PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

ESCUELA DE INGENIERIA DE SISTEMAS

DISERTACIÓN DE GRADO PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERÍA DE SISTEMAS

TEMA:

"USO DE DISPOSITIVOS DE HUELLA DIGITAL PARA EL SISTEMA DE CONTROL DE INGRESO Y SALIDA DEL PERSONAL DOCENTE DE LA ESCUELA DE INGENIERÍA DE SISTEMAS DE LA PUCESA"

AUTOR:

VERA ALTAMIRANO NANCY GEOVANNA

ASESOR:

ING. VICTOR CHUNCHA

AMBATO – ECUADOR

2008

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE AMBATO

ESCUELA DE INGENIERIA DE SISTEMAS

HOJA DE APROBACION

TEMA: "USO DE DISPOSITIVOS DE HUELLA DIGITAL PARA EL SISTEMA DE CONTROL DE INGRESO Y SALIDA DEL PERSONAL DOCENTE DE LA ESCUELA DE INGENIERÍA DE SISTEMAS DE LA PUCESA"

AUTOR: VERA ALTAMIRANO NANCY GEOVANNA

Víctor Chuncha. Ing. f._____
DIRECTOR DE LA DISERTACION.

Patricio Medina Ing. MSc.
CALIFICADOR. f._____

Wigberto Sánchez Ing. MSc.
CALIFICADOR. f._____

Santiago Acurio. Ing.
DIRECTOR DE LA ESCUELA DE SISTEMAS. f._____

Pablo Poveda Mora Ab.
SECRETARIO GENERAL DE LA PUCESA. f._____

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Nancy Giovanna Vera Altamirano portadora de la cédula de ciudadanía No. 180336978-2 declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de Ingeniería de Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.

Nancy Giovanna Vera Altamirano
CI. 180336978-2

RESUMEN

La presente investigación es un estudio del funcionamiento y automatización del control de ingreso de personal por medio de huellas digitales, que permitió el desarrollo de un sistema denominado “Sistema de Ingreso de Personal”, para automatizar el control de ingreso de los Docentes a sus horas de clases de la Escuela de Ingeniería de Sistemas de la Pontificia Universidad Católica del Ecuador, Sede Ambato.

Como resultado de esto el sistema puede realizar lo siguiente:

1. El uso de equipos KBio nos permite la obtención de huellas digitales y emplearlas en un sistema de control de ingresos de los Docentes.
2. Con la información recolectada o ingresada el sistema permitirá realizar reportes ya sea de forma individual, colectiva o por fechas.
3. El sistema almacena en una Base de Datos la información tanto de registro como los marcajes realizados durante el día del KBio.
4. La herramienta permite el ingreso de información a la base de datos en forma tanto manual como automáticamente, de acuerdo a su requerimiento.
5. La herramienta permite organizar los registros de forma que se pueda obtener informes en tiempo real, además de manera individual o grupal.
6. El sistema permite modificar la información de acuerdo a la necesidad del informe requerido previo a su impresión.
7. Se proporciona una interfaz grafica de fácil manipulación y que permite el funcionamiento del sistema de forma sencilla.
8. El control de acceso de los equipos Kbio es mediante identificación biométrica por huella dactilar. Un sistema seguro y fiable, elimina la posibilidad de suplantación de identidad por transferencia.

ABSTRACT

This investigation is a study of the operation and automation of staff entry control by means of fingerprints, which allowed the development of a system called "Staff Entry System". It automates the control of the professor entry to class at the Systems Engineering School at the Pontifical Catholic University of Ecuador in Ambato .

As result of this, the system can do the following:

1. The use of KBio equipments allows us to obtain fingerprints and to use them for the control of the professor entry system.
2. With the gathered information the system will allow us to write either individual, collective or by dates reports.
3. The system stores registry in a Database as well as markings made during the day of KBio.
4. This tool allows us to load information in the database manually or automatically as it is required.
5. This tool allows us to organize records so that reports can be obtained in real time, either individually or by groups.
6. The system allows us to modify the information according to the need of the required report before printing.
7. An easy to use graphical interface which allows the system functioning in a simple way is provided.
8. Kbio equipment access control is done by biometric identification through fingerprint; a secure and trustworthy system, which eliminates the possibility of supplanting identity for transfer.

TABLA DE CONTENIDO

TABLA DE GRAFICOS

INTRODUCCION

En la actualidad el uso de huella digital se ha convertido en un control seguro y fácil de aplicar y automatizar en los diferentes ámbitos de seguridad, sin embargo, aun no es una técnica común en nuestro medio el control de este tipo en entidades públicas y privadas.

Existen diferentes técnicas y ámbitos en los que se puede aplicar el control de huella digital, sin embargo, en el presente proyecto se va a investigar sobre la automatización del control de ingreso de personal con el fin de llegar a obtener un mejor rendimiento y puntualidad de parte de los Docentes. Esto conlleva a un proceso de investigación, desarrollo de un sistema que permite capturar la huella del Docente y recopilar en forma automática los datos de registro como horas y fechas de ingreso.

El sistema facilitara el ingreso de la huella digital y obtener reportes personalizados del registro del Docente a sus horas de clase. Este sistema será de gran ayuda para la Escuela de Ingeniería de Sistemas de la PUCESA, ya que se va a poder mantener un mejor control de la asistencia de los Docentes a sus horas de labores con tan solo registrar la huella en el dispositivo KBio.

CAPITULO I

1.1 PROYECTO DE ESTUDIO

1.1.1 Problema

La carencia de un sistema de ingreso y salida del personal docente de la Escuela de Ingeniería de Sistemas de la PUCESA a sus horas de clase en el periodo 2006-2007, esto provoca la pérdida de tiempo la misma que podría repercutir en la impuntualidad de los docentes.

1.2 DELIMITACIÓN

Dentro del área de automatización y control, la Escuela de Ingeniería de Sistemas de la PUCESA tiene la obligación de impartir los mejores conocimientos de los avances tecnológicos a sus estudiantes por lo cual es necesario y fundamental que tanto Estudiantes como Docentes comprendan la importancia de aprovechar sus horas de clases al máximo y para que de esta manera no queden dudas ni vacíos en sus conocimientos.

Para la implementación de este sistema de ingreso y salida del personal docente se requiere de un dispositivo de huella digital el mismo que trabajara con el programa Visual Basic y Access.

Con este tipo de dispositivos podemos obtener diversos tipos de reportes del personal docente como se detalla a continuación:

- La aplicación permitirá registrar los datos del docente, sus horas de entradas y salidas, consultar reporte de asistencia y puntualidad. Además, este dispositivo permitirá a cualquier persona conocer un resumen de la asistencia y puntualidad de sus compañeros, de esta forma, todos en la Escuela de Sistemas se convierten en monitores de la puntualidad.

- El sistema permitirá conocer que docente ha laborado dentro y fuera de la universidad, quienes no asistieron, o quienes no laboran en ese día. No necesita introducir claves de acceso.

- Resumen mensual**.-** Estudiar la puntualidad de los docentes mes a mes con solo ver en el calendario e identifique rápidamente quiénes son los docentes que presentan más incidentes de inasistencia o impuntualidad.

1.3 IMPORTANCIA Y JUSTIFICACION

1.3.1 Importancia.

Una mejor enseñanza y aprendizaje es fundamental ya que hoy en día hay mucho desinterés por parte de los alumnos por ciertas materias y esto es lo que ocasiona que los Docentes no completen sus horas de enseñanza y dejando grandes vacíos en los conocimientos de los estudiantes.

Conocimientos que serán de gran necesidad para el desarrollo profesional del estudiante en el campo laboral.

A nivel Nacional los estudiantes podrán desempeñarse profesionalmente de manera exitosa por la buena enseñanza en la Escuela y tendrán un mejor perfil profesional lo que facilitaría su integración laboral en el ámbito nacional y de esta manera se aporta al crecimiento y desarrollo del país.

La implementación del sistema será de gran beneficio para la escuela ya que permitirá el control automatizado de los horarios de clase, la asistencia de los docentes así como los atrasos y las inasistencias de los mismos. Mediante reportes se conocerá todo cuanto sea necesario para el control de ingreso y salidas de los docentes.

1.3.2 Justificación.

Desde el punto de vista Tecnológico se justifica la implementación del Control ingreso y salida de los Docentes en la PUCESA ya que en muchas de las situaciones con el control manual los docentes únicamente firman y no se sabe si entraron o no a la horas de clases y si llegaron puntual o no, con este sistema el control será mas estricto y confiable y no se podrá alterar los repotes.

En lo Económico, se justifica la implementación de este sistema puesto que la inversión será asumida por nosotros los desarrolladores y se reflejara en la mejora del

proceso de control de asistencia de los docentes lo que disminuirá notablemente el desperdicio de tiempo y recursos de a universidad.

1.4 OBJETIVOS

1.4.1 Objetivo General

Implementación de un Sistema Informático que permita controlar el ingreso y salida del personal docente de la Escuela de Ingeniería de Sistemas de la PUCESA utilizando dispositivos de huella digital para automatizar el control de atrasos y faltas de los docentes a sus horas laborables.

1.4.2 Objetivos Específicos

- Desarrollar un sistema de reportes que permita conocer las horas de entradas y salidas de los docentes así como su asistencia diaria en la Escuela de Sistemas.

- Conocer que docentes laboraron, quienes no asistieron a laborar, o quienes no laboran en ese día.

- Diseñar una aplicación que permita el manejo de sanciones por atraso a la hora de clases y consultarlos.

- Analizar la puntualidad de los docentes mes a mes e identificar quiénes presentan más incidentes de inasistencia o impuntualidad

1.5 HIPOTESIS

Con la implementación de dispositivos de huella digital, los estudiantes aprovecharan al máximo sus horas de enseñanza y adquirirán mejores conocimientos y al mismo tiempo se incrementará el índice de puntualidad.

1.6 ASPECTOS METODOLOGICOS

1.6.1 Paradigma

En este proyecto de disertación se utilizarán dos paradigmas descritos a continuación.

Racionalista.- Porque el proyecto tiene la implementación de software y programas.

Pragmático.- Porque el resultado final es el control de ingreso/salida de los Docentes dando importancia a los resultados obtenidos por este control.

1.6.2 Métodos de Investigación

Durante el proceso de investigación del presente proyecto de disertación, se utilizará el Método Científico para plantear las bases de la investigación. Además será una Investigación Experimental en la medida en que se desarrolla el sistema se experimentan los resultados del funcionamiento de los instrumentos de Automatización y Control.

1.6.3 Tipo de Investigación

En este proyecto se llevará a cabo una Investigación de Tipo Bibliográfica, puesto que se realizará primeramente un estudio de las especificaciones y compatibilidad del software y hardware que se adquiera, y una Investigación Experimental porque se probarán y diagnosticaran los instrumentos de automatización y Control adquiridos, antes de implementarlos en las aulas de la Escuela de Sistemas.

