UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de un sistema de control de acceso de personal utilizando lectores biométricos de huella digital y de tarjeta inteligente para ser implementado en un edificio de oficinas.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO ELÉCTRICO – ELECTRÓNICO

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

LÓPEZ RODRÍGUEZ LUIS MANUEL

MOSCARDO RÍOS ARMANDO

DIRECTOR DE TESIS: M.I. JUAN MANUEL GÓMEZ GONZÁLEZ

2008

Jurado asignado:

Presidente	Ing. Juan José Carreón Granados
Vocal	M.I. Juan Manuel Gómez González
Secretario	M.I. Antonio Salvá Calleja
1er. Suplente	M.I. Ricardo Garibay Jiménez
2do. Suplente	M.I. Norma Elva Chávez Rodríguez

Sitio donde se desarrolló el tema:

Facultad de Ingeniería

Director de tesis:

Ing. Juan Manuel Gómez González

AGRADECIMIENTOS

A mis padres, ***Julia Rodríguez*** *y* ***Manuel López****, que sin escatimar esfuerzo alguno me han proporcionado sus enseñanzas, amor, cariño, confianza, apoyo, impulso, desvelos y sacrificios que iniciaron desde mis primeros días en mi vida, y ahora que empieza una nueva etapa tambien muy importante; con la idealización de nuevas metas y horizontes que conquistar espero contar con todo su apoyo y cariño.*

A mi hermano, ***Julio****, por compartir sus voces de aliento, desafíos, entusiasmo, cariño, solidaridad y compañía.*

A mis familiares, abuelo y abuela , tíos y tías por los buenos consejos y regaños que bien han valido la pena.

A la ***Facultad de Ingeniería*** *de la* ***Universidad Nacional Autónoma de México*** *por brindarme todas esas oportunidades de crecimiento, no solo profesional sino integral como ser humano.*

Al Ingeniero ***Juan Manuel Gómez González****, no solo por todo el tiempo y dedicación que me brindo para llevar por buen camino este trabajo, sino por su amistad sincera.*

A mis sinodales ***M. I. Antonio Salva Calleja****,* ***M.I Norma Elva Chávez , M. I. Ricardo Garibay Jiménez y al Ing. Juan J. Carreón****, por su colaboración.*

A mis amigos ***José Luis, Edgar, Edgar Castro, Eduardo, Francisco, Javier, Alberto, Armando, Iván, Josué, Omar, Sergio, Pablo, Alejandro, Juan Carlos, Karina, Fátima, Lulu, Janet****, a mis primos* ***Nadia, Luis Enrique, Ricardo, Wendy, Alfredo, Ivett , Francisco*** *pero en especial a mis grandes amigas* ***Ana, Diana y Verónica*** *por ocupar un lugar especial por las vivencias y gratos momentos que siempre llevaré en mi mente y corazón.*

Finalmente, a todos los que contribuyeron directa o indirectamente con su apoyo en este trabajo.

Luis Manuel López Rodríguez

A mis padres, ***Jaime Armando Moscardo Manríquez*** *y* ***Luz del Carmen Ríos Olvera****, que siempre me han mostrado su gran amor, reflejándose en el respeto, confianza y apoyo que me han brindado a lo largo de toda mi vida, desde mi infancia hasta el día de hoy; esperando con completa seguridad que su amor incondicional me seguirá por el resto de mis días en esta tierra.*
Gracias por su consuelo y apoyo cuando fracaso o me deprimo y; muchas gracias más por compartir y alegrarse conmigo en mis logros y éxitos, como lo es la culminación de mis estudios y mi formación como profesionista.

A mis hermanas, ***Miriam del Carmen*** *y* ***Jessica Teresa*** *por ser vivos ejemplos de amor, honestidad y responsabilidad. Gracias por exhortarme a seguir siempre adelante hasta llegar a la meta.*

A mi amigo ***Enrique Nieto Ledesma*** *y su familia por su amistad y por el amor que han manifestado a mi persona y a mi familia. Gracias por estar siempre ahí en los momentos importantes.*

A la ***Universidad Nacional Autónoma de México*** *y a todas sus instituciones y organismos, principalmente a la* ***Facultad de Ingeniería,*** *por ofrecer todo un conjunto completo de oportunidades y opciones que permitieron mi crecimiento y mi formación integral, no sólo como profesionista, sino como ser humano.*

Al ***M.I. Juan Manuel Gómez González****, por el esfuerzo y tiempo invertido para dirigir nuestra tesis, compartiendo su experiencia y consejos para culminar con éxito este trabajo.*

A mis sinodales ***M. I. Antonio Salva Calleja****,* ***M.I Norma Elva Chávez , M. I. Ricardo Garibay Jiménez y al Ing. Juan J. Carreón****, por su tiempo y participación para evaluar este trabajo.*

A todos mis maestros por sus enseñanzas en las asignaturas que cursé. Gracias por ser profesionistas bien preparados en la docencia y por el interés mostrado en la formación académica de sus alumnos.

A todos mis compañeros de escuela y amigos que compartieron conmigo momentos y vivencias increíbles que marcaron mi vida, y que ahora están grabados en mi corazón.

A ***Luis****, por su amistad y por ser el mejor compañero que pude tener para elaborar este trabajo. Gracias por los regaños y llamadas de atención.*
¡Lo logramos!

Armando Moscardo Ríos

ÍNDICE

CAPÍTULO 4

Introducción

El desarrollo de Sistemas de Control de Acceso, hace indispensable utilizar tecnologías que proporcionen una mayor confiabilidad, y sin duda que permitan unirse entre ellas para tener un mayor nivel de seguridad respecto a las tecnologías ya existentes, ejemplo de estas son las tecnologías de código de barras y banda magnéticas, que hoy en día han sido reducidas a herramientas para el registro y salida de productos en cualquier tienda de autoservicios, esto debido a que como sistemas de control tienen un nivel bajo que no le permiten la manipulación de los datos o registrar eventos ocurridos en una determinada situación.

Con la entrada del siglo XXI, las empresas se enfrentan un constante cambio, que hace a la tecnología una herramienta para facilitar las actividades cotidianas que ayuda a crear más bienes y servicios, mejorar la calidad de atención al cliente y reducir gastos, en un esfuerzo para seguir siendo competitivas. Además, están descubriendo que las áreas de seguridad han cambiado en los ultimas tres décadas y que no solo es clave en el control de personas, sino también que si son utilizadas correctamente, puede ser una ventaja competitiva para obtener un mayor eficiencia en el manejo de sus recursos.

Durante los últimos años el desarrollo de las tecnologías biométricas y de tarjetas inteligente que han sido un apoyo a las nuevas tecnologías de control de acceso. Todos estos servicios facilitan que las empresas construyan nuevas aplicaciones para sus sistemas de control de acceso dando una amplia gama de aplicaciones que anteriormente no se tenía acceso para sus clientes o para los usuarios del sistema internos y externos. Conforme las empresas empezaron a conocer los beneficios de consolidar sus sistemas de control de acceso en una variedad de servicios múltiples, la migración a estas arquitecturas no se hizo esperar.

La empresa a la cual realizamos la implementación de sistema de control de acceso (omitiremos el nombre de la empresa por razones de información confidencial) no es ajena a estos cambios en tecnologías de control de personal, ya que debido a la importancia que tiene para ella, por la venta de sistema de

seguridad, requiere de una permanente interacción con los sistemas de seguridad y la facilidad de mostrar sus productos con sus probables clientes mostrando las ventajas que conlleva tener instalado un sistema de seguridad.

Esta empresa tiene como objetivos principales el incrementar los niveles de seguridad dentro de sus oficinas y proporcionar más seguridad a las áreas más desprotegida, creando mecanismos que garanticen esta seguridad mediante el apoyo de su división DSCA (División de Sistemas de Control de Acceso) de como punto de partida par después hacer la implementación dentro de todas sus áreas de trabajo.

Y en conjunto tiene una fuerte influencia en temas que proveen una integración de productos y servicios para la solución de la administración electrónica de la seguridad. Mas específicamente cuando se habla de seguridad de personal, visitantes, contratistas y por supuesto de los bienes e información confidencial. Esta es una de las razones por la que la organización, la automatización y el control completo de los accesos han llegado a ser esenciales. Con sus soluciones de control de acceso pueden determinar automáticamente quien puede entrar, ir a donde, cuando y bajo que condiciones con lo que se tiene un amplio control de los recursos con lo que cuenta una empresa.

La administración responsable de la seguridad permite que reduzcas al mínimo el riesgo implicado en el acceso no autorizado al edificio (o parte de el) por lo que las situaciones de inseguridad y de robos substanciales no deben ocurrir: Con el Control de acceso se tiene una ayuda inestimable para una administración eficiente en las crisis de desalojo del edificio en el caso de un siniestro de fuego o de cualquier otra emergencia, incluyendo el cumplir estándares de certificación internacionales de seguridad.

DSCA es Líder en soluciones tecnológicas, control de de acceso y seguridad en la administración de nominas y procesos administrativos brindado la confianza de confidencialidad y llevando el trabajo a un nivel profesional.

Su misión es el de unificar todos los requerimientos que cuenta una empresa en el manejo de sus accesos y de su personal alrededor de un único concepto, la identificación personal por medio de una tarjeta o biometría. Promueve el desarrollo tecnológico y apoyar los programas de modernización administrativa.

CAPITULO 1

SISTEMA DE CONTROL DE ACCESO

1.1.- Definición de un sistema de control de acceso.

En este trabajo tiene como uno de sus objetivos hacer un estudio de los sistemas de control de acceso, para después utilizar los resultados obtenidos para tener las herramientas necesarias y diseñar un sistema completo capaz de ofrecer soluciones, prácticas y confiables que satisfagan las necesidades y problemas de control y seguridad que tiene una compañía que cuenta con un edificio de oficinas en la Ciudad de México.

Por esta razón, a lo largo de este trabajo se mencionará en diversas ocasiones el término "Sistema de control de acceso de personal" o simplemente "Sistema de control de acceso". Definiremos entonces, para los propósitos de este trabajo, a un sistema de control de acceso como: *"Un sistema electrónico autónomo que tiene la facultad de permitir o impedir el acceso de una o más personas a una área física designada, tomando en cuenta una base de datos y condiciones establecidas, llevando un registro electrónico de cada incidente ocurrido"*.

En términos generales la base de datos está compuesto por:

a) Números de identificación personal (ID´s)
b) Grupos de accesos
c) Horarios

De esta manera definiremos también a un usuario del sistema como: *"Una persona que cuenta con un número de identificación personal válido para el sistema"*

El número de identificación personal para cada usuario es único, el grupo de accesos identifica las áreas autorizadas en las que puede ingresar un usuario y el horario hace referencia al intervalo de tiempo en el cual un usuario puede ingresar a un área que pertenezca a su grupo de accesos.

Otros datos como el nombre completo de cada usuario, el puesto que desempeña en la empresa, o su edad, son meramente informativos y no tienen relación con los requisitos o condiciones que se deben cumplir para conceder o no el acceso a un área determinada.

Las condiciones más comunes en un sistema de control de acceso típico, así como una descripción general del proceso que realiza el sistema con los datos y las condiciones establecidas para conceder o negar el acceso se pueden observar en el diagrama de flujo de la figura 1.1.

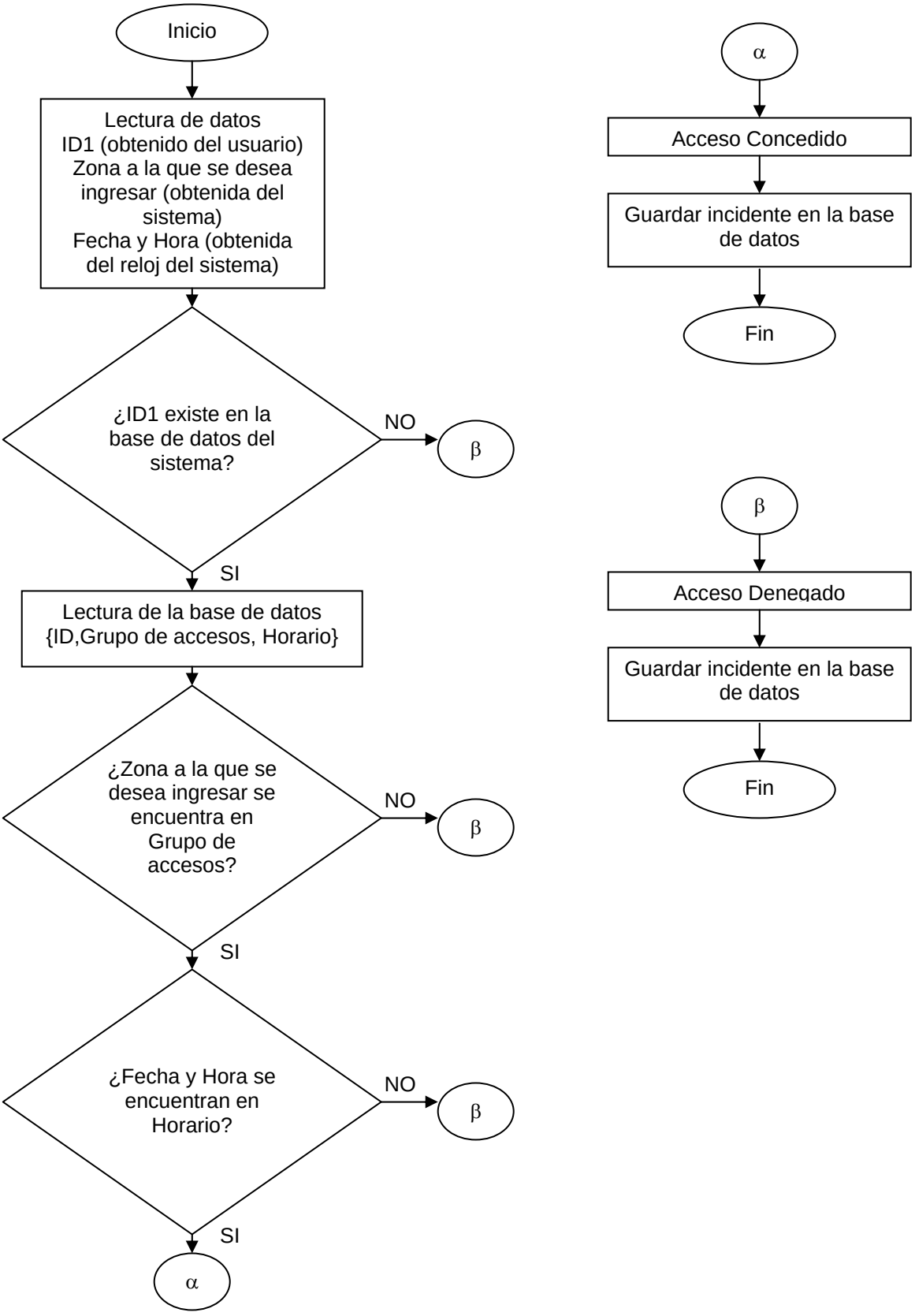


Figura 1.1.- Diagrama de Flujo del proceso de un sistema de control de acceso típico para conceder o negar un acceso

En la figura 1.1 se observa como el sistema necesita de tres datos para empezar su proceso, un número que designamos como ID1 ingresado al sistema por el usuario, una Zona que es un identificador del área en donde se esta solicitando un acceso; este identificador lo conoce el sistema y está asociado al campo de Grupo de accesos de la base de datos, el cual puede contener a su vez uno o más identificadores de Zona. Por último el sistema también lee la fecha y la hora en que se ha hecho la solicitud de acceso; este dato lo obtiene de un reloj interno con el que cuenta el sistema.

Algo más que podemos resaltar de esta figura, es el hecho de que no importando si se concede o no el acceso, se guarda el registro del incidente ocurrido en la base de datos, lo que permite conocer porque el sistema negó o concedió un acceso, logrando con esto tener un control de los usuarios que ingresaron a un área determinada y de los posibles intentos de violación a áreas no autorizadas en horarios no autorizados realizados por usuarios del sistema.

En un Sistema de Control de Acceso, todos los componentes del sistema están conectados entre sí, y se centraliza todo el manejo y supervisión del sistema en una computadora, que tendrá instalado un Software de Gestión, Administración, Control y Supervisión.

Independientemente del Sistema de Control de Acceso que se trate, para el caso de los sistemas completos, se agregan otros elementos adicionales. A continuación, iremos detallando cada uno de esos elementos, explicando las características de cada uno brevemente y finalizaremos sintetizando todo, en un gráfico que representa en forma sencilla, una instalación típica.

1.2.- Componentes de un sistema de control de acceso.

Un sistema de control de acceso físico básico está compuesto por:

- Lectores
- Tarjetas (o algún otro medio que contenga un ID o permita la obtención del mismo)
- Un panel de control
- Cerraduras
- Fuentes de alimentación
- Software de control, monitoreo y reporteo

En algunos casos se pueden agregar algunos elementos secundarios que no se relacionan directamente con los Sistemas de Control de Acceso, sino con los sistemas de detección de intrusos y de emergencia, pero que pueden ser un requerimiento para la persona que solicita el sistema de acceso. Estos elementos pueden ser: sensores (de puerta abierta, de vidrio roto, de humo, de movimiento, etc.) y bocinas o sirenas.

Un sistema puede tener tantos lectores y cerraduras que sean necesarias para una aplicación requerida, sin embargo, lectores y cerraduras se encuentran limitados por el panel de control de acceso. Afortunadamente también se puede tener más de un panel y comunicar cada panel entre sí para poder resolver este problema.

Un lector es un dispositivo electrónico que se encarga de ingresar y transmitir la información al sistema de control de acceso, mediante la lectura de un medio electrónico, biométrico o una combinación de los dos. Los lectores más comunes son los lectores de código de barras, de banda magnética, de proximidad, tarjeta inteligente y biométricos.

Un acceso que se desee controlar requiere forzosamente de un lector y de una cerradura, se puede agregar un lector más si se desea controlar la entrada y la salida a un acceso. En el caso de que se utilice un solo lector por acceso, es necesario contar con un dispositivo (que puede ser un botón o palanca de emergencia por ejemplo) para liberar la salida.

Al panel de control o unidad de control, entran y salen las distintas conexiones del sistema, como son los lectores y las cerraduras, y también los sensores y las bocinas, si se usa con señales de alarmas.

Tendremos también, todas las borneras para hacer las conexiones del/los lector/es, la cerradura o el elemento que se utilice y las entradas de sensores y salidas de alarmas (En el caso de abrepuertas muy elementales, no existen estas características).

En este dispositivo se encuentra el microprocesador que realiza el proceso al que se hace referencia en el diagrama de flujo de la figura 1.1 en el cual se lleva acabo la lógica de funcionamiento del sistema. Además, está compuesto por los dispositivos electrónicos necesarios para poder mandar señales eléctricas a los lectores, las cerraduras para que estas se abran o se cierren y para poder recibir señales provenientes de diferentes tipos de sensores (de puerta abierta, de vidrio roto, de humo, etc.) la memoria donde se guardan las tarjetas habilitadas, el reloj de tiempo real y la memoria para los eventos que se registran.

Todas las Unidades de Control necesitan recibir la energía de alimentación para su funcionamiento, es por ello que se vuelven importantes contar con las suficientes fuentes de alimentación. Seguramente, no todos los fabricantes de equipos, poseen el mismo criterio, así que es posible que nos encontremos con equipos que se alimentan directamente con la red de 110 VAC y otros que lo harán con 12 o 24 VDC.

También debemos contemplar, de la misma forma, las fuentes de alimentación para la cerradura o dispositivo y sirenas, si se utilizan.

En la figura 1.2 se observa el diagrama de un panel de control de acceso comercial mostrando algunos de sus componentes, y conectores más importantes; se puede ver en la parte inferior de la figura los conectores para los lectores, los relevadores de la parte derecha de la figura permiten la apertura o cierre de las cerraduras dependiendo del estado en el que se encuentren (normalmente cerrado o normalmente abierto) y por último en la parte izquierda se observan los conectores para los sensores de alarma que ya mencionamos. En los últimos capítulos de este trabajo que hacen referencia a la implementación del sistema de control de acceso, abordaremos más a fondo los componentes de un panel de control.

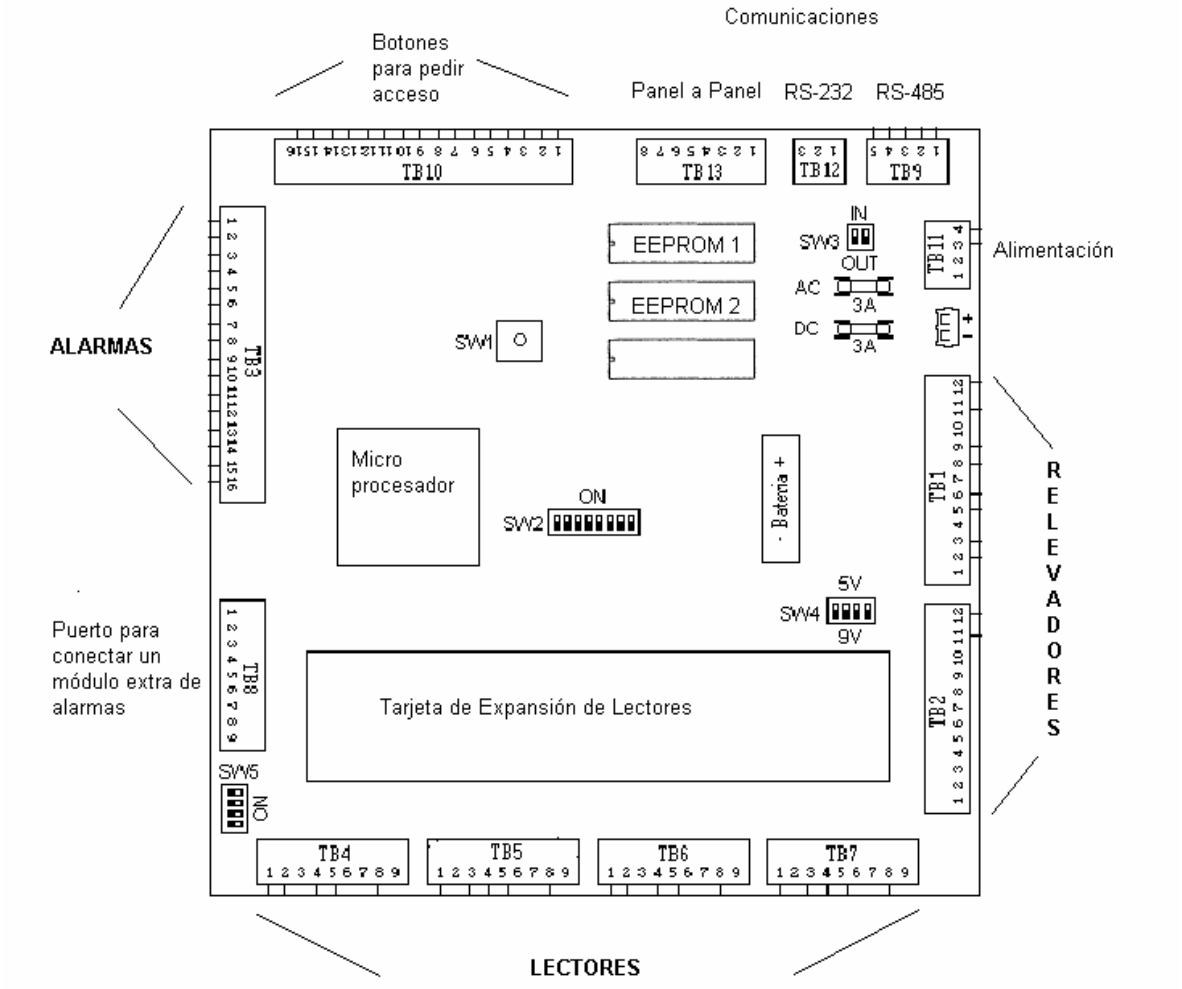


Figura 1.2- Diagrama de un panel de control comercial.

Por último una cerradura es un dispositivo electrónico que mantiene un acceso cerrado, hasta que recibe una señal del panel de control, momento en el cual la cerradura se libera permitiendo el acceso. Las cerraduras más comunes son las chapas eléctricas, los electroimanes y otras chapas electromagnéticas, las barreras vehiculares y los torniquetes de media altura o de altura completa.

1.3.- Funcionamiento de un sistema de control de acceso típico.

En el capítulo 1.1 “Definición de un sistema de control de acceso”, establecimos el proceso que realiza un sistema de control de acceso para conceder o denegar un acceso; en este capítulo ampliaremos un poco más la explicación de este proceso pero enfocado a los componentes de hardware que mencionamos en el capítulo anterior. Esto nos permitirá dar un panorama mucho más completo del funcionamiento de un sistema de control de acceso típico.

El proceso comienza con la llegada del usuario al acceso por el cual desea entrar o salir, el usuario presenta ante el lector el medio en el cual está almacenado su número de identificación personal (este medio puede ser una tarjeta, una característica biométrica o ambas, como mencionamos con anterioridad). El lector entonces envía una cadena de bits codificada con información del medio utilizado, en donde se encuentra el número de identificación ID1 del usuario, al panel de control; el microprocesador dentro del panel de control toma esta cadena de bits, la decodifica y realiza el proceso descrito en la figura 1.1 para conceder o negar el acceso. Una vez que el sistema decide conceder el acceso, el panel manda una señal para cambiar el estado de un relevador (asociado a ese acceso) al cual esta conectado una cerradura; de esta manera la cerradura se libera y el usuario puede pasar a través del acceso (Figura 1.3).

El sistema cuenta además con un software de configuración, monitoreo y reporteo (CMR) instalado en una computadora preferentemente dedicada; con este software se configuran los parámetros relacionados al sistema de control de acceso como son: Los usuarios, los lectores, los horarios, los grupos de accesos las asociaciones de los relevadores con los accesos a controlar. También mediante este software se monitorea en tiempo real cada una de las incidencias que ocurren en el sistema y que son almacenadas en la base de datos; por último con este software se pueden generar reportes filtrados por incidencias, por usuarios o por fechas.

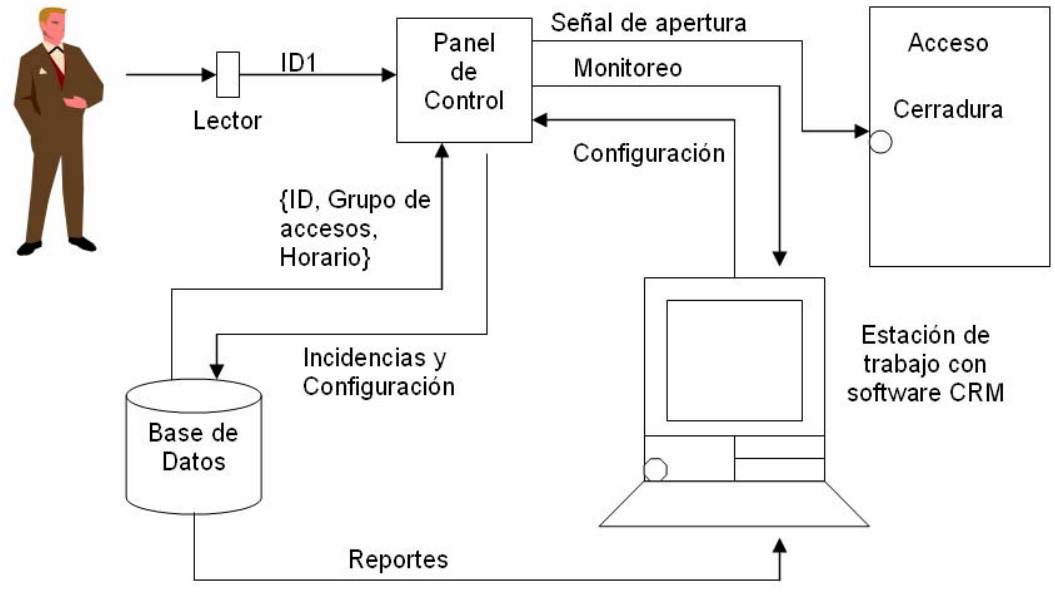


Figura 1.3.- Sistema de Control de Acceso Típico.

CAPÍTULO 2

MARCO TEÓRICO

2.- Marco teórico.

2.1.- Tecnologías aplicadas al control de acceso.

Un sistema de control de acceso puede estar integrado de tarjetas de identificación, lectoras, cerraduras automáticas y computadoras para procesar diversos reportes y su eficacia dependerá de las características técnicas de los equipos utilizados y del software. Un buen diseño del sistema de control de acceso es fundamental para determinar las jerarquías de acceso para empleados y visitantes y, en base a las necesidades del usuario, determinar el tipo de tarjetas de identificación (de banda magnética, de código de barras, de chip, con fotografía, etc.), el tipo de lectoras (de aproximación, de ranura, de lectura de huella digital, de iris, etc.) y el tipo de reportes de control que el usuario requerirá. Ya mencionamos que lo primero que debemos determinar es justamente qué tipo de tecnología vamos a instalar y para esto es necesario nombrar las tecnologías más comunes existentes en el mercado.

Banda Magnética: Es la tecnología más conocida y difundida. Su ventaja es su difusión, popularidad y el bajo costo, pero en sí es, de todos los medios de identificación, el más vulnerable de todos. Sólo se recomiendan en oficinas o establecimientos administrativos.

El lector en sí, es de los más económicos, pero posee un cabezal magnético, el cual sufre cierto desgaste cada vez que se pasan las tarjetas. El tiempo de duración, depende exclusivamente del ambiente, frecuencia de uso y el trato que se le dé al utilizarlos.

Código de Barras: La ventaja de esta tecnología, es que sus tarjetas al ser pasarlas por el lector, no existe rozamiento con un cabezal, con lo cual su vida útil es levemente mayor, pero si se raya el código impreso puede quedar ilegible, obligando al cambio de tarjeta. El costo de las tarjetas es similar a las magnéticas, y a pesar de que se las puede proteger contra fotocopias, son bastante vulnerables en lo que a seguridad se refiere.

Proximidad: Con este tipo de tecnología es imposible que pueda duplicarse una credencial o tarjeta. La tarjeta no tiene rozamiento de ningún tipo (se comunica con el equipo por radio frecuencia), por lo cual no se desgasta. Hoy en día es una de las tecnologías más moderna y efectiva, por su practicidad y bajo costo de mantenimiento. Son ideales en situaciones de máxima seguridad y alta tecnología. Es el sistema más ágil, porque no necesita que la tarjeta sea pasada en un sentido específico, lo que le da una mayor velocidad de lectura y poca resistencia al uso por parte de los usuarios, porque incluso puede ser leída la tarjeta dentro de una billetera, una cartera, etc.

El precio de esta tecnología se ha equiparado actualmente con los lectores comunes de código de barras. Logra sin dudas, la mejor relación precio/rendimiento.

Touch Memories: Es una pastilla electrónica, encapsulada en acero inoxidable de unos 16mm de diámetro, que se transportan con un soporte plástico tipo llavero. Brindan un muy alto nivel de seguridad, ya que son altamente resistentes al desgaste, siendo ideales para ambientes industriales, aunque no son recomendables para ambientes con alto grado de generación de corriente estática (P. Ej.: oficinas con mucha alfombra y ambientes muy secos). Su tecnología de avanzada evita la posibilidad de duplicarlas. Realmente muy confiables.

Biométricos: El funcionamiento de esta tecnología se basa en la lectura de alguna parte del cuerpo humano, eliminando por completo el uso de las tarjetas. Su principal ventaja radica en la seguridad, pero hasta el momento no son de uso masivo. Seguramente con el tiempo se irán superando algunas dificultades, entre ellas el costo, y en un futuro de mediano plazo, llegarán a ser un estándar más.

