que la probabilidad de un falso *no-match* en la entrada contra el patrón del usuario es igual que en el modo de verificación, a menos que esta expresión no considere que la probabilidad de que un *match* falso pueda ocurrir antes de que se visite el patrón correcto.
- $FMR_N = 1-(1-FMR)^N$, quiere decir, la probabilidad que un *match* falso ocurra, cuando en la entrada pueden ocurrir *match* falsos para una o más plantillas en la base de datos. FMR_N entonces se calcula como: uno menos la probabilidad de que no se haga ningún *match* falso con cualquiera de las plantillas de la base de datos. La expresión *(1-FMR)* es la probabilidad de que la entrada no tenga un *match* falso para una sola plantilla de usuario, y $(1-FMR)^N$ es la probabilidad que la entrada no tenga un *match* falso con cualesquiera de las plantillas de la base de datos. Si FMR es muy pequeño, la expresión puede reducirse a $FMR_N \cong N*FMR$., y por lo tanto se puede decir que la probabilidad del *match* falso aumenta linealmente con el tamaño de la base de datos.

Este resultado tiene implicaciones serias para el diseño de los sistemas grandes de identificación. Generalmente, la velocidad de procesamiento se percibe como el problema más grande para una aplicación de identificación.

Si los patrones en la base de datos tienen un mecanismo de clasificación/indexación, es decir que solamente una porción de la base de datos

se explora durante la identificación, esto da lugar a una diversa formulación de $FNMR_N$ y de FMR_N:

- $FNMR_N = RER + (1 - RER)*FNMR$, donde RER (*Retrieval Error Rate*), es la probabilidad de que la plantilla de la base de datos que corresponde al dedo explorado sea evaluado incorrectamente por el mecanismo de recuperación. Se obtiene la expresión anterior en base a la siguiente discusión: en caso de que la plantilla no se recupere correctamente (este suceso con la probabilidad RER), el sistema genera siempre un *no-match* falso, mientras que en el caso donde la recuperación devuelve una plantilla correcta (esto sucede con la probabilidad (1 - RER)), el índice de un falso *no-match* del sistema, es FNMR. También, esta expresión es solamente una aproximación pues no considera la probabilidad de un *match* falso de una plantilla incorrecta antes de que se recupere la correcta (Cappelli, Maio, y Maltoni, 2000c).

- $FMR_N = 1-(1-FMR)^{N*P}$, donde P (también llamado régimen de penetración) es el porcentaje medio de la base de datos explorada durante la identificación de una huella digital en la entrada.

La formulación exacta de desvíos en un sistema de la identificación se expone en Cappelli, Maio, y Maltoni (2000c).

2.3. PARTES DEL SISTEMA

Estos sistemas abarcan:

- *Hardware* para adquisición de la imagen,
- Componentes de proceso de la imagen,
- Componentes para generación de la plantilla
- Emparejamiento o *matching*
- Almacenamiento.

Dependiendo del fabricante el proceso puede diferenciarse levemente de la secuencia descrita, especialmente en la extracción de las características distintivas, pero en general el proceso básico es similar.

Estos componentes se pueden establecer dentro de un solo periférico o dispositivo independiente, o se puede separar entre un dispositivo periférico, una PC local, y un servidor central. A partir de los componentes de proceso de la imagen, estas partes se encierran en una sola, ésta es el "*software*".

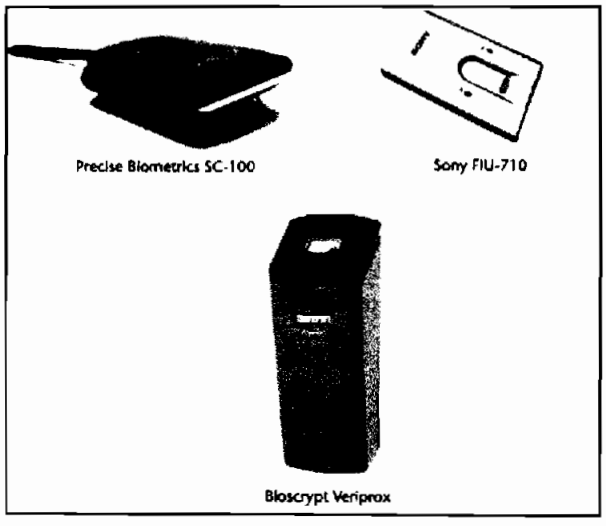


Figura 2.6: Dispositivos *finger-scan*[10] [5]

2.3.1. *Hardware* para Adquisición de la Imagen [5]

La superficie en la cual se coloca el dedo se llama "cristal de exposición", también referido simplemente como explorador. Los cristales de exposición se pueden hacer de varios materiales, tales como cristal, plástico, silicio, y polímeros. Existen capas adicionales que se utilizan para prevenir daño al cristal de exposición como rasguños; esto hace que se reduzca la capacidad del dispositivo para adquirir imágenes de alta calidad de la huella dactilar. Dependiendo del tipo de *finger-scan* se utilizan diversas tecnologías en las áreas de contacto entre la huella dactilar y el cristal de exposición. Por ejemplo se puede utilizar cámaras

[10] *Finger-scan* hace referencia al dispositivo biométrico asociado al identificador; "dedo escaneado".

fotográficas *chip-based*[11] con proyección de imagen ultrasónica, o a través de cambios en los campos capacitivos generados por el dedo o el común método óptico, métodos que se los estudiará más adelante. Las medidas tomadas se convierten en código digital.

Un cristal de exposición es una de las piezas que conforman el "módulo" del *finger-scan,* el módulo es el bloque básico del sistema . Un módulo contiene normalmente al cristal de exposición unido a un tablero de circuito impreso pequeño, junto con un conector estándar, que permite que la información digitalizada sea transmitida al periférico o a un dispositivo independiente. Muchos de los módulos de hoy vienen con la capacidad de ejecución de toda la adquisición de la imagen, procesamiento de imagen, generación de la plantilla, y el proceso de identificación y verificación con la plantilla almacenada, claro está para un pequeño conjunto de usuarios. Estos módulos envían simplemente decisiones de *match/no-match* a un dispositivo externo.

Los módulos se pueden construir en los dispositivos periféricos de un PC, encajados en teclados, en las computadoras portátiles, o las tarjetas de PCMCIA, o también se los puede encontrar integrados en los dispositivos de control de una puerta de acceso, o formando parte de los terminales.

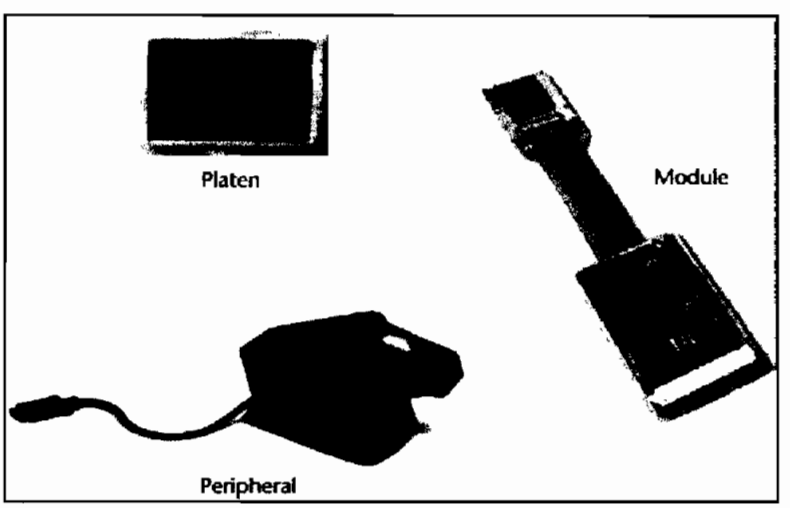


Figura 2.7: Partes del sistema *finger-scan.* [5]

[11] Término que se utiliza para indicar que el equipo o dispositivo es construido en base a *chips* o circuitos integrados.

Existen varios escenarios que pueden darse, según como se diseñe el sistema *finger-scan*, éstos se muestran en la figura 2.8.

Los resultados de la identificación se transmiten del sistema biométrico en el formato apropiado para la autentificación en los sistemas lógicos o físicos de acceso.

Estos sistemas pueden estar integrados firmemente con sistemas externos (sistemas operativos, componentes elegantes de autentificación de tarjeta, cerraduras electrónicas de una puerta, teléfonos móviles, etc.) o pueden pasar simplemente una contraseña, como en el caso del presente diseño.

Esta parte de la integración es una parte extremadamente importante en el sistema biométrico, en éste, se integró el sistema *finger-scan* a un control de asistencia, trabajo que se lo detallará en el capítulo 3.

2.3.1.1. Tecnologías para la Adquisición [5] [17]

Hay varias alternativas de acercamientos al problema de adquirir imágenes de la huella dactilar con la suficiente calidad para crear plantillas o *templates*. Los métodos ópticos, silicio, y ultrasonido son los métodos principales en uso por la industria *finger-scan*.

2.3.1.1.1. Tecnología Óptica

De hecho, el reconocimiento por medios ópticos es el más viejo y depurado. El usuario coloca el dedo sobre en un cristal de exposición, el cual está construido de un plástico duro revestido o una placa de vidrio que se ilumina desde adentro. La captura de la imagen se hace por medio de un sensor basado en un CCD (Dispositivo Acoplado por Carga) similar a los que se usan en *scanners* y cámaras digitales, sobre la cual se convierten las crestas y los valles o surcos en formato digital para que aparezcan como líneas negras, grises, y blancas. El CCD (*Charge Coupled Device*), es el elemento fundamental de todo *scanner*, independientemente de su forma, tamaño o mecánica. Consiste en un elemento

electrónico que reacciona ante la luz, transmitiendo más o menos electricidad según sea la intensidad y el color de la luz que recibe; es un auténtico ojo electrónico.

A más de la sensibilidad a irregularidades posteriores al registro inicial, y que en realidad afectan a todos los sistemas de huellas dactilares, el método óptico puede resultar particularmente sensible a la presencia de grasa y suciedad en general. El hecho es que estos cuerpos extraños van dejando en la placa una huella fantasma llamada imagen latente u oculta que, con el tiempo, puede afectar la exactitud del dispositivo. Para compensar este efecto, algunos fabricantes guardan en memoria la imagen latente de la última huella de modo que al tomar la siguiente la "restan" de la nueva imagen obtenida.

La tecnología óptica tiene varias ventajas: se ha probado, en un cierto plazo confiable, que es resistente a la descarga electrostática, es bastante barato, y puede proporcionar resoluciones de hasta 500 DPI, el estándar patrón para las imágenes de alta calidad de la huella dactilar. Las debilidades de la tecnología óptica incluyen tamaño (el cristal de exposición debe tener suficiente área superficial y profundidad para capturar imágenes de buena calidad), y una susceptibilidad a las minucias falsas.

Los dispositivos ópticos se los encuentra principalmente en accesos lógicos y físicos. La mayoría de los dispositivos diseñados para adquirir las imágenes para los sistemas de AFIS, se basan en proyección de imagen óptica.

2.3.1.1.2. Tecnología del Silicio o Capacitivo

Por su parte, el sistema capacitivo consiste en establecer un campo eléctrico entre dos componentes aislados eléctricamente, en este caso el dedo y un *chip*. Este sistema es más preciso que el anterior porque las mediciones del campo eléctrico pueden diferenciar líneas de surcos (como si fuera una imagen tridimensional), pero por otro lado el contacto con el *chip* puede afectarlo con el tiempo.

existirá aberturas de aire en los valles. Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a soltarse trayendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento.

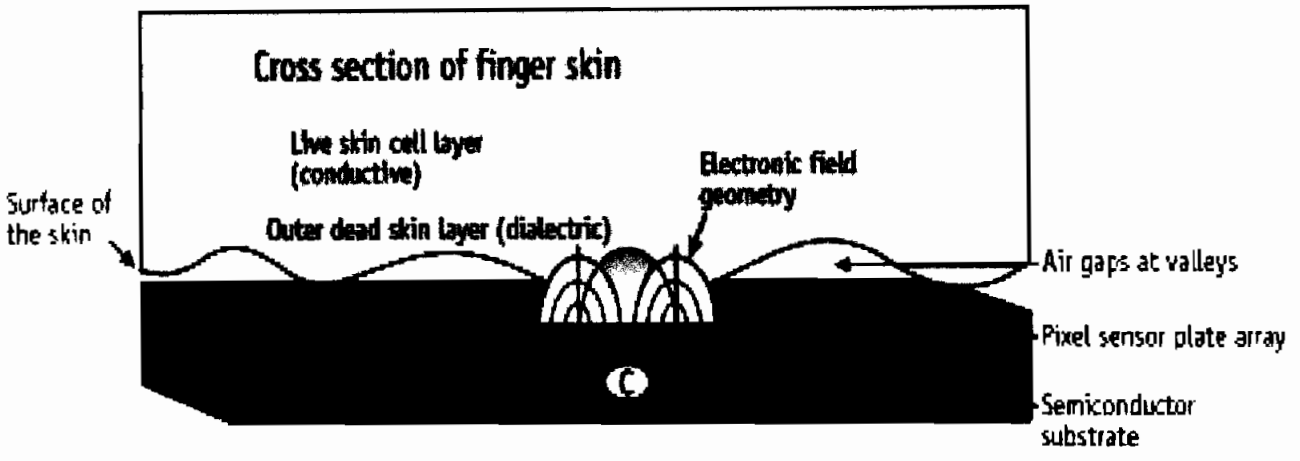


Figura 2.9: Sensor capacitivo clásico. [17]

2.3.1.2.2. Sensor de Matriz de Antena

Un pequeño campo RF es aplicado entre dos capas conductoras, una oculta dentro de un *chip* de silicón (llamado plano de referencia de la señal de excitación) y la otra localizada por debajo de la piel del dedo (ver figura 2.10).

El campo formado entre estas capas reproduce la forma de la capa conductora de la piel en la amplitud del campo AC. Diminutos sensores insertados por debajo de la superficie del semiconductor y sobre la capa conductora, miden el contorno del campo. Amplificadores conectados directamente a cada plato sensor convierten estos potenciales a voltajes, representando el patrón de la huella. Estas señales son acondicionadas en una etapa siguiente para luego ser multiplexadas fuera del sensor.

Estos dispositivos no dependen de las características de la superficie, tales como las aberturas de aire entre el sensor y el valle, empleado para detectar ese valle.

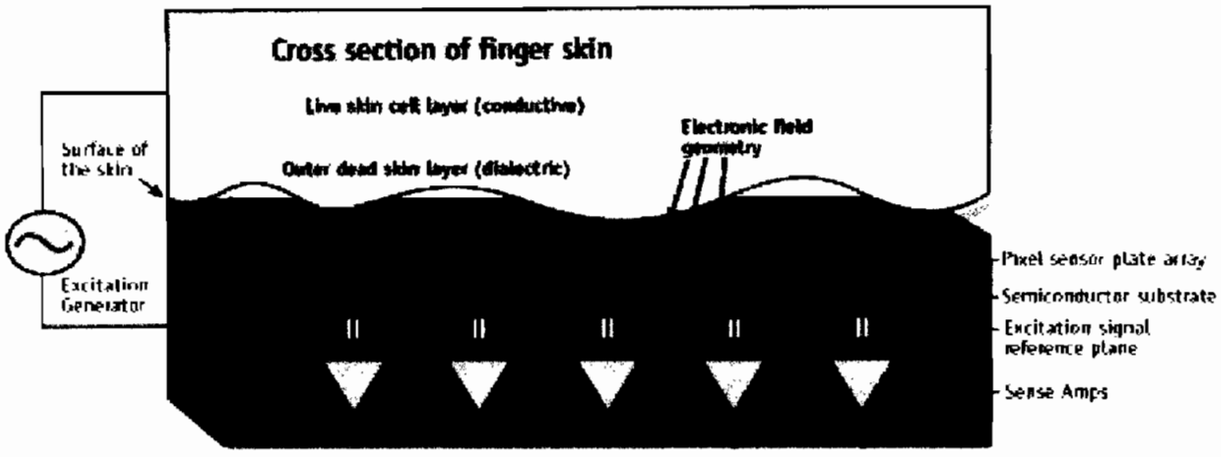


Figura 2.10: Sensor de Matriz de Antena. [17]

En la figura 2.11 se puede observar la forma típica de un sensor aplicado a sistemas de reconocimiento de huellas dactilares.

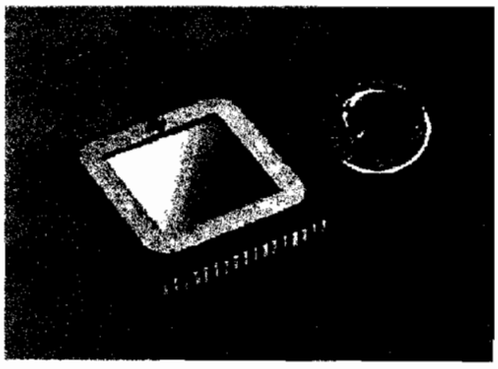


Figura 2.11: *Scanner* a disposición comercial. [17]

Varios *scanners fingerprint*, basados en las tecnologías de detección examinadas anteriormente, están comercialmente disponibles.

Ciertamente, las características principales de un equipo biométrico basado en la huella dactilar dependen del sensor específico que determina las características de la imagen (dpi, área, y gama dinámica), tamaño, coste, y durabilidad.

sistemas operativos. Dependiendo del uso y de la infraestructura donde los *scanners* de la huella dactilar tengan que ser empleados, éstos deberán tener compatibilidad con más de un sistema operativo, y en detalle la ayuda de sistemas operativos abiertos como Linux, podría ser una característica importante.

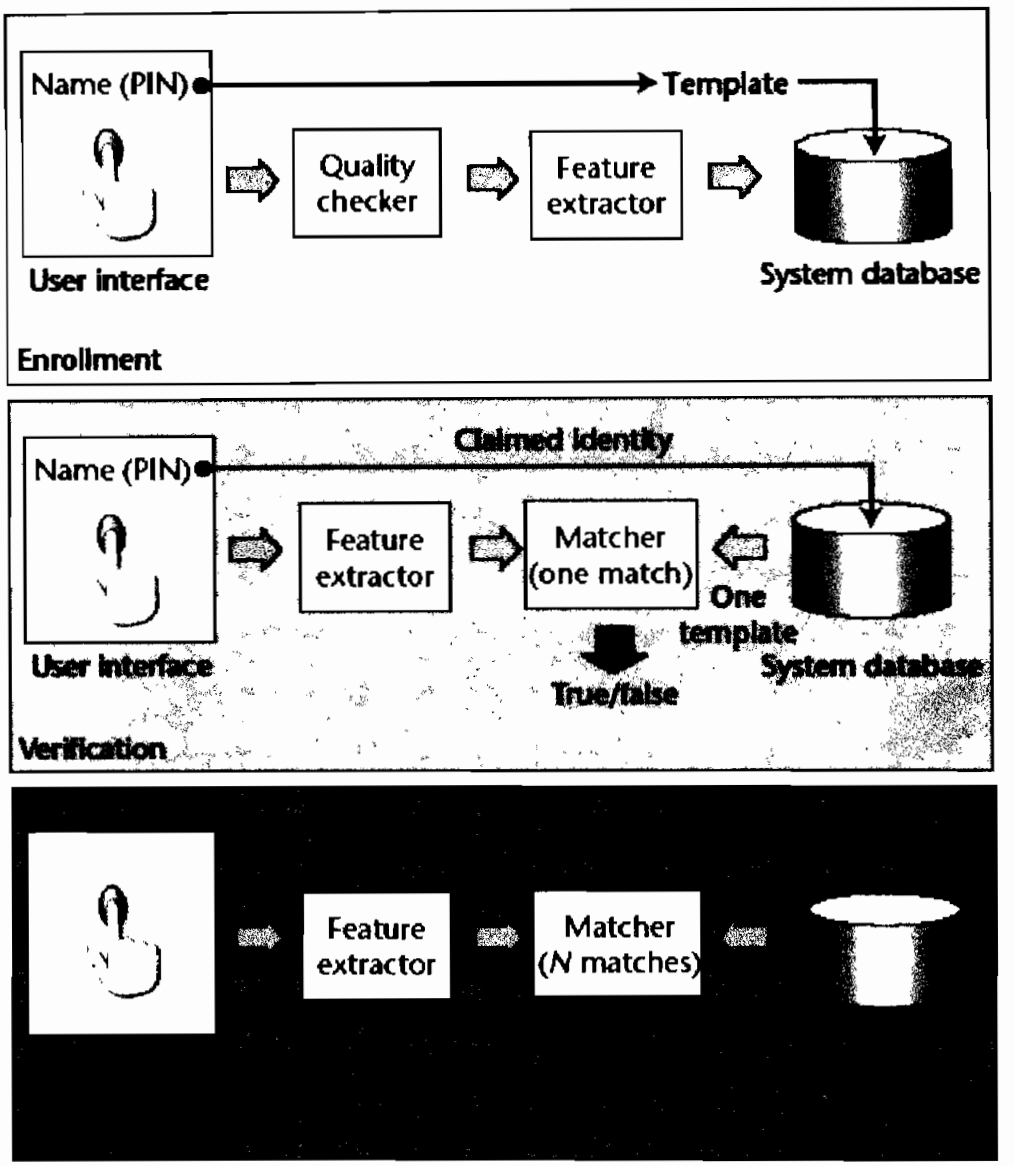


Figura 2.13: Diagramas de bloque de inscripción, verificación, e identificación. [33]

2.3.2.1. Componentes de proceso de la imagen

Una huella dactilar está formada por crestas y valles (surcos) en la superficie de la punta del dedo. Cada individuo tiene huellas dactilares únicas, esta situación se presenta por la localización y características de las crestas.

Un Sistema identificador de huellas dactilares está basado en la comparación de detalles diminutos en la estructura de crestas y valles de una huella dactilar. Cada

El módulo que se encargue del mejoramiento de la imagen de la huella, deberá tratar con cualquier región que se le presente, claro está que si le toca la opción (c), éste deberá enviar una señal de huella no captada para que, según el sistema éste vuelva a tomar otra imagen de la huella tratada.

(a) (b) (c)

Figura 2.14: (a) Región bien definida; (b) Región dañada recuperable (c); Región dañada no-recuperable. [34]

2.3.2.1.1. Adquisición de la imagen

El primero paso es adquirir una imagen de alta calidad de la huella dactilar. La calidad de la imagen se mide en puntos por pulgada (DPI); más puntos por pulgada dan como resultado una imagen de alta resolución. Comúnmente estos sistemas pueden adquirir las imágenes de 500 DPI, que es el estándar para la huella dactilar forense, resolución recomendada por el FBI. La calidad de la huella digital, más baja encontrada generalmente en el mercado está entre 300 y 350 DPI, ver figura 2.15.