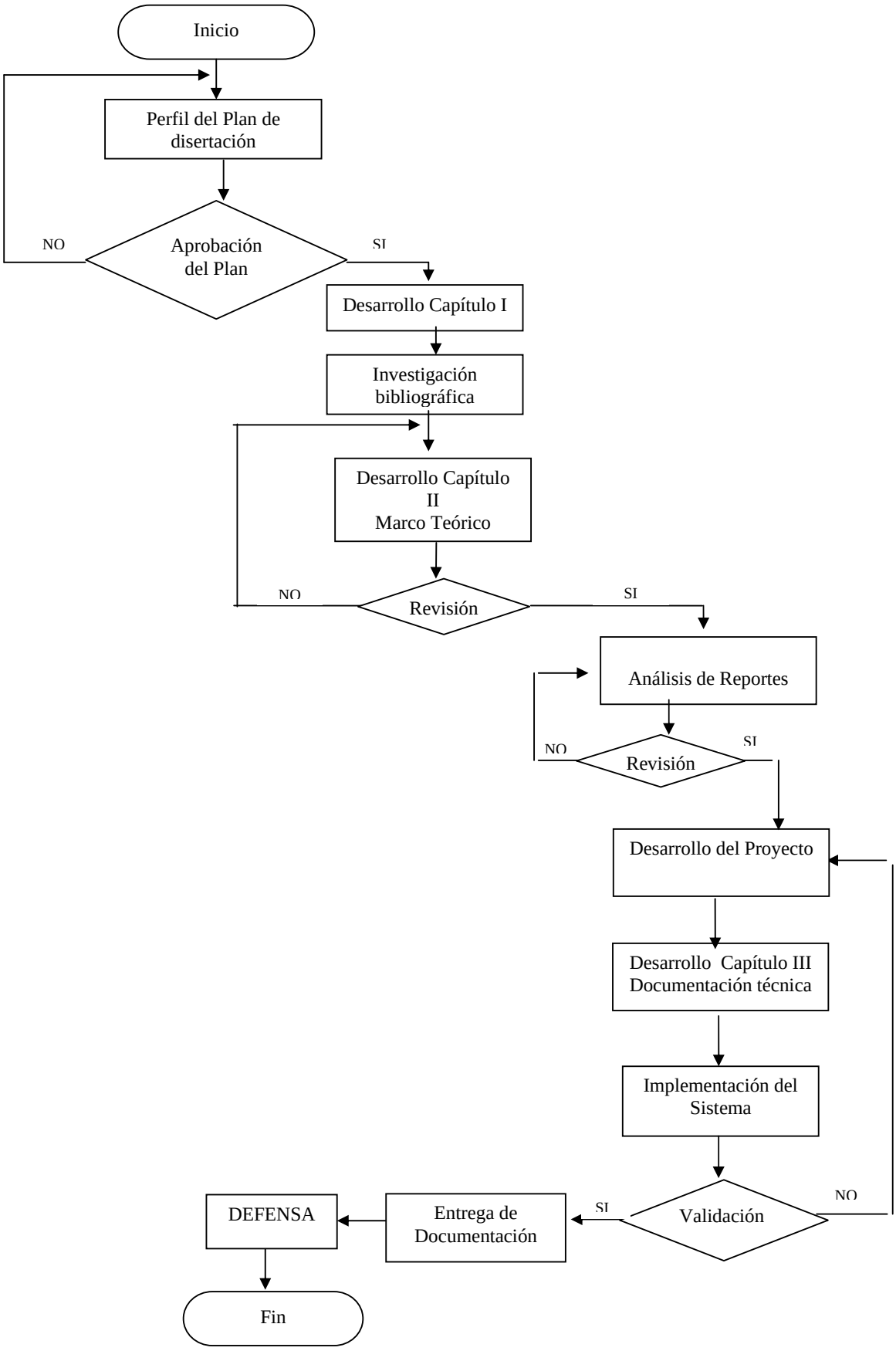
1.6.4 Técnicas de Investigación

En la presente investigación se requiere extraer información de diferentes fuentes, para esto se realizará la búsqueda de información en el Internet, así como el uso de manuales. Esto nos llevara a utilizar las técnicas de fichaje que permita clasificar y organizar las fuentes de consulta.

1.6.5 Nivel de Investigación

Descriptivo, ya que se realizará una descripción de la tecnología necesaria para la realización del control de ingreso y salida que será utilizado únicamente por los Docentes.

1.6.6 Esquema de Procedimiento



CAPITULO II

MARCO TEÓRICO

2.1 AUTOMATIZACIÓN Y CONTROL

En los últimos 20 años, los sistemas de control han sobrellavado cambios fundamentales. Estos cambios han sido liderados por una nueva arquitectura en la cual la computadora es el corazón del sistema. Los cambios en el control han transformado las aplicaciones de prueba, control y automatización de instrumentos y dispositivos de caja poco integrados y muchas veces incompatibles a sistema de control y automatización de alto desempeño y altamente integrados. En el centro de estos cambios se encuentra un componente que cada vez se hace importante, el software.

El software, es altamente integrado y productivo que permite que los ingenieros y científicos tomen ventaja de estos beneficios como:

- Avances en el hardware de las computadoras personales han impulsado mejoras en el desempeño significativas y reducción de costos en sistemas de control comparados con instrumentos tradicionales.

- Crear un conjunto de herramientas, desde arquitecturas de drivers y conectividad a instrumentos hasta ambientes de desarrollo abierto y estándares, brinda a los

ingenieros la libertad de crear nuevos sistemas de control personalizables y muy poderosos.

- Definir el control como “la manipulación directa de las magnitudes de un sistema llamado planta a través de otro sistema llamado sistema de control”

2.1.1 Conceptos y Definiciones

Automatismo: El control automático de procesos es parte del progreso industrial desarrollado durante lo que ahora se conoce como la segunda revolución industrial. El uso intensivo de la ciencia de control automático es producto de una evolución que es consecuencia del uso difundido de las técnicas de medición y control. Su estudio intensivo ha contribuido al reconocimiento universal de sus ventajas.

El control automático de procesos se usa fundamentalmente porque reduce el costo de los procesos industriales, lo que compensa con creces la inversión en equipo de control.

Automatización: Aplicación de sistemas automáticos en la realización de un proceso.

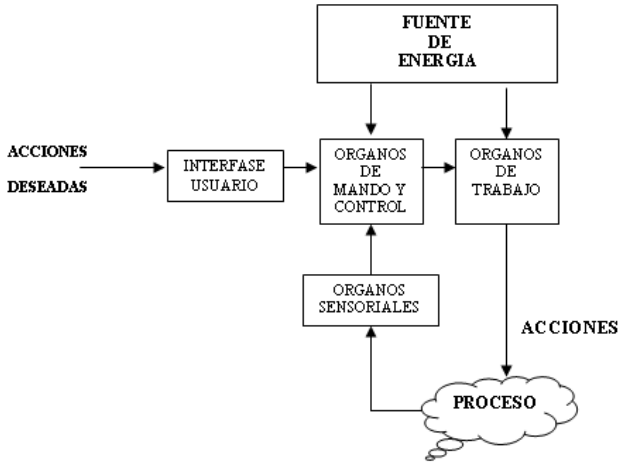


Figura 1. Elementos Sistemas Automáticos

Acciones.- Actuación sobre el medio o proceso, con frecuencia son operaciones que se pueden repetir indefinidamente. Suelen ser acciones humanas susceptibles de ser sustituidas por acciones mecánicas realizadas por los órganos de trabajo.

Fuentes de Energía.- Las operaciones y movimientos de los sistemas automáticos suponen un gasto energético que ha de ser aportado por un medio externo.

Suele denominarse fuente de potencia a aquella que suministra energía a los órganos de trabajo que actúan sobre el proceso.

Órganos de Mando y Control.- Representa el sistema que decide cuando realizar, y en su caso, el valor que han de tener algunos de los parámetros que definen una acción o tarea.

Órganos Sensoriales.- Son sistemas cuya misión consiste en captar o medir determinados valores o magnitudes durante la realización del proceso. Estos órganos

proporcionan información a los órganos de mando para que estos puedan dividir consecuentemente.

Procesos Continuos.- Las magnitudes que determinan la evolución del proceso cambian de forma continua en el tiempo.

Procesos Discretos o Discontinuos.- Las magnitudes que determinan la evolución del proceso cambian de forma discreta o discontinua y suelen tomar solo determinados valores.

El sistema evoluciona mediante eventos. Estos eventos son también conocidos como procesos de eventos discretos. En los procesos discretos se actúa sobre objetos concretos también llamados elementos discretos.

Procesos por Lotes.- Son procesos discretos en los que intervienen más de un elemento o pieza inicial para ser transformados en un solo producto.

Regulación Automática.- Mecanismos que permiten actuar durante un proceso continúo con el fin de que las magnitudes alcancen un valor determinado.

Cuando este valor se mantiene constante en el tiempo se dice que se esta ante un problema de regulación.

Cuando este valor varia en el tiempo se dice que se esta ante un problema de servomecanismo.

El concepto de Automatización industrial suele aplicarse al control de procesos discretos. Los órganos de mando reciben información discreta del proceso y proporcionan órdenes discretas sobre los órganos de trabajo.

Los sistemas de mando adquieren una estructura secuencial:

- El proceso se divide en una serie de estados.
- Cada estado se activa y desactiva de forma secuencial.
- Cada estado activo tiene asociada una serie de acciones.

2.1.2 Automatización de Procesos

La simulación se ha constituido en una gran herramienta para el diseño, análisis, y optimización de sistemas y procesos industriales. La disponibilidad de computadores personales cada vez más avanzada con menor costo y de fácil uso, acompañados por programas de aplicación y lenguajes de programación altamente flexibles, ha permitido la masificación del uso de diferentes técnicas de simulación y control de procesos. Este trabajo se concreta en la aplicación de técnicas de modelaje, simulación y control de procesos haciendo uso de la tecnología PC y un lenguaje de programación netamente gráfico que permite la construcción de modelos mediante un paradigma de programación. Cambiando este lenguaje de programación con tareas de adquisición y control entrada/salida para el PC, se puede configurar un sistema de simulación y control capaz de manejar señales reales (analógicas y digitales, de entrada y salida) y ejecutar modelos matemáticos de control de procesos en tiempo real.

La simulación de sistemas se ha convertido en una poderosa herramienta para la toma de decisiones que nos permite lo siguiente:

- Predecir el resultado de las acciones que se tomen sobre el proceso o sistema de control.
- Comprender porqué los eventos ocurren.
- Identificar áreas problemáticas antes de la implementación del sistema.
- Explorar los efectos de las modificaciones.
- Evaluar ideas y su viabilidad e identificar sus ineficiencias.

2.1.3 Autómatas Programables

Los autómatas programables aparecieron en los Estados Unidos de América en los años 1969 – 1970, particularmente en el sector de la industria del automóvil; fueron empleados en Europa alrededor de dos años mas tarde. Su fecha de creación coincide con la era del microprocesador y con la generación de la lógica cableada modular.

El autómata es la primera máquina con lenguaje, es decir, un calculador lógico cuyo juego de instrucciones se orienta hacia los sistemas de evolución secuencial. El autómata programable es un percusor y constituye para los automatistas un esbozo de la maquina ideal.

El autómata programable satisface las exigencias tanto de procesos continuos como discontinuos. Regula presiones, temperaturas, niveles y caudales así como todas las funciones asociadas de temporizacion, cadencia, conteo y lógica. También incluye

una tarjeta de comunicación adicional, el autómata se transforma en un poderoso satélite dentro de una red de control distribuida.

Figura 2. Autómata

El autómata programable es un aparato electrónico programable por un usuario programador y destinado a gobernar, dentro de un entorno industrial, máquinas o procesos lógicos secuenciales.

Un autómata programable esta constituido por:

Fuentes de Alimentación.- Es la encargada de convertir la tensión de la red, de 220v de corriente alterna baja a tensión de corriente continua normalmente a 24v. Siendo esta la tensión de trabajo en los circuitos electrónicos que forma el autómata.

Unidad Central de Procesos o CPU.- Se encarga de recibir las ordenes del operario por medio de la consola de programación y el modulo de entradas. Posteriormente las procesa para enviar repuestas al modulo de salidas. En su memoria se encuentra residente el programa destinado a controlar el proceso.

Contiene las siguientes partes:

- Temporizadores y contadores
- Memoria de programa

- Memoria de datos
- Memoria imagen de entrada
- Memoria de salida

Módulo de Entrada.- Es al que se unen los captadores (interruptores, finales de carrera, pulsadores). Cada cierto tiempo el estado de las entradas se transfiere a la memoria imagen de entrada. La información recibida en ella, es enviada al CPU para ser procesada de acuerdo a la programación.

Se pueden diferenciar dos tipos de captadores conectables al módulo de entrada:

- **Los captadores pasivos.-** Son los que cambian su estado lógico (activado o no activado) por medio de una acción mecánica. Estos son los interruptores, pulsadores, finales de carrera.

- **Los captadores activos.-** Son dispositivos electrónicos que suministran una tensión al autómata, que es función de una determinada variable.