Con la identificación biométrica se puede tener un control realmente eficiente y preciso de los usuarios de un sistema de control de acceso, logrando saber con certeza, en base a uno o varios parámetros biométricos, que la persona que utilice esta forma de reconocimiento sea en verdad el usuario al que corresponda el mismo parámetro o parámetros biométricos. Esto no sucede con el, código de barras o la banda magnética. Solamente la identificación biométrica puede proveer un registro real de las actividades de las personas, eliminando la posibilidad de que estas accedan a lugares a los que no tienen autorización.

En este trabajo revisaremos los aspectos básicos de cada uno de los tipos de sistemas biométricos, dedicándole un mayor espacio a los sistemas y lectores de huella digital; pero antes es conveniente revisar algunos conceptos relacionados a la biometría.

2.2.- Biometría.

El término biometría se deriva de las palabras griegas “bio” (vida) y “metria” (medir) y hace referencia a la identificación o verificación de la identidad de forma automática de un individuo, empleando sus características biológicas, psicológicas y de conducta. La idea básica es que nuestros cuerpos, nuestros rasgos individuales y comportamiento contienen características únicas, que se pueden utilizar para distinguirnos de los demás.

La identificación de una persona por sus características biométricas ha sido utilizada prácticamente desde la aparición del hombre sobre el planeta. Uno de los más antiguos ejemplos para el reconocimiento de las personas es el rostro. Desde comienzos de la civilización los seres humanos han utilizados los rostros o las caras para reconocer e identificar individuos conocidos (familiares) y desconocidos. Esta simple tarea se volvió más desafiante a medida que la población fue creciendo y a la migración de individuos de otras comunidades. Este concepto de reconocimiento humano-humano es también visto en la identificación de un individuo por su voz. Las personas utilizan estas características para reconocer, de una manera inconsciente, familiares, amigos y conocidos.

A través de la historia, diversas civilizaciones han utilizado otras características biométricas como medios de identificación como las huellas dactilares de la mano.

En función de las características biométricas usadas para el reconocimiento, se puede establecer dos tipos de biometría:

- Biometría estática: abarca a aquellas características que se refieren a los aspectos físicos como el rostro, las huellas digitales y el iris.

- Biometría dinámica: abarca a aquellas características basadas en la conducta, tales como la voz y la firma caligráfica.

Con los sistemas biométricos se tiene la capacidad del reconocimiento de estos patrones para llevar a cabo las comparaciones de identidad y con ello la validez a las características del usuario con las características almacenadas de cada usuario.

A continuación revisaremos algunos conceptos básicos de la estructura común de la mayoría de los sistemas biométricos.

2.2.1.- Estructura de un sistema biométrico.

Un sistema biométrico típico consta de cinco componentes:

1.- Un sensor que obtiene la muestra biométrica del usuario y la convierte a un formato digital.

2.- Algoritmos de procesamientos de señales o imágenes, según sea el caso, que mejoran la calidad de la muestra eliminando el ruido y resaltando las características biométricas que pueden ser medidas, para formar la platilla biométrica (template).

3.- Una base de datos que contiene la información de las plantillas biométricas, con las cuales va a ser comparada la nueva plantilla biométrica generada por los algoritmos de procesamiento de señales.

4.- Un algoritmo de correspondencia que compara la nueva plantilla biométrica con una o con más plantillas guardadas en la base de datos.

5.- Un proceso de decisión (que puede ser automatizado o asistido) que en base a los resultados del algoritmo de correspondencia toma una decisión acerca de la acción a seguir si la identificación o verificación del usuario fue exitosa o no.

Con la identificación biométrica se puede tener un control realmente eficiente y preciso de los usuarios de un sistema de control de acceso, logrando saber con certeza, en base a uno o varios parámetros biométricos, que la persona que utilice esta forma de reconocimiento sea en verdad el usuario al que corresponda el mismo parámetro o parámetros biométricos. Esto no sucede con el, código de barras o la banda magnética. Solamente la identificación biométrica puede proveer un registro real de las actividades de las personas, eliminando la posibilidad de que estas accedan a lugares a los que no tienen autorización.

Los sistemas biométricos permiten establecer un alto nivel de confiabilidad para el reconocimiento de una persona, basándose en su criterio de identificación y verificación. A continuación presentamos los aspectos que tienen que ver con el reconocimiento, verificación e identificación.

2.2.2.- Reconocimiento, Identificación y Verificación.

Hasta ahora, hemos hecho uso indistinto de los términos reconocimiento, identificación y verificación cuando hablamos sobre sistemas biométricos y sobre la identidad de un usuario. Sin embargo, para futuros capítulos de este trabajo es necesario establecer la diferencia entre cada uno de estos términos.

Reconocimiento es un término general y no necesariamente implica identificación o verificación. Todos los sistemas biométricos realizan un “reconocimiento” para “volver a conocer” una persona que ha sido previamente enrolada.

Verificación es la tarea que realiza un sistema biométrico para confirmar la identidad reclamada por un individuo, comparando la muestra presentada con una o con más plantillas previamente enroladas. De esta manera el usuario se identifica mediante un método típicamente no biométrico, como un código (ID) o una tarjeta, y el sistema debe de comprobar (verificar) que la identidad proporcionada es correcta.

Por otro lado identificación es la tarea que realiza un sistema biométrico para establecer la identidad de un individuo. Para esto el sistema toma una muestra biométrica del individuo y la compara con todas las plantillas de la base de datos. En este caso la persona puede o no existir en la base de datos y el sistema debe de estar conciente de ello.

En otras palabras, la verificación se hace uno a uno y la identificación se hace uno a muchos (Figura 2.1). La verificación es usada en sistemas de control de acceso físico o lógico, donde se requiere autentificar o validar la identidad de una persona. Por el contrario la identificación es usada comúnmente por los servicios sociales y policíacos para establecer la identidad de una persona desconocida en base a sus características biométricas.

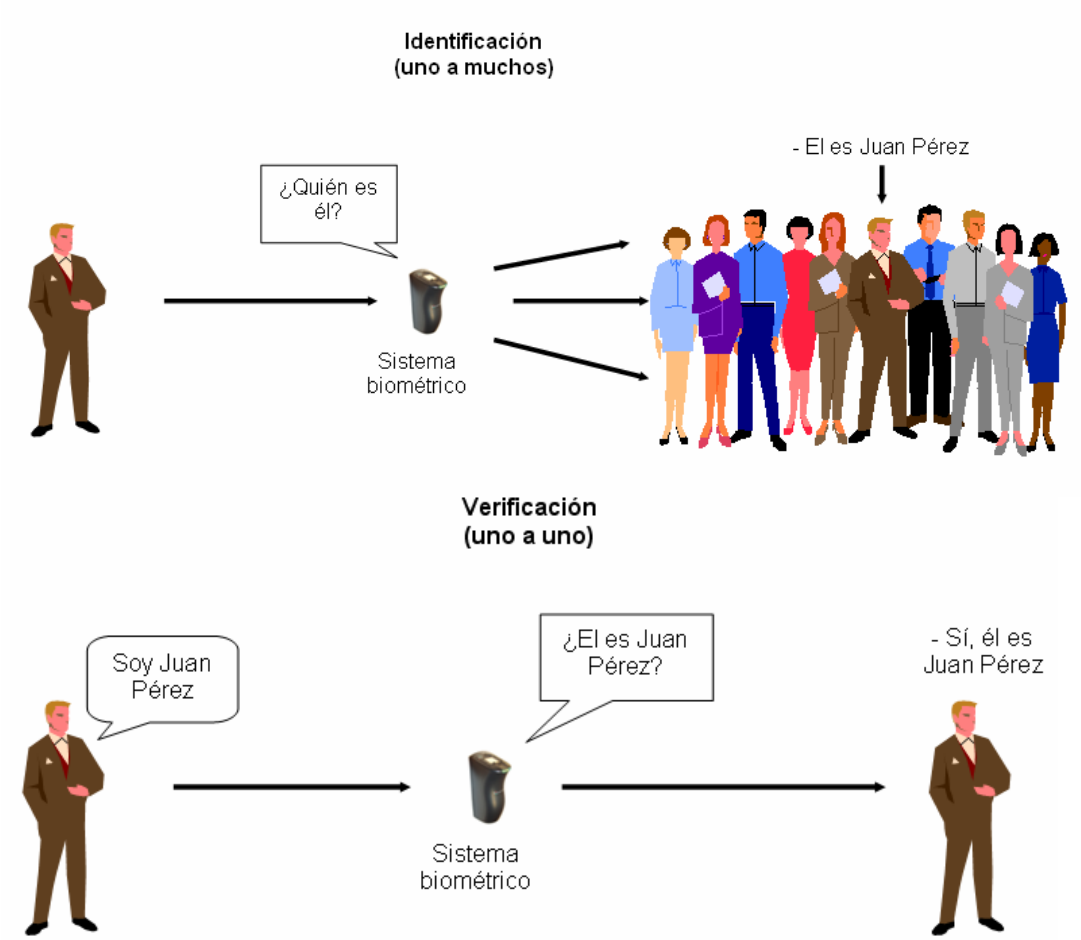


Figura 2.1.- Identificación vs. Verificación.

En los sistemas biométricos sólo se puede obtener la aceptación o el rechazo a un sistema, sin embargo se puede producir que el sistema acepté a un impostor o rechacé a un usuario estos dos casos pueden ocurrir debido a que al comparar al usuario con la muestra existente en el sistema este tiene dos posibles respuestas que son "semejante" o "no semejante", esto es siempre archivado con una asignación de un valor numérico, correspondiendo a las similitudes entre ellas y el valor numérico es comparado con un valor de umbral el cual es el encargado de decidir cual es "aceptado" y cual no lo es.

Las distribuciones de los valores similares de intentos genuinos y de los intentos fallidos no pueden ser separadas completamente por un valor de umbral. En cambio sus distribuciones coinciden en algunas partes y como resultado se obtiene una mayor seguridad y la probabilidad de cometer menos errores al dejar acceder a una persona ajena al sistema.

2.2.3.- Falsa aceptación

Falsa aceptación: Promedio de Aceptación Falso (FAR):La probabilidad que un sistema biométrico incorrectamente identifique a un individuo o falle en rechazar a un impostor. Consiste en aceptar a alguien que no pertenece a la base

de datos del sistema; por ejemplo, alguien podría clonar una credencial de identificación, o adueñarse de los números confidenciales de una persona para hacer una transacción en perjuicio de su legítimo dueño y hasta falsificar su firma. En la Figura 2.2 el comportamiento de la distribución y probabilidad que un sistema biométrico identifique y acepté a un usuario y que en realidad deberían ser rechazado.

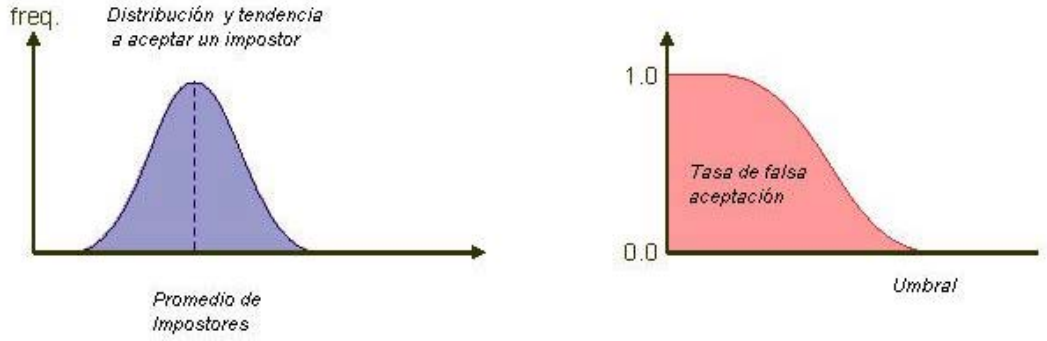


Figura 2.2.- Graficas de distribución de falsa aceptación.

2.2.4.- Falso rechazo

Falso rechazo: Promedio de Rechazos Falsos (FRR): La probabilidad de que un sistema biométrico falle en identificar o verificar la identidad de un usuario o una persona que si pertenezca a la base de datos del sistema.

En la Figura 2.3 se muestra la distribución y probabilidad de que el sistema biométrico no acepté a alguien que sí pertenece a la base de datos del sistema, pero su identificación no se pudo realizar por múltiples motivos, como puede ser: que la imagen de la huella esté muy dañada, o a que tenga deterioros en su superficie, o a que el lector no tenga la calidad suficiente para tomar correctamente la lectura.

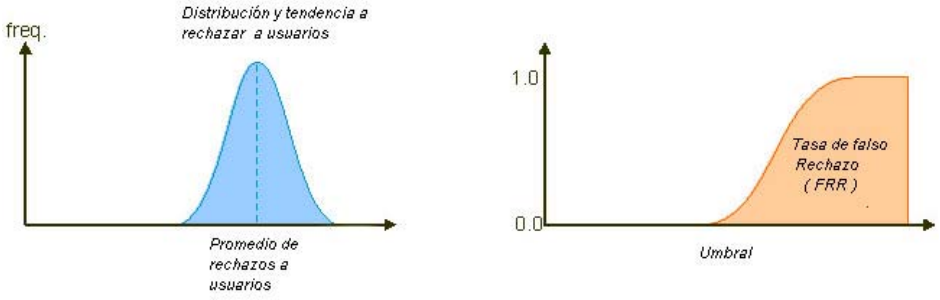


Figura 2.3.- Graficas de distribución de falso rechazo.

Por ejemplo podemos escoger un valor del umbral tan alto, que ninguna característica impostora exceda este límite. Como resultado, ninguno de los rasgos biométricos serán aceptados falsamente por el sistema. Por otro lado los rasgos biométricos de los usuarios del cliente con las marcaciones mas bajas que las marcaciones del impostor más altas se

rechazan falsamente. Contra esto, podemos escoger el valor del umbral tan bajo, que ningún rasgo biométrico del los usuarios del cliente se rechaza falsamente. Entonces, por otro lado, algunos rasgos biométricos del impostor se aceptan falsamente. Si escogemos el valor de umbral en alguna parte entre esos dos puntos, habrá falsos rechazos y las falsas aceptaciones ocurrirán.

Al escoger el valor del umbral se vuelve un problema si las distribuciones del cliente y el impostor marcan un traslape, como se muestra en la figura 2.4. Imagen de la izquierda. En la parte derecha, se despliegan la falsa aceptación y las proporciones de falso rechazo.

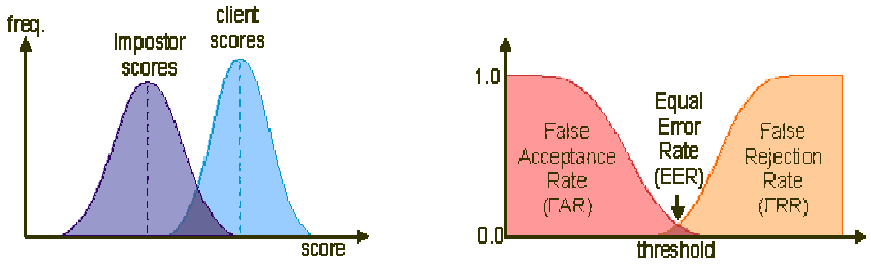


Figura 2.4.- Visualización de la unión de las dos distribuciones.

Si las distribuciones se traslapan, el FAR y FRR se intersecan en un cierto punto. El valor del FAR al de FRR es el mismo para los dos, se le conoce como Equal Error Rate (EER).

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

2.3.- Sistemas y tecnologías biométricas.

Actualmente, gracias a la evolución tecnológica contamos con sistemas y lectores biométricos para casi cualquier variable biométrica; sin embargo, algunos de estos sistemas se encuentran en fase de estudio y/o desarrollo. Entre los sistemas y lectores biométricos más utilizados y que se encuentran en el mercado, tenemos los siguientes:

- Geometría de la mano.
- Firma.
- Reconocimiento facial.
- Reconocimiento de voz.
- Iris.
- Huella digital.

De los anteriores sistemas, el sistema más seguro en la actualidad es el reconocimiento por iris, utilizado en aeropuertos, centrales nucleares y centros de gran seguridad. Las huellas dactilares han sido siempre relacionadas con temas policiales y actualmente se ha aceptado para el uso de credenciales, el reconocimiento facial permite la detección automática de personas incluso sin su conocimiento. De manera que cada tecnología biométrica es mayormente utilizada en alguna aplicación en especial.

En este trabajo revisaremos los aspectos básicos de cada uno de estos sistemas, dedicándole un mayor espacio a los sistemas y lectores de huella digital (porque actualmente es la tecnología biométrica más utilizada en diversas aplicaciones).

2.3.1.- Geometría de la mano.

El reconocimiento de la geometría de la mano es uno de los sistemas implementados más comunes, debutando en el mercado a finales de los ochentas y desde ese tiempo han sido aceptados por el público gracias a su facilidad de uso y a su capacidad de ser integrado sin dificultad a sistemas de control de asistencia y de control de acceso físico y lógico principalmente.

Uno de los mayores defectos que tienen estos sistemas de reconocimiento, es que las características físicas obtenidas de la geometría de la mano no son únicas para cada individuo, lo que limita las aplicaciones de los sistemas de reconocimiento de la geometría de la mano. Es por esta razón que esto sistemas se utilizan como sistemas de verificación únicamente.

Los dispositivos de reconocimiento de geometría de la mano se componen básicamente de una placa (donde se coloca la palma de la mano), de una cámara CCD (Charge-Coupled Device) o "*dispositivo de cargas* (eléctricas) *interconectadas o acopladas"*, de un espejo y de un microprocesador que se encarga de medir distancias y de almacenarlas en una memoria o base de datos.

La mano del usuario se coloca en la placa con la palma boca abajo, para que la posición de la palma sea correcta se utilizan cinco sensores que guían al usuario en la colocación de su mano.

La cámara CCD captura una imagen de la superficie de la parte superior de la mano y una imagen del perfil auxiliándose de un espejo colocado en un ángulo de 110° a 130° con respecto a la placa (Figura 2.5).

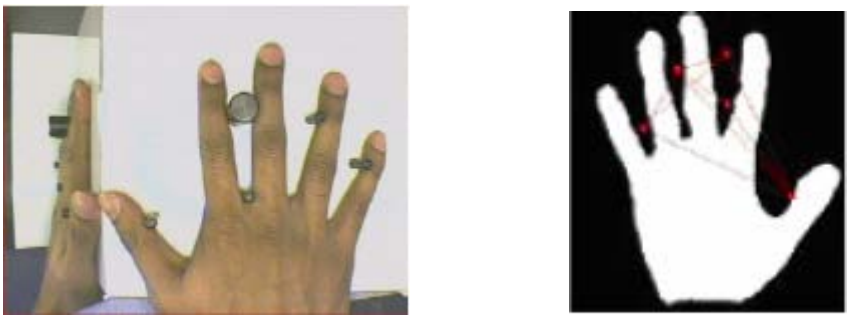


Figura 2.5.- (Izq.) Imagen de la superficie y perfil de la mano, vista por la cámara CCD. (Der.) Imagen de la silueta de la mano incluyendo ejemplos de medición de distancias.

De la imagen obtenida de la silueta de la mano, 31,000 puntos son analizados y 90 mediciones son realizadas por el microprocesador (Figura 2.6). Algunos ejemplos de estas medidas son:

- Las longitudes de cada dedo medidas desde el nudillo hasta la punta del dedo.
- El grosor de cada falange.
- El grosor de la mano, etc.

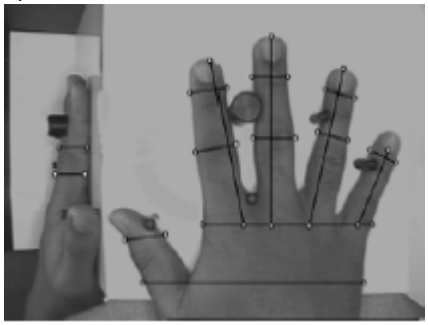


Figura 2.6.- Ejemplos de mediciones de distancias.

Toda la información y mediciones obtenidas son guardadas en un espacio aproximado de nueve bytes, un número muy pequeño en comparación a las necesidades de almacenamiento de otros dispositivos biométricos.

El proceso de enrolamiento de un sistema típico de reconocimiento de la geometría de la mano requiere la captura de tres imágenes secuenciales de la mano, las cuales son evaluadas y medidas para crear una plantilla de las características del usuario. Cuando en un proceso de verificación un usuario reclama su identidad mediante el ingreso de un número de identificación personal, el sistema manda llamar la plantilla almacenada que corresponde al número ingresado; el usuario coloca su mano en la placa y el sistema crea una plantilla de verificación y la compara con la plantilla creada en el proceso de enrolamiento. Una puntuación de similitud es generada y si la puntuación se encuentra dentro de un umbral establecido en el sistema, la reclamación de la identidad se acepta o se rechaza.

2.3.2.- Firma.

Los dispositivos reconocedores de la firma utilizan las características físicas y de comportamiento que un individuo exhibe cuando firma su nombre (o escribe cualquier otra palabra o frase). Estos dispositivos no deben de confundirse con los sistemas de captura de la firma, que son utilizados para capturar una imagen de la firma y son comunes en diversos comercios donde se capturan firmas para autorizar transacciones.

El reconocimiento dinámico de la firma utiliza múltiples características en el análisis de la caligrafía de un individuo. Estas características varían en uso y en importancia dependiendo del fabricante del sistema y son obtenidas utilizando tecnologías de sensibilidad de contacto como los que utilizan los PDAs o pizarrones digitales.

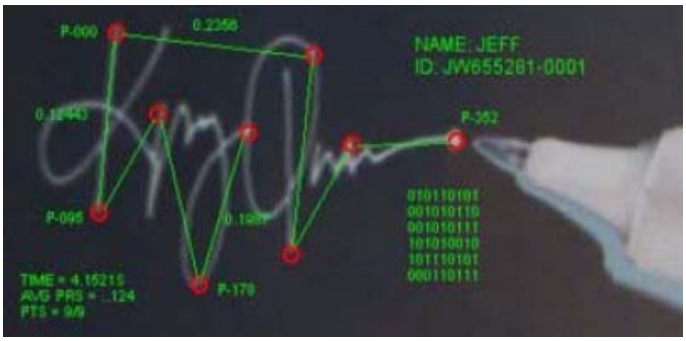


Figura 2.7.- Representación gráfica del reconocimiento dinámico de la firma: Cuando un individuo firma sobre el pizarrón digital, varias mediciones son realizadas y procesadas para comparación.

Muchos de los rasgos usados para el reconocimiento de la firma son características dinámicas en lugar de características estáticas o geométricas, aunque algunos fabricantes también incluyen estas últimas características en el análisis. Las características dinámicas más comunes son: la velocidad, la aceleración, la sincronización, la presión y la dirección de los trazos en la firma, analizados en los ejes X,Y, y Z. La figura 2.8 ilustra estas características dinámicas en una firma. Las posiciones en X y en Y son usadas para mostrar cambios en la velocidad en las dos direcciones respectivas (indicadas por las líneas más claras), mientras que la dirección en Z (línea obscura) es utilizada para mostrar cambios en la presión con respecto al tiempo.

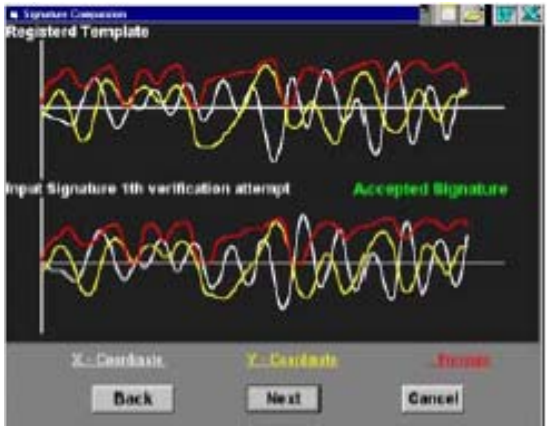


Figura 2.8.- Representación gráfica de las características dinámicas de una firma. En la parte superior de la figura se muestran las características de una plantilla almacenada en el sistema, mientras que en la parte inferior se muestran las características obtenidas de una firma digitalizada que trazó un individuo sobre un pizarrón digital.

El proceso de verificación se realiza mediante la comparación de las características dinámicas existentes en una plantilla almacenada en una base de datos con respecto a las características dinámicas de una firma trazada por un individuo. Si la comparación alcanza o sobrepasa un porcentaje de similitud previamente establecido en el sistema, se acepta la firma y la verificación concluye satisfactoriamente.

Las características utilizadas para el reconocimiento dinámico de la firma son casi imposibles de duplicar. A diferencia de una imagen gráfica de la firma (que puede ser duplicada por un falsificador humano entrenado, o mediante una fotocopia, o incluso mediante el uso de software de diseño o edición de imágenes), las características dinámicas son complejas y únicas y dependen del estilo caligráfico de cada individuo. Sin embargo, se ha observado que estas características dinámicas pueden variar en presencia de factores externos, en otras palabras, la firma y la manera de firmar de un individuo pueden cambiar con el paso del tiempo, o debido a una lesión o enfermedad en las manos, muñecas o dedos, lo que dificulta el reconocimiento dinámico de la firma.

2.3.3.- Reconocimiento facial.

Los seres humanos utilizamos diariamente los rostros para reconocer individuos. Los primeros algoritmos de reconocimiento facial utilizaban modelos geométricos simples, pero el proceso de reconocimiento ha madurado a una disciplina de representaciones matemáticas sofisticadas y a procesos de correspondencia en el transcurso de los últimos diez años. El reconocimiento facial puede ser usado para verificación o identificación.

Lo sistemas de reconocimiento facial están englobados dentro de las técnicas FRT (Face Recognition Thecniques) o técnicas de reconocimiento facial. Estas técnicas de aproximación al reconocimiento facial, pueden clasificarse en dos categorías según el tipo de aproximación *holística* o *analítica*. La aproximación holística (método de las eigenfaces) considera las propiedades globales del

patrón, mientras que la segunda considera un conjunto de características geométricas de la cara.

Dentro del enfoque holístico se encuentra el algoritmo de Análisis de Componentes Principales (PCA) conocido también como el método de las eigenfaces, al igual que cualquier algoritmo de reconocimiento facial, requiere del siguiente proceso:

- Detección.- Mediante un sistema de video o una cámara CCD.
- Alineación.- Una vez detectada una cara, el sistema determina la posición, el tamaño y la posición de la cabeza.
- Normalización.- La imagen de la cabeza se escala y se rota para poder ser colocada en un tamaño y actitud apropiados. La normalización se realiza sin importar la localización y la distancia de la cabeza de la cámara fotográfica. La luz no afecta el proceso de la normalización.
- Representación.- El sistema traduce los datos faciales a un código único. Este proceso de codificación permite una comparación más fácil de los datos faciales adquiridos con los datos faciales almacenados.
- Comparación.- Los datos faciales adquiridos se comparan a los datos almacenados y (idealmente) se relacionan con al menos una representación facial almacenada.

El método de las eigenfaces consiste en la recolección de fotos de individuos. Se adquiere un conjunto de imágenes con diferentes gestos faciales (rostro en 2 dimensiones). Se procesan como mencionamos anteriormente y después todas estas imágenes son combinadas y posteriormente almacenadas en un vector de áreas (unas claras y otras oscuras), para así poder agruparlas en la base de datos. Como cualquier color puede ser creado por la mezcla de colores primarios, cualquier imagen facial puede ser construida por la mezcla de ellos, con diferentes intensidades de luz (Figura 2.9). Después al aplicar el algoritmo PCA sobre los vectores de áreas se obtiene un vector unidimensional. Cuando se presenta el usuario, el sistema obtiene una imagen de su rostro y el vector unidimensional asociado a esa imagen obtenido por el PCA y compara este vector con los vectores asociados a las imágenes almacenadas para lograr una identificación o una verificación.

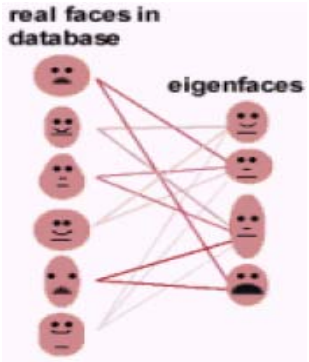


Figura 2.9.- Reconstrucción de rostros de la base de datos a partir de un conjunto de eigenfaces.

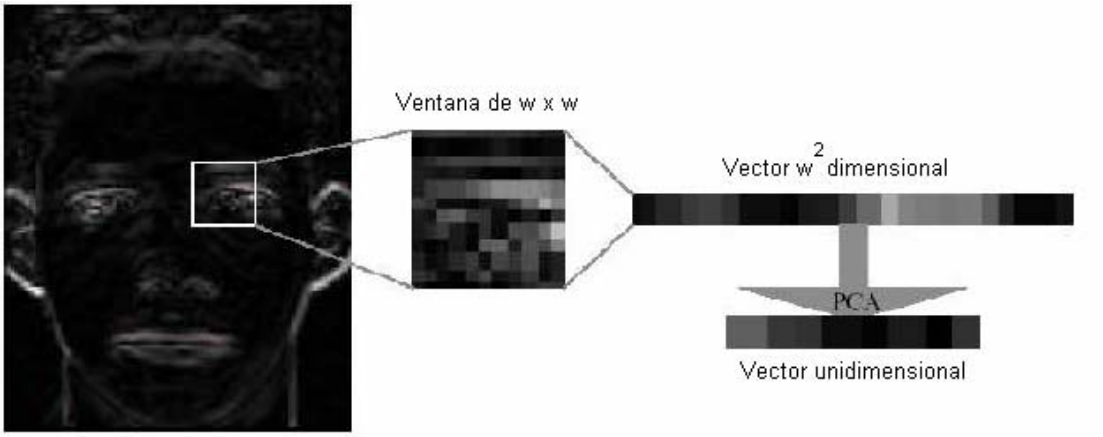


Figura 2.10- Obtención del vector unidimensional por medio del PCA.

La aproximación analítica es muy similar a la técnica de reconocimiento de la geometría de la mano en el que se toman medidas de las distancias entre diferentes puntos de interés, como la distancia entre un ojo a la nariz por ejemplo. Uno de estos métodos emplea un escáner para obtener un mapa del rostro humano en tres dimensiones. Empleando algoritmos matemáticos similares a los utilizados en búsquedas de Internet, la computadora mide las distancias entre determinados puntos de la muestra en la superficie del rostro. A continuación, son reconfiguradas como líneas rectas en un espacio tridimensional, creando una imagen nueva y abstracta capaz de actuar a modo de firma inequívoca de un rostro humano (Figura 2.11).

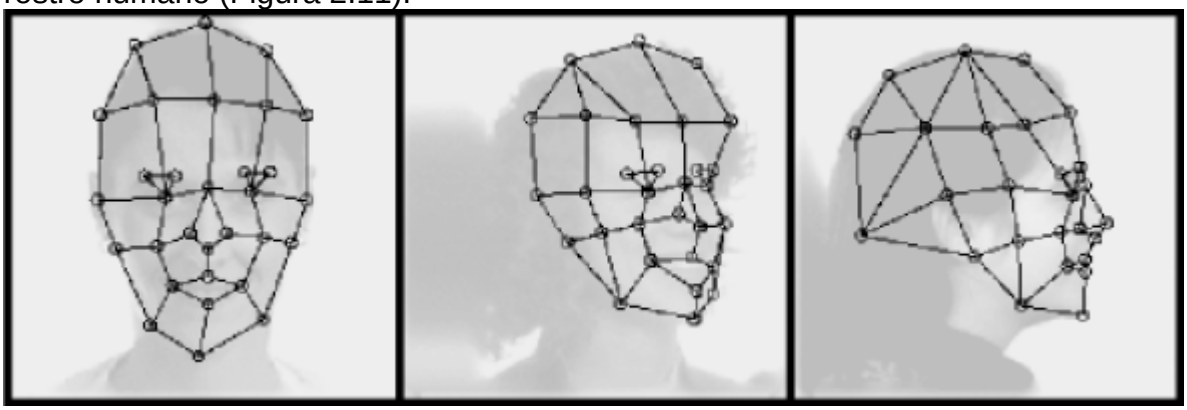


Figura 2.11.- Imágenes de un rostro obtenidas a partir de un algoritmo que emplea el enfoque analítico.