Figura 2.15: Típicas imágenes adquiridas por los sistemas *finger-scan*. [5]

La adquisición de la imagen es un desafío importante para el sistema porque la calidad de la huella digital puede variar substancialmente de persona a persona y dedo a dedo. Algunas poblaciones son más probables que otras para la facilidad de adquisición de las huellas dactilares, debido a los rasgos fisiológicos. Además, los factores ambientales pueden afectar la adquisición de la imagen.

Para obtener una inscripción eficaz, el centro de la huella dactilar debe ser colocado en el cristal de exposición. Muchos usuarios desconocedores de la tecnología colocarán su dedo en un ángulo tal que solamente aparezca una porción superior o inferior de la huella digital. Esto da lugar a pocas características distintivas que son situadas durante la inscripción y la verificación, reduciendo la probabilidad de una operación exitosa. Un factor adicional en la adquisición de la imagen que puede afectar la exactitud y el funcionamiento de un sistema de estas características es el tamaño del cristal de exposición. Algunos fabricantes de *finger-scan* han desarrollado cristales de exposición más pequeños para fabricar dispositivos compactos y reducir costes. Sin embargo, hay un contra que se debe tomar muy en cuenta, los cristales de exposición muy pequeños adquieren una porción más pequeña de la huella dactilar, lo que significa que menos datos están disponibles para crear y emparejar plantillas.

Una vez que se adquiera una imagen de alta calidad, debe ser convertida a un formato utilizable. Es aquí donde interviene un paso muy importante para la adquisición de la plantilla o *template*: El mejoramiento de la imagen.

2.3.2.1.2. Mejoramiento de la Imagen

Debido a las imperfecciones de la imagen adquirida, en algunos casos el algoritmo de extracción puede obviar algunas minucias, y en otros se pueden añadir minucias falsas. Las imperfecciones de la imagen pueden también generar errores al determinar las coordenadas de cada minucia y su orientación relativa en la imagen.

Todos estos factores contribuyen a disminuir la fiabilidad del sistema de reconocimiento, puesto que el reconocimiento de huellas dactilares está basado

en la comparación, dentro de unos límites de tolerancia, del patrón biométrico, o conjunto de minucias extraidas, adquirido "en vivo"[12] y el proceso de almacenamiento.

Para asegurarse de que el funcionamiento de un sistema automático de la huella digital para la identificación/verificación sea robusto con respecto a la calidad de las imágenes de la huella dactilar, es esencial incorporar un algoritmo que realce la imagen de la huella dactilar, cuyo objetivo sea obtener una región bien definida de la huella a reconocer.

El diagrama del algoritmo de limpieza de una huella dactilar se muestra en la figura 2.16:

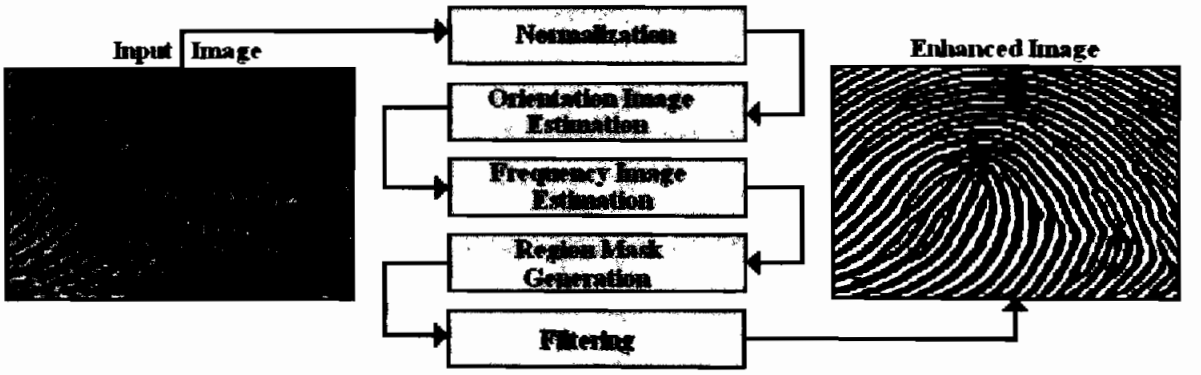


Figura 2.16: Diagrama general para el mejoramiento de la imagen de una huella. [34]

Éste es un esquema básico y completo, en otros trabajos se añaden otros pasos que pueden están inmersos en cualquiera de los señalados en la figura 2.16.

a. Normalización de la imagen [35]

El objetivo de esta fase es disminuir el rango de variación de grises entre los valles y las crestas de la imagen para facilitar el proceso en las siguientes etapas; es decir, tener una cierta independencia de las propiedades de la imagen, como lo

[12] La imagen gráfica recién obtenida del lector es conocida como una lectura en vivo o *live scan*

son: brillo y contraste, y así poder comparar huellas por su índice de calidad que se debe definir para el algoritmo. La ecuación correspondiente es la siguiente:
Sea I(x,y) la imagen de entrada,

$$N(x,y) = \frac{(N^{\circ}\ \ Niveles - 1)}{(\max(I) - \min(I))}.(I(x,y) - \min(I)). \qquad (2.5)$$

Donde:

I(x,y), nivel de gris de la imagen en la coordenada (x,y).

min(I),max(I): mínimo y máximo nivel de gris en la imagen respectivamente.

N(x,y), nivel de gris de la imagen normalizada en la coordenada (x,y).

Los siguientes pasos se aplican a cada bloque de 16x16 pixels, y la finalidad será hallar un mapa de direcciones y luego el mapa de períodos. Este último mapa será el que provea la frecuencia de cada bloque para el procesamiento local de los filtros de Gabor.

b. Cálculo del campo orientación y mapa del período [35] [36]

La Orientación de la Imagen **O**, está definida como una imagen **N x N**, donde **O(i,j)** representa la orientación local de la cresta en el píxel **(i,j)**. La orientación de la cresta está usualmente especificada por un bloque; una imagen está dividida en un conjunto de bloques no traslapados **w x w** y una orientación de la cresta local está definida por cada bloque.

El campo de direcciones u orientación, representa la orientación local de las crestas que contiene la huella. Para estimarlo, la imagen se divide en bloques de 16x16 píxels y se calcula la inclinación para cada píxel, en coordenadas **x** e **y**.

El ángulo de orientación se calcula a partir de la información de la inclinación. Frecuentemente, en algunos bloques, el ángulo de orientación no se calcula correctamente debido a ruidos y daños en los valles y las crestas de la imagen capturada.

Los tipos de singularidad del *core* vienen asociados con el tipo de estructura general de la huella. La estructura global o singularidad de las huellas se puede clasificar en forma general en: arco, lazo y espiral.

Figura 2.20: (a) Arco, (b) Lazo, (c) Espiral. [38]

De esta manera la estructura de la huella dactilar de algún usuario pertenece a una de estas clases. La imagen direccional calculada anteriormente da información de la estructura global de la imagen de la huella digital.

El punto delta se podría pensar que es un tipo especial de singularidad asociada con el del tipo arco. Existen algunos métodos para la detección de estas singularidades, uno de ellos es el de Poincaré. (Ver **ANEXO B**)

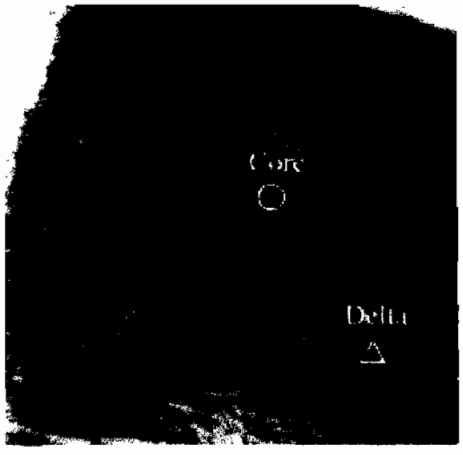


Figura 2.21: Puntos singulares en una huella dactilar. [39]

2.3.2.2.2. Extracción de minucias [2] [40]

En la última etapa, se extraen las minucias de la imagen simplificada o adelgadaza, obteniendo el patrón biométrico de la huella (plantilla/*template*). Para ello, se determina si cada píxel de la imagen adelgazada pertenece o no a una cresta, y en el caso de que así sea, si pertenece a una bifurcación o un principio o final de cresta obteniéndose un grupo de candidatos a minucias. A continuación, todos los puntos en el borde de la zona de interés se borran.

Luego se deben eliminar las minucias falsas. Una manera de saber si existen éstas, es medir la densidad de minucias por unidad de área, puesto que no puede exceder un cierto valor por la estructura general de una huella, todos los conjuntos de puntos candidatos cuya densidad excede este valor son sustituidos por una simple minucia localizada en el centro del conjunto.

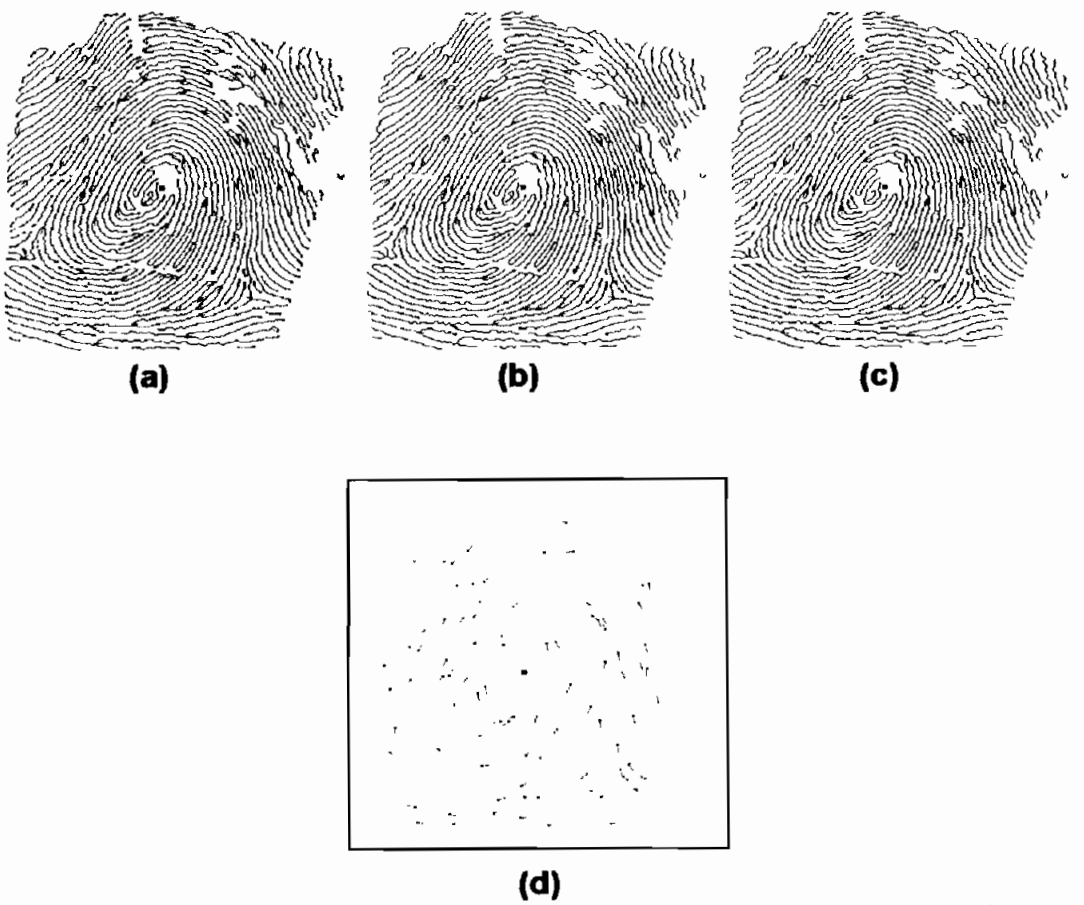


Figura 2.22: (a) Primera extracción de minucias, (b) y (c) Proceso de eliminación de minucias falsas, (d) Patrón de minucias. [35]

Figura 2.23: Eje y minucias extraidas. [40]

Adicionalmente, el algoritmo de extracción de minucias coloca un eje de coordenadas sobre la huella, posicionándolo de tal forma que el centro del eje esté sobre el *core* de la huella y alineando el eje con la orientación de la huella, teniendo en cuenta la singularidad delta, (ver figura 2.23).

Para que dos plantillas basadas en minucias concuerden no es necesario que concuerden todas las minucias que se han extraido de las huellas. De por sí se pueden obtener resultados muy precisos con tan solo coincidir un tercio del total de minucias.

2.3.2.3. Emparejamiento o "*matching*" [2]

2.3.2.3.1. Algoritmo de comparación de minucias

El emparejamiento automático o "*matching*" de la huella digital no sigue necesariamente un mismo conjunto de pautas. De hecho, aunque el emparejamiento automático basado en las minucias de la huella digital es inspirado por el procedimiento manual, una gran cantidad de acercamientos se han diseñado durante los últimos 40 años, y muchos de ellos explícitamente para ser puestos en ejecución en una computadora. Una clasificación de los métodos que siguen cierta tendencia para el proceso de "*matching*" de la huella digital es:

- *Correlation-based matching* (emparejamiento basado en la correlación): Más conocida como la "basada en patrones". Se sobreponen dos imágenes de la huella digital, y la correlación (en el nivel de la intensidad) entre los *píxels* correspondientes se calcula para diversas alineaciones (ejemplo, las varias dislocaciones y rotaciones);
- *Minutiae-based matching* (emparejamiento basado en las minucias): Las minucias se extraen de dos huellas digitales y se almacenan como sistemas de puntos en el plano de dos dimensiones. Este método consiste esencialmente en encontrar la alineación entre la plantilla (minucias almacenadas) y las minucias de la entrada, como resultado se tiene el número máximo de pares de minucias coincidentes.
- *Ridge feature-based matching* (emparejamiento basado en características de la cresta): La extracción de las minucias es difícil en imágenes de muy baja calidad, mientras que otras características de las crestas de la huella digital se pueden apreciar (ej., orientación y frecuencia local, forma de la cresta, información de la textura) y se pueden extraer más confiablemente que las minucias, aunque su distinción es generalmente más baja. Los acercamientos que pertenecen a esta familia comparan huellas digitales en términos de las características extraidas del patrón de la cresta.

El método basado en las características de la cresta, no es muy difundido, siendo los dos primeros lo más utilizados.

Se estudiará el método basado en las minucias para luego realizar una comparación con el basado en patrones.

a. Formulación del problema

Sea **T** e **I** la representación de la huella digital de la plantilla y de la entrada, respectivamente. En este método la representación de la huella digital es un vector característico (de longitud variable) cuyos elementos son las minucias de la huella digital. Cada minucia se puede describir por un número de cualidades, incluyendo su localización en la imagen de la huella digital, la orientación, el tipo

(por ejemplo terminación o bifurcación de la cresta), un peso basado en la calidad de la imagen de la huella digital en la vecindad de las minucias, etc. La mayoría de las minucias comunes que emparejan dichos algoritmos consideran cada minucias como un trío **m** = {*x*, *y*,*θ*} donde **x** e **y** son las coordenadas rectangulares de la minucia y θ la orientación definida como la orientación local de la cresta asociada.

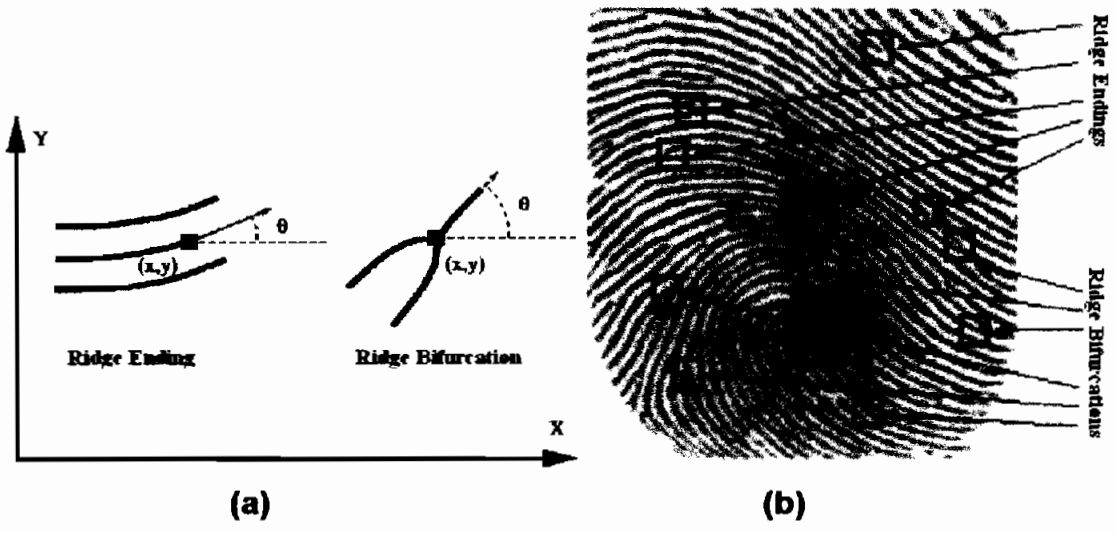


Figura 2.24: (a) Una minucia se caracteriza por la posición y la orientación; (b) Varios detalles señalados en una huella. [34]

Sea:

$$T = \{m_1, m_2, ..., m_m\} \qquad m_i = \{x_i, y_i, \theta_i\}, \qquad i = 1..m$$
$$I = \{m'_1, m'_2, ..., m'_n\} \qquad m'_j = \{x'_j, y'_j, \theta'_j\} \qquad j = 1..n,$$

donde **m** y **n** denotan el número de minucias en **T** e **I**, respectivamente.

Una minucia $\mathbf{m'_j}$ en **I** y una minucia $\mathbf{m_i}$ en T son considerados "*matching*" o emparejados si la distancia espacial (***sd***) entre ellas es más pequeña que una tolerancia dada $\mathbf{r_0}$ y la diferencia de la dirección (***dd***) entre ellas es más pequeña que una tolerancia angular $\mathbf{\theta_0}$.

$$sd(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \le r_0 \qquad (2.6)$$

$$dd\left(m'_j, m_i\right) = \min\left(\left|\theta'_j - \theta_i\right|, 360^\circ - \left|\theta'_j - \theta_i\right|\right) \leq \theta_0 \qquad (2.7)$$

La ecuación (2.7) toma el mínimo de $|\theta'_j - \theta_i|$ y de $360^\circ - |\theta'_j - \theta_i|$, por la circularidad de ángulos (la diferencia entre los ángulos de 2° y 358° es solamente 4).

Las tolerancias definidas por r_0 y θ_0 se necesitan compensar por los errores inevitables hechos por algoritmos de extracción de características y las pequeñas distorsiones plásticas que son causadas por el cambio de posición de las minucias.

El alineamiento de las dos huellas digitales es un paso obligatorio para maximizar el número de minucias emparejadas. Concretamente el alineamiento de dos huellas digitales requiere el desplazamiento en **x** e **y** y la rotación θ que se recuperará posteriormente, e implica probablemente otras transformaciones geométricas:

- La escala tiene que ser considerada cuando la resolución de las dos huellas digitales puede variar, por ejemplo las dos imágenes de la huella digital han sido tomadas por los analizadores operatorios en diversas resoluciones.
- Otras transformaciones geométricas podrían ser útiles para emparejar minucias en caso de que una o ambas huellas digitales sean afectadas por distorsiones severas.

En cualquier caso, tolerar un número más alto de transformaciones da lugar a grados de libertad adicionales a la unidad emparejadora de las minucias: cuando se diseña una unidad emparejadora necesita ser evaluada cuidadosamente, ya que cada grado de libertad da lugar a un número enorme de nuevas alineaciones posibles y esto aumenta de manera importante la posibilidad de dar un *match* a dos huellas digitales de diversos dedos.

Sea ***mapa (.)*** la función que traza las minucias m'_j de **I** en m''_j según una transformación geométrica dada; por ejemplo, considerando un desplazamiento de [Δx, Δy] y una rotación hacia la izquierda θ alrededor del origen. (El origen se selecciona generalmente como las minucias del centro de la figura (es decir, el punto medio); antes del paso de igualación, las coordenadas de las minucias son ajustadas restando las coordenadas del centro de la figura):

$$map_{\Delta x,\Delta y,\theta}\left(m'_j = \{x'_j, y'_j, \theta'_j\}\right) = m''_j = \{x''_j, y''_j, \theta'_j + \theta\} \quad donde$$
$$\begin{bmatrix} x''_j \\ y''_j \end{bmatrix} = \begin{bmatrix} \cos\theta & -sen\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x'_j \\ y'_j \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \tag{2.8}$$

Sea ***mm(.)*** una función indicador que devuelve 1 en el caso que las minucias m''_j y m_i emparejan según las ecuaciones (2.6) y (2.7):

$$mm\left(m''_j, m_i\right) = \begin{cases} 1 & sd\left(m''_j, m_i\right) \le r_0 \quad y \quad dd\left(m''_j, m_i\right) \le \theta_0 \\ 0 & de\ otra\ manera \end{cases} \tag{2.9}$$

Entonces, el problema de emparejar podría formularse como:

$$\underset{\Delta x,\Delta y,\theta,P}{maximize} \sum_{i=1}^{m} mm\left(map_{\Delta x,\Delta y,\theta}\left(m'_{P(i)}\right), m_i\right) \tag{2.10}$$

donde **P(i)** es una función desconocida que determina el apareamiento entre las minucias de **I** y de **T**; en detalle, cada minucia tienen exactamente un compañero en la otra huella digital o no tienen ningún compañero.

1. $P(i) = j$ indica que el compañero de m_i en T es la minucia m'_j en I.
2. $P(i) = nulo$ indica que esas minucias m_i en T no tiene ningún compañero en I.
3. Una minucia m'_j en I tal que $\forall\ i = 1..m,\ P(i) \neq j$ no tiene ningún compañero en T.

4. $\forall\ i=1..m,\ k=1..m,\ i\neq k \Rightarrow P(i)\neq P(k)\ \ o\ \ P(i)=P(k)=nulo$ (esto requiere que cada minucia en I esté asociada a un máximo de minucias en T.

Note que, en general, $P(i)=j$ no significa necesariamente que las minucias m'_j y m_i emparejen en el sentido de las ecuaciones (2.6) y (2.7) pero solamente ese par es el más probable bajo la transformación actual.