Módulo de Salidas.- Es el encargado de activar y desactivar los actuadores (bobinas de contactores, lámparas, motores pequeños).

La información enviada por las entradas al CPU, una vez procesada, se envía a las memorias imagen de salidas, de donde se envía a la interfase de salidas para que estas sean activadas y a la vez los actuadotes que en ellas están conectados.

Según el tipo de proceso a controlar por el autómata, podemos utilizar diferentes módulos de salidas. Existen tres tipos que son:

- **A relés.-** Son usados en circuitos de corriente continua y corriente alterna. Están basados en la conmutación mecánica, por la bobina del relé, de un contacto eléctrico normalmente abierto.

- **A triac.-** Se utilizan en circuito de corriente continua y corriente alterna que necesitan maniobras de conmutación muy rápidas.

- **A transistores a colector abierto.-** Son utilizados en circuitos que necesiten maniobras de conexión / desconexión muy rápidas. El uso de este tipo de módulos es exclusivo de los circuitos de corriente continua.

Terminal de Programación.- El terminal o consola de programación es el que permite comunicar al operario con el sistema. Las funciones básicas son las siguientes:

- Transferencia y modificación de programas
- Verificación de la programación
- Información del funcionamiento de los procesos

Como consolas la programación pueden ser utilizadas las construidas específicamente para el autómata, tipo calculadora o bien un ordenador personal, que

soporte un software específicamente diseñado para resolver los problemas de programación y control.

Periféricos.- Los periféricos no intervienen directamente en el funcionamiento del autómata, pero sin embargo ayuda a la labor del operario.

Los más utilizados son:

- Grabadoras a cassettes.
- Impresoras.
- Cartuchos de memoria EPROM.
- Visualizadores y paneles de operación OP.
- Memorias EEPROM.

2.2 HUELLAS DIGITALES

La identificación biométrica es la verificación de la identidad de una persona basado en características de su cuerpo o de su comportamiento, utilizando por ejemplo la mano, el iris del ojo, la voz o la cara en el reconocimiento facial. Los métodos de identificación biométrica, como aquellos usados en las películas de James Bond, el inolvidable agente 007, que nos parecían increíbles hace unos años, son ahora una realidad.

Aunque los estudios biométricos no son perfectos, sí son una herramienta muy poderosa para identificar personas. De todos los sistemas de identificación

biométrica existentes, las huellas dactilares son las únicas legalmente reconocidas como prueba fidedigna de identidad. Es un sistema que además de ser efectivo, es cómodo de aplicar y la autenticación se obtiene rápidamente.

Huellas digitales, insumo de la bioidentificación.

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo.

Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce una copia o negativo de la huella.

Las huellas digitales se toman de los dedos índices de ambas manos, tanto por la comodidad al capturarlas, como porque estos dedos están menos propensos que los pulgares a sufrir accidentes que dejen cicatriz.

Son únicas e irrepetibles aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente.

La gente tiene diminutos "valles y crestas" de piel en la punta de los dedos que eran de gran utilidad a los ancestros de la raza humana, pues les permitían asir cosas con mayor facilidad. Estos valles y crestas se forman por una combinación de factores genéticos y ambientales aleatorios, como la posición del feto en un momento particular y la composición y densidad exacta del líquido amniótico que lo rodea.

Antecedentes

Las huellas digitales han tenido diferentes usos a lo largo de la historia de la humanidad. Debido a que las huellas digitales son un rasgo distintivo entre los seres humanos, estas han sido utilizadas como medio de identificación. Según B.C. Bridgest, especialista en la materia, las huellas digitales comenzaron a usarse en las antiguas civilizaciones.

“Algunos de lo primeros usos prácticos de la identificación mediante impresiones dactilares son acreditados a los chinos; quienes la aplicaban diariamente en sus negocios y empresas legales mientras tanto el mundo occidental se encontraba en el periodo conocido como la edad oscura”.

Asimismo, dice Bridgest, en el libro de leyes chino de Yung Hwui:
“Se establecía que para divorciarse de la esposa, el esposo debía dar un documento que expusiera siete razones para hacerlo. Todas las letras deberían estar escritas con su propia mano y signar el documento con sus huellas dactilares”

A las huellas digitales, también se les menciona en la Biblia:

“Y puso un sello sobre su mano para memoria ante sus ojos” (Éxodo 13:9) y se refiere a ellas precisamente como una característica distintiva entre los seres humanos.

En investigaciones criminalísticas han sido utilizadas desde el siglo XIX y en la actualidad, haciendo uso de métodos electrónicos se constituyen en un recurso mucho más efectivo en este campo.

En México (artículo 1834 del Código Federal Civil) como en otros países del mundo, las huellas digitales son reconocidas legalmente como sustituto de la firma escrita, indispensable para imponer obligación en un contrato o documento, en los casos en que la persona involucrada no pueda o no sepa firmar.

Figura 3. Una huella digital

Clasificación:

En la figura 4 aparecen 8 puntos característicos que hay en un dedo, éstos se repiten indistintamente para formar entre 60 y 120 (por ejemplo 10 orquillas 12 empalmes 15 islotes, etc.) A estos puntos también se llaman minutae, o minucias, término utilizado en la medicina forense que significa “punto característico”

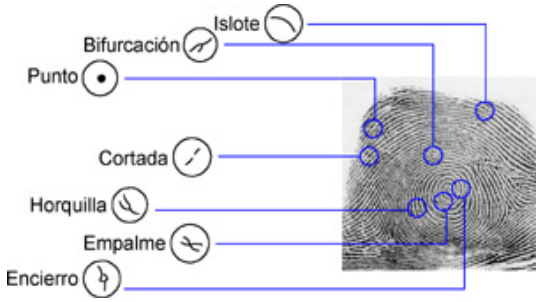


Figura 4. Clasificación de la huella digital

En la actualidad, la huella digital es capturada por un aparato electrónico, el cual obtiene la huella y la clasifica. Los criterios de clasificación se basan en algoritmos diseñados para distinguir las principales características de la huella, y almacenar la mayor cantidad de información posible.

La intención de la tecnología de huella digital es identificar de manera precisa y única a una persona por medio de su huella digital. Certificando la autenticidad de las personas de manera única e inconfundible por medio de un dispositivo electrónico que captura la huella digital y de un programa que realiza la verificación.

Las contraseñas proporcionan algo de protección, pero recordar y saber dónde están guardados los diferentes códigos de cada máquina es un problema en sí mismo. Con las tarjetas inteligentes, sucede algo similar: si perdemos nuestra tarjeta no podremos hacer uso de las facilidades que brinda. Parecería lógico utilizar algún identificador que no se pudiese perder, cambiar o falsificar. Las técnicas de la biometría se aprovechan del hecho de que las características del cuerpo humano son únicas y fijas. Los rasgos faciales, el patrón del iris del ojo, los rasgos de la escritura, la huella

digital, y otros son los que se utilizan para estas funciones, incluyendo incluso el ADN.

2.2.1 Características

Podríamos decir que los seres humanos tienen tarjetas de identificación integradas, muy fácilmente accesibles: sus huellas digitales, las cuales son diseños realmente únicos.

Un lector de huella digital lleva a cabo dos tareas:

- Obtener una imagen de su huella digital, y
- Comparar el patrón de valles y crestas de dicha imagen con los patrones de las huellas que tiene almacenadas.

Los métodos principales de obtener una imagen de una huella digital son:

Sensores Ópticos Reflexivos.- Se basan en la técnica más antigua, consiste en colocar el dedo sobre una superficie de cristal o un prisma que está iluminado por un diodo LED. Cuando las crestas de las huellas del dedo tocan la superficie, la luz es absorbida, mientras que entre dichas crestas se produce una reflexión total. La luz resultante y las zonas de oscuridad son registradas en un sensor de imagen.

En la práctica existen algunas dificultades con esta técnica: las imágenes obtenidas con dedos húmedos y secos son muy diferentes y, además, el sistema es sensible al

polvo y a la suciedad de la superficie. La unidad tiene un tamaño considerable, poco práctico y caro. Este sistema es fácil de engañar y si la piel está deteriorada o dañada, la huella no se reconoce correctamente. El reconocimiento de la huella dactilar de las personas mayores también es difícil de hacer ya que la piel no es lo suficientemente elástica. En algunas circunstancias esto puede producir un reconocimiento falso. Si la huella almacenada fue tomada con menos presión, se pueden producir aceptaciones falsas.

Sensores Ópticos Transmisivos.- Esta técnica funciona sin contacto directo entre el dedo y la superficie del sensor. La luz pasa a través del dedo desde la cara de la uña, y al otro lado, mientras que una cámara toma una imagen directa de la huella digital. La humedad no produce ninguna dificultad. El sensor ve a través de la superficie de la piel sobre una superficie más profunda y produce una imagen multiespectral. El uso de diferentes longitudes de onda para generar imágenes nos proporciona información de diferentes estructuras subcutáneas, indicación de que el objeto en cuestión es un dedo genuino. El uso de filtros polarizados ortogonales asegura que solamente la luz que tiene importancia a su paso bajo la piel es la que pasa, y bloquea la luz que se reflejaría directamente de la superficie. Solamente unos dedos artificiales muy precisos podrían tener la posibilidad de engañar a este sensor.

Sensores Capacitivos.- El sensor es un circuito integrado de silicio cuya superficie está cubierta por un gran número de elementos transductores (o píxeles), con una resolución típica de 500 dpi. Cada elemento contiene dos electrodos metálicos adyacentes. La capacidad entre los electrodos, que forma un camino de realimentación para un amplificador inversor, se reduce cuando el dedo se aplica

sobre dicha superficie: se reduce más cuando detecta crestas y menos cuando detecta el espacio entre ellas.

El sensor es susceptible a las descargas electrostáticas. Estos sensores sólo trabajan con pieles sanas normales, ya que no son operativos cuando se utilizan sobre pieles con zonas duras, callos o cicatrices. La humedad, la grasa o el polvo también pueden afectar a su funcionamiento.

Sensores de Alta Frecuencia.- Estos sensores son una variación de la técnica capacitiva descrita anteriormente. Cada píxel contiene un único electrodo, mientras que el dedo actúa como el otro electrodo, o de manera más precisa, el electrodo es la capa subcutánea, que es un buen conductor y que no se ve afectada por la grasa, el polvo, los callos o perturbaciones similares. Un contacto más exterior, rodeado por una señal débil de RF, se acopla sobre el dedo. La amplitud de la señal en cada electrodo es pues proporcional a la capacidad de acoplamiento local: si es más elevada indica que se trata de una cresta, mientras que si es menos elevada se trataría de un valle entre crestas.

A diferencia de los sensores capacitivos anteriores, esta técnica puede detectar las crestas y los valles en la capa de las células vivas en lugar de la superficie de piel de las células muertas. La tensión y la frecuencia de la señal de RF se pueden ajustar para obtener la mejor imagen.

Sensores Mecánicos.- Se trata de decenas de miles de diminutos transductores de presión que se montan sobre la superficie del sensor. Un diseño alternativo utiliza

conmutadores que están cerrados cuando son presionados por una cresta, pero permanecen abiertos cuando están bajo un valle. Esto sólo proporciona un bit de información por píxel, en lugar de trabajar con una escala de grises.

Sensores Térmicos.- En este caso el sensor detecta el calor conducido por el dedo, el cual es mayor cuando hay una cresta que cuando hay un valle. Se ha desarrollado un componente de silicio con una matriz de píxeles denominado "FingerChip", es decir, "circuito integrado al dedo", cada uno de los cuales está cubierto con una capa de material piroeléctrico en el que un cambio de temperatura se traduce en un cambio en la distribución de carga de su superficie. La imagen está en la escala de grises que tiene la calidad adecuada incluso con el dedo desgastado, con suciedad, con grasa o con humedad. El sensor dispone de una capa protectora robusta y puede proporcionar una salida dinámica.

