UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ESPECIALIDADES EMPRESARIALES

TÉCNICO SUPERIOR ELECTRÓNICO EN COMPUTACIÓN

PRESENTACIÓN DEL TEMA DE TESIS DE GRADO

AULA INTELIGENTE CON SISTEMA BIOMÉTRICO DACTILAR

ELABORADO POR:

CARMEN LUCÓNG RIVAS

WILLIE MARTÍNEZ GUTIÉRREZ

2006-2007

TABLA DE CONTENIDO

TABLA DE GRÁFICOS

LM BIOMETRICS.A.

1. MISIÓN DE LA EMPRESA

La empresa ***"LM BIOMETRICS S.A."*** trabajará con eficiencia, ética y disciplina motivando y capacitando a nuestros colaboradores para cubrir todas las expectativas de nuestros clientes en la implementación de la tecnología biométrica dactilar que, como fin, tiene satisfacer la necesidad de control de asistencia de personal y alumnado a los centros educativos, para esto ha puesto a su disposición el producto de aula inteligente; es decir llevar un registro total de asistencias para luego obtener una información eficaz para efecto de roles de pago de los catedráticos e ingreso del alumnado.

2. VISIÓN DE LA EMPRESA

Mantener satisfechos a nuestros clientes en cuanto al producto que le ofrecemos conservando nuestra ética en el trabajo.

Facilitar la comunicación entre proveedores y la empresa, mediante la implementación de una intranet y extranet.

Poner a disposición de los clientes o los que aún no nos conocen, nuestra página web.

Nos hemos trazado un plazo de dos años para cumplir nuestra visión.

3. PLANTEAMIENTO DEL PROBLEMA

Te invitamos a que formes parte de nuestros primeros clientes en una de las empresas que pondrá la diferencia al brindar los servicios de implementación de aulas inteligente con sistemas biométricos dactilares, empresa que llevará a cabo las soluciones a los problemas que se suscitan en los centros educativos, escuelas institutos colegios y universidades especialmente laboratorios de computación., en el mercado encontramos que se implementan aulas automatizada de tal forma que si no tienen implementado tecnología en redes (cableado estructurado), su servicio se enfocará entonces en colocar en redes todas esas máquinas, colocar aplicaciones que se puedan compartir entre el alumnado para su pedagogía, un proyector , una video cámara y sorpresa! ya está su aula inteligente.

Nosotros abarcaremos más. Nos enfocaremos a lo inteligente de verdad, automatizado realmente, vamos a dejar las carpetas de asistencias a un lado, indirectamente se formará un ambiente agradable entre el aula y el alumno, se tendrá control de asistencias y sobre todo se alineará más la responsabilidad y puntualidad tanto para el profesor como para los estudiantes.

Aclaremos que en la implementación, empezaremos por realizarla con instituciones pequeñas, que necesitarán de este tipo de control pero que no tiene presupuesto para gastar de seis mil a diez mil dólares por aula.

Además que no podrán adquirir dispositivos caros para encendido/apagado de luces, PC, etc. Nuestra empresa se enfocará a este tipo de instituciones educativas con poco presupuesto ya que la gran parte de lo que vamos a implementar son diseños (controlador On/Off) y software (sistemas de interfaz del scanner dactilar) ni comerciales, ni industriales sino para realizar tareas específicas a pequeña escala.

4. JUSTIFICACIÓN DEL TEMA

La idea de implementar una aula inteligente con sistema biométrico dactilar y un controlador de encendido y apagado de equipos de computación, surgió puesto que en el mercado ofrecen automatizar una casa, lo que conocemos como Domótica y que es de muy alto costo por los cuales no podemos acceder fácilmente. Podríamos decir que según un pequeñísimo estudio de mercado realizado a un grupo de personas, nos daríamos cuenta que la gente de clase social media prefiere lo antiguo a gastar grandes cantidades de dinero. Pero ese no es nuestro punto; nos preguntamos ¿Por qué no, un aula inteligente, un aula automatizada? No nos conformemos con las máquinas en red. La tecnología es tan variada en este tiempo que sería un desperdicio no hacer que abarque más situaciones o lugares, facilitando así la interacción del hombre con la computadora.

Es hora de que toda ésta tecnología, este al alcance de la clase media, de instituciones educativas que manejan laboratorios de computación o aulas sencillas en las que por alguna u otra manera necesitan controlar el acceso a ésta e indirectamente obligar a su entrada a la hora que es, olvidémonos de las tarjetas de marcar, de entrada de estudiantes o trabajadores que no pertenecen a esa clase o área, implantemos la puntualidad que ya se está perdiendo, ya que no debe ser una obligación sino mas bien una virtud, nos han de preguntar ¿Por qué la puntualidad? Porque el sistema tendrá de manera configurable una flexibilidad de minutos de entrada y salida, éste tiempo dependerá de las políticas de la institución.

En realidad la tecnología ha cambiado durante y desde mucho tiempo atrás, lo que nosotros ofrecemos en realidad es un sistemas de acceso, por una parte el mismo que se controlaba mediante firmas, tarjetas y que con el tiempo, surgió lo que ahora conocemos como biometría, sin necesidad de que en alguna ocasión se olvide dicha identificación, porque no dirán que se les olvido la mano, ya que se olvida la cédula, el pasaporte, el carnet pero no el dedo. Con

este sistema no van a tener que revisar asistencia de alumnos y profesores ya que obligatoriamente para acceder a su clase tendrán que identificarse en el escaner dactilar, tanto alumno como maestro y brindándole detalles de aula, materia, hora de entrada/salida y duración de la clase, igual los alumnos tendrán tiempo para entrar según lo configurado por el sistema caso contrario tendrá que esperar a la hora siguiente, esto evitará interrupciones entre clases. Además desde donde se encuentre el servidor o el controlador de dispositivos, podremos acceder a encendido automático u apagado automático de los equipos que se encuentren conectados a él.

El proyecto puede ampliarse mediante cambios de dispositivos y programación, ya que puede ser utilizado a nivel masivo, registrando las entradas de personal de oficina, de obreros conserjes, en un parqueadero de vehículos, pero en este caso sólo va a ser implementado de manera educativa.

Cabe recalcar, que la empresa instalará y configurará los dispositivos que hemos detallado según lo establecido y cualquier cambio y requerimiento que se necesite por parte de la institución, se hará de manera adicional, así como su costo.

También es importante mencionar que al principio, como todo cambio, afectará según el área o institución en la que se implemente, por ende dependerá de el entorno en el que el sistema trabajará.

Con la administración de estos dispositivos usted podrá actuar sobre ellos desde sus propios pulsadores.

En la vida todo es costumbre, acostumbrémonos y aceptemos la idea de que este proyecto atraerá mejoras tanto en el área de control educativo como empresarial.

5. OBJETIVOS DEL ESTUDIO

5.1. OBJETIVO GENERAL

Asociar conocimientos adquiridos en las diversas materias recibidas a lo largo de la Carrera, ofreciendo así un servicio excelente para que compita en el mercado. Prestando una ayuda al campo de control educativo y dando asesoría y poniendo a decisión de nuestros clientes, el uso de la tecnología que se ve a tan largo alcance en muchas instituciones educativas.

Integrar de tal manera a todo el entorno, para una buena organización, control, inspección y seguridad. La implementación de este sistema, dará como resultado que la persona encargada pueda realizar otras actividades que sean acorde a su área.

5.2. OBJETIVOS ESPECÍFICOS

5.2.1. Control de asistencias de alumnos

La implementación de esta aula inteligente permitirá que cuando el alumno se identifique para ingresar al aula, lo guarde en la base de datos como asistencia, siempre y cuando no se haya retirado antes de la primera hora, si fuese así le hará valer el tiempo que estuvo en clase haya sido continuo o intercalado. Estas configuraciones son por default; sí existe posibilidad a ser cambiadas.

5.2.2. Ayuda de administración a los jefes de piso

Ellos tendrán un login para el acceso a la configuración de encendido y apagado de equipos, si la clase necesita de la utilización de un televisor para mostrar algún video, este encendido se podrá configurar aquí. En cuanto a su tiempo de On/Off dependiendo de los requerimientos.

5.2.3. Control de horas dictadas por los maestros

Los profesores para ingresar a un aula obviarán la acción de recoger la carpeta ya que irán directamente al curso correspondiente, se identificarán con su huella dactilar. Y para ayuda del profesor este sistema podrá cruzar con la aplicación de pagos de sus horas para que haga el cálculo correspondiente.

5.2.4. Seguridad en cuanto al personal que ingrese

Como es un sistema de acceso ingresará solamente el personal registrado a la hora autorizada, quedando grabado en la base de datos el día y la hora que ingresó, ya que éste como todo sistema presentará opción de reportes y print.

5.2.5. Información de aulas y horarios

Las confusiones y atrasos que se presentaban los primeros días de clases cuando no hay pleno conocimiento ¿donde? y ¿en que aula?, es la clase, con esto será solucionado; ya que se podrá acercar a cualquier scanner biométrico y consultar si pertenece a esa aula, si es así, indicará mediante mensajes, en que aula toca recibir la clase.

Por tal razón es muy importante la completa organización; ya que esta configuración se la realizará previamente y estará sujeta a cambios en cualquier momento.

Cabe indicar que todo tiene opciones a realizar cambios, pero sólo la persona a cargo de este sistema en la institución educativa, decidirá si desea cambiar sus configuraciones, cada cierto tiempo, lo cual no recomendamos que se haga muy seguido, si no perderemos la línea de organización, para pasar por esos cambios muy continuos no va a valer de nada la organización del sistema, tengamos en claro que toda la implementación debe ayudar al personal, no darle problemas, si el caso se da, está siendo mal administrado.

6. METODOLOGÍA

La empresa se encargará de dar servicios de implementación, configuración y asesoría de ¿Cómo?, ¿Cuánto?, ¿Dónde? y que requisitos necesitará para tener en su institución un aula inteligente. Cuando el cliente nos pida información o asesoría por primera vez, será de manera gratuita. Nosotros visitaremos el lugar, haremos un estudio a nivel de instalaciones eléctricas y de cableado, con previo conocimiento de los requerimientos que nos hace el cliente. Si él desea el aula inteligente tal y como nosotros la instalamos sin cambios de software la instalación de los dispositivos y configuración de éstos tomará menos tiempo, pero en el caso de que en los requerimientos haya que hacer cambios completamente en el software necesitaremos más tiempo.

El tiempo que nos tardemos en dejar implementada el aula inteligente, dependerá del número y de los cambios que desee o necesite que se le haga al software por el cual trabajaremos por default. Necesitaremos conocer los dispositivos que desee conectar a la tarjeta controladora de equipos.

Necesitaremos también conocer un plano detallado de los puntos de corriente que existen en el lugar a implementarse.

Además necesitaremos saber si tiene o no un servidor disponible para el proyecto, esto también dependerá de la información que se tenga que manejar, si es poco y es una sola aula, le recomendaríamos que utilice uno que ya este siendo utilizado con alguna aplicación pequeña o una máquina destinarla para ello.

Daremos mantenimiento gratuito durante los primeros tres meses, luego si se presenta daño a nivel de software eso no cubrirá la garantía, los equipos instalados si. Se trabajará con el 50% de adelanto, el saldo cuando el aula este funcionando. Todo movimiento que se realice será respaldo con documentos sellados.

7. AULA INTELIGENTE CON SISTEMA BIOMÉTRICO

7.1. INTRODUCCIÓN

Las aulas inteligentes ya han sido implementada en países como Argentina, Brasil y entre otros, pero ¿Qué tienen estas aulas inteligentes? ¿Qué es un aula inteligente? *(ver anexo 1)*

7.1.1. Concepto de aula inteligente

Generalmente hablando y haciendo una analogía con el ser humano, es un sitio físico o virtualmente creado que mediante hardware y software simulan la participación de una o varias personas, haciendo así que sus aplicaciones sean aprovechadas a nivel empresarial, industrial, grandes y pequeñas empresas, y porque no aplicarla en las casas (ese concepto entra en otro tema denominado Domótica "casa inteligente"). Teniendo en cuenta ésta premisa, entonces un aula inteligente, en este caso de tesis, es un lugar físico que simula la participación de otros empleados, que ayuda en la mejor organización y control de efectividad.

En una aula común y corriente y ya con otra clase de tecnología que no es la biométrica, los profesores llegan a la institución recoge su carpeta, se dirige al curso correspondiente, llegan los estudiantes a la hora que se les da la gana, entran interrumpen la clase, el profesor es interrumpido, se pierde el hilo de la clase, así desencadenando una serie de eventos para algunos desagradables para otros no, pero estos eventos desagradables especialmente, ¿Le convienen a la institución? La respuesta es una sola *No,* con un sistema de Aula Inteligente se evitan muchas situaciones de estas.

Para nuestro proyecto de Tesis abarcaremos la tecnología biométrica como principal contenido para la asesoría de Aula Inteligente con sistema biométrico.

Hoy en día, los sistemas de autentificación convencionales, no dan abastos para la creciente demanda de usuarios. De ahí la necesidad por implementar sistemas que empleen la biometría

como método de autentificación y/o identificación. Cuando se habla de autentificación, se alude a un sistema en que el usuario anuncia su identidad y el mecanismo comprueba la veracidad de ésta. Cuando se refiere a identificación, es un sistema capaz de indicar de qué usuario se trata con sólo alguno de sus datos biométricos. Los datos biométricos de un individuo son aquellos rasgos físicos innatos que lo hacen único y permiten una eficiente identificación.

7.2. CARACTERÍSTICAS

Se caracteriza por ser un sistema rápido, confiable, y que va a eliminar errores finales en las actas de asistencias evitando así problemas futuros entre alumnos y maestros, dejando un registro claro, con la posibilidad de ser revisado y confiando en que no habrá el error humano, desapareciendo los contratiempos, la puntualidad de alumnos y maestros, será necesaria para dar comienzo a la hora, lo que dará mayor fluidez a la clase y se cumplirá con la duración exacta de la misma.

7.3. FUNCIONALIDAD

La funcionalidad se va a ver presente cuando el director de la carrera con un clic entre al sistema e identifique de manera rápidas mediante la base de datos implementada la asistencia del profesor y el tema dictado, el alumno podrá adquirir mas importancia por las asistencias a clases ya que el ingreso será registrado también mediante su huella dactilar.

El sistema indicará las salidas y entradas de cada alumno al aula para evitar falsas entradas. Entre otras funcionalidades como arranque/parada remota de equipos, control de accesos, etc.

7.4. REQUISITOS

Se lo podrá utilizar con un servidor compartido; ya que no son muchos los profesores y el alumnado, si es factible de manejar mediante una potente máquina sin necesidad de ser especialmente un servidor dedicado.

Lo que se recomendaría hasta como plan de contingencia es tener instalado otro disco duro para seguridad, poderlo configurar como espejo de capacidad menor o igual al principal para evitar algún desastre en perdida de información. Que el aula tenga una buena instalación eléctrica y con algunos puntos de entrada de 120v -220v reguladas para hacer posible la conexión de los dispositivos esenciales que integrarán el Aula Inteligente.