La expresión (2.10) requiere que el número de compañeros de minucias esté maximizado, independientemente de que tan determinantes sean estos compañeros; es decir si dos minucias se conforman con las ecuaciones (2.6) y (2.7), entonces su contribución a la expresión (2.10) se hace independientemente de su distancia espacial y de su diferencia de dirección. Las alternativas de solución de la expresión (2.10) pueden ser introducidas en un residual (es decir, la distancia espacial y la diferencia de la dirección entre las minucias), para la alineación óptima también considerada al momento de dar un *match*.

El problema de la expresión (2.10), es trivial cuando la alineación correcta (Δx, Δy, θ) se conoce, en efecto, el apareamiento (es decir P(i)) puede ser determinado ajustando para cada i=1...m.

- $P(i)=j$ si $m''_j=map_{\Delta x,\Delta y,\theta}(m'_j)$ está más cercano a m_i entre las minucias $\{m''_k=map_{\Delta x,\Delta y,\theta}(m'_k)\,|\,k=1..n,\ mm(m''_k,m_i)=1\}$

- $P(i)=nulo$ $si\ \forall\ k=1..n,\ mm(map_{\Delta x,\Delta y,\theta}(m'_k),m_i)=0.$

Cada minucia que se acople, tienen que ser marcada para evitar que otra acople dos veces o más a la misma minucia. En la figura 2.25 se muestra un ejemplo de las minucias que se aparean dada una alineación de la huella digital.

La maximización en (2.10) puede ser solucionada fácilmente si se conoce la función **P** (correspondencia de las minucias); en este caso, la alineación

m_1 de T y m''_3 no pueden emparejar, las minucias m_3 y m''_6 no pueden acoplarse debido a su gran diferencia de dirección.

2) Concordancia cualitativa, que requiere que los detalles minuciosos correspondientes deben ser idénticos.
3) Factor cuantitativo, que especifica que por lo menos cierto número (un mínimo de 12 según las pautas forenses en los Estados Unidos) de detalles minuciosos correspondientes debe ser encontrados.
4) Detalles minuciosos correspondientes, que se deben correlacionar idénticamente.

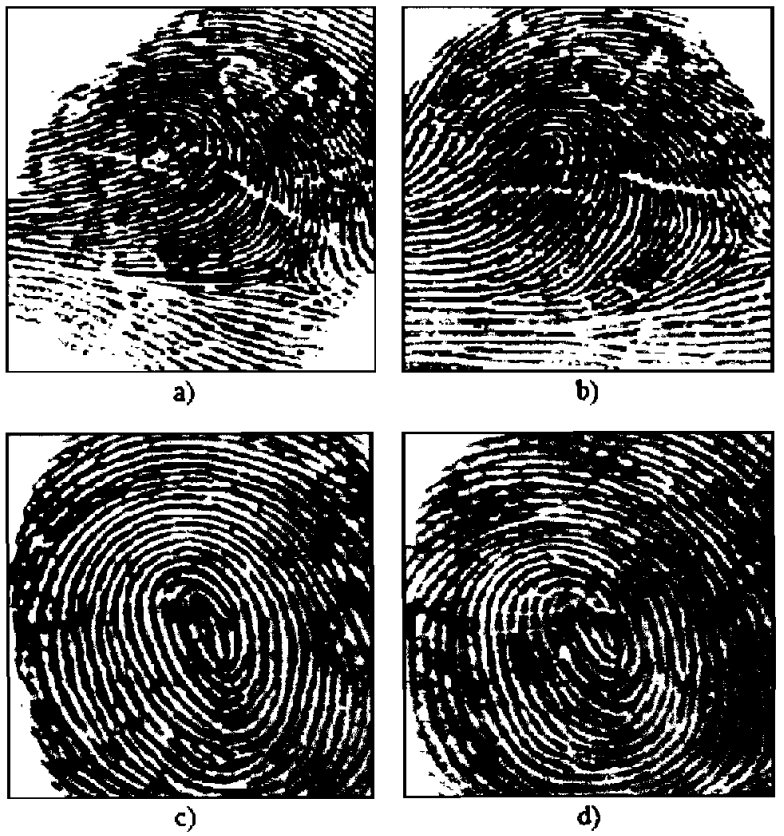


Figura 2.27: Dificultad en emparejar la huella digital. Las imágenes de la huella digital en (a) y (b) son diferentes a un ojo inexperto pero ellas son impresiones del mismo dedo. Las imágenes de la huella digital en (c) y (d) son iguales miradas con un ojo inexperto pero ellas son de diversos dedos. [2]

2.3.2.3.2. Emparejamiento de plantillas basadas en patrones [40]

Un dispositivo lector toma una imagen gráfica de la huella digital, típicamente capturándola como una imagen TIFF (*Tagged Image File Format*). La imagen gráfica recién obtenida del lector es conocida como una lectura en vivo (*live scan*)

Las plantillas basadas en patrones miden entre 500 y 700 bytes en promedio cuando se comprimen y cerca de 1,024 bytes sin comprimir. Las comparaciones y otras funciones relacionadas sólo se pueden llevar a cabo con la plantilla 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.

Esto afecta tanto en capacidad de memoria como en tiempo de ejecución, siendo técnicamente mejor el método de las minucias.

b. Sensibilidad a los cambios físicos

Los cambios físicos en el dedo son referidos a cicatrices, cortaduras, arrugas, lunares y manchas diversas, debido a accidentes o a causas normales de trabajo.

Cuando un sistema basado en minucias procesa una huella digital, una cicatriz, arruga o mancha puede resultar en unas cuantas minucias, pero éstas sólo representarán un pequeño porcentaje del total de minucias extraidas. Si 20% de las minucias que se extraen se deben a cambios fisiológicos de la huella desde que la plantilla se tomó por primera vez, aún se cuenta con el 80% de las minucias restantes para comparar. Puesto que una buena comparación se puede lograr con tan sólo el 30% de las minucias, la disponibilidad del 80% ofrece un margen de seguridad bastante amplio.

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. Los cambios físicos pueden oscurecer elementos críticos de la imagen e incrementar significativamente las diferencias entre dos imágenes del mismo dedo, reduciendo así la posibilidad de obtener una concordancia precisa.

c. Seguridad y reproducción (*playback*)

La seguridad es una consideración importante cuando se comparan los tipos de plantilla. Una técnica posible para evadir la seguridad biométrica de una huella

digital sería la de obtener una plantilla real y reproducirla en el sistema de verificación. Aún con una variedad de métodos de seguridad y encriptación, las plantillas se deben descifrar para poder ser usadas por los algoritmos de comparación. En consecuencia, un individuo con la determinación suficiente podría obtener una plantilla.

Se debe considerar que cuando se extrae una plantilla basada en minucias de una huella digital, pequeñas variaciones en la orientación y colocación del dedo en el dispositivo lector pueden afectar ligeramente las minucias generadas. Esto significa que el mismo dedo colocado múltiples veces en un dispositivo lector producirá minucias ligeramente diferentes cada vez. Como sea, esto no causa efecto en la precisión de los algoritmos de comparación (como se ha mencionado anteriormente, variaciones menores en las minucias no afectan el resultado de la comparación). Consecuentemente, si el mismo dedo se presenta múltiples veces, concordará, pero no perfectamente, en el sentido que las plantillas obtenidas nunca serán absolutamente idénticas. Esto presenta un método para detectar la presentación de una plantilla robada: si una comparación es exacta significa que la plantilla resultó ser idéntica, minucia por minucia, con la plantilla de la base de datos. Por lo tanto, la plantilla recién obtenida debe ser un duplicado de alguna en la base de datos y no puede provenir de una lectura en vivo.

2.3.2.4. Almacenamiento de la huella

El almacenamiento de las imágenes de las huellas dactilares sería el paso final de este sistema biométrico. En el caso del método de extracción de minucias, lo que se guarda es una plantilla o *template* de la huella; sin embargo, dependiendo de la aplicación y propósito, el sistema puede guardar la imagen de la huella para en base a ésta trabajar. Como se mencionó, dependiendo de la aplicación, se vería la cantidad de recursos de disco para dicho almacenamiento.

Por ejemplo, si una empresa necesita un sistema de control de asistencia para sus empleados, suponiendo que dicha empresa tiene a su disposición 1000 empleados, en un sistema de extracción de minucias se necesitaría:

Utilizando un equipo de la empresa Identix; una plantilla: 350 bytes. Tomando por cada empleado dos lecturas de dos dedos diferentes, se necesitaría almacenar 2000 plantillas, a razón de 350 bytes por plantilla, se necesitaría alrededor de 700 Kbytes, o sea menos que 1 Gbyte, memoria moderada para un PC residencial.

Pero existen agencias que se dedican exclusivamente a recopilar la mayor cantidad de imágenes de huellas dactilares, especialmente para casos criminalísticos y forenses, la más grande, el FBI.

En la figura 2.29 se presenta la imagen de una huella digital que mide 768 x 768 *pixels* (= 589.824 bytes):

Figura 2.29: Imagen de una huella dactilar de 768x768 *pixels*. [41]

Este es un archivo grande comparado con una plantilla de minucias, pero recuerde que el FBI guarda imágenes de huellas dactilares, no plantillas.

El FBI captura huellas digitales a una resolución de 500 DPI (puntos por pulgada) y 256 niveles de gris (8 bits de resolución en la escala de gris). Cada tarjeta contiene 14 imágenes y el fichero resultante de la digitalización de cada tarjeta ocupa aproximadamente 10 MB. El FBI tiene una base de datos de unos 200 millones de expedientes de huellas digitales, debiendo así mantenerse una base de datos de alrededor de 2000 Terabyte, y cada día en la base del FBI se acumulan en promedio de 30.000 a 50.000 tarjetas nuevas. [41]

En razón de la cantidad de información, el FBI se encontró con la necesidad de establecer algún mecanismo para la compresión de estos datos.

Las imágenes de las huellas dactilares pueden clasificarse como una clase específica de imágenes con características definidas de orientación y continuidad de crestas. De los métodos de compresión desarrollados hasta la presente, el

único orientado exclusivamente a la compresión de imágenes de huellas dactilares es el especificado por el estándar WSQ (*Wavelet Scalar Quantization*/ Cuantización Escalar de La Transformada *Wavelet*), desarrollado por la división criminal de servicios informativos de la justicia del FBI (CJIS), con la ayuda del *National Institute of Standards and Technology* (NIST) y del Laboratorio Nacional de Los Álamos (LANL). Basado en la transformada *wavelet* y la cuantización escalar, con este estándar de compresión, se puede manejar compresiones de 1:12.9, es decir que la imagen de la huella dactilar se vería reducida a 45621 bytes, lo cual permite ahorrar una gran cantidad de espacio en disco.

2.4. VENTAJAS Y DESVENTAJAS

La tecnología *finger-scan* tiene algunas ventajas sobre las tecnologías competentes, algunas de las cuales son atribuibles a la tecnología misma, otras son derivadas del mercado.

2.4.1. Ventajas [2] [5]

2.4.1.1. Tecnología probada para altos niveles de exactitud

Es una tecnología actual y probada en varios campos de la seguridad, capaz de registrar alta exactitud. La huella dactilar se ha reconocido y se ha comprobado hasta la saciedad como un identificador altamente distintivo; la clasificación, el análisis, y el estudio de huellas dactilares ha existido por décadas.

Hay características fisiológicas más distintivas que la huella dactilar (el diafragma y la retina, por ejemplo), pero estas tecnologías se han desarrollado solamente durante los últimos años.

2.4.1.2. Gama de ambientes

Puede ser desplegado en una gama de ambientes. Los requisitos reducidos del tamaño y de energía, junto con la resistencia a los cambios ambientales tales

como iluminación de fondo y temperatura, permite que la tecnología sea desplegada en una amplia gama de ambientes de acceso lógicos y físicos. El tamaño de los dispositivos actuales ha evolucionado de tal manera que alcanzan dimensiones menores a 1.5 x 1.5 centímetros capaces de adquirir y de procesar imágenes de alta calidad.

Además, en lo que respecta a la huella dactilar, hay más soluciones en el mercado biométrico que en el resto de tecnologías combinadas. Aunque esto puede abrumar al cliente por el número de soluciones en el mercado, esto ha dado lugar a un número de soluciones robustas para los PC de escritorio, computadoras portátiles, acceso físico, y ambientes de alta seguridad.

2.4.1.3. Ergonómico, Facilidad de uso

Emplea dispositivos ergonómicos, fáciles de usar. El acto de colocar un dedo en un dispositivo es en gran parte intuitivo y se puede captar con un poco de entrenamiento. Muchas otras tecnologías biométricas requieren interacciones complejas usuario-sistema, mientras que los dispositivos *finger-scan* generalmente se diseñan para un proceso de fácil repetición. Además, estos diseños han mejorado substancialmente, los primeros *finger-scan* eran de gran tamaño y se pedía la colocación constante del dedo, mientras que muchos dispositivos de hoy realizan la alineación adecuada internamente con la imagen captura en primera instancia.

2.4.1.4. Capacidad de almacenar múltiples huellas de una sola persona

La capacidad de almacenar múltiples huellas de una sola persona puede aumentar exactitud y flexibilidad en el sistema. El hecho de que la mayoría de la gente puede almacenar hasta 10 huellas en un sistema biométrico presta ventajas en seguridad y flexibilidad. Por ejemplo, requerir la colocación de dos dedos sucesivamente puede hacer que el sistema probabilísticamente sea mucho más seguro. Otra funcionalidad es permitir que un usuario se verifique con uno de sus varios dedos almacenados, reduce la probabilidad que el usuario tenga un falso rechazo del sistema. Los usuarios pueden almacenar ciertos dedos específicos

para activar comandos que permitan una respuesta física o una alarma interna, o permitir varias acciones de control dependiendo del dedo escaneado.

Para reducir la probabilidad que la información biométrica sea robada y reutilizada, un sistema puede desafiar al usuario a colocar uno de sus dedos y comprobar que la respuesta correcta es aceptada.

2.4.2. Desventajas [2] [5]

Las siguientes debilidades afectan casi a todas las soluciones *finger-scan*, pero éstas pueden ser atenuadas con un diseño inteligente del sistema.

2.4.2.1. El funcionamiento puede deteriorarse en un cierto plazo

Aunque la huella dactilar es una característica fisiológica estable, existen usuarios que trabajan con sus manos, la piel puede dañarse, cortarse y hasta gastarse, claro está que ésta vuelve a brotar. A pesar que la inscripción se la haga con imágenes de alta calidad, no se puede escapar a esta realidad, pero existen soluciones como el almacenar la huella de más de un dedo, o que el sistema cada cierto plazo actualice su plantilla, debiendo ser este proceso transparente al usuario.

2.4.2.2. Asociación con usos forenses y criminalísticos

La asociación de la huella dactilar con usos forenses y criminalísticos causa cierto malestar en un porcentaje de usuarios. El estigma unido a las huellas dactilares ha limitado eventualmente el crecimiento y la aceptación de esta tecnología. Una de las causas es el miedo de saber que si bien sus huellas dactilares son captadas para un uso específico, éstas puedan ser utilizadas para usos forenses e incluso para implicar a una persona en un crimen. Claro está que, si la gente se familiariza más con la forma como trabajan estos dispositivos no causaría ningún temor, pues la plantilla no es una imagen y tampoco va ser fácil reconstruirla a partir de ella.

2.4.2.3. Necesidad de despliegue

Para que esta tecnología se convierta en una solución biométrica penetrante, estos dispositivos deben estar presentes en los tableros de escritorio, en los teclados, en los sitios de acceso, en los PCs y en cualquier localidad en donde se requiere la autentificación. En comparación con la tecnología biométrica de la voz por ejemplo, ésta se ha desarrollado fácilmente gracias a los varios dispositivos que tratan este tipo de señal, como son los teléfonos y los micrófonos que ahora vienen con acceso directo a los PCs para grabar cierto mensaje y tratarla según la necesidad. Un *scanner* de huellas dactilares no se lo compra en cualquier electrónica, pero según este estudio, esta tecnología a corto plazo puede encontrarse en cualquier lugar, incluso en la puerta de su casa.

CAPÍTULO

3

IMPLEMENTACIÓN Y EVALUACIÓN DEL PROTOTIPO

CAPÍTULO 3

DISEÑO, IMPLEMENTACIÓN Y EVALUACIÓN DEL PROTOTIPO

3.1. REQUERIMIENTOS DEL SISTEMA DE CONTROL DE ASISTENCIA (SCA)

Es claro que la Biometría ofrece tareas de identificación y verificación o autenticación de una persona, esto da una gama sin fin de aplicaciones en las cuales se necesite la presencia de un individuo en particular. Una de esas es el control de asistencia de los empleados y trabajadores, sistema de uso general en empresas públicas y privadas. En la mayoría de estas empresas se hace uso de sistemas electromecánicos, sistemas que no cumplen labores de verificación o autenticación; esto es un problema cuando los empleados dejan de lado sus responsabilidades y se dedican a engañar al sistema haciendo que otros compañeros o personas ajenas a la Institución registren su asistencia y por consiguiente no es sancionada por dicha inasistencia. En todo caso la duda reinará en cuanto a la puntualidad y cumplimiento de las horas de trabajo de un empleado o trabajador mientras se usen estos sistemas electromecánicos.

Este proyecto utilizará el identificador biométrico de la huella dactilar de Identix para desarrollar un sistema de control de asistencia (SCA) en red para la Escuela Politécnica Nacional (EPN) con el propósito de reemplazar al sistema actual, que es de funcionamiento electromecánico.

Antes de analizar los requerimientos del SCA a implementarse se verá la necesidad de su implementación como una política laboral y se estudiará el sistema actual de control de asistencia con el que cuenta la EPN.

3.1.1. El Control de Asistencia es una Política Laboral

En general las políticas laborales son directrices para la toma de decisiones. Una vez establecidas, cada vez que se deba tomar una decisión no será necesario

3.2. DISEÑO DEL SISTEMA

En el diseño del SCA intervendrán tanto componentes de *Hardware* y de *Software*, en este sentido y para una mejor explicación el diseño se dividirá en estos dos elementos.

3.2.1. *Hardware* del SCA

3.2.1.1. Equipo de Red

Los Terminales se ubicarán en sitios similares a los actuales, en tanto que el equipo servidor deberá estar en un área restringida; dependiendo del administrador del sistema, éste podrá ubicarse en la Dirección de Recursos Humanos.

La estructura de la red del SCA se muestra en la figura 3.3. En este caso se hace uso de concentrador o *hub* para interconectar los computadores, aún cuando se puede utilizar la infraestructura de red existente de la EPN, la Polired; con esta solución se ahorraría la compra o el uso de un concentrador y del cableado de interconexión entre los Terminales y el Servidor.

Los requerimientos mínimos sugeridos para los computadores que actuarían como Terminales o Clientes serían:

- Procesador Intel Pentium IV 1.8 GHz
- 256 MB de memoria RAM.
- 40 GB Disco Duro.
- Tarjeta de red.

El equipo Servidor debe tener mayor capacidad de procesamiento, velocidad y memoria virtual para poder manejar varias sesiones de los terminales, aunque en este caso serían máximo dos; se debe asegurar un funcionamiento rápido y seguro para el SCA.

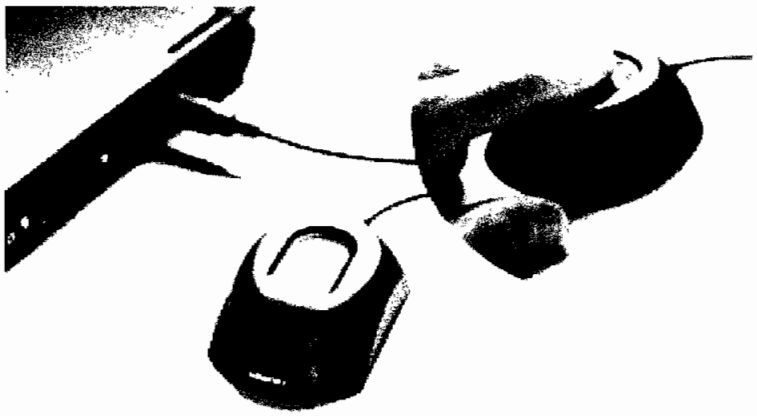


Figura 3.4: Lector de huellas dactilares DFR-200 de Identix. [43]

3.2.2. *Software* del SCA

3.2.2.1. Herramientas para el desarrollo de la aplicación

Para el desarrollo de la aplicación se utilizarán las siguientes herramientas.

3.2.2.1.1. Sistemas Operativos

Como se mencionó se tendrá una red con dos Terminales y su respectivo Servidor, por lo que la aplicación a implementarse necesitará de sistemas operativos:

- *Windows Server.*-Se recomienda la versión 2000 por la flexibilidad de introducir cualquier contraseña, ya que la versión 2003 sólo permite contraseñas mínimas de 7 caracteres teniendo que introducir al menos 3 símbolos adicionales a las letras del alfabeto. La contraseña es un elemento primordial en el sistema, esto se lo abordará más adelante cuando se hable del código del empleado y las cuentas de *Biologon* 3.0; este *software* dará la funcionalidad del Computador Servidor.

- *Windows* Client.- Se debe utilizar una versión de *Windows* actual, tales como *Windows* 2000 o XP.

3.2.2.1.2. *Biologon* 3.0 [4]

BioLogon 3.0 es un *software* biométrico basado en la huella dactilar, propietario de Identix, diseñado para trabajar con todos los lectores de huellas dactilares de la mencionada empresa.

Evita el acceso no deseado de otros usuarios gracias a la autenticación rápida y sencilla de sus huellas dactilares cuando acceden a un dominio de *Windows*, a un árbol de NDS (Servicios de directorio de Novell) o a una estación de trabajo local. El sistema analiza las características únicas de identificación del usuario para asociar una persona a un perfil de usuario y así poder garantizar el acceso individual al sistema. En el proceso de inscripción, el sistema almacena una plantilla de huellas dactilares en una base de datos guardada en el sistema *Windows*. En el acceso, el usuario puede colocar un dedo o una secuencia de varios dedos inscritos en el lector de huellas dactilares.

El *software* de seguridad de *BioLogon* crea una plantilla de la huella dactilar basándose en la información de minucias disponible en la huella. El *software* compara la plantilla con la información existente en la base de datos. El sistema otorga el acceso sólo cuando el proceso de comparación finaliza con éxito. El sistema almacena una representación en dos dimensiones de aproximadamente 10-70 datos de minucias; el sistema almacena estos puntos como vectores en un plano X-Y. Como se vio en al capítulo II es casi imposible invertir el proceso y crear una imagen de una huella dactilar a partir de la información almacenada. Alguna persona externa al sistema no podría recuperar esta información fácilmente de la base de datos y utilizarla para fines no autorizados, ya que los datos se cifran y se almacenan en una ubicación segura en el entorno de *Windows*.

