

ESTUDIO DE FACTIBILIDAD PARA EL CONTROL DE ACCESO BIOMÉTRICO,
EN UNA EMPRESA EMPLEANDO LECTORES DE HUELLA DIGITAL

JORGE ENRIQUE GUTIÉRREZ RICARDO

UNIVERSIDAD DE LA SALLE
ESPECIALIZACION GERENCIA DE PROYECTOS EN INGENIERIA
BOGOTÁ D.C.

2007

ESTUDIO DE FACTIBILIDAD PARA EL CONTROL DE ACCESO BIOMÉTRICO,
EN UNA EMPRESA EMPLEANDO LECTORES DE HUELLA DIGITAL

JORGE ENRIQUE GUTIÉRREZ RICARDO

Proyecto de Grado

UNIVERSIDAD DE LA SALLE
ESPECIALIZACION GERENCIA DE PROYECTOS EN INGENIERIA
BOGOTÁ D.C.

2007

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, enero de 2008

DEDICATORIA

Este trabajo está dedicado a nuestro Padre santo por haberme iluminado a lo largo de esta especialización y colmado de bendiciones.

Quiero dedicárselo a mis padres y familiares, siendo este trabajo un reflejo de un objetivo trazado cuando decidí formarme como gerente de proyectos.

AGRADECIMIENTOS

Los más sinceros agradecimientos para mis padres, que siempre me han apoyado en todo lo que realizo y gracias al esfuerzo de ellos he alcanzado muchas de las metas que me he propuesto.

También agradezco el apoyo de todas las personas que me han colaborado en mi formación como gerente de proyectos y a lo largo de mi vida.

CONTENIDO

	Pág..
LISTA DE TABLAS	i
LISTA DE FIGURAS	ii
INTRODUCCION	1
2. ANTECEDENTES	3
3. DESCRIPCION DEL PROBLEMA	5
4. FORMULACION DEL PROBLEMA	6
5. JUSTIFICACION	7
6. OBJETIVOS	9
6.1 GENERAL	9
6.2 ESPECIFICOS	9
7. ALCANCES DEL PROYECTO	10
8. MARCO REFERENCIAL	11
9. MARCO NORMATIVO	13
9.1 ESTANDAR ANSI / INCITS 358	14
9.2 ESTANDAR NISTIR 6529	14
10. MARCO TEÓRICO	15
10.1 BIOMETRÍA	15
10.1.1 APLICACIONES	24
10.2 FINGER PRINT	25
10.2.1 MEDIDAS DE DESEMPEÑO	29

11. EVALUCION TECNICA	32
11.1 SISTEMA BIOMETRICO.	32
11.2 ANALISIS COMPLETO DE LA ARQUITECTURA BÁSICA DE UN CONTROL DE ACCESO BIOMÉTRICO	35
11.2.1 BASE DE DATOS	38
11.2.2 INTERFAZ DE USUARIO	39
11.2.3 HARDWARE	42
12. ESTUDIO DE MERCADEO	47
12.1 EL PRODUCTO	47
12.1.1 CONTROL DE ACCESO BIOMETRICO	47
12.1.2 INSTALACIÓN Y MANTENIMIENTO	48
12.1.3 PRODUCTOS SUSTITUTIVOS	48
12.1.4 PRODUCTOS COMPLEMENTARIOS	49
12.2 EL CONSUMIDOR	49
12.2.1 POBLACIÓN	49
12.2.2 CONSUMIDORES ACTUALES Y TASA DE CRECIMIENTO	50
12.3 DEMANDA DEL PRODUCTO	51
12.3.1 SITUACION ACTUAL DE LA DEMANDA	51
12.4 OFERTA DEL PRODUCTO	54
12.5 LOS PRECIOS DEL PRODUCTO	56

12.6 COMERCIALIZACIÓN	57
12.6.1 PROMOCIÓN Y PUBLICIDAD	57
12.7 ESTRUCTURA ORGANIZATIVA	58
12.7.1 GERENCIA ADMINISTRATIVA	58
12.7.2 GERENCIA DE VENTAS	59
12.7.3 GERENCIA DE OPERACIONES	59
13. EVALUACION FINANCIERA	61
13.1 MATERIALES	61
13.2 MANO DE OBRA	62
13.3 EVALUACION FINANCIERA	64
13.4 VPN	65
14. CONCLUSIONES	66
BIBLIOGRAFIA	67

LISTA DE TABLAS

	Pág.
TABLA.1 CUADRO COMPARATIVO DE DIFERENTES DISPOSITIVOS LECTORES DE HUELLA	34
TABLA2. MATERIALES DIRECTOS DEL PROCESO PRODUCTIVO	61
TABLA3. ACTIVIDADES Y CARGA LABORAL EN EL PROCESO PRODUCTIVO	62
TABLA4. SALARIO DIARIO	63
TABLA5. ANALISIS DE COSTOS PARA EL PRIMER AÑO	63
TABLA6. ANALISIS FINANCIERO A 5 AÑOS	64

LISTA DE FIGURAS

	Pág.
Figura 1. Huella digital	26
Figura 2. Características de reconocimiento de una huella Digital	28
Figura 3. Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación μ para un sistema biométrico	31
Figura 4. Arquitectura básica de un control de acceso biométrico	32
Figura 5. Dispositivo usado para el proyecto.	33
Figura 6. Diagrama de flujo del sistema.	37
Figura 7. Tabla para registro de visitantes.	38
Figura8. Base de datos creada por el controlador	39
Figura 9. Instalador Biometric Finger Print.	39
Figura 10. Controladores	40
Figura 11. Registro de visitantes.	41
Figura 12. Transmisión serial asíncrona RS-232.	43

Figura 13. Diagrama de pines MAX 232.	44
Figura14. Promedio de empleados en pequeñas empresas.	52
Figura15. Tipo de control de acceso más usado.	53
Figura16. Problemas de control de acceso en las empresas	53
Figura17. Necesidad de las empresas por incrementar la seguridad	54
Figura18. Conocimientos sobre un control de acceso biométrico.	56
Figura19. Aceptación de pago propuesto para implementar un sistema de control biométrico.	57
Figura20. Estructura organizacional	60
Figura21. Evaluación financiera a 5 años	64

INTRODUCCIÓN

Los avances tecnológicos con los que se relaciona la gente hoy en día están sujetos a cambios constantes, por tal razón motivan a las diferentes entidades o personas a estar a la vanguardia. Es importante que una institución este consiente de este avance, compare en que nivel tecnológico esta ubicada y este dispuesta a realizar los cambios necesarios. La tecnología brinda herramientas para establecer distintos niveles de seguridad en industrias, contra fenómenos naturales, seguridad informática e identificación y acceso de personal.

Enfocado con respecto a la identificación y acceso de personal, las compañías están implementando sistemas que facilitan el acceso con información propia de cada usuario, dentro de este campo existen varias alternativas que brindan soluciones para cada una de las necesidades, cabe mencionar métodos como fingerprint (escaneo de la huella digital), escaneo del iris, reconocimiento de voz y reconocimiento a través de tarjetas magnéticas.

La identificación biométrica es uno de los avances más importantes dentro del control y reconocimiento de personal perteneciente a una entidad sin importar su actividad económica, por tal motivo es necesario conocer a qué se refiere cuando se habla de biometría.

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

La biometría es una tecnología basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos.

La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana.

La identificación por medio de huellas digitales constituye una de la forma más representativa de la utilización de la biometría. Una huella digital está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados “puntos de minucia”. Cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intenta acceder a un sistema en general.

Estos avances en la identificación de las huellas han abierto un gran campo en el área de la seguridad. Muchos sistemas requieren el ingreso masivo de personal a instalaciones en donde algunas personas deben acceder o ser restringidas. Los sistemas de identificación dactilar presentan una solución a este problema.

2. ANTECEDENTES

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, parece que en un futuro no muy lejano estos serán los sistemas que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario: son más amigables para el usuario (no va a necesitar recordar *passwords* o números de identificación complejos, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética; las principales razones por la que no se han impuesto ya en nuestros días es su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento.

Dentro de los sistemas de autenticación biométrica se encuentran sistemas basados en verificación de: voz, escritura, huellas, patrones oculares (retina-iris), geometría de la mano, entre otros. Estos sistemas son los denominados **biométricos**, basados en características físicas del usuario a identificar. El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptología se limita aquí a un uso secundario, como el cifrado de una base de datos de patrones retinales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos.

La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Obviamente aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes o sistemas el agente ha de ser un dispositivo

que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado sector.

Dentro de la aplicación de los lectores de huellas digitales se encuentra la apertura de puertas de garajes, cerraduras que ya no necesitan de una llave sino de un lector biométrico, la restricción el acceso del personal de una oficina a determinadas habitaciones, el control de entrada y salida de personal, el control de acceso a computadores y servidores, la gestión de acceso de los socios a clubes y sus de pendencias.

3. DESCRIPCIÓN DEL PROBLEMA

Actualmente para las pequeñas empresas el control de acceso de personal es realizado manualmente o podría decirse artesanalmente teniendo en la entrada (puerta de ingreso a las instalaciones) un vigilante; la cantidad de personas empleadas y no empleadas que ingresan a sus instalaciones puede ser muy elevado en el día. Para que el vigilante pueda diferenciar que personas tiene acceso autorizado o no a las instalaciones el usuario debe presentar su carné siendo el reconocimiento visual la principal forma de control de acceso de los empleados. Para controlar la hora de ingreso de los empleados existe el método de marcación de tarjeta quien con un reloj mecánico sella la hora de la entrada del personal este mismo proceso se realiza para la salida, para el visitante que va a ingresar a las instalaciones, el vigilante realiza una llamada a la oficina hacia la cual se dirige para que autoricen su ingreso, si este es autorizado se registra en una planilla de visitantes el nombre del mismo. De hecho en algunos casos sólo se registra el nombre del visitante, si este viene en vehículo, si no es el caso sólo se pide la autorización para controlar el acceso del personal a las áreas restringidas.

Este proceso de verificar que los empleados cumplan con los horarios establecidos es lento, e inseguro dada esa información está almacenada en planillas que pueden llegar a ser cientos de hojas en un mes y que no presenta ningún tipo de organización de datos, además que no es veraz que la hora de ingreso y salida plasmada en éstas planillas sea real. No es confiable porque el personal encargado del control de acceso (vigilante) carece de información detallada de los usuarios para determinar quienes tienen acceso y quiénes no. Cuando se producen los cambios de turno, y un vigilante o recepcionista es nuevo, este no tiene la capacidad de saber que personas tienen autorizado el ingreso y sólo con el tiempo puede dominar la técnica del reconocimiento visual. Entonces el sistema actual no proporciona información detallada y organizada del personal que hace parte de la institución.

El sistema es inseguro porque no tiene la capacidad de determinar con exactitud cuántas personas en total (empleados + no empleados) se encuentran dentro de las instalaciones de la institución, además no se tiene un registro histórico organizado de las personas ajenas al plantel (visitantes) que ingresaron a las instalaciones, que permita determinar o analizar la situación en caso de una eventualidad que afecte la seguridad de la compañía.

En la actualidad, existen muchos sistemas de control de acceso de personal, como los que se nombran a continuación: lectoras por código de barras, banda magnética, teclado PIN, biométricos. Las medianas empresas no acceden a adquirir estos tipos de sistema debido a que es muy costoso si se tiene en cuenta la relación costo–beneficio de instalar u operar dicho sistema.

4. FORMULACIÓN DEL PROBLEMA

¿Es factible desarrollar un sistema de control de acceso por medio de identificación biométrica, para el personal perteneciente a una pequeña empresa empleando lectores de huella digital?

5. JUSTIFICACIÓN

Los requerimientos primordiales de los sistemas informáticos que desempeñan tareas importantes son los mecanismos de seguridad adecuados a las dependencias que se intenta proteger; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos activos del sistema, generalmente usuarios) que intentan acceder a los objetos (la empresa en si), mediante un proceso de identificación dactilar.

Los sistemas que habitualmente utilizan los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, sino autenticar que esa persona es quien dice ser realmente.

Los métodos de autenticación se suelen dividir en tres grandes categorías, en función de lo que utilizan para la verificación de identidad: A. algo que el usuario sabe, B. algo que éste posee, y C. una característica física del usuario o un acto involuntario del mismo. Esta última categoría se conoce con el nombre de autenticación biométrica.

Ejemplos de estos mismos son: un *pass Word* es algo que el usuario conoce y el resto de personas no, una tarjeta de identidad es algo que el usuario lleva consigo, la huella dactilar es una característica física del usuario.

Cualquier sistema de identificación ha de poseer unas determinadas características para ser viable; obviamente, ha de ser fiable con una probabilidad muy elevada (tasas de fallo de 10^{-4} en los sistemas menos seguros), económicamente factible para la organización, ha de soportar con éxito cierto tipo

de ataques (por ejemplo, cualquier persona que pueda descifrar el *pass Word de algún usuario*).

Las técnicas de password son de una vulnerabilidad alta, las tarjetas magnéticas y de proximidad pueden ser utilizadas para suplantación de personas o falsificación de la tarjeta.

Cabe recordar que el diseño de un control de acceso utilizando alguno de los métodos antes mencionados, se usa simplemente para validar o no a un usuario es hay donde se ve la importancia del diseño que se quiere implementar, es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico.