7.5. VENTAJAS

El implementar un aula inteligente como es nuestro objetivo ofrecer, ahorrará tiempo; ya que el ingreso manual de asistencias en carpetas se obviará, además controlará las horas y clases dictadas por el profesor y éstas mediante la base de datos se podrán relacionar con la del control de pagos y evitará equivocaciones a la hora de contabilizar el total de horas de cada profesor. Todo esto es lo que el sistema llevará de manera automática mostrando su huella dactilar, de igual manera para los estudiantes.

8. LA BIOMETRÍA

8.1. ¿QUÉ ES LA BIOMETRÍA?

Históricamente la biometría se ha utilizado ya desde tiempo con tarjetas inteligentes como forma de identificación personal, las llaves, señal de entrada para algún sitio, todos se pretenden ser únicos y se emplean para verificar la actividad de su portador. Aunque dichos instrumento de utilización suelen se violados debidos a su facilidad de ser copiados. Todos estos inconvenientes pueden ser solucionados con el uso de la *biometría* ya que el ser humano por el momento no ha sido clonado de forma verídica; ya que no ha sido aprobada su acción y para cuando llegue esto los sistemas de biometría también serán mejorados.

Entonces:

La Biometría se define como la identificación automatizada de una persona viva, basada en las características fisiológicas o de comportamiento. Hay muchos tipos de tecnologías biométricas en el mercado que procesan las siguientes variables: reconocimiento de rostro, huellas dactilares, geometría manual, sistema venoso de la retina, iris y reconocimiento de firma y voz.

8.2. FUNCIONAMIENTO

Los sistemas biométricos se componen de un hardware y un software; el primero captura la característica concreta del individuo y el segundo interpreta la información y determina su aceptabilidad o rechazo, todo en función de los datos que han sido almacenados por medio de un registro inicial de la característica biométrica que mida el dispositivo en cuestión. Ese registro inicial o toma de muestra es lo que determina la eficacia del sistema. En el caso de las huellas dactilares, un usuario coloca el dedo en un sensor que hace la lectura digital de su huella, después, el programa guardará la información como un modelo; la próxima vez que ese

usuario intente acceder al sistema deberá repetir la operación y el software verificará que los datos correspondan con el modelo. El mismo principio rige para la identificación por el iris/retina, con ayuda de videocámara, el rostro, la mano completa, etc. Las tasas de exactitud en la verificación dependen en gran medida de dos factores: el cambio que se puede producir en las personas, debido a accidentes o a envejecimiento, y las condiciones ambientales, como humedad en el aire, suciedad y sudor, en especial en la lectura que implique el uso de las manos.

En cuanto a qué partes del cuerpo son las más adecuadas para su utilización en identificación biométrica, aunque en principio cualquiera sería susceptible de ser usada, para su elección se atiende a criterios prácticos concretos. Lo ideal es que se trate de una característica física robusta, es decir, no sujeta a grandes cambios; que sea lo más distintiva posible en relación con el resto de la población, que sea una zona accesible, disponible y, por supuesto, aceptable por el usuario que, en ocasiones, puede llegar a percibir algunos dispositivos biométricos como excesivamente intrusivos.

Por último, hay que hacer una distinción entre aquellos dispositivos que miden el comportamiento y los que miden una característica fisiológica. Entre los primeros se encuentran el análisis de la dinámica de la firma y el del golpe en el teclado; los segundos incluyen la huella dactilar, la geometría de la mano y el dedo, la termografía facial y la exploración del iris o la retina. El reconocimiento de la voz es un parámetro biométrico basado en ambos análisis, el fisiológico que determina la zona vocal y el de comportamiento del lenguaje y las palabras usadas. Evidentemente aquellos dispositivos que se basen en el comportamiento requieren de la cooperación del usuario, mientras que se puede identificar fisiológicamente a cualquiera sin su cooperación e incluso sin su conocimiento, como en el caso de la imagen captada por una videocámara.

8.3. MÉTODOS DE IDENTIFICACIÓN BIOMÉTRICA vs. MÉTODOS CLÁSICOS DE IDENTIFICACIÓN

A pesar de la importancia de la criptología en cualquiera de los sistemas de identificación de usuarios vistos, existen otra clase de sistemas en los que no se aplica esta ciencia, o al menos su aplicación es secundaria. Es más, actualmente estos son los sistemas que se están imponiendo en la mayoría de situaciones en las que se haga necesario autenticar un usuario: "son más amigables".

Las principales razones por la que no se han impuesto en su totalidad son por la falta de conocimiento de la gente, piensan en su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento. Todo sistema dependiendo de lo que implique su daño tiene un grado de dificultad menor o mayor.

Los métodos de identificación biométrica se prefieren a los métodos clásicos de identificación por varias razones:

- *Es necesaria la presencia física del individuo que va a ser identificado.*
- *Con la identificación basada en técnicas biométricas no es necesario recordar*

Una contraseña o llevar una tarjeta de identificación.

La revolución en la tecnología de la información ha producido un rápido incremento en el uso de PINS y contraseñas. Por esto es necesario restringir el acceso a datos personales.

Para conocimiento general acerca de con que partes del cuerpo podemos hacer nosotros un reconocimiento biométrico, presentamos a continuación una lista de opciones:

8.4. COMPARACIÓN DE MÉTODOS BIOMÉTRICOS

	Ojo - Iris	**Ojo - Retina**	**Huellas dactilares**	**Geometría de la mano**	**Escritura – Firma**	**Voz**
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos

Aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y mesurable del individuo (esto incluye desde la forma de teclear ante un ordenador hasta los patrones de ciertas venas, pasando por el olor corporal), tradicionalmente ha estado basada en cinco grandes grupos.

Los dispositivos biométricos tienen tres partes principales; por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar. Además disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos (que son considerados válidos), y también ofrecen una interfaz para las aplicaciones que los utilizan.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: captura o lectura de los datos que el usuario a validar presenta, extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar), comparación de tales características con las guardadas en una base de datos, y decisión de si el usuario es válido o no. Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo (False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechazo a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

8.5. TIPOS DE MÉTODOS BIOMÉTRICOS

Cada sistema biométrico utiliza una cierta clase de interfaz, un sensor o mecanismo de captura determinado y un software específico. La identificación por geometría de la mano o huellas digitales, la más extendida, crea una imagen digital tridimensional, que es capturada, calibrada y guardada en un archivo. Para la identificación por el ojo existen dos sistemas: topografía del iris, identificando en pocos segundos más de 4.000 puntos, y topografía de la retina, midiendo con luz infrarroja de baja intensidad 320 puntos predefinidos en el diagrama de las venas.

El reconocimiento facial compara las características faciales con una imagen previamente escaneada, lo mismo que la identificación por voz con un patrón pregrabado, que analiza la presión del aire y las vibraciones sobre la laringe. La identificación por firma mide el tiempo, la presión, la velocidad, el ángulo de colocación del lápiz y la velocidad de las curvas, todo a través de un lápiz óptico con el que la persona firma en un soporte específico o pad. Por último, los sensores de olor, aún en desarrollo, utilizan un proceso químico similar al que se produce entre la nariz y el cerebro, sin que los perfumes sean capaces de enmascarar el olor particular de cada uno.

La identificación biométrica experimenta una aceptación creciente debido a la reducción de los costos de los dispositivos y a su alta confiabilidad. Por ello, no se restringe su uso a aplicaciones de alta seguridad, como bancos e instalaciones gubernamentales, sino que también se extiende a las empresas, para el control de clientes y empleados y en el acceso a oficinas y plantas comerciales e industriales. Aunque la lista sería interminable, algunas de las aplicaciones de la identificación mediante sistemas biométricos serían los servicios públicos, servicios policiales, penitenciarios, instituciones de salud, permisos de conducir, inmigración,

registro de armas, controles de acceso, tiempo y asistencia, seguridad de redes informáticas, comercio electrónico, educación, etc.

8.5.1. Verificación de huellas

Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Por tanto, parece obvio que las huellas se convertirían antes o después en un modelo de autenticación biométrico, desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales, y el uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica.

Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta). Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí sino que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 o 40 de éstas. Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, denegándosele obviamente en caso contrario. *(Ver anexo 2)*

Los sistemas basados en reconocimiento de huellas son relativamente baratos (en comparación con otros biométricos, como los basados en patrones retinales) sin embargo, tienen en su

contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en cuenta contra estos sistemas es psicológico, no técnico: hemos dicho en la introducción que un sistema de autenticación de usuarios ha de ser aceptable por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso.

La identificación por huella dactilar se puede dividir en dos grandes grupos:

- *Específica- basada en los puntos de discontinuidad de terminaciones bifurcaciones, denominados puntos de minucia.*
- *General- aproximación macroscópica. Se tienen en consideración el sentido de las Crestas pupilares, por ejemplo arcos, curvas y espirales.*

Podemos decir que la identificación dactilar es muy precisa ya que el índice de error es muy bajo. El precio de estos sistemas comparados con otros sistemas biométricos es muy bajo y su aceptación por el usuario muy alta. La base del éxito de este sistema es su aplicación en diferentes campos. Es una tecnología comprobada y su capacidad de registrar la diversidad de huellas aumenta su exactitud y flexibilidad drásticamente. *(Ver anexo 3)*

Técnicas de reconocimiento de huellas

Entre todas las técnicas biométricas, la identificación basada en las huellas dactilares es el método más viejo, el cual ha sido usado en numerosas aplicaciones. Una huella esta formada por una serie de crestas y surcos localizados en la superficie del dedo. La singularidad de una huella puede ser determinada por dos tipos de patrones: el patrón de crestas y surcos, así como el de detalles.

Existen dos técnicas para realizar la verificación de las huellas:

1. Basada en Detalles: Esta técnica elabora un mapa con la ubicación relativa de "detalles" sobre la huella, los cuales permiten ubicar con certeza a un individuo. Sin embargo, existen algunas dificultades cuando se utiliza está aproximación. Es muy difícil ubicar los detalles con precisión cuando la huella suministrada es de baja calidad. También este método no toma en cuenta el patrón global de las crestas y los surcos. Entre algunos detalles que podemos encontrar en una huella, tenemos: *(Ver anexo 4)*
2. Cada individuo posee uno y solo uno, arreglo de detalles.
3. El mismo puede ser descrito por un modelo de probabilidad:
4. Basadas en correlación: Este método viene a mejorar algunas dificultades presentadas por la aproximación creada por los el patrón de detalles, pero inclusive él mismo presenta sus propias fallas, está técnica requiere de la localización precisa de un punto de registro el cual se ve afectado por la rotación y traslación de la imagen.

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

- Anillo de Crestas.
- Lazo Derecho.
- Lazo Izquierdo.
- Arco.
- Arco de Carpa.

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

Dentro del proceso de reconocimiento es necesario emplear técnicas muy robustas que no se vean afectadas por algún ruido obtenido en la imagen además de incrementar la precisión en tiempo real. Un sistema comercial empleado para la identificación de huellas dactilares requiere de un muy bajo promedio de rechazos falsos (FRR)1 para un promedio de aceptación falso (FAR)2. Como por ejemplo:

Un dedo (FRR y FAR): 1:1000

- Dos Dedos (FRR y FAR): 1:1000000

El siguiente es un diagrama de bloques de un sistema utilizado para la verificación de huellas dactilares. En el mismo se describen en forma general las operaciones lógicas necesarias para llevar a cabo la identificación: *(Ver anexo 5)*

8.5.1.1. La Huella Genética Posteriormente

Además de los diversos proyectos de muchos países para la construcción de bases de datos de huellas digitales, para control de la inmigración, por ejemplo, en EE.UU. tienen planes para hacer lo mismo aplicado a la identificación de pacientes hospitalarios. Por otro lado, ya existe la tecnología para incorporar diminutos dispositivos de reconocimiento biométrico a objetos de uso cotidiano, tales como teléfonos móviles, ordenadores portátiles, teclados, tarjetas bancarias, armas de fuego, el volante del coche, etc.

Con toda seguridad, la tecnología también llegará a desarrollar un sistema de identificación automática por el ADN y, de hecho, la viabilidad de sistemas basados en el análisis del ADN es una de las líneas de investigación abiertas en la actualidad.

Por otro lado, muchos estados americanos ya disponen de la base legal para tomar muestras de ADN de los criminales convictos y el propio Departamento de Defensa estadounidense se propone crear un registro de ADN, un banco de datos, con millones de muestras de los miembros de las fuerzas armadas. De ahí a su extensión a la población en general tal vez haya un paso. Sólo faltaría el dispositivo capaz de reconocer en pocos segundos la estructura molecular de un individuo simplemente con tenerlo enfrente. Como toda nueva tecnología, la identificación biométrica plantea ventajas evidentes, pero también riesgos, muchas veces encubiertos, derivados de su mala utilización, como la invasión de la privacidad y el control y la vigilancia exhaustivos que permitiría ejercer sobre los ciudadanos, al más puro estilo orwelliano.

8.5.2. Verificación de voz.

En los sistemas de reconocimiento de voz no se intenta, como mucha gente piensa, reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

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, imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique. Como veremos, 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 extraídas de un conjunto bastante grande.

De cualquier forma, sea cual sea el modelo, 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...). Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

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, el del nombre de cada usuario, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autenticado y luego reproducir ese sonido para conseguir el acceso; casi la única solución consiste en utilizar otro sistema de autenticación junto al reconocimiento de voz.

Por contra, 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 habría de ser mucho mayor y la velocidad para localizar la parte del texto que el sistema propone habría de 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 hace variar el tono de

voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso ha de ser autorizado o no; incluso el estado anímico de una persona varía 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.*(Ver anexo 6*)

8.5.2.1. Sensores Para El Reconocimiento De Voz.

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

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

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

8.5.3. Verificación de escritura

Aunque la escritura (generalmente la firma) no es una característica estrictamente biométrica, como hemos comentado en la introducción se suele agrupar dentro de esta categoría; de la misma forma que sucedía en la verificación de la voz, el objetivo aquí no es interpretar o entender lo que el usuario escribe en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica. ***(Ver anexo 7)***

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que

habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas (por eso se les suele denominar *Dynamic Signature Verification*, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo...

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

Contra este problema la única solución (aparte de una concienciación de tales usuarios) es relajar las restricciones del sistema a la hora de *aprender* firmas, con lo que tiene deceso en su seguridad. Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

8.5.4. Verificación de patrones oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes o bien analizan patrones retinales, o bien analizan el 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. La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos por un lado, los usuarios *no se fían* de un haz de rayos analizando su ojo, y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas. Aunque los fabricantes de dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación, y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial (aparte del hecho de que la información es procesada vía *software*, lo que facilita introducir modificaciones sobre lo que nos han vendido para que un lector realice otras tareas de forma enmascarada). Por si esto fuera poco, se trata de sistemas demasiado caros para la mayoría de organizaciones y el proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevadas. De esta forma, su uso se ve reducido casi sólo a la identificación en sistemas de alta seguridad, como el control de acceso a instalaciones militares.