Ediciones de *BioLogon*

Las tres ediciones que presenta *BioLogon* son:

- *BioLogon Desktop*
- *BioLogon* Cliente/Servidor

- *BioLogon* para NDS eDirectory Cliente/Servidor

De las cuales para el desarrollo del presente proyecto se utilizará la edición de Cliente/Servidor ya que es la solución que se ajusta a las necesidades del sistema.

a. Edición Cliente/Servidor

La edición de *BioLogon* Cliente/Servidor administra las plantillas de huellas dactilares de forma central en un dominio de *Windows*, sólo para cuentas de dominio de red. Con inscribir la huella dactilar una sola vez, se podrá acceder a una cuenta especificada desde cualquier Cliente de *BioLogon* 3 del dominio.

Ofrece seguridad de acceso a la red para estaciones de trabajo con *Windows* 95/98/Me/NT4/2000/XP y *BioLogon Client*. Los usuarios pueden pertenecer a redes LAN y WAN, así como a estaciones remotas y locales.

b. *BioShield*

Una de las herramientas de *Biologon* 3 es *BioShield*, la cual en general proporciona control de acceso a las aplicaciones como por ejemplo, la caja de herramientas, el explorador o las propiedades de *Windows*. La parte de interés es la automatización de la tarea de introducción de contraseñas, lo cual se logra con una herramienta de *BioShield* denominada el Banco de Contraseñas.

Banco de Contraseñas

Permite accede a las aplicaciones o a los cuadros de diálogo de autenticación mediante la huella dactilar, utilizando las huellas dactilares para iniciar una sesión de forma rápida en una aplicación, un cuadro de diálogo o una página Web. Puede liberar la información de autenticación de acceso (nombre de usuario y contraseña) colocando el dedo en el lector de huellas dactilares. Antes de acceder, se debe introducir la información de autenticación en la base de datos del Banco de contraseñas de *BioShield*, es decir, inscribir al usuario para que pueda hacer uso de la aplicación. Cuando se intente ingresar al cuadro de diálogo

configuración, operando como si fueran servidores individuales.

Una vez vistas las herramientas que se utilizarán en el desarrollo de esta aplicación, se empezará con el desarrollo del mismo. El *software* que se desarrolla en este proyecto se divide en dos componentes principales: *software* del Servidor y *software* del Terminal o Cliente.

3.2.2.2. *Software* del Servidor

Es el *software* más importante y con mayor complejidad de implementación, será el corazón del sistema el cual no podrá dejar de funcionar en los días de asistencia de los empleados; entre las funciones principales que realizará este *software* se tiene:

- Llevará la base de datos de los empleados de la EPN, tanto los datos personales como biométricos.

- En esta aplicación se ingresará y se almacenarán los datos de administración del sistema, tales como: Horarios, Vacaciones, Justificaciones y Asignaciones de Horario, etc.

- Mantendrá la base de datos de los registros de asistencia, aquí se almacenará la asistencia diaria de los empleados para su posterior tratamiento.

- Procesará la información de asistencia de los empleados para un cierto período indicado por el administrador del sistema, y como resultado se obtendrán diversos tipos de reportes, entre ellos el más importante, el de minutos atrasados.

Para el desarrollo del *software* del Servidor, asumiendo que el computador encargado para esta función está ya configurado con el sistema operativo

la instalación normal. Para más detalle acerca de la instalación de *Biologon* 3.0 Cliente/Servidor y de los controladores del lector, referirse al manual de instalación y operación (**ANEXO E**).

Biologon 3.0 trabaja para cuentas de *Windows*, por lo que cada empleado será tratado como un usuario del domino de red. La clave de *Windows* es muy importante, pues es ésta la que se utilizará para los registros de asistencia del empleado; en el momento que se cree la cuenta de usuario del empleado se deberá escoger la clave que será la misma con la que el empleado se registra en el SCA.

Antes de inscribir las huellas dactilares de un empleado, éste debe ser registrado como un usuario del dominio de *Windows* con su respectiva clave. Una vez creada la cuenta del empleado, se debe proceder a la inscripción de sus huellas dactilares en *Biologon* 3.0; para más detalles de este proceso, referirse al manual de instalación y operación (**ANEXO E**). Se tomarán por lo menos dos huellas dactilares de cada empleado como una medida preventiva, por ejemplo ambos pulgares, de esta manera el empleado podrá registrar su asistencia con cualquiera de sus huellas.

3.2.2.2.3. Programación y Base de Datos

El interfaz está desarrollado en *Visual* 6.0 el cual interactuará con SQL para el almacenamiento y procesamiento de los datos del sistema.

a. Tablas de la Base de Datos del SCA

Las tablas que maneja SCA se presentan en la figura 3.5, cada una de ellas designada según el tipo de datos que almacenará.

Las cadenas entre tablas significan que éstas se encuentran enlazadas, se debe ver la dirección de la llave; si la llave sale significa que cada vez que se crea un dato en esa tabla, éste tiene que estar enlazado a un dato en la otra. Por ejemplo, a la tabla de Empleados se enlaza la tabla Vacaciones, esto quiere decir que se puede crear un dato (empleado) en la tabla de Empleados sin ningún requerimiento o dependencia de otra, pero al crear un dato en la tabla Vacaciones, éste debe estar enlazado obligatoriamente a un dato en la tabla de

tablas que no tengan cadena alguna quieren decir que son independientes de las demás.

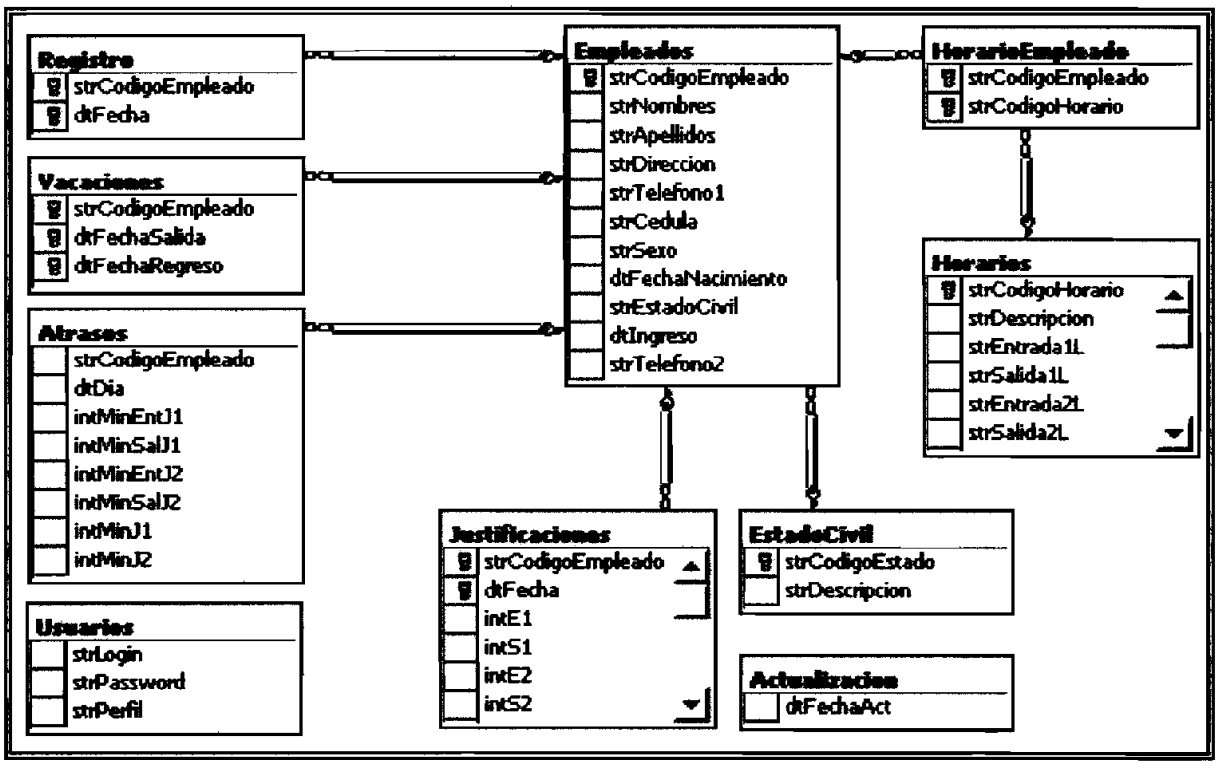


Figura 3.5: Diagrama de interacción de las tablas de la Base de Datos del SCA.

Tabla Empleados.- Se almacenará toda la información personal de los empleados de la EPN, y para cada uno se tendrá los siguientes datos:

- Código
- Nombres
- Apellidos
- Cédula
- Fecha de Nacimiento
- Sexo
- Estado Civil
- Dirección
- Teléfono de la Casa y la extensión donde se lo puede localizar en la EPN.

Cada uno de los datos estará identificado en la tabla con nombres relacionados a los mismos, por ejemplo, el dato de "Nombres" se guardará en la variable strNombres. A esta tabla se enlazan todas las demás exceptuando la tabla de Usuarios, la razón es lógica, todo gira entorno al empleado.

Tabla Estado Civil.- A veces las tablas grandes necesitan de otras para poder interactuar con eficiencia. La tabla Estado Civil contiene cuatro tipos de datos asociados a la variable strEstadoCivil de la tabla de empleados, cuyas descripciones son: Casado, Soltero, Divorciado y Viudo, cada uno referido con un código.

Tabla Horarios.- Es la más grande del SCA, contiene un horario almacenado específico. Esta tabla no se enlaza a ninguna, por eso se puede crear un horario independientemente de las otras tablas.

Dependiendo del tipo de horario, las variables se llenan o se quedan vacías excepto strCodigoHorario y strDescripción. Existen veinticuatro variables más, cuatro por cada día desde el lunes hasta el sábado. Por ejemplo para el día lunes se tiene: strEntrada1, strSalida1, strEntrada2 y strSalida2; si se tiene un horario de jornada única para el día lunes, se llenarán las variables: strEntrada1 y strSalida2, esto más por comodidad en el momento de presentar los datos en un interfaz programado; si es jornada doble se llenarán todas las variables.

Tabla HorarioEmpleado.- Es la tabla encargada de asignar a un empleado un horario en particular, por ello estará enlazada a las dos tablas: Empleados y Horarios, esto quiere decir que para crear una asignación, debe estar obligatoriamente enlazado un empleado y un horario de sus respectivas tablas, lo cual se manejará con los respectivos códigos: strCodigoEmpleado y strCodigoHorario.

Tabla Registro.- Encargada de llevar los registros diarios de cada empleado, es decir la respectiva asistencia, cada registro es una "timbrada" en cierta hora del día de un empleado en particular para todos los días laborables.

(entrada y salida)

cada empleado. Se puede ingresar varias fechas de vacaciones para un solo empleado, como éstas se encuentran enlazadas con la tabla Empleados, cada vez que nos refiramos a vacaciones se debe tener asociado a un empleado en particular.

Tabla Atrasos.- En el SCA se deberá calcular los minutos atrasados del empleado, esta tabla guarda esos minutos y tiene una estructura similar a la de la tabla Horarios. Los atrasos se calculan para una entrada y/o salida dependiendo de la jornada, la diferencia radica que aquí se refiere al día y fecha del atraso, ya que no todos los días lunes por ejemplo se tendrá igual asistencia. El SCA solo envía a la tabla en la base de datos los días en los cuales haya habido por lo menos un atraso, caso contrario no lo almacena.

Tabla Justificaciones.- Creada con la misma filosofía de la tabla de atrasos, aplicable únicamente a los días que el empleado se haya atrasado.

Tabla Usuarios.- Tabla independiente que almacenará los diferentes usuarios que ingresarán al SCA, existirán dos tipos: Administrador y Usuario. El Administrador tendrá derecho a modificar y crear en el SCA, en cambio el Usuario solo tendrá derecho a consulta.

Tabla Actualización.- Tabla independiente que almacenará la última fecha de actualización del registro, proceso que se estudiará mas adelante. Este dato se renueva cada vez que se actualice el registro para que la próxima vez que se llame a esta función el SCA evalúe proceso desde esa fecha.

b. Programación en *Visual* 6.0

La pantalla de ingreso a la aplicación se muestra en la figura 3.6; en ella se debe ingresar:

- *Login*, nombre con el cual se identifica el usuario o administrador.
- *Password*, clave del usuario o administrador.
- Servidor, nombre del servidor al cual se conecta.

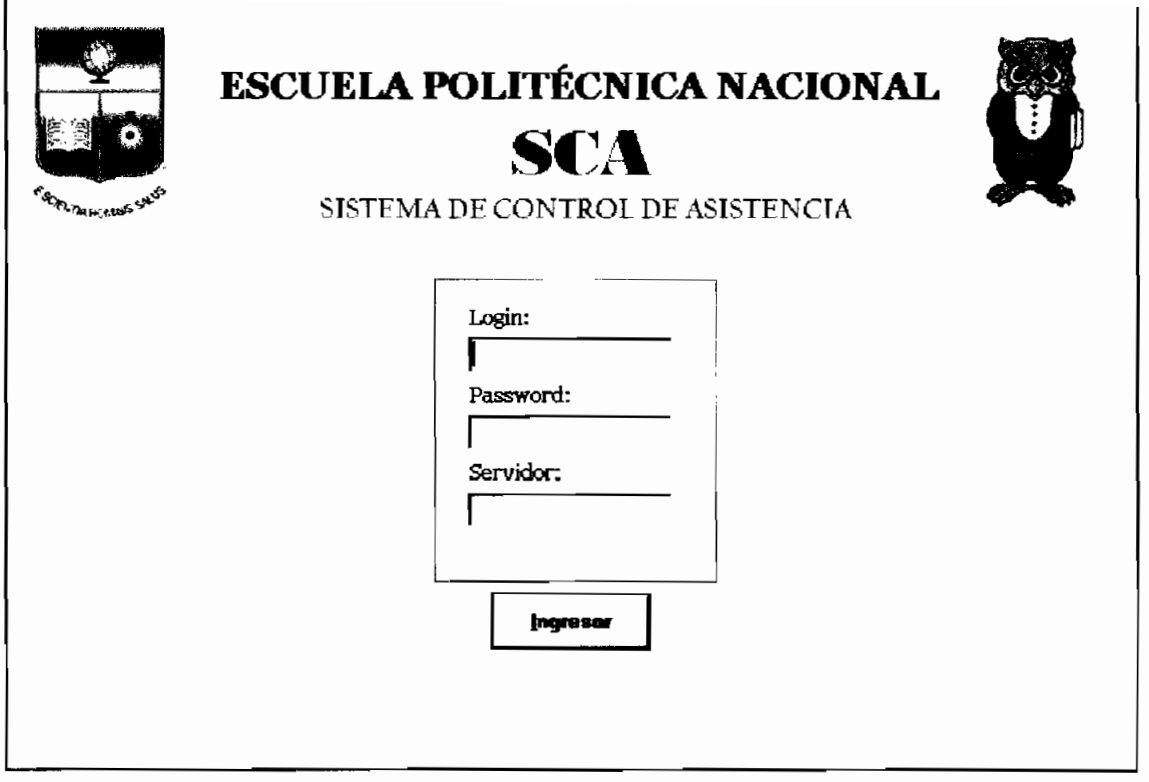


Figura 3.6: Pantalla de ingreso a la aplicación del Servidor.

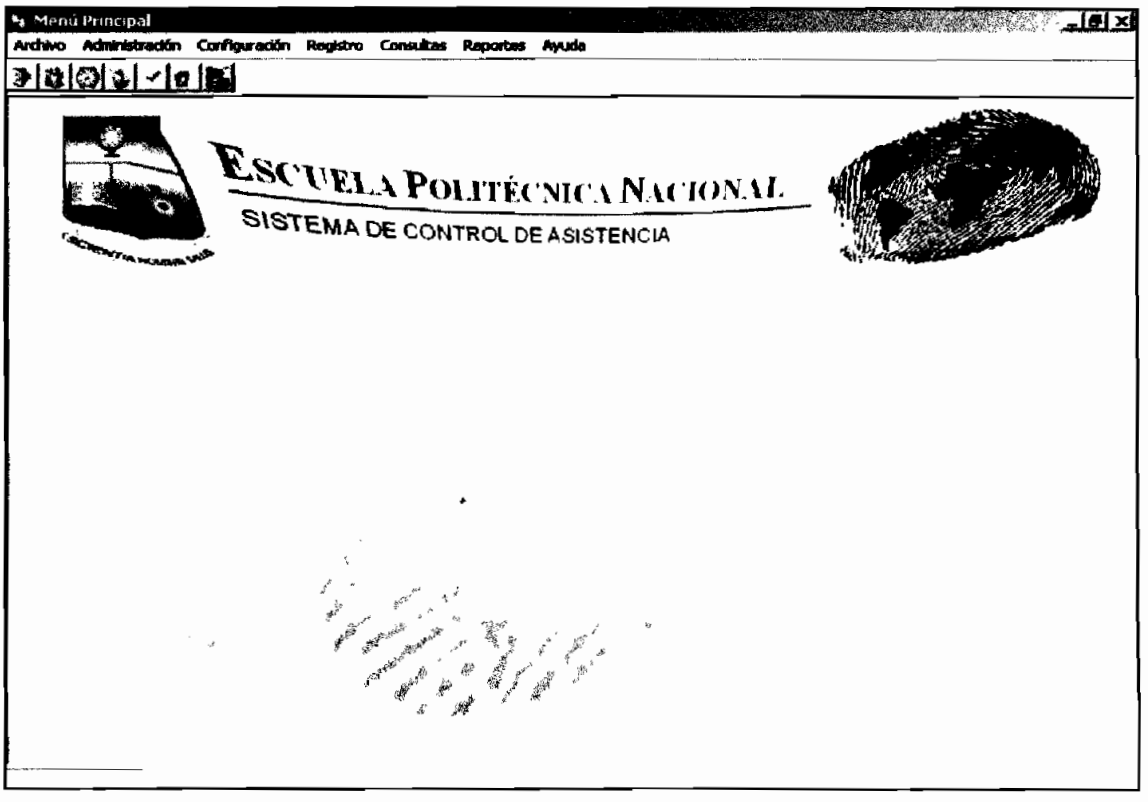


Figura 3.7: Interfaz principal de la aplicación del Servidor.

Empleados

Despliega la grilla de la figura 3.8, en la cual se tiene a todos los empleados registrados.

Al pulsar la opción "Agregar" se despliega una ventana como el de la figura 3.9, permitiendo ingresar los datos personales del empleado para ser almacenados en la tabla Empleados.

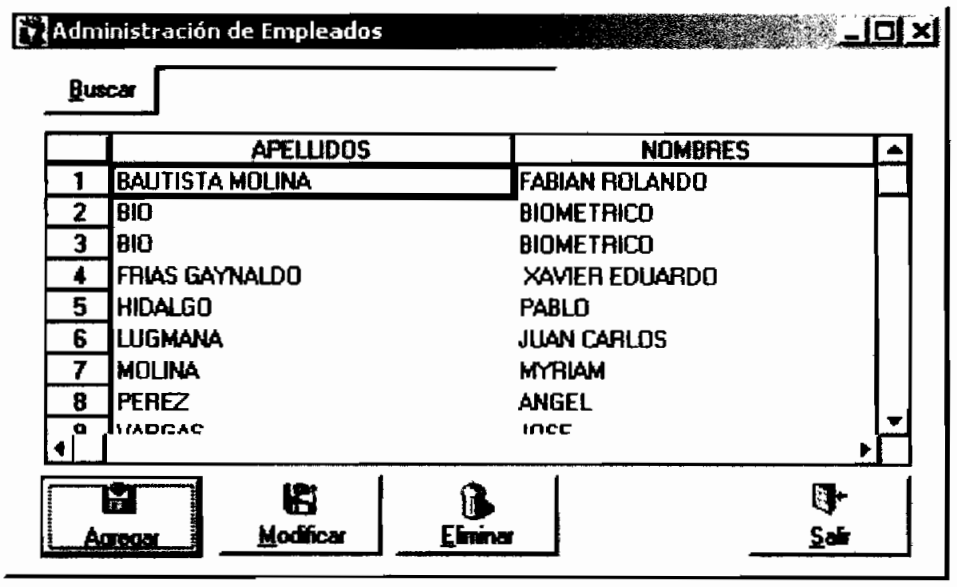


Figura 3.8: Grilla programada para ordenar y desplegar los nombres de los empleados de la EPN.

De estos datos son obligatorios los cuatro primeros; en el caso de que no llenen estos campos el empleado no podrá ser ingresado en la base de datos. En los campos en los cuales se deba introducir solo texto, existen filtros que no permiten ingresar símbolos o números ajenos al campo.

El campo de mayor importancia es el de Código, mediante el cual el empleado será identificado para cualquier operación en el sistema incluida la de registro de asistencia; este campo puede tener una longitud de hasta 10 caracteres. El Código y la clave informática de la cuenta de usuario del empleado en *Windows*

- **Jornada Única.-** Jornada normal de ocho horas, se debe agregar media hora de almuerzo. Este tipo de horario solo permite ingresar la hora de entrada; la hora de salida es calculada por el sistema sumando las ocho horas y media mencionadas.

- **Jornada Diferenciada.-** Puede darse el caso que tenga que trabajar una jornada diferente a la normal de ocho horas, en este caso se ingresa la hora de entrada y salida del empleado. La mínima jornada que permite ingresar el sistema es de una hora.

- **Jornada Diferenciada Doble.-** En este tipo de horario se tiene doble jornada, entre jornadas debe haber un mínimo de una hora. Se deberá ingresar la hora de entrada y salida de ambas jornadas.

La opción para escoger el tipo de horario es por día; la combinación de estas alternativas da una infinidad de opciones que cubren las necesidades de la EPN en cuanto a horarios de empleados.

Una vez definido el tipo de horario diario, se ingresa a una pantalla final donde se ingresará las horas propiamente dichas. Un ejemplo de definición e ingreso se aprecia en las figuras 3.12 y 3.13.

El sistema permite modificar el horario creado, se debe tomar en cuenta que si el horario está asignado, el horario de los empleados asignados también cambiará, y si trata de eliminarlo el SCA retornará un error debido al enlace con la tabla de asignaciones de horario.