Se hace necesario ver la factibilidad de diseñar y sacar al mercado un sistema que solucione problemas cotidianos a la entrada de la las organizaciones pequeñas tales como: el control de acceso de personal al plantel es lento, sin registro alguno y sometido a errores humanos.

Al implementar un sistema de control de acceso por medio de identificación biométrica, las pequeñas empresas ofrecerán un ambiente confiable, seguro e integro para los empleados que hacen parte del plantel.

6. OBJETIVOS

6.1 GENERAL

Realizar un estudio de factibilidad para comercializar el control de acceso biométrico, teniendo en cuenta costos, instalación y mantenimiento de este tipo de acceso.

6.2 ESPECÍFICOS

- Identificar a través de un estudio técnico, el desarrollo de un software compuesto por: Una Base de datos, motor de búsqueda, reconocimiento y validación de los usuarios según sus propios datos.
- Determinar los costos sobre el desarrollo de este tipo de control de acceso, teniendo en cuenta la fiabilidad del método escogido.
- Identificar las principales normas existentes sobre este tipo de control de acceso.
- Determinar a través de un estudio de mercadeo para ver la factibilidad de la comercialización de este tipo de control de acceso.

7. ALCANCES DEL PROYECTO

Este estudio proveerá información de factibilidad, técnica, económica y normativa sobre el producto propuesto.

En el estudio técnico se propone el control de acceso a dos (2) tipos de usuarios:

- Control de acceso a personal perteneciente a la entidad
- Ingreso de visitantes.

En el estudio del control de acceso biométrico se requiere adquirir conocimientos de tecnologías que vienen siendo implementadas desde hace varios años que permiten escoger una serie de alternativas que guiarán al proyecto por el camino más viable sin incurrir en lo exagerado dando como escogido métodos que no puedan estar al alcance de quienes pretenden desarrollarlo, permitiendo motivar el empleo de estos métodos en las instituciones que lo requieran.

Dentro de las ventajas en la implementación del control de acceso biométrico encontramos:

- Elimina suplantaciones de identidad de los empleados, controlando el ingreso de personas no autorizadas a la entidad.
- Organiza las horas de ingreso y salida de los empleados.
- Disminuye costos de funcionamiento.
- No existe riesgo de falsificación.
- El medio de identificación es única y personal.
- Método seguro de identificación, pues no existe dos huellas digitales iguales en el mundo.
- Bajo costo de implementación permitiendo instalaciones en ciertas etapas interactuando con otros tipos de controles de seguridad.

8. MARCO REFERENCIAL

Dentro de los términos más relevantes que se mencionan en el desarrollo de este diseño se encuentra el significado de la biometría que no es más que la medida de un patrón único en cada ser humano para este caso será la huella digital.

La criptografía que es un método milenario utilizado en las tecnologías actuales para “disfrazar” datos a los que solamente cierta cantidad de personas podrá tener acceso por medio del cifrado de los datos en cuestión.

Cuando se hace referencia a los dispositivos captadores son aquellos encargados del reconocimiento de la huella y envío de los datos con los que el usuario se validará o no dentro de la entidad, este dispositivo hace parte del hardware o parte física del cual se compone el control de acceso.

Por otra parte, es importante hablar sobre el hardware y el software, que en este caso es la parte lógica o intangible del prototipo dentro de este se encuentra la base de datos, motores de búsqueda (encargado de buscar y comparar en la base de datos el tren de bits proveniente del lector de huellas) y programa para la inserción de cada huella digital.

Para que exista una debida transferencia de datos entre el software y el hardware es necesario la utilización de protocolos de comunicación que se encargan de que ambas partes se entiendan, realizando la transferencia de diferentes niveles de voltaje a niveles de lógicos de 0 voltios (nivel bajo) y 5 voltios (nivel alto) así se garantiza que se lleven a cabo las acciones para las que el sistema fue diseñado.

También se puede encontrar los elementos actuadores finales que se encargan del accionamiento de motores, electroimanes o solenoides para el movimiento de las barreras físicas, las cuales impiden que alguien pueda entrar a la entidad sin

antes hacer su reconocimiento, estas barreras físicas se conocen con el nombre de barreras de seguridad (peatonal y vehicular), para este caso en específico.

Otro concepto de gran importancia dentro de los sistemas de seguridad basados en identificación biométrica son los dispositivos de señalización audio-visual que permiten al usuario conocer en que estado esta el proceso de validación para su acceso. Se hace referencia a dispositivos que generan señales lumínicas (semáforo) y auditivas (buzzer), así el usuario puede reconocer si su validación dentro del sistema fue exitosa o no.

El software y el hardware siempre estarán interactuando uno con respecto al otro, esto quiere decir que si uno falla el otro también y todo el sistema saldrá de su correcto funcionamiento.

Para determinar una pequeña empresa En Colombia la ley 905 y 504 de Mipymes hacen referencia a la clasificación de las empresas en el país según su dimensión.

Los principales indicadores son: el capital propio, número de trabajadores. El más utilizado suele ser según el número de trabajadores. Este criterio delimita la magnitud de las empresas de esta forma:

Microempresa si posee menos de 10 trabajadores.

Pequeña empresa: si tiene menos de 50 trabajadores.

Mediana empresa: si tiene un número entre 50 y 250 trabajadores.

Gran empresa: si posee más de 250 trabajadores.

9. MARCO NORMATIVO

En los últimos años se ha notado una preocupación creciente por las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas. Esta preocupación es reflejo del creciente interés industrial por este ámbito tecnológico, y a los múltiples beneficios que su uso aporta. No obstante, la estandarización continua siendo deficiente y como resultado de esto, los proveedores de soluciones biométricas continúan suministrando interfaces de software propios para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor.

A nivel mundial el principal organismo que coordina las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC).

En Estados Unidos desempeñan un papel similar el Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el American National Standards Institute (ANSI).

Existen además otros organismos no gubernamentales impulsando iniciativas en biometría tales como: Biometrics Consortium, International Biometrics Groups y BioAPI (este último compuesto por las empresas Bioscrypt, Compaq, Iridium, Infineon, NIST, Saflink y Unisis).

Los estándares más importantes son: Estándar ANSI X.9.84 Estándar creado en el año 2001, por la ANSI (American National Standards Institute) y actualizado en el año 2003, define las condiciones de los sistemas biométricos para la industria de

servicios financieros haciendo referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.

9.1 Estándar ANSI / INCITS 358

Estándar creado en el año 2002 por ANSI y BioApi Consortium, que presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.

9.2 Estándar NISTIR 6529

También conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en el año 1999 por NIST y Biometrics Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica. El Common Biometric Exchange File Format (CBEFF) describe un conjunto de elementos de información necesarios para dar soporte a tecnologías biométricas de forma común. Esta información puede ser ubicada en un solo archivo para intercambiar información biométrica entre diferentes componentes de sistemas o entre sistemas. El resultado promueve interoperabilidad de programas de aplicación basados en biometría y sistemas desarrollados por diferentes vendedores para permitir intercambio de información biométrica. El concepto inicial de CBEFF fue logrado a través de una serie de tres talleres co-patrocinados por National Institute of Standards and Technology y Biometric Consortium. A partir de estos tres talleres, se creó CBEFF, en coordinación con organizaciones industriales (the BioAPI Consortium, X9.F4 Working Group, International Biometric Industry Association e Interfaces Group of TeleTrust) y usuarios finales. Las aplicaciones de CBEFF simplifican integración de software y hardware proporcionado por diferentes vendedores.

10. MARCO TEÓRICO

10.1 BIOMETRÍA

Los orígenes de la biometría se remontan a los años setenta, cuando la empresa NEC comienza a trabajar junto al FBI en algunos estudios de como automatizar biométricamente algunas características del ser humano. De esa forma se comienzan a desarrollar una serie de algoritmos matemáticos con la finalidad de representar, por ejemplo, una huella dactilar. Cabe mencionar que aun no se ha comprobado que existan dos huellas digitales totalmente iguales.

Estos sistemas incluyen un dispositivo de captación que en segundos obtiene una muestra biométrica de la persona y la compara con una base de datos, donde se analiza si corresponde o no a la identidad de la persona en cuestión.

La inserción de todas estas tecnologías y métodos totalmente automáticos genera cambios en la manera de vivir de las personas es el caso, que cuando se desee verificar un saldo en una cuenta bancaria se acude a Internet y entrando con un usuario y unas claves se puede ver el estado de cuenta, cuando es necesario pagar servicios como la luz eléctrica se acude a la página de Internet y realizando una transferencia con unas claves secretas se puede realizar el movimiento. Todo esto quiere decir que la gente que desee moverse para realizar una serie de actividades se vera en la obligación de utilizar claves o agentes que permitan la identificación dentro de un sistema. Para que todas estas operaciones funcionen a la perfección se necesitan algunas herramientas adicionales como la encriptación, el cifrado, la firma digital, las cuales permiten obtener la certeza necesaria para continuar validado dentro las diferentes partes que exigen una confirmación.

La forma en que el mundo ha ido automatizándose ha sido a través de los sistemas de seguridad donde la prioridad de los sectores industriales en el mundo ha ido cambiando de tal forma que la eficiencia y la efectividad ha sido enfocadas

en la medida que se posea un buen sistema de computo para prestar mejor servicio, así es cómo los sistemas de seguridad han ido evolucionando de lo digital a lo biométrico.

Para proteger la privacidad de las personas ha sido necesario idear toda una nueva infraestructura que aunque ha costado millones de dólares, en estos momentos se están desarrollando tecnologías basadas en la biometría como pueden ser los patrones de las huellas digitales, del iris, del tono de voz, entre otros.

Los sistemas biométricos de seguridad están basados en documentos, archivos de información relacionada a la identificación de las personas, estableciendo los patrones necesarios para el desarrollo de esta tecnología. Estos métodos biométricos ya son utilizados en varios ámbitos y principalmente con el propósito de reemplazar a los ya existentes como passwords, tarjetas de crédito, consultas bancarias en cajeros automáticos etc.

La biometría toma en cuenta elementos morfológicos únicos y propios de cada persona.

El desarrollo tecnológico de la mano con el aumento incesante de las comunicaciones; tanto en volumen como en diversidad, conlleva a la necesidad de asegurar la identidad de los usuarios en los accesos locales y remotos a los datos informatizados. La importancia y valor de estos datos manejados, motiva a los delincuentes a superar los sistemas de seguridad existentes, lo que obliga a los usuarios a instalar nuevos sistemas cada vez más potentes y fiables.

Estas necesidades de autenticación y seguridad, unidas a las ya existentes anteriormente en materia de seguridad de accesos físicos, han determinado un interés creciente por los sistemas electrónicos de identificación y autenticación.

Su denominador común es la necesidad de que sean medios simples, prácticos y fiables, para verificar la identidad de una persona.

El mercado de los controles de acceso se abrió con el crecimiento de los sistemas, pero ninguno a tenido un resultado eficaz contra el fraude, porque todos utilizan un elemento externo como pueden ser las tarjetas de identificación, llaves, claves etc.

Es frecuente olvidar una clave de acceso. Para evitar estos olvidos, se suele anotar esta clave en agendas o cuadernos, perdiendo así toda confidencialidad. La contraseña o clave es un método de pre-selección y no de control de acceso eficaz.

Existen varios sistemas para verificar la identidad de un individuo, sin embargo la biometría se considera como el método más apropiado, ya que ciertos rasgos de cada persona, son inherentes a ella y sólo a ella.

La biometría permite una autenticación segura, al contrario del empleo de contraseñas o tarjetas, ya que estos últimos pueden ser robados o utilizados por personas no autorizadas.

La combinación de los últimos avances en biometría y en electrónica ha permitido el desarrollo de las más modernas soluciones. La biometría son técnicas que permiten establecer una relación entre una persona y un determinado patrón asociado a ella de forma segura e intransferible.

Utiliza la información biológica para autenticar la identidad. La idea básica es que nuestros cuerpos contienen características únicas, como ya sabemos se puede utilizar para distinguirnos de los demás

Los sistemas biométricos se basan en características o rasgos físicos medibles ó personales de comportamiento, los cuáles son usados para reconocer o verificar la identidad de una persona a través de medios automáticos.

Un indicador biométrico es alguna característica con la cual se puede realizar biometría, cualquiera que sea el indicador debe cumplir con los siguientes requerimientos¹:

- Universalidad, lo cual significa que cada persona debe de tener esas características.
- Unicidad, lo cual significa que dos personas no deben de ser la misma en términos de las características.
- Permanencia, lo cual indica que las características deben ser invariantes con el tiempo.
- Colectibilidad, lo cuál indica que las características pueden ser medibles cuantitativamente.

Las Funciones de los sistemas biométricos son²:

- Verificación ¿es el usuario que dice ser?
- Identificación ¿Quién es?

Se puede hacer Reconocimiento automático de individuos empleando:

- Características fisiológicas que son medidas físicas de partes del cuerpo humano
- Características de comportamiento que son cómo realiza cada persona determinadas acciones.

¹ Zdenek Ríha, Václav Matyáš, Biometric Authentication Systems, año 2000, FIMU, Republica Checa, Pagina 35, 36

² Nalini Ratha, Ruud Bolle, Automatic Finger Print Recognition System, EDITORS, pags 55, 56, 57.

Se puede decir que la persona es “la llave” para poder acceder a un sistema.

Existen Dos tipos de métodos de reconocimiento, colaborativos y no colaborativos.