2.3.4.- Reconocimiento de voz.

Los sistemas de reconocimiento de locutores tienen por objetivo discriminar a los usuarios a partir de sus características de la voz, mediante el análisis y tratamiento de la señal de voz. Generalmente se tiende a confundir este tipo de sistema con el de reconocimiento de palabras o interpretador de comandos hablados, estos sistemas de reconocimiento de palabra existen comercialmente para ser integrados a una computadora personal. Este reconocimiento de palabras no es biometría, ya que solo está diseñado para reconocer palabras.

En un sistema para el reconocimiento de voz, se emplea la señal de voz que a largo plazo o en el orden de segundos debe considerarse no estacionarías puesto que sus características temporales se ven sometidas a constantes fluctuaciones física y de conducta con el objetivo de analizar patrones de habla e identificar al interlocutor pero que cuando el tiempo de análisis es muy corto la señal se comporta como una señal que contiene ruido o sea una señal cuasi-estacionaria. Los sonidos sonoros son periódicos, debido a la vibración de las cuerdas vocales y son sonidos de alta energía y estabilidad a corto plazo. Y los sonidos sordos son generados a partir de una constricción en el flujo de aire proveniente de los pulmones y esto produce sonidos de alta frecuencia y baja energía y relativa estabilidad a corto plazo.

Dada la periodicidad de los sonidos sonoros la representación espectral de dicho sonido estará caracterizada por la aparición de la frecuencia fundamental de vibración de las cuerdas vocales junto con sus armónicos.

El espectro de la señal de voz se compone fundamentalmente de dos componentes claramente diferenciadas. La envolvente espectral y la estructura final. Los sistemas de reconocimiento de voz pretenden discriminar identidades.

La estructura final de la señal de voz no comprende información acústica relacionada con la identidad del locutor. Y la envolvente espectral si contiene información a nivel acústico que nos sirve para discriminar al usuario.

Para llevar a cabo está tarea, el patrón creado previamente por el interlocutor, debe ser digitalizado y mantenido en una base de datos que generalmente es una Cinta Digital de Audio.

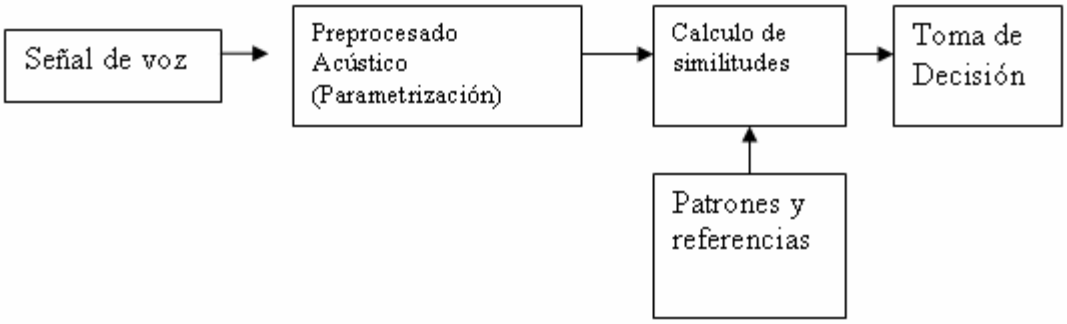
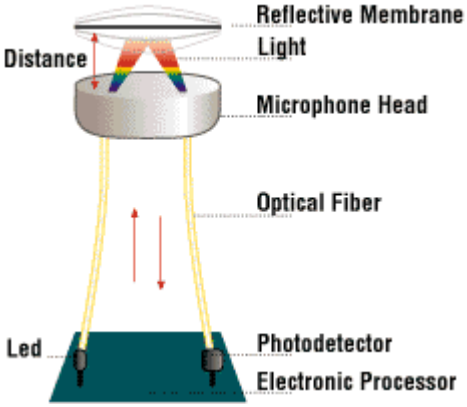


Figura 2.12.- Diagrama de bloques de un sistema de reconocimiento de voz.

En algunos sistemas podemos encontrar los micrófonos ópticos unidireccionales (Figura 2.13), los cuales operan de la siguiente forma: la luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra; cambiando así las características de la luz reflejada. Un foto-detector registra la luz reflejada que en conjunto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido (figura 2.14).



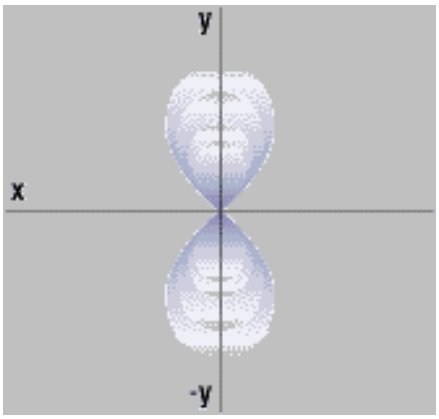


Figura 2.13.- Micrófono óptico. Figura 2.14.- Campo de Recepción del Micrófono.

2.3.5. Iris.

El iris es la membrana interna del ojo, localizado por detrás de la cornea y delante del cristalino que esta atravesada por la pupila. Una propiedad que el iris comparte con las huellas dactilares es la morfología aleatoria de su estructura. No existe alteración genética en la expresión de esta membrana más allá de su forma anatómica, fisiología, color y apariencia general. La textura del iris por si misma es aleatoria y posiblemente caótica. Pero el iris disfruta de ventajas prácticas adicionales sobre las huellas dactilares y otras variables biométricas, como son:

- La facilidad de registrar su imagen a cierta distancia, sin la necesidad de contacto físico o invasivo y quizás discretamente.
- El alto nivel de aleatoriedad en su estructura que permite 266° de libertad que pueden ser codificados y una densidad de información de 3.4 bits por mm^2 de tejido.
- Estable y sin cambio durante el periodo de vida del sujeto.

El propósito del reconocimiento del iris es obtener en tiempo real, con alto grado de seguridad, la identidad de una persona; empleando análisis matemático del patrón aleatorio que es visible dentro del ojo a cierta distancia. Debido a que el iris es un órgano interno protegido (inmune a influencias ambientales) con textura aleatoria, estable (sin cambios), él puede ser usado como una clave viva que no necesita ser recordada pero que siempre estará ahí.

El iris se ve afectado por la pupila cuando ésta reacciona a la luz. Las deformaciones elásticas que ocurren con la dilatación y contracción son rápidamente corregidas empleando algoritmos matemáticos que se encargan de localizar los bordes interno y externo del iris.

Para el análisis de la estructura es necesario emplear operaciones de demodulación matemática empleando los wavelets en 2D de Gabor. Primero es necesario localizar los bordes interno y externo del iris, detectar y excluir los párpados si ellos se interponen. Estas operaciones de detección son llevadas a cabo empleando operaciones integro-diferenciales. Luego se define un sistema de coordenadas bidimensional en el cual se ubica el tejido del iris de una forma que

los cambios de la pupila, las variaciones de la cámara por el acercamiento y la distancia del ojo; no generen efectos. Este sistema de coordenada es polar (parte real e imaginaria).En la figura 2.15 se ilustra el proceso mencionado para la identificación del iris. En la fase de demodulación el patrón detallado del iris es codificado en un código de 256 bytes, el cual representa todos los detalles de la textura empleando fasores en el plano complejo.

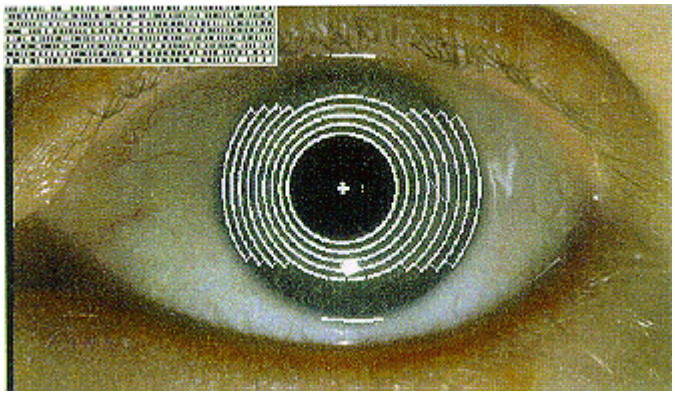


Figura 2.15.- Mapa del Iris. En la parte superior se aprecia el código generado.

En sistemas para el reconocimiento del iris es común encontrar cámaras de vídeo de tipo CCD. En la figura 2.15 se puede apreciar un diagrama de bloques de esta cámara. El corazón de la cámara es un circuito integrado tipo CCD. Este dispositivo consiste de varios cientos de miles de elementos individuales (píxeles) localizados en la superficie de un diminuto CI (Circuito Integrado). Cada píxel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la camera), almacenando una pequeña carga de electricidad. Los píxeles se encuentran dispuestos en forma de malla con registros de transferencia horizontales y verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). Esta transferencia de señales ocurre 6 veces por segundo.

En la figura 2.16, podemos apreciar un arreglo comercial de este tipo de CI. En el campo de procesamiento de imágenes, este integrado ha revolucionado todo lo establecido, siendo el componente principal de las llamadas cámaras fotográficas digitales.

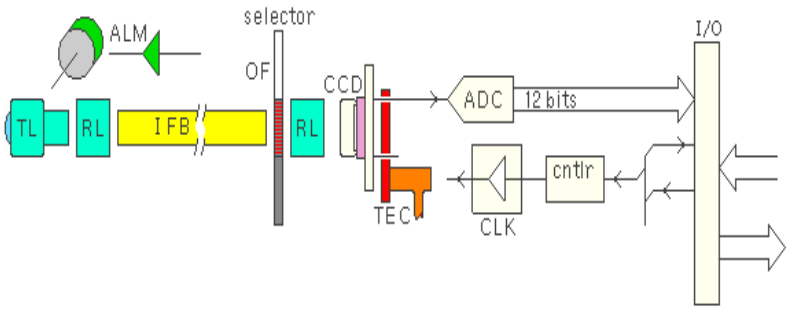


Figura 2.16.- Diagrama de bloques de la Cámara CCD.

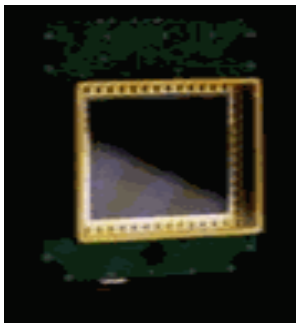


Figura 2.17.- Sensor CCD.

2.4.- Huella Digital.

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 **l**os dibujos y son los formados por las crestas papilares y los surcos interpupilares, son rugosidades que forman salientes y depresiones.

Antes de empezar a estudiar los sistemas de reconocimiento de huella digital es necesario estudiar las características biológicas y físicas que se encuentran en la huella digital:

Se le da el nombre de crestas papilares a los relieves epidérmicos situados en la palma de las manos y en la planta de los pies, biológicamente son unas glándulas de secreción de sudor situadas en la dermis, también llamadas glándulas sudoríparas. Constan de un tubo situado en el tejido celular subcutáneo, formado por un glomérulo glandular con un canal rectilíneo, que atraviesa la dermis, para venir a terminar en la capa córnea de la epidermis, concretamente en el poro, que es un orificio situado en los lomos de las crestas papilares.

Una vez que el sudor sale al exterior, se derrama por todas las crestas y se mezcla con la grasa natural de la piel, dando lugar a que cuando se toque o manipule un objeto apto para la retención de huellas, éstas se queden impresas en el mismo.

Los dibujos que aparecen visibles en la epidermis, está demostrado científicamente y comprobado por la experiencia, que son perennes, inmutables y diversiformes:

- Son *perennes*, porque desde que se forman en el sexto mes de la vida intrauterina, permanecen indefectiblemente invariables en número, situación, forma y dirección hasta final de nuestra vida.
- Son *inmutables*, ya que las crestas papilares no pueden modificarse fisiológicamente. Si hay un traumatismo poco profundo, se regeneran y se es profundo, las crestas no reaparecen con forma distinta a la que tenían, sino que la parte afectada por el traumatismo resulta invadida por un dibujo cicatrizal.
- Son *diversiformes* pues no se ha hallado todavía dos impresiones idénticas producidas por dedos diferentes.

La singularidad de una huella puede ser determinada por los tipos de patrones de crestas y surcos. Además 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.

2.4.1.-Clasificación

Los patrones de huellas digitales están divididos en varios tipos principales, todos ellos matemáticamente detectables. Los detalles son puntos característicos o también se designan así a las particularidades papilares que, en detalle, ofrecen las crestas y valles en su curso por el dactilograma natural y su impresión. Es decir son las convergencias, desviaciones, empalmes interrupciones fragmentos etc. de las crestas y sus surcos. A estos puntos también se llaman minutae, o minucias, término utilizado en la medicina forense que significa "punto característico". Estos puntos serán de gran importancia para nuestro estudio y se dará más énfasis en temas siguientes. Las siguientes figuras muestran los detalles que se puede encontrar en la huella.

Figura 2.18.- Minucias en la huella digital.

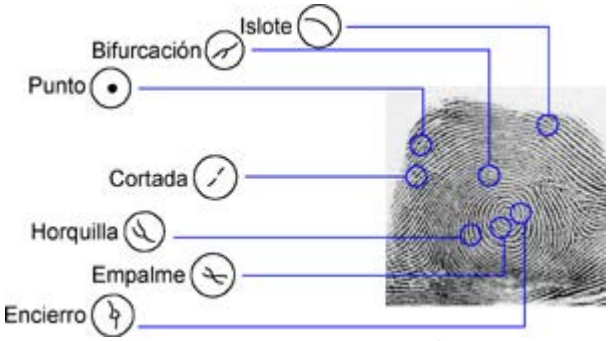


Figura 2.19.-Puntos característicos.

Finalmente, para cerrar este apartado relativo al estudio morfológico de la huella dactilar, vamos a introducir dos singularidades presentes en algunas huellas, en función de su tipología, denominada Core y Delta.

El Core responde al punto localizado en la zona del núcleo de la huella, donde una de las crestas cambia bruscamente su dirección y describe un ángulo de 180° retorna por tanto a la posición de origen.

El Delta es un punto características del dibujo papilar de algunas huellas que puede presentar forma de triángulo o de trípode, está formado por la aproximación o fusión de las crestas existentes en la zona frontera marginales basilar y el núcleo de la huella.

Su importancia radica en que en la zona donde se halla ubicada, así como en sus aproximaciones, aparecen muchos puntos característicos

Todos los dactilogramas coinciden en el hecho de que las crestas papilares no describen formas aleatorias, sino que se agrupan hasta llegar a constituir sistemas definidos por la uniformidad de su orientación y figura.

Estas clases pueden estar incluidas en función del número de deltas presentes en las huellas, se catalogan así: Adeltas, si la huella no presenta ninguna delta; Monodelta, si presenta una única delta; Bidelta, si presenta un total de 2 deltas. A continuación detallaremos las seis clases propias de la clasificación, así como un conjunto de ejemplos de las morfologías correspondientes a cada una de ellas.

- Arco: subtipo del grupo Adelta.
- Bucle hacia la derecha: subtipo del grupo Monodelta.
- Bucle hacia la izquierda: subtipo del grupo Monodelta.
- Doble Bucle: subtipo del grupo Bidelta.
- Remolino: Subtipo del grupo Bidelta.

Estas clasificaciones son importantes si se tiene una gran base de datos con lo que se puede reducir el tiempo de búsqueda de la persona a la que se pretende identificar. En la figura 2.20 se muestra algunas de las formas mas comunes.

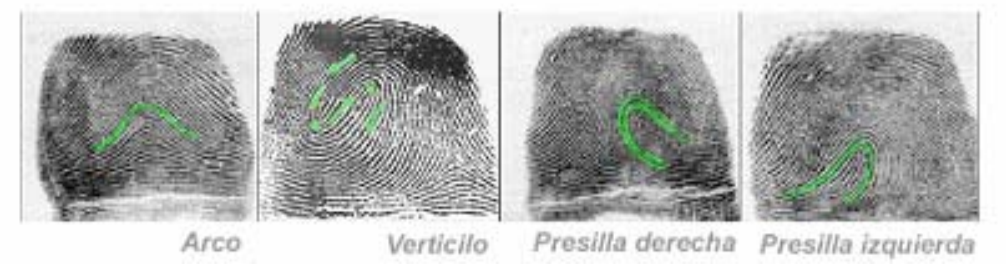


Figura 2.20.-Clasificación de huellas digitales.

2.4.2.- Reconocimiento de los patrones de una huella.

Un sistema de comparación de la huella digital involucra varias fases las cuales mencionaremos y detallaremos en esta sección.

Primero se mencionara la fase de la adquisición de la huella dactilar: está fase se compone de la adquisición de la imagen de la huella a través de los lectores de huella.

Segundo paso se requiere clasificar la huella: con la ayuda de un filtrado de la parte central de la huella a través de filtros Gabor, da como resultado una discriminación de las crestas presentes de la huella, en función de la dirección (0˚, 45˚,90˚, 135˚). Esta información se cuantificará posteriormente para generar el denominado código de la huella para realizar la clasificación de la huella.

Después se mostrara la fase de preprocesamiento de la imagen. La cual involucra el calcular los vectores de las minucias y obtener su dirección de campo y su crecimiento, para después hacer la segmentación de la huella.

Seguimos con la fase de extracción de rasgos. Las posiciones de las minucias son determinadas y con ello podemos pasar a la formación de las

plantillas que nos ayudaran para la parte de identificación y comparación de las imágenes.

Comparación del Modelo: finalmente la fase de comparación. Los rasgos de las huellas son comparadas con una muestra que se encuentra en la base de datos del sistema.

Verificación/identificación: La verificación se llevará a cabo a partir del número obtenido en el proceso anterior (normalmente entre 0 y 1), relativo al nivel de semejanza entre el modelo de referencia y el modelo candidato. Este número de semejanza se comparará con un umbral de seguridad establecido por el sistema; como resultado de dicha comparación se obtendrá la verificación o no del individuo. El proceso de identificación, por su parte entregará como resultado, a la persona que presente una plantilla con un mayor nivel de similitud con respecto a la entrada biométrica parametrizada.

2.4.3.-Proceso de preprocesamiento de una huella.

En este apartado nos centraremos en una parte del nivel algorítmico de cada una de las etapas del preprocesamiento del la huella dactilar, hasta obtener una plantilla de la huella desde obtener la dirección de los campos, segmentación, adelgazamiento, etc.

2.4.3.1.-Direcciones de los campos

En este paso lo primero es aplicar un algoritmo que extrae la información de las direcciones del las crestas y valles de la huella a partir de las tonalidades que conforman la imagen de la huella digital; estas tonalidades se presentan en la escala de grises para cada uno de los puntos o píxeles que forman la imagen. El método es basado en el vector gradiente de la escala de grises en la imagen. El objetivo del algoritmo es determinar el sentido de circulación de las líneas (crestas o valles) alrededor de cada punto de la imagen.

La imagen es almacenada como una matriz, donde el valor de cada elemento es el valor del nivel de gris del punto correspondiente. Existen diferentes estimadores para la dirección de las líneas alrededor de un punto. Entre ellos vale la pena mencionar el estimador de mínima varianza y el estimador de mínima diferencia.

En este trabajo se utilizara el estimador de mínima diferencia como el más adecuado. Para obtener la dirección asociada a un punto dado en la imagen, se construye una transformación que asigne a cada punto su dirección; para ello se escogen primero las direcciones posibles de cada punto (recorrido de la transformación) y el tamaño y forma de la región alrededor del punto que se tendrá en cuenta.

Para su procesamiento digital, el modelo de una imagen es una matriz y esta dado por la ecuación 2.1:

$$\left(a_{ij}\right) = \left(a[i, j]\right) \qquad 2.1$$

Que contiene en cada una de sus componentes el valor correspondiente al nivel de intensidad de gris o de color presente en la imagen original en la misma

coordenada o el mismo punto; la matriz esta conformada por valores discretos. Con la matriz se definen las vecindades de radio N de un punto [i, j] como los conjuntos de valor real R[i, j] y poder manejar un margen real y con el cual se va a trabajar en el procesamiento:

$$R_N[i,j] = \{a[k,l] : \|k-i\| \le N, \|i-j\| \le N\} \quad 2.2$$

El escoger un radio de las vecindades para el procesamiento es muy importante ya que se debe garantizar que en la vecindad de cada punto haya suficiente información acerca de la dirección de las líneas vecinas. Es por esto que N depende del grosor de las crestas y valles de la huella, lo cual es un parámetro muy ligado con el método de adquisición y su resolución.

Si tenemos M posibles direcciones numeradas de 0 a M − 1, y definimos como dirección M, la que se presenta en regiones con alto nivel de ruido o en regiones muy uniformes donde no se pueda estimar la dirección, el conjunto de direcciones posibles esta dado por la ecuación 2.3:

$$s = \{0,1,2,3,...,M\}. \quad 2.3$$

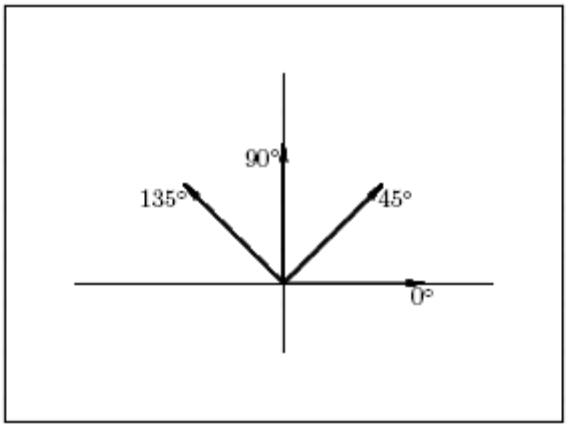


Figura 2.21.- Posibles direcciones

Las direcciones se escogen como se muestra en la figura 2.21 y el ángulo correspondiente a cada dirección está dado por la ecuación 2.4:

$$\theta_k = \frac{180^o}{M-1} k.....k = 0,1,.....M-1. \quad 2.4$$

A lo largo de cada dirección y dentro de la vecindad de cada punto, se define un conjunto de puntos

$$T^k_{[i,j]} = \{[m,n] \mid [m,n] \in R_N[i,j] \ y \ [m,n] \ldots está \quad en \quad la \quad dirección \quad k\} \quad 2.5$$

En cada punto se puede definir un estimador Sk[i,j] para cada una de las direcciones posibles, así:

$$S^k_{(i,j)} = \sum_{|m,n \ | \in T^k | i,j|} \delta(\alpha[m,n], \alpha[i,j]) \quad 2.6$$

La transformación asigna al punto la dirección donde $S^k[i, j]$ toma el valor mínimo (si existe). Es posible que $S^k[i, j]$ sea el mismo para todo k, lo cual indicaría que el punto [i, j] esta localizado en una región muy ruidosa o donde no se presentan valles o crestas.

Es claro que esta definición presenta ciertos inconvenientes, ya que el máximo se puede presentar en varias direcciones, lo cual no daría un valor único para la imagen de un punto. Para salvar este inconveniente se hace la siguiente consideración:

Si al calcular el máximo de las sumas $S^k[i, j]$ alrededor de un punto, este se presenta en exactamente dos direcciones adyacentes, se elige cualquiera de ellas; de otra forma, se le asigna la dirección M (dirección indefinida).

Con esto se consigue asignarle a cada punto de la imagen original de la huella un valor en el rango 0 . . ,M que identifica la dirección del flujo de la cresta o valle al cual pertenece el punto.

Luego de obtener la matriz de direcciones, se realiza un proceso que consiste en agrupar puntos de la imagen en regiones llamadas segmentos, y calcular la dirección predominante en el segmento; de esta forma se obtiene una matriz de dimensión mas pequeña, en la cual se ha reducido la redundancia pero se sigue conservando la información acerca de las direcciones de las líneas, la cual va a ser de fundamental importancia en la clasificación de la huella.

2.4.3.2.-Segmentación

El proceso de segmentación consiste en dividir la huella en regiones disyuntas. En este caso las regiones son cuadradas y su tamaño es fijo para toda la imagen. En cada una de estas regiones se aplica un algoritmo para calcular la dirección predominante en la región.

Básicamente, el proceso se reduce a definir una variable aleatoria X que represente la dirección de un determinado punto dentro de un segmento de la imagen.

Se realiza el cálculo de la distribución de probabilidades de esta variable aleatoria, hallando la frecuencia de cada dirección en el segmento y se almacena en un arreglo.

Esta distribución de probabilidades puede tener diversas formas, las cuales se analizan a continuación.

• Uniforme: si las frecuencias de todas las direcciones son iguales. Esto indica que el segmento contiene líneas en varias direcciones, que el segmento contiene mucho ruido o que es una región plana. Por esto es imposible asignarle la dirección especifica al segmento en el intervalo 0, . . .M, y entonces se le asigna el valor M (Figura 2.22), la figura también nos ilustra el histograma de los valores de los píxeles que se en encuentran en una imagen.

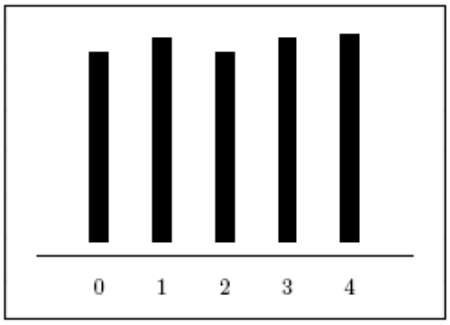


Figura 2.22.- Histograma con valores semejantes

• Unimodal: si se presenta un máximo de frecuencia, y la relación entre este y el siguiente es superior a un determinado umbral. En este caso hay una frecuencia predominante y la dirección de esta es asignada al segmento

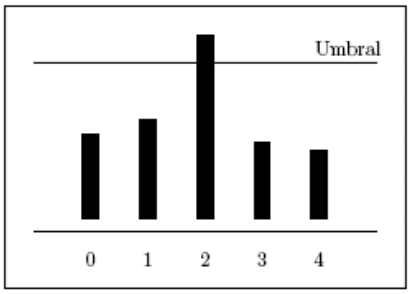


Figura 2.23.- Histograma con un valor predominante

• Bimodal: si se presenta un máximo de frecuencia en una dirección k, y hay exactamente otra dirección con un valor de frecuencia muy cercano (determinado por un umbral). En este caso hay dos direcciones predominantes, y se asigna al segmento la dirección del ángulo medio (aproximada) entre las dos predominantes. Si son adyacentes, se puede escoger cualquiera de las dos (Figura 2.24). Y si existen varias frecuencias con valores muy cercanos al máximo, se asigna al segmento dirección M (indefinida).

Los valores asignados a la dirección de cada segmento se asignaron por este método, ya que los resultados experimentales mostraron su efectividad, aunque existen diversos métodos para escoger la dirección del segmento, a saber:

– se escoge como dirección predominante del segmento
– el valor esperado de la dirección recorriendo todo el segmento,
– se escoge la mediana,
– se escoge la moda.

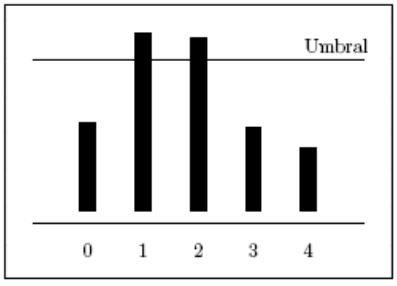


Figura 2.24.- Histograma con dos valores predominantes.

El estudio estadístico de estos estimadores y de los tipos de distribuciones permite concluir que la moda es el más robusto en este tipo de imágenes, y el algoritmo de asignación de direcciones a cada segmento se reduce a calcular la moda de la distribución, es decir, el valor de dirección más repetida o de mayor probabilidad.

Se calculan los dos valores siguientes a este en cuanto a probabilidad se refiere. Y se elige cierto umbral que determina el nivel de indecisión cuando se tienen dos direcciones cuyas probabilidades son muy cercanas. Si la relación entre las dos direcciones con probabilidades muy cercanas es menor al umbral, se escoge como dirección predominante la moda de la distribución (dirección más probable). Si esta relación no es superior al umbral, se compara con la siguiente dirección en orden de probabilidades y se verifica de nuevo la condición del umbral entre el segundo y el tercero. Si esta se cumple, se decide por el promedio entre el primero y el segundo; si no, se determina el punto con una dirección indefinida, que se representa con un código direccional especial. Básicamente se trata de tener un criterio de decisión basado en la dispersión de la distribución de direcciones en un segmento. Debe tenerse en cuenta que cuando se cumpla la condición del umbral entre el segundo y el tercer valor de la distribución, el promedio de las direcciones debe hacerse de tal forma que no se genere error, como se ve en el eje.

Dirección	Probabilidad
0°	0.4
45°	0.001
90°	0.009
135°	0.39

Tabla 2.1.- Posibles direcciones y sus probabilidades.

Si se supone un umbral de valor 0.5, es claro que la razón entre las direcciones predominantes 0^0 y 135^0 es mayor al umbral y se escogería el promedio de estas direcciones. Si se hiciera el promedio aritmético se llegaría a un resultado erróneo (67.5^0). En este caso se puede considerar la dirección 0^0 como 180^0 y el promedio obtenido es 157.5^0.

Una vez asignada a cada segmento de la matriz de imagen una dirección específica, esta nueva matriz es utilizada para detectar la presencia de regiones singulares dentro de la huella. Llamaremos regiones singulares a los segmentos de la imagen donde la circulación de las líneas presente patrones de tipo delta, núcleo o espiral. Un delta es un patrón de flujo de líneas en el cual estas llegan paralelas a un punto y en el se bifurcan, saliendo por dos direcciones diferentes.

Un núcleo es una región donde las líneas llegan a un punto y se devuelven para salir por la misma dirección en que llegaron. Una espiral es el patrón de flujo en el cual las líneas no entran ni salen al segmento sino que circulan en el. En la Figura 2.25 se observan los posibles patrones de flujo, para los segmentos. Para la detección de puntos singulares se realiza el cálculo de la variación del ángulo entre la dirección de los segmentos vecinos y el segmento que es necesario calcular, a lo largo de una circunferencia que lo rodee (figura 2.25). Este ángulo neto permite determinar si la región analizada es singular o no, y qué tipo de

singularidad se presenta. Es por esto que la confiabilidad de la matriz de direcciones es bastante importante.

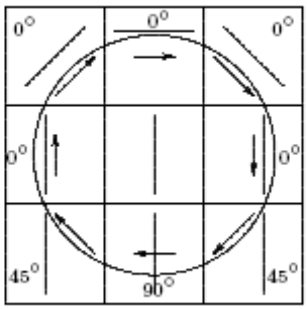


Figura 2.25.- Región tipo núcleo.

2.4.3.3.- Algoritmo ridge–valley

El procedimiento ridge–valley, (cresta–valle), tiene como objetivo filtrar y adelgazar la imagen de una huella digital adquirida previamente. El procesamiento de la imagen se hace por ventanas de tamaño definido, lo que hace necesario definir dimensiones adecuadas para este tipo de filtros.

En el proceso de filtrado se realiza simultáneamente la binarización de la imagen, la cual puede tener cualquier cantidad de niveles de gris. Por lo tanto, se realiza un filtrado direccional, que además de definir un umbral local determina también la dirección de cada punto. El resultado final: cada punto tiene asociado un tono (blanco o negro) y una dirección que lo caracterizan.