Asignación.- Esta opción permite asignar a un empleado un horario previamente creado; estos datos se guardan en la base de datos y cada vez que se refiera al horario del empleado el sistema sabrá cuál de los horarios está relacionado con el mismo. De igual manera se utiliza la funcionalidad de grilla para escoger el empleado para la asignación; una vez seleccionado el empleado, se despliega una pantalla como la de la figura 3.14.

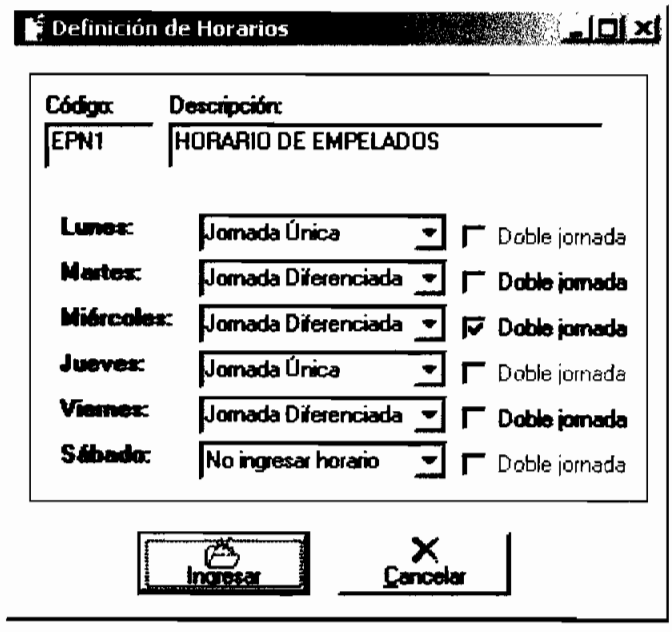


Figura 3.12: Definición de horarios.

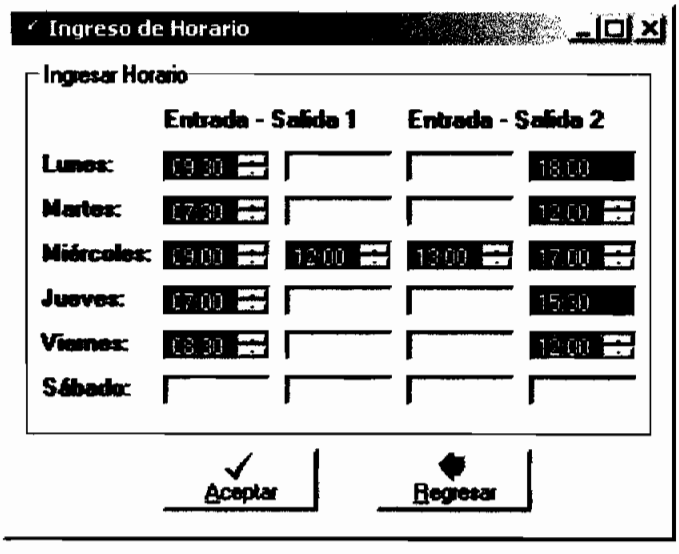


Figura 3.13: Ingreso de las horas de entrada y salida.

Se puede escoger uno de los horarios existentes mediante la lista del combo "Horario" la cual se carga automáticamente con los horarios almacenados en la tabla Horarios al momento de desplegarlo, así mismo se puede modificar y eliminar una asignación realizada.

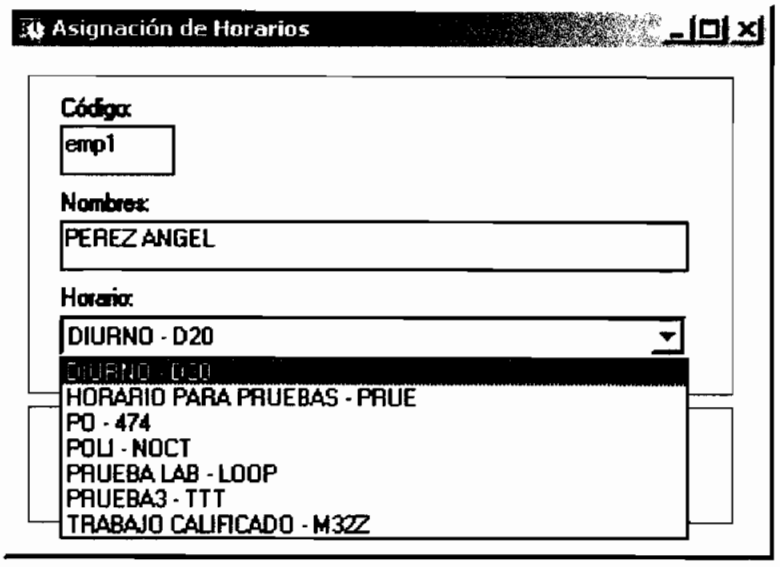


Figura 3.14: Ventana para la asignación de horarios.

Justificaciones

Si un empleado ha faltado cierto día por un motivo justificado, éste puede hacer uso de las justificaciones para no permitir que esos minutos atrasados sean sancionados en su rol de pagos. El SCA consulta todos los días atrasados para registrarlos como posibles días a ser justificados, ya sea parte o total de los mismos.

Para que un día de atraso sea tomado como candidato a ser justificado, debe haber pasado por un proceso que evalúe la asistencia del empleado, este proceso se ejecuta con la "Actualización del Registro", en la cual se toman todos los datos (asistencias) de la tabla de registros de los empleados de la EPN y se realiza la evaluación desde la última fecha de actualización hasta la fecha presente. La "Actualización del Registro" se verá mas adelante en su respectivo menú. Por lo tanto, solo aparecerán los días atrasados que se hayan encontrado hasta la última actualización del registro.

Al momento de seleccionar el menú Justificación, utilizando la funcionalidad de la grilla se desplegará una lista de los empleados de la EPN, se escogerá uno de ellos y se seleccionará "Agregar", que quiere decir que se agregará una

justificación para ese empleado, en ese momento se desplegará una pantalla en la cual se debe escoger desde y hasta qué fecha se desea visualizar los días atrasados para su posible justificación (ver figura 3.15). El SCA solo permitirá desplegar los días de atraso hasta la última actualización del registro, pues los demás días aunque ya hayan transcurrido hasta la presente fecha no estarán disponibles sino hasta una nueva actualización del registro, ver figura 3.16.

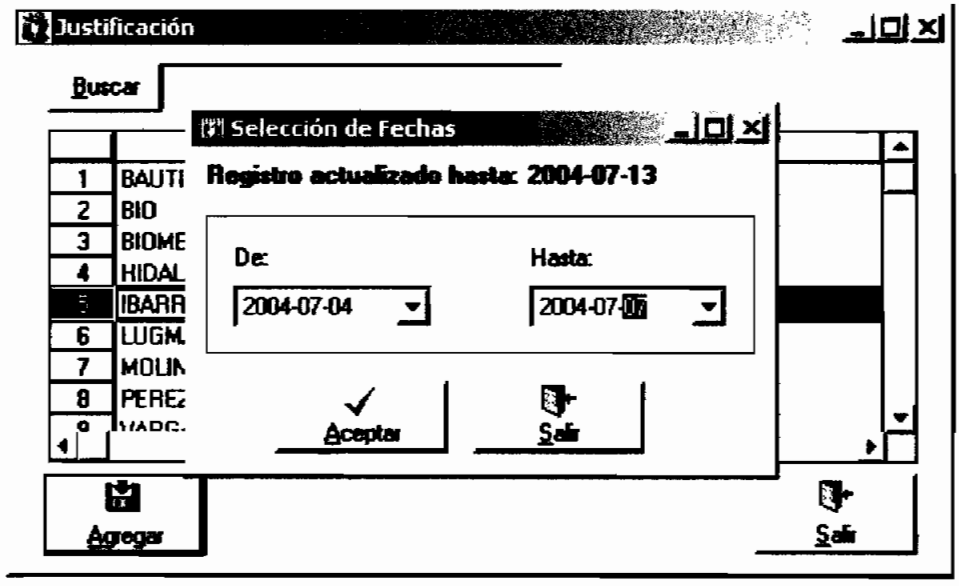


Figura 3.15: Ventana de selección del rango de fechas de atraso para una posible justificación.

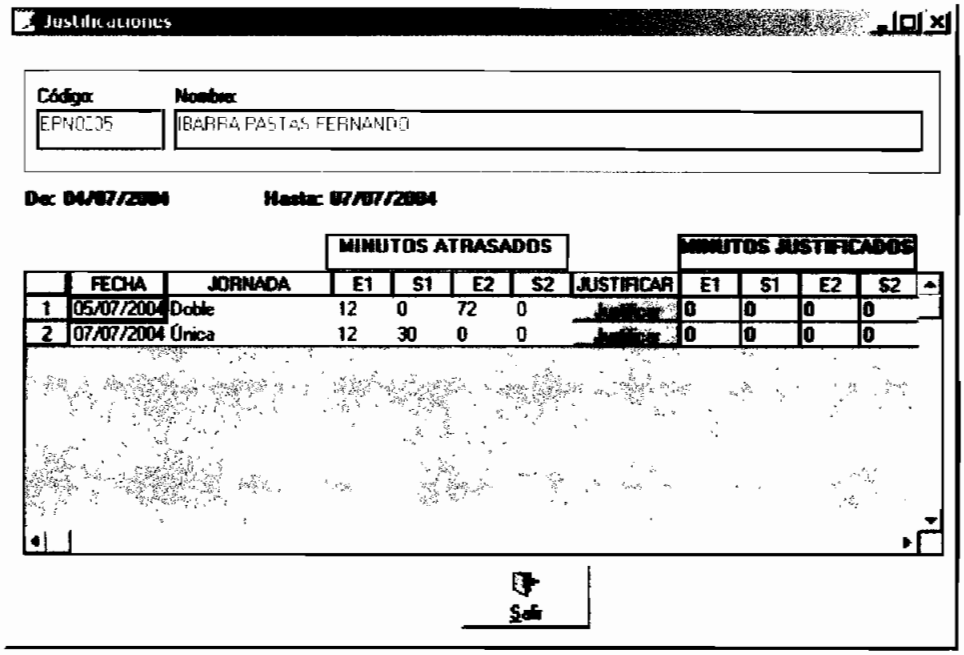


Figura 3.16: Ventana de justificaciones.

Los días atrasados se presentan con la fecha, tipo de jornada y los minutos atrasados en la respectiva entrada o salida. Si se desea justificar algún atraso, se debe pulsar el botón "Justificar" en la fila del día correspondiente; dependiendo de la jornada se desplegará el tipo de ventana, jornada única o diferenciada tal como se indica en la figura 3.17.

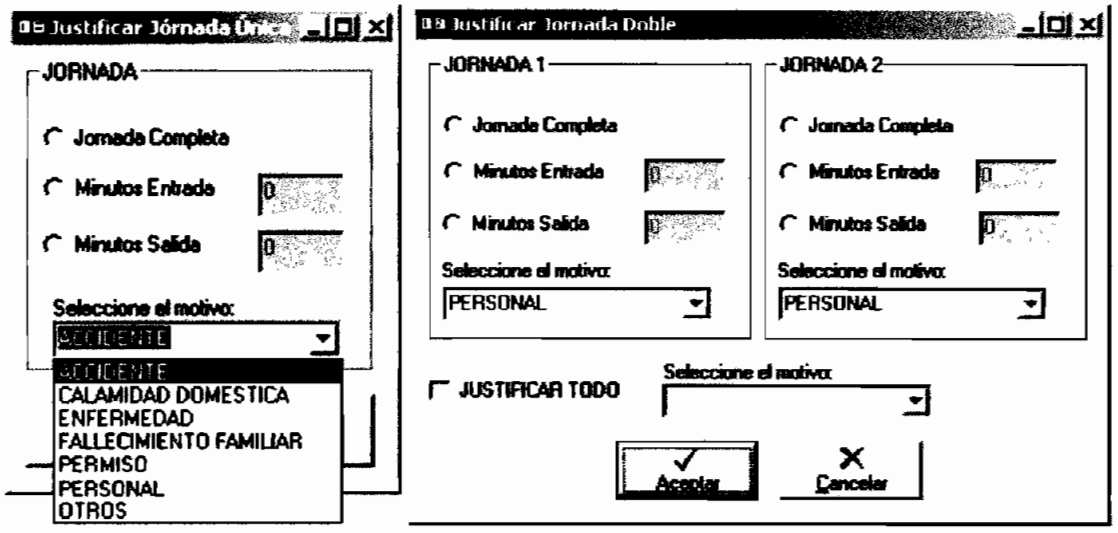


Figura 3.17: Ventanas de justificación, (a) Para jornada única o diferenciada, (b) Para jornada diferenciada doble.

Estas pantallas tienen los respectivos filtros para no ingresar datos incoherentes en el día de atraso como por ejemplo, justificar más minutos de los atrasados, ingresar justificaciones en jornadas que no se atrasó, etc. Existen seis motivos de justificación: Accidente, Calamidad Doméstica, Enfermedad, Fallecimiento familiar, Permiso y Personal, en caso de no estar definido el motivo en las opciones, se ingresará "Otros".

Vacaciones

Esta opción permite que un empleado de la EPN que haya salido de vacaciones no sea tomado en cuenta durante la evaluación de asistencia en los días de ausencia. Se despliega la grilla que se ha manejado anteriormente, se escoge el empleado que saldrá de vacaciones y se despliega una pantalla como la señalada en la figura 3.18.

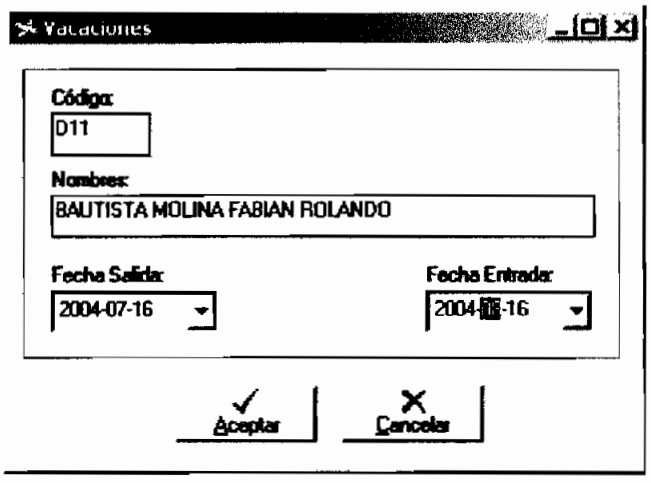


Figura 3.18: Pantalla de ingreso de vacaciones.

Aquí se tiene dos datos que el sistema debe almacenar: Fecha de Salida y Fecha de Entrada. El sistema no admite que la fecha de salida sea menor que la fecha de regreso de las vacaciones, tampoco puede ser menor que la fecha de registro de las vacaciones.

Se puede ingresar varias vacaciones para que éstas se activen en el transcurso del año; si se tiene varias vacaciones, la opción de modificar o eliminar siempre será respecto a las últimas vacaciones ingresadas y si las vacaciones están transcurriendo o ya transcurrieron en fechas anteriores, ya no es posible eliminarlas o modificarlas.

b.3. Menú Registro

El momento que empiece a registrarse la asistencia de los empleados se ingresará en la base de datos para cada día, el código y fecha-hora de sus registros, éstos se acumulan hasta que un proceso de decisiones evalúe la asistencia de los mismos. Este proceso lo realiza la opción "Menú Registro".

Como se vio en las Justificaciones, la actualización del registro es crucial para la evaluación de atrasos y justificaciones. El diagrama de la figura 3.19 permite visualizar cómo ocurre este proceso desde el momento que se pulsa la opción "Actualizar".

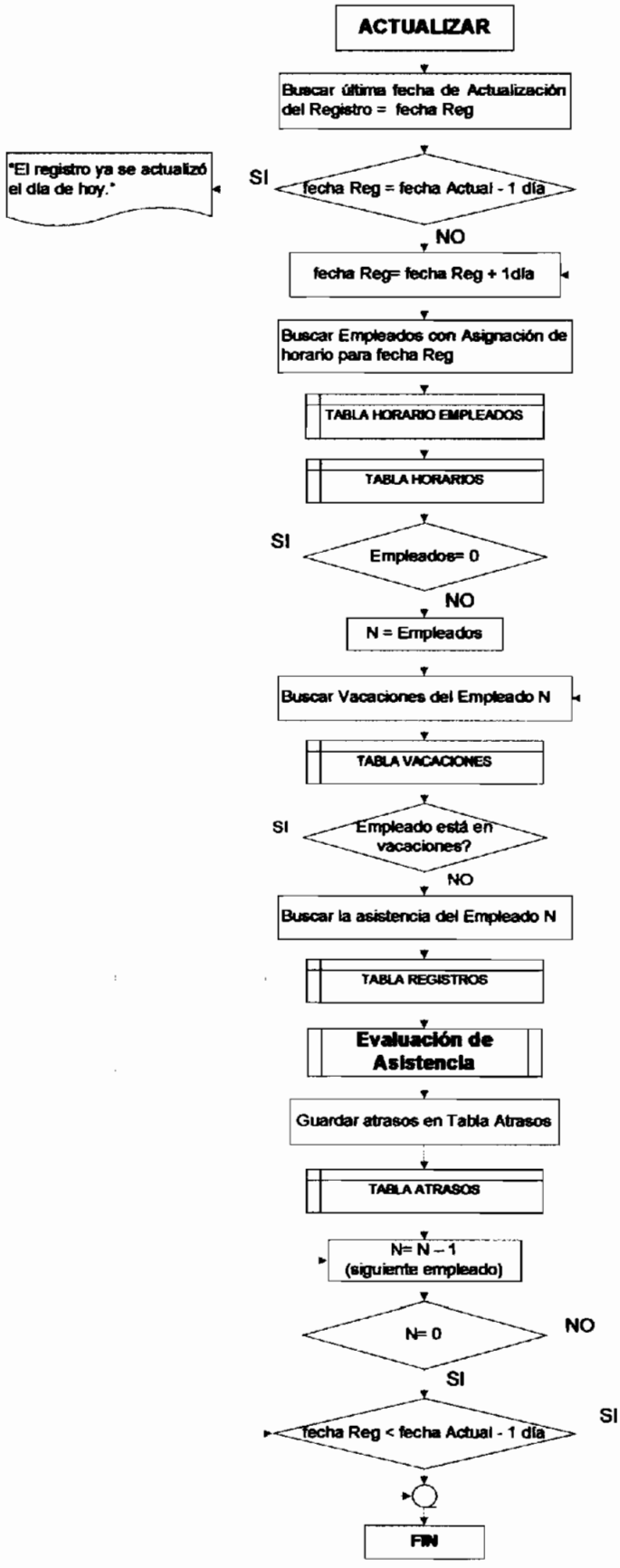


Figura 3.19: Proceso de Actualización del Registro de Asistencia.

El proceso ocurre desde la fecha de la última actualización hasta un día antes del día que se actualiza; primero se consulta la última actualización del registro, si ya se ha actualizado éste envía un mensaje de aviso. En caso que el registro no esté actualizado, para cada día se consulta los empleados que debieron laborar esa fecha y si éste está en vacaciones; se calcula los atrasos si los mismos existen para cada empleado encontrado, y así se repite para los días restantes hasta un día antes de la fecha de actualización.

Cabe señalar que en la tabla de Atrasos sólo se guardan los días que tengan al menos un atraso. En la figura 3.19 se muestra la función "Evaluación de Asistencia", ésta se explica a continuación.

Un empleado tendrá la obligación de registrar sus entradas y salidas del trabajo; el registro será el proceso con el cual un empleado inscriba la hora de entrada o salida de su trabajo mediante el uso del SCA. De esa manera según el horario asignado al empleado, éste tendrá solo dos opciones: registrarse dos o cuatro veces en un día determinado.

El sistema no tendrá problemas si el empleado registra sus entradas y salidas normalmente, es decir que si trabaja una sola jornada, éste tendrá que tener dos registros, ni más ni menos, lo mismo sucede con la jornada doble, en este caso deberá tener cuatro registros. ¿Pero qué sucede si se tiene menos o más registros en un día de los que debería tener? Si existe el número de registros normal que debe haber en un día, se asume una asistencia normal del empleado, o sea, que el primer registro del día debe ser la entrada al trabajo, y el último la salida. Parece sencillo, pero si hay menos o más registros de los normales, ¿cómo saber si el primero es realmente una entrada y no una salida?

Para ilustrar este problema se propone el siguiente ejemplo: un empleado tiene que registrarse cuatro veces en un horario de jornada doble cuya asistencia es: 08:00 a 12:00 y de 14:00 a 17:00. El SCA quiere evaluar su asistencia pero encuentra que el empleado en ese día sólo tiene tres registros en la base de datos: 08:00, 13:00 y 17:00. Es evidente que no ha registrado su salida a medio

día ¿o será que no registró su entrada a la segunda jornada? Cómo saber qué registro se le olvidó, la salida o la entrada. Aquí surgen algunas opciones que pudieron haber pasado, por ejemplo: vino en la mañana normalmente y registró la entrada pero salió sin registrarse una hora después o sea a las 09:00 a realizar otras actividades y regresó a la jornada de la tarde pero registrando su respectiva entrada. Otra opción es que vino en la mañana y se olvidó de registrar su salida a medio día. Una tercera posibilidad es que cumplió normalmente con su jornada de la mañana y se olvidó de registrar la entrada de la segunda jornada. Una cuarta opción es que cumplió con la jornada de la mañana y salió a las 13:00 y se fue a realizar otras actividades, como era tarde solo regresó por sus cosas y registró la salida de la segunda jornada; y así puede haber una infinidad de estos casos.

El SCA debe tomar decisiones en estos casos, para lo cual considera las siguientes reglas:

1. Un empleado no podrá registrarse más veces que el número de registros normales de un determinado día, si éste quiere registrarse más de lo debido, el SCA lo rechaza.

2. En el registro de la primera entrada a la EPN, el SCA no permitirá el mismo sino a partir de media hora antes de la hora de entrada.

3. Si el SCA detecta que el empleado no ha registrado la entrada o salida de una jornada, éste registra la jornada como una falta.

4. Para que una entrada sea considerada como tal debe ser registrada a partir de media hora antes a la hora de señalada.

5. Si existe divergencia en que un registro es entrada o salida, se aplicará la regla # 4 para esta decisión.

Con estas reglas el SCA realiza la "Evaluación de Asistencia" de los empleados de la EPN, y para una mejor comprensión se presentan los algoritmos

implementados en el *software* mediante los diagramas de flujo de las figuras 3.20 a 3.23 para los posibles casos que se puedan presentar.