Sistemas de autenticación biométrica. Donde el usuario está informado de la presencia de un sistema biométrico. Es necesario que esté familiarizado con él y debe decidir utilizarlo o no³, dentro de estas clases se encuentra:

- Huella dactilar
- Retina
- ADN
- Geometría de la Mano
- Palma de la mano
- Forma de andar
- Temperatura corporal
- Tecleo
- Características faciales
- Iris
- Voz

Huella dactilar. Su primer uso conocido se remonta a la Antigua Babilonia, donde los reyes firmaban las tabletas de arcilla grabando las yemas de sus dedos antes de cocerlas. Más tarde, en China, durante la Dinastía Tangen el año 650 d.C., se estableció que para divorciarse de una mujer, el marido debía exponer siete motivos y firmar el documento con las huellas dactilares. También en la India se empezó a emplear pronto esta marca en documentos legales⁴.

El Reconocimiento de huella dactilar se basa en la extracción de características de la huella. Se realiza comparando los surcos y estrías de la yema de nuestros

³ <http://www.tiendalinux.com>, Autenticación de usuarios, Marzo 15 de 2006-9:30 pm.

⁴ Luis Moran, Sistema de detección de huella digital, 2002, Mexico, pag 31.

dedos, y los puntos en los que estos terminan o se bifurcan. Este sistema tiene una presencia en el mercado de aproximadamente el 48%.

Ventajas:

- Pequeña variabilidad en el tiempo
- Buena precisión, tiene una Fiabilidad de 1 en 64.000 millones son iguales

Inconvenientes:

- Se asocia a temas penales
- No aporta información adicional

Reconocimiento facial. Es la Extracción de características de la cara, analizando el rostro en función de ciertos puntos claves, se obtiene una plantilla única que permite autenticar a una persona de forma precisa y este análisis se puede hacer, geométrico e información de textura y forma⁵.

Se pueden distinguir una serie de puntos claves en un rostro: Distancia entre los ojos, anchura de la nariz, profundidad de la cuenca del ojo, pómulos, línea del mentón, barbilla.

Su proceso va unido a un sistema de video vigilancia, Una vez detectada una cara, el sistema determina la posición, el tamaño y la posición de la cabeza, La imagen de la cabeza se parametriza y se rota para poderla poner en un tamaño apropiado. La normalización se realiza sin importar la localización y la distancia de la cabeza a la cámara fotográfica. La luz no afecta el proceso de la normalización, el sistema traduce los datos faciales a un código único, este proceso de codificación permite una comparación más fácil de los datos faciales adquiridos con los datos faciales almacenados, los datos faciales adquiridos se comparan

⁵ Nalini Ratha, Ruud Bolle, Automatic Finger Print Recognition System, EDITORS, pag 26.

con los datos almacenados y se relacionan con al menos una representación facial almacenada.

Ventajas:

- Puede ser no colaborativo
- Aporta información adicional de expresión, estado de ánimo.
- Es comprobable por un operador humano

Inconvenientes:

- Muy dependiente de iluminación
- Puede ser variable con el tiempo

Análisis de la mano. Es el Reconocimiento de las Características de la mano especialmente de la palma. La identificación se realiza midiendo las características físicas de la mano y dedos desde una perspectiva 3D. Este sistema tiene una presencia en el mercado de un 11%. Las características pueden ser: Geométricas e información de textura y forma.

En el procedimiento se transforman en una serie de patrones numéricos las características de la mano (grosor y localización de las venas) y de algunos dedos (longitudes, anchuras, altura) luego estos patrones se comparan en una base de datos⁶.

Ventajas:

- Poco intrusivo.
- Procesamiento muy rápido.

Inconvenientes:

- Dispositivos de lectura de tamaño medio.

⁶ Luis Moran, Sistema de detección de huella digital, 2002, México, Pág. 29.

El ojo. La franja de tejido coloreada que rodea nuestra pupila, muestra un conjunto de rasgos característicos que forman un patrón exclusivo para cada individuo. Tiene una Fiabilidad de 1 entre 1078 para que sean iguales y su Presencia en el mercado es del 9%⁷.

- Escáner de retina. Es la extracción de características de las venas del fondo del ojo se puede hacer mediante: Iluminación del fondo del ojo a través de la pupila mediante luz infrarroja, información de la forma de las venas en el fondo del ojo.

Ventajas:

- Alta seguridad

Inconvenientes:

- Es muy preciso pero se considera intrusivo(viola la privacidad)
- Lectura interna del fondo del ojo.

- Reconocimiento por iris. Es la Extracción de características de la textura del iris. En 11 milímetros de diámetro cada iris concentra más de 400 características. Rasgos, surcos radiales, Zona pupilar, borde pigmentado, zona Ciliar, collarete y criptas.

Para obtener estas características una cámara escanea el iris y genera una imagen que es analizada por medio de los algoritmos de Daugman para obtener el código del iris (IrisCode). Éste código ocupa solo 256 bytes, luego es buscada en una basa de datos donde encuentra un código homólogo⁸.

⁷ Luís Moran, Sistema de detección de huella digital, 2002, México, Pág. 29, 30.

⁸ Zdenek Ríha, Václav Matyáš, Biometric Authentication Systems, año 2000, FIMU, Republica Checa, Pagina 18-21

Ventajas:

- No se ha reportado ninguna falsa aceptación.
- Podría llegar a dar información adicional (Iridología).
- Podría llegar a ser no colaborativo.

Inconvenientes:

- Intrusivo.
- Todos los sistemas de reconocimiento de iris dependen de la calidad con la que se capte la imagen del iris.
- Dependen de la cooperación del usuario para capturar una imagen del iris de buena calidad.

La voz. La diferencia con otras medidas biométricas reside en la necesidad de tomar varias muestras diferentes, ya que la voz varía dependiendo de la situación, puede verse influenciado por una congestión nasal, por ejemplo. Es susceptible al engaño si se producen grabaciones. Su fiabilidad se encuentra por debajo de otros sistemas biométricos.

En el proceso se estudia el timbre, intensidad y frecuencia, acumulando esta medición con la situación en la que se toma la muestra nos referimos a que puede ser difusa en el sentido de que debemos evaluar el estado de ánimo de la persona, alegre, con un tono sensual o simplemente enfado⁹.

⁹ Zdenek Ríha, Václav Matyáš, Biometric Authentication Systems, año 2000, FIMU, Republica Checa, Pagina 28

Otras técnicas de sistemas biométricos. Donde el usuario no tiene que realizar ninguna acción. El sistema puede no ser detectado por el usuario. Resulta mucho más cómodo para el usuario. El sistema puede extraer las características biométricas del usuario a distancia.

Nuevos métodos.

- Análisis facial termográfico.
- Análisis facial Tridimensional.
- Análisis por geometría de la oreja.

10.1.1 APLICACIONES.

- Seguridad en la movilidad y accesos
- Aeropuertos, fronteras, centrales eléctricas, centros de control de suministro, instalaciones industriales, instituciones públicas, control hospitalario de neonatos.
- Seguridad en las transacciones en el comercio electrónico y banca.
- Cajeros automáticos, verificación de uso de tarjetas de crédito en comercios, pago por Internet
- Seguridad en el acceso y firma de documentos electrónicos
- Sector sanitario, industrial, administración pública, comercio, actas notariales.
- Validación de firma digital, sistemas de voto electrónico y voto por Internet.
- Seguridad en el acceso a equipos industriales.
- Maquinaria que sólo deba ser utilizada por personal específicamente formado.

10.2 FINGER PRINT.

El nacimiento de las técnicas de identificación a través de las huellas dactilares, a pesar de transcurrido el tiempo es la herramienta más eficaz para la identificación de personas.

“La utilidad de la huella digital aparece gracias a que un científico que se encontraba en Japón, se le ocurre tomar muestras de las personas que habitaban el poblado para compararlas con otras huellas obtenidas en unas excavaciones arqueológicas, el investigador Henry Faulds pretendía determinar la antigüedad de las excavaciones sin embargo logra detectar que las huellas son diferentes en cada persona independientemente de su raza. Los pobladores cuentan que algunos pobladores lograron robarle algunas pertenencias y Faulds gracias al banco de huellas que tenía en su poder pudo descubrir a los ladrones.”¹⁰

Junto a esta forma de identificación han surgido el ADN y el iris en el ojo, cómo otras formas adicionales para corroborar las identidades.

Un sistema biométrico en particular es aquel que utiliza la huella dactilar. Esta huella representa un patrón único de identificación entre las personas, aun entre gemelos. Este patrón conserva la misma forma desde la formación del feto hasta la muerte de la persona con esto satisface las características de los sistemas biométricos. Estas características representan un medio más robusto y confiable para un sistema de seguridad.

Con el incremento del procesamiento de los computadores se han ido desarrollando sistemas automatizados para realizar la clasificación e identificación de huellas dactilares. Básicamente los sistemas biométricos basados en huellas dactilares son de dos tipos:

¹⁰ <http://www.homini.com>, 10 de Marzo de 2006

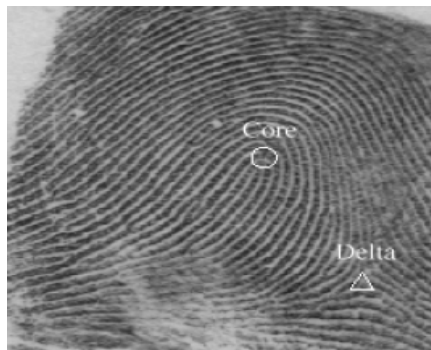
- Automatic Fingerprint Authentication System (AFAS).
- Automatic Fingerprint Identification System (AFIS).

En un AFAS la entrada es la identidad de la persona y la imagen de la huella dactilar de esa persona; y la salida es una respuesta de si ó no, indicando si la imagen de entrada pertenece a la persona cuya identidad es proporcionada.

En un AFIS la entrada es solo la imagen de la huella dactilar y la salida es una lista de identidades de personas que pueden tener la huella dada, además de una puntuación de cada identidad indicando el grado de similaridad entre ésta y la huella dada.

Ambos sistemas utilizan los detalles formados en las huellas dactilares. Estos detalles llamados “rizados” son definidos como un segmento de curva simple. La combinación de varios rizados forma un patrón de huella dactilar. Las pequeñas características formadas por el cruce y terminación de rizados son llamadas minucias. Además de las minucias, las huellas dactilares contienen dos tipos especiales de rasgos llamados puntos core y delta como se ve en la figura.

Figura 1. Huella digital



<http://www.idex.com/>.

Estos puntos son referidos como los puntos de singularidad de una huella dactilar.

El punto core es definido como el punto mas alto en el rizado curvo mas interior.

Este punto es generalmente usado como punto de referencia para la codificación de minucias.

Etapas del proceso:

- Medición de minucias.
- Emparejado.
- Filtrado y binarización.
- Comparación (verificación identidad).
- Parametrización y búsqueda (identificación).

La huella dactilar presenta líneas paralelas que se curvan, se unen entre ellas, se cortan bruscamente. La identificación se va a realizar observando tales puntos singulares. De tales puntos, los que más importan son aquellos donde: Se acaba una línea y se bifurca una línea.

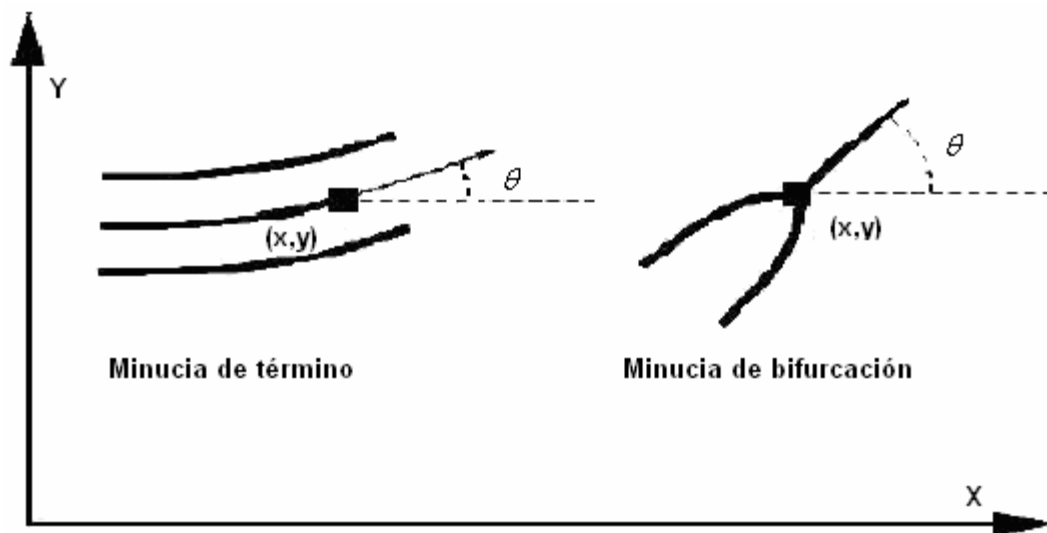
A ambos tipos de puntos se les llama minucias. El motivo por el que tanto nos interesan es que entre los dos suman casi el 80 % de los puntos singulares antes enumerados. En concreto, las terminaciones de línea representan el 60.6 % de puntos singulares mientras que las bifurcaciones de rizado representan el 17.9 % de tales puntos. A una minucia se le atribuyen dos características:

La posición: La cual la denotaremos con dos coordenadas (x, y), la orientación: La cual cuantificaremos como el ángulo comprendido entre la horizontal hacia la

derecha y la prolongación del rizado con sentido positivo en contra de las agujas del reloj¹¹.