Finalmente, se agrupan los píxeles en ventanas más grandes para definir una matriz de direcciones, la cual es muy útil para el análisis de los puntos característicos. Para el análisis de las huellas se definen (inicialmente) ventanas de 9×9 pixels1, en donde el píxel central corresponde al punto al cual se le va a determinar su tono y dirección. En la figura 2.26, este punto está marcado con una P. los puntos marcados con números iguales conforman líneas de una dirección definida que atraviesan la ventana pasando por el punto en consideración y son los empleados en el análisis, en tanto que los que aparecen como blancos son puntos que no importan.

7		6		5		4		3
8		7	6	5	4	3		2
		8				2		
1		1		P		1		1
		2				8		
2		3	4	5	6	7		8
3		4		5		6		7

Figura 2.26.- Ventanas para determinar el valor de P.

Teniendo en cuenta esta ventana, se define un parámetro conocido como slit sum(suma direccional), el cual consiste en realizar la suma de los píxeles en una de las ocho direcciones definidas. Entonces tenemos:

$$S_i = \sum_{j=0}^{3} P_{i,j} \qquad 2.7$$

El tamaño adecuado para una ventana de estas es aquel que tenga un ancho superior al ancho de las crestas, para poder abarcar la información suficiente y necesaria. Se puede observar a partir de la figura que las direcciones definidas corresponden a los siguientes ángulos:

Dirección	Ángulo
1	0.0˚
2	26.5˚
3	45˚
4	63.5˚
5	90˚
6	116.5˚
7	135˚
8	153.5˚

Tabla 2.2.- Ángulos de los píxeles cercanos de P.

Donde. S_i es una sumatoria desde i = 1, 2,. . . 8 y los $P_{i,j}$ son los puntos que comparten igual dirección. Estas sumas son empleadas en el análisis que sigue. El binarizador busca definir un umbral a partir del cual se puedan clasificar los puntos como blancos (surcos) o negros (crestas). Se realizan dos aproximaciones: definición local del umbral, y comparación de sumas direccionales. El método de definición de un umbral local asigna a un píxel el color blanco si la suma S es mayor que el promedio de los píxeles considerados en la ventana. Aprovechando las sumas direccionales, un píxel será blanco si:

$$S \rangle \frac{1}{8}\sum_{i=1}^{8} S_i. \qquad 2.8$$

$$S = 4P \qquad 2.9$$

Observando que S es cuatro veces el valor del punto analizado, ya que cada suma direccional es la suma de cuatro píxeles. La comparación de sumas direccionales toma el promedio de los valores máximo y mínimo de estas sumas como parámetro para definir el umbral. Así, un punto será blanco si:

$$\frac{s_{\max} + s_{\min}}{2} > \frac{1}{8}\sum_{i=1}^{8} s_i \qquad 2.10$$

Es claro que si un píxel está en un valle, una de sus sumas direccionales tendrá un valor alto, en tanto que las otras no, ya que deben cruzar algunas crestas cuyos píxeles tienen un valor bajo. Un caso idéntico ocurre cuando el píxel está en una cresta, sólo que en este caso, una suma tendrá un valor muy bajo, mientras las demás no tanto. El método ridge–valley unifica estos dos criterios para definir el umbral, de tal forma que un punto será considerado blanco sí:

$$S + s_{\max} + s_{\min} > \frac{3}{8}\sum_{i=1}^{8} s_i \qquad 2.11$$

A medida que se realiza la binarización, cada píxel es asociado con la dirección de su mayor (menor) suma direccional si pertenece a un valle (cresta), completando así su caracterización.

La dirección de cada punto no brinda ninguna información acerca de los detalles que pueda tener una huella. Por lo tanto, es necesario agruparlos en ventanas cuya dimensión permita identificar los puntos característicos. Esto genera una matriz de direcciones cuyo tamaño depende de las dimensiones de la imagen y de la ventana que, además de disminuir la información requerida, realiza un proceso de suavizamiento de las direcciones al promediar las de los píxeles dentro de la ventana. Las ventanas seleccionadas inicialmente para este fin son de 16 × 16 píxeles. Promediar las direcciones trae como efecto el suavizamiento de las direcciones y el aumento de los niveles del cuantificador, que antes era de ocho niveles. Hay que tener cuidado al realizar el promedio de las direcciones: si se realiza el promedio común y corriente, se introduce un gran error.

Por ejemplo, ángulos de 153.5 y 0º promediados dan un resultado de 76.75º, cuando seguramente la dirección mas apropiada es la de 167.0º (correspondiente al promedio entre 153.5º y 180º). Para evitar este error, se emplean las componentes vectoriales de cada uno de los píxeles en términos de su ángulo: (cos θ , sin θ). Así, la ventana final estará caracterizada por un vector q tal que:

$$\angle \vec{q} = \arctan \frac{\sum_{i=1}^{n^2} \sin(2\theta_i)}{\sum_{i=1}^{n^2} \cos(2\theta_i)} \qquad 2.12$$

$$\left\| \vec{q} \right\| = \frac{1}{n^2} \sqrt{\left(\sum_{i=1}^{n^2} \cos(2\theta_i) \right)^2 + \left(\sum_{i=1}^{n^2} \sin(2\theta_i) \right)^2} \qquad 2.13$$

Donde n es la longitud de un lado de la ventana.

La magnitud del vector da una medida de la confiabilidad del resultado. En una región borrosa si

$$\left\| \vec{q} \right\| << 1, \qquad 2.14$$

Tanto que en una región bien definida sí se cumple que:

$$\left\| \vec{q} \right\| \approx 1. \qquad 2.15$$

2.4.3.4.- Adelgazamiento

Para obtener la información de los detalles es necesario realizar el proceso de adelgazamiento de la imagen con el fin de obtener curvas cuyo espesor sea de un píxel.

Así es posible determinar sin ambigüedades la estructura de la huella. Por ejemplo, es muy difícil determinar si existe curvatura cuando el grosor de la imagen analizada es de 4 píxeles: aún si se detecta la presencia de la curva es muy difícil determinar que tan cerrada es.

Es muy importante definir el esquema que se va a emplear para realizar el adelgazamiento, ya que no se puede permitir la generación de puntos no conectados cuando originalmente lo estaban. Existen algunos algoritmos que por sus características pueden producir este tipo de efectos. Otros evitan este problema, pero su complejidad es tal que el procesamiento de la imagen es muy lento y no sirve para una aplicación como esta, en la cual el análisis debe ser llevado a cabo en tiempo real. Por lo tanto, es necesario buscar un algoritmo que cumpla como mínimo con las dos condiciones expuestas.

Históricamente, el problema de adelgazar un patrón correspondiente a una imagen ha sido tratado y se han encontrado diversas aproximaciones al algoritmo ideal. El estudio de los principales algoritmos de adelgazamiento existentes muestra que en su totalidad estos están enfocados a aplicaciones específicas, como adelgazamiento de caracteres escritos, seguimiento de arterias e identificación de cromosomas. Se observó el desempeño de los algoritmos con imágenes correspondientes a huellas dactilares y se descubrieron los posibles casos excepcionales donde los algoritmos fallan. El factor predominante es la distancia entre líneas; esta distancia en huellas dactilares es mucho más pequeña que en caracteres o arterias. Además, el grosor de las mismas es pequeño y por lo tanto los puntos que deben ser borrados son relativamente pocos. Si se usan los algoritmos convencionales, estos conectan líneas que en la realidad no están conectadas. Es por esto que, cualquiera que sea el algoritmo escogido, se debe realizar un ajuste para acomodarse al estilo de patrones de las huellas dactilares.

Para obtener el esqueleto de una imagen existen tres aproximaciones básicas:

- **Seguimiento de bordes**. Este método consiste en recorrer la imagen en repetidas ocasiones, detectando los puntos que conforman el borde de la imagen. En cada recorrido se eliminan los puntos que no degeneren la imagen de acuerdo con unas condiciones dadas. Cuando en un barrido de la imagen no se produzcan cambios, se ha obtenido el esqueleto de la imagen.

- **Propagación de frentes de fuego**. Consiste en la aplicación del principio de Huygens para la propagación de las ondas. Para una imagen, se supone que cada punto del borde de la misma es un punto generador de

ondas esféricas. Tan pronto choquen dos ondas se tendrá el punto deseado del esqueleto de la imagen.

- **Adelgazamiento metódico**. Este algoritmo genera el esqueleto de la imagen calculando la distancia de cada punto interno al borde. A partir de las distancias más pequeñas se genera el esqueleto. Este método, al igual que el anterior, supone una mayor complejidad computacional.

Para el análisis de huellas digitales el método de seguimiento de bordes, es el más adecuado ya que el grosor de las líneas originales no es muy grande y por lo tanto son pocos los puntos que se deben borrar. Por la misma característica de la imagen, los bordes son demasiados, como para emplear el segundo o el tercer método, ya que estos emplean cada punto del borde para generar el esqueleto.

Dentro de los algoritmos que emplean el método iterativo de adelgazamiento se pueden nombrar los siguientes: CLT (Classical Thinning Algorithm), CG (Contour Generating Algorithm), y CGT (Contour Generating Thinning Algorithm). Este último es una combinación de los dos anteriores. Posteriormente se desarrolló un algoritmo con base en el CGT que disminuía la erosión del patrón, conocido como SPTA (Safe Point Thinning Algorithm) el cual resulta bastante apropiado para huellas dactilares.

El algoritmo de adelgazamiento que emplea el método clásico barre la imagen en su totalidad y en cada pasada elimina algunos puntos que no conforman el esqueleto. El algoritmo de generación de contorno propone fijar la atención sólo sobre los puntos que conforman el borde de la imagen, reduciendo así el tiempo de procesamiento. La combinación de estos dos da origen al algoritmo de adelgazamiento por generación de contorno y al SPTA. Sus conceptos básicos son explicados a continuación.

Los 8 vecinos de un punto ***p*** están definidos como los 8 puntos adyacentes a ***p***. Los puntos $n_0, n_2, n_4 n_6$ se llaman 4vecinos de ***p***. En la literatura estos últimos se conocen como los vecinos ortogonales de ***p***. Se dice que un esqueleto es j–conectado (j toma el valor de 4 u 8). Si entre cualquier par de puntos oscuros $\boldsymbol{p}_0$ y $\boldsymbol{p}_n$ existe un camino $\boldsymbol{p}_0, \boldsymbol{p}_1 \ldots \boldsymbol{p}_{i-1}, \boldsymbol{p}_i, \boldsymbol{p}_{i+1} \ldots \boldsymbol{p}_n$ tal que $\boldsymbol{p}_{i-1}$ es un j vecino de $\boldsymbol{p}_i$ para $1 \leq i \leq n$ .También se define un punto final, como un punto oscuro con por lo menos un 8–vecino oscuro. Inicialmente se define un conjunto $S = \{1\}$ para identificar todos los puntos del objeto y el conjunto $S = \{0\}$ para identificar todos los puntos del fondo. La binarización se encarga de definir a la imagen bajo estas especificaciones. Cada punto analizado ***p*** tiene ocho vecinos. Estos vecinos son denominados de acuerdo a la distribución que se muestra a continuación: n_3, n_2, n_1 n_4 $n_0, n_5, n_6 n_7$.

n_3	n_2	n_1
n_4	p	n_0
n_5	n_6	n_7

Figura 2.27.- Vecinos cercanos de P.

El primer paso necesario es identificar los bordes de la imagen. Para tal fin se barre la imagen en forma horizontal o vertical. Cada punto ***p*** de S que sea un borde es marcado con el número 2 y su posición es almacenada en un vector. Es importante notar que esta es la única vez que se recorre la imagen en su totalidad. Posteriormente se recorren las direcciones almacenadas en el vector que contiene los bordes de la imagen. Cada punto ***p*** que sea un borde será borrado si su eliminación cumple las siguientes condiciones:

i) No borra terminaciones.
ii) No rompe la conectividad del patrón.
iii) No causa erosión excesiva.

Este proceso se repite hasta que no produzca ninguna modificación en el barrido. En ese momento se tendrá la imagen adelgazada, o lo que es lo mismo, su esqueleto. Para que no se produzca una imagen con un esqueleto sesgado es necesario determinar el orden en que esta se recorre. En realidad no se cuenta con un solo vector para almacenar los bordes sino con cuatro; cada uno de estos almacena una clase de borde, siendo estas clases los vecinos izquierdos, derechos, superiores e inferiores. Cada vez que se recorre la imagen se recorre en realidad uno de estos vectores. Para evitar un esqueleto que no corresponda a la imagen analizada es necesario que el orden en que se generan estos vectores sea el mismo que aquel en el que se recorre la imagen. Es decir, si se generó primero el vector de los vecinos superiores, este debe ser el primer vector en recorrerse al realizar el análisis. Las distribuciones y condiciones de los puntos bajo las cuales un punto p que es del borde puede ser suprimido se muestran a continuación para el caso de un punto del borde izquierdo.

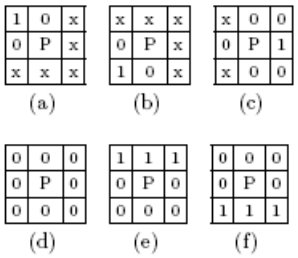


Figura 2.28.- Posibles distribuciones alrededor de P.

De acuerdo con estas distribuciones, ***p*** debe ser suprimido si:
$n_0 = 1$ y ***p*** no pertenece a las ventanas (a), (b) y (c);
$n_0 = 0$ y ***p*** pertenece a las ventanas (d), (e) y (f).

Haciendo las respectivas rotaciones se obtienen las condiciones para los puntos de los bordes derecho, superior e inferior.

Igualmente se pueden obtener las siguientes expresiones booleanas que determinan los puntos que pertenecen al esqueleto, denominados en la literatura safe points (SP).

Para los del lado derecho se tiene:

$$S_0 = n_4 \cdot (n_5 + n_6 + n_2 + n_3) \cdot (n_6 + \overline{n}_7) \cdot (n_2 + \overline{n_1}) \qquad 2.16$$

Para los superiores:

$$S_2 = n_6 \cdot (n_7 + n_0 + n_4 + n_5) \cdot (n_0 + \overline{n}_1) \cdot (n_4 + \overline{n}_3) \qquad 2.17$$

Para los del lado izquierdo:

$$S_4 = n_0 \cdot (n_1 + n_2 + n_6 + n_7) \cdot (n_2 + \bar{n}_3) \cdot (n_6 + \bar{n}_5) \quad 2.18$$

Para los inferiores:

$$S_7 = n_2 \cdot (n_3 + n_4 + n_0 + n_1) \cdot (n_4 + \bar{n}_5) \cdot (n_0 + \bar{n}_7) \quad 2.19$$

Todo el análisis anterior es una pequeña parte de lo que es necesario para la tratamiento digital de una imagen de la huella digital, y nos ejemplifica todo el los procesos requeridos para tener una imagen de buena calidad, para poder conseguir la extracción de los detalles que nos servirán para identificar y verificar si el propietario de la huella pertenece a la base de datos del sistema y poder tener acceso o no tenerlo.

En la figura 2.29 muestra la parte del procesamiento y extracción de detalles de una imagen, con los bloques que acabamos de analizar.

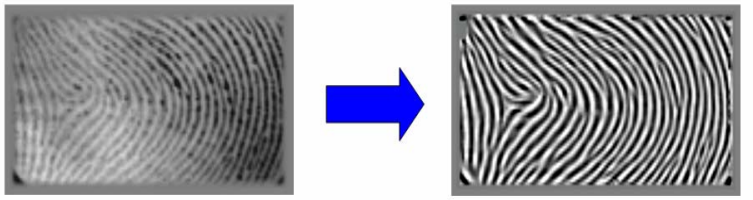


Figura 2.29.-Imagen tratada.

2.4.4.- Técnicas de reconocimiento de huella digital.

Entre las técnicas biométricas, la identificación y verificación basada en las huellas dactilares es el método más recurrente, el cual ha sido usado en numerosas aplicaciones. Como ya se menciono una huella esta formada por una serie de crestas y surcos localizados en la superficie de los dedos.

Esta sección presentamos una muestra de los diferentes métodos y algoritmos que son utilizados en la automatización del reconocimiento de las huellas digital. Primero la estructura general de una huella dactilar o digital es adquirida y procesada por los lectores. Este estudio es simplemente de clasificación e identificación.

Se mencionaran los algoritmos de una manera informal, principalmente sin el uso de formulas o los seudo códigos. En nuestra opinión las principales características para el reconocimiento de las huellas digitales. Existen una técnica para realizar la verificación de las huellas:

Basada en Detalles: En esta técnica se elaboran mapas con la ubicación relativa de "detalles" sobre la huella, los cuales permiten ubicar con certeza a un usuario. Con este conjunto de puntos, se va a generar 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 minucia 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 minucias 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.

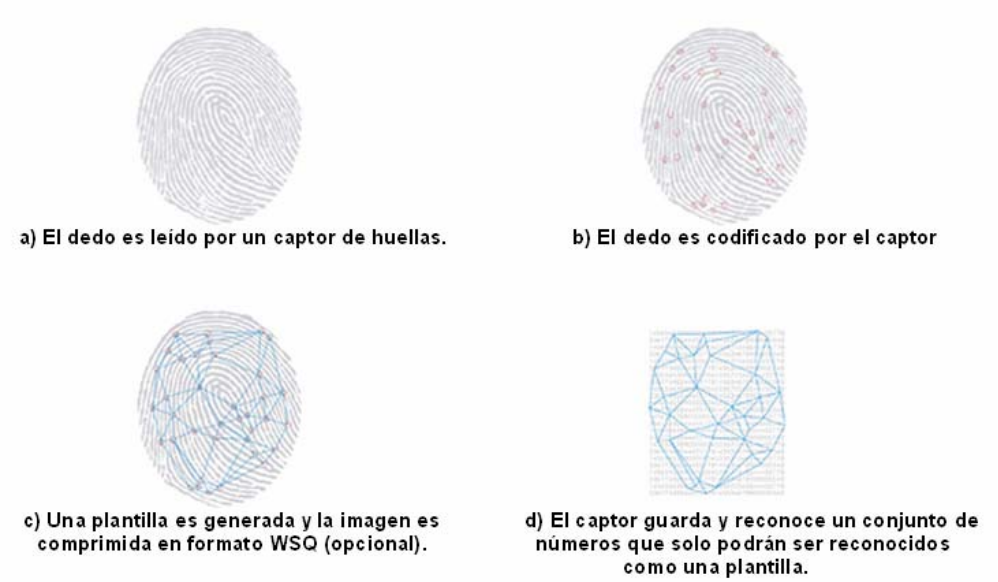


Figura 2.30.-Pasos del análisis de los puntos característicos.

También este método no toma en cuenta el patrón global de las crestas y los surcos. En la figura 2.31 muestra algunos ejemplos de los detalles que pueden ser reconocidos en la imagen de la huella digital.

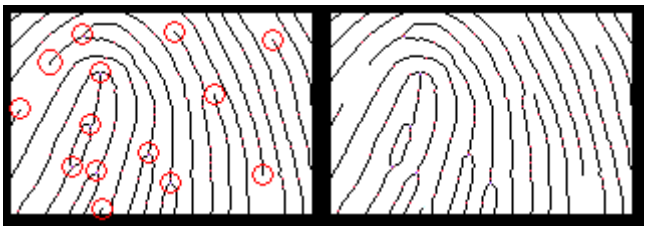


Figura 2.31.- Trazado del patrón de detalles.

El patrón de detalles puede ser descrito por un modelo de probabilidad:

$$P(C) = P(N) * P(M) * P(A) \qquad 2.20$$

Donde:

$P(N) = f$ (Ley de Poisson)

$P(M) = f$ (Frecuencia de aparición del detalle)

$P(A) = f$ (Número de permutaciones posibles de detalles)

Basadas en correlación: Mediante la correlación bidimensional de dos imágenes, es posible detectar si una imagen está presente en la otra y en que posición. De esta forma, puede llevarse a cabo simultáneamente la segmentación del objeto dentro de la imagen y su reconocimiento. Usualmente, el objeto O(x,y)

presente un tamaño menor a la imagen de la escala I(x,y) en la que desea comprobarse la presencia de O.

El cálculo de la correlación puede llevarse a cabo mediante la expresión

$$R_{o\,i}(i,j) = \sum\sum I(x,y)\ O(x-i,y-1), \quad para\ i = 1,.....M \quad j = 1,.....N \qquad 2.21$$

Donde $I(x,y)$ es de MxN pixels y $O(x,y)$ de mxn pixels.

Este método viene a mejorar algunas dificultades presentadas por la aproximación creada por los el patrón de detalles, pero inclusive él mismo presenta sus propias fallas, está técnica requiere de la localización precisa de un punto de registro el cual se ve afectado por la rotación y traslación de la imagen. Se requiere de la posición exacta de los puntos de referencia para así contar las uniones entre cada huella. Cada huella requiere de plantillas que pueden ir de unos cien bytes hasta llegar a unos mil bytes dependiendo del nivel de seguridad que se le es exigido.

Los algoritmos no almacena la huella digital del dedo vivo. En vez, genera una plantilla de 166 dpi basada en esta huella digital para proteger la privacidad de usuarios.

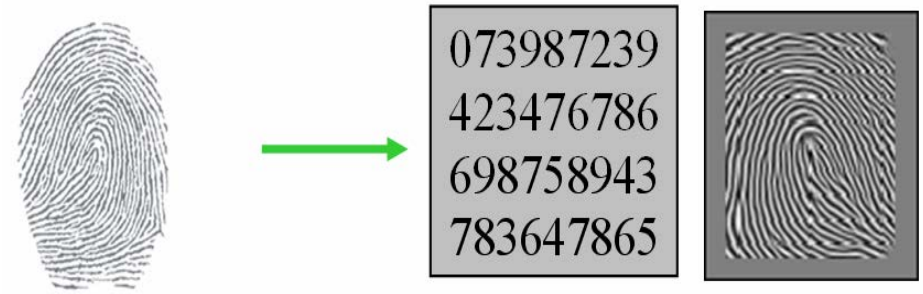


Figura 2.32.a.-Plantillas de una Huella.

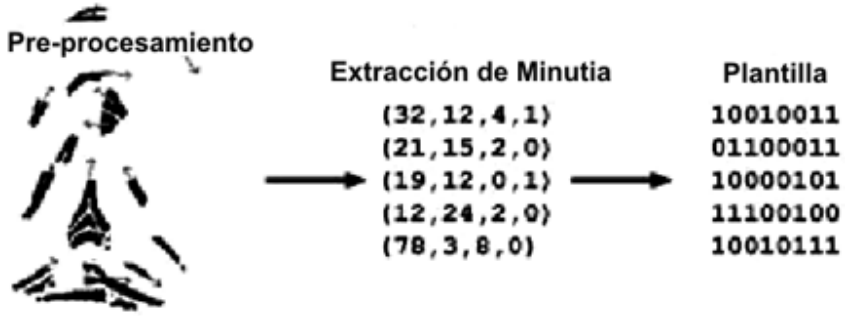


Figura 2.32.b.-Plantillas de una Huella.

Para obtener una coincidencia, el sistema del lector no necesita encontrar el patrón entero de minucias en la muestra y en la imagen almacenada, simplemente debe encontrar un número suficiente de patrones de minucias que ambas imágenes tengan en común. El número exacto varía de acuerdo a la programación del lector. Los siguientes bloques son utilizados para la verificación de huellas dactilares. Todo el diagrama de bloques describe en forma general las

operaciones lógicas necesarias para llevar a cabo la identificación:

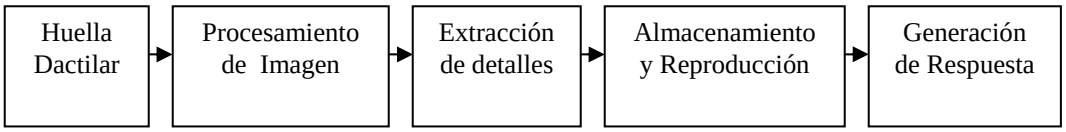


Figura 2.33.- Diagrama de bloques de un sistema reconocimiento de huellas dactilares.

Tal vez el bloque más crítico dentro del sistema propuesto arriba es el de adquisición de muestra. El mismo será mostrado a continuación.

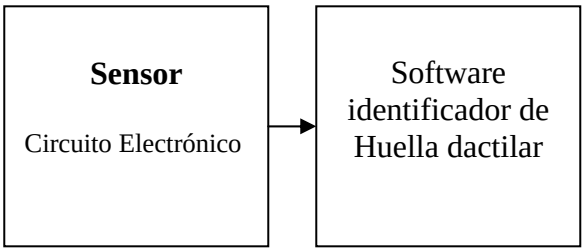


Figura 2.34.- Bloque de un sistema de Huella dactilar.

2.4.5.- Sensores para huellas digitales.

La primera fase en un sistema de reconocimiento de huella digital es la adquisición de la huella. En el pasado la huella dactilar era obtenida por rodillos y un poco de tinta en cada uno de los dedos. Actualmente muchos sensores son capaces de capturar una huella basado en los principios de la óptica, presión, temperatura y capacitancia.

Sensores Ópticos para lectores de huella digital: Un sensor óptico funciona con un dispositivo CCD, como el usado en las cámaras digitales, que tienen un arreglo de diodos sensible a la luz que generan una señal eléctrica en respuesta a fotones de luz. Cada diodo graba un píxel, un pequeño punto que representa la luz que le es reflejada. Colectivamente, la luz y perfiles oscuros forman una imagen de la huella leída. El proceso de lectura comienza cuando usted pone su dedo sobre la ventana del lector, el cual tiene su propia fuente de iluminación, típicamente un arreglo de LEDs, para iluminar las crestas de la huella digital. El CCD genera, de hecho, una imagen invertida del dedo, con áreas más oscuras que representan más luz reflejada (las crestas del dedo) y áreas más claras que representan menos luz reflejada (los valles entre las crestas).

Antes de comparar la información obtenida con la almacenada, el procesador del lector se asegura de que el CCD ha capturado una imagen clara. Checa la oscuridad promedio de los píxeles, o los valores generales en una pequeña muestra, y rechaza la lectura si la imagen general es demasiado oscura o demasiado clara. Si la imagen es rechazada, el lector ajusta el tiempo de exposición para dejar entrar más o menos luz, e intenta leer la huella de nuevo.

Si el nivel de luz es adecuado, el lector revisa la definición de la imagen (que tan precisa es la imagen obtenida). El procesador busca varias líneas rectas que se mueven horizontal y verticalmente sobre la imagen, y si esta tiene buena definición, una línea que corre perpendicular a las crestas será hecha de secciones alternantes de píxeles muy claros y muy oscuros.

Sensores de Capacitancia para lectores de huella digital: Como los lectores ópticos, los lectores capacitivos de huella digital generan una imagen de las crestas y valles que conforman una huella digital, pero en vez de hacerlo con luz, los capacitores utilizan corriente eléctrica.

Las figuras de abajo muestran ejemplos de sensor capacitivo. El sensor está hecho de uno o más chips que contienen un arreglo de pequeñas celdas. Cada celda incluye dos placas conductoras, cubiertas con una capa aislante.

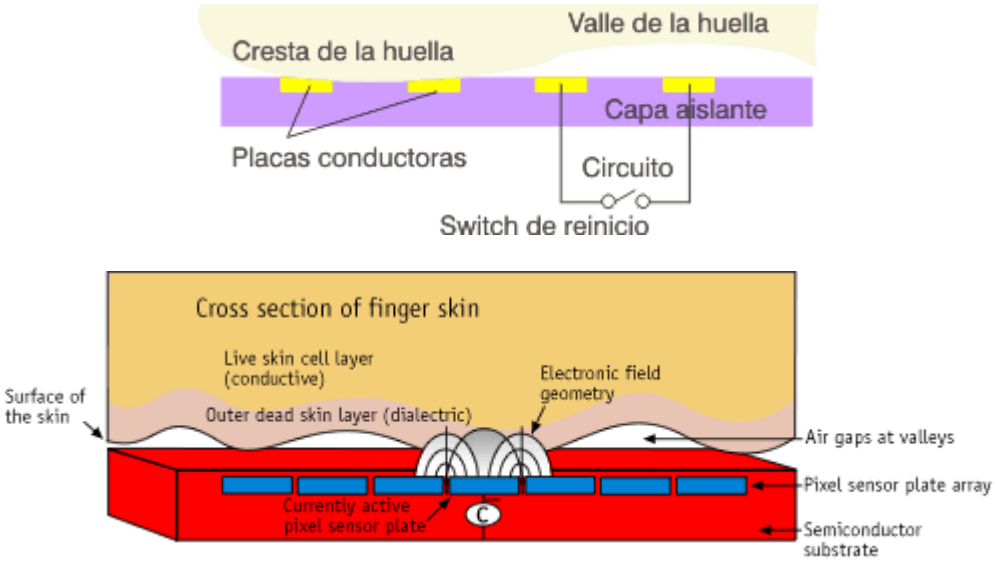


Figura 2.35.- Sensores capacitivos clásico

Las celdas son más pequeñas que el ancho de una cresta del dedo. El sensor es conectado a un integrador, un circuito eléctrico construido sobre la base de un amplificador operacional inversor que altera un flujo de corriente. La alteración se basa en el voltaje relativo de dos fuentes, llamado la terminal inversora y la terminal no-inversora. En este caso, la terminal no-inversora es conectada a tierra, y la terminal inversora es conectada a una fuente de voltaje de referencia y un bucle de retroalimentación que incluye las dos placas conductoras, que funcionan como un capacitor, esto es, un componente que puede almacenar una carga. La superficie del dedo actúa como una tercera placa capacitiva, separada por las capas aislantes en la estructura de la celda y, en el caso de los valles de la huella, una bolsa de aire.

Al variar la distancia entre las placas capacitivas (moviendo el dedo más cerca o más lejos de las placas conductoras), se cambia la capacitancia (o habilidad para almacenar una carga) total de el capacitor. Gracias a esta cualidad, el capacitor en una celda bajo una cresta tendrá una capacitancia más grande que

el capacitor en una celda bajo un valle. Ya que la distancia al dedo altera la capacitancia, la cresta de un dedo resultará en una salida de voltaje diferente a la del valle de un dedo.

El procesador del lector lee esta salida de voltaje y determina si es característico de una cresta o un valle. Al leer cada celda en el arreglo de sensores, el procesador puede construir una imagen de la huella, similar a la imagen capturada por un lector óptico.

La principal ventaja de un sensor capacitivo es que requiere una verdadera forma de huella digital y no sólo un patrón de luz y oscuridad que haga la impresión visual de una huella digital. Esto hace que el sistema sea más difícil de engañar. Adicionalmente, al usar un chip semiconductor en vez de una unidad CCD, los lectores capacitivos tienden a ser más compactos que los ópticos.

Sensor de matriz de antena: Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a perder elasticidad consiguiendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento en los sensores de capacitancia así que un pequeño campo RF es aplicado entre dos capas conductoras, una oculta dentro de un chip de silicio (llamado plano de referencia de la señal de excitación) y la otra localizada por debajo de la piel del dedo. (Ver figura 2.36) El campo formado entre estas capas reproduce la forma de la capa conductora de la piel en la amplitud del campo AC. Diminutos sensores insertados por debajo de la superficie del semiconductor y sobre la capa conductora, miden el contorno del campo. Amplificadores conectados directamente a cada plato sensor convierten estos potenciales a voltajes, representando el patrón de la huella. Estas señales son acondicionadas en una etapa siguiente para luego ser multiplexadas fuera del sensor.