Los algoritmos primero evalúan si los registros son entradas o salidas en base a las reglas # 2, 3 y 4 revisadas anteriormente y en caso de encontrar una jornada que le falte un registro, automáticamente anula la jornada total.

Como se mencionó solo se tendrá dos posibilidades, cuatro o dos registros obligatorios, a este proceso se denomina "Toma de Decisiones".

Para una mejor comprensión se tiene la siguiente declaración de variables:

Descripción	**Diagrama de Flujo**
Variables almacenadas en la Base de Datos TABLA HORARIOS	
Entrada a la Primera Jornada	Entrada 1
Salida de la Primera Jornada	Salida 1
Entrada a la Segunda Jornada	Entrada 2
Salida de la Segunda Jornada	Salida 2
Variables del Registro de asistencia del Empleado TABLA REGISTRO	
No se puede decir si son entradas o salidas antes de la toma de decisiones, ya que puede haber uno, dos, tres, cuatro o ningún registro.	Registro 1
	Registro 2
	Registro 3
	Registro 4
Variables asignadas después de la Toma de Decisiones de entradas y salidas	
Entrada a la Primera Jornada	Entrada Eval 1
Salida de la Primera Jornada	Salida Eval 1
Entrada a la Segunda Jornada	Entrada Eval 2
Salida de la Segunda Jornada	Salida Eval 2

En el caso de jornada única sea diferenciada o no, se tendrá las siguientes variables:

Descripción	Diagrama de Flujo
Variables almacenadas en la Base de Datos TABLA HORARIOS	
Entrada	Entrada 1
Salida	Salida 1
Variables del Registro de asistencia del Empleado TABLA REGISTRO	
No se puede decir si son entradas o salidas antes de la toma de decisiones, ya que puede haber uno, dos o ningún registro.	Registro 1
	Registro 2
Variables asignadas después de la Toma de Decisiones de entradas y salidas	
Entrada	Entrada Eval 1
Salida	Salida Eval 1

El código fuente de estos algoritmos se encuentra documentado en el **ANEXO D**, en las siguientes páginas:

- Algoritmo de la figura 3.20 en las páginas 94 y 95 como la subrutina "evalua4Registros".
- Algoritmo de la figura 3.21 en las páginas 93 y 94 como la subrutina "evalua3Registros".
- Algoritmo de la figura 3.22 en las páginas 92 y 93 como la subrutina "evalua2Registros".

Para el caso de la "Toma de Decisiones" de **jornada única** sea diferenciada o no el algoritmo se lo presenta en la figura 3.23 y su código fuente se encuentra documentado en el **ANEXO D** página 91 como la subrutina "evaluaUnicaDif".

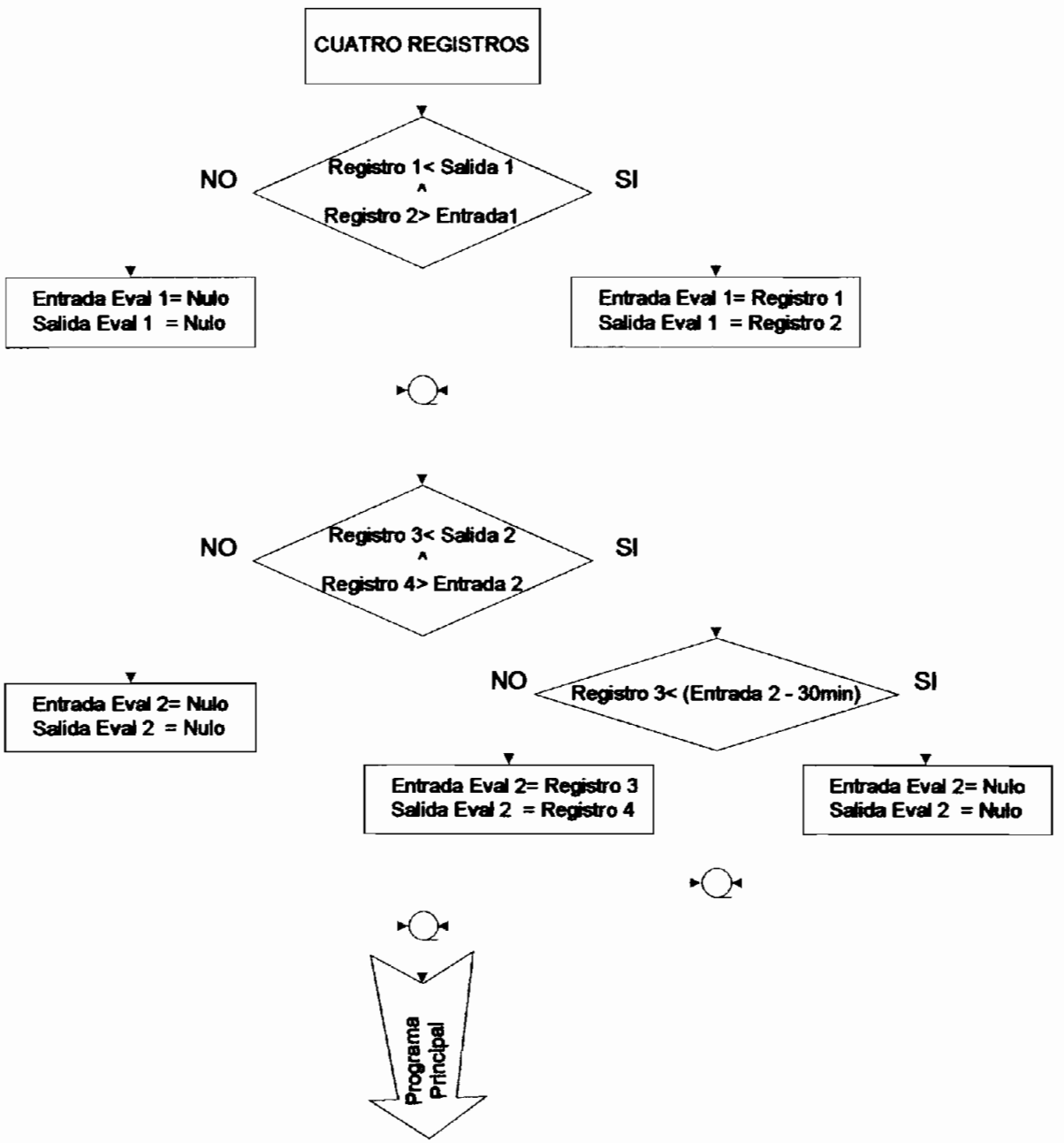


Figura 3.20: Proceso de Toma de Decisiones para jornada diferenciada doble, opción: cuatros registros del empleado.

Después de la Toma de Decisiones viene la Evaluación General (ver figuras 3.24 y 3.25), proceso con el cual se calcularán los minutos atrasados en el caso de que el empleado los tenga.

Las variables a tomarse en cuenta en la Evaluación General son:

Minutos Atrasados	
Descripción	**Diagrama de Flujo**
Entrada de la Primera Jornada	Atraso E1
Salida de la Primera Jornada	Atraso S1
Entrada de la Segunda Jornada	Atraso E2
Salida de la Segunda Jornada	Atraso S2

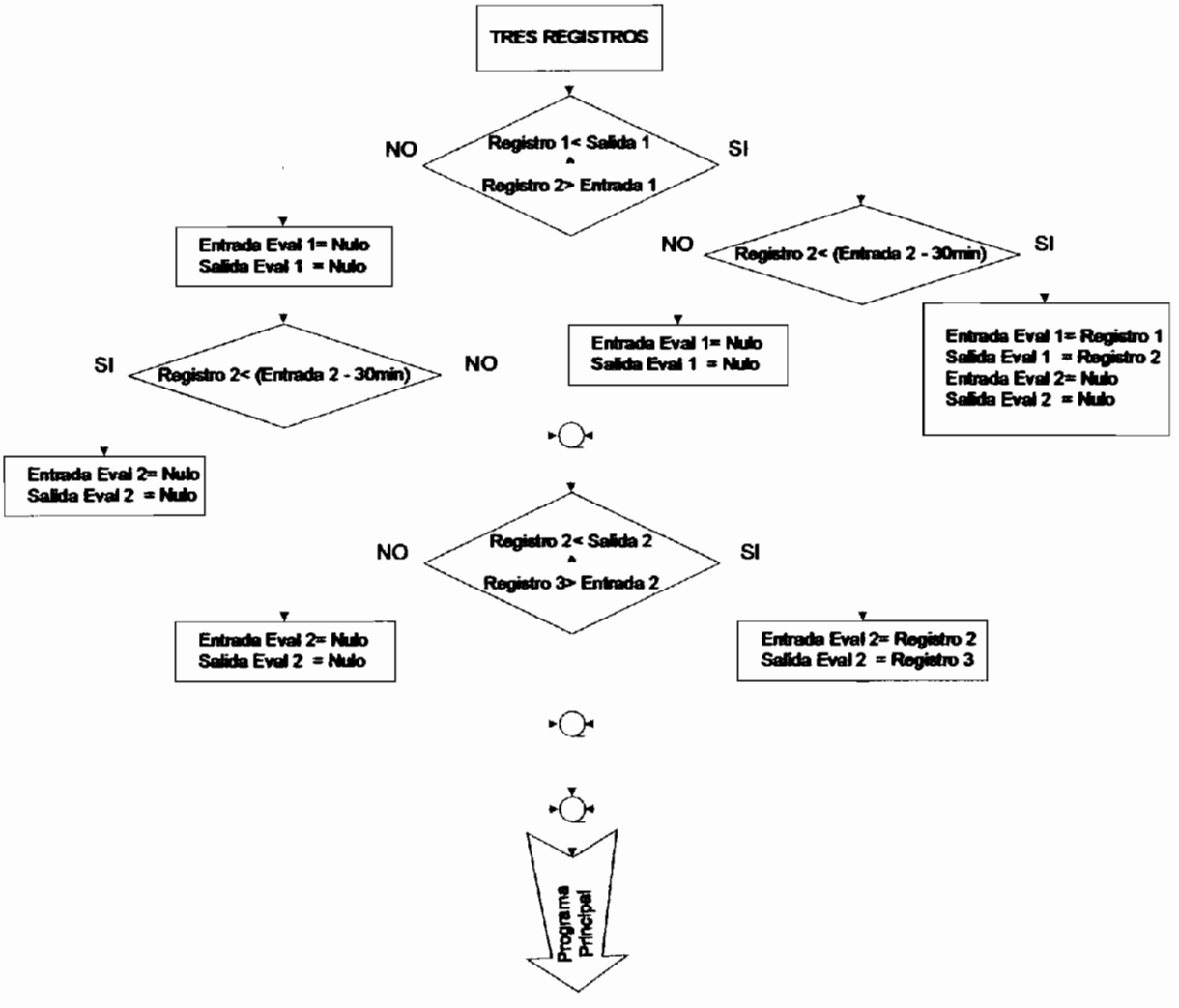


Figura 3.21: Proceso de Toma de Decisiones para jornada diferenciada doble, opción: tres registros del empleado.

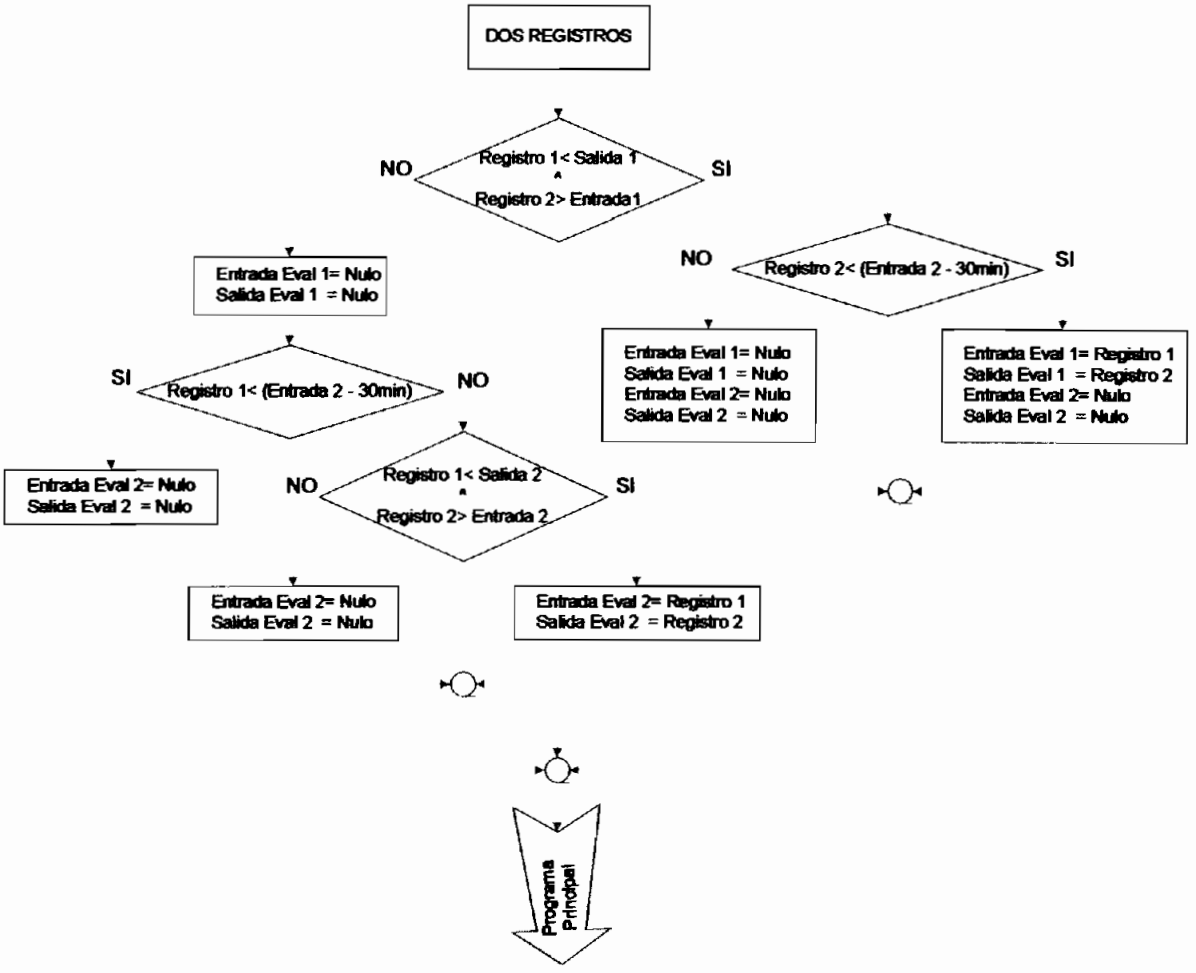


Figura 3.22: Proceso de Toma de Decisiones para jornada diferenciada doble, opción: dos registros del empleado.

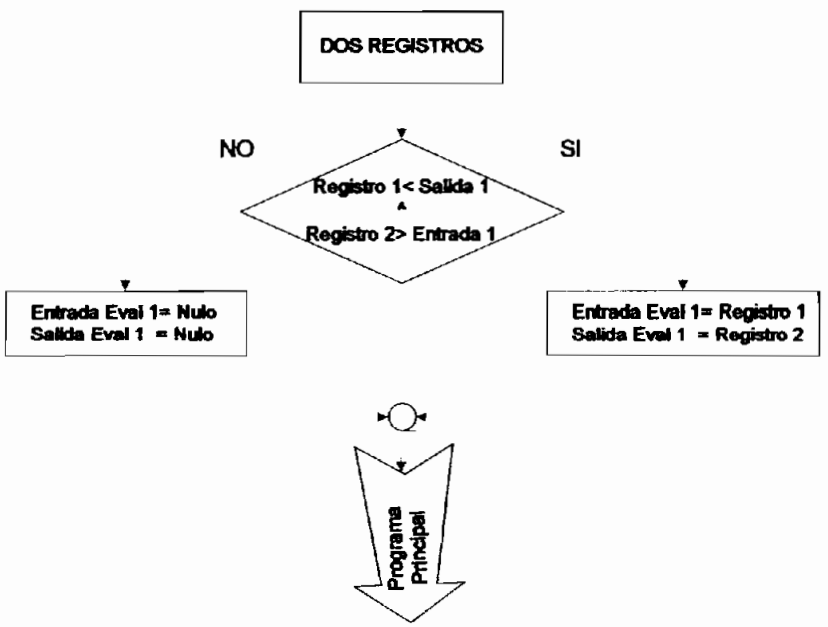


Figura 3.23: Proceso de Toma de Decisiones para jornada única o diferenciada.

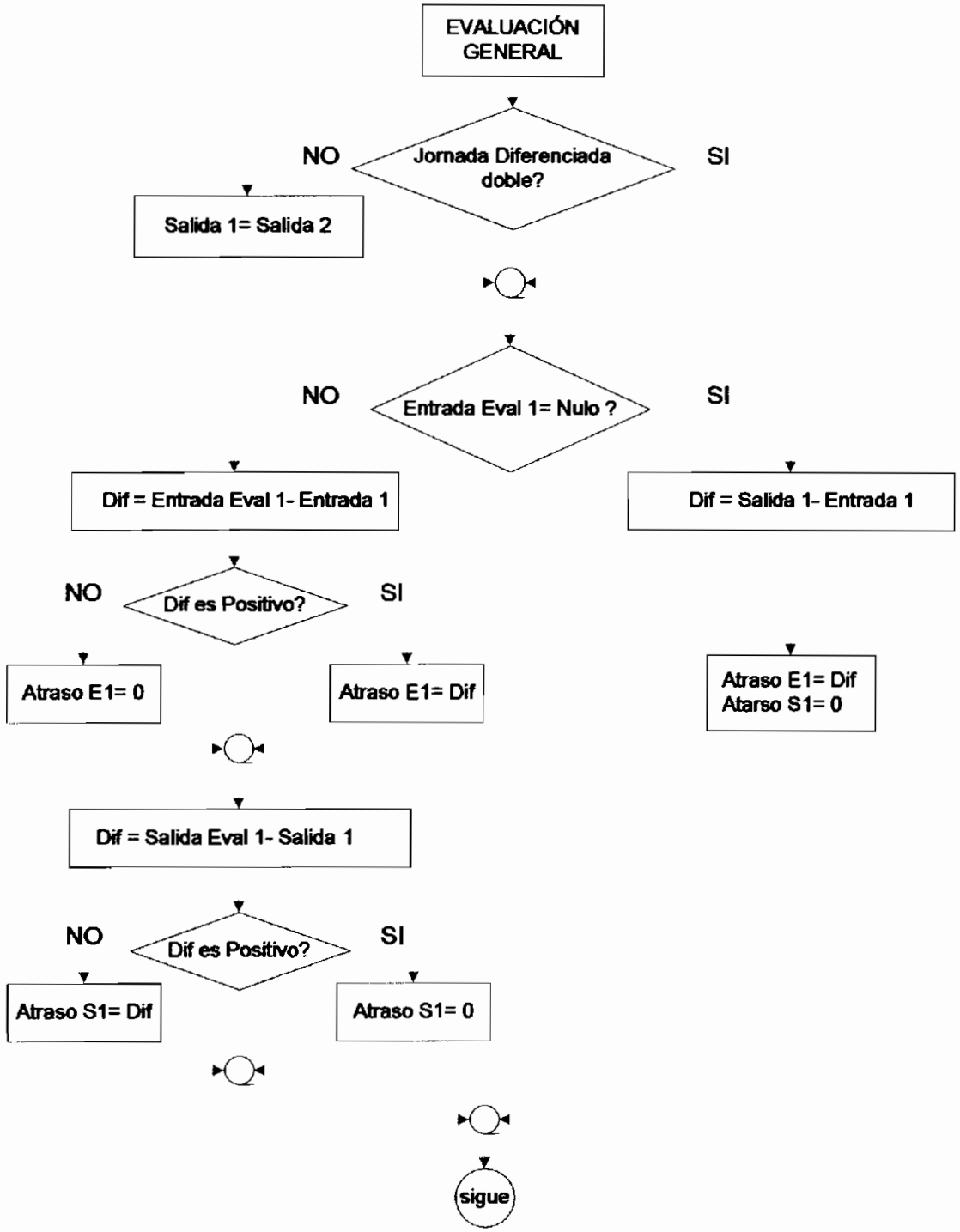


Figura 3.24: Proceso de la subrutina "Evaluación General". Parte 1 de 2.

El código fuente de la subrutina de las figuras 3.24 y 3.25 se encuentra documentado en el **ANEXO D** páginas 95 - 97 como la subrutina "EvaluacionGeneral".

Todos estos procesos se ejecutan con solo pulsar en el menú Registro la opción Actualizar.

Cabe recordar que el proceso de Toma Decisiones y cálculo de los minutos atrasados o Evaluación General se lo realiza para todos los empleados que tengan un horario asignado. Se debe tener cuidado de no asignar un horario a un empleado si éste aun no va a registrarse en los siguientes días; el momento que hay una asignación automáticamente pasa a este proceso, si el empleado no es notificado que debe registrarse desde cierto día, el SCA evaluará esos días como faltas a partir de la última actualización del Registro. Para evitar inconvenientes, se debe asignar el horario al empleado el día que empiece a registrarse y además actualizar el Registro para que empiece desde ese día su evaluación de asistencia.

b.4. Menú Consultas

Permite ingresar a la base de datos del SCA en modo sólo lectura, de una manera rápida, para poder consultar datos de interés, como son:

- Asistencia.
- Datos personales del empleado.
- Horario asignado al empleado.
- Vacaciones.
- Horarios existentes en el SCA.

El usuario no podrá modificar ningún parámetro en este menú.

b.5. Menú Reportes

Mediante la programación en *Visual* 6.0 y con la ayuda de la herramienta de Microsoft Office 2003, Microsoft Office Excel, el SCA puede realizar reportes listos para ser impresos desde Excel. El usuario sólo debe escoger el tipo de reporte que desea para que automáticamente se despliegue una hoja de Excel con el

- Registrar la asistencia de los empleados mediante la autenticación de la huella dactilar.

- Informar al empleado la hora exacta con la cual el SCA está funcionando.

- Indicar al empleado en cada inscripción el número de registros que tiene en ese día.

- Hacer cumplir la regla #2 de la Toma de Decisiones del SCA.

- Cuando se realice un registro exitoso de un empleado, no permitir un nuevo registro hasta cinco minutos después para aquella persona; esto es debido a la inseguridad del empleado en el momento de registrarse pudiendo desencadenar una serie de registros innecesarios y que al final lo perjudican.