En la figura 2 vemos claramente dichas mediciones en los dos tipos de minucias θ .

Figura 2. Características de reconocimiento de una huella digital



www.idex.com

¹¹ <http://www.idex.com>, 10 de Marzo de 2006

10.2.1 MEDIDAS DE DESEMPEÑO.

La información provista por las huellas permite particionar la 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 alguna huella en la base de datos. Sin embargo, las huellas 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 se posee 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 de persona autorizada es aceptada y un impostor es rechazado son correctas, mientras que las salidas restantes no lo son. El grado de confianza 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:

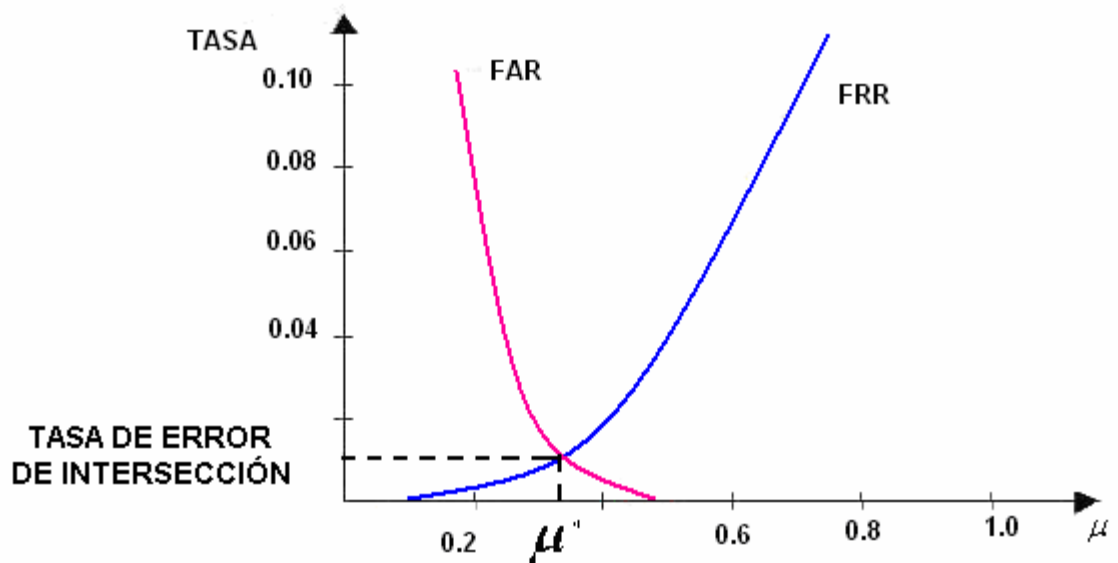
- Tasa de falsa aceptación (*FAR*: False Acceptance Rate). Se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado.
- Tasa de falso rechazo (*FRR*: False Rejection Rate). Definida como la frecuencia relativa con que un individuo autorizado es rechazado como 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 figura. El grado de seguridad deseado se define mediante el umbral de aceptación (μ), un número real perteneciente al intervalo $[0,1]$ que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

Figura 3. Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación μ para un sistema biométrico



Zdenek Ríha, Václav Matyáš, Biometric Authentication Systems, año 2000, FIMU, Republica Checa, Pagina 8.

La FRR es una función estrictamente creciente y la FAR una estrictamente decreciente en U . La FAR y la FRR al ser modeladas como función del umbral de aceptación tienen por dominio al intervalo real $[0,1]$, que es además su recorrido, puesto que representan frecuencias relativas. La figura anterior muestra una gráfica típica de la FRR y la FAR como funciones de U . En esta figura puede apreciarse un umbral de aceptación particular, denotado por u^* , donde la FRR y la FAR toman el mismo valor. Este valor recibe el nombre de tasa de error de intersección (cross-over error rate) y puede ser utilizado como medida única para caracterizar el grado de seguridad de un sistema biométrico. En la práctica, sin embargo, es usual expresar los requerimientos de desempeño del sistema, tanto para verificación como para identificación, mediante la FAR. Usualmente se elige un umbral de aceptación por debajo de u^* con el objeto de reducir la FAR, en forma insignificante en relación del aumento de la FRR.

11. EVALUCION TECNICA

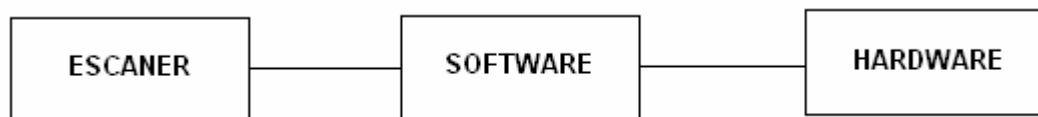
Existen diferentes métodos para desarrollar soluciones de control de acceso en este caso acceso a un sector, las características que hacen parte de estas soluciones cambian unas con respecto a las otras por este motivo no todas son las más óptimas o menos vulnerables, dentro de estos métodos se encuentran los lectores de códigos barras, validación por medio tarjetas magnéticas, tarjetas inteligentes y tarjetas de proximidad. La mayoría están reemplazándose, pues ahora se implementan sistemas que brindan un mayor grado de seguridad en comparación con sistemas que no son eficientes y se prestan a una vulnerabilidad mayor, puesto que todas necesitan de un papel o cartón plástico para la autenticación, Los elementos físicos a los que se hace referencia están expuestos a hurtos o pérdidas ocasionales esto conlleva a suplantaciones de persona.

El grupo se enfocó en un sistema de control de acceso biométrico debido a que este posee un grado de vulneración muy bajo, ya que el carné o llave de acceso la tenemos incorporada dentro de nosotros o es propia de cada uno, este sistema tiene un costo razonable teniendo en cuenta el nivel de seguridad que se presta.

11.1 SISTEMA BIOMETRICO.

El sistema de control de acceso biométrico que se desarrolló consta de tres componentes básicos como se muestra en la figura:

Figura 4. Arquitectura básica de un control de acceso biométrico



El escáner. Este dispositivo se encarga de la adquisición analógica-digital de un indicador biométrico de una persona, en particular la huella digital.

Actualmente el mercado ofrece una gran variedad de lectores de huella digital que van desde pequeñas aplicaciones hasta dispositivos robustos.

El escáner escogido es fabricado por Digitalpersona y se utiliza en pequeñas aplicaciones como validación en sitios Web, acceso a cuentas de usuario, etc.

Figura 5. Dispositivo usado para el proyecto.



www.digitalpersona.com

Ofrece grandes ventajas como el reconocimiento de los patrones de huella en un lapso de tiempo corto, interfaz compatible con puertos USB, sistema operativo comercial (Microsoft Windows® XP Professional Edition/Home Edition/Media Center Edition/Tablet PC Edition), su tamaño es reducido y permite facilidad de instalación en recintos, realiza un escaneo óptico y un switcheo rápido entre usuarios.

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

La forma en que se captura la imagen para posteriormente vectorizarla y generar su código, se genera internamente en conjunción con el drive del dispositivo, la captura se realiza al presionar el dedo sobre la parte sensible y una vez detectada la presión sobre el se realiza el escaneo.

Una vez realizada la operación completa se genera un código de 901 caracteres que será de hoy en adelante el código para el reconocimiento de la huella digital que se capturó. Estos 901 caracteres representan la interpretación de todos y cada uno de los elementos que integran a la huella digital capturada, que la representan diversos elementos los cuales están dispuestos en forma única en cada ser humano.

Una vez obtenido este código, se puede almacenar en una base de datos para su posterior uso para la identificación de personas. La forma en que se realiza la captura de dicho código es: obtener un código que sea real, se debe tomar una muestra de la huella dactilar, de esta muestra se obtiene un código que es el mas aproximado posible al de la huella escaneada. Una vez obtenido dicho código, solo resta hacer la verificación y para esto solo se toma la muestra a comparar contra el código capturado.

Tabla1. Cuadro comparativo de diferentes dispositivos lectores de huella.

NOMBRE	DIMENSIONES	INTERFAZ	SISTEMA OPERATIVO	SOFTWARE	TECNOLOGIA
Microsoft® Fingerprint Reader	82.0 mm Largo 50.0 mm Ancho 15.7 mm profundo	USB	Microsoft Windows® XP Professional Edition/Home Edition/Media Center Edition/Tablet PC Edition	Fingerprint Password Manager version 1.0	Escaneo de huella óptico
Fingerprit Recognition Hamster	25.3 mm Ancho 40.7mm Largo 67.7 mm Alto	USB	Windows 98/Me/NT4/2000/XP	SecuEnterprise Standard.	Escaneo de huella digital óptico
Futronic's FS80 USB2.0	45 mm Ancho 63 mm Largo 26 mm Alto	USB			Sensor de tecnología CMOS y

Fingerprint Scanner.					sistema optico
One Touch Pro		USB	Windows 98, ME, 2000 y XP.	librerías de desarrollo (SDK Gold o Platinum)	Escaneo de huella óptico
Fx2000 Desktop Fingerprint Scanner	Area sensible 0.98" ´ 0.52"	USB	Windows 95/98/98ME/NT/2000/XP , Linux	BiometriKa fingerprint recognition software	Escaneo de huella óptico

11.2 ANALISIS COMPLETO DE LA ARQUITECTURA BÁSICA DE UN CONTROL DE ACCESO BIOMÉTRICO.

Software. Para el desarrollo de este sistema, se creo una base de datos en Microsoft Acces, dentro de esta base de cargaron tablas con la información personal de los usuarios para este caso empleados de la empresa y visitantes. Adicionalmente cuenta con una ventana de eventos en tiempo real que describe los procesos que están siendo llevados a cabo por el programa.

Modulo de registro.

- En el menú de opciones se selecciona registrar nuevo usuario.
- Preparación y captura de la muestra de huella dactilar.
- Verificar que la imagen tenga una calidad alta.
- Almacenar los datos.

Modulo de Verificación.

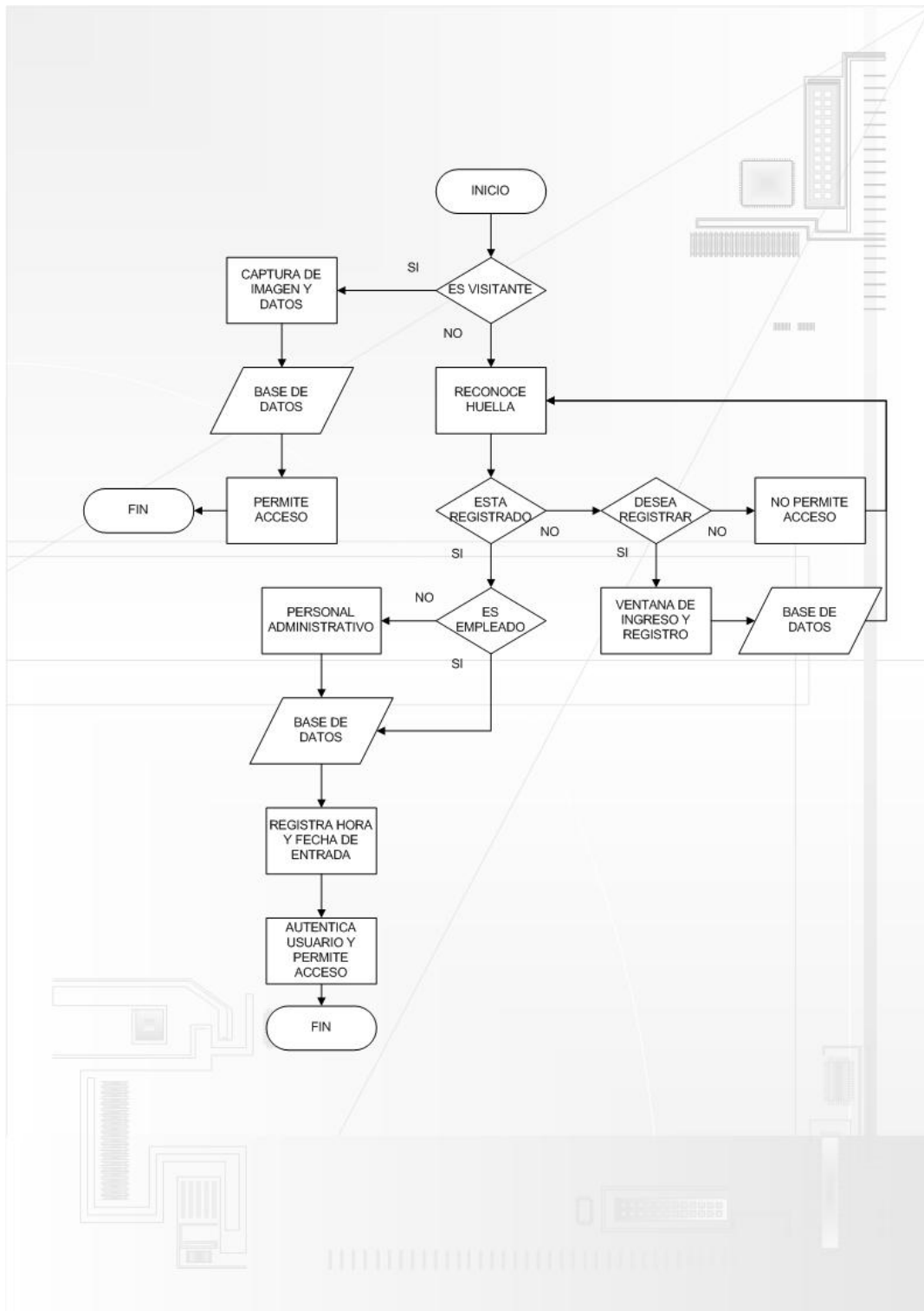
Ingresar por el menú de opciones al modo de identificación.