8.5.4.1. Retina

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. *(Ver anexo 8)*

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

infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

8.5.4.2. Iris

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo - de hasta 266 grados de libertad - , inalterable durante toda la vida de la persona. 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. La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 *KBytes*) suficiente para los propósitos de autenticación. Esa muestra, denominada *iriscode* es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos. ***(Ver anexo 9)***

Sensores Para Reconocimiento Del Iris.

En sistemas para el reconocimiento del iris es común encontrar cámaras de vídeo de tipo CCD. En la figura 9 se puede apreciar un diagrama de bloques de la cámara es un circuito integrado tipo CCD (Dispositivo de Carga Acoplada).

Este dispositivo consiste de varios cientos de miles de elementos individuales (píxeles) localizados en la superficie de un diminuto CI.

Cada píxel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la camera), almacenando una pequeña carga de electricidad. Los píxeles se encuentran dispuestos en forma de malla con registros de transferencia horizontales y verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). Esta transferencia de señales ocurre 6 veces por segundo.

En la, podemos apreciar un arreglo comercial de este tipo de CI. En el campo de procesamiento de imágenes, este integrado ha revolucionado todo lo establecido, siendo el componente principal de las llamadas Cámaras Fotográficas Digitales.

8.6. SENSORES UTILIZADOS EN TECNOLOGÍA BIOMÉTRICA DACTILAR

Citamos algunos, pero entraremos en detalle con el que utilizaremos en mayor cantidad para nuestros servicios de la empresa:

Sensores termoeléctricos

Sensores Ópticos

Sensores Capacitivos

Sensores E-Field (de Campo Eléctrico)

Sensores sin contacto

Surface Pressure Sensor

8.6.1. Sensores Termoeléctricos

El método termoeléctrico es menos común. Por ejemplo el Fingerchip™ utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas *(slices)* y se pone en marcha un software especial que reconstruye la imagen del dedo. Este método permite al Fingerchip™, obtener una gran cualidad, 500 puntos por imagen impresa de la huella dactilar con 256 escalas de gris. El sensor mide la temperatura diferencial entre las crestas pupilares y el aire retenido en los surcos. Este método proporciona una imagen de gran cualidad incluso cuando las huellas dactilares presentan alguna anomalía como sequedad o desgaste con pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua.

Además, también cuenta con la ventaja de autolimpiador del sensor, con lo que se evitan las huellas latentes. Se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores sino que permite que se copie la huella para falsificarla y acceder así al sistema. De hecho, este método de arrastre que utiliza la tecnología basada en el calor hace que el Fingerchip esté por encima de otras tecnologías. El Fingerchip™ funciona con bajas temperaturas, alto porcentaje de humedad, etc. *(Ver anexo 10)*

Otra ventaja es la reproducción de una imagen grande de alta cualidad y siempre un sensor limpio. La desventaja es que la cualidad de la imagen depende un poco de la habilidad del

usuario que utiliza el escáner. La segunda desventaja es el calentamiento del sensor que aumenta el consumo de energía considerablemente.

Este calentamiento es necesario para evitar la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar. El elevado volumen de diseño del escáner permite que su precio sea bajo ya que en el proceso de manufacturación se necesita menos silicona.

8.6.2. Sensores E-Field (de Campo Eléctrico)

El sensor de campo eléctrico funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). La tecnología basada en los campos eléctricos afirma ser útil para cualquiera y poder trabajar bajo cualquier condición, por dura que ésta sea, del "mundo real", como por ejemplo piel húmeda, seca o dañada. *(Ver anexo 11)*

Esta tecnología origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Se utiliza un amplificador *under-píxel* para medir la señal. Los sensores reproducen una imagen clara que se corresponde con mucha exactitud a la huella dactilar y que es mucho más nítida que la producida por sensores ópticos o capacitivos. Esto permite a la tecnología de campo eléctrico la lectura de huellas que otras tecnologías no podrían. En la tecnología de campo eléctrico, la antena mide las características de la capa subcutánea de la piel generando y detectando campos lineales geométricos que se originan en la capa de células de la piel situada bajo la superficie de la misma. ***(Ver anexo 12)***

Esto contrasta con los campos geométricos esféricos o tubulares generados por el sensor capacitivo que sólo lee la superficie de la piel. Como resultado, huellas que con sensores capacitivos son casi imposibles de leer, se pueden reproducir con éxito por sensores de tecnología de campo eléctrico.

Una desventaja es la baja resolución de la imagen y el área pequeña de imagen lo que produce un índice de error alto (EER).

8.6.3. Sensores Capacitivos

El método capacitivo es uno de los más populares. Al igual que otros escáner, genera una imagen de las cresta y valles. En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos conductores cubiertos por una capa aislante. La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato***. (Ver anexo 13)***

La mayor ventaja es que se requiere una huella real pero se pueden presentar problemas si la yema del dedo está húmeda o muy seca. En este caso se obtendrán imágenes negras o pálidas.

Entre las empresas líderes en este sector se encuentran: Infineon, Verdicom, Sony y ST *Microelectronics.*

9. MÉTODOS A EMPLEARSE

Entre los métodos tenemos variedad pero vamos a considerar los siguientes:

9.1. MÉTODO FINGER-SCAN DE IDENTIFICACIÓN

9.1.1. Conocimientos a tener en cuenta para la interpretación de una huella en el sistema

Como conocimiento previo una *huella dactilar* es la representación morfológica superficial de la epidermis de un dedo. Posee un conjunto de líneas que se encuentran dispuestas en forma paralela (colinas o ridge lines y furrows). Sin embargo estas líneas se interceptan y a veces terminan en forma abrupta. Los puntos donde las colinas se abrupta se conocen como detalles.

Otros puntos singulares de una huela dactilar son aquellos donde la curvatura de la columna es máxima. Esos puntos recibe el nombre de centros y detalles. Las características mas interesantes que presentan tanto los puntos singulares centros y deltas son únicos para cada individuo y permanecen inalterados a través de su vida.

A pesar de esta variedad de detalles, las más importantes de 18 son las bifurcaciones y terminaciones de colinas. Esto se debe a que las terminaciones de colinas representan aproximadamente el 60.6% del porcentaje de todas las huella y las bifurcaciones el 17.9%.

Además varios de los detalles menos típicos pueden ser representados en función de las dos señales; ya que sumando estas dos dan un porcentaje mas delante de la cuarta parte la cual no llega al cien por ciento, pero con este porcentaje es factible el reconocimiento real de la huella sin tener la posibilidad que exista otra huella similar, el porcentaje faltante lo ocupan los 16 detalles restantes.

9.2. TRANSFORMADA DE HOUGH

Solución de interpretación que se utilizo para la interpretación en el sistema biométrico fue basada en Hough.

Consideremos que para una imagen de *n* puntos de interés se desea encontrar subconjuntos de esos puntos que residan sobre líneas complejas. Este problema que ha simple vista parece ser sencillo, presenta una complejidad computacional elevada a utilizar una técnica de fuerza bruta. Una de estas soluciones consiste en encintrar todas las líneas determinadas por cada par de puntos en la imagen y luego encontrar todos los subconjuntos de puntos que se encuentra cerca de estas líneas. La complejidad de este algoritmo es ***alta***, lo que representa un costo elevado.

Los detalles de esta transformación ya lo vemos en solución del sistema biométrico el cual esta implementado en Visual Basic 6.0, y esta basado en formulas matemáticas y coordenadas mediante detalles de máximo y mínimo pero en este caso como nuestra empresa va ha dar el servicio con este sistemas ya implementado, la programación en si es un poco abstracto, nosotros vamos a dar el servicio de instalación del dispositivo implementándolo ya en si y como producto final será el ***Aula Inteligente***.

9.3. TRANSFORMADA DE HOUGH GENERALIZADA

Generalizando la transformada que hace posible la interacción del scanner de huella digital con nosotros esta asociada a la creación de un método que permita el reconocimiento de formas geométricas mas complejas que la de una línea por ejemplo de una circunferencia y elipse. El procedimiento anterior se generaliza mejor con el objeto de encontrar transformaciones generales entre conjunto de puntos. Para tener una idea más amplia del tema tenemos luego de esta aclamación que hacer transformación de vectores (Query y Template).

Esta transformación debe considerar incluso que para dos vectores de características de una misma huella dactilar puede existir diferencia entre esas, como la desaparición de algunos detalles, la variación de la posición y orientación local de algunas de estas debido al ruido que introduce el sensor y las deformaciones elásticas que presenta la piel.

9.4. HERRAMIENTAS NECESARIAS DE SOFTWARE

9.4.1. Módulo de tratamiento de la huella

Almacenamiento de la huella: El formato de BITMAP de Windows se utiliza como formato de entrada de las imágenes (huellas), por su facilidad y compatibilidad en intercambiar imágenes entre aplicaciones. El origen de la BITMAP es indiferente (scanner, cámara, archivo).

Filtrado de la imagen:

Evaluación de la calidad de la huella

Adelgazamiento de la huella

Extracción de detalles

9.4.2. Módulo de comparación de huellas

Está basado en dos grupos de detalles, correspondientes a las dos huellas a comparar. Para determinar que estas dos imágenes diferentes pertenecen al mismo dedo del individuo, es necesario adoptar un sistema sensible, lo cual es posible que de una similitud a la misma. (*Ver anexo 14)*

9.4.3. Rendimiento

El objetivo de todo sistema de identificación es el establecer un método automático para determinar si la imagen de dos huellas son equivalentes o no.

9.4.4. Tasas de Error

Nos podemos encontrar con las siguientes después de la etapa de rendimiento:

Falsa aceptación

Falso Rechazo

Entre estas dos tenemos el 21.5% de error

9.4.5. Exactitud en la identificación: medidas de desempeño

La información provista por los templates permite particionar su base de datos de acuerdo a la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las “clases” así generadas permiten reducir el rango de búsqueda de algún témplate en la base de datos.

Sin embargo, los templates pertenecientes a una misma clase también presentarán diferencias conocidas como *variaciones intraclase*. Las variaciones intraclase implican que la identidad de una persona puede ser establecida sólo con un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue “personal autorizado” o “impostor”. Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

- Una persona autorizada es aceptada,
- Una persona autorizada es rechazada,
- Un impostor es rechazado,
- Un impostor es aceptado.

Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son. El grado de confidencia asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos tasas de errores [9]:

Tasa de falsa aceptación (*FAR*: False Acceptance Rate), que se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado,

Tasa de falso rechazo (*FRR*: False Rejection Rate), definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor.

La *FAR* y la *FRR* son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos. Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa, como muestra la . El grado de seguridad deseado se define mediante el umbral de aceptación u, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

9.5. ¿CÓMO FUNCIONA?

Cada usuario debe registrarse ya sea alumno o profesor mediante un procedimiento muy sencillo y rápido creándose una característica matemática de la huella digital, llamada patrón biométrico digital (témplate). Este patrón se almacena por cada uno de los usuarios en un servidor, para ser consultado y comparado cada vez que el usuario intente acceder al sistema protegido. (*Ver anexo 15)*

Durante la verificación que se produce ante la solicitud del acceso el usuario debe presentar su identificación en este caso la huella dactilar para ser comparada durante la almacenada en el proceso de registro, si esta registrada su huella debe coincidir con dicho patrón.

10. DISPOSITIVO A UTILIZAR PARA ESCANEO DE HUELLA

10.1. STAFF ON TIME PRO

Staff on time Pro es una solución de control de presencia y acceso, basada en tecnología biométrica que utiliza las huellas dactilares de los empleados en este proyecto serán estudiantes y alumnos para identificarlos, evitando así otros métodos como las cartulinas y las tarjetas de proximidad que permiten el uso indebido de éstos. Con Staff on time Pro además de controlar la presencia de los empleados se puede también controlar el acceso, a determinadas áreas de la empresa, siendo configurables distintos niveles de seguridad independientes por cada empleado. El software Staff on time está compuesto de dos módulos:

Staff on time Admin y Staff on time ID El módulo admin., es en el que se centra la gestión de las bases de datos de Staff on time. Podrá gestionar el organigrama de su empresa, horario, festivo, consultar diferentes tipos de listados, etc. El módulo ID recoge los fichajes de los empleados. Cada escaneo de la huella dactilar (cada fichaje) queda registrado en la base de datos Staff on time, la cual podrá consultar mediante el módulo Staff on time Admin.

También con Staff on time se incluye la aplicación Staff on time Info que le permite saber en tiempo real si cada trabajador está en la empresa, si ya se ha marchado o si ha salido a hacer alguna gestión u otro tipo de salida. (*Ver anexo 16)*

10.2. POSIBILIDADES DE CONFIGURACIÓN

Acceso

Presencia

Presencia y acceso (con un solo terminal).

10.3. CARACTERÍSTICAS

Hasta 360 empleados, configurable para múltiples compañías y departamentos, permite el registro de 2 huellas para cada empleado, asignación de diferentes tipos de permisos de acceso a áreas restringidas independientes por cada empleado:

Configurable para múltiples tipos de horarios, posibilidad de asignar festivos, impresión del calendario laboral por meses, listados de presencia y acceso.

Editables y configurables mediante filtros, listados de incidencias de presencia (fichajes sin completar, realizados…), listados de incidencias de acceso (acceso no permitido por permisos, acceso por usuario no registrado).

Listados de informes de presencia con: Comentario/salida especial, puntualidad en cada entrada y salida, horas trabajadas por día, medias de puntualidad (totales o por turno), media de horas trabajadas, total de horas trabajadas y por turno del periodo seleccionado, listado de informes de acceso con: área a la que se ha tenido acceso, fecha y hora.

Permisos de accesos al módulo admin. individualizados, disponible en: Español, Francés, Inglés, Italiano y Portugués, posibilidad de configurar salidas especiales por gestiones personales, salida al médico, salida comercial mediante fichajes con códigos especiales, exportación a formato CSV (formato estándar compatible con Excel, Access…) de empleados, fichajes y códigos especiales. Esta característica permite la integración de los datos obtenidos con Staff on time con otras aplicaciones o sistemas externos de gestión y/o control propios de cada empresa, puede operar con múltiples puntos de entrada/salida, facilidad de colocación de la huella que permite evitar errores tanto en el registro como en el uso habitual del dispositivo ofreciendo más libertad en la pulsación y colocación del dedo en el escáner dactilar, cuidado y resistente diseño del terminal que permite su colocación en pared o sobremesa.

10.4. REQUISITOS MÍNIMOS

PC compatible 586 o compatible, 128 MB de memoria RAM, lector de CD-ROM, puerto USB, puerto Serie RS-232, 20 MB de espacio libre en el disco duro, pantalla de 800x600 a 16 bits, Windows XP, 2000, Me o 98.