Gracias a la funcionalidad de *Biologon* 3.0 Cliente/Servidor, la autenticación biométrica se la realizará en el Terminal mediante la herramienta de *BioShield*, como resultado éste enviará el código del respectivo empleado por la red hacia el Servidor; una vez que lo reciba se guardará en la base de datos junto con la hora y día exacto del registro de asistencia. El Terminal contabilizará el número de registros para cada empleado, de modo que cada vez que el empleado acuda a inscribir su asistencia se le informará el número de registro que hasta el momento lleva en ese día, el *software* no permitirá un número mayor de registros que el indicado en su horario.

Un diagrama de funcionamiento del Cliente se presenta en la figura 3.26.

Como se puede apreciar en el diagrama una vez que el empleado inscribe su huella, Biologon 3.0 con su herramienta BioShield validará la huella, si la validación es favorable Bioshield devuelve el código del empleado y pasa al siguiente proceso que es conectarse al Servidor para que con el código del empleado se puedan extraer los datos mencionados. Se evaluará si ese día

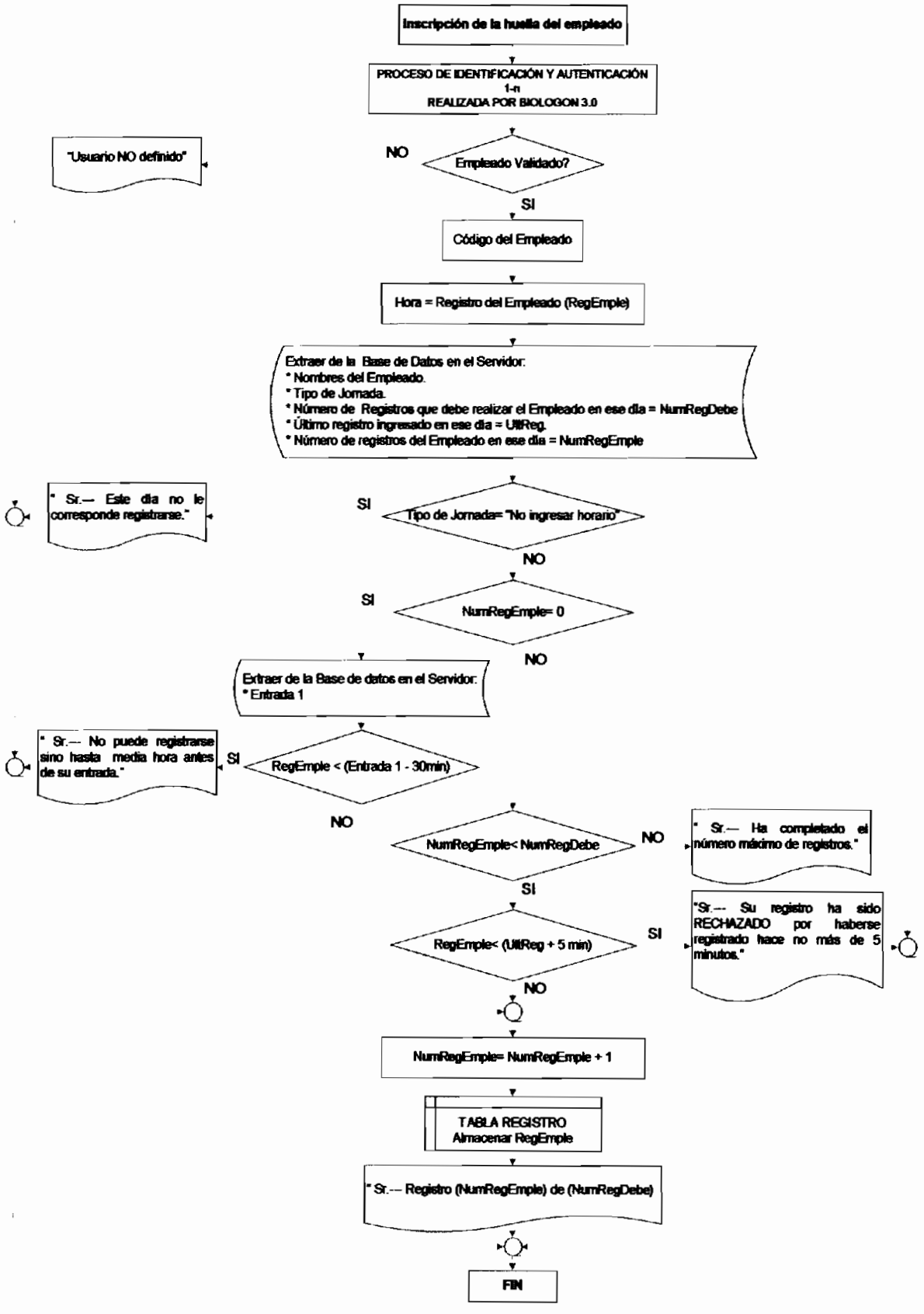


Figura 3.26: Proceso de inscripción de un registro en el Terminal.

debe trabajar o no, si debe trabajar chequea si el registro inscrito es el primero del día; si es el primero se asegura que no sea antes de media hora a la primera entrada caso contrario lo rechazará, si no es el primero verifica que no se inscriba en más registros que los que debe, en cuyo caso se rechazará. La última comprobación es chequear que el registro no sea tan reciente, mínimo deben haber pasado cinco minutos del último registro. Para una mayor compresión se sugiere revisar el código fuente de este *software* que se encuentra en el **ANEXO D** páginas 139- 144.

El interfaz que va a interactuar con el empleado se presenta en la figura 3.27.

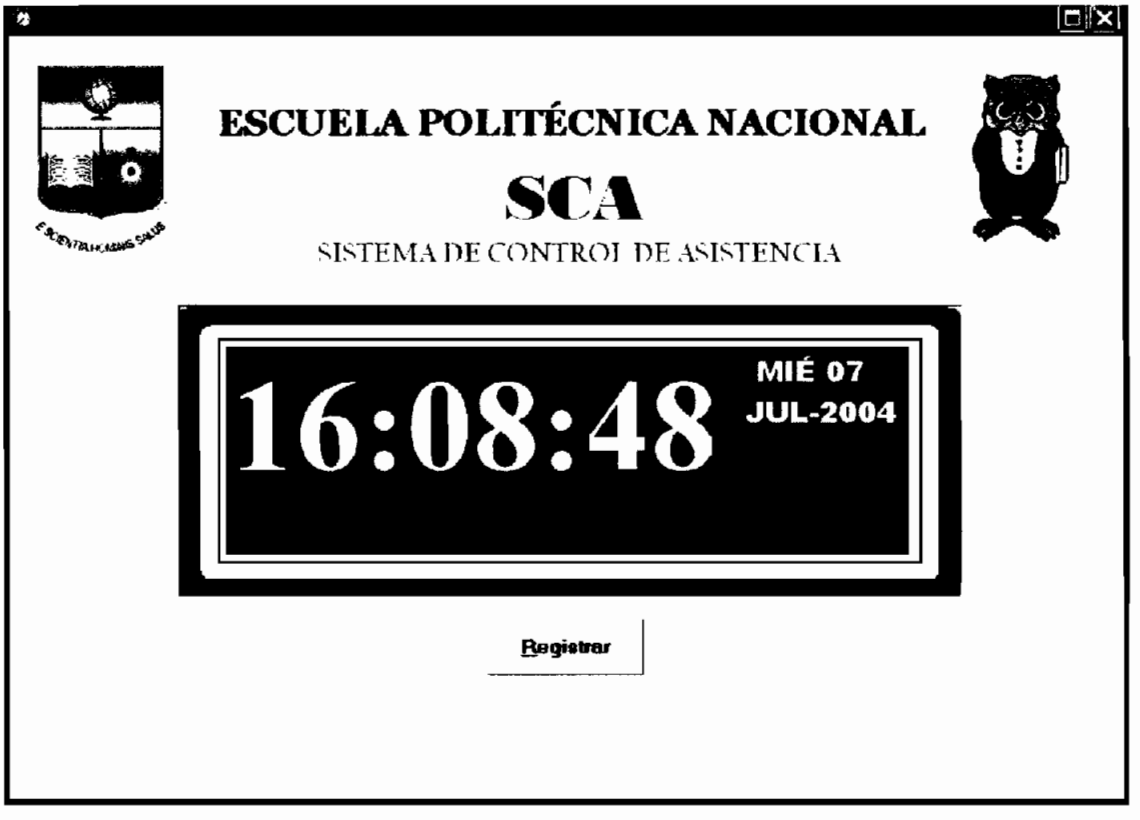


Figura 3.27: Interfaz de inscripción para los registros de asistencia.

En el momento que el empleado pulse el botón "Registrar" aparecerá una pantalla como la de la figura 3.31 y el lector de huellas dactilares empezará a emitir una luz roja invitando a que el empleado coloque su dedo sobre el mismo, luego de lo cual *Biologon* 3.0 empezará la validación del usuario, si la validación es favorable *Biologon* 3.0 devolverá la clave de usuario o código de empleado para seguir con el proceso.

Como se estudió, *Biologon* 3.0 cuenta con una herramienta denominada *Bioshield* la cual permite proteger el ingreso a aplicaciones de *Windows* o similares. Cuando algún usuario desea ingresar a una aplicación normalmente debe pulsar un botón o icono, al realizar esta acción se despliega una ventana que le pide ingresar tanto el *Login* o Nombre de usuario y *Password* o Clave de acceso y se pulsa comúnmente un botón "Aceptar", si los campos son los correctos el ingreso se efectúa. *Bioshield* realiza toda esta tarea cuando valida a un usuario, es decir ingresa el nombre de usuario y clave almacenados en la Base de Datos de *Biologon* 3.0 en los respectivos campos y pulsa el botón "Aceptar".

Aprovechando esta funcionalidad, el botón o icono sería el botón "Ingresar" del interfaz de usuario de la figura 3.27, y se debería elaborar una pantalla de acceso en *visual* 6.0, la cual debe tener dos campos de texto, para los nombres y clave de usuario respectivamente y un botón "Aceptar" que indicaría al *software* de Terminal que el campo con el clave o código del empleado está lleno y puede capturarlo para seguir con el proceso. Para que una aplicación esté protegida por *Bioshield*, se debe registrar a los usuarios en el "Banco de Contraseñas" que es una opción del mismo. Como un resumen se presenta la elaboración y protección de la pantalla de captura del código del empleado:

1. Se elaboró una pantalla en *visual* 6.0, la cual cuenta con las dos cajas de texto para nombre y contraseña de usuario y el botón "Aceptar", ver figura 3.28.

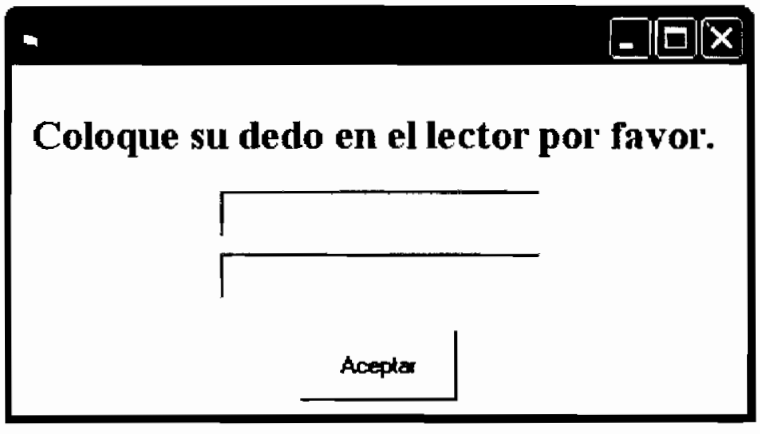


Figura 3.28: Pantalla de captura del código del empleado.

2. Se procede a la protección de la pantalla con *Bioshield* mediante el Banco de Contraseñas. Para ello se desplegará una pantalla que le preguntará con qué nombre y contraseña desea ingresar a la aplicación, se debe escoger la opción "Utilizar mis credenciales de *Windows*" ya que posteriormente se debe ingresar los demás usuarios o empleados creados en el domino de *Windows* (ver figura 3.29). La aplicación queda protegida y se podrá ingresar solamente con un permiso de acceso perteneciente al usuario que se encuentre en esa sesión de *Windows*.

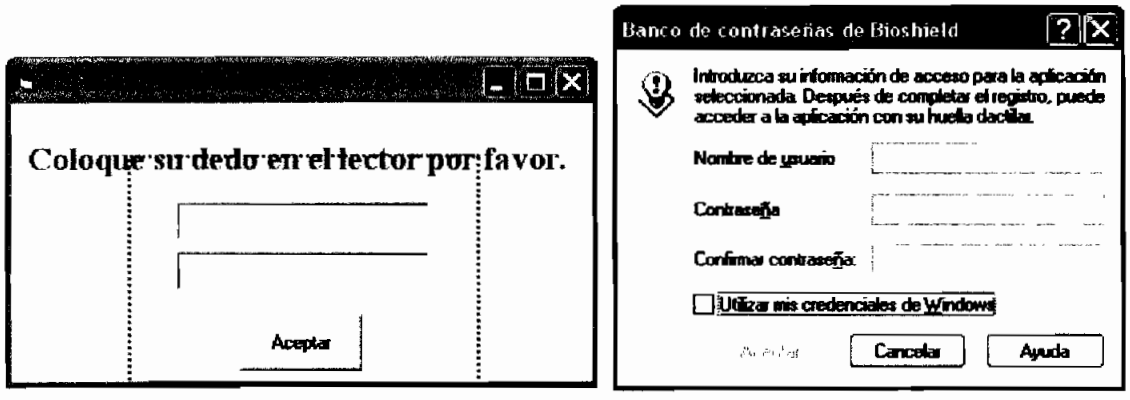


Figura 3.29: Protección de la pantalla de captura del código del empleado utilizando el Banco de Contraseñas de *Bioshield*.

3. Para ingresar a los demás usuarios o empleados del dominio se debe ir a la opción propiedades de *Bioshield*, en la que se desplegará una pantalla y en la caja de "Aplicaciones" aparecerán todas las aplicaciones protegidas, en este caso solo una: Reloj1-n que es la pantalla que indica la hora en la que se registra el usuario (ver figura 3.30). Para agregar los demás empleados se debe escoger el único usuario y seleccionar copiar, esta opción muestra todos los usuarios (empleados) del domino a los cuales se puede copiar el acceso, de esa manera se va añadiendo a todos los empleados, Para más detalles sobre la protección de aplicaciones mediante *Bioshield* referirse al manual de instalación y operación, **ANEXO E**.

De esta manera se recupera el código del empleado para el proceso de inscripción de registros, cabe recalcar que el código es la clave o contraseña de *Windows* con que se inscribió al empleado en el dominio. Solo se utilizará la caja de texto con la clave, la otra se ignora.

3.3. EVALUACIÓN DEL PROTOTIPO

El paquete *Biologon* 3.0 que se adquirió para la evaluación del SCA incluye una licencia para cinco usuarios, razón por la cual se realizó la evaluación con cinco empleados. Se ingresó cinco horarios diferentes, uno para cada empleado.

Para la evaluación no fue necesario tener cinco personas distintas, con una sola es suficiente ya que se puede inscribir hasta diez huellas dactilares de una sola persona, una huella puede ser inscrita como si fuera una persona diferente; de esa manera en la evaluación se puede forzar varias situaciones que pueden ocurrir en una semana laboral.

La base datos de los empleados se presenta en la figura 3.32.

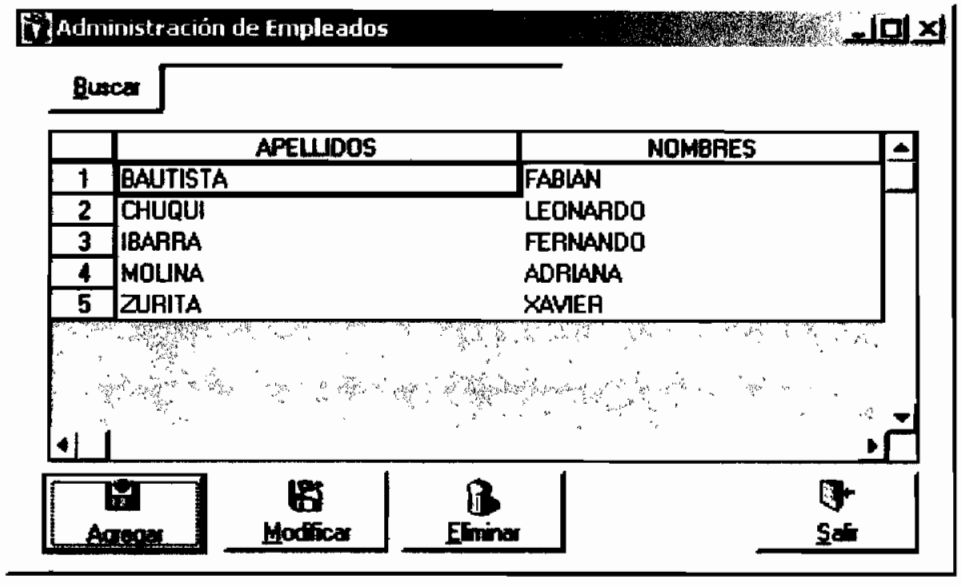


Figura 3.32: Lista de empleados para la evaluación del SCA.

Los horarios asignados se muestran en las figuras 3.33 a 3.37.

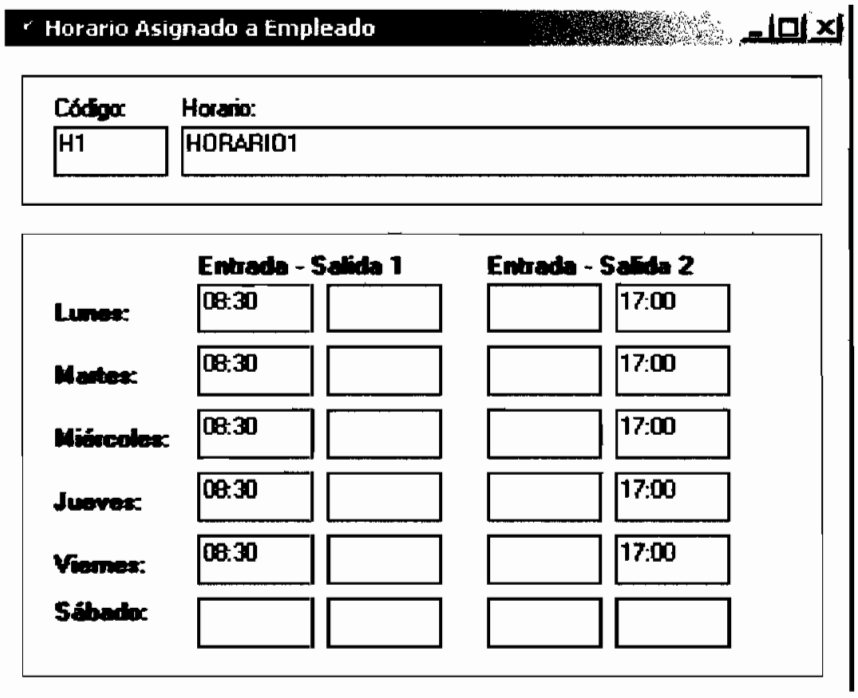


Figura 3.33: Horario asignado al empleado FABIAN BAUTISTA.

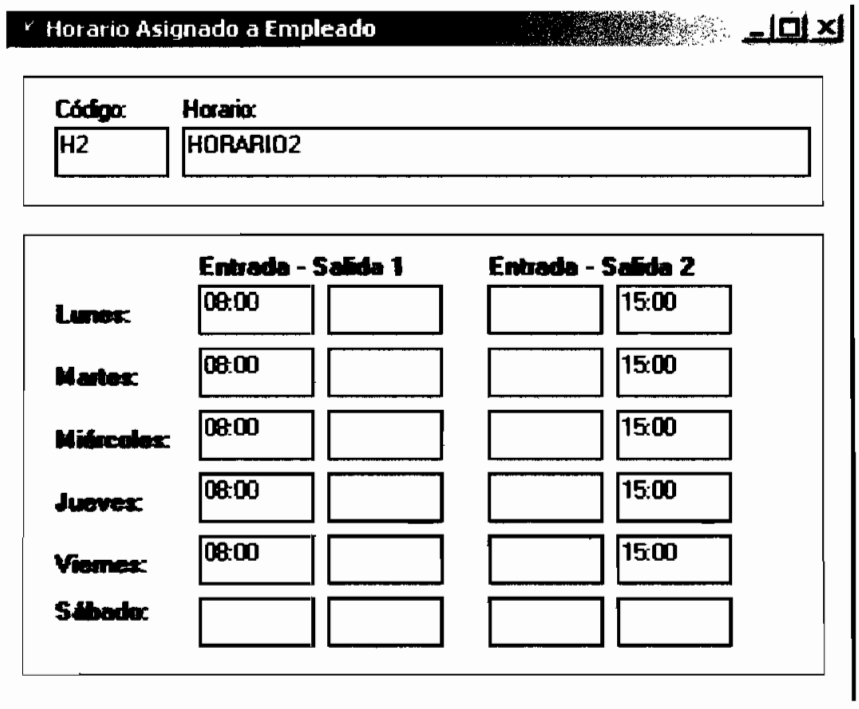


Figura 3.34: Horario asignado al empleado LEONARDO CHUQUI.