- Captura de la huella dactilar.
- Buscar el ID (código asignado a una huella especifica), en la base de datos.
- Extraer de la base de datos, nombre y apellido, Documento, código, programa, actividad, estado de vigencia.

- En el evento de que el usuario ubique la huella en el escáner el programa registra en una tabla de la base de datos fecha, hora de ingreso y por que sensor en particular se esta haciendo la verificación. Además se obtiene información acerca de la calidad de la huella verificada. El proceso se resume de la siguiente forma: Ubicación, detección, captura, calidad e identificación.

Diagrama de flujo

Figura 6. Diagrama de flujo del sistema.



11.2.1 Base de Datos. El sistema de almacenamiento, esta basado en el programa de Microsoft Acces, esta compuesto por dos bases de datos la primera FingerDataBase y una segunda USRDataFinger.

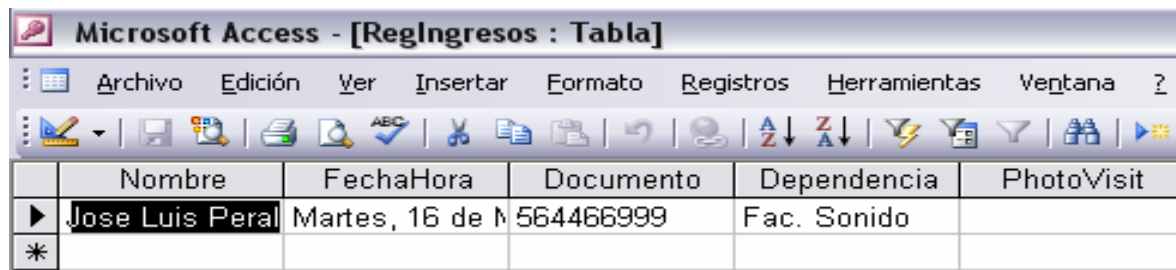
En la base de datos de usuarios (USRDataFinger) se encuentran tres tablas:

Tabla de registro de usuarios (usrfinger), contiene información en 14 columnas, la primera de ellas guarda el ID (código de usuario asignado para validarse, asignado por el software), otros campos son: nombre, apellidos, identificación, photo ID, programa, código, actividad, fecha de registro, activo, origen huella.

Tabla de historial de accesos, en donde se registran cada uno de los eventos realizados por el usuario como vía de entrada, fecha y hora actuales además del nombre, código y actividad.

Tabla para el registro de visitantes, en esta tabla se cargara la información pertinente al personal visitante con un registro fotográfico captado al momento de entrar a la instalación.

Figura 7. Tabla para registro de visitantes.



	Nombre	FechaHora	Documento	Dependencia	PhotoVisit
▶	Jose Luis Peral	Martes, 16 de M	564466999	Fac. Sonido	
*					

La base de datos (FingerDataBase) es la interfaz lógica usada por el controlador para asignar una identificación a cada usuario. De allí se toma el número de identificación para enlazar a la base de datos de usuarios.

Figura8. Base de datos creada por el controlador



ID	template
1	binarios largos
2	binarios largos
3	binarios largos
4	binarios largos

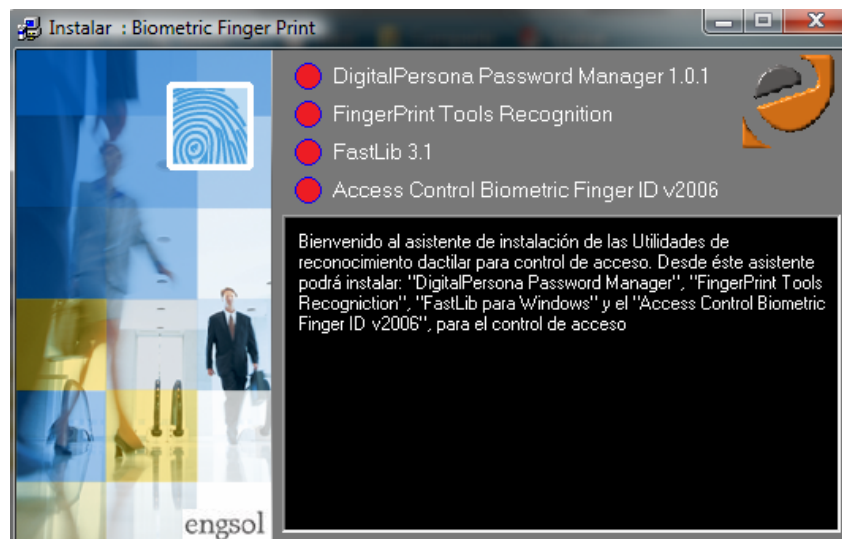
* (Autonumérico)

Registro: 1

11.2.2 Interfaz de usuario. Dentro de esta interfaz existe un menú que permitirá que la organización instale todos los programas necesarios para que el prototipo de control de acceso por lectores biométricos funcione de manera correcta. Estos controladores son:

DigitalPersona Password manager 1.0.1, GrFingerX free, FastLib 3.1 y Access control Biometric Finger ID v2006 (programa diseñado para el estudio de factibilidad).

Figura 9. Instalador Biometric Finger Print.



Compuesto por tres partes principales cada una de ella encargada del acceso, registro y verificación.

Ventana Principal de identificación, esta ventana muestra un menú de opciones, el cual está compuesto por tres acciones distintas, registrar nuevo usuario, modo de identificación y registro de visitantes.

Inicialmente, al abrir el programa el sistema está en modo de identificación y el entorno grafico muestra la información específica de cada usuario con su respectiva fotografía (si ya está registrado), en la parte superior izquierda tiene un icono donde indica si el usuario fue validado, contiene dos alarmas visuales las cuales indican por donde se está validando el usuario y el otro si fue exitosa su validación. En el momento de la validación, el programa esta enviando cuatro datos por el puerto serial, cada uno de ellos es interpretado como acceso o no acceso dependiendo de la ubicación de ingreso, Los códigos que genera el programa son: 21 no acceso peatonal1, 20 da acceso peatonal1, 23 no acceso peatonal2, 24 da acceso peatonal2.

Para el funcionamiento del programa se requieren una serie de controladores de uso libre, para el reconocimiento del escáner de huella (GrFingerXCtrl1), habilitación del puerto serial (ctlSerialPort), control de apertura de ventanas (CommonDialog). Que son invocados al momento de ejecutar el programa.

Figura 10. Controladores



Registro de nuevo usuario, para poder acceder a esta ventana primero se debe hacer el escaneo de la huella, el programa hace la captura de la huella y según su calidad (alta, media o baja) le permite hacer el registro.

Si la calidad de la muestra es alta, el programa habilita la ventana de registro de usuario, en esta ventana se carga la información personal por usuario. Para la vigencia del acceso se hace necesario activar un checkbox que indica si el usuario está en periodo de vigencia dentro de la compañía, de lo contrario el sistema denegara el acceso, dentro de este formulario se encuentra un espacio para la foto de usuario y por ultimo un campo para la fecha proporcionado de manera automática por el programa.

Registro de visitantes, en este formulario se digita la información del las personas ajenas a la institución, dentro de el se carga nombre completo, fecha/hora, número de documento de identificación y dependencia a la que se dirige. En el proceso de registro el usuario dejara un registro fotográfico que es almacenado en las carpetas creadas para tal fin.

Figura 11. Registro de visitantes.

Nombre	FechaHora	Documento	Dependencia
Jose Luis Perales	Martes, 16 de Mayo de 2006 02:00:02 p.m.	564466999	Fac. Sonido

Nuevo Ingreso

Registro fotografico

Guardar

REGISTRO DE VISITANTES

11.2.3 Hardware. En esta parte de la construcción del sistema de validación biométrica se deben contemplar las diferentes etapas que permitirán el control de los actuadores finales (Electro Iman para puerta), aquí se recibirá toda la información que recopile el computador después de haber realizado el proceso a cargo del software como captura, comparación y validación.

Protocolo de comunicación serial RS-232. Las comunicaciones serie se utilizan para enviar datos a través de largas distancias, ya que las comunicaciones en paralelo exigen demasiado cableado para ser operativas.

Los equipos de comunicación en serie se pueden dividir entre simples, half-duplex y full-duplex. Una comunicación serie simplex envía información en una sola dirección. Half-duplex significa que los datos pueden ser enviados en ambas direcciones entre dos sistemas, pero una sola dirección al mismo tiempo. En una transmisión full-duplex cada sistema puede enviar y recibir datos al mismo tiempo. Hay dos tipos de comunicaciones síncronas o asíncronas. En una transmisión sincrónica los datos son enviados en bloques, el transmisor y el receptor son sincronizados por uno o más caracteres especiales llamados caracteres synch.

Normalmente cuando no se realiza ninguna transferencia de datos, la línea del transmisor se encuentra en estado alto. Para iniciar la transmisión de datos, el transmisor coloca esta línea en bajo durante determinado tiempo, lo cual se le conoce como bit de arranque (start bit) y a continuación empieza a transmitir con un intervalo de tiempo los bits correspondientes al dato, empezando siempre por el BIT menos significativo (LSB), y terminando con el BIT mas significativo.

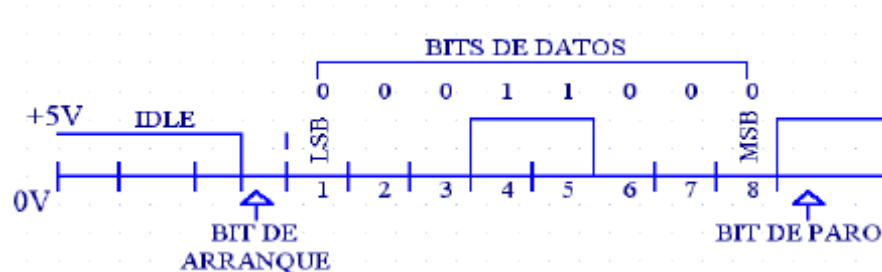
Si el receptor no está sincronizado con el transmisor, este desconoce cuando se van a recibir los datos. Por lo tanto el transmisor y el receptor deberán tener los mismos parámetros de velocidad, paridad, número de bits del dato transmitido y de BIT de parada.

En los circuitos digitales, cuyas distancias son relativamente cortas, se pueden manejar transmisiones en niveles lógicos TTL (0-5V), pero cuando las distancias aumentan, estas señales tienden a distorsionarse debido al efecto capacitivo de los conductores y su resistencia eléctrica. El efecto se incrementa a medida que se incrementa la velocidad de la transmisión.

Todo esto origina que los datos recibidos no sean igual a los datos transmitidos, por lo que no se puede permitir la transferencia de datos.

La siguiente figura muestra la estructura de un carácter que se transmite en forma serial asíncrono.

Figura 12. Transmisión serial asíncrona RS-232.



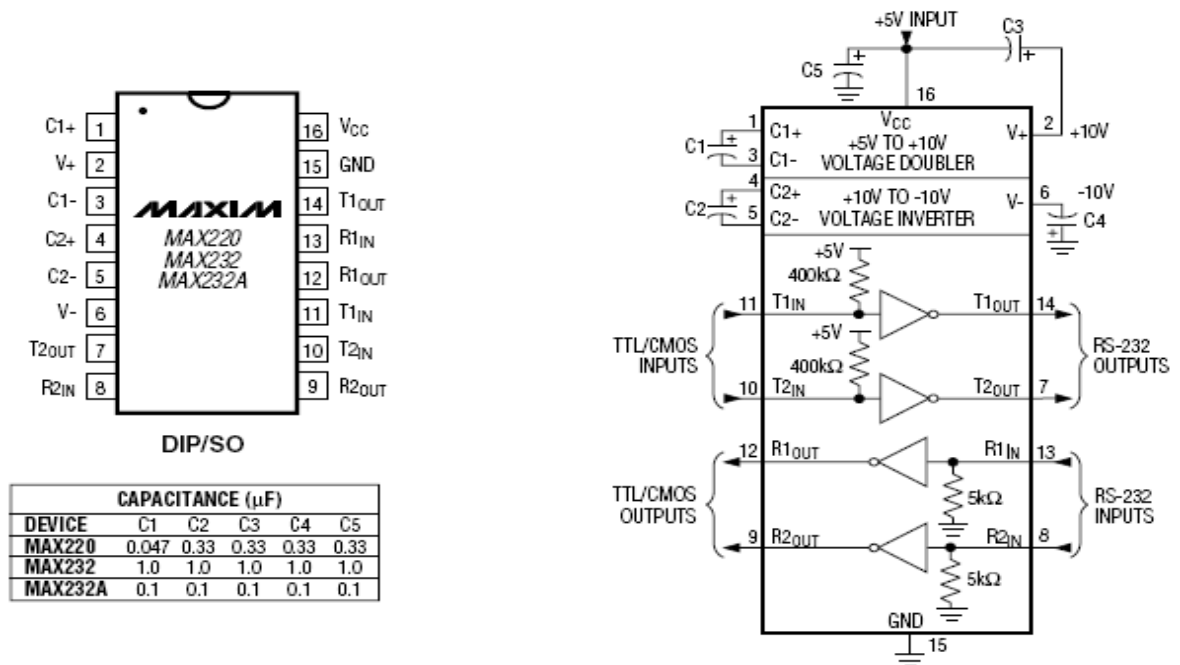
Documento Protocolo RS-232, Ing. Eric López Pérez

El Puerto serial del computador es compatible con la RS-232 este estándar está diseñado para comunicar un PC con un Modem. En los computadores modernos se utilizan los DB-9 macho. Los voltajes para un nivel lógico alto están entre -3 V y -15V. Un nivel lógico bajo tendrá un voltaje entre +3V y +15V los voltajes mas usados son +12V y -12V por esta razón se utilizara el MAX 232 para obtener voltajes lógicos de 0V y 5V.