10.5. CONTENIDO.- PRECIO.- ¿POR QUÉ LA ELECCIÓN?

Software y manual (CD-ROM), Terminal dactilar con alimentador de corriente, peana de sobremesa para el terminal y guía de instalación rápida

Nombre	Precio	Garantía
Staff on time Pro,	$340	2 años

Se pudo haber escogido cualquier otro dispositivo de escaneo, el porqué de la elección del Time Pro es debido a que este soporta otro tipo de sistema u aplicación para trabajar en conjunto y así puede cumplir nuestras expectativas en cuanto a lo que deseamos ofrecer en servicios para que se diferencie de los demás compañías y dispositivos ya que añadiremos el dispositivo la aplicación expuesta desarrollada en Visual Basic 6.0 con una Base de Datos Realizada en Access. También con otra configuración podemos utilizar SQL.

11. DISPOSITIVO CONTROLADOR PARA ENCENDIDO/APAGADO INTELIGENTE DE EQUIPOS DE COMPUTACIÓN

Hay variedad de dispositivos en el mercado pero no hay mejor que la ampliación de un dispositivo construido en clases, que con ayuda de programación assembler y unos cuantos dispositivos añadidos se podrá utilizar para la funcionalidad de nuestro objetivo.

11.1. DESCRIPCIÓN DEL CONTROLADOR

El dispositivo electrónico es una interfaz que, conectada a la línea telefónica, es capaz de recibir y atender llamadas entrantes, con el fin de controlar uno o más artefactos conectados al mismo, desde un aparato telefónico remoto. El microcontrolador utilizado es un AT89S8252 fabricado por ATMEL. También fue necesario incorporar al circuito un conversor a binario y un controlador para comunicación serie RS-232, ambos genéricos.

11.2. FUNCIONES

Nuestro dispositivo es capaz de recibir e interpretar tonos a través de la línea telefónica, y posteriormente tomar determinadas acciones relacionadas con el control de otros dispositivos electrónicos (como podrían ser los electrodomésticos hogareños). Esto permite al usuario tener control en forma remota de determinados equipos, utilizando un aparato telefónico convencional, mediante el teclado del mismo, según el siguiente protocolo: Esperar *x* rings antes de atender el teléfono (configurable).

Una vez atendido el teléfono, solicitar una contraseña para dar el servicio a quien está llamando. Luego de validada la contraseña, se pasa al menú de opciones.

Se usarán casi todos los dígitos del teléfono (salvo 6, 7, # y *). En nuestro trabajo práctico pretendemos manejar 9 relés, aunque en principio se ha implementado uno solo (en el proyecto de tutoría grupal en la asignatura de materiales y circuitos), relacionando cada uno con cada dígito numeral del teclado. Una vez atendida la llamada, el menú de opciones es el siguiente:

(1)Encendido: Una vez marcada esta opción, el sistema queda a la espera de otro dígito (este segundo dígito ingresado indica el número de relé a encender).

(2) Apagado: Una vez marcada esta opción, el sistema queda a la espera de otro dígito (este segundo dígito ingresado indica el número de relé a apagar).

(3) Consulta: Una vez marcada esta opción, el sistema queda a la espera de otro dígito (este segundo dígito ingresado indica el número de relé a consultar). Si el relé está encendido, entonces se emite un beep largo a través de la línea telefónica, y si está apagado se emite un beep corto.

(4) Cambio de contraseña: Se utiliza para cambiar la contraseña de acceso. Una vez marcada esta opción, el sistema queda a la espera de los 4 dígitos para la nueva contraseña.

(*5) Cambio de la cantidad de rings de espera*: se utiliza para cambiar el parámetro que indica la cantidad de rings a esperar antes de atender la llamada entrante. Una vez marcada esta opción, el sistema queda a la espera de un dígito que indica la nueva cantidad de rings.

(*6-7) Disponibles.*

(8) Reinicio: El sistema se reinicia pero sin desbloquear al usuario. Esto es particularmente útil cuando el usuario, luego de seleccionar algunas opciones, no sabe en qué situación está.

(*9) Salir:* Corta la llamada.

11.3. GENERACIÓN DE LAS SEÑALES DE RESPUESTA

Luego de la selección de cualquiera de las opciones, el sistema emite un *beep largo* para indicar “si”. En algunos casos, el sistema emite un *beep corto* para indicar “no”; esto sucede cuando la contraseña ingresada es inválida, o para indicar que un relé se encuentra apagado. Ambos *beeps* se emiten por el pin 0 del puerto 1 (P1.0).

11.4. ADMINISTRACIÓN DE CONTRASEÑA Y DE RINGS

11.4.1. Administración de Contraseña

Antes de poder utilizar cualquiera de las opciones, el usuario deberá identificarse (es decir, ingresar la contraseña, y que ésta sea validada por el sistema). Una vez validada la contraseña, el sistema emite una melodía para indicar al usuario que ya puede comenzar a utilizar el dispositivo. La contraseña es única (no se permiten múltiples usuarios), y está compuesta de 4 caracteres alfanuméricos (0-9, # ó *). La primera vez que se utiliza el sistema, o cuando el sistema es reseteado externamente (a través de un pulsador al efecto), se espera el ingreso de la contraseña por defecto (1111). Posteriormente, el usuario puede modificarla mediante la opción 4.

11.4.2. Administración de la cantidad de rings de espera

El sistema espera una cierta cantidad de rings antes de atender la llamada (análogamente al funcionamiento de un contestador automático). Esa cantidad es configurable mediante la opción 5, aunque por defecto se toma el valor 3. Solo acepta un dígito, con lo cual se podrá configurar hasta 9 rings de espera.

11.5. INTERFAZ PC CON DISPOSITIVOS QUE INTERFIEREN

11.5.1. Interrupciones

Interrupción externa 0 (IE0).

Disparada cuando el circuito integrado conversor de DTMF a binario pone en alto el pin 12 (INT0) del microcontrolador, notificando la presencia de un dígito válido en sus 4 salidas.

Interrupción externa 1 (IE1).

Disparada por el circuito detector de rings, con cada detección efectuada.

Interrupción del puerto serie (RI/TI).

Disparada por software (TI) cuando se tiene un carácter para enviar por comunicación serie RS232, o por hardware (RI) cuando se ha recibido un carácter por la misma vía.

Interrupción del timer 0 (TF0).

Disparada por el timer 0 cuando transcurre una cantidad determinada de segundos sin que el usuario haya seleccionado alguna opción. Permite administrar un time-out, impidiendo que el programa quede en un bucle de espera infinito en caso de que se corte la comunicación telefónica sin un desbloqueo explícito con la opción 9.

11.5.2. Descripción de puertos

Puerto P1 (0): Salida de la señal. Por este pin el sistema emite la señal con diferentes duraciones para representar “si” o “no”.

(1): Encendido y apagado del relé. El sistema pone en alto este pin para encender el relé, o lo pone en bajo para apagarlo.

(2): Comunicación establecida. Cuando el sistema “atiende” la llamada entrante, pone en bajo este pin, y lo mantiene en ese nivel mientras dure la comunicación telefónica.

(3) – (7): No utilizados.

Puerto P2 (0): Entrada del bit 4 desde el conversor DTMF a binario.

(1): Entrada del bit 3 desde el conversor DTMF a binario.

(2): Entrada del bit 2 desde el conversor DTMF a binario.

(3): Entrada del bit 1 desde el conversor DTMF a binario.

(4) - (7): No utilizados.

Puerto P3 (0): Entrada de caracteres desde el controlador de comunicación serie (HIN232).

(1): Salida de caracteres hacia el controlador de comunicación serie (HIN232).

(2): Interrupción externa 0, disparada por el conversor DTMF a binario, cuando se ha recibido un carácter válido.

(3): Interrupción externa 1, disparada por el circuito detector de rings, cuando se recibe un ring por la línea telefónica.

(4) - (7): No utilizados.

11.6. LISTADO DE COMPONENTES

A continuación se detallan los componentes utilizados en la implementación del proyecto:

(Ver anexo 18)

Resistencias	
56 ohms 1W	1 unidad
100 ohms	1 u.
820 ohms	1 u.
1K	2 u.
2K2	2 u.
10K	2 u.
47K	2 u.
56K	1 u.
68K	1 u.
220K	3 u.
270K	1 u.

Circuitos integrados	
AT89S8252	1 unidad
HIN232	1 u.
ULN2003	1 u.
CM8870	1 u.
Optoacoplador 4N27	1 u.
Optoaislador LCA110	1 u.
Puente de diodos W04	1 u.
Transistor MPSA42 NPN	1 u.
Transistor MJE340 NPN	1 u.
Diodo 1N5250	2 u.
Diodo 1N4148	2 u.

Capacitores	
33 pF	2 unidades
10 nF 100V	2 u.
100 nF	2 u.
120 nF	1 u.
470 nF	1 u.
1 uF	4 u.
1 uF 63V	2 u.
4,7 uF	1 u.
10 uF	1 u.

Cualquier microcontrolador basado en el 8051 es válido para el proyecto, pero en particular, el AT89S8252 permite la programación “en sistema” (ISP). Cualquier controlador para comunicación RS-232 es válido para el proyecto. Se recomendó el MAX232, y se optó por el HIN232 por ser más económico. El ULN2003 es un controlador para poder conectar diferentes cargas al circuito (relés, LEDs, displays, etc.). En nuestro caso lo utilizamos para controlar el relé, y para la generación de la onda acústica que emitimos a través de la línea telefónica.

El L7805 es un regulador de tensión continua, que establece a su salida 5 volts. (*Ver anexo 17)*

Otros	
Relé TDS-0502 (o similar)	1 unidad
Cristal 12 Mhz	1 u.
Cristal 3.5795 Mhz	1 u.
L7805	1 u.
Varistor	1 u.
Jack telefónico	1 u.
Pulsador	1 u.
Conector DB9	1 u.
Conector DB25	1 u.
Jumper	2 u.
Zócalo de 16 pines	2 u.
Zócalo de 18 pines	1 u.
Zócalo de 40 pines	1 u.
Plaqueta univ. BK-06	1 u.

11.7. PRODUCTO DESARROLLADO

11.7.1. CÓDIGO ASSAMBLER

```
; *** CODIGO ASSAMBLER ***

TIMEOUT_H_LIMIT     EQU 0x02

; TIMEOUT_H_LIMIT     EQU 0xFF

RINGS_ANSWER        EQU 0X03        ; cant. Rings de espera antes de contestar la
llamada

EEMEN           EQU 00001000b   ; EEPROM access enable bit

EEMWE               EQU 00010000b   ; EEPROM write enable bit

WDTRST              EQU 00000010b   ; EEPROM RDY/BSY bit

WMCON               DATA 96h        ; watchdog and memory control register

RELAY_1_STATUS      EQU 0x0001      ; dirección en EEPROM en donde se almacena
el estado del relé 1
```

```
Q_RINGS_X       EQU 0x0A        ; dirección en EEPROM en donde se almacena la cantidad de rings (se reservan los 10 primeros bytes para el estado de los relés)
Q_RINGS_DEFAULT EQU 0x03        ; cantidad de rings “por defecto”, si aún el usuario no setéo alguna cantidad
UNDEFINED       EQU 0xFF        ; significado que le asignamos a lo “indefinido” (para cualquier uso que lo requiera)
SWITCHED_OFF    EQU 0x00        ; valor almacenado en EEPROM para indicar que el relé está apagado
SWITCHED_ON     EQU 0x01        ; valor almacenado en EEPROM para indicar que el relé está encendido
RING_TIME_WAIT  EQU 0x10        ; cantidad de iteraciones de espera hasta que transcurra el ring completo
SETTINGS_SERIAL EQU 0xF3        ; valor con el cual se carga el timer 1 para la generación de baudios para 2400 bps
                                ;  dependiendo del valor del Xtal (0xF3=12 Mhz  y 0xF4=11.0592 Mhz)

; *** SEGMENTO DE DATOS ***
DSEG AT 0x30
R_CHAR:         DS 1    ; carácter recibido por el puerto serie
T_CHAR:         DS 1    ; carácter a transmitir por el puerto serie
DIGIT:          DS 1    ; dígito recibido por el conversor DTMF->Binario, en P2.0 P2.1 P2.2 P2.3
PASSWORD:       DS 4    ; almacena la password (ver cómo darle persistencia)
```

PASS_LOADED: DS 4 ; almacena la password cargada por el usuario para luego comparar contra PASSWORD

BYTES_PASS: DS 1 ; variable utilizada por la rutina GET_PASS en el proceso de logueo

AUX: DS 1 ; variable auxiliar que puede ser utilizada por cualquier subrutina

Q_RINGS: DS 1 ; variable en donde se almacena la cantidad de rings que espera el circuito antes de atender la llamada entrante

Q_RINGS_AUX: DS 1 ; variable en donde se van “contando” los rings detectados

TIMEOUT_H: DS 1 ; byte más significativo del contador de timeout

TIMEOUT_L: DS 1 ; byte menos significativo del contador de timeout

FREQUENCY_H: DS 1 ; parámetro “frecuencia” recibido por la rutina SOUND (byte más significativo)

FREQUENCY_L: DS 1 ; parámetro “frecuencia” recibido por la rutina SOUND (byte menos significativo)

LENGTH: DS 1 ; parámetro “duración” recibido por la rutina SOUND

; *** SEGMENTO DE MEMORIA DIRECCIONABLE DE A BIT ***

BSEG AT 0x00

LOGUED: DBIT 1 ; indica si el usuario está logueado

SWITCH_ON: DBIT 1 ; indica que se ha seleccionado la opción de encender relay

SWITCH_OFF: DBIT 1; indica que se ha seleccionado la opción de apagar relay

CHECK_RELAY: DBIT 1; indica que se ha seleccionado la opción de consultar relay

CHANGE_PASS: DBIT 1; indica que se ha seleccionado la opción de cambiar la contraseña