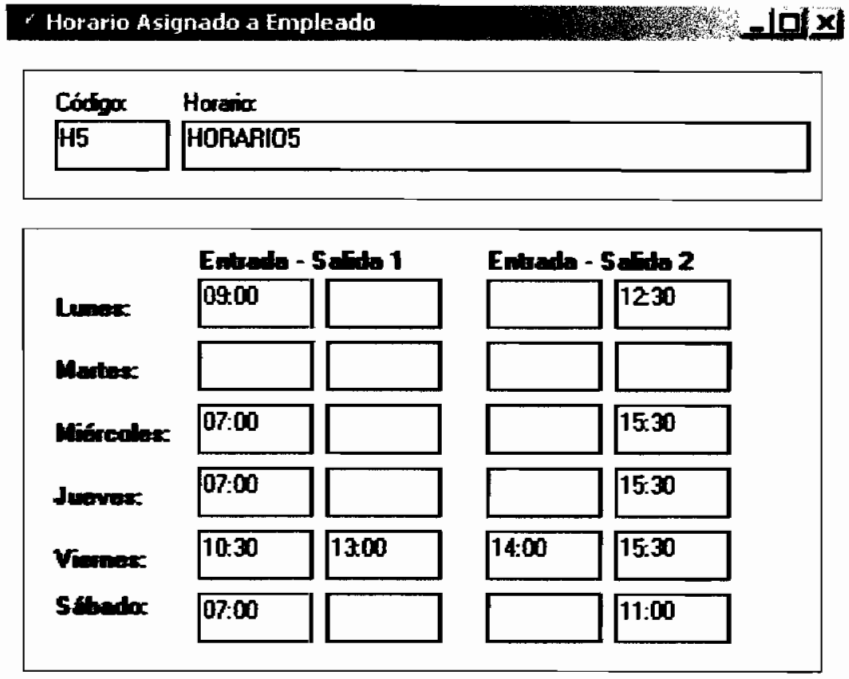
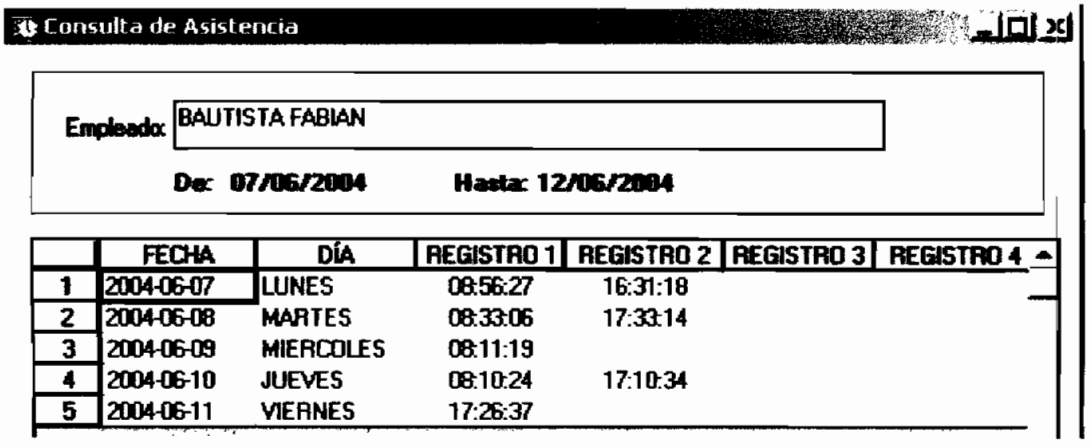


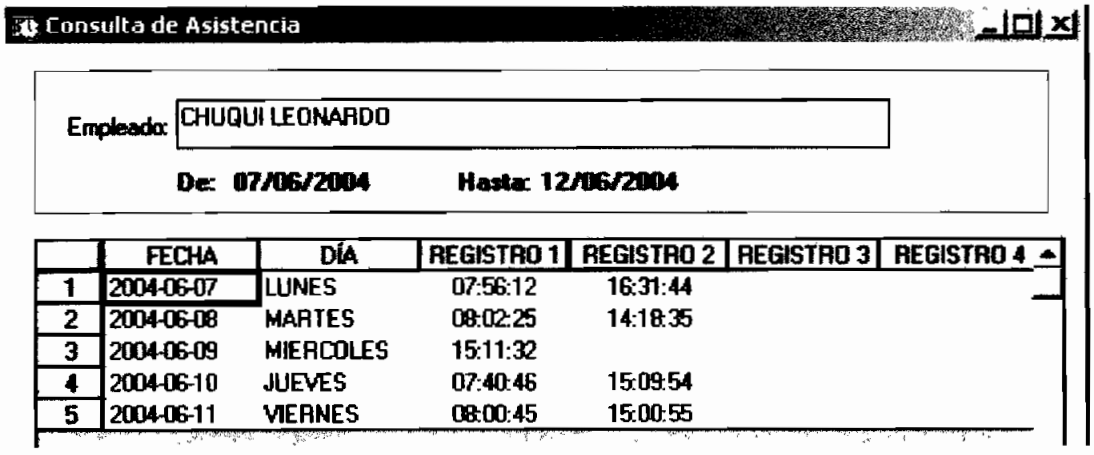
Figura 3.37: Horario asignado al empleado XAVIER ZURITA.

La evaluación duró una semana, aunque para este caso se pudo realizar la misma en menos de hora adelantando el reloj del sistema, los efectos son los mismos ya que el SCA trabajará con la fecha y hora del equipo Servidor. La asistencia de cada empleado se muestra en las figuras 3.38 a 3.42; en ellas se puede apreciar la mayor cantidad de casos que puede ocurrir cuando el SCA sea implementado en la EPN.



	FECHA	DÍA	REGISTRO 1	REGISTRO 2	REGISTRO 3	REGISTRO 4
1	2004-06-07	LUNES	08:56:27	16:31:18		
2	2004-06-08	MARTES	08:33:06	17:33:14		
3	2004-06-09	MIERCOLES	08:11:19			
4	2004-06-10	JUEVES	08:10:24	17:10:34		
5	2004-06-11	VIERNES	17:26:37			

Figura 3.38: Asistencia del empleado FABIAN BAUTISTA.



	FECHA	DÍA	REGISTRO 1	REGISTRO 2	REGISTRO 3	REGISTRO 4
1	2004-06-07	LUNES	07:56:12	16:31:44		
2	2004-06-08	MARTES	08:02:25	14:18:35		
3	2004-06-09	MIERCOLES	15:11:32			
4	2004-06-10	JUEVES	07:40:46	15:09:54		
5	2004-06-11	VIERNES	08:00:45	15:00:55		

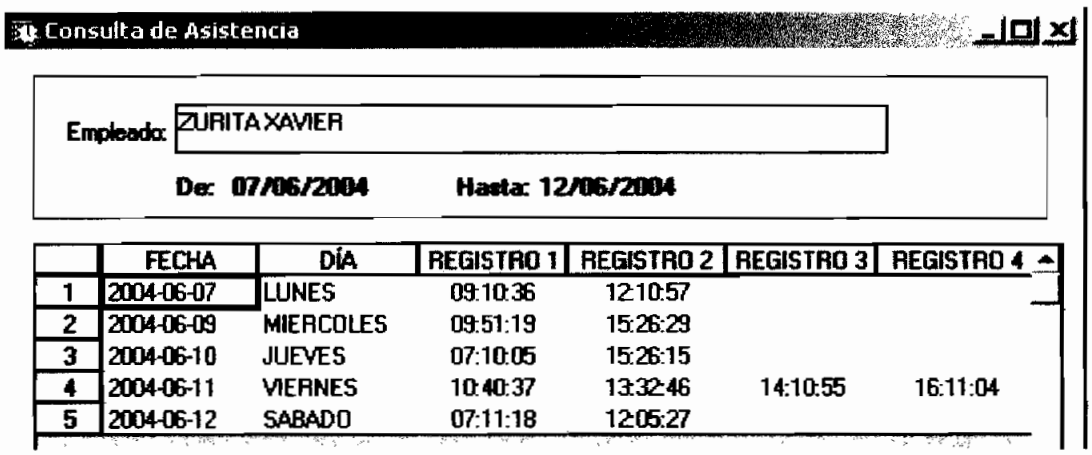
Figura 3.39: Asistencia del empleado LEONARDO CHUQUI.

	FECHA	DÍA	REGISTRO 1	REGISTRO 2	REGISTRO 3	REGISTRO 4
1	2004-06-07	LUNES	06:38:40	13:11:12	13:30:34	16:31:27
2	2004-06-08	MARTES	07:06:03	12:06:32	12:56:42	16:32:52
3	2004-06-09	MIERCOLES	07:00:47	12:50:56	16:51:07	
4	2004-06-10	JUEVES	06:56:56	12:10:03	16:10:12	

Figura 3.40: Asistencia del empleado FERNANDO IBARRA.

	FECHA	DÍA	REGISTRO 1	REGISTRO 2	REGISTRO 3	REGISTRO 4
1	2004-06-07	LUNES	07:38:58	13:30:53	16:31:35	
2	2004-06-08	MARTES	08:49:51	17:50:00		
3	2004-06-11	VIERNES	08:40:10	15:40:26		

Figura 3.41: Asistencia de la empleada ADRIANA MOLINA.



	FECHA	DÍA	REGISTRO 1	REGISTRO 2	REGISTRO 3	REGISTRO 4
1	2004-06-07	LUNES	09:10:36	12:10:57		
2	2004-06-09	MIERCOLES	09:51:19	15:26:29		
3	2004-06-10	JUEVES	07:10:05	15:26:15		
4	2004-06-11	VIERNES	10:40:37	13:32:46	14:10:55	16:11:04
5	2004-06-12	SABADO	07:11:18	12:05:27		

Figura 3.42: Asistencia del empleado XAVIER ZURITA.

Luego que se realizó la actualización del Registro se obtuvo el siguiente reporte de minutos atrasados, resultado esperado según los horarios y asistencias de cada empleado (ver figura 3.43).

ESCUELA POLITÉCNICA NACIONAL

SISTEMA DE CONTROL DE ASISTENCIA

REPORTE DE ASISTENCIA

De 07/06/2004 a 12/06/2004

Codigo	Nombre	MinAtrasados	MinJustificados	Total
EPN3	BAUTISTA FABIAN	1078	0	1078
EPN2	CHUQUI LEONARDO	464	0	464
EPN1	IBARRA FERNANDO	1056	0	1056
EPN4	MOLINA ADRIANA	409	0	409
EPN5	ZURITA XAVIER	250	0	250

Figura 3.43: Reporte de minutos atrasados.

Durante el desarrollo de la aplicación también se realizó varias pruebas referentes a: justificaciones, vacaciones, ingreso de datos del empleado, ingreso de horarios, reportes y consultas; obteniendo resultados favorables.

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Para los sistemas informáticos es muy difícil conseguir un sistema totalmente seguro, según la mayoría de expertos es imposible, por eso se "suaviza" la definición de seguridad y se pasa a hablar de fiabilidad que es la probabilidad de que un sistema se comporte tal cual se espera de él, y por tanto se habla de sistemas fiables en lugar de sistemas seguros.

- Mantener un sistema fiable consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

- Las políticas de seguridad son los mecanismos utilizados para implementar seguridad en cualquier sistema, sea informático o no; las políticas son una herramienta básica para garantizar la protección incluso de la propia red. Define responsabilidades y reglas a seguir para evitar amenazas o minimizar sus efectos en caso de que se produzcan.

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

- Un identificador biométrico debe cumplir los siguientes requerimientos: Universalidad, Unicidad, Permanencia, y Cuantificación

- El alcance de las aplicaciones biométricas cubre no solamente a los especialistas en computación y seguridad, sino también a los propios gerentes de negocios y administradores que deben conocer las nuevas

tecnologías para así tomar decisiones relacionadas con la seguridad de sus empresas.

- La Autenticación Biométrica por sí sola no puede resolver todas las necesidades de autentificación y seguridad, sino que se le ha de considerar como una herramienta más: "La Biometría no es un elemento aislado, su eficacia depende del entorno". Se debe entender a la seguridad biométrica como un elemento complementario en un entorno seguro que añade un nivel más de seguridad al sistema.

- En general, todos los sistemas biométricos se basan en un proceso que se inicia con el suministro de una muestra de la característica física o de comportamiento por parte del usuario; a partir de la información capturada se conforma una representación digital que involucra los atributos correspondientes a un modelo matemático. Esta información que se guarda encriptada, constituye el **perfil o plantilla**.

- La fase de correspondencia es el proceso por el cual un Sistema Biométrico busca similitudes entre la muestra obtenida en vivo y la respectiva plantilla. Para buscar correspondencias se pueden utilizar dos procesos distintos: la identificación o reconocimiento (1:N) y la autenticación o verificación (1:1).

- Un Sistema Biométrico se evalúa mediante las tasas de *aceptaciones equivocadas* y *rechazos equivocados*. Las primeras se refieren a permitir el acceso a la persona indebida, mientras que los segundos dan cuenta de los no reconocimientos de usuarios legítimos.

- Los productos biométricos en general pueden hacerse más seguros si se los vuelve más "estrictos" en sus comparaciones con el perfil almacenado, pero al mismo tiempo que se gana bajando la tasa o porcentaje de aceptaciones equivocadas, también subirá la tasa de rechazos equivocados; además un aumento de la sensibilidad del sistema lleva a tener mayor procesamiento y retardo en el reconocimiento.

- Un Sistema Biométrico tiene tres tipos de tareas: la inscripción, la identificación y la verificación. Todas estas tareas necesitan una imagen de entrada y todas se cumplen vía *software*; de ahí que ésta es la parte más compleja de un diseño biométrico.

- Las técnicas biométricas más importantes y difundidas que se usan en la actualidad son: huellas dactilares, forma de la cara, geometría de la mano, reconocimiento de iris y retina, patrón de voz y reconocimiento de firma.

- Los sistemas biométricos basados en características oculares generalmente son los que ofrecen mayor seguridad gracias a la unicidad de los patrones individuales y la calidad de los dispositivos de captura, pero a la vez son los más costosos del mercado. Tienen la ventaja que una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano.

- La mayoría de los Sistemas de reconocimiento de huellas dactilares, se hallan englobados dentro de los sistemas AFIS (Sistemas de Identificación Automática de Huellas Dactilares), constituyendo un elemento indispensable dentro de las investigaciones policiales.

- La extracción de características de la huella dactilar basada en minucias supera a la basada en patrones en : tamaño de plantilla, sensibilidad a los cambios, seguridad y almacenamiento, siendo ésta la razón principal por la cual la mayoría de fabricantes de dispositivos y *software finger-scan* utilizan la extracción de características basada en minucias.

- La principal desventaja del Sistema Biométrico basado en el reconocimiento de la huella dactilar es la asociación con usos forenses y criminalíticos.

- Una de los motivos por el cual las tecnologías biométricas no se han difundido masivamente, es la falta de un estándar de programación así

como la dificultad de integración de estos sistemas con los sistemas de seguridad existentes en las empresas.

- La mayoría de empresas, públicas y privadas utilizan controles de asistencia basados en sistemas electromecánicos los cuales no cumplen labores de verificación o autenticación; esto es un problema cuando los empleados dejan de lado sus responsabilidades y se dedican a engañar al sistema haciendo que otros compañeros o personas ajenas a la Institución registren su asistencia. El SCA se basará en principio de identificación y autenticación biométrica basada en la huella dactilar desechando toda posibilidad de un registro falso de asistencia.

- El Sistema de Control de Asistencia (SCA) de los empleados de la Escuela Politécnica Nacional es una política laboral que beneficia tanto a la Institución como al empleado ya que evita favoritismos y exige al empleado a ingresar y salir de su puesto de trabajo a las horas señaladas en su jornada, convirtiéndose en un beneficio para las personas que ocupan el servicio de ellos.

- El SCA al utilizar el identificador biométrico de la huella dactilar hace uso de la característica principal de la seguridad biométrica que es su intransferibilidad, es decir que ningún individuo puede suplantar la identidad de otra persona, de esta manera la posibilidad de que una persona de registrando la asistencia de otro individuo es casi nula.

- El SCA es una herramienta de gran ayuda para la Dirección de Recursos Humanos, permitirá un control más exhaustivo de la asistencia de cada empleado así como también mantener información valiosa sobre la responsabilidad de cada uno de ellos.

- Los sistemas biométricos incluyen *hardware* y *software*, por lo que el SCA al basarse en este tipo de sistemas está formado por estos dos componentes: el primero es el encargado de capturar las características de la huella dactilar, mientras que el segundo componente, el *software*, interpreta y elabora los datos resultantes para luego compararlos con el perfil existente para así determinar su aceptación o rechazo en el registro de asistencia.

- Debido a que en la Institución se hace investigación, deja abierta la posibilidad de que el SCA se actualice en el futuro con otras técnicas de autenticación biométricas o incluso se implemente una autenticación fuerte de huella y tarjeta de identificación.

- La principal desventaja del SCA es la dependencia de otros sistemas operativos como lo es *Windows Server* 2000 y *Biologon* 3.0, si uno de éstos sistemas deja de operar correctamente, el SCA deja de funcionar.

- Vulnerar al SCA implementado en la Institución no es tarea fácil pero tampoco imposible, usando técnicas domésticas como la del "*Super Glue*" estudiada en este proyecto se podría engañar al lector de huellas dactilares, pero esto dependería más de la habilidad, experiencia y herramientas del falsificador, esto representa tiempo y dinero, factores que sí influyen en un empleado de la Institución, y además puede quedar al descubierto y ser sancionado por dicha falta.

- Uno de los mayores beneficios del SCA es la interacción de las personas con este tipo de sistemas biométricos, de tal manera que se adiestran con la utilización de un interfaz biométrico facilitando para un futuro la implementación de estos sistemas en cualquier otra área de la Institución.

- La tecnología biométrica avanza a pasos agigantados y no solo ayuda a la seguridad lógica sino también a la seguridad física, puede ayudar a disminuir el alto índice de robos de autos y hogares, así como también ayudar a discapacitados a ejecutar tareas que para ellos sea imposible de

realizar, en ese entorno todos tenemos la responsabilidad de involucrarnos con estas técnicas que ayudan en nuestras labores.

4.2. RECOMENDACIONES

- Para que el SCA trabaje con eficiencia se debe extraer periódicamente toda la información de la Base de Datos del sistema y guardarla como respaldos, de esa manera todos los procesos de evaluación de asistencia y registro se ejecutarán con mayor rapidez.

- Se debe implementar seguridades físicas en los terminales, ya que cualquier empleado o persona ajena puede hurtar el equipo o parte de él y dejar el sistema sin funcionamiento.

- El SCA trabaja como un módulo independiente de *Biologon* 3.0 lo cual permite implementar otro tipo de autenticación o a la vez una autenticación fuerte, la administración de la asistencia de los empleados de la EPN no se afectará en lo absoluto.

- El costo de las licencias del Biologon 3.0 hacen que el sistema se encarezca, lo cual sugiere la utilización del SDK de Biologon que es un paquete de menor costo y con mayor flexibilidad de implementación; además éste se podría utilizar en otros proyectos que involucren el factor seguridad.

- La principal debilidad del SCA es la configuración de la hora y fecha, tanto del Servidor como del Terminal, se debe en lo posible tratar que ésta permanezca inalterable desde el momento en que empiece a trabajar el sistema ya que su cambio podría causar daños irrecuperables a la información del SCA.

BIBLIOGRAFÍA

[1] COBB, Stephen; **Manual de Seguridad para PC y Redes Locales**; Primera edición; Mc Graw Hill; España; 1994.

[2] D. MALTONI; D. MAIO; A.K. JAIN; S. PRABHAKAR; **Handbook of Fingerprint Recognition**; Primera Edición; Springer Verlag; New York; 2003.

[3] FARLEY, Marc; STEARNS, Tom ; HSU, Jeffrey; **Guía LAN TIMES de seguridad e Integridad de datos**; Primera Edición; Osborne/Mc Graw Hill; España; 1998.

[4] IDENTIX; **Manual del usuario de BioLogon 3.0**; Segunda Edición; Estados Unidos; 2002.

[5] NANAVATI, Samir; THIEME, Michel; NANAVATI, Raj; **Biometrics: Identity Verification in a Networked World A Wiley Tech Brief;** Primera Edición; John Wiley & Sons; Canadá; 2002.

[6] VILLALÓN HUERTA, Antonio; **Seguridad en UNIX y Redes**; Segunda Edición; 2002.

Referencias Electrónicas:

[7] http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5122/Libro.pdf.

[8] http://www.vialidad.cl/estandares/7Estandaresseguridad.pdf

[9] http://www.biometriaaplicada.com/que_es.html

[10] http://www.nrtec.com.mx/informacion.htm

[11] http://grupos.unican.es/genetica/Documentos/PRACTICA%204.doc

[12] http://www.delitosinformaticos.com/articulos/102485416026690.shtml

[13] http://www.eafit.edu.co/revista/107/montoya.pdf

[14] http://www.angelfire.com/la2/revistalanandwan

[15] http://sircbaleares.com/control/biometria.htm

[16] http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

[17] http://neutron.ing.ucv.ve/revistae/No6/Olguin%20Patricio/ SEN_BIOMETRICOS. html

[18] http://www.e-sistemas1.com/servicios/reconocimiento_facial/

[19] http://ww2.grn.es/merce/2002/biometrics.html

[20] http://www.terra.es/tecnologia/articulo/html/tec8347.htm]

[21] http://ja2003.unileon.es/SUBMISSIONS/viar/117.pdf

[22] http://inform.nu/Articles/Vol3/v3n1p01-07.pdf

[23] http://mail.udlap.mx/~tesis/msp/gutierrez_g_l/capitulo2.pdf

[24] http://www.neotec.com.pa/ComoPorque/handreader/tecnologia.htm

[25] http://ja2003.unileon.es/SUBMISSIONS/viar/85.pdf

[26] http://www.eurokiosks.org/whtpaperses_summit_biometrics.html

[27] http://www.insys.com.mx/biometria/lectores.htm

[28] http://venus.javeriana.edu.co/tgrado/2001-1/iris.PDF

[29] http://www.iriscan.com

[30] http://www.ct.upc.es/departaments/eel/JCEE/JCEE2001/PDFs%202000/13ESPINOSA.pdf

[31] http://eudoxo.fata.unam.mx/documents/cienciahoy/cienciaSeptiembre2003-2.pdf

[32] http://onin.com/fp/fphistory.html

[33] http://biometrics.cse.msu.edu/j2033.pdf

[34] http://proton.ucting.udg.mx/expodec/sep2000/memo/li03.pdf

[35] http://iie.fing.edu.uy/investigacion/grupos/gti/timag/trabajos/2003/huellas/html/node1.html.

[36] http://www.turismo.uma.es/turitec/turitec2002/actas/Microsoft%20Word%20-%207.MARAVAL.pdf

[37] http://www.tic.udc.es/scg/proyect/biomet1/proyecto-biometria.pdf

[38] http://www.ieee.org/organizations/eab/precollege/faraday/worksheets/02fr.pdf

[39] http://www.depi.itchihuahua.edu.mx/electro/electro2001/mem2001/articulos/dsp3.pdf

[40] http://www.neotec.com.pa/ComoPorque/biometricos/MinuciasvsPatrones.htm (Identix).

[41] http://www.c3.lanl.gov/~brislawn/FBI/FBI.html

[42] http://www.imesd.net/main.php?n_id=30102

[43] http://www.identix.com/products/pro_info_fprint_biotouch.html

[44] http://mat21.etsii.upm.es/ayudainf/aprendainf/VisualBasic6/vbasic60.pdf

[45] http://www.xlwebmasters.com/doc.php?op=sql

[46] http://www.sav.us.es/formaciononline/asignaturas/asigpid/apartados/textos/recursos/deteccionfacial03/doc.doc