El Circuito MAX-232 soluciona los problemas de niveles de voltaje cuando se requiere enviar unas señales digitales sobre una línea RS-232. Este chip se utiliza en aquellas aplicaciones donde no se dispone de fuentes dobles de +12 y -12

Voltios. El MAX 232 necesita solamente una fuente de +5V para su operación, internamente tiene un elevador de voltaje que convierte el voltaje de +5V al de doble polaridad de +12V y -12V. Cabe mencionar que existen una gran variedad de CI que cumplen con la norma RS-232 como lo son: MAX220, DS14C232, MAX233, LT1180A.

Figura 13. Diagrama de pines MAX 232.



www.maxim.com

Microcontroladores. Los dispositivos lógicos se encargarán de recibir un dato serial y realizar las funciones convenientes para las cuales fue programado, en este caso realizar las acciones de visualización (señales auditivas y visuales) y control de los dispositivos físicos de seguridad.

En el prototipo se contemplan dos tipos de microcontroladores, un PIC 16F877 y dos PIC 16F84 de Microchip.

➤ PIC16F877. Este dispositivo se encarga de recibir los datos seriales por medio de la USART (Universal Synchronous Asynchronous Receiver Transmitter) provenientes del computador, este último envía una trama de 8 bits con un código binario el cual fue asignado por software, este código es el que le informa al hardware que entrada debe habilitar y realizar las funciones de los actuadores por cualquiera de las entradas.

El programa cargado en el PIC se encarga de habilitar el otro microcontrolador en donde realiza tareas de manera independiente, con el fin de controlar las entradas y no crear un conflicto en el acceso, por que si se utiliza toda la aplicación apelando a un solo dispositivo controlador no se podrán realizar los dos tipos de procesos simultáneamente generando retardos en el momento de la validación.

➤ PIC16F84. Fácil de trabajar para esta aplicación específica, tiene un buen desempeño, es asequible respecto a costos y se encuentra con facilidad en el mercado. Para el proyecto se utiliza un dispositivo de estos, uno para controlar el acceso peatonal, este realizará las funciones pertinentes para los actuadores finales y para la visualización o información al usuario.

Este microcontrolador está programado para que controle el acceso peatonal, dentro de las funciones de este dispositivo se encuentra diferentes etapas como son:

➤ Manual-automático (Enable), este modulo habilita o no el sistema. De ser necesario un acceso continuo y sin registro se des energiza solo la parte peatonal sacándola de funcionamiento, en este caso se necesita de una persona que supervise el proceso de acceso.

➤ Electro-iman: Este dispositivo constituye el hardware para dar el acceso, instalado en la puerta principal por donde acceden todas la personas. Se le

induce una corriente para crear un campo magnético, reteniendo así la puerta evitando que sea abierta, cuando se da acceso se desenergiza y la puerta puede girar libremente, para volver a energizar la barra, el microcontrolador energiza de nuevo el solenoide en un tiempo determinado. El electroiman es activado por un transistor Tip41 en corte y saturación.

➤ Indicadores: para informar al usuario de todos los eventos utilizamos señales audio-visuales, para esto se emplearon leds de encapsulado grande, los cuales habilitamos con transistores 2N3904 configurados en corte y saturación

12. ESTUDIO DE MERCADEO

Con este estudio de mercado se trata de determinar el espacio que ocuparía nuestro producto en el mercado ya determinado como son las pequeñas empresas. Cuando nos referimos a un espacio en el mercado nos referimos a la necesidad que tienen los consumidores actuales y potenciales de nuestro producto.

Se pretende identificar las empresas productoras y las condiciones en que se está suministrando el producto, igualmente la formación del precio y de la manera como llega el producto a los consumidores y usuarios.

El estudio de mercado busca probar que existe un número suficiente de consumidores, pequeñas empresas y otros entes que en determinadas condiciones, presentan una demanda que justifican la inversión en la producción del producto.

12.1 EL PRODUCTO

El producto presentado es un control de acceso Biométrico para pequeñas empresas, esto para aumentar el nivel de seguridad en estas.

12.1.1 CONTROL DE ACCESO BIOMETRICO. El producto consta de un lector biométrico, Scan Digitalpersona con características compatibles con puertos USB, sistema operativo comercial (Microsoft Windows® XP Professional Edition/Home Edition/Media Center Edition/Tablet PC Edition), su tamaño es reducido y permite facilidad de instalación en recintos, realiza un escaneo óptico y un switcheo rápido entre usuarios, el cual debe ser instalado en la entrada de la empresa, consta de un Software el cual es diseñado para este proyecto, este tiene compatibilidad con cualquier tipo de PC o Servidor, el cual debe cumplir con determinadas

características como un sistema operativo Windows XP aplicación de Microsoft Access y físicamente debe tener un puerto USB y un puerto serial para transmisión de datos. Consta de un sistema actuador con un impreso (plaqueta electrónica) el cual incluye la alimentación y permite el acceso según lo procesado por el software.

12.1.2 INSTALACIÓN Y MANTENIMIENTO. Al desarrollar este tipo de control de acceso, necesariamente se desprenden subproductos, en este caso la prestación de servicios para dicho producto en cuanto a instalación se presta el servicio para puntos adicionales y la implantación completa del producto, y el mantenimiento que es un servicio, el cual se presta para el correcto funcionamiento del producto con visitas en ciertos tiempos para hacer mediciones y que el sistema este siempre operativo y funcional.

12.1.3 PRODUCTOS SUSTITUTIVOS. En el mercado encontramos diferentes tipos de control de acceso, los cuales pueden sustituir el nuestro, pero si los evaluamos desde el punto de vista nivel de seguridad, algunos se pueden quedar cortos, es el caso de control de acceso por identificación visual, es muy propenso a errores debido a que es realizado por humanos, este es el más primitivo y es de los más costosos pues requiere de personal, esto conlleva a pago de los vigilantes, carga laboral.

Existe otro tipo por medio de tarjetas magnéticas, es eficiente pero su nivel de seguridad es mucho menor, pues se presta a suplantaciones y el mantenimiento es mucho más costoso, pues se trabaja con tarjetas programadas, las cuales se pueden extraviar o dañar.

Existen sustitutos mucho más eficientes, pero demasiado costosos, en cuanto al dispositivo a emplear y el mantenimiento es mucho mas costoso.

12.1.4 PRODUCTOS COMPLEMENTARIOS. Todo sistema electrónico de seguridad es vulnerable, lo que se busca es disminuir este rango de vulnerabilidad, para este sistema se requiere necesariamente de un operador/supervisor, el cual va a estar gestionando el sistema y vigilando la operación del mismo, a la vez que realiza un control adicional para que el sistema no sea vulnerado. Además se puede reforzar mediante un sistema completo de cámaras, un circuito cerrado de televisión, el cual este monitoreando el sistema y soportando mediante grabación los eventos presentados en el sistema.

12.2 EL CONSUMIDOR

12.2.1 POBLACIÓN. Este proyecto está enfocado a pequeñas empresas, una empresa es un organismo social integrado por elementos humanos, técnicos y materiales cuyo objetivo natural y principal es la obtención de utilidades, o bien, la prestación de servicios a la comunidad, coordinados por un administrador que toma decisiones en forma oportuna para la consecución de los objetivos para los que fueron creadas. Para cumplir con este objetivo la empresa combina naturaleza y capital.

Para determinar una pequeña empresa En Colombia la ley 905 y 504 de Mipymes hacen referencia a la clasificación de las empresas en el país según su dimensión.

Los principales indicadores son: el capital propio, número de trabajadores. El más utilizado suele ser según el número de trabajadores. Este criterio delimita la magnitud de las empresas de esta forma:

Microempresa si posee menos de 10 trabajadores.

Pequeña empresa: si tiene menos de 50 trabajadores.

Mediana empresa: si tiene un número entre 50 y 250 trabajadores.

Gran empresa: si posee más de 250 trabajadores.

12.2.2 CONSUMIDORES ACTUALES Y TASA DE CRECIMIENTO

Sólo el 2% de las Pymes en Colombia invierten en tecnología, y por ello es necesario que estas empresas aceleren su inversión en Tecnologías de Información y Comunicaciones (TIC) para ser competitivas en el mercado global. Este panorama fue presentado en el marco de la mesa redonda "Tecnología, oportunidad de crecimiento para las Pymes en Colombia", realizada por Cisco y ACOPI.

A continuación algunas cifras de un estudio realizado por FUNDES Colombia sobre las razones y prioridades en la inversión en Tecnologías de Información y Comunicación.

Según estudio realizado por FUNDES Colombia, la Pyme invierte en TIC's con los siguientes propósitos:

- 30% en tecnologías de la información
- 28% en equipamiento
- 12% para mejoramiento de sus productos
- 10% para el gerenciamiento de su negocio
- 10% para el desarrollo de nuevos productos
- 9% para el mejoramiento de su productividad

Factores que se consideran para la compra de tecnología:

- 48% Costos de la tecnología
- 30% Adaptación al negocio
- 20% Costos de consultoría

Las prioridades de las Pymes para sus gastos en TI son:

- 42% Adquirir o actualizar PC's

- 39% Mejorar la seguridad de la red
- 32% Fortalecer el servicio al cliente
- 23% Expandir o actualizar la red
- 21% Mejorar la capacidad de almacenamiento
- 21% Automatización de cadena de valor
- 20% Mejorar herramientas para la fuerza de ventas
- 19% Mejorar finanzas

12.3 DEMANDA DEL PRODUCTO

Con base a la encuesta realizada, vamos a determinar las cantidades del producto que los consumidores están dispuestos a adquirir. En la encuesta se cuantifica la necesidad real o psicológica de una población de consumidores, con disposición de poder adquisitivo suficiente y con unos gustos definidos para adquirir el producto que satisfaga las necesidades del cliente.

12.3.1 Situación actual de la demanda.

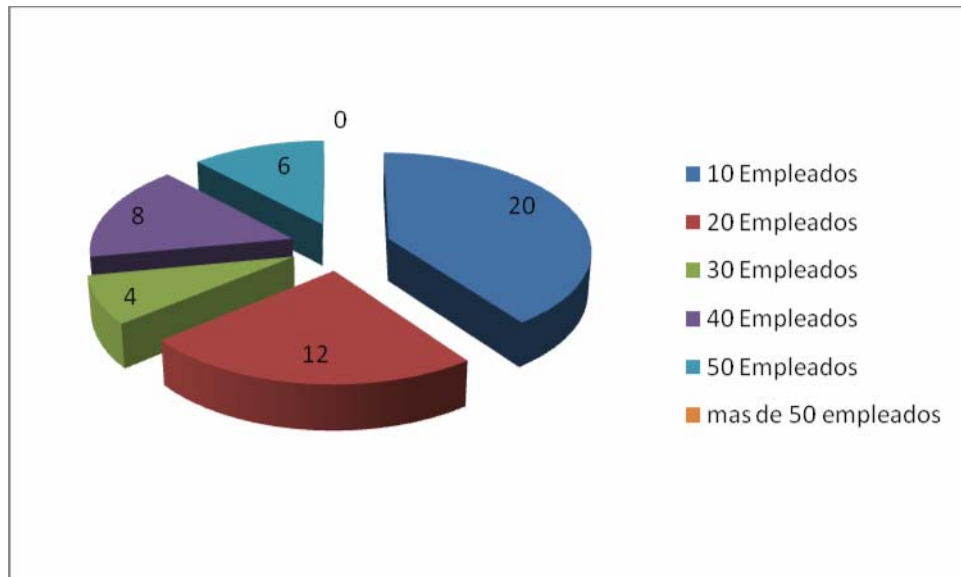
Hay diferentes maneras de controlar el acceso a los activos informáticos de las empresas. Los siguientes son los utilizados por las empresas según respuestas a una encuesta realizada por Informationweek a más de 8,100 empresas de todos los tamaños.

- 90% Claves de Acceso básicas para los usuarios.
- 50% Múltiples logines y claves.
- 25% Software para controlar el acceso a los PC's.
- 19% Software de conexión único.
- 18% Candados para terminales y palabras clave.
- 11% Software de control de acceso para Mini y Mainframes.
- 5% Claves únicas, códigos de acceso y tarjetas inteligentes.
- 3% Biometría para autenticación del usuario.