CHANGE_RINGS: DBIT 1; indica que se ha seleccionado la opción de cambiar la cantidad de rings

```
EXIT:           DBIT 1  ; indica que se ha seleccionado la opción de salir (desloguearse)
DIG_PRESSED:    DBIT 1   ; indica si se ha presionado un dígito en el teléfono remoto
SEND_CHAR:      DBIT 1   ; indica si se quiere transmitir por RS-232 el byte almacenado en
T_CHAR
COMP_RESULT: DBIT 1   ; indica el resultado de la rutina COMPARE_PASS (0=distintas;
1=iguales)
NO_FIRST:       DBIT 1   ; permite ignorar el primer carácter debido al encendido del
circuito, y que molesta

; *** SEGMENTO DE CÓDIGO ***
CSEG AT 0x00

; *** Vector de interrupciones *** ;
ORG 0x00
INIT:           LJMP SET_PASSWORD
                ORG 0x03
                LJMP EI0_HANDLER            ;   EI0_HANDLER   =   External
Interrupt 0 Handler
                ORG 0x0B
                LJMP T0_HANDLER                     ; T0_HANDLER = Timer 0
Handler
                ORG 0x13
                LJMP EI1_HANDLER ;I1_HANDLER = External Interrupt 1 Handler
                ORG 0x1B
                RETI
```

```
                ORG 0x23
                LJMP SI_HANDLER         ; SI_HANDLER = Serial Interrupt Handler
                ORG 0x2B
                RETI
                ; *** Fin vector de interrupciones *** ;

                ; *** Se setéa la contraseña por defecto (1111) ***
SET_PASSWORD:           MOV R0,#PASSWORD
                MOV @R0,#0x01
                INC R0
                MOV @R0,#0x01
                INC R0
                MOV @R0,#0x01
                INC R0
                MOV @R0,#0x01

                ; *** Se setéa la cantidad de rings de espera por defecto (3 rings) ***
                MOV R0,#Q_RINGS
                MOV @R0,#RINGS_ANSWER

                CLR NO_FIRST

                JMP MAIN

                ORG 0x50
```

```
                ; *** Acceso a EEPROM para recuperar configuraciones ***
MAIN:           ORL WMCON,#EEMEN            ; se habilita el acceso a EEPROM
                MOV DPTR,#RELAY_1_STATUS
                MOVX A,@DPTR                ; se lee el estado del relé desde EEPROM
                CJNE A,#SWITCHED_ON,RELAY_OFF2
                SETB P1.1                   ; se enciende el relé
                JMP RELAY_ON2
RELAY_OFF2:     CLR P1.1                    ; se apaga el relé
RELAY_ON2:      SETB P1.2                   ; para indicar “desatendido”
                ANL P1,#00000110B           ; “AND lógico” para inicializar P1 (
P1.0=BEEP ; P1.1=CONTROL RELÉ ; P1.2=CONTROL CIRCUITO ATENDIDO )
                MOV P2,#0xFF                ; P2 va a manejar I/O con el teléfono remoto
                MOVX A,@DPTR
                MOV A,#Q_RINGS_DEFAULT      ;  se asigna la cantidad “por defecto”
DEFINED:        MOV Q_RINGS,A
                XRL WMCON,#EEMEN            ; se deshabilita el acceso a EEPROM
                ; *** Fin acceso a EEPROM ***
                CLR LOGUED
                CLR SWITCH_ON
                CLR SWITCH_OFF
                CLR CHECK_RELAY
                CLR CHANGE_PASS
                CLR CHANGE_RINGS
                CLR EXIT
                CLR DIG_PRESSED
```

```
CLR SEND_CHAR
SETB IT0                ; interrupción externa INT0 por flanco descendente
SETB IT1                ; interrupción externa INT1 por flanco descendente

MOV BYTES_PASS,#0x00
MOV Q_RINGS_AUX,#0x00
MOV AUX,#0x00
MOV TIMEOUT_L,#0x00
MOV TIMEOUT_H,#0x00

MOV TL0,#0x00           ; inicialización del timer 0 para que
MOV TH0,#0x00           ; cuente 65536 cuentas
CLR TF0                 ; se limpia el flag de overflow

; *** Inicialización de la comunicación SERIE RS-232 ***
MOV A,PCON      ; en las 3 primeras líneas se pone en 0
CLR ACC.7       ; el bit SMOD (bit 7 de PCON). Así, para calcular
MOV PCON,A      ; el “baud rate” se divide por 32 (sino habría que dividir por 16)
MOV SCON,#0x52 ; setéa el puerto serie en MODO 1, REN=1, TI=0 y RI=0
MOV TMOD,#0x21 ; setéa el timer 0 en MODO 1 (16 bits auto-reload) y el timer 1 en MODO 2 (8 bits auto-reload)
MOV TH1,#SETTINGS_SERIAL
```

```
CLR TR0
                SETB TR1        ; arranca el timer 1
                MOV IE,#0x96    ; habilita la interrupción para la comunicación serie,
                                ; la interrupción externa 1, y la interrupción del timer 0
                JMP WAIT

                ORG 0x0100
WAIT:           JNB DIG_PRESSED,WAIT ; espera hasta que se presione algún dígito
                JB LOGUED,USER_LOGUED
                CALL GET_PASS
                JMP WAIT
USER_LOGUED:    JNB SWITCH_ON,NEXT2
                CALL RELAY_ON
                JMP WAIT
NEXT2:          JNB SWITCH_OFF,NEXT3
                CALL RELAY_OFF
                JMP WAIT
NEXT3:          JNB CHECK_RELAY,NEXT4
                CALL GET_RELAY
                JMP WAIT
NEXT4:          JNB CHANGE_PASS,NEXT5
                CALL CH_PASS
                JMP WAIT
NEXT5:          JNB CHANGE_RINGS,NEXT9
                CALL CH_RINGS
```

```
                JMP WAIT
NEXT9:          JNB EXIT,CALL_BACK
                CALL EXIT_PROGR
                JMP WAIT
CALL_BACK:      CALL DIG_HANDLER
                JMP WAIT

; EXTERNAL INTERRUPT 0 HANDLER
; Maneja la interrupción externa 0, la cual se dispara cuando un nuevo dígito fué presionado
; en el aparato telefónico remoto.
; El dígito, en binario, entra por P2.0 P2.1 P2.2 P2.3 (Q4 Q3 Q2 Q1), se lo lee, y se lo
; coloca en DIGIT. Lo importante de esta subrutina es que REBATE el dígito recibido (dado
que
; lo recibe al revés). También setéa DIG_PRESSED para que el programa principal actúe.
EI0_HANDLER:    PUSH ACC
                PUSH B
                CLR TR0
                MOV A,P2
                MOV B,#0x00
BIT_0:          JNB ACC.0,BIT_1
                SETB B.3
BIT_1:          JNB ACC.1,BIT_2
                SETB B.2
BIT_2:          JNB ACC.2,BIT_3
                SETB B.1
```

```
BIT_3:      JNB ACC.3,SWAP_END
            SETB B.0
SWAP_END:   MOV DIGIT,B
            MOV A,DIGIT
            CJNE A,#0x08,NO_RST
            POP B
            POP ACC
            DEC SP
            MOV R0,SP
            MOV @R0,#0x00
            INC SP
            MOV R0,SP
            MOV @R0,#0x01
            CLR SWITCH_ON
            CLR SWITCH_OFF
            CLR CHECK_RELAY
            CLR CHANGE_PASS
            CLR CHANGE_RINGS
            CLR EXIT
            CLR DIG_PRESSED
            MOV TIMEOUT_L,#0x00  ; se resetéa el contador de time-out,
            MOV TIMEOUT_H,#0x00  ; debido a que el usuario presionó una tecla
            MOV TL0,#0x00        ; inicialización del timer 0 para que
            MOV TH0,#0x00        ; cuente 65536 cuentas
            SETB TR0
```

```
                RETI
NO_RST:         POP B
                POP ACC
                JNB NO_FIRST,IGNORE
                SETB DIG_PRESSED
IGNORE:         SETB NO_FIRST
                MOV T_CHAR,DIGIT        ; para debugging
                SETB SEND_CHAR          ; para debugging
                MOV TIMEOUT_L,#0x00  ; se resetéa el contador de time-out,
                MOV TIMEOUT_H,#0x00  ; debido a que el usuario presionó una tecla
                MOV TL0,#0x00        ; inicialización del timer 0 para que
                MOV TH0,#0x00        ; cuente 65536 cuentas
                SETB TR0
                RETI
; TIMER 0 HANDLER
; Maneja la interrupción asociada al overflow del timer 0.
; Es utilizada para administrar un time-out en caso de que un usuario corte la comunicación
telefónica
; sin desloguearse (cuando se produce el time-out, se limpian todos los flags, y por
consiguiente,
; el sistema queda en condiciones de poder ser utilizado nuevamente.
T0_HANDLER:     PUSH ACC
                CLR TR0
                MOV A,TIMEOUT_H
                CJNE A,#TIMEOUT_H_LIMIT,NO_TIMEOUT
```

```
                DEC SP
                MOV R0,SP
                MOV @R0,#0x50
                INC SP
                MOV R0,SP
                MOV @R0,#0x00
                RETI
NO_TIMEOUT:     MOV A,TIMEOUT_L
                CLR C
                ADD A,#0x01
                MOV TIMEOUT_L,A
                JNC NO_OVERFLOW
                MOV A,TIMEOUT_H
                ADD A,#0x01
                MOV TIMEOUT_H,A
NO_OVERFLOW:    MOV TL0,#0x00       ; inicialización del timer 0 para que
                MOV TH0,#0x00       ; cuente 65536 cuentas
                CLR TF0             ; se limpia el flag de overflow
                POP ACC
                SETB TR0
                RETI
; EXTERNAL INTERRUPT 1 HANDLER
; Maneja la interrupción externa 1, la cual se dispara con cada “ring” de una llamada entrante.
; Si atiende la llamada entrante, entonces habilita la interrupción IE0 para recibir los dígitos.
EI1_HANDLER:    PUSH ACC
```

```
                CLR EX1; se deshabilita la interrupción para que ignore todas las
interrupciones siguientes en el mismo ring
                                        ;  significando así una interrupción por ring.
                CLR TF0
                SETB TR0                ; arranca el timer 0
                MOV A,#RING_TIME_WAIT
NEXT_STEP:      DEC A
                JNB TF0,$
                CLR TF0
                JNZ NEXT_STEP
                CLR TF0
                CLR TR0

                INC Q_RINGS_AUX
                MOV A,Q_RINGS_AUX
                MOV 0x4C,A
                CJNE A,Q_RINGS,NO_ANSWER
                SETB EX0
                MOV TIMEOUT_L,#0x00  ; se resetéa el contador de time-out,
                MOV TIMEOUT_H,#0x00 ; debido a que el usuario presionó una tecla
                SETB TR0        ; arranca el timer 0
NO_ANSWER:      SETB EX1
                POP ACC
                RETI
; SERIAL INTERRUPT HANDLER
```

```
; Maneja la interrupción provocada por los flags RI y TI cuando se recibe un byte por comunicación
; serie RS-232, o cuando se terminó de transmitir el último byte, respectivamente.
; Pone en R_CHAR el caracter recibido, y transmite el caracter almacenado en T_CHAR, siempre y cuando
; esté seteado el bit SEND_CHAR.
SI_HANDLER:     JNB RI,SEND
                MOV R_CHAR,SBUF
                CLR RI
SEND:           JNB TI,END_SI_HANDLER
                JNB SEND_CHAR,END_SI_HANDLER
                CLR TI
                CLR SEND_CHAR
                MOV SBUF,T_CHAR
END_SI_HANDLER:     RETI
; GET PASSWORD
GET_PASS:       PUSH ACC
                MOV A,#PASS_LOADED
                ADD A,BYTES_PASS
                MOV R0,A
                MOV @R0,DIGIT
                INC BYTES_PASS
                MOV R1,BYTES_PASS
                CJNE R1,#0x04,NOT_LOADED
LOADED:             CALL COMPARE_PASS
```

```
                MOV BYTES_PASS,#0x00
                JNB COMP_RESULT,NOT_LOADED
                SETB LOGUED
NOT_LOADED:     CLR DIG_PRESSED
                POP ACC
                RET
; SWITCH RELAY ON
; Setéa un bit en el puerto 1 (P1) para encender el relay solicitado. Por ejemplo, SETB P1.1
enciende
; el relay 1. Para ello, consulta el valor en DIGIT.
; Limpia los bits DIG_PRESSED y SWITCH_ON.
RELAY_ON:       PUSH ACC
                MOV R0,DIGIT
                CJNE R0,#0x01,RELAY_ON_END
                SETB P1.1

                ; se escribe en EEPROM el estado del relé (para darle persistencia)
                ORL WMCON,#EEMEN    ; se habilita el acceso a EEPROM
                                    MOV DPTR,#RELAY_1_STATUS
                MOV A,#0x01         ; 0x01 significa “encendido”
                MOVX @DPTR,A ; escribe la EEPROM con el contenido del acumulador
                ; Loop de espera hasta que concluya la escritura a EEPROM
LOOP_RELAY_ON:          MOV A,WMCON  ; se lee el estado de escritura de la EEPROM
                ANL A,#WDTRST                           ; se crequéa RDY/BSY
                JZ LOOP_RELAY_ON ; vuelve a loopear si está seteado BSY (“busy”)
```

```
                XRL WMCON,#EEMEN            ; se deshabilita el acceso a EEPROM
                CALL LONG_BEEP
RELAY_ON_END:   CLR DIG_PRESSED
                CLR SWITCH_ON
                POP ACC
                RET
; SWITCH RELAY OFF
; Limpia un bit en el puerto 1 (P1) para apagar el relay solicitado. Por ejemplo, CLR P1.1 apaga el
; relay 1. Para ello, consulta el valor en DIGIT.
; Limpia los bits DIG_PRESSED y SWITCH_OFF.
RELAY_OFF:      MOV R0,DIGIT
                CJNE R0,#0x01,RELAY_OFF_END
                CLR P1.1

                ; se escribe en EEPROM el estado del relé (para darle persistencia)
                ORL WMCON,#EEMEN    ; se habilita el acceso a EEPROM
                MOV DPTR,#RELAY_1_STATUS
                MOV A,#0x00         ; 0x00 significa “apagado”
                MOVX @DPTR,A ; escribe la EEPROM con el contenido del acumulador
                        ; Loop de espera hasta que concluya la escritura a EEPROM
LOOP_RELAY_OFF:  MOV A,WMCON   ; se lee el estado de escritura de la EEPROM
                ANL A,#WDTRST                       ; se crequéa RDY/BSY
                JZ LOOP_RELAY_OFF ; vuelve a loopear si está seteado BSY (“busy”)
                XRL WMCON,#EEMEN            ; se deshabilita el acceso a EEPROM
```

```
                CALL LONG_BEEP
RELAY_OFF_END:  CLR DIG_PRESSED
                CLR SWITCH_OFF
                RET

; GET RELAY STATUS
; Consulta si un relay está encendido o apagado, para lo cual accede al bit correspondiente
; en el puerto 1 (P1).
; Limpia los bits DIG_PRESSED y CHECK_RELAY.
GET_RELAY:      MOV R0,DIGIT
                CJNE R0,#0x01,GET_RELAY_END
                JNB P1.1,RELAY_IS_OFF
                CALL LONG_BEEP
                JMP GET_RELAY_END
RELAY_IS_OFF: CALL SHORT_BEEP
GET_RELAY_END:  CLR DIG_PRESSED
                CLR CHECK_RELAY
                RET
; CHANGE PASSWORD
CH_PASS:        PUSH ACC
                MOV R0,#PASSWORD
                MOV R1,#0x00
NEXT:           MOV @R0,DIGIT
                INC R0
                INC R1
```

```
                CLR DIG_PRESSED
                CJNE R1,#0x04,WAIT_BYTE
                JMP END_CH_PASS
WAIT_BYTE:      JNB DIG_PRESSED,WAIT_BYTE
                JMP NEXT
END_CH_PASS:    CALL LONG_BEEP
                CLR CHANGE_PASS
                CLR LOGUED              ; le obligo al usuario que se vuelva a loguear
                POP ACC
                RET
; CHANGE RINGS
CH_RINGS:       PUSH ACC
                MOV Q_RINGS,DIGIT
                CLR DIG_PRESSED

                ORL WMCON,#EEMEN        ; se habilita el acceso a EEPROM
                MOV DPTR,#Q_RINGS_X
                MOV A,Q_RINGS
                MOVX @DPTR,A; escribe la EEPROM con el contenido del acumulador
                ; Loop de espera hasta que concluya la escritura a EEPROM
LOOP_CH_RINGS:  MOV A,WMCON             ; se lee el estado
de escritura de la EEPROM
                ANL A,#WDTRST           ; se crequéa RDY/BSY
                JZ LOOP_CH_RINGS ;vuelve a loopear si está seteado BSY (“busy”)
                L WMCON,#EEMWE  ;se deshabilita el acceso a EEPROM para escritura
```

```
                XRL WMCON,#EEMEN          ; se deshabilita el acceso a EEPROM
                CALL LONG_BEEP
                CLR CHANGE_RINGS
                POP ACC
                RET
; EXIT PROGRAM
; Desloguéa el usuario, y arranca todo nuevamente.
EXIT_PROGR:     CALL LONG_BEEP
                DEC SP
                MOV R0,SP
                MOV @R0,#0x50
                INC SP
                MOV R0,SP
                MOV @R0,#0x00
                RET
; COMPARE PASSWORDS
; Compara la password ingresada por el usuario contra la password almacenada en memoria.
; Setéa el CARRY si son iguales.
COMPARE_PASS:           PUSH ACC
                MOV R0,#PASSWORD
                MOV R1,#PASS_LOADED
                MOV R2,#0x00
NEXT_BYTE:      MOV A,@R0
                MOV AUX,@R1
                CJNE A,AUX,BAD_PASS
```

```
                INC R0
                INC R1
                INC R2
                CJNE R2,#0x04,NEXT_BYTE
CORRECT_PASS:   SETB COMP_RESULT
                CALL INTRO
                JMP END_CMP
BAD_PASS:       CLR COMP_RESULT
                CALL SHORT_BEEP
END_CMP:        POP ACC
                RET
; SHORT BEEP
; Emite un beep corto.
SHORT_BEEP:     PUSH ACC
                CLR TR0                 ; se para el timer
                CLR TF0
                MOV R0,#0xFF
LOOP2_SB:       MOV A,#0xFF
LOOP1_SB:       MOV TH0,#0xFC
                MOV TL0,#0x18
                SETB TR0
                JNB TF0,$
                CLR TR0
                CLR TF0
                CPL P1.0
```

```
                INC A
                CJNE A,#0xFF,LOOP1_SB
                INC R0
                CJNE R0,#0x00,LOOP2_SB
                MOV TH0,#0x00
                MOV TL0,#0x00
                SETB ET0
                SETB TR0
                POP ACC
                RET
; LONG BEEP
; Emite un beep largo.
LONG_BEEP:      PUSH ACC
                CLR TR0
                CLR TF0
                MOV R0,#0xFF
LOOP2_LB:       MOV A,#0xFF
LOOP1_LB:       MOV TH0,#0xFE
                MOV TL0,#0x0C
                SETB TR0
                JNB TF0,$
                CLR TR0
                CLR TF0
                CPL P1.0
                INC A
```

```
                CJNE A,#0xFF,LOOP1_LB
                INC R0
                CJNE R0,#0x02,LOOP2_LB
                MOV TH0,#0x00
                MOV TL0,#0x00
                SETB ET0
                SETB TR0
                POP ACC
                RET
; SOUND
; Dados los parámetros FREQUENCY_H, FREQUENCY_L y LENGTH, emite un sonido.
SOUND:          PUSH ACC
                CLR TR0
                CLR TF0
                MOV A,#0xFF
LOOP2_SOUND:    MOV R0,#0xFF
LOOP1_SOUND:    MOV TH0,FREQUENCY_H
                MOV TL0,FREQUENCY_L
                SETB TR0
                JNB TF0,$
                CLR TR0
                CLR TF0
                CPL P1.0
                INC R0
                CJNE R0,#0xFF,LOOP1_SOUND
```

```
                INC A
                CJNE A,LENGTH,LOOP2_SOUND
                MOV TH0,#0x00
                MOV TL0,#0x00
                SETB ET0
                SETB TR0
                POP ACC
                RET
; DELAY
; Espera una cierta cantidad de tiempo, especificada en LENGTH
DELAY:          PUSH ACC
                CLR TR0
                CLR TF0
                MOV A,#0xFF
LOOP2_DELAY:    MOV R0,#0xFF
LOOP1_DELAY:    MOV TH0,#0xFF
                MOV TL0,#0xCE
                SETB TR0
                JNB TF0,$
                CLR TR0
                CLR TF0
                INC R0
                CJNE R0,#0xFF,LOOP1_DELAY
                INC A
                CJNE A,LENGTH,LOOP2_DELAY
```

```
                MOV TH0,#0x00
                MOV TL0,#0x00
                SETB ET0
                SETB TR0
                POP ACC
                RET
; INTRO
; Genera una melodía para introducción
INTRO:          MOV FREQUENCY_H,#0xFE
                MOV FREQUENCY_L,#0x0C
                MOV LENGTH,#0x02
                CALL SOUND
                CALL DELAY
                CALL SOUND
                CALL DELAY
                CALL SOUND
                MOV LENGTH,#0x04
                CALL DELAY
                MOV LENGTH,#0x02
                CALL SOUND
                CALL DELAY
                CALL SOUND
                CALL DELAY
                CALL SOUND
```

```
MOV LENGTH,#0x04
CALL DELAY
MOV FREQUENCY_H,#0xFE
MOV FREQUENCY_L,#0x0C
MOV LENGTH,#0x02
CALL SOUND
CALL DELAY
MOV FREQUENCY_H,#0xFE
MOV FREQUENCY_L,#0x5F
CALL SOUND
CALL DELAY
MOV FREQUENCY_H,#0xFD
MOV FREQUENCY_L,#0x8F
CALL SOUND
CALL DELAY
MOV FREQUENCY_H,#0xFD
MOV FREQUENCY_L,#0xD4
CALL SOUND
CALL DELAY
MOV FREQUENCY_H,#0xFE
MOV FREQUENCY_L,#0x0C
CALL SOUND
 RET
```