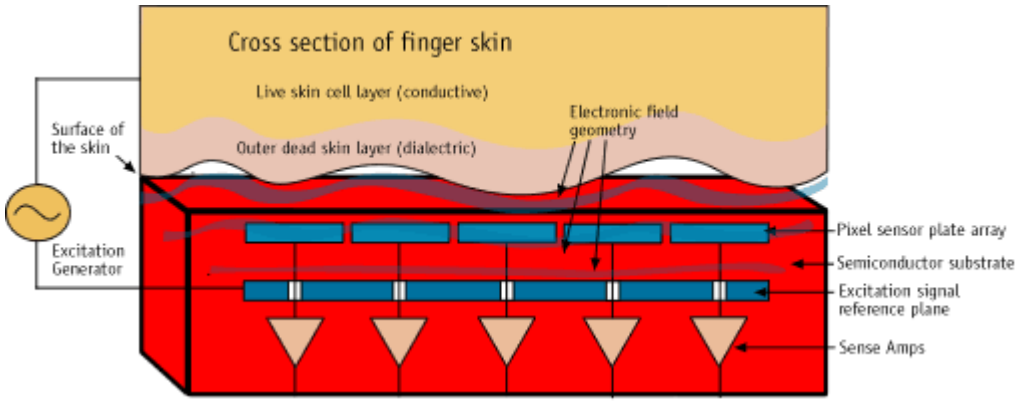


Figura 2.36.- Sensor de Matriz de Antena.

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

Sensores ultrasónicos para huella digital: En este caso el sistema envía un barrido de ondas ultrasónicas (mayores de 20kHz) que rebotan la base de huella. Esta tecnología desarrollada durante la última década para la adquisición digital de huellas dactilares, en la diferencia de impedancias acústicas existentes entre cresta y los valles de la huella, lo que la convierte en una tecnología más resistente que las anteriores, a posibles errores ya que realiza una lectura tridimensional no bidimensional. De forma análoga evitara los posibles errores de lectura producida por presencia de partículas ajenas en la piel o en la platina de escaneo.

Para cada nivel de superficie, las ondas ultrasonoras son reflejadas parcialmente, por tanto, traspasadas también de forma parcial. Esta penetración de las ondas produce señales de retorno en sucesivas profundidades posibilitando de esta forma, la medida de la profundidad del valle presentes entre crestas continuas de la huella. Debemos notar también que en este sistema de adquisición responde a un sistema de captación no invasivo, ya que trabaja con ondas de presión acústica, no magnética. En la figura 2.37 se puede observar la forma típica de un sensor comercial aplicado a sistemas de reconocimiento de huellas dactilares.

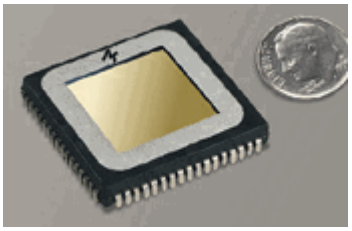


Figura 2.37.- Sensor comercial.

2.5.- Uso de Tarjetas para el control de acceso.

En este apartado se van a dar una visión de las principales alternativas que han ido surgiendo a lo largo del tiempo. De cada una de estas alternativas se dará una descripción sobre la tecnología utilizada, así como su uso y sus ventajas e inconvenientes.

Las tarjetas se pueden dividir en dos grandes grupos: aquellas que incluyen información digitalizada (en una banda magnética, código, chip) y las que solamente tienen información visual. Ambos tipos de tarjeta pueden incluir alguna fotografía del usuario.

Cuando se incluye la información, éstas pueden ser clasificadas en las que son solo para lectura contienen información de la persona que no puede ser alterada una vez que ha sido emitida y las de lectura y escritura contienen datos que además de ser leídos pueden ser actualizados con nueva información, estas últimas son conocidas como tarjetas inteligentes.

El predominio en el uso de bandas magnéticas y código de barras en las tarjetas, que tuvo una de sus primeras aplicaciones comerciales en la década de los ochenta para el transporte público en Londres, enfrenta desde hace algunos

años la competencia de la tecnología de tarjetas inteligentes. En estas, la presencia de un diminuto procesador permite, con un alto grado de seguridad, el almacenamiento de gran cantidad de información.

Es preciso hacer una introducción sobre cual sería el uso que tendría una tarjeta de identificación dentro de un Sistema de Control de Acceso.

2.5.1.-Tarjetas de Código de Barras.

Esta tecnología se introdujo en México a mediados de los ochenta, al igual que en la mayor parte del mundo y casi al mismo tiempo se empezó a utilizar como tecnología para control de acceso físico y control de asistencia, esto debido a que se empezaron a utilizar los números de identificación personal. También se requería por seguridad que este número se encontrara codificado, por estas razones se utilizaron tarjetas impresas con números de identificación personal codificados, mediante una simbología, en un código de barras.

Los códigos de barras son una técnica utilizada para la recolección de datos (tal como la captura manual, el reconocimiento óptico y la cinta magnética), con imágenes o símbolos formados por combinaciones de barras y espacios paralelos, de anchos variables.

Se entiende por símbolo a la visualización física, en otras palabras a la impresión de un código de barras. Mientras que una simbología es la forma en que se codifica la información.

Figura 2.38.- Ejemplo de un código de barras típico.

Los códigos de barras representan un método simple y fácil para codificación de información de texto que puede ser leída por dispositivos ópticos, los cuales envían dicha información a una computadora o microcontrolador.

Existen diferentes simbologías o lenguajes de códigos de barras y cada una tiene sus propias reglas para cada carácter (letra, número puntuación), codificación, impresión y requerimientos de decodificación, chequeo de error y otras características. Las diferentes simbologías difieren en la forma en que representan la información y en el tipo de información que pueden codificar: algunas sólo codifican números, letras y algunos caracteres de puntuación. Otros ofrecen codificación hasta de 128 o 256 caracteres, juegos ASCII. Las simbologías más recientes incluyen opciones para codificar múltiples lenguajes dentro del mismo símbolo; permiten codificación definida del usuario para información especial o adicional y también permiten la reconstrucción de la información si el símbolo se daña.

2.5.1.1.- Estructura y tipos de códigos de barras.

Existen varios tipos de códigos de barras, y esto se debe a que las simbologías están diseñadas para resolver problemas específicos. De acuerdo al tipo de necesidad de identificación interna del negocio, de acuerdo con los requisitos que se deben cumplir para poder comerciar según las normas del mercado, se debe optar por el sistema de codificación mas adecuado. Es decir, existen diferentes simbologías para las diferentes aplicaciones, y cada una de ellas tiene características propias. Las principales características que definen a una simbología de código de barras son las siguientes:

- Numéricas o alfanuméricas
- De longitud fija o de longitud variable
- Discretas o continuas
- Número de anchos de elementos
- Autoverificación
- Quiet Zone (es el área blanca al principio y al final de un símbolo del código de barras)

Cabe hacer mención que el ancho de las barras y los espacios, así como el número de cada uno de éstos varía para cada simbología.

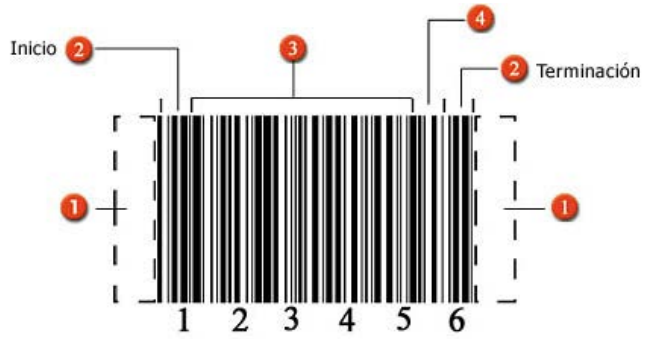


Figura 2.39.- Estructura básica de un código de barras de una dimensión.

1. Quiet zone: Se le llama así a la zona libre de impresión que rodea al código y permite al lector óptico distinguir entre el código y el resto de información contenida la tarjeta de identificación.

2. Caracteres de inicio y terminación: Son marcas predefinidas de barras y espacios específicos para cada simbología. Como su nombre lo indica, marcan el inicio y terminación de un código. En el ejemplo que se muestra son iguales, pero en otras simbologías pueden diferir uno de otro.

3. Caracteres de datos: Contienen los números o letras particulares de la información codificados según cada simbología.

4. Checksum: Es una referencia incluida en el símbolo, cuyo valor es calculado de forma matemática con información de otros caracteres del

mismo código. Se utiliza para ejecutar un chequeo matemático que valida los datos del código de barras. Aunque puede ser importante en cualquier simbología, no son requeridos en todas ellas.

Existen otros códigos utilizados para diferentes aplicaciones, en el caso de los sistemas de control de acceso no existe un código único; y dado que el dato a codificar para estos sistemas es una cadena de números los códigos más utilizados para representar el ID de un usuario son los códigos entrelazado 2 de 5, 3 de 9.

2.5.1.2.- Códigos de barras de dos dimensiones.

Cuando se piensa en la densidad de información, los códigos de barras tienen una aparente debilidad: la dimensión vertical no contiene ninguna información, sino que sólo provee una redundancia que:

a) Habilita la decodificación de códigos parcialmente dañados y
b) Hace posible leer el código donde el usuario no tiene que ser muy cuidadoso acerca de la orientación y los límites registrados.

La idea de utilizar la dimensión vertical dio paso al desarrollo de los códigos de doble dimensión, también conocidos como simbologías apiladas o multirrenglones. Estas nuevas tecnologías crean una matriz de renglones y columnas de datos codificados, entre las cuales tenemos al código PDF417 (Portable Data File), el cual fue propuesto por Symbol Technologies en 1989 y fue liberado en octubre de 1992; éste difiere de los códigos tradicionales en los siguientes aspectos:

a) Permite hilvanar lecturas parciales y por lo tanto ángulos de lectura mayores que esos de otros códigos de una densidad dada. Esto hace posible la lectura sin contacto incluso con lectores tipo CCD.
b) Permite no sólo detectar errores, sino también corregirlos.

Figura 2.40.- Código de barras en dos dimensiones (específicamente se trata de un código PDF417).

2.5.1.3.- Lectura y verificación de un código de barras.

En un sistema de código de barras, el escáner (o lector) es el dispositivo que interpreta la simbología del código de barras. El lector interpreta las barras y los espacios dirigiendo un haz de luz sobre el símbolo de código de barras.

El procedimiento que realiza un lector para leer un código de barras es el siguiente:

1.- El símbolo de código de barras es iluminado por una fuente de luz visible o infrarrojo (ubicada en el lector); las barras oscuras absorben la luz y los espacios en blanco las reflejan nuevamente hacia el lector.

2.-El lector recibe mediante un fototransistor las fluctuaciones de luz y las transforma en impulsos eléctricos.

3.- Un decodificador usa algoritmos matemáticos para traducir los impulsos eléctricos en un código binario y transmite el mensaje decodificado a una terminal manual, PC, o en este caso, en un sistema de control de acceso. El decodificador puede estar integrado al escáner o ser externo al mismo. Los escáneres usan diodos emisores de luz visible o infrarroja (LED), láser de Helio-Neón o diodos láser de estado sólido (visibles o infrarrojos) como emisor del haz luminoso con el fin de leer el símbolo.

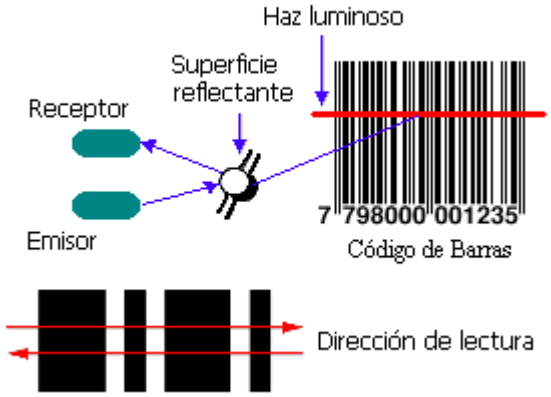


Figura 2.41.- Componentes principales en la lectura de un código de barras.

2.5.2.- Tarjeta de Banda Magnética.

Ampliamente conocidas y utilizadas, las tarjetas de banda magnética tuvo su aparición en los años 50, con lo “moda del plástico “que hizo que se plantease que las tarjetas de identificación pasasen a ser de plástico en lugar de papel o de cartón. Posteriormente surgieron aplicaciones que utilizaban dicha tarjeta de plástico para otros servicios.

La **banda magnética** (llamada a veces *magstripe* como abreviación de *magnetic stripe*) es toda aquella banda oscura que está compuesta por partículas

ferromagnéticas embebidas en una matriz de resina (generalmente epoxi) y que almacenan cierta cantidad de información mediante una codificación determinada que polariza dichas partículas.

La banda magnética de una tarjeta se basa en los mismos principios que una cinta de audio. El medio magnético se compone de diminutas partículas con forma de aguja dispersas sobre un substrato flexible.

En el proceso de fabricación, estas agujas se orientan paralelas a la mayor dimensión de la banda. Al aplicar un campo magnético externo, las agujas se magnetizan de modo permanente. Su dirección varía en función de la polaridad del campo, pudiendo presentarse dos únicos casos N-S o S-N.

El campo magnético es suministrado por un electroimán, cuya polaridad depende de la dirección de la corriente eléctrica. La tarjeta es un simple soporte (normalmente de plástico). Las Tarjetas de Banda Magnética toman su nombre de la banda magnética, con un grosor de 0.5 pulgadas, que presentan. Las dimensiones de estas tarjetas se ajustan al estándar ISO 7810. La posición y propiedades de la banda magnética se describen en el estándar ISO 7811.

La **norma internacional ISO/IEC** define las características físicas de las tarjetas en 3 formatos básicos.

- **CR-80:** Mide 86 x 54mm. (Estándar tarjeta de crédito), con un grosor de 0,76mm.
- **CR-90**: Mide 92 x 60mm. (CNI format).
- **CR-100**: Mide- 95 x 67mm.

La norma **ISO 7810/7811** define las características de la posición de la banda magnética en la tarjeta, la técnica de grabación y encriptado de caracteres.

PISTA1: Contiene 79 caracteres alfanuméricos210 bpi encryption density.
PISTA2: Contiene 40 caracteres numéricos - 75 bpi encryption density.
PISTA3: Contiene 107 caracteres numéricos - 210 bpi encryption density.

Muy recientemente, esta norma ha sufrido una nueva expansión mediante la inclusión de las características de las bandas magnéticas de alta coercitividad (HICO). Estas normas, así como otras dedicadas al entorno financiero.

El estándar 7812 describe como se obtiene el número del cliente que se estampa sobre la tarjeta.

Por su parte, el estándar 7813 describe cual es la información que aparece en cada una de las pistas de la banda magnética.

2.5.2.1.- Estructura de las tarjetas de Banda Magnética.

La primera apreciación importante es que la banda magnética puede situarse tanto en la parte anterior como posterior de la tarjeta. En la banda magnética aparecen tres pistas longitudinales donde se almacena diferentes informaciones.

Estas pistas se nombran como Pista 1, Pista 2 y Pista 3, empezando en la pista más próxima a la periferia de la tarjeta. Cada una de ellas tiene unas

propiedades de grabación y estructura interna diferente, aunque presentan ciertas características en común.

Cuando se almacena información en una pista se graba en primer lugar el bit b1 y el último bit es el bit de paridad del carácter. Al final de cada pista se graba un carácter de LRC, calculado como sigue:

Se toman los caracteres de la pista, sin tener en cuenta el bit de paridad.

Los bits del carácter se eligen de modo que el número de bits a valor 1 en toda la pista, incluyendo el propio carácter, es un número par.

Estructura de la Pista 1: La Pista 1 fue desarrollada por la Internacional Air Transportation Association para su uso en aplicaciones de venta automática de billetes. Las principales características son:

- Densidad de Grabación de 210 bpi.
- Capacidad de 79 caracteres alfanuméricos.

La codificación de los caracteres se ajustan a un código ASCII de 6 bits, más un bit de paridad impar. La información que contiene es la siguiente:

- Un campo para el Número de la Cuenta Principal, con un límite de 18 dígitos.
- Un campo para el Nombre, con un límite de 26 caracteres.

En el resto de los caracteres se almacena información diversa como la fecha de caducidad de la tarjeta o el tipo de la tarjeta.

Esta pista sólo puede ser utilizada para realizar operaciones de lectura.

Estructura de la Pista 2: La Pista 2 fue definida por la American Bankers Association con el fin de permitir transacciones financieras on-line. Las principales características son:

- Densidad de Grabación de 75 bpi.
- Capacidad de 40 caracteres alfanuméricos.

La codificación de los caracteres se ajustan a un código BCD de 4 bits, más un bit de paridad impar. La información que contiene es la siguiente:

- Un campo para el Número de la Cuenta Principal, con un límite de 19 dígitos.
- En el resto de los caracteres se almacena información diversa.
- Esta pista sólo puede ser utilizada para realizar operaciones de lectura.

Estructura de la Pista 3: La Pista 3 se utiliza en la realización de transacciones financieras. Las principales características son:

- Densidad de Grabación de 210 bpi.
- Capacidad de 107 caracteres dígitos.

La codificación de los caracteres se ajustan a un código BCD de 4 bits, más un bit de paridad impar. La información que contiene es la siguiente:

- Un campo para la Versión Codificada del Número de Identificación Personal
- Un campo para el Código del país.
- Un campo para el Límite Autorizado.
- Un campo para el Número de la cuenta asociada.
- Esta pista se utiliza tanto para operaciones de lectura y escritura.

- Además, suele ser reinscrita cada vez que se accede a la información que contiene.

2.5.2.2.- Proceso de Grabación.

Desde el punto de vista técnico, el mecanismo de grabación y lectura de datos es idéntico al utilizado en las grabaciones de música en una cinta o de una película en un video, salvo que aquí se utiliza grabación digital. El principio de funcionamiento radica en la curva de histéresis figura siguiente que presentan los materiales ferromagnéticos.

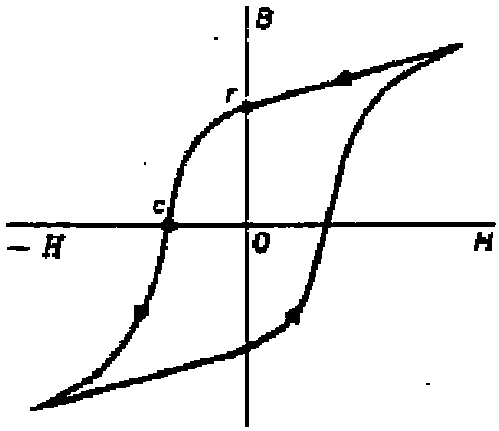


Figura 2.42.- Curva de Histéresis de los materiales ferromagnéticos.

Este curva indica que en un material de este tipo, al inducirse un campo electromagnético en un determinado sentido, se produce una polaridad magnética de un determinado sentido, se produce una polarización magnética de un determinado signo, siendo de signo contrario si el campo inducido es de sentido contrario. Sin embargo, la propiedad realmente interesante de este tipo de materiales es la de que mantienen la polarización aunque se retire el campo inducido, por lo que sirve de dispositivo de almacenamiento. Para cambiar la polarización, hay que inducir un campo electromagnético de mayor intensidad de valor superior a un umbral, el cual se le denomina coercitividad, por lo que si el campo inducido es inferior, la información sigue permaneciendo inalterable. El valor que tiene este umbral, la coercitividad, determina si la tarjeta es de baja coercitividad (LOCO) o de alta coercitividad (HICO), siendo evidente mas estable la información grabada en la tarjeta HICO.

Con este principio, el método de grabación de datos se puede entender fácilmente. El mecanismo se basa en hacer pasar la banda magnética a una determinada velocidad frente a una cabeza grabadora. Esta cabeza grabadora tiene una bobina enrollada a su alrededor por la que se hace pasar una corriente alta, en un sentido si se quiere grabar un 1 y en sentido contrario si se quiere grabar un 0. Esta corriente crea una polarización magnética en aquella zona de la banda en la que tiene influencia la cabeza. Una vez grabados los datos, la banda queda polarizada por fragmentos con determinados signos.

El proceso de lectura se basa en el principio inverso al de grabación. Radica en la propiedad que tienen las variaciones de polaridad magnética de

inducir una corriente en una bobina. Por lo tanto, al hacer pasar la banda magnética por una cabeza de lectura (que tiene otra bobina para la lectura) con una velocidad constante, las transiciones de polaridad de la banda provocarán pulsos de corriente inducidos en la bobina, en uno u otro sentido. Como se tiene la diferencia de tiempo entre un pulso y otro, y se sabe la velocidad a la que circula la banda y la densidad de bits grabados en la banda, se puede determinar fácilmente el número de 1 y 0 que se encuentran entre dos pulsos.

Estructura del Material Magnético: También es posible modificar la estructura del material magnético. La idea básica es la incorporación de ciertos bloques de agujas diminutas cuya polaridad es perpendicular a la polaridad habitual. El proceso de grabación produce un patrón único que permite identificar la tarjeta, y que se fija magnéticamente, de modo que no pueda modificarse, en la Pista 0.

Esta técnica requiere un lector específico que permita interpretar las cuatro pistas.

Figura 2.43.- Lector de Barra Magnética.

Para mejorar la seguridad, la lectura se realiza mediante un sistema de modulación en frecuencia y en amplitud. La última solución comentada es modificar la localización del material magnético. De modo habitual, el material magnético sólo aparece en el espacio reservado a la banda magnética.

Una idea es situar, fuera de la zona reservada a la banda magnética, material magnético de ciertas propiedades. En estas zonas se fija magnéticamente cierta información que permite aumentar el nivel de seguridad. De este modo se reducen la posibilidad de falsificación y alteración de los datos.

Las primeras versiones tenían siete zonas, una en cada uno de los extremos y tres a lo largo del eje longitudinal de la tarjeta Las últimas versiones sólo poseen cinco zonas, una en cada uno de los extremos inferiores y tres a lo largo del eje longitudinal de la tarjeta.

2.5.3.-Tarjetas Ópticas.

Para eliminar una de las grandes barreras que presentaba la tarjeta de banda magnética, la de baja capacidad de almacenamiento surgieron el en mercado diversas alternativas. Una de ellas se baso en el desarrollo de la tecnología de almacenamiento óptico. Los fundamentos de esta tecnología son

conocidos desde los años 30, pero hasta los años 80 no se aplicó. Las tarjetas ópticas son de gran utilidad ya que puede tener una capacidad muy alta o también se pueden utilizar tarjetas ópticas de baja capacidad. Un ejemplo son las tarjetas de teléfono, que se han utilizado en diferentes países como Italia y el Reino Unido. Estas tarjetas poseen una banda similar a las tarjetas de banda magnética en donde se sitúa una superficie magnética. El consumo del crédito de la tarjeta se realiza mediante la aplicación de calor sobre la superficie óptica, en la que produce cierta Marcas cuando se consume el crédito de la tarjeta, aparece una delgada línea de marcas a lo largo de la banda de la tarjeta. Lógicamente, estas tarjetas no se pueden reutilizar ya que resulta imposible restituir la superficie óptica.

2.5.3.1-Estándares Ópticos.

Dado que el desarrollo de esta tecnología es muy reciente, todavía no se ha establecido un estándar definitivo en cualquier caso, los fabricantes utilizan unas tecnologías comunes, que permiten afirmar que sí existen unos estándares, al menos desde un punto de vista comercial. Varios fabricantes de Japón, Europa y Estados Unidos siguen los estándares soportados por el Drexler European Licensees Association (DELA), soporta un grupo con el mismo nombre relacionado con el ANSI, (American Nacional Standards Institute), que desarrolla estándares para tarjetas ópticas.

- ISO también ha desarrollado unas versiones preliminares de los estándares,
- ISO 11693 (Tarjetas de Memoria Óptica).
- ISO 11694 (Tarjetas de Memoria Óptica - Método de Grabado Lineal).

No existe un método de grabación y lectura no estándares, y además no son compatibles.

2.5.3.2.-Lectura y Grabación.

Fundamentos: La tarjeta óptica consta de una superficie magnética y se compone de dos capas, una con un nivel de refracción de la luz muy alto, y la segunda con un nivel muy bajo. Estas capas se superponen y se recubren por un plástico transparente y el conjunto se sitúa sobre un substrato opaco, que forma el Soporte de la Tarjeta.

A continuación se encuentra la capa óptica de grabación, que es donde se va almacenar los datos por el procedimiento que vamos a ver a continuación. Y por ultimo se encuentra el sustrato y una nueva capa protectora.

El medio de identificar un bit como 0 o como 1, es mediante la aparición de nivel diferente de refracción, por la aparición de un agujero o una deformación de la superficie magnética.

En el proceso de escritura, se hace incidir sobre la tarjeta un haz láser de alta potencia solo en el caso de que se quiera escribir un 1 (o si se usa codificación negativa, un 0). Este Haz crea un hoyo en la capa óptica que modifica las características de reflexión de dicha capa en el punto. El hoyo creado,

que tiene un diámetro máximo de 5 micras, se sitúa entre unas guías de 1,4 micras, delimitan la tarjeta en pistas de unas 12 micras cada una.

La lectura se realiza haciendo incidir sobre la lectura un haz de menos potencia y detecta la existencia o no de reflexión (dependiendo si no ha habido hoyo o si lo ha habido respectivamente). El detector dará una secuencia de 1 y 0 que mostrara la información grabada en la tarjeta.

La tecnología óptica se fundamenta en las propiedades de los Diodos Láser (LD), aunque también pueden utilizarse Diodos Emisores de Luz (LED). Las propiedades de la luz láser, Coherencia y Monocromaticidad, permite concentrar la luz en pequeñas regiones la utilización de esta propiedad permite:

- Aumentar la densidad de información.
- Reducir el consumo del grabador.

Lo habitual es utilizar el LD para realizar la grabación de información y los LED para la lectura. El método más comúnmente utilizado es el Grabado Lineal. En este sistema la información se almacena en un formato lineal x-y. Aparecen pistas longitudinales que contienen un vector de agujeros que representan los bits de información normalmente el lector se mueve de modo longitudinal, mientras que el movimiento del cabezal es lateral, el número de pistas varía entre los diferentes fabricantes, aunque los valores habituales suelen ser próximos a 2500 pistas. Para mejorar la precisión en las operaciones de lectura y escritura de información, suele aparecer un formato inicial de la superficie, compuesto por Guías de Pistas. Dichas guías ayudan en el posicionado del cabezal de lectura/ escritura.

La reflectividad de estas guías es diferente de la reflectividad de los dos materiales ópticos. Las pistas también se dividen en sectores, por lo que es necesario grabar las direcciones de éstos cuando se da formato a las pistas un método de formato alternativo define pistas circulares sobre la tarjeta óptica, con el objeto de mejorar la capacidad.

2.5.3.3.-Tarjetas Ópticas Borrables.

En la actualidad existen en el mercado discos ópticos que permiten el borrado y reescritura de información de las diferentes opciones, desde aleaciones cristalino-amorfo reversibles hasta efectos ópticos no lineales, sólo dos tecnologías se han desarrollado.

- Almacenamiento Magneto-Óptico Híbrido.
- Almacenamiento Magneto-Óptico.

Magneto-Óptico Híbrido: Dicha tecnología no es básicamente óptica, sino que utiliza un LED para situar un cabezal magnético en una pista. Estas pistas se definen mediante unas guías de pistas situadas sobre el material magnético de este modo se aumenta la capacidad de un disco de 3.5" a 21 Mbytes, y el lector puede seguir manejando discos tradicionales.

Magneto-Óptico: En este caso, se utilizan las propiedades ópticas del material magnético, y es útil para aumentar la capacidad de dicho material. Se fundamenta en dos fenómenos:

- El Efecto Faraday de la Transmisión de la Luz.
- El Efecto Magneto-Óptico de Kerr de la Reflexión de la Luz.

La mayoría de los fabricantes han utilizado el segundo de los efectos mencionados. Un rayo de luz polarizada puede cambiar su orientación al incidir sobre una superficie magnetizada dichos cambios de orientación se pueden transformar en cambios de intensidad, mediante la utilización de un polarizador.

Los bits se graban como en las bandas magnéticas, pero no de modo longitudinal sino perpendiculares a la superficie magnéticas se desmagnetizan si se alcanza una temperatura superior al Punto de Curie. Al enfriarse su magnetización se relaciona con la del campo magnético externo. Esta propiedad es utilizada en la escritura, calentando la superficie magnética con un LD, e instalando un cabezal magnético que aporta un campo magnético constante.

2.5.4.-Tarjetas Inteligentes.

Básicamente una Tarjeta Inteligente es una tarjeta plástica del tamaño de una tarjeta de crédito convencional, que contiene un pequeño microprocesador, que es capaz de hacer diferentes cálculos, guardar información y manejar programas, que están protegidos a través de mecanismos avanzados de seguridad.

Debemos distinguir entre lo que es una Tarjeta Inteligente y lo que es una Tarjeta Chip. No se trata de lo mismo, ya que el chip no es lo que la hace "Inteligente", si no el microprocesador, por esto existen diferentes tipos de tarjetas, de las cuales, unas son "Inteligentes", y otras son de "memoria".

2.5.4.1.- Clasificación de las tarjetas chip.

Los diferentes tipos de Tarjetas Chip, se distinguen por el tipo de circuito integrado con el que cuente la tarjeta, estas se pueden clasificar en dos categorías:

1. Tarjetas con circuito integrado de memoria.

1.1 De Contacto.

1.2 Sin Contacto.

2. Tarjetas con circuito integrado con microprocesador. (Tarjeta Inteligente)

2.1 De Contacto.

2.2 Sin Contacto.

Estas tarjetas con circuito integrado, pueden contar con aplicaciones financieras, para ser utilizadas como sistemas de pago y/o como tarjetas que contienen información, para accesos o intercambios de información. La complejidad del chip varía de acuerdo con la aplicación o aplicaciones, para lo cual una tarjeta en particular está diseñada.

Existen diferentes tipos de chip, que van desde simples sistemas de memoria, hasta sofisticados sistemas que contienen un microprocesador.

Las tarjetas que contienen microprocesadores pueden ser utilizadas para aplicaciones que requieren altos niveles de seguridad, múltiples aplicaciones y también para aplicaciones de productos emergentes como "Monederos Electrónicos" o tarjetas prepagadas.

Si agrandamos el recuadro dorado para ver en detalle de qué consta, tenemos lo siguiente:

Figura 2.44.- Detalles de los chip en las tarjetas.

Este cuadrado dorado que se encuentra en la tarjeta es el contacto con el Chip. Este cuenta con 8 diferentes puntos de contacto. La forma y distribución de estos puntos de contacto, varía de acuerdo al fabricante, pero de todas formas conservan las mismas funciones. VCC es la fuente de poder del chip. RST es el Reset. CLK (Clock) es el reloj. Los dos puntos RFU (Reserved for Future Use) son puntos reservados para un uso futuro. GND (ground) es la "tierra" del Chip. VPP es el punto donde se encuentra la memoria EEPROM. Por último, I/O es el Input Output del Chip.

Generalmente, el chip se encuentra ubicado debajo de los contactos, y está conectado a estos a través de alambres a los diferentes puntos de contacto. El chip de memoria contendrá solamente memoria, pero el que cuenta con microprocesador, contará con Random Acces Memory (RAM) o memoria de acceso aleatorio, Read Only Memory (ROM) y memoria no volátil o solo lectura.

Las Tarjetas Inteligentes Sin Contacto, tienen un Chip con las mismas características de las que son de Contacto, pero este se encuentra conectado a una antena y se encuentra en la parte interior de la tarjeta.

Las aplicaciones de las tarjetas inteligentes cubren un amplio rango de usos y en ellas se podría registrar desde el ADN de una persona, hasta sus huellas digitales, la historia médica, información financiera, estatus legal, migratorio y judicial, entre muchos otros datos posibles.