2.2.2 Fundamentos

Los lectores de huella digital computarizados siempre han aparecido en películas de espías resguardando el acceso a lugares restringidos, pero en el mundo real eran una tecnología bastante exótica hasta hace unos años, cuando empezaron a aparecer en todos lados para controlar el acceso a edificios que necesitaban alta seguridad, e incluso en "mouse" y teclados para computadora, reemplazando o complementando el uso de passwords para dar acceso a una PC.

En la televisión los lectores de huella digital típicamente empalman varias imágenes de huellas digitales para encontrar una que corresponda. En realidad, este no es un

modo práctico para comparar las huellas digitales. Una imagen borrosa puede hacer que dos imágenes de la misma huella se vean bastante diferentes, así que raramente se podrá obtener un empalme perfecto. Adicionalmente, utilizar la imagen completa de la huella digital en un análisis comparativo utiliza muchos recursos del procesador, y además hace más sencillo robar los datos impresos de la huella de alguien.

En vez de esto, la mayoría de los lectores compara rasgos específicos de la huella digital, generalmente conocidos como minutae. Típicamente, los investigadores humanos y computadoras se concentran en puntos donde las líneas de las crestas terminan o donde se separan en dos (bifurcaciones). Colectivamente estos y otros rasgos distintivos se llaman típica.

El software del sistema del lector utiliza algoritmos altamente complejos para reconocer y analizar estas minutae. La idea básica es medir las posiciones relativas de la minutae.

Una manera simple de pensar en esto es considerar las figuras que varios minutae forman cuando dibuja líneas rectas entre ellas. Si dos imágenes tienen tres terminaciones de crestas y dos bifurcaciones formando la misma figura dentro de la misma dimensión, hay una gran probabilidad de que sean de la misma persona.

Para obtener una coincidencia, el sistema del lector no necesita encontrar el patrón entero de minutae en la muestra y en la imagen almacenada, simplemente debe

encontrar un número suficiente de patrones de minutae que ambas imágenes tengan en común. El número exacto varía de acuerdo a la programación del lector.

2.2.3 Dispositivos Lectores de Huellas Digitales

HandPunch.- Este usa la tecnología de geometría biométrica. La terminal captura una imagen tridimensional de la mano cada vez que una persona marca. El tamaño y forma de la mano son usados para verificar la identidad con una exactitud sin igual, las huellas digitales de la mano no son usadas. Luces rojas y verdes le notifican a la persona de su estado cada vez que marca. Tiene un teclado para la programación y administración de los datos.

Es un equipo muy robusto y confiable, recomendado para ambientes extremos, plantas industriales, en general, lugares donde las personas no siempre tienen las manos limpias. El cual es un requisito indispensable si planea usar huella digital.

Figura 5. HandPunch

Lector de huella digital USB.- Es la solución más económica para el control de personal y control de comedor, entre otras aplicaciones. Tiene un sensor óptico y un conector USB y debe conectarse a un computador para su funcionamiento, el mismo

que puede ser usado en otras actividades, mientras SquareNet funciona en background.

El reconocimiento de huellas es muy rápido y preciso (menor a un segundo). A la vez que el registro de las personas es un proceso muy sencillo.

Figura 6. Lector de huella digital USB

Lector de Huellas RS-120S.- Es un producto que permite la captura, procesamiento y verificación de huellas digitales utilizando el mismo como un periférico de entrada más en una equipo que opera con los Sistemas Operativos Windows. El mismo realiza un barrido óptico de alta resolución y a partir de la imagen así obtenida por medio de sofisticados algoritmos matemáticos obtiene un "template" o "firma" de dicha huellas, la cual puede servir para determinar y verificar la identidad de una persona con distintos fines aplicativos. El mismo dispositivo también tiene por medio de su capacidad de procesamiento integrada, la posibilidad de realizar la comparación de dos huellas y determinar con un alto grado de seguridad si las mismas pertenecen o no a la misma persona. En esta operación el dispositivo posee extremadamente bajos valores de los índices de performance FRR y FAR (False Reject Ratio o sea probabilidad de rechazar como falsa una huella que debería ser aceptada como perteneciente al sujeto en verificación; Falsa Aceptación Ratio o sea

probabilidad de aceptar como verdadera una huella que no pertenece al sujeto en verificación).

Con su capacidad de lectura en los 360°, no tiene ninguna importancia como sea presentado el dedo sobre el lector para que se pueda realizar una correcta verificación o rechazo de su correspondiente huella digital (en muchos otros lectores del "eje" del dedo debe ser orientado dentro de un estrecho ángulo con respecto al eje del lector, para que su funcionamiento sea satisfactorio)

Figura 7. Lector de Huellas RS-120S

De muy sencilla instalación en un puerto USB 2.0 para aprovechar al máximo su velocidad el dispositivo puede ser utilizado en el control de acceso a sistemas, archivos, etc. Dicha instalación es totalmente "Plug & Play" y los drivers son provistos en el CD-ROM acompañante, así como las aplicaciones FingerUser que permite el control de acceso a equipos bajo Windows y la aplicación FingerLock que permite la encripción de archivos, carpetas enteras o aún discos enteros utilizando como clave para dicha encripción la huella digital capturada, tal que dichos archivos o carpetas solo serán accesibles (abrir, modificar) para la persona que posee la huella digital con la cual se realizó la encripción.

Como un valor adicional, el dispositivo podrá ser integrado en cualquier aplicación para actividades tales como control de acceso a sitios protegidos, control de horarios,

apertura de puertas o barreras, operaciones de comercio electrónico, sistemas de fidelidad del clientes, cobro de pensiones u otros beneficios, etc. En otras palabras: en toda aplicación en donde el determinar con precisión y certeza la identidad de una persona sea un tema relevante. Para esta integración será necesario la compra por separado de un SDK que provee la librería y DLL necesarias para contar con las funciones de captura de la huella (imagen y su template), las funciones de verificación de huellas y las otras funciones necesarias para la operación del dispositivo desde una aplicación que invoca e integra dichas funciones (dicha integración es posible desde múltiples lenguajes de programación en uso hoy en día en el entorno Windows como lo son Visual C++, Delphi, Visual Basic, etc.).

Funcionalidades:

- Instalación Plug & Play
- Cumple plenamente con las especificaciones USB 2.0, compatible con USB 1.1
- Alta definición de las imágenes capturadas
- Sistema monolítico lo cual garantiza que no habrá riesgos de pérdida de calidad debida a desajustes en la óptica.
- Diseño ergonómico y compacto.
- Moderado consumo y sin necesidad de fuentes de alimentación adicionales.
- Permitir el control de acceso a PCs, servidores, sitios WEB, etc.
- Protección de documentos con encripción de alto nivel.
- Protección de la identidad en actividades de comercio electrónico e Internet (seguridad y confidencialidad).
- SDK opcional para la integración a otras aplicaciones del usuario

Especificaciones:

- Tiempo de captura menor a 2 segundos (enrolamiento)
- Tiempo de verificación menor a 1 segundo
- Voltaje de operación: 5 V CC (provistos por la interfase USB)
- Consumo: Menor a los 200 mA
- Comunicación con el PC: USB 2.0
- Resolución mejor que 500 dpi
- Ángulo de captura: 360°
- Temperatura de operación: de -5 ° C a 50 ° C
- Humedad relativa ambiente: entre el 10 y 80% (sin condensación)
- Sistemas operativos soportados: Windows 2000, Windows XP

Terminal KIMALDI KBIO OFFLINE.- Control de accesos con identificación biométrica por huella dactilar. Sistema seguro y fiable. Elimina la posibilidad de suplantación de identidad por transferencia y duplicación de tarjetas o códigos. Simplemente con poner el dedo sobre el lector el usuario es identificado, si se trata de un usuario registrado, se produce la apertura automática del acceso. Control de accesos con identificación biométrica off-line de huella dactilar y gestión de usuarios de la base de datos on-line.

Figura 8. Terminal KIMALDI KBIO OFFLINE

Características del Sistema:

Control de accesos con identificación biométrica off- line de huella dactilar y gestión de usuarios de la base de datos on-line. Disponible en conectividad RS-232, Ethermet (TCP/IP y UDP), Wi-Fi (o CAN según proyecto).

Control de acceso biométrico de huella dactilar y adicionalmente con lectura de proximidad y banda magnética.

Los modelos biométricos incorporan un registro de 8.000 eventos que guardan la fecha, hora y resultado de la identificación. El registro de eventos se recupera mediante interrogación a partir del programa del host.

Disponible matching biométrico de huella dactilar 1:N y 1:1 (biometría más proximidad).

Funcionamiento de los modos de Control de Accesos

El terminal KBio-Offline tiene la capacidad de ejecutar identificaciones por cuenta propia, y a partir de ahí activar el relé de acceso. Para ello, se requiere el sensor

biométrico FIM01, que incorpora un potente motor de búsqueda, a la vez que permite la gestión centralizada de los procesos de alta y baja de usuarios.

También se gestionan desde el Host aquellas funciones adicionales que el integrador del sistema quiera añadir (las teclas F1 y F2, así como las entradas digitales, están para este propósito).

Control de Accesos, modo Offline

Como el propio nombre del producto indica, el modo de funcionamiento habitual para este terminal es el Control de Accesos, en modo Offline. Así pues, una vez el Host haya programado el FIM01 con las huellas dactilares autorizadas, se puede operar de modo totalmente independiente de dicho Host: el terminal KBio-Offline recibe una petición de acceso a través de su interfase de usuario y pone en marcha el FIM01 para el proceso de identificación. Si la identificación llevada a cabo resulta positiva, se activa un relé para apertura de acceso. El evento es comunicado al Host a modo puramente informativo y sin perjuicio del funcionamiento autónomo del dispositivo.

La interacción con el usuario viene definida por una serie de parámetros que se pueden configurar desde el Host y son almacenados en la memoria no volátil del terminal:

- Time-Out del proceso de identificación.
- Temporizacion del relé de apertura de acceso.
- Temporizacion de la interfase de usuario (LED verde, LED rojo, zumbador).
- Tiempo de guarda de la barrera óptica.

El usuario puede iniciar el proceso de identificación simplemente situando sobre el sensor biométrico un dedo que haya sido previamente registrado. La barrera óptica situada sobre el sensor detectará la presencia del dedo y desencadenará el proceso de identificación por parte del FIM01.

De modo alternativo, se puede iniciar el proceso de identificación pulsando la tecla verde de entrada sobre la carátula del terminal.

A continuación, el sensor FIM01 procederá al escaneo de la huella digital. Si el resultado de la identificación es positivo, se activará el relé de apertura de acceso. También se activará el LED verde de la KBio-Offline y se mandará un evento al Host 1. Si por el contrario la identificación es negativa, se activarán el LED rojo y el zumbador.

Control de Accesos: otras funcionalidades

Existen dos teclas más, F1 y F2, y tres entradas digitales, cuya operación es reportada al Host (ver sucesos Status de las entradas digitales y Pulsación de tecla). De este modo, se pueden definir funcionalidades adicionales en modo Online.

También es posible bloquear y desbloquear el terminal desde el Host, de forma que no se puedan producir identificaciones ni accesos.

Dada la capacidad del sensor biométrico FIM01 para almacenar marcajes, se ha incorporado al terminal KBio-Offline la funcionalidad de Control de Presencia.

El terminal KBio se encarga de asociar a cada marcaje del sensor FIM01 un código de incidencia, que el usuario debe marcar antes de iniciar la identificación.

Adicionalmente, se puede configurar el terminal KBio para que actúe un relé de acceso ante un marcaje correcto. De esta forma, obtenemos un terminal biométrico con Control de Presencia y Acceso.

Estas prestaciones se combinan con la posibilidad de realizar identificaciones 1:1, con lo que podemos gestionar hasta un máximo de 4000 usuarios registrados.

Modo Control de Presencia

El modo por defecto de Control de Presencia se realiza mediante identificación 1:N. Su principal ventaja es la de no requerir ningún elemento adicional para identificar usuarios (es decir, no hace falta distribuir tarjetas de identificación), aunque el tiempo necesario para la identificación no lo hace recomendable para más de 500 usuarios.