; DIGIT HANDLER

; Subrutina de “callback”. De acuerdo al dígito presionado (opción seleccionada), setéa el bit

```
DIG_HANDLER: MOV R0,DIGIT
OPTION_1:    CJNE R0,#0x01,OPTION_2
             SETB SWITCH_ON
             JMP DIG_HAN_END
OPTION_2:    CJNE R0,#0x02,OPTION_3
             SETB SWITCH_OFF
             JMP DIG_HAN_END
OPTION_3:    CJNE R0,#0x03,OPTION_4
             SETB CHECK_RELAY
             JMP DIG_HAN_END
OPTION_4:    CJNE R0,#0x04,OPTION_5
             SETB CHANGE_PASS
             JMP DIG_HAN_END
OPTION_5:    CJNE R0,#0x05,OPTION_9
             SETB CHANGE_RINGS
             JMP DIG_HAN_END
OPTION_9:    CJNE R0,#0x09,DIG_HAN_END
             SETB EXIT
             SETB DIG_PRESSED  ; se setéa DIG_PRESSED, porque el exit es una
operación unaria, y debe ingresar directamente a la subrutina EXIT_PROGR
             RETI
DIG_HAN_END: CLR DIG_PRESSED
             CALL LONG_BEEP
             RET
END
```

11.7.2. CÓDIGO VISUAL BASIC

```
Private Sub Form_Load()
        ShockwaveFlash1.Movie = App.Path + "\huella.swf"
        End Sub
        Private Sub Image3_Click()
        Decision = 2
        Captura.Show 1
        End Sub

        Private Sub Image4_Click()
        Decision = 1
        Impresora.Show 1
        End Sub

        Private Sub Image5_Click()
        Close All
        Unload Me
        End Sub
        Private Sub ShockwaveFlash1_OnReadyStateChange(newState As Long)
        End Sub
Private Sub Combo1_Click()
            Cadena = "Nombre='" & Trim(Combo1.Text) & "'"
             With Tarjeta
               .    FindFirst Cadena
               If .NoMatch Then
               Else
                 On Error GoTo 0 ' Desactiva la detección de errores.
                 On Error Resume Next    ' Retarda detección de errores.
                 Cadena2 = App.Path + "\" + Trim(.Fields(0)) + ".jpg"
                 Image1.Picture = LoadPicture(Cadena2)
                 If Err.Number = 53 Then

                 End If
```

```
                Resume
            End If
        End With
    End Sub

Private Sub Command1_Click()
        If Combo1.Text = "" Then
            Label8.Caption = "Introduce el NOMBRE"
        Else
            Lector_Huella.TerminaVerificacion
            Lector_Huella.CrearUsuario
        End If
    End Sub

Private Sub Command2_Click()
    Lector_Huella.TerminaVerificacion
    Lector_Huella.Desconecta
    Unload Me
    End Sub

Private Sub Form_Activate()
    Set db = OpenDatabase(App.Path + "\Lector3.mdb")
    Set Tarjeta = db.OpenRecordset("Registro", dbOpenDynaset)
    Set Tarjeta2 = db.OpenRecordset("ENT_SAL", dbOpenDynaset)
    Data1.RecordsetType = 1
    Text1.Text = ""
    Lector_Huella.Conecta
    If Decision = 1 Then
      Command1.Enabled = False
      Command4.Enabled = False
      Command3.Enabled = False
      Text2.Enabled = False
      Text3.Enabled = False
      ext4.Enabled = False
      Text5.Enabled = False
      Text6.Enabled = True
```

```
    Text7.Enabled = True
    Text8.Enabled = True
    Text9.Enabled = True
    Combo1.Enabled = True
    Combo2.Enabled = False
    Combo3.Enabled = False
    Lector_Huella.Verifica
  If Decision = 2 Then
    Command1.Enabled = True
   '   Lector_Huella.CrearUsuario
  End If
  With Tarjeta
      cuantos = 0
      .MoveFirst
      Do While Not .EOF
       Combo1.AddItem .Fields(1), cuantos
       .          MoveNext
        cuantos = cuantos + 1
     Loop
  End With
  Shape1.FillColor = &H8000&
  Shape2.FillColor = &H8000&
  Shape3.FillColor = &H8000&
  Shape4.FillColor = &H8000&
  End Sub

Prívate Sub Lector_Huella_ImagenMuyBorrosa()
   Shape2.FillColor = &HFF&
  End Sub

  Private Sub Lector_Huella_ImagenMuyBrillante()
   Shape3.FillColor = &HFF&
  End Sub

  Private Sub Lector_Huella_ImagenMuyObscura()
   Shape4.FillColor = &HFF&
```

```
End Sub

Private Sub Lector_Huella_NoCentrado()
 Shape1.FillColor = &HFF&
End Sub


Private Sub Lector_Huella_PreRegistro(ByVal aNumHuellas As Integer)
   Shape1.FillColor = &H8000&
   Shape2.FillColor = &H8000&
   Shape3.FillColor = &H8000&
   Shape4.FillColor = &H8000&
   Label3.Caption = Str(aNumHuellas)
End Sub

Private Sub Lector_Huella_Registered(ByVal aValue As String)
   Dim codigo As Variant
   Dim cad As String
    codigo = aValue
    Text1.Text = aValue
    cad = "Nombre='" & Combo1.Text + "'"
    With Tarjeta
      .FindFirst cad
      If .NoMatch Then
        .       AddNew
        .Fields(0) = Text2.Text
        .Fields(1) = Combo1.Text
        .Fields(2) = Combo2.Text
        .Fields(3) = Text3.Text
        .Fields(4) = Combo3.Text
        .Fields(5) = Text4.Text
        .Fields(6) = Text5.Text
        Fields(7) = Text7.Text
         .Fields(8) = Text6.Text
        .Fields(9) = Mid(codigo, 1, 300)
        .Fields(10) = Mid(codigo, 301, 600)
        .Fields(11) = Mid(codigo, 601, 900)
```

```
        Else
          .Edit
          .Fields(9) = Mid(codigo, 1, 300)
          .Fields(10) = Mid(codigo, 301, 600)
          .Fields(11) = Mid(codigo, 601, 900)
        End If
        .Update
      End With
    End Sub

Private Sub Lector_Huella_RegistroFallo()
        Print "REGISTRO FALLO"
        End Sub


Private Sub Lector_Huella_TerminaVerificacion()
          Label8.Caption = "Siguiente Registro"
        End Sub

If Data1.Recordset.EOF Then
          Exit Do
        End If
        If  Lector_Huella.Concuerdan(Text1.Text, aValue) Then
          Label8.Caption = "Registro Encontrado"
          If IsNull(Data1.Recordset(1)) Then
            Combo1.Text = " "
          Else
             Combo1.Text = Data1.Recordset(1)
          End If
          If IsNull(Data1.Recordset(0)) Then
             Text2.Text = " "
          Else
             Text2.Text = Data1.Recordset(0)
          End If
          If IsNull(Data1.Recordset(3)) Then
            Text3.Text = " "
          Else
```

```
    Text3.Text = Data1.Recordset(3)
End If
If IsNull(Data1.Recordset(5)) Then
    Text4.Text = " "
Else
    Text4.Text = Data1.Recordset(5)
End If
If IsNull(Data1.Recordset(6)) Then
    Text5.Text = " "
Else
    Text5.Text = Data1.Recordset(6)
End If


If insole(Data1.Recordset(2)) Then
    Combo2.Text = " "
Else
    Combo2.Text = Data1.Recordset(2)
End If
If IsNull(Data1.Recordset(4)) Then
    Combo3.Text = " "
Else
    Combo3.Text = Data1.Recordset(4)
End If
If IsNull(Data1.Recordset(7)) Then
    Text7.Text = " "
Else
    Text7.Text = Data1.Recordset(7)
End If
If IsNull(Data1.Recordset(8)) Then
    Text6.Text = " "
Else
    Text6.Text = Data1.Recordset(8)
End If
Text8.Text = Time()
 On Error GoTo 0 ' Desactiva la detección de errores.
 On Error Resume Next    ' Retarda detección de errores.
```

```
cadena3 = App.Path + "\" + Trim(Data1.Recordset(0)) + ".jpg"
ClaveT = Data1.Recordset(0)
Hora_Ent = Data1.Recordset(7)
Hora_Sal = Data1.Recordset(8)
Image1.Picture = LoadPicture(cadena3)
If Err.Number = 53 Then
  Image1.Picture = LoadPicture("c:\Delegacion\mientras.jpg")



End If
Resume
Data1.Recordset.MoveLast
Exit Do
End If
Data1.Recordset.MoveNext
Loop
If Lector_Huella.Concuerdan(Text1.Text, aValue) = False Then
Label8.Caption = "Registro Incorrecto Intente de Nuevo"
MsgBox ("Registro No Encontrado")
Combo1.Text = ""
End If
If Lector_Huella.Concuerdan(Text1.Text, aValue) = True Then
With Tarjeta2
If Time() >= Hora_Sal Then
    Cadena6 = " "
    Cadena6   = "Clave_Maestro='" &       Trim(ClaveT) & "'
    and  Fecha='" &
Format(Date, "Long Date") & "'"
    .    FindFirst Cadena6
    If .NoMatch Then
      .  AddNew
      .Fields(0) = ClaveT
      .Fields(1) = Format(Date, "Long Date")
      .Fields(2) = Time()
      .Fields(3) = Time()
      .Fields(4) = "FALTA"
```

```
                .Fields(5) = "FALTA"
               .Update
              Else
               If .Fields(4) = "FALTA" Then


                .Edit
                .Fields(3) = Time()
                .Fields(5) = "FALTA"
                .Update
               Else
                .Edit
                .Fields(3) = Time()
                .Update
               End If
              End If
            Else
             Cadena6 = "Clave_Maestro='" & Trim(ClaveT) & "' and Fecha='"
& Format(Date,
        "Long Date") & "'"
             .      FindFirst Cadena6
             If .NoMatch Then
             .      AddNew
             .Fields(0) = ClaveT
             .Fields(1) = Format(Date, "Long Date")
             .Fields(2) = Time()
              Hora = Hour(Hora_Ent)
              Minutos = Minute(Hora_Ent)
              Segundos = Second(Hora_Ent)
              Hora1 = Hour(.Fields(2))
              Minutos1 = Minute(.Fields(2))
              Segundos1 = Second(.Fields(2))
              Hora1 = Hora1 - Hora
              Minutos1 = Minutos1 - Minutos
              Segundos1 = Segundos1 - Segundos
              If Hora1 < 1 Then
                If Minutos1 > 30 Then
```

```
Cadena4 = "FALTA"
                    Else
                      Cadena4 = Str(Hora1) + ":" + Str(Minutos1) + ":" +
Str(Segundos1)
                    End If
                  Else
                    Cadena4 = "FALTA"
                  End If
                  .Fields(4) = Cadena4
                 .       Update
                  Else
                    Label8.Caption = "ENTRADA REGISTRADA"
                    MsgBox ("  CONTINUAR")
                    Label8.Caption = " "
                  End If
                End If
              End With
            End If
            Lector_Huella.Verifica
          End Sub

Private Function BuscarEnBase(Optional ByVal sBusqueda As String = "") As Long
                    Dim sSQL As String
                  Dim l As Integer
                 On Local Error Resume Next
                 If Len(sBusqueda) Then
                    sSQL = "SELECT * FROM ENT_SAL WHERE " & sBusqueda
                    Print sSQL
                    Set db = OpenDatabase(App.Path + "\Lector3.mdb")
                    Set RsBuscar = db.OpenRecordset(sSQL, dbOpenSnapshot)
                    Data1.RecordsetType = 1
                    Data1.Refresh
                 End If
                  RsBuscar.MoveLast
                  l = RsBuscar.RecordCount
                  RsBuscar.MoveFirst
                  If RsBuscar.EOF Then
```

```
      Print "Hola"
    End If
End Function

Private Sub Command1_Click()
Dim i As Integer
    If Check1.Value = 1 Then
      If List2.ListCount = 1 Then
        MsgBox ("No se puede Agregar mas de un Registro")
      Else
       List2.AddItem List1.List(List1.ListIndex)

      End If
    End If
    If Check2.Value = 1 Then
       For i = 0 To List1.ListCount - 1
          List2.AddItem List1.List(i), i
      Next i
  End If
    If Check3.Value = 1 Then
       List2.AddItem List1.List(List1.ListIndex)
    End If
 End Sub

Private Sub Command2_Click()
      If List2.ListCount >= 1 Then
       List2.RemoveItem (List2.ListIndex)
      End If
End Sub

Private Sub Command3_Click()
Dim SQL_Busqueda As String
Dim Fecha1, Fecha2 As Date
Dim i As Integer
 SQL_Busqueda = ""
 CadAnd = " "
```

```
If Text1 <> "" Then
    SQL_Busqueda = "Fecha  =" + Format(Text1.Text, "Long Date")
End If
 If Text2 <> "" Then
    SQL_Busqueda = SQL_Busqueda + " and Fecha <=" + Text2.Text
End If


If (Text1 <> "" Or Text2.Text <> "") And List2.ListCount() > 0 Then
        SQL_Busqueda = SQL_Busqueda + " and "
 End If
For i = 0 To List2.ListCount - 1
   SQL_Busqueda = SQL_Busqueda + "CLAVE_MAESTRO = " + "'" +
List2.List(i) + "'"
   If i <> List2.ListCount - 1 Then
      SQL_Busqueda = SQL_Busqueda + " or "
   End If
Next i
BuscarEnBase (SQL_Busqueda)
End Sub

Private Sub Command4_Click()
Unload Me
End Sub

Private Sub Form_Activate()
Dim Entrada, SQLCad1, SQLCad2 As String
Set db = OpenDatabase(App.Path + "\Lector3.mdb")

Set Tarjeta = db.OpenRecordset("Registro", dbOpenDynaset)

Data1.RecordsetType = 1
Text2.Enabled = False
Label2.Enabled = False

Tarjeta.MoveLast
```

```
With Tarjeta
    cuantos = 0
    .MoveFirst

    Do While Not .EOF
    If IsNull(.Fields(0)) Then
       Entrada = "xxxxxx"
    Else
        Entrada = .Fields(0)
    End If
     List1.AddItem Entrada, cuantos
     .          MoveNext
     cuantos = cuantos + 1
  Loop
 End With
End Sub
```