Como mecanismo de control de acceso las tarjetas inteligentes hacen que los datos personales y de negocios solo sean accesibles a los usuarios apropiados, esta tarjeta asegura la portabilidad, seguridad y la confiabilidad en los datos. La incorporación de un circuito integrado ofrece varios elementos nuevos que pueden favorecer su utilización generalizada:

a) Miniaturización:

Las densidades de integración de controladores y memorias que se alcanzan en la actualidad, permiten ofrecer un nuevo abanico de posibilidades y de funciones, lo que origina su expansión en el mercado y un nuevo medio de intercambio de información.

b) Lógica programable:

La tarjeta inteligente incorpora la potencia de los ordenadores, incluyendo las funciones lógicas y de control que se aplican a los negocios, junto con funciones avanzadas de seguridad y nuevas aplicaciones.
Interfaz directa en sistemas de comunicación

Las comunicaciones están en crecimiento constante. Cada nuevo avance ofrece un nuevo campo en el que puede aplicarse las tarjetas inteligentes. Las especificaciones físicas, eléctricas, el formato de los comandos y todo lo relacionado con tarjetas se especifica en la norma ISO 7816

2.5.4.2.- Características de las tarjetas inteligentes.

Las más importantes son:

- Inteligencia: Es capaz de almacenar cualquier tipo de información, además es autónoma en la toma de decisiones al momento de realizar transacciones.
- Utiliza clave de acceso o PIN: Para poder utilizarse es necesario digitar un numero de identificación personal, es posible además incorporar tecnología mas avanzada como identificación por técnica biométrica, huella digital o lectura de retina.
- Actualización de cupos: Después de agotado el cupo total de la tarjeta inteligente es posible volver a cargar un nuevo cupo.

2.5.4.3.- Configuración y estructura de tarjetas inteligentes.

Las tarjetas inteligentes (smartcards) son similares a las de los bancos pero que llevan un chip integrado donde se almacena el certificado de forma segura (ISO 7816)*. Existen las que además incorporan un microprocesador con una memoria de hasta 4KB (ISO 7816/ISO 14443) que le permite una serie de tareas como:

- Almacenar.
- Encriptar información.
- Leer y escribir datos.

Una tarjeta inteligente contiene un microprocesador de 8 Bytes con su CPU, su RAM y su ROM, su forma de almacenamiento puede ser EPROM o EEPROM, el programa ROM consta de un sistema operativo que maneja la asignación de almacenamiento de la memoria, la protección de accesos y maneja las comunicaciones. El BUS de datos es total mente inaccesible desde afuera del chip de silicio por lo mismo la única manera de comunicar esta totalmente bajo control de sistema operativo y no hay manera de poder introducir comandos falsos o requerimientos inválidos que puedan sorprender las políticas de seguridad.

Las tarjetas inteligentes dependen de tres zonas fundamentales:

- Zona Abierta: Contiene información que no es confidencial. (el nombre del portador y su dirección).
- Zona de Trabajo: Contiene información confidencial. (Aplicaciones bancarias: cupo de crédito disponible, el número de transacciones permitidas en un periodo de tiempo).
- Zonas Secretas: La información es totalmente confidencial. El contenido de estas zonas no es totalmente disponible para el portador de la tarjeta, ni tiene por que conocerla la entidad que la emite ni quien la fabrica.

Un ejemplo que permitirá explicar la configuración de las diferentes tipos de tarjetas de almacenamiento es la tarjeta 2k/2. El término 2k/2 nos indica la capacidad de almacenamiento y como esta distribuida la información de las memorias. Para explicar los términos anteriores utilizaremos la tarjeta de 2k bits/2 la cual los términos “2K bits” nos indica que tiene una capacidad de (256 Bytes , 32 Bloques de memoria) y la parte de “/2” esta nos indica que la tarjeta esta dividida en una página con dos áreas de aplicación.

Toda la información se puede encontrar en tarjetas de 2k bits/2, 16 k bits/2 ,16k/16 de capacidad de almacenamiento.

La primera área es de los Bloques [6 – 18].
Los Bloques [6 – 18] son aplicados para la identificación del usuario.

La segunda área es de los bloque [19 – 31].
Los Bloques [19 – 31] son utilizados para guardar alguna otra información de interés de los usuarios.

Los Bloques [0 – 5] son dedicados a la información de los fabricantes.
Los primeros cinco Bloques pueden tener la siguiente información:

Bloque 0 Número de serie de la tarjeta y número que la identifica.
Bloque 1 Configuración de la tarjeta y los algoritmos de identificación.
Bloque 2 Guarda los valores de seguridad
Bloque 3 Contiene la primera llave o contraseña
Bloque 4 Contiene la segunda llave o contraseña
Bloque 5 No es muy comúnmente usada pero se puede guardar alguna información del fabricante

Los otros tipos de tarjetas también indican su capacidad de almacenamiento con sus respectivas áreas de trabajo.

Una llave (site code o facility code) es una contraseña que puede proteger la información de la tarjeta que puede ser leída o cambiada. Las llaves no se pueden modificar una vez que fueron colocadas estas llaves son para evitar la falsificación de esa tarjeta en particular y para tener la confianza de que estas tarjetas no puedan ser utilizadas en otros lectores del mismo proveedor. Se encuentran una variedad de llaves que protegen cada una de las áreas de aplicaciones en las tarjetas.

2.5.4.4.- Funcionamiento de las tarjetas inteligentes.

Las tarjetas se activan al introducirlas en un lector de tarjetas. Un contacto metálico, o incluso una lectura láser, como en un CD-ROM, permite la transferencia de información entre el lector y la tarjeta, actualmente comienzan a existir casas comerciales cuyos productos permiten leer una tarjeta inteligente desde el propio ordenador personal.

Las comunicaciones de las tarjetas inteligentes se rigen por el estándar ISO 7816/3, la tasa de transferencia de datos es de 9600 baudios en modo asincrónico. Las tarjetas y los lectores contienen complicados algoritmos encriptados que pueden distorsionar la información enviada de tal forma que sea poco inteligible e impedir la obtención de los algoritmos y los números aleatorios de cada tarjeta. Además si el lector estuvo leyéndola en varias ocasiones la información transmitida pudo ser diferente en cada una de las ocasiones que fue leída también cada tarjeta contiene un único numero serial o contraseña que es encriptada y guardada en ella y con esto tener un sola contraseña para cada una de las tarjetas.

Los lectores constantemente están emitiendo una señal a una frecuencia de 13.56 MHz y cuando localiza una o varias tarjetas el proceso de identificación comienza mandándole sus encriptados números de identificación. El lector manda señales para conocer si existe una tarjeta cercana.

Figura 2.45.- Lector Buscando una tarjeta.

En la posibilidad de que varias tarjetas estén mandando su número de identificación al mismo tiempo los lectores silencias a todas las tarjetas y solo seleccionan a una e identifican su encriptado número de identificación a este proceso es llamado como anti-colisión.

Figura 2.46.- Identificación mutua.

Cada tarjeta y cada lector contienen:

- NIP contraseña secreta (diversificada con la (numero serial de la tarjeta) en la tarjeta).
- NIP algoritmo de autentificación mutua.
- Generador de números aleatorios.

El primer paso de la seguridad de los sistemas; es que nunca es usado el numero serial de la tarjeta para el control de acceso este número no esta encriptado debido a los estándares de ISO.

Cada tarjeta manda una cadena de 64 bits en la cual contenga el número serial de la tarjeta **(NST)** con un número aleatorio generado por la tarjeta. Después el lector a través del algoritmo Hash 0 diversifica la NST y obtiene la NIP contraseña de la tarjeta, la contraseña calculada por el lector deberá coincidir con la contraseña escrita en la tarjeta.

Figura 2.47.- Validación y transferencia de información.

Lo cual lleva a que el lector y la tarjeta se manden una serie de datos para comprobar que uno y otro sea un equipo que pertenezca al sistema y que puede descifrar la información que se va transmitir y con ello permitir el acceso al usuario.

Después de localizar alguna tarjeta se manden una serie de datos para comprobar que uno y otro sea un equipo que pertenezca al sistema y que puede descifrar la información

Figura 2.48.- Aceptación y desencriptación de la información.

A continuación el diagrama completo del la comunicación entre el lector y la tarjeta

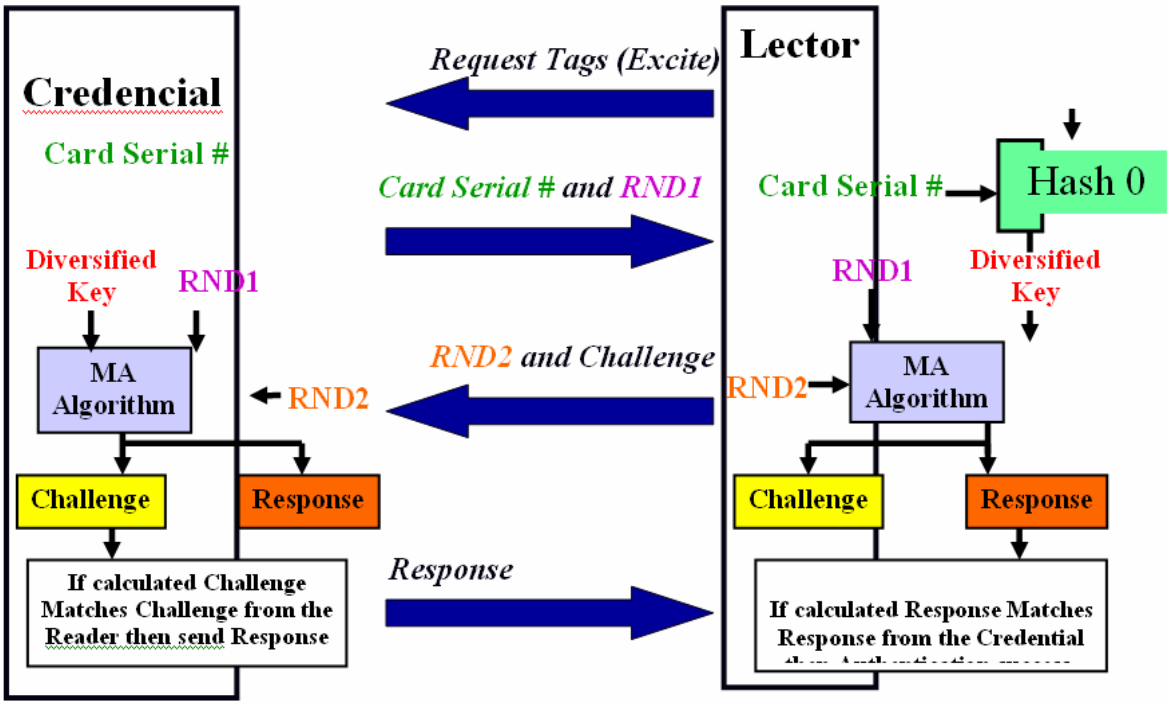


Figura 2.49.- Diagrama de Bloques del proceso de identificación.

2.6.- Protocolo Wiegand.

El término Wiegand es empleado para diversas características relacionadas a lectores y tarjetas de controles de acceso. Desafortunadamente, la palabra es usada sin mucho cuidado y puede llevar a una confusión innecesaria. Para evitar esta confusión definiremos lo que es Wiegand:

1.- Una interfase específica lector - tarjeta
2.- Una interfase específica binaria lector - panel de control
3.- Una señal electrónica de transmisión de datos
4.- El “estándar” binario de formato de la información de una tarjeta de 26 bits.
5.- Un efecto electromagnético
6.- Una tecnología de tarjetas de control de acceso

A principios de 1970 John Wiegand desarrolló una nueva tecnología superior para codificar información binaria en una tarjeta y poder leerla con un lector. Previamente a su invención, la mayoría de las tarjetas usaban banda magnética (usada aún al día de hoy) o un parche embebido de bario-ferrita (obsoleto) para contener un número binario de identificación en una tarjeta. Ambas tecnologías sufrieron de lectores y tarjetas que se gastaban considerablemente en su uso, y de la relativa facilidad de poder decodificar la información. La tecnología desarrollada por Wiegand mejoró radicalmente la fiabilidad y el período de vida del lector y la tarjeta. Además presentó las bases de lo que serían las tarjetas de proximidad y las tarjetas inteligentes.

En nuestros días se sigue utilizando esta tecnología, en especial el estándar de 26 bits en los sistemas de control de acceso. Este formato establece principalmente la forma en que deben ser codificados los datos leídos por un lector para poder ser transmitidos a un panel de control, el cual utilizando las reglas establecidas en el estándar 26 y consiste en decodificar la información y extraer el número de la tarjeta (el cual es el número de identificación del usuario) y en base a los procesos vistos anterior mente figura 2.49. garantizar que el acceso se otorgue o no.

El formato Wiegand 26 es un formato abierto, lo que ha permitido que diferentes desarrolladores y fabricantes de sistemas de control de acceso, de lectores y de tarjetas ofrezcan al público soluciones en controles de acceso que sean compatibles con soluciones de sus competidores. Por ejemplo, se puede utilizar un lector de un fabricante con el panel de control de otro fabricante sin temor a que estos sean incompatibles, siempre y cuando ambos soporten el formato. De hecho, hoy en día, esta tecnología no se ha vuelto exclusiva de las tarjetas y lectores de tarjetas de control de acceso, una gran mayoría de fabricantes y diseñadores han modificado sus productos para hacerlos compatibles con este formato, como ejemplo, algunos lectores biométricos cuentan ya con este tipo de formato para transmisión de datos.

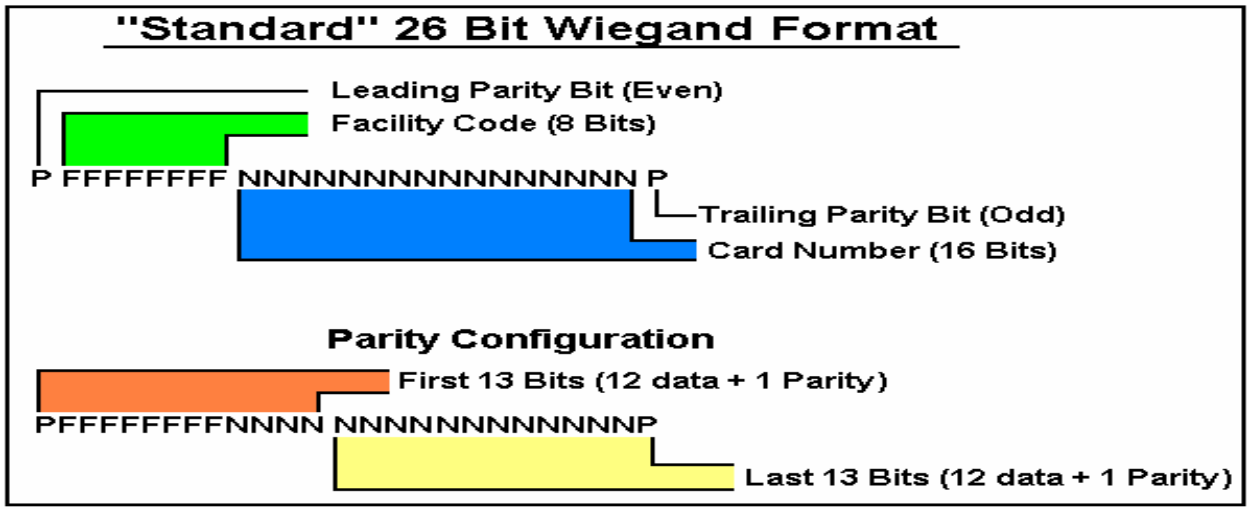


Figura 2.50.- Estructura del formato estándar Wiegand de 26 bit

La Figura 2.50 muestra la estructura delformato Wiegand 26 bit. El facility code (también llamado site code) es un número único de 8 bits puesto por el fabricante con fines de seguridad y para mostrar su funcionamiento lo ilustraremos con un ejemplo:

Supongamos que la Delegación B de la Ciudad de México tiene un sistema de control de accesos en sus oficinas y utiliza lectores y tarjetas de la compañía A; por otro lado, una segunda compañía C de México cuenta también con un sistema de control de acceso con lectores y tarjetas de la compañía A. Un usuario de la compañía C tiene una tarjeta con el número 23 y tiene permitido entrar a todas las zonas restringidas por el control de acceso y en la Delegación B un usuario tiene también una tarjeta con el número 23. Eso quiere decir que si el usuario de la Delegación B quisiera acceder a las instalaciones de la compañía C podría hacerlo, porque su número de tarjeta coincide con el número de la tarjeta de un usuario de la compañía C y ambas tarjetas son del mismo fabricante.

En realidad esto no sería posible gracias al facility code, porque cuando ambas empresas compraron sus tarjetas a la compañía A, la compañía A colocó un número único a cada una de las tarjetas de ambas empresas. En el caso de la Delegación B se tiene por ejemplo el número 123 como facility code, mientras que la compañía C de México tiene el número 55 como facility code. La mayor parte de los paneles de control de acceso compatibles con Wiegand 26 comparan primero que el facility code de la cadena de bits que le es enviada por el lector sea el mismo número del facility code que se configuró para ese sistema; si el número es el mismo entonces siguen con el proceso, si no lo es, el proceso termina y en la mayoría de los sistemas se guarda un registro en la base de datos y/o se hace la advertencia de que el facility code o el site code es incorrecto. Sin embargo no todos los paneles de control de acceso toman en cuenta el facility code, por lo que se debe tener cuidado.

El card number es el número de identificación (ID) que se ha asignado al portador de la tarjeta, en la mayoría de los casos este número lo codifica también

el fabricante o puede ser escrito (a través de un medio electrónico o magnético, dependiendo de la tecnología) a la tarjeta por el administrador del sistema de control de acceso. Este número se encuentra directamente relacionado al número de usuarios del sistema, por lo que se pueden tener hasta 65535 tarjetas y usuarios.

Los bits de paridad son usados como un método simple para verificar la precisión de la información transmitida entre el lector y el panel de control. En este formato, los primeros 13 bits deben contener un número par de 1´s y los últimos 13 bits deben contener un número impar de 1´s. De manera que si los primeros 12 bits de datos resultan en un número impar, el primer bit de paridad se pone a 1; de igual manera el segundo bit de paridad se pone a 1 o a 0 para obtener como resultado que los últimos 13 bits contengan un número impar de 1´s. Hay que hacer la aclaración de que algunos paneles de control de acceso verifican la paridad de la cadena de bits que les llega y algunos otros no.


CAPITULO 3
ANÁLISIS Y DISEÑO DEL CONTROL DE ACCESO

3.- Análisis y diseño del control de acceso.

3.1.- Introducción.

Uno de los errores más comunes en ventas, es cuando se empieza a ofrecer un producto, sin haber siquiera averiguado previamente las necesidades del solicitante. En la actualidad, donde el servicio juega un papel preponderante, es imposible instalar un sistema sin conocer la necesidad concreta del cliente, por lo que es necesario que el cliente nos haga saber cuáles son sus requerimientos y necesidades concretas.

Diversas técnicas pueden ser aplicadas para conseguir este objetivo, pero no hay que descuidar que el objetivo es la definición exacta de las necesidades del cliente, porque si logramos satisfacerlas de la manera más cercana a la realidad que el cliente espera, mucho mejor será el resultado de nuestra gestión, para que le podamos seguir proveyendo otras soluciones.

Para este trabajo se nos solicitó realizar un estudio en una empresa ubicada en la Ciudad de México para implementar en un futuro cercano un sistema de control de acceso que cumpla con las necesidades de seguridad requeridas en sus oficinas (omitiremos el nombre de la empresa por razones de información confidencial).

3.2.- Definición del producto.

Es bastante común que se pida un "Control de Acceso" como una solución genérica, pero de manera involuntaria y por falta de información y conocimiento, se puede estar mezclando conceptos y en realidad se necesita de otra solución que puede ser un Control de Asistencia del Personal, un Control de Visitas, un Control de intrusión, un Circuito Cerrado de Televisión (CCTV), o bien se trate realmente un Sistema de Control de Accesos propiamente dicho; esto es lo primero que se debe definir en conjunto con el cliente.

Si bien no vamos a profundizar demasiado en este tema dado que ya tratamos a detalle las tecnologías utilizadas para el control de acceso, para este caso, partimos de la base que a la que nos estamos refiriendo a un requerimiento específico de un Sistema de Control de Acceso o a un Abre Puertas Inteligente.

Dentro de lo que denominamos "Control de Acceso" podemos encontrar dos grandes divisiones: "Control de Visitas" y "Control de Acceso de Personal". Si bien puede ser bastante clara la función de cada uno, podemos sintetizar diciendo que el primero, se refiere a todos los controles que se hacen en una empresa o establecimiento de los ingresos y egresos de personas ajenas (visitantes) a la empresa y el segundo del personal que labora en la compañía. Estas soluciones pueden ser independientes o en algunos casos se pueden combinar ambos sistemas. De igual manera puede integrarse un Control de Intrusos o un CCTV en la solución completa.

Sobre este tema específicamente, nos vamos extender en las siguientes páginas, no obstante haremos un breve resumen de las distintas opciones más utilizadas en el mercado actual. Este es el punto, quizás, más importante, porque en realidad define la característica "visible" de todo el equipo instalado, que estará en función del perfil del los usuarios, del ambiente de trabajo, de la logística de la empresa, de las necesidades del cliente y del presupuesto asignado al proyecto.

3.3.- Datos generales de la empresa.

Es una compañía regiomontana que tiene oficinas en Monterrey Nuevo León y en la ciudad de México; además de tener presencia en toda la República Mexicana a través de distribuidores y socios de negocios.

Tiene varias líneas de negocio que trabajan en conjunto para ofrecer soluciones en informática y tecnología a diversas empresas para facilitar sus procesos administrativos y operativos.

Las líneas de negocio o sus divisiones son:

- Sistemas de control de acceso (que se encarga de las soluciones tecnológicas y de hardware en general)
- Servicios (que se encarga de las soluciones informáticas)
- Networking (que se encarga de las soluciones en comunicaciones y redes)

Sus oficinas en la Ciudad de México se encuentran ubicadas en la Col. Ciudad de los Deportes en la figura 3.1 se muestra un plano de las oficinas de la D.S.C.A (División de Sistemas de Control de Acceso), donde será instalado el sistema de control de acceso.

Esta división al igual que la empresa está en continuo crecimiento y busca innovar y conseguir la mejor tecnología para ofrecerla a sus clientes, entre los cuales se encuentran: AVON Cosmetics, Grupo Pepsico Internacional, BACHOCO, entre otros.

La D.S.C.A. desea implementar un control de acceso en sus oficinas y en parte del edificio principal de la compañía persiguiendo tres motivos principales:

1.- Proteger los recursos y activos con los que cuenta la división (equipo electrónico, de cómputo) y sus instalaciones.

2.- Tener un mayor control de sus empleados (esto incluye la asistencia de los mismos y los lugares a los que acceden).

3.- Que el control de acceso funcione como apoyo a la imagen corporativa de la empresa y como una herramienta de ventas y negocio, para clientes potenciales que visiten la compañía o se quieran asesorar acerca del funcionamiento de los sistemas de control de acceso en sus oficinas.

3.3.1.- Presupuesto.

Para la implementación del sistema de control de acceso en las Oficinas de D.S.C.A. la empresa cuenta con el siguiente presupuesto de la empresa:

No. de Partida	Concepto	Centro de Costos	Subtotal (USD)
1	Equipo para control de acceso	D.S.C.A.	$23,000
2	Tarjetas para control de acceso (500)	Empresa	$2,000
3	Cableado, Instalación, Configuración y puesta en marcha del control de acceso	D.S.C.A.	$3,000
		Total Presupuestado	$ 28,000 USD

Tabla 3.1.- Presupuesto para el sistema de control de acceso.

Como se observa en esta tabla, el presupuesto total con el que cuenta la empresa para la implementación y puesta en marcha del sistema de control de acceso es de $28,000 USD, del cual el 92.85% ($26,000 USD) lo cubre D.S.C.A. mientras que el 7.15% ($2,000 USD) restante lo cubre la empresa.

En base a este presupuesto, en los siguientes subtemas elaboraremos una propuesta económica atractiva de los equipos, consumibles y servicios requeridos para la implementación del sistema de control de acceso. La cual no consistirá en presentar las opciones más económicas; si no en presentar las opciones más viables en cuanto a las características técnicas acordes a las necesidades y requerimientos del cliente, buscando además en la medida de lo posible, quedar por debajo del presupuesto establecido. En caso de exceder el presupuesto, se negociará con D.S.C.A. ya que, la empresa se encuentra en disposición de sacar una partida adicional si fuera necesario.

3.4.- Situación actual de los accesos a controlar.

Actualmente en las oficinas de D.S.C.A no se tiene un control de acceso electrónico como tal, sólo se cuenta con un electroimán instalado en la puerta de la bodega marcado en el plano de la figura 3.1 acceso 8. Este electroimán se encuentra conectado a una fuente de 12 V de DC y con un teclado numérico. En la entrada la alimentación del electroimán se corta cuando la contraseña ingresada en el teclado es correcta. Para la salida, la alimentación del electroimán es cortada por medio de un botón.

Para la puerta de entrada a las oficinas generales de D.S.C.A. figura 3.1 acceso 3 se tiene actualmente dos lectores de código de barras y una terminal colectora de datos que utilizaban los empleados para checar su asistencia y para entrar o salir de las oficinas; se cuenta además con un electroimán en la puerta con su propia fuente de alimentación y un relevador conectado a una de las salidas de la terminal colectora que libera el electroimán. Actualmente este acceso ya no se encuentra controlado por la terminal colectora, por lo que se han desconectado los lectores y el electroimán para tener siempre acceso libre para cualquiera.

Tanto la puerta a la oficina de Gerencia General de la D.S.C.A. figura 3.1 acceso 4, la puerta de la oficina de Dirección de Proyectos figura 3.1 acceso 5 y la puerta del Centro de Computo figura3.1 acceso 7 no cuentan con ningún tipo de control actualmente y no están instalados ningún tipo de lector a la entrada ni a la salida, de igual manera la puertas cuentas únicamente con una cerradura convencional. El acceso al comedor figura 3.1 acceso 6 no cuenta con una puerta física ni una cerradura; es un acceso “libre”.

La puerta principal del edificio de la empresa que da a la calle cuenta con una contrachapa eléctrica de AC; un botón ubicado en el área de recepción figura 3.1 acceso 1 se encarga de cortar la alimentación de la contrachapa lo que libera la puerta para entrar o salir; sin embargo actualmente también se cuenta con un guardia de seguridad en la entrada que abre la puerta jalando el pasador de la chapa.

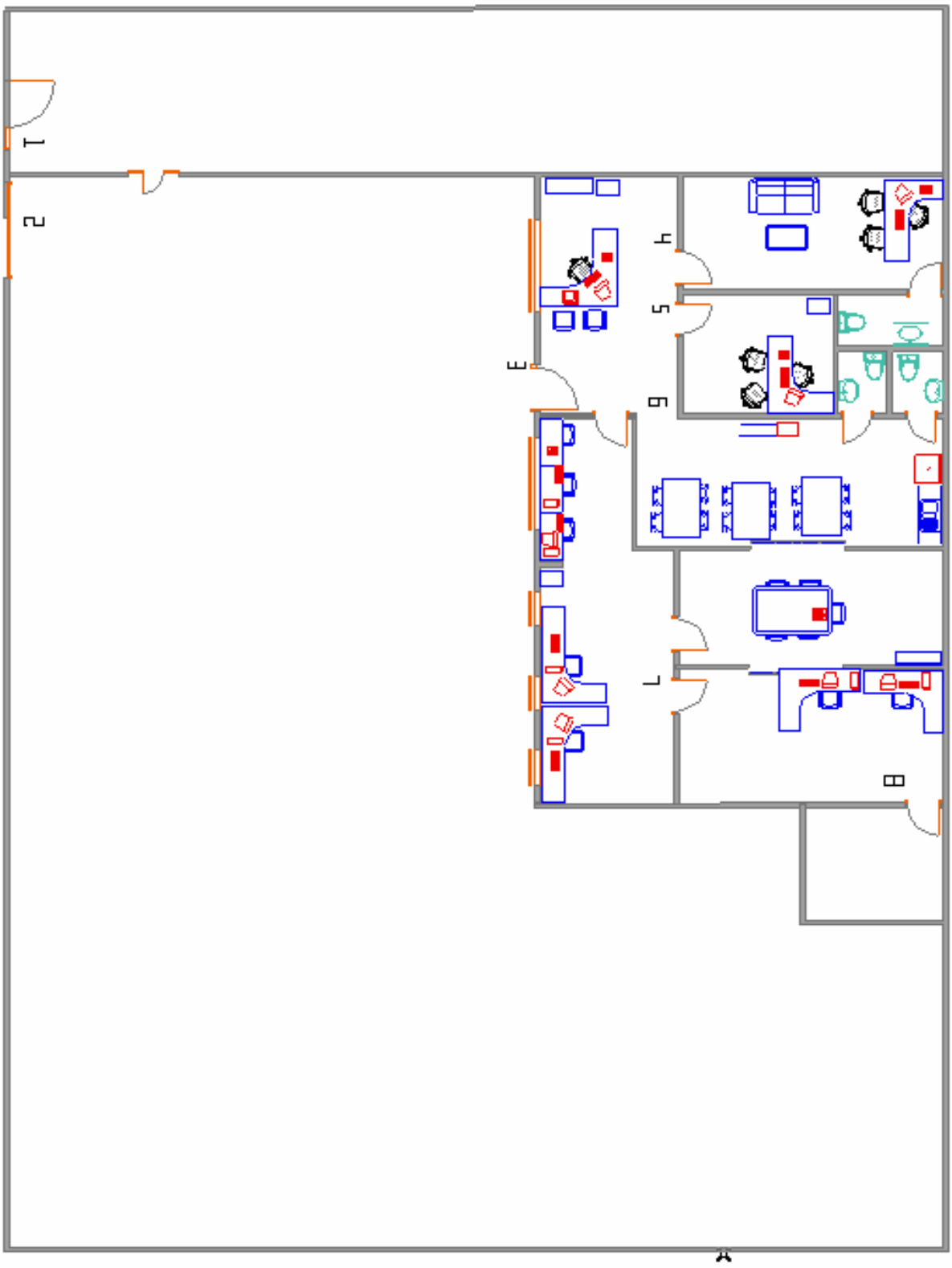


Figura 3.1.- Plano de las oficinas de la D.S.C.A.

El proceso que se sigue para permitir la entrada o salida de un visitante o empleado al edificio principal de Empresa es:

1.- El visitante o empleado toca un timbre ubicado a un lado de la puerta del lado de la calle para que se le abra la puerta.

2.- El guardia una vez que escucha el timbre abre la puerta jalando el pasador de la chapa.

3.- Si el guardia no se encuentra en el área de la puerta principal o no escucha el timbre, la recepcionista presiona el botón bajo su escritorio para cortar la alimentación de la contrachapa.

4.- Cuando un visitante o empleado desea abandonar las instalaciones de Empresa le solicita al guardia que le abra la puerta o en su defecto, él mismo abre la puerta.

El estacionamiento de Empresa figura 3.1 acceso 2 es de uso exclusivo para los empleados y los vehículos de la empresa de todas sus divisiones y para el acceso al mismo se cuenta con un portón eléctrico controlado por un botón. Cuando un vehículo desea entrar o salir del estacionamiento, toca el claxon del automóvil y el mismo guardia que se encarga de la puerta principal, al escuchar el claxon presiona el botón que abre el portón; el automóvil entra o sale del estacionamiento y el guardia anota en una bitácora la hora de entrada y/o salida así como la cantidad de gasolina con la que cuenta el automóvil.