El terminal KBio-Offline presenta, en este modo de configuración, el LED amarillo parpadeante. Con ello, se pretende indicar la necesidad de pulsar una tecla antes de iniciar la identificación. Las teclas permitidas son F1 y F2, además de sus variantes ALT+F1, ALT+F2, cuyo significado será atribuido por el software de la aplicación. La tecla verde no tiene ningún efecto. Una vez se ha pulsado la tecla adecuada, el sensor biométrico se activa inmediatamente. El usuario debe identificarse justo a continuación, de lo contrario se agota el tiempo para la identificación.

El terminal KBio-Offline responde con un código de LEDs y pitidos, en función de si la identificación ha resultado positiva ó negativa. Igualmente, se generan unas tramas de notificación hacia el Host, independientemente de si existe comunicación o no.

Los marcajes (identificación FIM01 y código de incidencia) se almacenan en el FIM01, hasta un máximo de 8192. Este número incluye todas las identificaciones (tanto positivas como negativas), aunque sólo las positivas llevan asociado un código de incidencia válido.

Características técnicas

- Dimensiones de la caja 1: 170mm x 112mm x 55mm
- Tensión de alimentación: 12VDC. ± 10%
- Consumo máximo 2: 600 mA (~450 mA en reposo)
- Sensor biométrico: Nitgen FIM01-HV
- Número máx. de usuarios:1000 (opcionalmente, 4000)
- Número máx. de marcajes: 8192.
- Conversor TCP: eCov 100 (opcional)
- Lector de proximidad: Lector Kimaldi RD125K (opcional).

Tarjeta de control

- Dimensiones: 100mm x 95mm x 25mm
- Tensión de alimentación: 12VDC.
- Consumo máximo 3: 180 mA (~140 mA en reposo)
- 9600,n,8,1 Bidireccional no simultáneo (conexión al FIM)
- Salida 5VDC: Intensidad máxima de 200 mA (conexión a FIM01)

- Interfase de usuario: Conexión a carátula de 3 LEDs y 3 pulsadores
- Barrera óptica: Conector de 4 contactos para LED y fototransistor
- Contactos relé: 1 contacto relé, normalmente abierto, 24V / 1 A
- Entradas digitales: 3 canales para la conexión de contactos relé. En circuito abierto (contacto abierto) su valor lógico será 0. En contacto a masa (contacto cerrado), valor lógico 1.

Interfase de usuario

- **Elementos de entrada:**

Barrera óptica.- Se puede iniciar una identificación simplemente colocando el dedo sobre el sensor biométrico.

Tecla verde ("entrar").- Se puede iniciar una identificación pulsando la tecla verde. Se usará obligatoriamente este modo si el LED amarillo ("Ready") está parpadeando.

Teclas F1, F2.- Códigos de incidencia en modo Control de Presencia. El teclado dispone de un modo extendido, de forma que disponemos de F1, F2, ALT+F1, ALT+F2.

Lector de Proximidad.- Opcionalmente, se puede iniciar una identificación 1:1 presentando una tarjeta de proximidad (125 Khz.) al terminal.

- **Elementos de salida:**

LED amarillo ("Ready").- Si está permanentemente encendido o en distintos modos de parpadeo, significa que el terminal está funcionando. Si está permanentemente apagado, es que el terminal no está operando.

LED verde ("OK").- Se enciende tras una correcta identificación del usuario.

LED rojo ("Error").- Se enciende tras una incorrecta identificación del usuario.

Zumbador.- Se activa en distintas circunstancias.

Barrera óptica

El terminal KBio-Offline permite controlar una barrera óptica para detectar la presencia de dedo sobre el sensor biométrico. Además de las condiciones normales de operación, la barrera óptica gestiona dos posibles situaciones de error:

Obstrucción permanente del haz. En su estado de reposo, la barrera óptica está detectando el haz de luz del LED emisor. Si no detectamos el haz durante mucho rato, podría ser debido a un fallo mecánico o electrónico. En condiciones normales, se pueden hacer entre 2 y 3 intentos de identificación consecutivos sin retirar el dedo del sensor biométrico, antes de que salte esta condición de error.

Interferencia por fuente de luz externa. Si se expone el terminal KBio-Offline a condiciones de luz solar extrema, se puede saturar el elemento receptor, y no detectar la presencia del dedo.

Tanto el bloqueo permanente del haz como la saturación del receptor desencadenan una situación de error, ante la cual el Host recibe una notificación (suceso Status barrera óptica, código 0xED). La interfase de usuario lo reflejará mediante el parpadeo del LED amarillo (“Ready”). Ante esta situación, es necesario pulsar la tecla verde (“Entrar”) para iniciar la identificación biométrica.

Se vuelve automáticamente a la normalidad en el momento en que se desbloquea el haz de luz o se elimina la interferencia externa (suceso Status barrera óptica, código 0x0D).

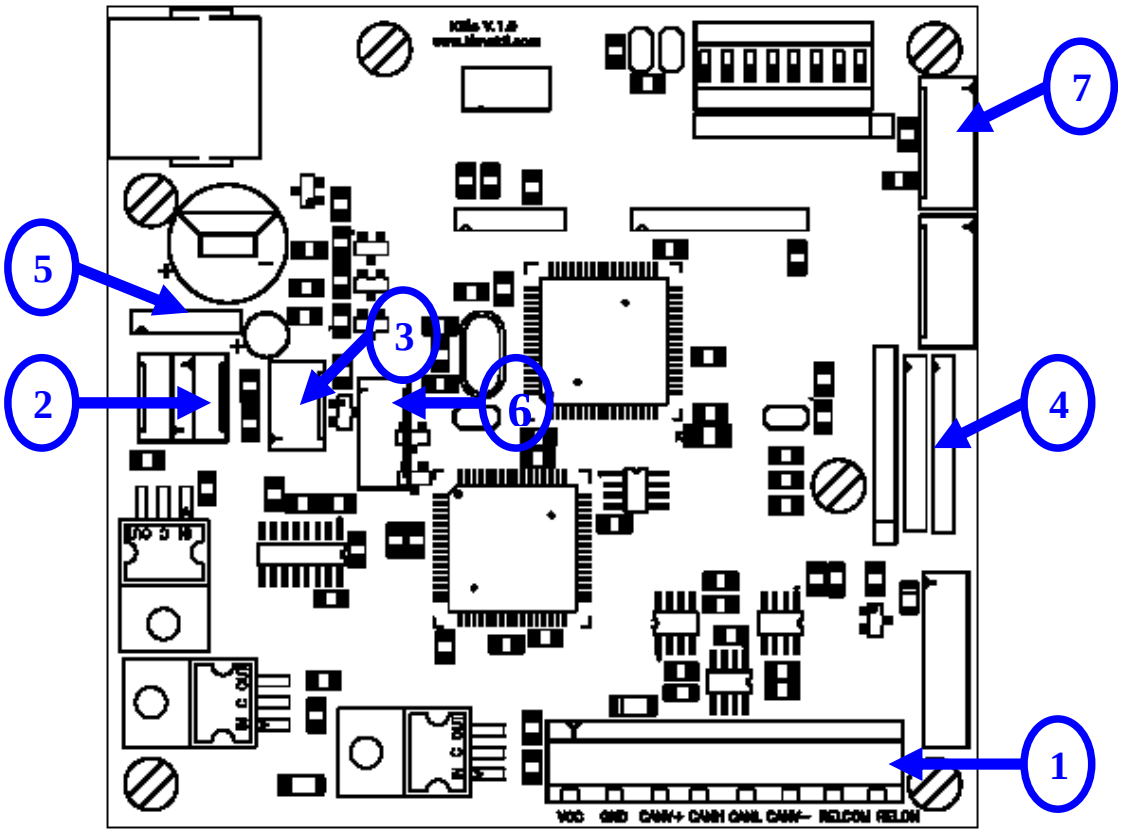


Figura 9. Esquema de conexionado

1. Conector Principal:

Pin 1 - Polo positivo alimentación (12Vcc)

Pin 2 - Polo negativo alimentación (GND)

Pin 3 - No Conectado

Pin 4 - No Conectado

Pin 5 - No Conectado

Pin 6 - No Conectado

Pin 7 - Polo 1 contacto relé 0

Pin 8 - Polo 2 contacto relé 0

2. Conector a FIM 01

3. Conector a barrera óptica

Pin 1 - Ánodo (+) del LED emisor

Pin 2 - Cátodo (-) del LED emisor

Pin 3 - Colector del Fototransistor de recepción

Pin 4 - Emisor del Fototransistor de recepción (GND)

4. Conector a carátula

Pin 1 - Ánodo (+) del LED Rojo (“Error”)

Pin 2 - Ánodo (+) del LED Verde (“OK”)

Pin 3 - Ánodo (+) del LED Amarillo (“Ready”)

Pin 4 - Común Cátodos (-) de los tres LEDs (GND)

Pin 5 - Común Teclas

Pin 6 - Tecla Verde (“Entrar”)

Pin 7 - Tecla F1

Pin 8 - Tecla F2

5. Entradas digitales

Pin 1 - GND

Pin 2 - Entrada Digital 0 (DIN 0)

Pin 3 - Entrada Digital 1 (DIN 1)

Pin 4 - Entrada Digital 2 (DIN 2)

Pin 5 – GND

6. Conector a eCov100 / RS-232:

Pin 1 - No Connect

Pin 2 - No Connect

Pin 3 - Señal Tx 232 al host (Pin nº 2 conector SubD hembra)

Pin 4 - Señal Rx 232 al host (Pin nº 3 conector SubD hembra)

Pin 5 - GND (Pin nº 5 conector SubD hembra)

Pin 6 - Salida 5VDC *para conversor eCov 100 solamente.*

7. Conector a lector de Proximidad RD125K (opcional).

2.2.4 Controles y/o Seguridades con Huellas Digitales

Las ventajas de un sistema biométrico de huella digital son que los atributos físicos de una persona suelen ser difíciles de falsificar, uno no puede adivinar una huella

digital como adivina un password, no puede perder sus huellas digitales como pierde una llave y no puede olvidar sus huellas digitales como puede olvidar un password.
A continuación se mencionan lugares donde se esta aplicando estos métodos de seguridad.

Actualmente se encuentran los ejecutivos de las aerolíneas en los Estados Unidos gracias a un nuevo proyecto que le obligará al personal del aeropuerto a ayudar a los agentes de inmigración cuando los pasajeros se dispongan a salir de los Estados Unidos. No contentos con la toma de las huellas digitales a la entrada, el Departamento de Seguridad Nacional, ha decidido que ajustar el sistema vigente de U.S. Visit dará una muestra perfecta de quién entra y quién se queda dentro de territorio estadounidense.

Las aerolíneas están furiosas. Alegan que ya bastante tienen con los precios del petróleo y toda la parafernalia impuesta a partir luego de los atentados del 11 de septiembre como para tener que asumir entre los USD 2 mil y los USD6 mil millones de dólares que representa esa mano extra a las autoridades migratorias. Amenazan con pasarle poco a poco los gastos al viajero.

De aprobarse la nueva medida dentro de los siguientes dos meses, todos los pasajeros deberán dejar sus huellas digitales a la salida a partir de enero de 2009. En realidad, el proceso ya había iniciado una prueba piloto en algunos aeropuertos internacionales en donde cada uno de los viajeros extranjeros debía acercarse antes de abordar el avión, a una cabina similar a un ATM para someterse al escáner de huellas y a la fotografía de rigor. Los expertos aseguran que el simulacro no dio los resultados

esperados y que por ello es necesario que las aerolíneas se hagan cargo del nuevo proceso.

Pero lo que más amarga a las aerolíneas es que en medio de los difíciles años financieros muchas han recortado personal y han tratado de que sus ventanillas de registro en los aeropuertos sean una especie de autoservicio donde el mismo pasajero se imprime, se registra en el vuelo y se hace cargo de su propio equipaje hasta la zona de requisas. Los costos de poner a tono la infraestructura tecnológica para que esté conectada con el sistema nacional de inmigración serán monumentales. Sin embargo para las autoridades federales el asunto no es tan complicado. Se trata según ellos de "dividir el costo entre los millones de pasajeros en determinado número de años para hacer la carga más liviana".