12. PROBLEMAS ENCONTRADOS DURANTE DESARROLLO DEL PROYECTO

Para culminar el proyecto vamos a necesitar un pequeño scanner que no esta a nuestro alcance económico; ya que necesitaríamos probar el pequeño programa realizado en visual Basic.

En el desarrollo de la tarjeta controladora tuvimos problemas en encontrar asesoramiento para realizar esta labor.

13. PRODUCTO ESPERADO

13.1. LIMITACIONES

Utilizado a nivel de Instituciones educativas con el fin de registrar entradas y salidas de profesorado y alumnos.

No se podrá conectar más de seis dispositivos en la tarjeta controladora.

Simultáneamente no podrán trabajar más de tres lectores biométricos.

13.2. RECOMENDACIONES

Darles mantenimiento a los equipos (lector) para que no existan fallas.

Evitar cambios muy continuos en la configuración de los equipos.

Capacitar a los alumnos, profesores y administradores para el correcto uso de los equipos.

13.3. VALOR AGREGADO QUE BENEFICIEN AL CLIENTE

Asesoría gratuita los primeros 3 meses.

Capacitación sin costo para el personal.

A los equipos vendidos servicio técnico los tres primeros meses sin valor alguno.

Garantía de los equipos.

Manuales y discos instaladores.

13.4. ANÁLISIS DE LA COMPETENCIA

Cabe recalcar que ya existen empresas que ofrecen éste servicio, pero a nivel de grandes empresas y con costos elevados, lo que nos va a diferenciar de los demás será el uso de la controladora de dispositivo, la implementación a nivel educativo a pequeña escala y el costo ya que este oscilará entre los $ 1400

14. DISEÑO DE LA EMPRESA

14.1. IDENTIDAD CORPORATIVA

LM BIOMETRICS S.A.
"Biometría a su alcance"

14.2. LEMA

"Biometría a su alcance"

15. BIBLIOGRAFÍA

http://www.eurokiosks.org/whtpaperses_summit_biometrics.html

http:// es.wikipedia.org/wiki/Biometría

http://www.consumer.es/accesible/es/tecnologia/internet/2005/11/02/146607.php

http://www.kimaldi.com/kimaldi/productos/sistemas_biometricos/lectores_huella_digital_para_pc/lector_huella_digital_nitgen_hamster

http://www.biometrics.org

http:// www.westcorp.com.ar/producto/biometric/huella/huella.html

TECNOLOGÍAS BIOMÉTRICAS APLICADAS A LA SEGURIDAD.

Juan A. Sigüenza; Merino Tapiador Mateos

Marjal Gómez Allende Darío

Reconocimiento y visión artificial

Addison Wesley –Ibero América

Revista de Informática Educativa y Medios Audiovisuales Vol. 2(5), págs. 33-48. 2005

“Simulación en Ingeniería

Eléctrica y Electrónica”. Disponible en:

www.mundo-electrónico.com

16. LIDERAZGO Y MOTIVACIÓN

- Por conseguir cliente a cada empleado se le incentivará con un 3% del costo del proyecto.
- Serán reconocidas las horas extras.
- Serán reconocido los sábados y feriados
- Al cumpleañero (a) perteneciente al grupo de trabajo se le dará el día libre o en caso de trabajo se le dará doble remuneración por dicho día.
- Existirán las prestaciones según la ley.
- Se respetarán a cabalidad los derechos de los trabajadores.

17. PRESUPUESTO DE ESTUDIO

PRESUPUESTO DE ESTUDIO

APROXIMACIONES DE ACTIVOS

Local propio

Auto propio

GASTOS GENERALES + MANO DE OBRA

Por mes

24Días laborables

Unidades /días	Descripción	Valor/unidad	Costo Total
1	Desarrollador	$ 500,00	$ 500,00
2	Técnicos	$ 320,00	$ 640,00
2	Auxiliares técnicos	$ 120,00	$ 240,00
1	Recepcionista	$ 120,00	$ 120,00
96	Almuerzos	$ 1,50	$ 144,00
24	Movilización-gasolina	$ 5,00	$ 120,00
	Planilla de varios	$ 60,00	$ 60,00
	Planilla de Teléfono	$ 80,00	$ 80,00
	Díptica	$ 300,00	$ 300,00
TOTAL			**$ 2.204,00**

COSTOS DE PRODUCTOS

*Nota: área de 8m*6m

COSTO PRODUCTO

Por unidad

Tarjeta Controladora	$	100,00
Dispositivo Biométrico	$	340,00
Monitor	$	100,00
*Cableado + varios	$	80,00
Costo total producto	**$**	**620,00**

COSTO PRODUCTO Mensual

20Unidades

Por 20 empresas, unidades educativas

Tarjeta Controladora	$	2.000,00
Dispositivo Biométrico	$	6.800,00
*Cableado	$	2.000,00
Chapa eléctrica	$	1.600,00
Costo total producto mensual	**$**	**12.400,00**

PRECIO VENTA PÚBLICO		
Por Unidad	**$**	**1.400,00**
Por Mes	**$**	**28.000,00**

DESGLOSE PRECIO VENTA AL PUBLICO	
1400	PVP
800	Empresa cobra de la instalación
600	Costo total producto

COSTO DE VENTA		
Por Mes		
COSTO PRODUCTO	$	12.400,00
GASTOS GENERALES + MANO DE OBRA	$	2.204,00
COSTOS TOTALES DE VENTA	**$**	**14.604,00**

GANANCIA MENSUAL NETA	**$**	**13.396,00**
PRECIO VENTA PÚBLICO	$	28.000,00
COSTOS TOTALES DE VENTA	$	14.604,00

PUNTO DE EQUILIBRIO	**INGRESOS - GASTOS FIJOS + GASTOS VARIABLES**	
GASTOS FIJOS	**$**	**2.204,00**

GASTOS VARIABLES **x*600**

INGRESOS **x*1400**

PUNTO DE EQUILIBRIO	
0=(X*1400)-(2404+(X*600))	
X=?	
0 =	X(1400,00+600,00) - 2204,00
X	$ 1,10

FUNCIÓN EN UNIDADES	
X	$ 2,00
Pérdida / Ganancia	$ 1.796,00

18. BITÁCORA

23 de octubre

Selección de tema para el proyecto de tesis

Visita a la biblioteca de la universidad Católica para verificar la originalidad del tema.

28 de octubre

Visita a la subintendencia de compañía para presupuestar la conformación de la misma.

4 de noviembre

Recopilación de Información

Vía Internet Pagina de la Universidad Autónoma de México www.unam.mx/

Visita a la Biblioteca Municipal de Guayaquil

Entrevista con alumnos de pregrado de Telecomunicaciones acerca de programación en Assembler multicontrolador.

12 de Noviembre

Ayudantias por parte de profesionales:

Ing. Francisco Hsieh

Ing. Mario Celleri

Ing. Fabricio Reyes

15 de Noviembre

Selección de la mejor información para la entrega de la propuesta.

Redacción de la información tomada.

22 de Noviembre

Entrega de propuesta

25 de Noviembre

Corrección de presupuesto

11 de Diciembre

Segunda corrección de presupuesto

4 de Enero

Exposición de la propuesta de tesis en presencia de la Lcda. Ana Ulloa

6 de Enero

Ampliación de los temas investigados

10 de Enero

Se integro las nuevas investigaciones al proyecto de tesis

20 de Enero

Asesoramiento con Técnicos especializados

25 de Enero

Se consiguió la programación y codificación en programa assambler

4 de Febrero

Se trabajo organizando la estructura de la tesis

9 de Febrero

Se arreglo los últimos detalles de la tesis y dejo lista para impresión

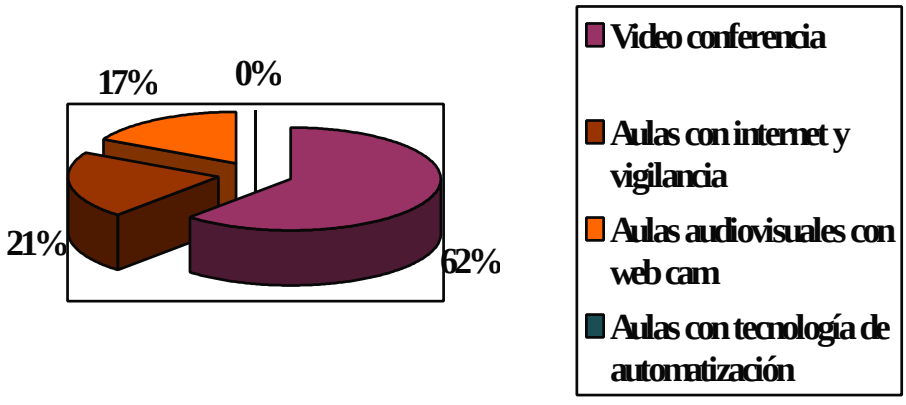
19. CONCLUSIONES

Nos damos cuenta que si este proyecto se llegara a implementar completamente se convertiría en una herramienta muy útil para el control, seguridad y facilidad en áreas de conferencia.

Durante todo el desarrollo hemos logrado integrar conocimientos adquiridos durante estos dos años de estudio, contando de igual manera con ayuda de nuestros catedráticos como también de profesionales externos a la Universidad.

Anexo 1

Usted conoce ¿Qué es un aula inteligente?