Es por ello, que el objetivo que tiene la empresa es hacerse de un sistema de control de acceso que le brinde la confianza y seguridad para proteger sus recursos y activos, y que el acceso de visitantes, empleados y automóviles no dependa de un control “humano” (el guardia de seguridad), el cual puede ser fácilmente violable o corruptible.

3.5.- Alternativa de solución.

A continuación presentamos una alternativa de solución para controlar cada acceso basado en las necesidades que se requieren cubrir en cada uno de los accesos.

Para el caso de la puerta principal al edificio de Empresa no es recomendable controlar ese acceso principalmente porque es una puerta que da a la calle y aunque es posible montar un lector en la pared externa del edificio, éste lector puede ser atacado por vandalismo; y aunque actualmente existen en el mercado contenedores antivandalismo elaborados de policarbonato que impiden que el lector sea dañado no son muy recomendables y no entran dentro de los estándares de seguridad en edificios (NOTA: mencionar en esta parte los estándares), es por ello que en la propuesta de control de acceso este acceso no estará controlado y el proceso para entrar o salir por la puerta principal seguirá siendo el mismo que mencionamos con anterioridad. Sin embargo serán montados

dos lectores dentro del edificio, uno de entrada y otro de salida que sólo harán la función de relojes checadores; es decir, los empleados checaran su asistencia en ellos y en el sistema se mostrará únicamente la hora de checada, pero no se liberará ningún acceso.

Un acceso muy importante es el de la bodega, porque dentro de ella se almacena equipo electrónico e informático muy valioso que está a la venta, o que se encuentra ya vendido; además de que se guardan herramientas, cables y equipo que utilizan los ingenieros y contratistas para trabajar, los cuales aproximadamente son unos cincuenta.

Este es por tanto uno de los accesos que más desea controlar D.S.C.A., y que el control en este acceso pueda garantizar un nivel de seguridad muy alto, para permitir que únicamente los trabajadores que tienen permitido ese acceso sean los únicos que puedan entrar y salir de la bodega. Por tal motivo proponemos utilizar un medio biométrico para acceder a la bodega, de esta manera garantizamos que sólo el personal permitido pueda entrar a está área (más adelante explicaremos a detalle porque podemos garantizar esto). Además por conveniencia, el lector que proponemos es un lector biométrico que utilice además la misma tecnología que los lectores convencionales que serán instalados en los demás accesos. La salida de este acceso puede realizarse por medio de otro lector biométrico o simplemente con un botón; nosotros sugerimos el botón porque el lector tiene un costo mayor y además no es necesario, porque lo que se desea controlar en realidad es la entrada.

El Centro de Cómputo es un acceso que también se desea controlar, sin embargo la empresa no cree que esta sea una zona de mucho riesgo, de manera que requiera de un control más exigente, como en el caso de la bodega; así que no creemos necesario utilizar lectores biométricos para este acceso, por lo que un lector “convencional” para la entrada será suficiente.

Sin embargo hay que hacer la anotación de que la bodega se encuentra prácticamente dentro del Centro de Computo; esto se debe principalmente al diseño arquitectónico de las oficinas, en donde en un principio el espacio destinado a la bodega fue diseñado como un archivero. Por lo tanto, un empleado que quiera entrar a la bodega tiene que pasar forzosamente por el Centro de Cómputo. Hay que aclarar además que no todos los empleados que tienen permitido el ingreso a la sala tienen también permitido el acceso a la bodega.

El tener un lector a la salida del Centro de Computo nos permite indirectamente controlar la salida de los usuarios que entraron a la bodega, por lo que se ve que en realidad no es necesario utilizar un lector a la salida de ésta.

En el caso del acceso a las oficinas generales de D.S.C.A. planteamos utilizar lectores convencionales a la entrada y a la salida, además de utilizar el electroimán que ya se encuentra instalado en el marco de la puerta para controlar este acceso. Asimismo pensamos colocar un botón debajo de la recepción para que la recepcionista pueda abrir la puerta a los visitantes. Los lectores a la entrada

y la salida servirán además para checar la asistencia exclusivamente a los empleados de D.S.C.A.. Los demás empleados de las otras divisiones checarán asistencia en los lectores de la entrada principal de Empresa.

Para la oficina de Gerencia general y Dirección de proyectos D.S.C.A. desea que se coloque un lector biométrico en la entrada principalmente por motivos de imagen, para cuando sean visitados por clientes. La salida será controlada por un botón ubicado en la pared a un lado de la puerta y se contará con otro botón ubicado cerca del escritorio para que el Gerente o el Director de proyectos puedan abrir desde sus lugares la puerta para los visitantes. Estas oficinas sólo el Gerente general y el Director de proyectos están autorizados para entrar a estas oficinas, además de un guardia de seguridad para que realice su rondín en la noche.

Para el comedor se desea controlar este acceso, debido a que se han presentado robos de los utensilios y cubiertos de la cocina, perpetuados por personal de las otras divisiones de Empresa; de igual manera, esta gente ha hecho mal uso de los hornos de microondas, refrigeradores y cafeteras, al grado de descomponerlos. Por ello para el comedor solo el personal de D.S.C.A. (personal de oficina, ingenieros y contratistas) estarán autorizados para utilizar este acceso.

Lo que proponemos para el caso del comedor es utilizar un lector convencional para la entrada; además, al no existir una puerta física, recomendamos colocar un torniquete de media altura de dos vías, en el cual serán montado el lector de entrada, y para la salida se dejará libre el torniquete. Este torniquete es muy utilizado en otras empresas o fábricas que cuentan con comedores, además de que visualmente es más atractivo.

Sin embargo se presenta una inconveniencia con los sanitarios, ya que al estar en la zona del comedor, una persona que quiera hacer uso de ellos tendrá forzosamente estar autorizado para utilizar el acceso del comedor, lo que deja fuera a los visitantes, pero este problema se puede resolver de manera simple, ya que existe un sanitario para visitantes ubicado en la entrada principal del edificio de Empresa. Además la ubicación física de los sanitarios representa una ventaja más para el control que la empresa desea tener sobre sus empleados, debido a que muchos empleados acostumbran pasar mucho tiempo en los sanitarios, aun cuando ya han hecho uso de ellos. Es por eso, que teniendo el acceso del comedor controlado se puede conocer además, cuánto tiempo pasan los empleados en los sanitarios, lo que permite tomar a la empresa las medidas que crea necesarias, como amonestaciones.

Para el estacionamiento proponemos dejar de utilizar el portón eléctrico, el cual ya es un modelo obsoleto y que presenta fallas eléctricas y mecánicas que impidan que se abra o cierre correctamente después de un uso constante. Sugerimos montar una barrera vehicular electrónica (conocida también como pluma) con un sensor que impida que la barrera baje mientras un automóvil se encuentre debajo de ella. Se colocará además dos lectores convencionales sobre

unos cuellos de ganso, uno para la entrada y otro para la salida, y dado que cada conductor tiene designado un único vehículo, se podrá saber que automóvil ingresa o abandona el estacionamiento de Empresa. Con esto se elimina la actividad innecesaria que realizaba el guardia de abrir o cerrar el portón para que entrara o saliera un automóvil; sin embargo no elimina la actividad que realiza el guardia de anotar el nivel de gasolina de cada automóvil que entra o sale para llevar un control. A pesar de esta inconveniencia, la empresa ha decidido que el guardia no se encuentre más en el área del estacionamiento, así que se dejará de llevar un control de la gasolina y se buscará en un futuro próximo alguna solución automatizada que permita llevar este control. Cabe mencionar que por decisión de la empresa no se removerá el portón eléctrico, el cual aunque no interviene en el control de acceso y que será utilizado para mantener cerrado el estacionamiento de las 23:00 hrs. a las 7:00 hrs. del día siguiente; fuera de este intervalo, el portón estará abierto y el acceso se realizará a través de la barrera vehicular.

Hay que mencionar además que como parte de nuestra propuesta planteamos que todos los accesos a excepción del comedor y del estacionamiento cuenten con sensores de puerta abierta, debido a que la gran mayoría de los sistemas de control de acceso tienen integrados pequeños módulos de control de intrusiones; por lo que al integrar estos sensores al sistema de control de acceso podemos hacer que se dispare una alarma (visual o sonora) cada vez que una puerta sea forzada y abierta.

De igual manera en los accesos antes mencionados se colocarán cierrapuertas neumáticos que se encargarán de cerrar la puerta de cada acceso una vez que ésta se ha abierto, de esta manera, las puertas de todos los accesos estarán cerradas siempre a menos de que sean abiertas por el sistema y una vez abiertas, después de un tiempo se volverán a cerrar. Sin estos cierrapuertas es imposible tener un control de acceso.

Hay que mencionar además que estas puertas contarán con un electroimán, a excepción de la puerta de las oficinas generales de D.S.C.A. que ya cuenta con uno y las cerraduras convencionales serán deshabilitadas a excepción nuevamente de la puerta principal que seguirá teniendo su chapa y contrachapa normal que será cerrada con llave por el guardia en las noches una vez que todo el personal se haya retirado y que será nuevamente abierta en las mañanas a partir de las 7:00 hrs.

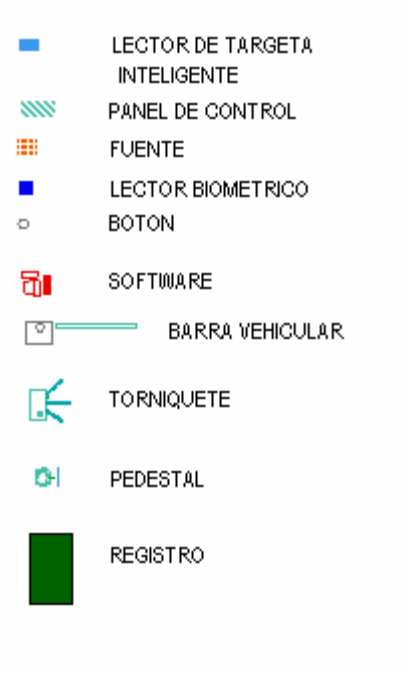
Todas las puertas de estos accesos se encuentran hechas de madera a excepción de la puerta de las oficinas generales de D.S.C.A. la cual es una puerta de vidrio con un marco metálico de aluminio, por lo que consideramos que esta puerta debe contar con un sensor de vidrio roto además del sensor de puerta abierta, dado que el sensor de puerta abierta se coloca en el marco de la puerta y si la puerta se quiebra o rompe, el sensor de puerta abierta no mandaría ninguna señal, porque el marco sigue en la misma posición, en cambio un sensor de vidrio roto al registrar la frecuencia del sonido que ocurre cuando se rompe la puerta manda una señal sistema, que a su vez puede disparar una alarma.

No creemos necesario colocar otro tipo de sensores como sensores de movimiento o sensores de humo porque no son necesarios porque se tiene un guardia de seguridad que esta presente todo el día y que realiza rondines por las noches, además se cuenta con un pequeño sistema de Circuito Cerrado de Televisión (CCTV) con cuatro cámaras instaladas en zonas de alto riesgo.

Este es a groso modo y de manera general la propuesta que presentamos como alternativa para el sistema de control de acceso en Empresa y D.S.C.A.; ahora a continuación mostraremos más a detalle cada elemento del sistema que se va a utilizar, por lo que incluiremos las características físicas, requerimientos, precios, ventajas y desventajas de diversos equipos y marcas para poder elegir el más conveniente para el sistema. Una vez que se ha hecho este análisis y se ha tomado la decisión del equipo que se va a utilizar para cubrir cada componente en del control de acceso, pasaremos a la integración de los componentes al sistema para así por fin tener el diseño del sistema de control de acceso completo que será implementado.

En el siguiente plano se puede mostrar los elementos de que va constar el sistema de control previendo las necesidades de la empresa.

Simbología



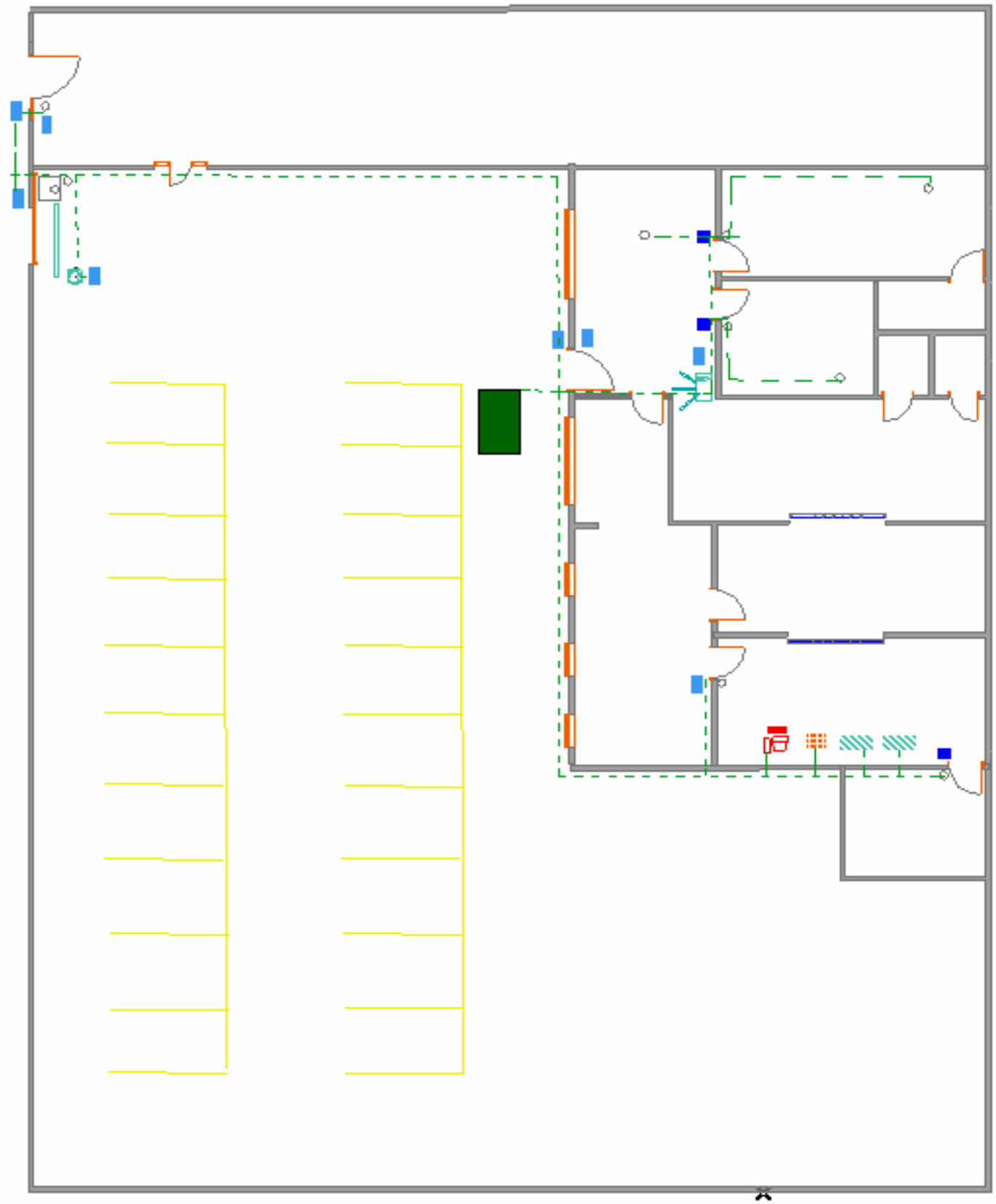


Figura 3.2.- Plano de D.S.C.A. proponiendo los elementos de sistema de control de acceso.

3.6.- Diseño del sistema de control de acceso.

En este apartado del trabajo realizaremos una investigación para mostrar varias opciones de los componentes que requeriremos para el sistema de control de acceso que se encuentran actualmente en el mercado y para cada uno destacaremos las siguientes características:

- Fabricante o proveedor
- Precio
- Características técnicas (eléctricas, mecánicas, físicas, etc.)
- Requerimientos para su instalación
- Ventajas y desventajas

En base a estas características tomaremos una decisión elegir el equipo correspondiente para cada componente del sistema, presentando una opción viable económica y funcional que cumpla las expectativas para cada acceso que se desea controlar y para el sistema en general.

Para facilitar esta tarea dividiremos el estudio en cada componente del sistema de control de acceso que definimos en el capítulo 2, los cuales son:

- Lectores
- Tarjetas (si son requeridas, ya que dependen directamente del lector escogido)
- Panel de control y software de control, monitoreo y reporteo
- Cerraduras y fuentes de alimentación

3.6.1.- Alternativas en el mercado de los sistemas de accesos.

Existen en el mercado diferentes alternativas a cuanto tecnologías de control de acceso, las marcas más importantes para la venta y distribución de ellas son BIOSCRIPT, HID, SECURITRON, KABA, DIGITAL PERSONA, Kimaldi, SYSCOM, IDENTIPASS, Honeywell, PCSC, ROSSLARE BASH, IDENSIS, entre otras y muy diversas empresas que se dedican a la venta de equipos de seguridad y controles de acceso.

Las características del sistema de control a utilizar será un equilibrio entre el precio de los equipos, mantenimiento, soporte, expansión compatibilidad, otro aspecto a tomar en cuenta, es la parte de proveedores de servicio. En el apéndice A mostramos una lista de algunos equipos que son utilizados en el uso de control de acceso, en esta sección mostramos las características de algunas marcas y empresas dedicadas a la venta de estos equipos también mostraremos las características de las lectoras y panel que se utilizara en el sistema de control de acceso mostrando una relación de las principales características y costos de los equipos.

Serie IQ. De PCSC

La serie de Controladores IQ permite el control de acceso y monitoreo de alarma y administración de relevadores externos. También incorpora procesador de 16 Bits, memoria Memory Flash, y circuitos de alarma análogica a digital, ofreciendo máxima eficiencia, confiabilidad y un mínimo de riesgos de violación de seguridad o de falsas alarmas.

Honeywell

La serie Honeywell permite el control de acceso y teniendo ciertas ventajas. Compatible con versiones previas de WINPAK (2.0 / PRO) así como NSTAR, trabaja con paneles NS2 + (NS2 de NSTAR actualizado), N1000 y Pro2200.

Centurión

IDenticard® ha hecho que el control de acceso confiable sea simple y económico para cualquier negocio con la introducción de Centurión, un sistema independiente con capacidad para 2 lectoras. Centurión es ideal para ser usado en aplicaciones pequeñas que requieran control de acceso a 1 o 2 puertas.

Cuando hablamos de los sistemas de Control de Accesos, una parte importante cuando se instala un Sistema de Control de Acceso, todos los equipos están conectados entre sí y se centraliza todo el manejo y supervisión del sistema en una computadora, que tendrá instalado un Software de Gestión, Administración, Control y Supervisión de todos los accesos. Generalmente en estos casos, la información de lo que está sucediendo en cada acceso (es indistinto que sean puertas, molinetes, barreras, etc.), se estará viendo en ese mismo momento en la PC de Gestión, teniendo en cuenta el panel elegido.

Lectoras

Muchos sistemas de Control de Acceso, además de permitir usar uno o dos lectores (no importa con qué tecnología), nos permiten combinar dichas tecnologías para facilitar y adecuar nuestras necesidades. Decimos que este es el punto, quizás, más importante, porque en realidad define la característica “visible” de todo el equipamiento instalado, que estará dada según el perfil del cliente, del ambiente de trabajo y el presupuesto asignado a la obra.

Para el caso de las lectoras las marcas bioscrypt y HID son unas de las más fuertes en el mercado y también son posibles elecciones para este proyecto ya que D.S.C.A. se dedica a vender y promocionar esta conjunto de lectoras.

Las características de los otros equipos requeridos para el control de acceso se muestran en el apéndice A. Lo cual dará una muestra de las posibilidades existentes en el mercado así como una imagen y su costo en el mercado.

3.6.2.- Análisis de lectores convencionales.

En la presentación de la alternativa de solución mencionamos dos tipos de lectores: lectores convencionales y lectores biométricos, sin embargo, hasta el momento no hemos especificado a que tipo de lectores nos referimos cuando hablamos de lectores convencionales y tampoco hacemos mención de que característica biométrica utilizaremos para los lectores biométricos.

Recordemos que habíamos mencionado con anterioridad las tecnologías para los diferentes tipos de lectores que utilizan como medio una tarjeta para brindar el acceso. Dichas tecnologías son:

- Código de barras
- Banda magnética
- Tarjetas de chip (con memoria o circuito integrado) de contacto y sin contacto

Hemos citado sus características principales e incluso algunas ventajas y desventajas para aplicaciones diversas. Pero en esta ocasión haremos un análisis más detallado de cada tecnología y su aplicación a los sistemas de control de acceso con el propósito de elegir la más adecuada para utilizarla como nuestro lector convencional.

3.6.3.- Análisis del lector biométrico.

La biometría permite una verdadera identificación y verificación de los usuarios, ya que esta tecnología se basa en el reconocimiento de un rasgo corporal único, por lo que reconoce a las personas en función de quienes son y no de lo que traen consigo como tarjetas, llaves, credenciales, etc. (que son utilizadas por las tecnologías de código de barras, banda magnética por ejemplo)

También utilizando un medio biométrico para verificar la identidad de un usuario se elimina el uso de claves de acceso o números de identificación (ID), el cual es un problema actualmente porque la gente tiene que recordar varios números y claves en su vida diaria para hacer uso de varios servicios. Como ejemplo podemos mencionar algunos:

- NIP para utilizar cajeros automáticos
- Passwords para acceso lógico a la red y acceso a un servidor de correo electrónico
- ID para control de acceso o para control de asistencia
- Claves para acceso a servicios telefónicos

Esto provoca implica un usuario saturado con tarjetas y múltiples códigos de acceso, que provocan retrasos y molestias al momento que el usuario olvida alguna de sus diferentes claves.

La solución consiste entonces en utilizar un sistema de verificación de identidad, seguro, portátil, fácil de usar, de bajo costo y difícil de copiar.

Como hemos visto con anterioridad las características biométricas son únicas en cada individuo, todo el mundo las tiene y además son difíciles de falsificar. Por lo que utilizar un lector biométrico para la verificación de identidad en zonas de una mayor seguridad se vuelve una excelente opción. No obstante, aún no hemos seleccionado la característica biométrica que vamos a utilizar para la verificación y por ende, aún no hemos seleccionado que tipo de lector y tecnología biométrica se implementará.

En el caso de los lectores biométricos recordemos que las tecnologías más utilizadas y que se encuentran en boga en estos momentos, las cuales son:

- Geometría de la mano
- Firma
- Reconocimiento facial
- Reconocimiento de voz
- Iris
- Huella digital

De estas tecnologías seleccionaremos la más conveniente para utilizarla como nuestro lector biométrico propuesto en la alternativa de solución.

3.6.4.- Selección de la tecnología biométrica a utilizar.

De acuerdo a un estudio que realizó el International Biometric Group (una asociación que agrupa a diversos fabricantes de sistemas de reconocimiento biométrico) en base a los ingresos estimados a finales del 2002 de sus miembros, el uso del reconocimiento a través de la huella digital ocupa el primer lugar de ventas, de lo que se concluye que la tecnología de huella digital domina más de la mitad del mercado de tecnologías biométricas (Figura 3.3). Por lo que actualmente, la identificación por medio de huella digital es la tecnología biométrica más utilizada en diversas aplicaciones.

Por otro lado en un estudio realizado también por la International Biometric Group en el 2002 nos da una perspectiva de las aplicaciones comerciales que se le han dado a las tecnologías biométricas para la verificación de la identidad (en este caso no se hace distinción de ninguna, por el contrario se encuentran agrupadas todas las tecnologías biométricas actuales).

En esta gráfica se observa que la aplicación más común para las tecnologías biométricas es el acceso físico y lógico, en otras palabras, actualmente los sistemas de reconocimiento biométrico son mayormente utilizados en los sistemas de control de acceso en primer lugar y en segundo lugar en los sistemas de acceso lógico a redes, internet, etc. (Figura 3.4).

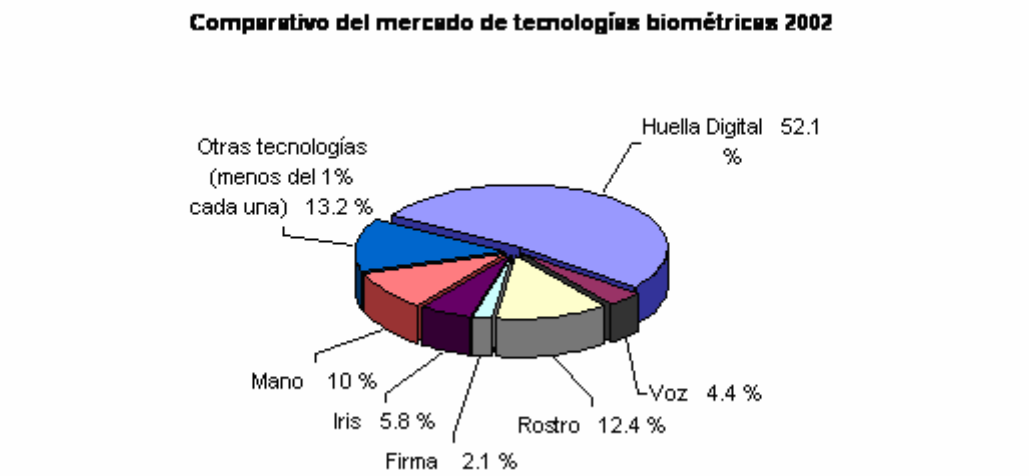


Figura 3.3.- Reporte del mercado de las tecnologías biométricas. Fuente: International Biometric Group.

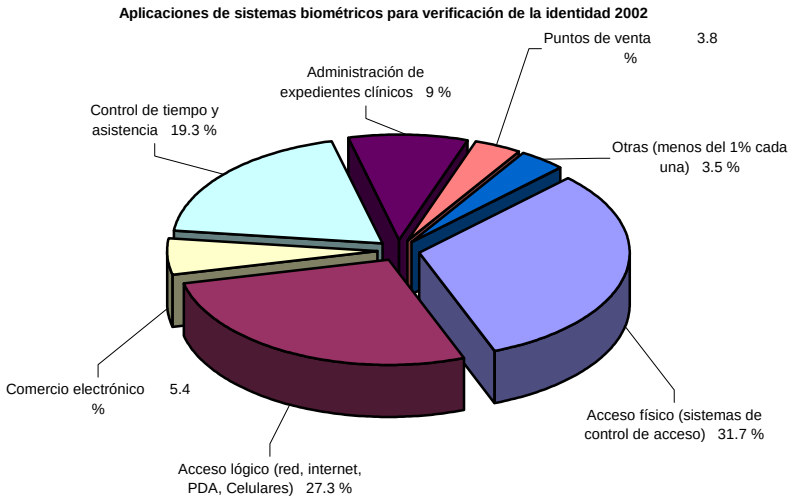


Figura 3.4.- Comparativo de las aplicaciones para sistemas de verificación biométrica. Fuente: International Biometric Group.

Sin embargo, no podemos basarnos únicamente en estadísticas para seleccionar la tecnología biométrica que vamos a utilizar; es necesario tomar en cuenta factores que pueden afectar el rendimiento del sistema biométrico evaluado.

En cuanto a estos factores, podemos distinguir dos grandes grupos, los inherentes al propio dispositivo o la tecnología empleada, y los ajenos al dispositivo y que afectan de una u otra forma a todos los sistemas. Dentro de los del primer grupo se pueden destacar fundamentalmente los factores ambientales, de los cuales podemos ver un resumen en la Tabla 3.2. En cuanto a los ajenos al dispositivo podemos destacar: el tiempo transcurrido entre la inscripción y prueba, y la composición de la población incluida en el estudio (edad, género, origen étnico, capacitación técnica o familiaridad con el sistema, número de usuarios, minusvalías o defectos fisiológicos, etc.). Por lo que el sistema y tecnología biométrica elegida debe ser menos afectada por los factores ambientales y además debe ser capaz de resolver la mayor cantidad de factores ajenos (que

dependen en su mayoría de los usuarios) de la mejor manera para el escenario requerido.

Factores ambientales	Iris	Caras	Huellas digitales Sensor óptico	Huellas digitales Sensor CMOS	Manos	Voz
Luz ambiente	X	X	X		X	
Ruido ambiente						
Temperatura			X	X	X	X
Ruido electromagnético	X	X	X	X	X	X
Humedad ambiental			X	X		
Suciedad y contaminantes	X	X	X	X	X	
Variaciones de voltaje	X	X	X	X	X	X
Golpes y vibraciones	X	X	X	X	X	X

Tabla 3.2.- Factores ambientales relacionados con cada tipo de sistema.

3.6.5.-Tarjetas en los sistemas de identificación biométrica.

En los sistemas de verificación, el usuario debe poder identificarse. Esto lo puede hacer de muchas formas distintas. La forma más sencilla en un principio es la de introducir un código de usuario, que el sistema busque en una base de datos central el patrón de dicho usuario y verifique la muestra obtenida con dicho patrón. Este sistema necesita una comunicación entre cada sitio de verificación y la base de datos, no pudiéndose hacer la verificación si se interrumpe dicha comunicación. En este tipo de sistemas, la tarjeta puede ser utilizada para almacenar el número de identificación del usuario (ID) y así no obligar a que dicho usuario lo tenga que recordar.

Pero los sistemas de verificación pueden ser implementados utilizando una filosofía de Base de datos Distribuida, en la que cada usuario lleve consigo su patrón y, por tanto, no sea necesario realizar comunicaciones con una base de datos central. El usuario, al identificarse, también le ofrece al sistema su patrón biométrico para realizar la verificación. Si bien la infraestructura en este tipo de sistema es mucho más sencilla, se plantea un problema mucho más grave: el patrón biométrico es una información extremadamente sensible, que debe ser altamente protegida. En este tipo de sistemas, la tarjeta podría ser utilizada, no sólo para albergar el código de usuario, sino su propio patrón. Detallaremos las posibilidades para poder realizar esto en una tarjeta inteligente.

3.6.6.- Ventajas e inconvenientes de las tarjetas.

En el capítulo anterior hemos revisado a detalle la tecnología de las tarjetas inteligentes, ahora para el diseño del sistema de control de acceso es necesario precisar su potencial aplicación al campo de los sistemas de identificación

biométrica. Para ello comenzaremos con los inconvenientes, que son fundamentalmente:

- Costo: en este caso nos encontramos con la tecnología más cara en cuanto a tarjetas, aunque sus lectores son más baratos. Pero también hay que tener en cuenta que, salvo en el mercado de la telefonía móvil, no ha habido una implementación masiva de estos productos (especialmente en nuestro país), y por lo tanto el precio de las tarjetas puede bajar sensiblemente.

- Cierto rechazo de los usuarios: el fracaso de anteriores iniciativas basadas en tarjetas inteligentes, tales como el monedero electrónico, puede llevar a muchos usuarios a rechazar inicialmente esta tecnología en otras aplicaciones. Además, el desconocimiento sobre la diferencia entre las tarjetas chip de memoria y las tarjetas inteligentes también lleva a la desconfianza de los usuarios sobre su seguridad, ya que piensan que si las tarjetas de telefonía pública son fáciles de duplicar, clonar o alterar, también lo puede ser su tarjeta de identificación biométrica.

Estos inconvenientes contrastan con las grandes ventajas existentes, que hacen que esta sea la tecnología preferida para los sistemas biométricos y por ende, para los sistemas de control de acceso que involucran sistemas biométricos. Las ventajas de las que hablamos son:

- Capacidad de almacenamiento: es muy superior a la de las bandas magnéticas y, por razones comerciales, superior a la de las tarjetas de memoria. En estos momentos se pueden encontrar tarjetas con más de 16 KB de memoria, se puede aumentar la capacidad si lo demanda el mercado.