La Comunidad Europea no se queda atrás y estudia seriamente el proyecto de impulsar la toma de registros biométricos para niños desde los 6 años que aspiren a visas, permisos de residencia en la UE y documentos de viaje. Para muchos, se trata de un arma eficiente contra el tráfico humano, sin embargo hay quienes se oponen a la norma por considerarla como una violación a la privacidad y a los derechos humanos.

La Unión Europea también ha sometido a consideración que todos los viajeros entrando y saliendo de Europa, sean sometidos a la toma de huellas digitales y fotografías. La idea es obtener la identificación de millones de ciudadanos y añadirlas a bases de datos que puedan ser compartidas por gobiernos amigos de todo el mundo con propósitos de estrechar más la seguridad y el control migratorio. Aún

se desconoce cuándo será implementada la nueva estrategia y se estima que será luego del próximo año.

Lo cierto es que las autoridades de los Estados Unidos ya tienen en sus archivos una base de datos de por lo menos 85 millones de personas. El FBI está formando una gran base de datos para asuntos criminales y judiciales que pueden ser intercambiados con otros países en caso de ser necesario. La idea es, según los europeos, "obtener la máxima interoperabilidad" a lado y lado del Atlántico a través de estándares comunes para huellas digitales e imágenes faciales. Incluso, las nuevas normas obligarían al pasajero a enviar su identificación y detalles del viaje mucho antes de que llegue al aeropuerto.

Detrás de estas medidas que las autoridades definen como un solo "paquete de seguridad", existe un último objetivo: el frenar aún más la inmigración ilegal. Los registros biométricos al final, crearán una especie de subclase social. Una que por temor a ser identificada plenamente -porque para entonces ni los pasaportes falsos podrán ser útiles- tendrá que vivir en la clandestinidad y presa en determinado territorio por el resto de sus días. Simplemente no podrán moverse sin ser detectados. Un gran avance, una gran tragedia.

2.2.5 Algoritmos.

Con este conjunto de puntos, el software biométrico de huella digital genera un modelo en dos dimensiones, según se muestra en el ejemplo, mismo que se almacena

en una base de datos, con la debida referenciación de la persona que ha sido objeto del estudio.

Para ello, la ubicación de cada punto característico o minutae se representa mediante una combinación de números (x, y) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir las minutaes entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible. Para llevar a cabo el proceso inverso o verificación dactilar, se utilizan estos mismos vectores, no imágenes.

			
El dedo es leído por un captor de huellas.	El dedo es codificado por el captor.	Una plantilla es generada y la imagen es comprimida	El captor guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla.

Figura 10. Procedimiento de Reconocimiento de la Huella

La biometría es el estudio de métodos automáticos para reconocer y diferenciar a los seres humanos. Para esto utiliza rasgos físicos o características de conducta, que son únicos para cada persona. Básicamente la biometría es una tecnología de seguridad

basada en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo, la huella digital, la retina, la voz, la palma de la mano, la cara, entre otros.

La biometría busca obtener, clasificar y utilizar la información de estas características, para reconocer e identificar a las personas, restringir el acceso a sitios no permitidos, controlar horarios en empresas, autenticar información, y muchas otras aplicaciones.

Para esto utiliza equipos electrónicos que desarrollan las mediciones biométricas, y algoritmos que permiten digitalizar, clasificar y almacenar la información para poder utilizarla después.

Los algoritmos encargados de clasificar las huellas digitales se basan en la forma de las mismas. Algunos algoritmos utilizados para clasificar huellas son los siguientes:

- **Mapa de detalles.-** Se elabora un mapa basado en la ubicación relativa de los detalles de la huella. De esta forma se puede crear una matriz, y ubicar los elementos de una huella digital:

- **Tipo de huella, basado en detalles.** Cada individuo posee uno y sólo un arreglo de detalles. El tipo de huella se determina por la frecuencia de aparición del elemento en la huella.

- **Basada en correlación.-** Este método es un poco más complicado, pero es con el que se obtienen los mejores resultados. El sistema de clasificación por correlación incorpora los dos sistemas anteriores, con la ventaja de que puede determinar si la huella digital presenta rotación.

Algoritmo general del sistema

El algoritmo general de un sistema biométrico basado en huellas digitales podría modelarse mediante el siguiente diagrama de bloques:

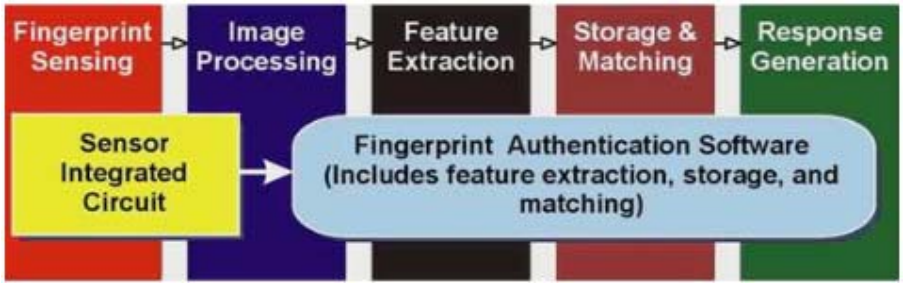


Figura 11. Algoritmo General del Sistema de Huellas Digitales.

- **Sensor de Huella digital:** Consiste en obtener la huella digital, utilizando un sensor. Generalmente se utilizan sensores capacitivos, que son dispositivos electrónicos con bastante precisión.

- **Procesamiento de imágenes:** Procesamiento de imágenes. La imagen obtenida se procesa para obtener una huella óptima. Existen algoritmos para regular el contraste, brillo y la definición de la huella, de modo que logre obtener una huella de calidad sin importar la presión del dedo sobre el sensor, ni la temperatura, ni ninguna otra variable.

- **Extracción de rasgos:** Es la extracción de características de la huella digital. Se extrae información del tipo de huella, se crea la matriz de detalles y se procesan los puntos de correlación necesarios para lograr identificar la huella posteriormente.

- **Almacenaje y correspondencia:** La huella se almacena en algún soporte, por ejemplo un disco duro, una base de datos o una tarjeta. Por ejemplo, el fabricante HID produce tarjetas inalámbricas que permiten almacenar información biométrica.

- **Generación Respuesta:** El sistema informa que el proceso está completo, que la huella ha sido verificada, analizada y almacenada de manera correcta.

2.3 REDES

Definir el concepto de redes implica diferenciar entre el concepto de redes físicas y redes de comunicación.

Respecto a la estructura física, los modos de conexión física, los flujos de datos, etc.; podemos decir que una red la constituyen dos o más ordenadores que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento, ...) sea software (aplicaciones, archivos, datos...).

Desde una perspectiva más comunicativa y que expresa mejor lo que puede hacerse con las redes en la educación, podemos decir que existe una red cuando están

involucrados un componente humano que comunica, un componente tecnológico (ordenadores, televisión, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios). Una red, más que varios ordenadores conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

Atendiendo al ámbito que abarcan, tradicionalmente se habla de:

- Redes de Área Local (conocidas como LAN) que conectan varias estaciones dentro de la misma institución,
- Redes de Área Metropolitana (MAN),
- Área extensa (WAN).

Por su soporte físico:

- Redes de cable
- Redes inalámbricas
- Redes de fibra óptica,
- Red de servicios integrados (RDSI).

Las distintas configuraciones tecnológicas y la diversidad de necesidades planteadas por los usuarios, lleva a las organizaciones a presentar cierta versatilidad en el acceso a la documentación, mediante una combinación de comunicación sincrónica y asincrónica.

La comunicación sincrónica (o comunicación a tiempo real) contribuiría a motivar la comunicación, a simular las situaciones, cara a cara, mientras que la comunicación asincrónica (o retardada) ofrece la posibilidad de participar e intercambiar

información desde cualquier sitio y en cualquier momento, permitiendo a cada participante trabajar a su propio ritmo y tomarse el tiempo necesario para leer, reflexionar, escribir y revisar antes de compartir la información. Ambos tipos de comunicación son esenciales en cualquier sistema de formación apoyado en redes.

A lo largo de la historia los ordenadores (o las computadoras) nos han ayudado a realizar muchas aplicaciones y trabajos, el hombre no satisfecho con esto, buscó mas progreso, logrando implantar comunicaciones entre varias computadoras, o mejor dicho: "implantar Redes en las computadoras"; hoy en día la llamada Internet es dueña de las redes, en cualquier parte del mundo una computadora se comunica, comparte datos, realiza transacciones en segundos.

En los Bancos, las agencias de alquiler de vehículos, las líneas aéreas, y casi todas las empresas tienen como núcleo principal de la comunicación a una RED.

Gracias a la denominada INTERNET, familias, empresas, y personas de todo el mundo, se comunican, rápida y económicamente.

Las redes agilizaron en un paso gigante al mundo, por que grandes cantidades de información se trasladan de un sitio a otro sin peligro de extraviarse en el camino.

Aplicación de las redes

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN (ya estaba antes) si genera nuevas aplicaciones viables, y algunas de ellas pueden

ocasionar importantes efectos en la totalidad de la sociedad. Para dar una idea sobre algunos de los usos importantes de redes de ordenadores, se verá brevemente tres ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación de valor añadido.

Una compañía que ha producido un modelo que simula la economía mundial puede permitir que sus clientes se conecten usando la red y corran el programa para ver como pueden afectar a sus negocios las diferentes proyecciones de inflación, de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente ó necesita de una máquina muy grande para correrlo.

Todas estas aplicaciones operan sobre redes por razones económicas: el llamar a un ordenador remoto mediante una red resulta más económico que hacerlo directamente. La posibilidad de tener un precio mas bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que solo se ocupen los enlaces de larga distancia cuado se están transmitiendo los datos.

Otra de las formas que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación(INTERNET). Como por ejemplo, el tan conocido por todos, correo electrónico (e-mail), que se envía desde una terminal, a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías e imágenes.

2.3.1 Conectividad

Una red de área local se utiliza para conectar los equipos de una organización entre sí. Sin embargo, una sola organización generalmente incluye diversas redes de área local, con lo cual a veces es necesario conectar estas redes entre sí. En tal caso, se necesita equipo especializado.

Cuando se trata de dos redes del mismo tipo, lo único que se necesita hacer es enviar las tramas de datos de una red a otra. De lo contrario, es decir, cuando las redes utilizan diferentes protocolos, será necesario convertir el protocolo antes de enviar las tramas. Por esta razón, el equipo que debe instalarse varía según la configuración de que se dispone.

El hardware principal que debe instalarse en redes de área local es:

- repetidores, utilizados para regenerar una señal;
- concentradores (hubs), utilizados para conectar múltiples hosts;
- puentes (bridges), utilizados para conectar redes de área local del mismo tipo;
- conmutadores (switches), utilizados para conectar varios elementos mientras segmentan la red.

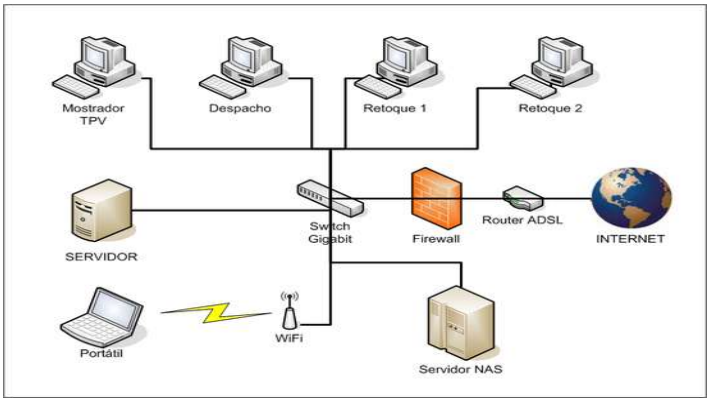


Figura 12. Redes

2.3.2 Dispositivos en Red

Una red de área local está compuesta por equipos conectados mediante un conjunto de elementos de software y hardware. Los elementos de hardware utilizados para la conexión de los equipos son:

- **La tarjeta de red** (a veces denominada “acoplador”): Se trata de una tarjeta que se conecta a la placa madre del equipo y que se comunica con el medio físico, es decir, con las líneas físicas a través de las cuales viaja la información.