Las alternativas para controlar los accesos son múltiples, sin embargo es claro que todavía basamos el sistema de seguridad en la combinación tradicional de usuario y clave de acceso

Al basarnos en pequeñas empresas encontramos un promedio de 20 empleados por empresa, como lo vemos en el siguiente grafico.

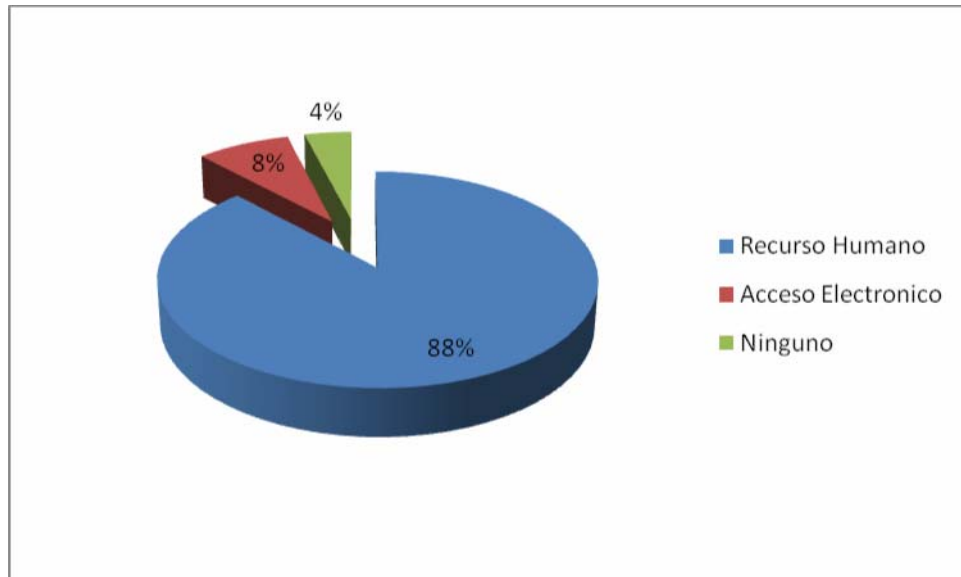
Figura14. Promedio de empleados en pequeñas empresas.



Según la encuesta realizada a 50 empresas obtenemos que:

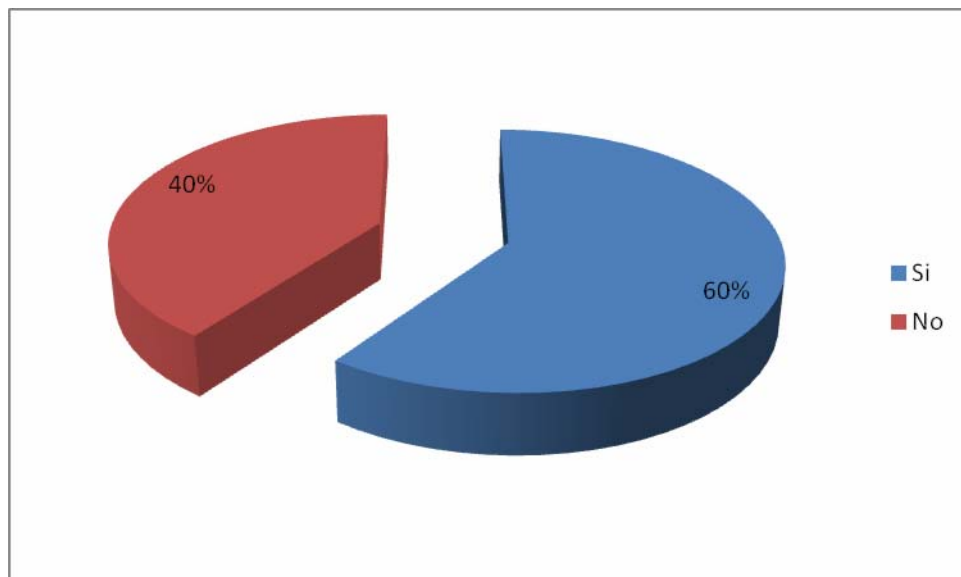
El 88% de las empresas emplean un sistema de control de acceso artesanal, empleando recurso humano para el control de acceso, un 8% emplea ayudas tecnológicas, como el uso de tarjetas electrónicas y un 4% no tiene ningún tipo de control de acceso.

Figura15. Tipo de control de acceso mas usado.



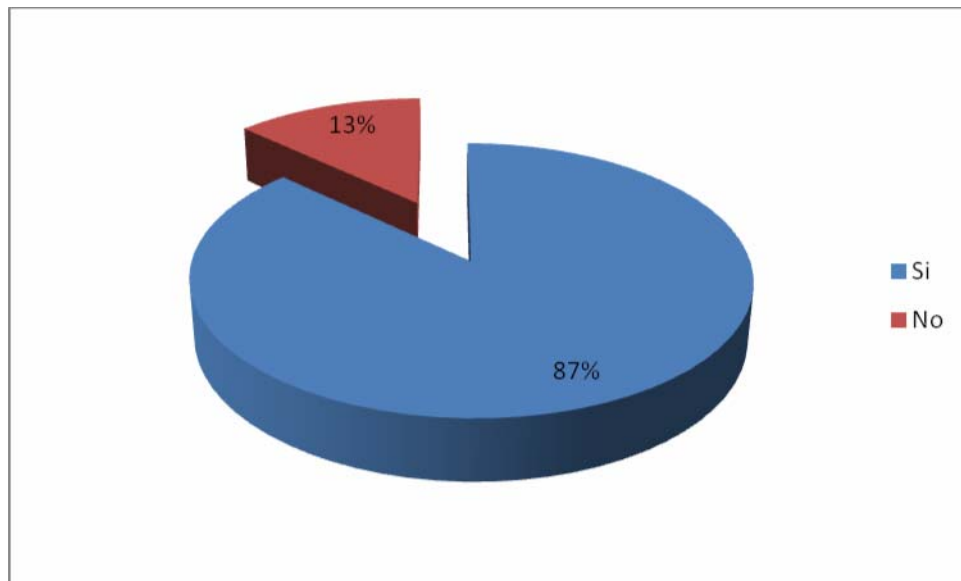
A la encuesta, responden el 60% que poseen problemas con el control de acceso del personal que ingresa a sus empresas.

Figura16. Problemas de control de acceso en las empresas



Las empresas encuestadas ven la necesidad de incrementar el nivel de seguridad y esto se refleja en el grafico.

Figura17. Necesidad de las empresas por incrementar la seguridad



12.4 OFERTA DEL PRODUCTO

Estudia las cantidades que suministran los productores del bien que se va a ofrecer en el mercado. Analiza las condiciones de producción de las empresas productoras más importantes. Se referirá a la situación actual y futura, y deberá proporcionar las bases para prever las posibilidades del proyecto en las condiciones de competencia existentes.

Actualmente encontramos diferentes proveedores de este tipo de control de acceso biométrico, los cuales ofrecen un servicio muy limitado, (dispositivo y software) y cobran a conveniencia, no prestan un servicio de soporte e instalación y los que lo prestan lo hacen a un precio muy elevado, el mercado nos permite cierta elasticidad, dependiendo del servicio a prestar y si es un software propio,

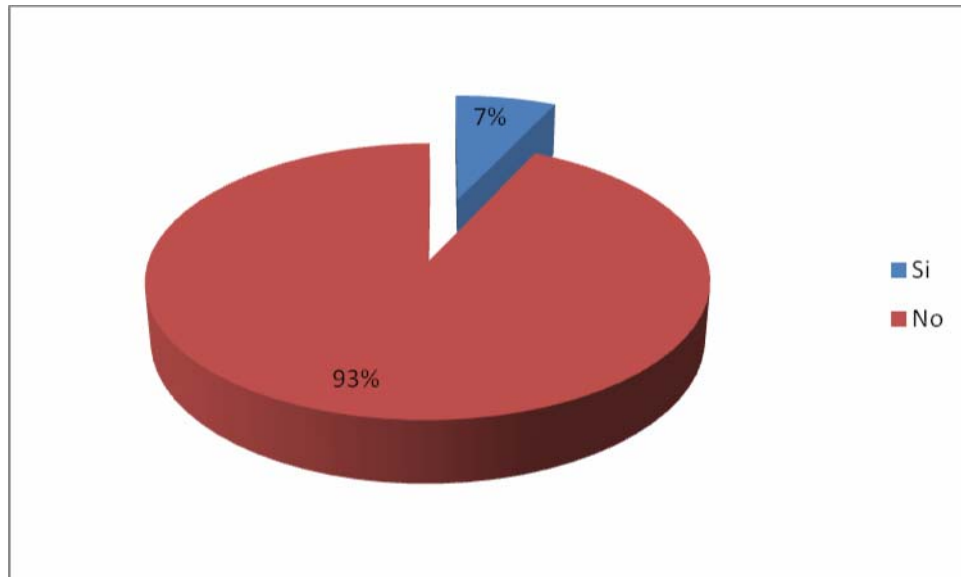
pues el costo de este nos permite entrar al mercado de forma más competitiva. El mercado se mueve por cosas ya importadas y están limitados al costo de estos y no permite variación en los precios.

Al ser un software propio, diseñado e implementado por nosotros, a futuro, nos permite mantener un costo de producción bajo y eso nos permite seguir siendo competitivos, las modificaciones hechas no requieren de mucha inversión.

- Los productores de este servicio, no están interesados a realizar desarrollo y búsqueda de soluciones a la medida de los clientes, ellos están interesados en comercializar los productos ya hechos y se limitan a realizar la comercialización de este tipo de producto.
- actualmente en Colombia no se realiza este tipo de desarrollo tecnológico, y los existentes se dedican a la comercialización, ellos están limitados a la evolución económica de los que desarrollan el producto, existen en el mercado exterior diversas empresas desarrolladoras de este tipo de productos, y lo que buscan los comercializadores locales es ver cuál de todos les representa menor costo. Ellos están sujetos a la variación de la moneda, impuestos de nacionalización del producto.

Al preguntar si conocen los beneficios de usar un sistema de control de acceso biométrico empleando huella dactilar las empresas responden:

Figura18. Conocimientos sobre un control de acceso biométrico.



Esto refleja que las empresas aun no conocen bien en que consiste un control de acceso biometrico y todo los beneficios que este conlleva, incrementando el nivel de seguridad de sus empresas.

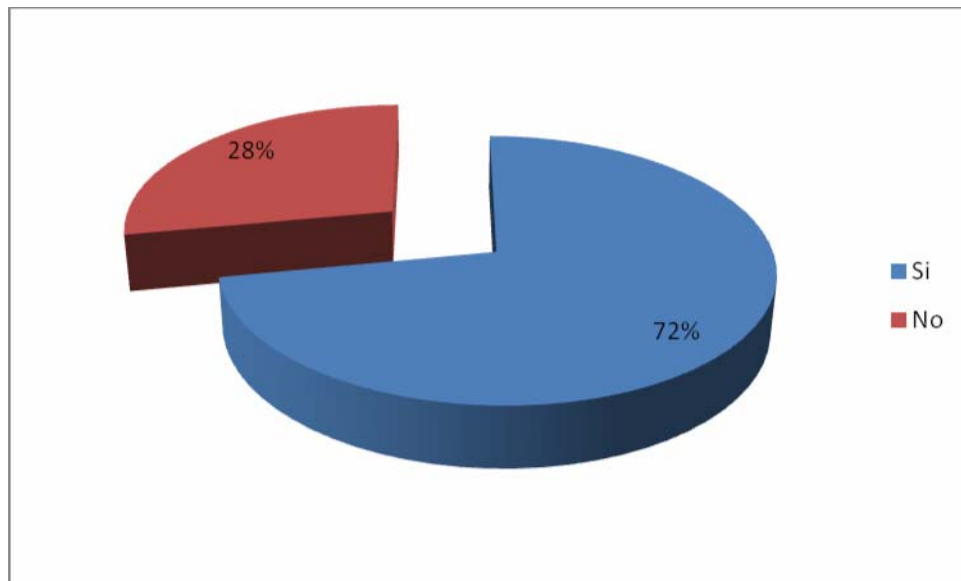
12.5 LOS PRECIOS DEL PRODUCTO

Actualmente en el mercado interno encontramos este tipo de productos a un valor aproximado de 2'000.000 sin la prestación del servicio instalación y soporte. Al traer el equipo de otro país, el costo del dispositivo el software disminuye, pero este incurre con costos de envío, nacionalización, igualmente incurre en la no instalación, y soporte del producto.

El precio del producto, analizando todos los factores anteriores oscila alrededor del 1'200.000 y el 1'500.000 incluyendo la instalación, y un periodo de soporte técnico. El valor de este producto se vera reflejado en el análisis financiero.

A la encuesta las empresas respondieron que están dispuestos a pagar un valor promedio de 1'500.000 de la siguiente forma:

Figura19. Aceptación de pago propuesto para implementar un sistema de control biométrico.



12.6 COMERCIALIZACIÓN

La comercialización de este producto se realiza a nivel de consumidores, se realiza según demanda y esto implica el llevar el producto a donde se requiere, este incluye la instalación, lo cual demanda la movilización de personal al sitio donde va a ser implementada la solución. Además que incurre en el suministro de materiales, para la instalación y todo esto se debe llevar a terreno.