Anexo 2

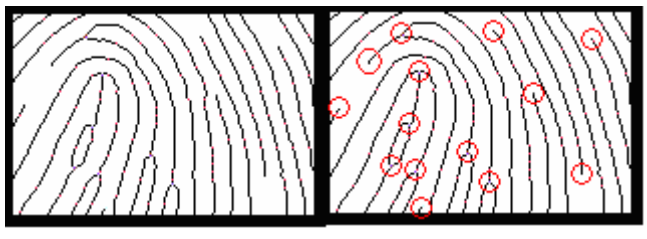
Ridge ending

Ridge bifurcation

Anexo 3

Tipos de formas de huellas dactilares

Anexo 4



Estructura de una huella dactilar

Anexo 5

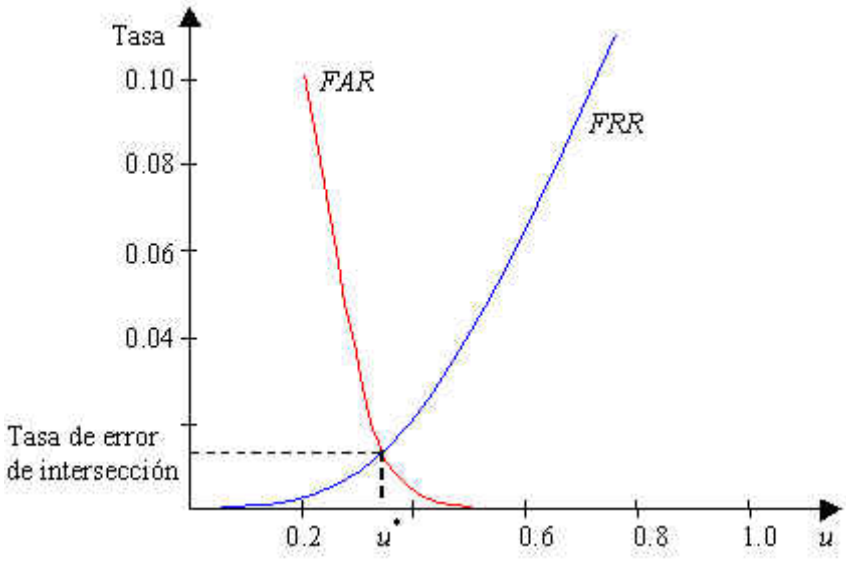
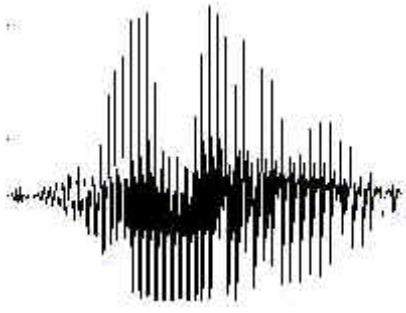


Gráfico FAR y FRR

Anexo 6

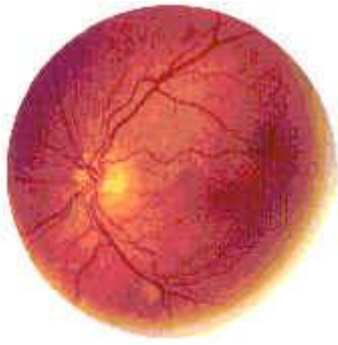


Verificación de voz

Anexo 7

Firma realizada con lápiz óptico

Anexo 8



Pupila

Anexo 9

Iris

Anexo 10

Authentec AS2500

Anexo 11

Infineon Finger Tip

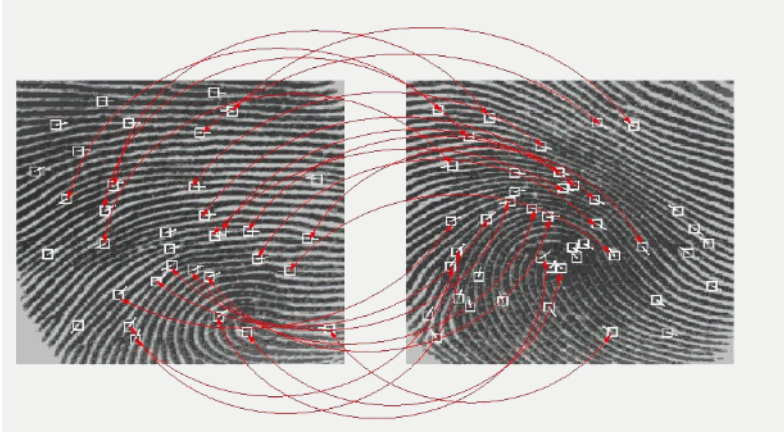
Anexo 12

Veridicom 5th Sense

Anexo 13

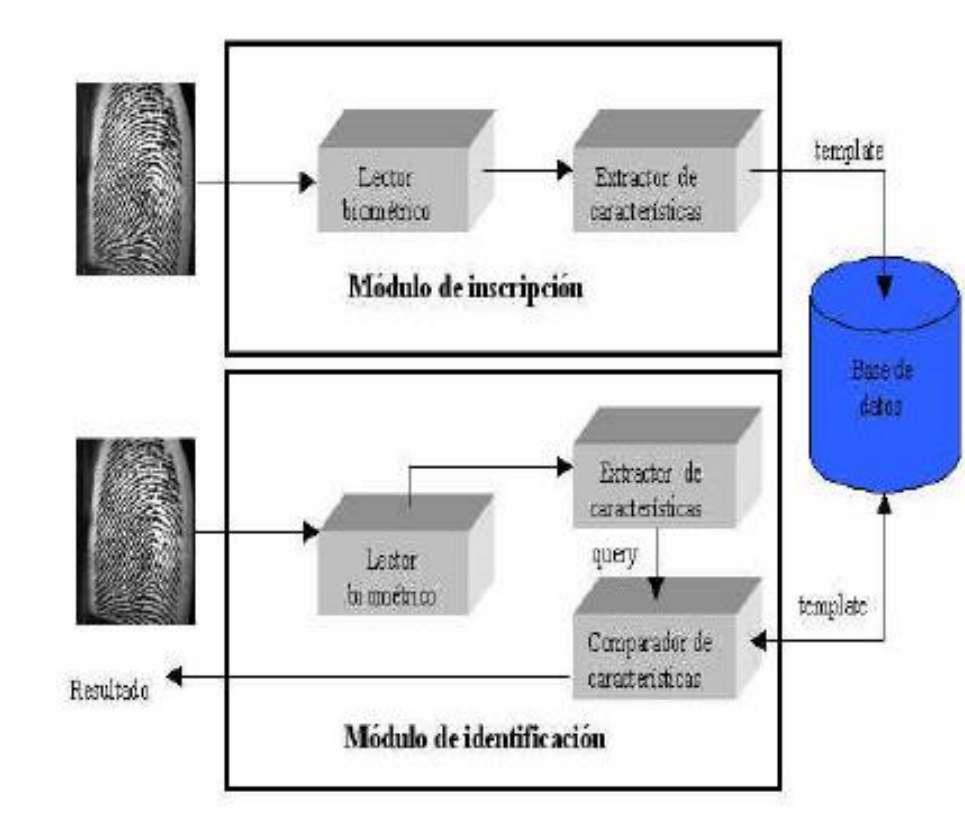
Authentec AES4000

Anexo 14



Proceso de comparación.

Anexo 15

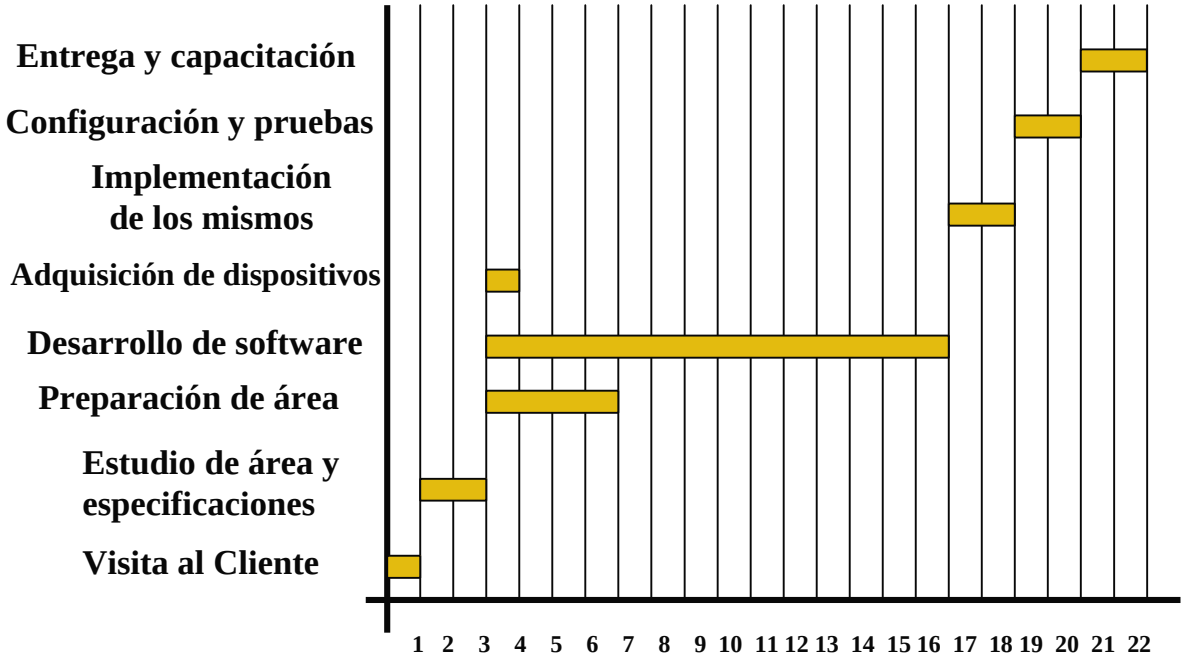


Arquitectura de un sistema biométrico para identificación dactilar

Anexo 16

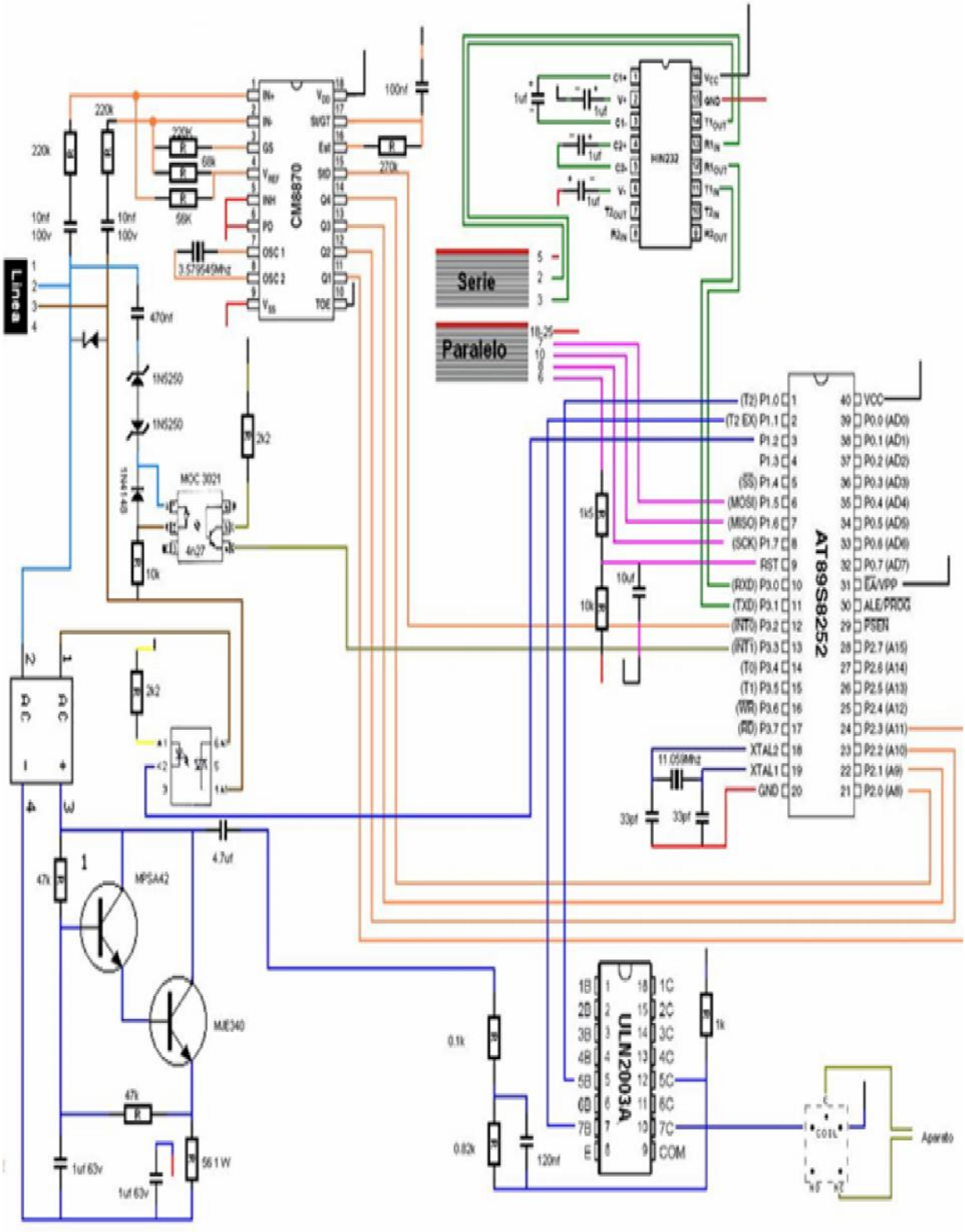
Scanner Biométrico

Anexo 17



Cronograma de implementación

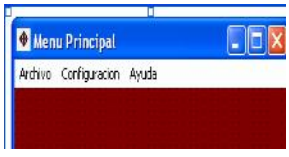
Anexo 18



Diagrama

Anexo 20

Anexo 21



GLOSARIO

Controladora: Dispositivo de interfase entre el computador y otros dispositivos.

Domótica: Casa Inteligente.

Assambler: Lenguaje de máquina de bajo nivel.

Biometría: Ciencia que estudia la variabilidad de los caracteres de herencia de los seres como la altura las huellas, etc.

FRR: Falso rechazo

FAR: Falsa aceptación

Anillo de crestas: Algoritmo que permite clasificar la huella dactilar.

ADN: Siglas del acido desoxirribonucleico depositario de las características genéticas.

Diodo: Componente que consiste en dos electrodos de polaridad opuesta.

Fibra óptica: Cuerpo sintético flexible por cuyo interior se propagan los rayos luminosos.

DSV: Verificación de asignatura dinámica.

CCD: Dispositivo de carga acoplada de miles de elementos individuales (píxeles).

CI: Circuito integrado.

Sensores: Dispositivo capaz de recibir una señal mecánica, acústica, luminosa, calorífica, eléctrica o electrónica**.**

Termoeléctrico: Fenómeno que tiene como efecto transformar la energía térmica en eléctrica o viceversa.

Capacitivo: Impedancia en un circuito.

Hough: Algoritmo de interpretación para un sistema biométrico.

Bitmap: Mapa de bits.

CSV: Formato estándar compatible con Excel, Access, etc.