- **El transceptor** (también denominado “adaptador”): Se utiliza para transformar las señales que viajan por el soporte físico en señales lógicas que la tarjeta de red puede manejar, tanto para enviar como para recibir datos.

- **El tomacorriente (socket)**: Es el elemento utilizado para conectar mecánicamente la tarjeta de red con el soporte físico.

- **El soporte físico de interconexión**: Es el soporte utilizado para conectar los equipos entre sí. Los principales medios de soporte físicos utilizados son:
  - el cable coaxial
  - el par trenzado
  - la fibra óptica.

2.3.3 Protocolos TCP-IP

Aunque poca gente sabe lo que es TCP/IP todos lo emplean indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, de entre los cuales destaca y es el más importante el protocolo IP. Bajo este nombre (TCP/IP) se esconde uno de los protocolos mas usados del mundo, debido a que es el mas usado por Internet y esta muy extendido en el sistema operativo UNIX.

En el 1973, DARPA inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información, y tenia por objetivo la interconexión de redes.

De este proyecto surgieron dos redes: Una de investigación, ARPANET, y una de uso exclusivamente militar, MILNET. Para comunicar las redes, se desarrollaron varios protocolos: El protocolo de Internet y los protocolos de control de transmisión. Posteriormente estos protocolos se englobaron en el conjunto de protocolos TCP/IP.
En 1980, se incluyo en el UNIX 4.2 de BERKELEY, y fue el protocolo militar standard en 1983. Con el nacimiento en 1983 de INTERNET, este protocolo se

popularizo bastante, y su destino va unido al de internet. ARPANET dejo de funcionar oficialmente en 1990.

TCP/IP es un conjunto de protocolos. La sigla TCP/IP significa "Protocolo de control de transmisión/Protocolo de Internet" y se pronuncia "T-C-P-I-P". Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del protocolo TCP y del protocolo IP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos. Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos:

- Dividir mensajes en paquetes;
- Usar un sistema de direcciones;
- Enrutar datos por la red;
- Detectar errores en las transmisiones de datos.

El conocimiento del conjunto de protocolos TCP/IP no es esencial para un simple usuario, de la misma manera que un espectador no necesita saber cómo funciona su red audiovisual o de televisión. Sin embargo, para las personas que desean administrar o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental.

Algunos de los motivos de su popularidad son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en maquinas de cualquier tamaño

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- Conectividad Universal a través de la red
- Reconocimientos de extremo a extremo
- Protocolos estandarizados

Estructura Interna.- El modelo básico en internet es el modelo Cliente/Servidor. El Cliente es un programa que le solicita a otro que le preste un servicio. El Servidor es el programa que proporciona este servicio.

La arquitectura de Internet esta basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (Internacional Standard Organization) para la interconexión de sistemas abiertos (OSI).

2.3.4 Configuraciones

- **Dirección IP**

Los equipos comunican a través de Internet mediante el protocolo IP (Protocolo de Internet). Este protocolo utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro números enteros (4 bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 194.153.205.26 es una dirección IP en formato técnico.

Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva.

El organismo a cargo de asignar direcciones públicas de IP, es decir, direcciones IP para los equipos conectados directamente a la red pública de Internet, es el ICANN (Internet Corporation for Assigned Names and Numbers) que remplaza el IANA desde 1998 (Internet Assigned Numbers Agency).

Una dirección IP es una dirección de 32 bits, escrita generalmente con el formato de 4 números enteros separados por puntos. Una dirección IP tiene dos partes diferenciadas:

- los números de la izquierda indican la red y se les denomina netID (identificador de red).
- los números de la derecha indican los equipos dentro de esta red y se les denomina host-ID (identificador de host).

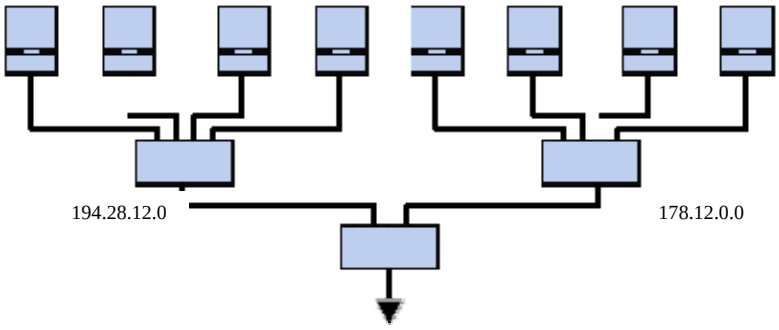


Figura 13. Ejemplo de Red

En una red escrita 58.0.0.0. Los equipos de esta red podrían tener direcciones IP que van desde 58.0.0.1 a 58.255.255.254. Por lo tanto, se trata de asignar los números de forma que haya una estructura en la jerarquía de los equipos y los servidores.

Cuanto menor sea el número de bits reservados en la red, mayor será el número de equipos que puede contener.

De hecho, una red escrita 102.0.0.0 puede contener equipos cuyas direcciones IP varían entre 102.0.0.1 y 102.255.255.254 (256*256*256-2=16.777.214 posibilidades), mientras que una red escrita 194.24 puede contener solamente equipos con direcciones IP entre 194.26.0.1 y 194.26.255.254 (256*256-2=65.534 posibilidades).

- **IPV6**

IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF

(Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características.

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades.

Características principales

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y mas nodos direccionables.

- Simplificación del formato del Header. Algunos campos del header IPv4 se quitan o se hacen opcionales
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, mas simple, que agiliza su procesado por parte del router.
- Posibilidad de paquetes con carga útil (datos) de mas de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en agregación.
- Capacidades de autenticación y privacidad.

CAPITULO III

CONTROL DE HUELLA DIGITAL

3.1 ANALISIS

3.1.1 Objetivo de Análisis

Determinar los requerimientos, delimitaciones, procesos y funciones de los dispositivos de huellas digitales para el sistema de control de ingreso y salida de los Docentes de la Escuela de Sistemas de la PUCESA.

3.1.2 Descripción General

En esta sección se realiza una descripción general de los dispositivos de huella digital desde la perspectiva técnica y de uso por parte de usuarios cuyo perfil se explica.

Perspectiva

El uso de dispositivos de huella digital el control de ingreso y salida de los docentes, será una aplicación de mucha utilidad y de fácil funcionalidad, los dispositivos son cajas Kbio Offline que interactúan conjuntamente con el sistema de control de ingreso y salida del personal docente de la Escuela de Ingeniería en Sistemas de la PUCESA .

Funciones

- **Entrada**

Dentro de las funciones de Entrada para los dispositivos de huella digital, se requerirá el registro de las huellas de todos los docentes de la Escuela de Sistemas.

El ingreso, modificación y eliminación así como su correcto registro de huellas de los docentes y su información relacionada como son: nombre del docente, fecha, hora, IP, aula. Se lo realizara con el sistema de control de ingreso y salida del personal.

- **Procesamiento**

Con los registros de las huellas en los dispositivos KBio, se realizaran los siguientes procesos:

- Validación de huella ingresada correctamente, para información requerida sobre el acceso de usuario y control.
- Verificación de la existencia de huella del docente, requerida para la realización de los procesos de manera adecuada.
- Búsqueda y extracción de datos de la caja del Kbio.
- Marcaje de las huellas de los docentes a sus horas de entrada y salida de clases.

- **Salidas**

El uso de dispositivos de huella digital, permitirá la salida de la información procesada por el dispositivo antes de ser enviada a la base de datos mediante el sistema de control de ingreso y salida del personal docente de la Escuela de Ingeniería de Sistemas de la PUCESA.

Características del Usuario

El uso de dispositivos de huella digital constituye una herramienta de apoyo al personal encargado del control de asistencia y puntualidad de los Docentes de la Escuela de Ingeniería de Sistemas de la PUCESA. Es por esta razón que los equipos son prácticos y de fácil registro ya que no toma más de un segundo en realizar el marcaje de entrada y salida del docente.

Por la explicación antes dada de los dispositivos de huella digital, es únicamente necesario tener un tipo de usuario el mismo que será el docente: Usuario.

El **Usuario,** en este caso serán todos los docentes quienes estarán sujetos únicamente a interactuar con en el dispositivo en lo que será el registro por primera vez de la huella digital y el marcaje de las horas de entrada y salida de sus horas de clases.

Restricciones

Para el correcto funcionamiento del los dispositivos de huella digital Kbio se requiere del sistema SIP y el acceso a la base de datos.

Una vez ingresada la huella digital se podrá realizar la extracción de datos correctamente con el sistema SIP, cabe recalcar que el sistema controlara huellas duplicadas para mantener integridad de información.

Suposiciones y Dependencias

Para el funcionamiento de los dispositivos de huella digital KBio serán necesarias las conexiones de los equipos con el sistema SIP.

3.1.3 Requisitos Específicos

Dentro de este segmento se analiza la usabilidad que los dispositivos de huella digital prestan a los usuarios. Entendiéndose por usabilidad a la manera de registrar y marcar la huella de los docentes en los equipos KBio con la facilidad que permite la realización de estas tareas y de manera ágil y sencilla.

Requisitos de Interfaz Externo

El docente que registre su huella será un usuario poco familiarizado con el dispositivo ya que en la actualidad se hablado mucho de este tipo de registro pero hay pocas empresas que lo están implementando.

Por otro lado las ventanas de mantenimiento y de procesos se encuentran estandarizadas en el sistema SIP.

Requisitos Funcionales

Para el correcto funcionamiento del registro e identificación de las huellas digitales será importante realizar el ingreso de la información de acuerdo a un orden lógico, similar al proceso de cedulación que no deberá repetirse el numero de identificación para dos docentes, con esto se garantiza que el procesamiento y salida de la información sea coherente. El sistema SIP proveerá los controles necesarios para evitar un incorrecto ingreso de la huella. Es importante un adecuado ingreso de las huellas, especialmente para evitar duplicados de las mismas, cuyos datos son necesarios para guardar la consistencia de información.

3.2 ANÁLISIS DE DISPOSITIVOS

3.2.1 Dispositivos

Las computadoras electrónicas modernas son una herramienta esencial en muchas áreas: industria, gobierno, ciencia, educación. En realidad en casi todos los campos de nuestras vidas.

El papel que juegan los dispositivos periféricos de la computadora es esencial; sin tales dispositivos ésta no sería totalmente útil. A través de los dispositivos periféricos podemos introducir a la computadora datos que nos sea útiles para la resolución de algún problema y por consiguiente obtener el resultado de dichas operaciones, es decir; poder comunicarnos con la computadora.

La computadora necesita de entradas para poder generar salidas y éstas se dan a través de dos tipos de dispositivos periféricos existentes:

- Dispositivos periféricos de entrada
- Dispositivos periféricos de salida.

3.2.2 Dispositivos de Entrada

Son aquellos que sirven para introducir datos a la computadora para su proceso. Los datos se leen de los dispositivos de entrada y se almacenan en la memoria central o interna. Estos convierten la información en señales eléctricas que se almacenan en la memoria central.

Los dispositivos de entrada típicos son los teclados, lápices ópticos, palancas de mando (joystick), CD-ROM, discos compactos (CD), etc. Hoy en día es muy frecuente que el usuario utilice un dispositivo de entrada llamado ratón que mueve un puntero electrónico sobre una pantalla que facilita la interacción usuario-máquina.

3.2.2.1 Tipos de Dispositivos de Entrada

Mouse o Ratón

La función principal del ratón es transmitir los movimientos de nuestra mano sobre una superficie plana hacia el ordenador. Allí, el software denominado driver se encarga realmente de transformarlo a un movimiento del puntero por la pantalla dependiendo de varios parámetros.