12.6.1 PROMOCIÓN Y PUBLICIDAD

Para dar a conocer el producto y los servicios que este conlleva se llevara a cabo para dar a conocer al público por medio de

- Perifoneo
- Tarjetas de presentación

- Mailing (correo electrónico)
- pagina web de la empresa comercializadora del producto.

Podemos ver que este estudio de mercadeo nos permitió identificar claramente las características del producto y el servicio que va de la mano de este para ser entregado al cliente final. Analizamos el comportamiento de este tipo de producto, el estado presente y futuro, vemos claramente la necesidad de las pequeñas empresas para tener acceso a este tipo de tecnología. Logramos visualizar el comportamiento del producto en el mercado y cual es su posible mercado en el medio. Aun existen muchas empresas que no poseen un control de acceso eficiente, esto debido a la desinformación y paradigmas, los cuales no les permiten visualizar los beneficios de estas tecnologías.

12.7 ESTRUCTURA ORGANIZATIVA

La empresa ENGSOL LTDA., está estructurada organizacionalmente por un presidente quien tiene a su cargo tres gerencias quienes les reportan directamente; Estos son:

12.7.1 Gerencia Administrativa: Esta es una gerencia de apoyo a la cual le reportan tres departamentos:

- Departamento de contabilidad: La función principal del departamento consiste en la contabilización de las transacciones diarias que realiza la empresa, manejo de caja chica, pago de nómina, declaración de los impuestos, conciliaciones bancarias, así como la presentación de los estados financieros básicos.
- Departamento de cobranzas y pagos: se encarga del pago a los proveedores, de las órdenes de compras, control de las compras de materiales, facturación, cobranzas a los clientes.

- Departamento de almacén: Registra la entrada y salida del material del depósito, solicitud de material del taller, codificación del material y revisión de las existencias del material.

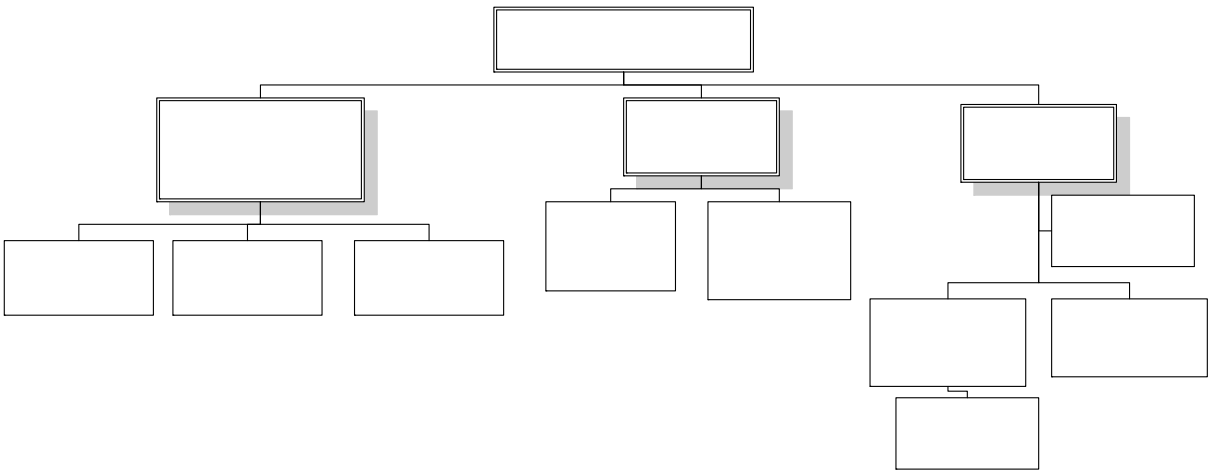
12.7.2 Gerencia de ventas: Esta gerencia está comprometida a proporcionar a los clientes la tecnología líder de la industria y productos innovadores, su principal función es promover y distribuir los productos a los clientes.

12.7.3 Gerencia de operaciones: Esta gerencia es la encargada de ejecutar las actividades principales de la empresa, la misma esta dividida en tres departamentos:

- Departamento de servicios y mantenimientos: Su función principal es proporcionar apoyo técnico y el servicio que requieran los clientes en los productos instalados.
- Departamento de proyectos: Este es un departamento clave para la empresa, en el cual interactúa la parte operativa y gerencial para atender clientes potenciales, brindándole un trato especial en función de las necesidades del usuario, prestándole asesoría en la escogencia de los productos que mejor se adapten a sus necesidades.

ESTRUCTURA ORGANIZACIONAL

Figura20. Estructura organizacional



13. EVALUACION FINANCIERA

Determinación del costo de los materiales directos y mano de obra directa.

La empresa ENGSOL, está dedicada a la instalación, actualización y soporte de tres tipos de productos, computadores, networking y seguridad electrónica, enfocados en este último se realiza este estudio de factibilidad para un incorporar una línea de producto el cual estamos presentando, control de acceso biométrico por finger print.

13.1 Materiales

En la tabla se calcularon los costos de los materiales directos involucrados en el proceso de fabricación del control de acceso biométrico.

Tabla2. Materiales directos del proceso productivo

No	DESCRIPCION	MODELO	CANTIDAD	C. UNITARIO	C.TOTAL
1	Scanner Biométrico	Digitalpersona	2	120.000	240.000
2	Baquela impresión	Baquela Estándar	1	3.000	3.000
3	Protocolo de comunicación serial RS-232	Max 232	1	5.000	5.000
4	Microcontrolador	Pic 16f877	1	20.000	20.000
5	Microcontrolador	Pic 16f84	1	15.000	15.000
6	Solenoide	Estándar	1	50.000	50.000
7	Swithes	Estándar	2	2.000	4.000
8	Indicadores	Led	4	1.000	4.000
9	Indicadores	Parlante	1	2.000	2.000
10	Canaleta plástica	Estándar	2m	3.000	3.000
11	Porta fusible	Estándar	1	500	500
12	Fusibles	1amp	1	200	200
13	Cable de datos	UTP Cat 5e	5m	2.000	10.000
14	Cable de alimentación	Dúplex 2x16	5m	400	2.000
15	Transformador	12vdc-5vdc	1	20.000	20.000
16	Caja metalica	Estándar	1	5.000	5.000
17	Otros	Estándar			50.000
TOTAL					433.700,00

En el proceso de ensamblaje e instalación del control de acceso, es necesario tomar en cuenta el desperdicio de material utilizado en la instalación, se estima un 10% del cable empleado en el proceso, este desperdicio está considerado dentro

de los costos totales del cable, ya que el mismo no puede ser reutilizado en otro proceso.

13.2 Mano de obra

En un sistema de costo basado en actividades, los costos de la mano de obra se deben imputar al proceso productivo y no a los productos, este enfoque se basa en que los empleados realizan actividades y los productos consumen actividades, es decir el costo de la mano de obra es un componente del costo de la actividad.

Los costos de mano de obra se asignaron al control de acceso, de acuerdo con la cantidad de horas hombre empleadas en cada actividad del proceso, como se observa en la tabla, en la misma se puede observar el tiempo total en la fabricación de tableros eléctricos expresados en días:

Tabla3. Actividades y carga laboral en el proceso productivo

DEPARTAMETNO	ACTIVIDADES	CARGA LABORAL
Servicios	Fabricación	
	Levantamiento de información	2 días
	Programación software	1 día
	Programación micro controladores	1 día
	Impresión de baquela	2 días
	Ensamble	4 días
	prueba	2 días
Servicios	Puesta en marcha	
	Transporte en sitio	1 día
	Instalación software	1 día
	Montaje de equipos en el lugar requerido	2 días
	Ejecución de cableado	3 días
	Prueba en presencia del cliente	2 días
TOTAL		21 días

El tiempo total para fabricación del producto: 21 Días.

Tabla4. Salario diario

EMPLEADO	SALARIO MENSUAL	DÍAS LABORABLES	COSTOS POR DIA
coordinador soporte técnico	800.000	24	33.333
Auxiliar técnico	450.000	24	18.750

En la siguiente tabla se determinó el costo por día de la mano de obra directa, se tomo como base los salarios mensuales de los empleados (Ing. De soporte técnico y auxiliar técnico), dividido entre el número de días laborables en el mes, arrojando como resultado el costo por día de cada empleado.

Entonces según nuestro estudio de mercadeo, en promedio de 50 empresas encuestadas, el 72% está dispuesto a adquirir el producto y a pagar un valor de 1'500.000 por control de acceso.

Esto nos arroja un total de 36 unidades posiblemente en ventas.

Si realizamos el análisis para un año, tenemos lo siguiente, teniendo unas ventas promedio de 26 unidades vendidas al año.

Tabla5. Análisis de costos para el primer año

	1 año 26und
Ingresos	39'000.000
Costos de operación	26'276.200
Ganancias gravables	12'723.800
Impuestos	6'240.000
Ganancia neta contable	6'483.800
Costos de inversión	1'000.000
Flujo de fondos neto	5'483.800

13.3 Evaluación Financiera

Al realizar la evaluación financiera para 5 años, tenemos con un ajuste del 6% promedio en el aumento salarial y un 4% en el aumento de los ingresos.

Figura21. Evaluación financiera a 5 años

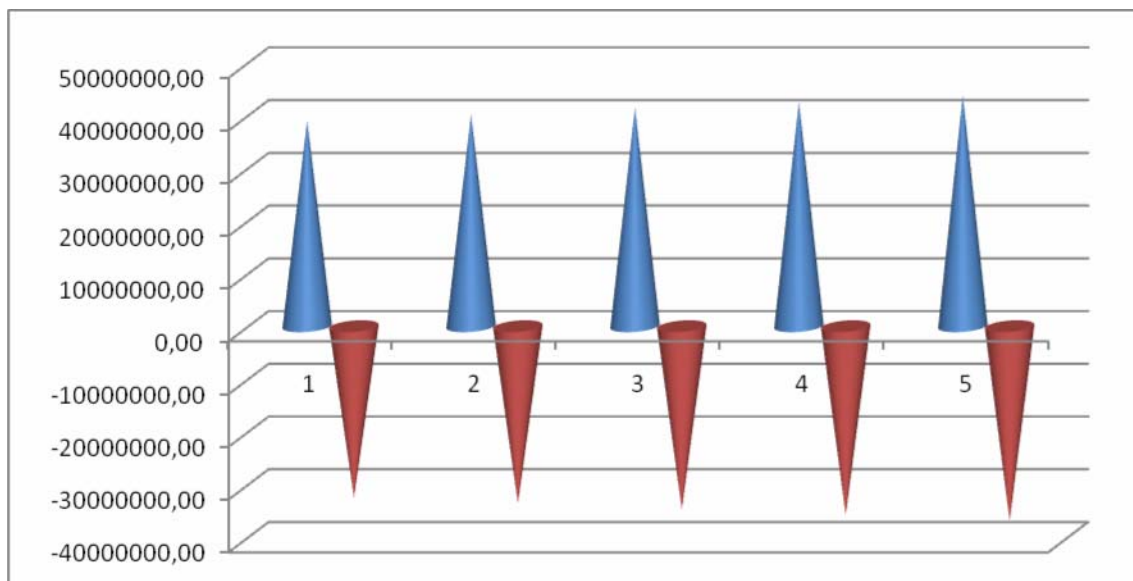


Tabla6. Analisis financiero a 5 años

	1	2	3	4	5
Ingresos	39'000.000	40'200.000	41'400.000	42'600.000	43'800.000
Costos de operación	26'276.200	27'176.200	28'076.200	28'976.200	29'876.200
Ganancias gravables	12'723.800	13'023.800	13'323.800	13'623.800	13'923.800
Impuestos	6'240.000	6'432.000	6'624.000	6'816.000	7'008.000
Ganancia neta contable	6'483.800	6'591.800	6'669.800	6'807.800	6'915.800
Costos de	1'000.000				

inversión					
Flujo de fondos neto	5'483.800	6'591.800	6'669.800	6'807.800	6'915.800

13.4 VPN

Si tomamos una tasa de oportunidad del 4%, algo superior a la ofrecida por el banco, tenemos una VPN de 31989790.5 positiva, esto nos indica que el proyecto es aceptable.

14. CONCLUSIONES

A nivel técnico es viable realizar el proyecto, pues la arquitectura es de fácil desarrollo, lo único para mejorar el sistema es buscar un scanner especializado para poder obtener mayor tráfico en cuanto a usuarios y poder ofrecer el producto a otro tipo de empresas.

En cuanto a la normatividad existente, podemos señarnos a los estándares internacionales que se están desarrollando para presentar el producto con calidad. vemos claramente la necesidad de las pequeñas empresas para tener acceso a este tipo de tecnología

A nivel de costos es viable desarrollar el proyecto pues los resultados que observamos de utilidad son positivos y con una buena proyección basándonos en el estudio de mercadeo.

BIBLIOGRAFIA.

ZDENEK Ríha, VÁCLAV Matyáš. Biometric Authentication Systems. Republica Checa, 2000. FIMU. 46 p.

RATHA Nalini, BOLLE Ruud. Automatic Finger Print Recognition System. EDITORS.

MORAN Luis. Sistema de detección de huella digital. México, 2002. 93p.

<http://www.homini.com>

<http://www.tiendalinux.com>

http://www.amazon.com/Books_Automatic_Fingerprint_Recognition_Systems

<http://www.nist.gov/cbeff>

<http://www.idex.com>

<http://www.maxim.com>

<http://www.digitalpersona.com>

<http://www.griaule.com>

<http://www.st.com>