En el momento de activar el ratón, se asocia su posición con la del cursor en la pantalla. Si desplazamos sobre una superficie el ratón, el cursor seguirá dichos movimientos. Es casi imprescindible en aplicaciones dirigidas por menús o entornos gráficos, como por ejemplo Windows, ya que con un pulsador adicional en cualquier instante se pueden obtener en programa las coordenadas (x, y) donde se encuentra el cursor en la pantalla, seleccionando de esta forma una de las opciones de un menú.

Figura 14. Mouse o Ratón

Teclado

Es el dispositivo más común de entrada de datos. Se lo utiliza para introducir comandos, textos y números. Estrictamente hablando, es un dispositivo de entrada y de salida, ya que los LEDs también pueden ser controlados por la máquina.

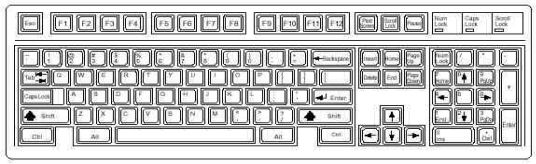


Figura 15. Teclado

Scanner

Ateniéndonos a los criterios de la Real Academia de la Lengua, famosa por la genial introducción del término cederrón para denominar al CD-ROM, probablemente nada; para el resto de comunes mortales, digamos que es la palabra que se utiliza en informática para designar a un aparato digitalizador de imagen.

Por digitalizar se entiende la operación de transformar algo analógico (algo físico, real, de precisión infinita) en algo digital (un conjunto finito y de precisión determinada de unidades lógicas denominadas bits). En fin, que dejándonos de tanto formalismo sintáctico, en el caso que nos ocupa se trata de coger una imagen (fotografía, dibujo o texto) y convertirla a un formato que podamos almacenar y modificar con el ordenador. Realmente un escáner no es ni más ni menos que los ojos del ordenador.

Figura 16. Scanner

Webcam

Una cámara web en la simple definición, es una cámara que esta simplemente conectada a la red o INTERNET. Como te puede imaginar tomando esta definición, las cámaras Web pueden tomar diferentes formas y usos.

En la Webcam radica un concepto sencillo; tenga en funcionamiento continuo una cámara de video, obtenga un programa para captar una imagen en un archivo cada determinado segundo o minuto, y cargue el archivo de la imagen en un servidor Web para desplegarla en una página Web.

Figura 17. Webcam

Joystick

Palanca que se mueve apoyada en una base. Se trata, como el ratón, de un manejador de cursor. Consta de una palanca con una rótula en un extremo, que permite efectuar rotaciones según dos ejes perpendiculares. La orientación de la palanca es detectada por dos medidores angulares perpendiculares, siendo enviada esta información al ordenador. Un programa adecuado convertirá los ángulos de orientación de la palanca en desplazamiento del cursor sobre la misma.

Figura 18. Joystick

Monito o Pantalla

Es el dispositivo en el que se muestran las imágenes generadas por el adaptador de vídeo del ordenador o computadora. El término monitor se refiere normalmente a la pantalla de vídeo y su carcasa. El monitor se conecta al adaptador de vídeo mediante un cable. Evidentemente, es la pantalla en la que se ve la información suministrada por el ordenador. En el caso más habitual se trata de un aparato basado en un tubo de rayos catódicos (CRT) como el de los televisores, mientras que en los portátiles es una pantalla plana de cristal líquido (LCD).

Figura 19. Monitor o Pantalla

3.2.3 Análisis de Dispositivos de Huella Digital Kbio-Offline

El KBio-Offline está concebido como un terminal de control de accesos y/o presencia con sensor biométrico la versión de conectividad es TCP/IP mediante la

inclusión del módulo conversor eCov-100, o simplemente de RS232 en ausencia del conversor.

Los terminales Offline están pensados para realizar identificaciones biométricas sin necesidad de conexión a un Host. A partir de tal identificación, se pueden desarrollar funcionalidades de control de accesos (activación de relé para la apertura de puerta), o bien de control de presencia (el sensor FIM01 dispone de reloj en tiempo real y de la posibilidad de gestionar marcajes, incluyendo el código de incidencia).

La identificación por defecto es 1: N, de forma que la huella escaneada se compara frente a todas las almacenadas en la base de datos del FIM01. Este proceso, por tanto, puede ser más lento a medida que aumenta el número de usuarios enrolados (más de 100).

El terminal KBio-Offline versión TCP, consta de los siguientes componentes:

- Sensor biométrico Nitgen FIM01-HV (en versiones para 1000 y 4000 usuarios)
- Tarjeta de control KBio-TCP. Contiene:
- Zócalo de conexión para Conversor eCov 100.
- Un relé.
- Interfase de usuario: zumbador, conexión a carátula, conexión a barrera óptica.
- Interfase de usuario: carátula que contiene tres LEDs y tres teclas.
- Detector de dedo (barrera óptica)
- Conversor TCP, eCov 100 (opcional).

- Lector de proximidad Kimaldi RD125K (opcional).

3.2.4 Ubicación de dispositivos KBIO.

Los dispositivos de huella digital KBio están distribuidos en el primer piso y en el piso de laboratorios de la PUCESA los cuales están conectados en red.

Figura 20. KBio en el Primer Piso

2.3.5 Implementación de los Dispositivos

Para la implementación del los dispositivos de huella digital Kbio es necesario una conexión a red y al sistema SIP para la comunicación y envió de información de los equipos al sistema.

CAPITULO IV

VALIDACIÓN Y VERIFICACIÓN DE RESULTADOS

4.1 OFICIOS DE VALIDACIÓN

4.2 VERIFICACION DE HIPOTESIS

Para la verificación de hipótesis se utilizó, el modus Ponendo Ponens de la lógica proposicional que dice: “Dada una proposición condicional y la afirmación del antecedente, puede concluirse la afirmación del consecuente”.

$$\begin{array}{l} P \rightarrow Q \\ P \\ \hline Q \end{array}$$

La hipótesis planteada en este proyecto es: “Con la implementación de dispositivos de huella digital, los estudiantes aprovecharan al máximo sus horas de enseñanza y adquirirán mejores conocimientos y al mismo tiempo se incrementará el índice de puntualidad”, por lo tanto se obtiene lo siguiente:

P: Con la implementación de dispositivos de huella digital (Premisa verdadera)
Q: Los estudiantes aprovecharan al máximo sus horas de enseñanza y adquirirán mejores conocimientos y al mismo tiempo se incrementará el índice de puntualidad.
Entonces:

(P) Con la implementación de dispositivos de huella digital $\longrightarrow$ **(Q)** Los estudiantes aprovecharan al máximo sus horas de enseñanza y adquirirán mejores conocimientos y al mismo tiempo se incrementará el índice de puntualidad.

(P) Con la implementación de dispositivos de huella digital

(Q) Los estudiantes aprovecharan al máximo sus horas de enseñanza y adquirirán mejores conocimientos y al mismo tiempo se incrementará el índice de puntualidad.

Con lo que mediante la utilización de este teorema la Hipótesis queda demostrada.

4.3 CONCLUSIONES

- Con la investigación realizada con anterioridad se determino que no existe un control adecuado del ingreso de los Profesores a sus horas de clases, ya que se utilizan controles manuales y no sistematizados.

- La precisión de la información dependerá de la inmediata recopilación de datos que se obtendrán de los equipos KBio, mediante la que se obtendrá informes en tiempo real.

- El registro de la huella es fácil y sencillo ya que no toma mas de tres segundos en realizarla, además es beneficioso porque nadie podrá duplicar o alterar el registro ya que los dispositivos cuentan con una base de datos interna la cual no permite el acceso en forma remota y podrá ser modificada únicamente con el programa SIP (Sistema de Ingreso de Personal).

- Los equipos KBio permite la identificación biométrica por huella dactilar además su funcionamiento es a tiempo real. Tiene la capacidad de almacenar hasta 4,000 huellas y 8192 marcajes.

- Simplemente con poner el dedo sobre el lector el usuario es identificado, si se trata de un usuario registrado, se produce el registro de la huella.

4.4 RECOMENDACIONES

- Mantener los equipos Kbio siempre en funcionamiento para la utilización de estos con el fin de no perder los registros en ningún momento y mantener siempre la información actualizada.

- Tomar muy en cuenta las direcciones IP de los KBios con el fin de conocer bien la ubicación de los mismos y mejorar la ejecución de reportes y obtención de los datos de los equipos.

- Completar la información de los Profesores con el ingreso de su huella personal con el fin de que los registros sean positivos y de manera efectiva.

- Mantener la integridad y cuidados de los equipos ya que estos son muy susceptibles a equipos magnéticos y a la humedad.

BIBLIOGRAFÍA

LIBROS:

- Comer E. Douglas, “Redes Globales de Información con Internet y TCP/IP”, Prentice-Hall, 1996

- Juan A. Sigüenza y Merino Tapiador Mateos, “Tecnologías Biométricas Aplicadas a la Seguridad”, Ra-ma, 2006

- José Viñals, “Huellas Dactilares”, Montesinos, 2004

- José Luís Rameral y Josep Balcells, “Autómatas Programables”, Marcombo

Internet:

- www.kimaldi.com Kimaldi

- http://fredimerino.8k.com/Tcpip.htm Protocolos TCP/IP

- http://usuarios.iponet.es/jsl/index.html Autómatas Programables

- http://es.wikipedia.org/wiki/Huella_digital Huella Digital

GLOSARIO DE TÉRMINOS

Actuadotes.- Son dispositivos capaces de generar una fuerza a partir de líquidos, de energía eléctrica y gaseosa. El actuador recibe la orden de un regulador o controlador y da una salida necesaria para activar a un elemento final de control como lo son las válvulas.

Bifurcaciones.- Es la división en ramales de las líneas que compone una huella.

Biometría.- La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como lo es la huella digital

DLL.- (Dynamic Linking Library - Librerías de Enlace Dinámico). DLL es la implementación de Microsoft del concepto de librerías compartidas en sistemas Windows. Generalmente estas bibliotecas llevan la extensión ".dll" o ".ocx" (para aquellas que contienen controles ActiveX), o ".drv" (controladores de sistema).

DPI.- Puntos por pulgada (ppp) del inglés dots per inch (DPI) es una unidad de medida para resoluciones de impresión, concretamente, el número de puntos individuales de tinta que una impresora o toner puede producir en un espacio lineal de una pulgada.

FIM01.- Es un módulo de reconocimiento de huella autónomo compuesto por un sensor óptico y una placa de procesado. Mediante la incorporación de una CPU de gran velocidad y un algoritmo de reconocimiento de huella optimizado, el FIM01 ofrece una alta capacidad de reconocimiento y una gran velocidad para operaciones de identificación 1:N, y para la carga y descarga de datos, proporcionando las condiciones óptimas para su aplicación en sistemas de control de acceso.

IP (Internet Protocol).- Protocolo de internet. Es la parte del protocolo TCP/IP encargada del direccionamiento (identificación del origen y destino).

KBIOMAXctl.- Es la librería que se utiliza para la programación de los equipos Kbio.

Minucias.- Detalle o rasgo irrelevante.

Minutae.- Es el conjunto de líneas que componen una huella digital.

OCX.- También conocido como ActiveX, es una tecnología de Microsoft que se utiliza en la programación del software, que se utiliza para la reutilización de código.

SDK.- (Software Development Kit - Kit de desarrollo de software). Un SDK es un conjunto de herramientas y programas de desarrollo que permite al programador crear aplicaciones para un determinado paquete de software, estructura de software,

plataforma de hardware, sistema de computadora, consulta de videojuego, sistema operativo o similar.

SIP.- Sistema de Ingreso de Personal

TCP/IP (Transmission Control Protocol / Internet Protocol).- Conjunto básico de protocolos de comunicación de redes, popularizado por internet, que permite la transmisión de información en redes de computadoras.

Template.- Es el registro de la huella digital en el equipo.