- Alta seguridad de la información almacenada: como se ha comentado, la información almacenada se puede proteger por claves o por otros procedimientos de seguridad. Además, dicha protección puede ser distinta dependiendo de la operación (es decir, lectura libre y escritura protegida por una clave, o lectura y escritura protegidas por claves distintas, o incluso prohibir una de las operaciones). Y como la información se puede guardar en distintos archivos, y cada archivo tiene sus propias reglas de acceso, las combinaciones de seguridad pueden ser muy elevadas.
- Alta seguridad en la transmisión de la información: en la mayoría de las tarjetas inteligentes existen algoritmos criptográficos de clave secreta, que permiten codificar la información que fluye hacia y desde la tarjeta. Si además esa codificación.

Los objetivos que se han sido diseñados para esta investigación son:

a) Identificar la cantidad de usuarios que pueden usar cada una de las áreas

b) Registrar la información que puede ser relevante en caso de un incidente de seguridad dentro del la empresa
c) Comparación de la efectividad de nuestro sistema con el sistema anterior.
d) Calidad del servicio
e) Evaluar la aceptación de los usuarios frente a la idea de cambiar de sistema.
f) Este proyecto consiste en instalar la mejor opción en equipo de seguridad considerando los costos y los requerimientos para cada una de las áreas de trabajo.
g) Software El sistema puede ser instalado en cualquier computadora que tenga Windows 98, Me, 2000 o XP. Los controladores o drives pueden variar conforme al sistema operativo que utilice.
h) Hardware**.-** El sistema incluye lectores de huellas digitales, lectores de tarjeta inteligente que permite el registro y la verificación del personal, que deberá ser conectada a la computadora mediante un puerto USB.

La solución del sistema incluye:

- Identificación personalizada de los usuarios
- Creación de una Base de Datos
- Descripción completa de campos de las tablas de la base de datos
- Reportes
- Soporte técnico en instalación y operación para garantizar que el cliente obtenga los resultados esperados
- Control de computadora a distancia
- Posibilidad de abrir cerraduras, torniquetes o barras de estacionamiento

3.6.7.- Elección de la tecnología a utilizar.

Tomando en consideración varios factores entre los que se encuentran las necesidades de la compañía; que desea mostrar las características, diseño, capacidad y ventajas de utilizar los equipos que vende, a los probables clientes y tomando otros factores que son el nivel de seguridad que requiere en cada una de las zonas donde va ha ser instalado el sistema, la compatibilidad de recursos entre los dispositivos, compatibilidad con otros equipos, que se puede integrar al sistema de control de acceso, y con ello se ha tomado la elección de los equipos que utilizaremos en las diversas zonas.

Bioscrypt (Lectores biométricos que utilizaremos).

Tomando en consideración la lista y las características individuales de los diversos equipos de seguridad podemos comenzar con la elección de cada uno de los elementos que utilizaremos en las diversas zonas. Que el sistema de seguridad necesita tener dentro de una determinada condición.

Por las ventajas mostradas en el capítulo anterior se ha elegido como equipos principales, las lectoras con sistema biométrico debido a su alto nivel de seguridad, para los lugares que requieren una mayor restricción de los usuarios y en los lugares que se tienen una mayor libertad o mayor numero de accesos se

ha elegido lectoras de tarjeta inteligente por sus múltiples ventajas (estas ya fueron dichas en capítulos anteriores).

Con lo que se recomienda que en el caso del de las lectoras biométrica tenga la capacidad de leer las tarjetas que serán utilizadas en las los lectoras de tarjeta inteligente y con esta ventaja, que puede leer la tarjeta y la huella los usuarios para tener una mayor confiabilidad y seguridad, que el cliente ha solicitado. Por lo que primera opción se propone la utilización de la lectora V-Station,A,H (iCLASS) ya que cuenta con esta ventajas

- Lector de huella digital con teclado, display LCD, y lector de tarjeta inteligente iCLASS integrado
- Almacenaje de hasta 3550 plantillas de huella digital (usando teclado) o sin límite (usando tarjeta iCLASS)
- Soporta tarjetas de iCLASS de HID de 16kB (2 o 16 áreas de aplicación), y OmniSmart de NexWatch
- Enrolamiento por PC o por teclado
- Soporta Horarios y Diario de Eventos
- Combinaciones de Verificación:

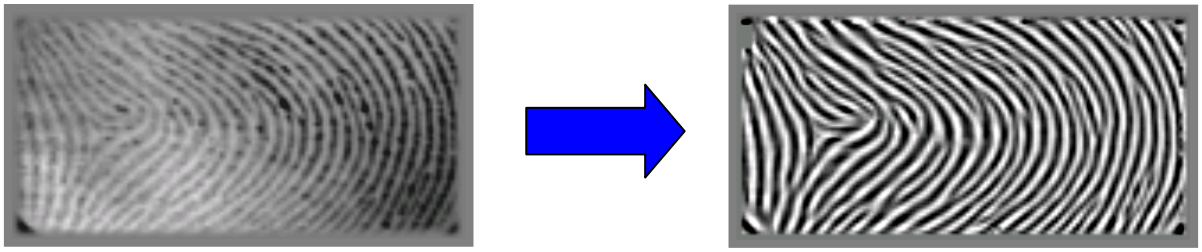
Teclado + Dedo	Tarjeta + Dedo
Teclado Solamente	Tarjeta Solamente
Teclado + Dedo + Password	Tarjeta + Dedo + Password
Teclado + Password	Tarjeta + Password

Niveles de seguridad del lector

Nivel de Seguridad	FRR	FAR
Muy alto	**1/100**	**1/20000**
Alto	**1/200**	**1/5000.**
Medio	**1/1000**	**1/1000**
Bajo	**1/5000.**	**1/200**
Muy bajo	**1/100000**	**1/100**
Ninguno	**0**	**1**
Solo Contraseña	**0**	**1**

Tabla 3.3.- Tabla valores de nivel de seguridad.

- Algoritmo de huella digital de reconocimiento de patrón de canto desarrollado para satisfacer los requisitos del departamento de defensa del E.E.U.U.
- Diseñado para compensar para cicatrices, rasguños, y dedos sucios.



Dedo capturado Plantilla generada

Figura 3.5. Imagen capturada y plantilla generada por un lector de huella bioscrypt

- Realce extenso del imagen: realce de cantos, reducción de ruido, valoración de contenta

Algoritmo de patrón de Canto vs. Minucias.

- Algoritmo de patrón de canto utiliza más área de la huella digital que un algoritmo de minucias (indicado por rectángulo verde contra círculos rojos)
- Algoritmos de minucias utilizan solo una fracción pequeña de la huella digital (indicado por círculos rojos)
- Puntos de minucias cambian con frecuencia con tiempo debido a cicatrices, hinchazón, etc (indicado por círculos azules)

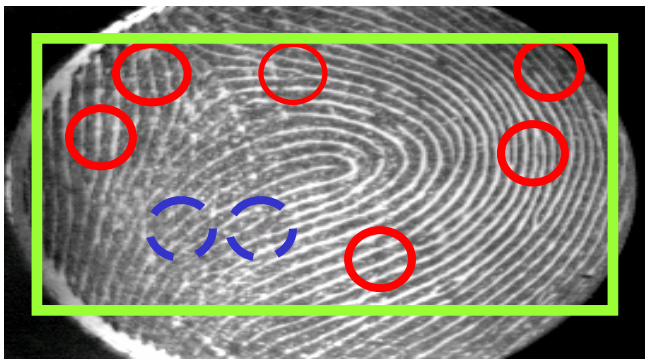


Figura 3.6. Algoritmo de patrón de canto vs minucias

Lectoras IClass (Lectores de tarjeta inteligente que utilizaremos).

En el caso de las lectoras de tarjeta inteligente se tomo como primera opción los productos que ofrecen la marca iclass por su gran versátibilidad y su seguridad incrementada que es llevada acabo por dos factores; la información se encuentra encriptada y una autentificación mutua entre la lectora y la tarjeta. Que impide entre otras cosas que la información o datos sean leída por cualquier otro equipo que no pertenezca al sistema, permitiendo con ello acceso o falsificación del las tarjetas.

Además que el empresa tiene entre su lista de productos estas lectoras entre las más pedidas por sus clientes esto le permite mostrar las ventajas que tiene estas lectoras en sus propias oficinas.

Las lectoras recomendadas son la lectora iclass R10 v1 para el interior de las oficinas y para el estacionamiento se recomienda una lectora para un mayor rango de lectura de proximidad con lo que se pone a prueba a la lectora R40 por las siguientes características.

Para la lectora R10

Credencial	Distancia máx.
iClass Card	7.6 cm
iClass Key	2.5 cm
iClass Tag	2.5 cm
iClass Prox	3.8 cm
MiFARE Card	5.0 cm

Tabla 3.4.- Valores de alcance para la lectora R10.

Para la lectora R40

Credencial	Distancia máx.
iClass Card	11.4 cm
iClass Key	2.5 cm
iClass Tag	2.5 cm
iClass Prox	5.0 cm
MiFARE Card	5.0 cm

Tabla 3.5.- Valores de alcance para la lectora R40.

La distancia de la lectura de la tarjeta es importante por que es la longitud máxima a la que la lectora puede leer las tarjetas.

IDentiPASS (Panel de control que utilizaremos).

Para el panel de control es recomendable utilizar el IDentiPASS debido a que puede controlar de 4 a 8 accesos y la gran mayoría manejan 2; otro buen punto que se debe mencionar es que este panel es mas robusto con lo que permite una integración de un mayor número de elementos que constituyen al sistema de control y cabe mencionar que este panel es uno con los que cuenta la empresa ya que tiene convenios con la empresa que los distribuye.

Características disponibles con el panel IDentiPASS aumentado:

PASSport es un módulo dinámico de cartografía que proporciona un tiempo real comunica con productos de seguridad de terceros.

Mapeo y Control de las puertas. Características que aumentan la seguridad permitiendo a usuarios puedan controlar la posición de puertas de sistema, con o sin lectores.

Registro de Acontecimiento. Se puede seleccionar alguna acción ocurrida dentro del sistema basada en un acontecimiento y registrarla para aumentar la seguridad.

Para los equipos de bloque de zonas como son la barra vehicular y torniquete utilizaremos los que comercializa la empresa Empresa en su división D.S.C.A..

Para el torniquete el modelo TOMSED TUT-60 es E opera en forma electrónica y está diseñado para hacer interfase en forma sencilla con cualquier instrumento de control de accesos. El sistema de control incluye una fuente de voltaje de 24 VDC. El torniquete puede ser: para ingreso controlado, control de ingreso sin salida, salida libre o entrada y salida controladas. Se puede tener cualquier combinación de cerrado o abierto en caso de falla para cualquier requerimiento.

Figura 3.7 Torniquete TOMSED TUT-60 y barrera vehicular Armex.

Para la barrera vehicular el modelo ARMEX que cuenta con un mecanismo motor a reductor por medio de banda con opción a cadena, su tamaño es 105 cm de alto 32 cm de largo y un brazo de 2.7 a 3.5 m y pesa 50 kg. Puede operar en forma electrónica y está diseñado para hacer interfase en forma sencilla con cualquier instrumento de control de accesos y su loop esta colocado en el piso.

IDenticard SYSTEMS

Equipo	Ventajas	Imagen y Costo
IDENTIPASS	Características principales SERIES IDentiPASS . Registro de los acontecimientos ocurridos . Ilimitados grupos de acceso virtuales asignados a un usuario . puerta flexibles y configuración de grupos de puertas . Acontecimientos y registros de los eventos realizados por los usuarios . Capacidad para 64.000 Tarjetas	 $2045 Dls $1650 Dls (tarjeta de expansión para 4 de lectores)

Tabla 3.6.- Equipos de IDentipass para sistemas de control de acceso.

bioscrypt ***Sistema Biométrico con Lectora de Proximidad Integrada.***

Equipo	Ventajas	Imagen y Costo
V-Station. Para instalación en interiores. Este modelo permite a un usuario autentificarse con su número de empleado para colocar posteriormente su huella dactilar, o si se prefiere, puede autentificarse primero con una tarjeta o credencial de proximidad para posteriormente colocar su huella. Es un equipo robusto que puede conectarse a la red de la institución/empresa con un cableado Ethernet pues puede asignársele una dirección IP. Puede contener desde 1 hasta 3,550 plantillas de huella y alojar más de 4,000 eventos. Cuenta con un software de administración Veriadmin incluido que permite el enrolamiento, administración y explotación de datos desde una PC de la red. Produce un archivo de eventos que deberá ser explotado por el cliente para su análisis posterior. Con su tecnología de relevador interconstruida puede activar la apertura de dispositivos de acceso como electroimanes, torniquetes y otros.	Comunicación: Puerto Ethernet, RS232, RS485, Wiegand. Voltaje 9-12V DC Temperatura de operación 0 a 60 grados centígrados .Altura 130 mm .Anchura 118 mm .Profundidad 63.5 mm .Tiempo de enrolamiento menos de 5segundos .Tiempo de verificación entre 1 y 2 segundos .Tamaño de plantilla de huella 350 bytes .Tasas de error Tasa de Falsa Aceptación y de Falso Rechazo iguales: 0.1% Niveles de seguridad: V-Station-A (Base) Múltiple: PIN solo, PIN & Huella, PIN & Huella & Password, PIN & Password V-Station-AP (Proximidad) Múltiple: PIN solo, PIN & Huella, PIN & Huella & Password, PIN & Password. La credencial de proximidad toma el lugar del PIN.	 $1,450.00 Dls.  $2300 Dls

Tabla 3.7.- Lectoras Bioscript para sistemas de control de acceso.

Lectores HID.

<table>
<tr><th>Equipo</th><th>Ventajas</th><th>Imagen y Costo</th></tr>
<tr>
<td>iClass R10.

Ideal para aplicaciones de control de acceso pues combina el mayor rango de lectura de proximidad de 13.56MHz de las credenciales iClass con la tecnología de credencial inteligente.

Lectoras y credenciales requieren llaves que empaten para operar. Toda transmisión entre lectora y credencial es cifrada utilizando un algoritmo seguro.</td>
<td>Frecuencia de transmisión: 13.56MHz

Distancia de lectura

<table>
<tr><th>Credencial</th><th>Distancia máx.</th></tr>
<tr><td>iClass Card</td><td>7.6 cm</td></tr>
<tr><td>iClass Key</td><td>2.5 cm</td></tr>
<tr><td>iClass Tag</td><td>2.5 cm</td></tr>
<tr><td>iClass Prox</td><td>3.8 cm</td></tr>
<tr><td>MiFARE Card</td><td>5.0 cm</td></tr>
</table>
Tamaño: 4.83X10.26X2.03 cm
Alimentación: 10 a16 VCD Corriente: 80mA promedio/300mA pico a 12VDC

Seguridad: Llaves de autentificación de 64 bits.

Instalación Interiores & exteriores
Interfases Wiegand

Temperatura de operación
-35° a 65° C
Humedad de operación
5-95% humedad relativa no condensada
Distancia de cable Wiegand: 150m</td>
<td> 
$250 Dls</td>
</tr>
<tr>
<td>iClass R40

Ideal para aplicaciones de control de acceso pues combina el mayor rango de lectura de proximidad de 13.56MHz de las credenciales iClass con la tecnología de credencial inteligente.

Lectoras y credenciales requieren llaves que empaten para operar. Toda transmisión entre lectora y credencial es cifrada utilizando un algoritmo seguro.</td>
<td>Distancia de lectura

<table>
<tr><th>Credencial</th><th>Distancia máx.</th></tr>
<tr><td>iClass Card</td><td>11.4 cm</td></tr>
<tr><td>iClass Key</td><td>2.5 cm</td></tr>
<tr><td>iClass Tag</td><td>2.5 cm</td></tr>
<tr><td>iClass Prox</td><td>5.0 cm</td></tr>
<tr><td>MiFARE Card</td><td>5.0 cm</td></tr>
</table>
Tamaño: 8.38 X 12.19 X 2.16 cm
Seguridad: Llaves de autentificación de 64 bits.

Instalación Interiores & exteriores

Interfases Wiegand</td>
<td> 
$700 Dls</td>
</tr>
</table>

Tabla 3.8.- Lectoras HID para sistemas de control de acceso.

Tarjetas HID.

<table>
<tr><th>Equipo</th><th>Ventajas</th><th>Imagen y Costo</th></tr>
<tr>
<td>iClass Card.

Credencial de acceso programable con proximidad por radiofrecuencia.</td>
<td>Distancia de lectura

<table>
<tr><th>Lectora</th><th>Distancia máx.</th></tr>
<tr><td>R10</td><td>7.6 cm</td></tr>
<tr><td>R30</td><td>8.9 cm</td></tr>
<tr><td>R40</td><td>11.4 cm</td></tr>
<tr><td>RK40</td><td>10.1 cm</td></tr>
<tr><td>RWK400</td><td>10.1 cm</td></tr>
</table>

.Seguridad: Con técnica de encriptación estándar se reduce el riesgo de credenciales duplicadas. Se pude incrementar la seguridad con encripción DES o triple DES.
Almacenamiento: Múltiples áreas de aplicación separadas, cada una protegida por llaves de lectura/escritura de 64 bits.
.Credenciales de 2Kbit y de 16Kbits (2K bytes)
.Material: Laminado de polivinilo - Polyvinyl chloride
Formato: Soporta hasta 85 bits, para más de 137,000 millones de códigos.
Opciones Banda magnética

Grabado de numeración externa: Slot vertical

Diseño (texto o gráfico)</td>
<td> 

$4.00 Dls</td>
</tr>
</table>

Tabla 3.9.- Tarjeta HID para sistemas de control de acceso.

Con la elección e instalación de estos equipos traerá importantes beneficios dentro de la empresa como es en la imagen de D.S.C.A. así como una herramienta de presentación de lo equipos ante los posibles clientes mostrando los beneficios de estos, su eficiencia, capacidad y desempeño.
También habrá una regulación en los tiempos de entrada y salida del personal y amplio control de los sucesos ocurridos dentro de la división.
Se proyecta recuperar la inversión en 12 a 16 meses. Los próximos objetivos son la instalación de este tipo de sistemas de control de acceso en las otras divisiones de la empresa.


CAPÍTULO
4
IMPLEMENTACIÓN

4.- Implementación.

En esta capitulo vamos a mostrar la parte del costo del proyecto también explicaremos los pasos que se requiere para poder llevar a cabo la implementación de un sistema de control tomando en consideración las instalaciones de los equipos, los plazos y las etapas que llevan cada una de ellas y la vinculación con las pruebas de todo el proceso para garantizar una participación continua y su máximo desempeño. Cotización autorizada, presentada en su momento ante el Director General de D.S.C.A, la cual representa el costo total del proyecto.

Nombre del Cliente: **D.S.C.A**
Atención a: Ing. Juan Carlos Arias

Part.	Cant.	Marca	Modelo	Descripcion de los Equipos	P.U.	SubTotal
1	2	Identicard	Identipass LT	Panel de control para 4 lectores (Incluye Transformador, Batería de respaldo y convertidor serial/ethernet Lantronix UDS 100.	$2,045	$4,090
2	1	Identicard	Identipass-EXP	Tarjeta de expansión de 4 lectores para panel Identipass	$1,650	$1,650
3	6	HID	iClass R10	Lector Wiegand de smartcard (13.56 Mhz) de 7.5 cm. de alcance	$250	$1,500
4	2	HID	iClass R90 (Long Reader)	Lector Wiegand de smartcard (13.56 Mhz) de 45 cm. De alcance	$700	$1,400
5	3	Bioscrypt	V-Smart iClass	Lector biométrico de huella digital con lector smartcard iClass integrado	$1,200	$3,600
6	1	CIDEP	Armex03	Barrera vehicular electrónica con brazo de 3 mts.	$1,850	$1,850
7	1	ERREKA	LOOP-0010	Loop de piso, detector de masa para automovil	$500	$500
8	1	Tomsed	TUT60	Torniquete electrónico de 3 brazos en acero inoxidable	$4,100	$4,100
9	500	HID	iClass Card	Tarjeta inteligente de 2 Kbits de memoria imprimible	$400	$2,000
10	4	POW-R-MAG	PM600PC	Chapa magnética (electroimán) de 6000 lbs. de fuerza. Incluye accesorios para montaje	$154	$616
11	4	Inalarm	INACP01	Cierrapuertas neumático	$30	$120
12	5	Inalarm	Sin modelo	Sensor de puerta abierta blanco(sensor magnético)	$5	$25
13	1	Inalarm	Sin Modelo	Sensor de vidrio roto	$10	$10
14	6	Syscom	SD-7101KBPE1	Botón de salida tipo push	$12	$72
15	3	Syscom	ELKP624	Fuente de 6, 12 y 24 VDC seleccionable a 1.2 A	$24	$72
16	3	Syscom	WP1.212	Batería recargable de respaldo de 12 VDC a 1.2 A	$8	$24
17	1	Sin Marca	Sin Modelo	Gastos de envío	$2,170	$2,170
18	1	Sin Marca	Sin Modelo	Canalización, cableado y montaje de todos los dispositivos. No incluye obra civil	$2,000	$2,000
19	1	Sin Marca	Sin Modelo	Instalación del sistema, configuración y puesta en marcha. Incluye capacitación en el sistema a 4 usuarios por 4 horas	$1,500	$1,500
					SUBTOTAL	$27,299
					IVA	$4,094.85
				PRECIO EN DOLARES	TOTAL	$31,393.85

Tabla 4.1.- Cotización autorizada para el proyecto.

Importe con letra: Treinta y un mil trescientos noventa y tres dólares con ochenta y cinco centavos.

Considerando que el tipo de cambio que se tomó el día del pago total del proyecto fue de $10.40 pesos por dolár, el costo total (con IVA) en pesos fue de: $326,496.04 (Trescientos veintiséis mil cuatrocientos noventa y seis pesos con 4 centavos)

Hasta el momento en el proyecto ya se tomado la elección de los equipos y siguiendo con el desarrollo de las etapas de la implementación del proyecto del sistema de control de acceso basado en el presupuesto aprobado por DSCA.

- Primera Etapa. Elaboración y seguimiento del plan de trabajo.
- Segunda Etapa. Implementación física del cableado y los dispositivos de control.
- Tercera Etapa. Implementación lógica (software) del sistema de control de acceso.
- Cuarta Etapa. Capacitación y entrega del proyecto.

4.1.- Elaboración del plan de trabajo.

En este plan se toma en cuenta los tiempos para realizar los servicios y requerimientos para la instalación de los equipos y software; que requiere el sistema de control de acceso. Además de una evaluación continua del proyecto.

Evaluación de la Implementación**:** Los plazos de implementación deben contar con evaluaciones periódicas que permitan detectar a tiempo problemas, debilidades y limitaciones e iniciar procesos formales para su corrección a tiempo. Algunos desarrolladores no ven con buenos ojos la introducción de cambios en el proyecto una vez iniciado el proceso de implementación, argumentando que introducirá retrasos e impactará el resto del proyecto.

Es por ello que debe definirse un protocolo formal (así como recursos y equipos de trabajo) para la revisión, corrección y adaptación de herramientas y sistemas en la fase de implementación sin que se produzca un impacto negativo significativo en la ejecución global del proyecto.

En ciertos casos se recomienda un equipo de trabajo paralelo al de desarrollo para la incorporación de los resultados de la evaluación a las fases semi-completadas del proyecto y su adecuación para no detener el avance del cronograma central de implementación.

A continuación mostramos el plan de trabajo establecido para la implementación del sistema de control el cual consiste en revisar los requerimientos, instalaciones, montajes configuración y pruebas de los equipos y para concluir capacitación y entrega del proyecto.

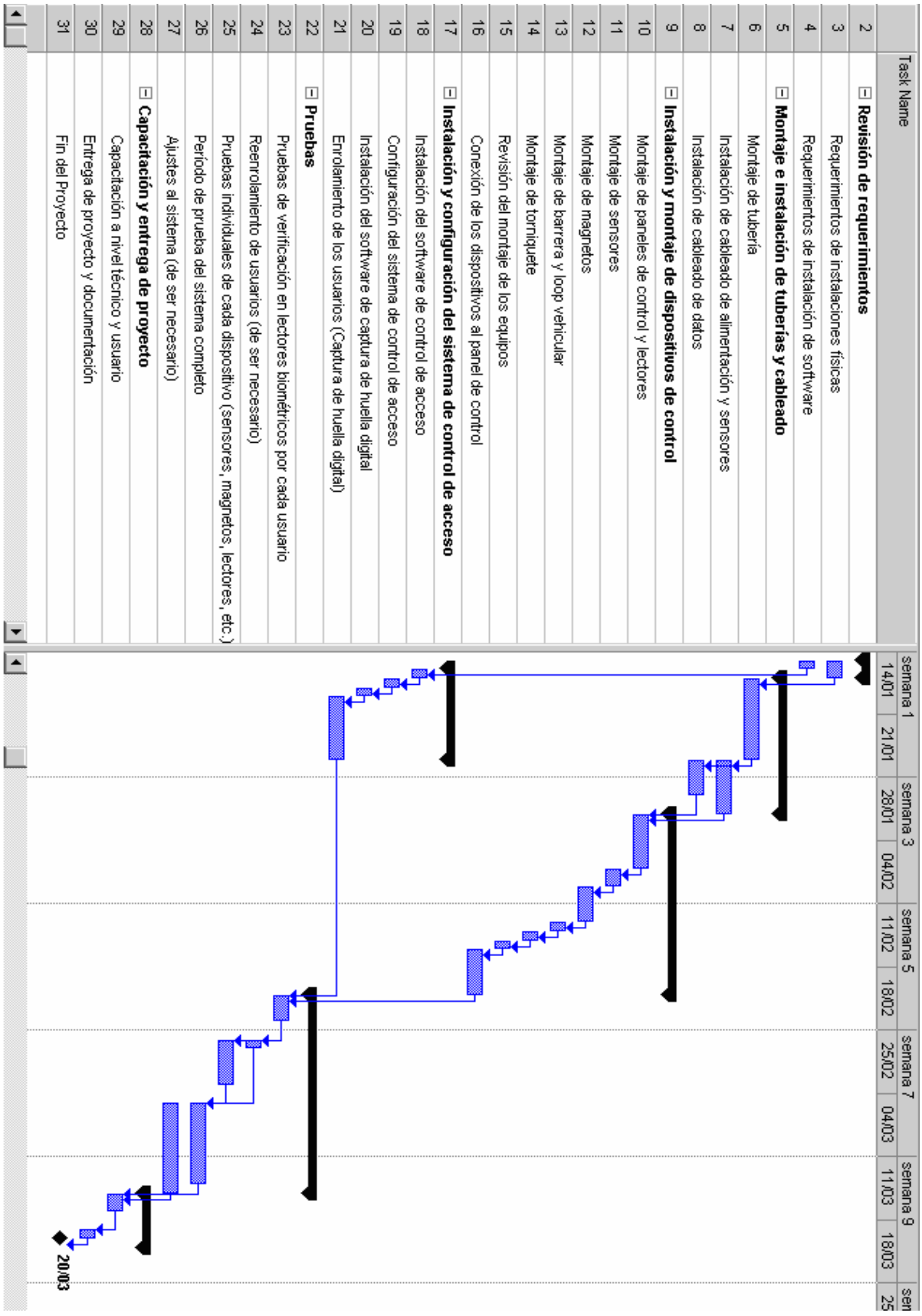


Figura 4.1.- Diagramas del plan del trabajo en meses.

4.2.- Implementación física de los dispositivos de control y cableado.

Definidos todos los elementos anteriores, procedemos a elaborar el proyecto de acuerdo a los plazos definidos y con procesos de evaluación a lo largo de la implementación para facilitar la detección a tiempo de problemas, debilidades y limitaciones. En esta sección mostraremos los planos de las instalaciones, debido a la necesidad de mostrar la ubicación de los accesos en donde se instalarán los equipos (lectoras, botones, paneles torniquetes y barra vehiculares) y sus respectivos diagramas de conexiones, para poder llevar acabo el cumplimiento de la instalación de los equipos prevista en el plan de trabajo y además tener un apoyo que nos permita detectar a tiempo problemas, debilidades y limitaciones e iniciar procesos formales para su corrección a tiempo. Una unidad puede afectar el resto y cómo podrá detectarse eso a tiempo solo teniendo la información correspondiente a cada equipo y tener un registro de los procesos que se llevaran acabo. Con lo que tenemos calidad técnica. Y una buena organización, que genera una instalación adecuada.

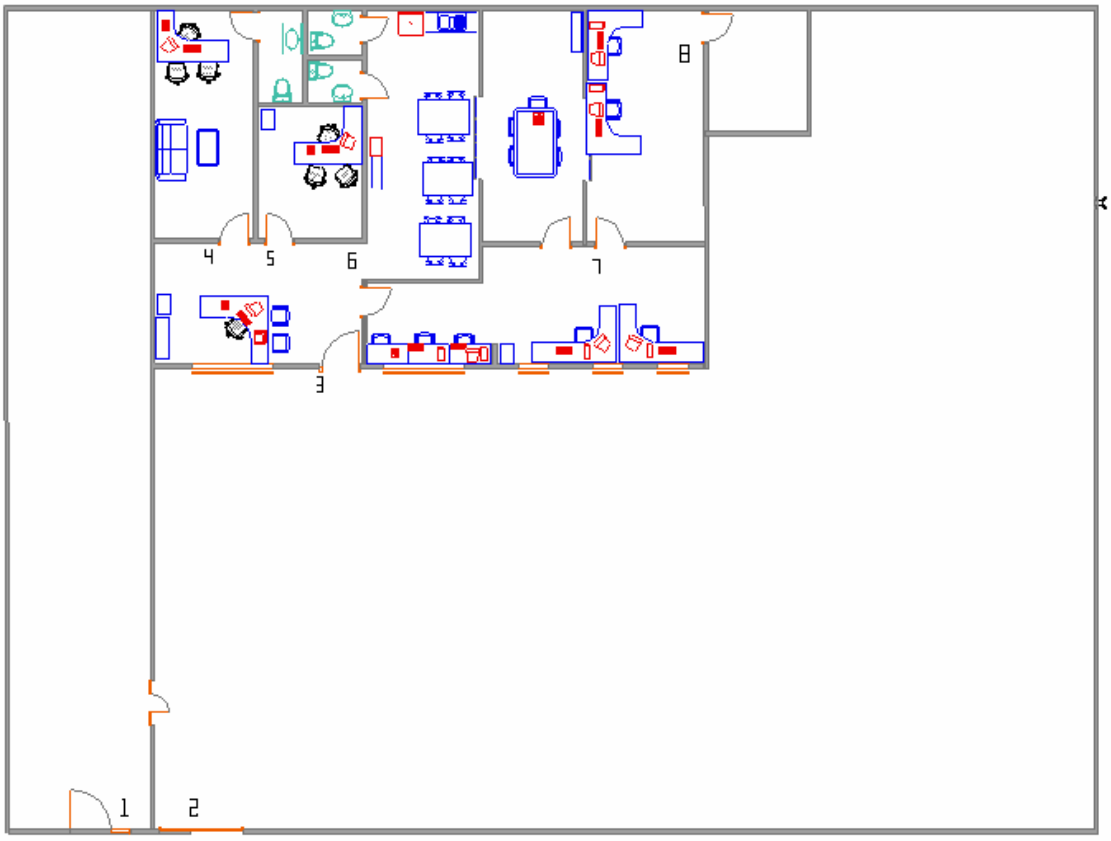


Figura 4.2. Plano arquitectónico de D.S.C.A

En la figura 4.2 podemos observar que existen 8 accesos marcados, y en los cuales se instalaran los equipos del sistema de control de acceso. En el siguiente plano (figura 4.3) se muestra la ubicación del cableado y el equipo se seccionado para cada zona.

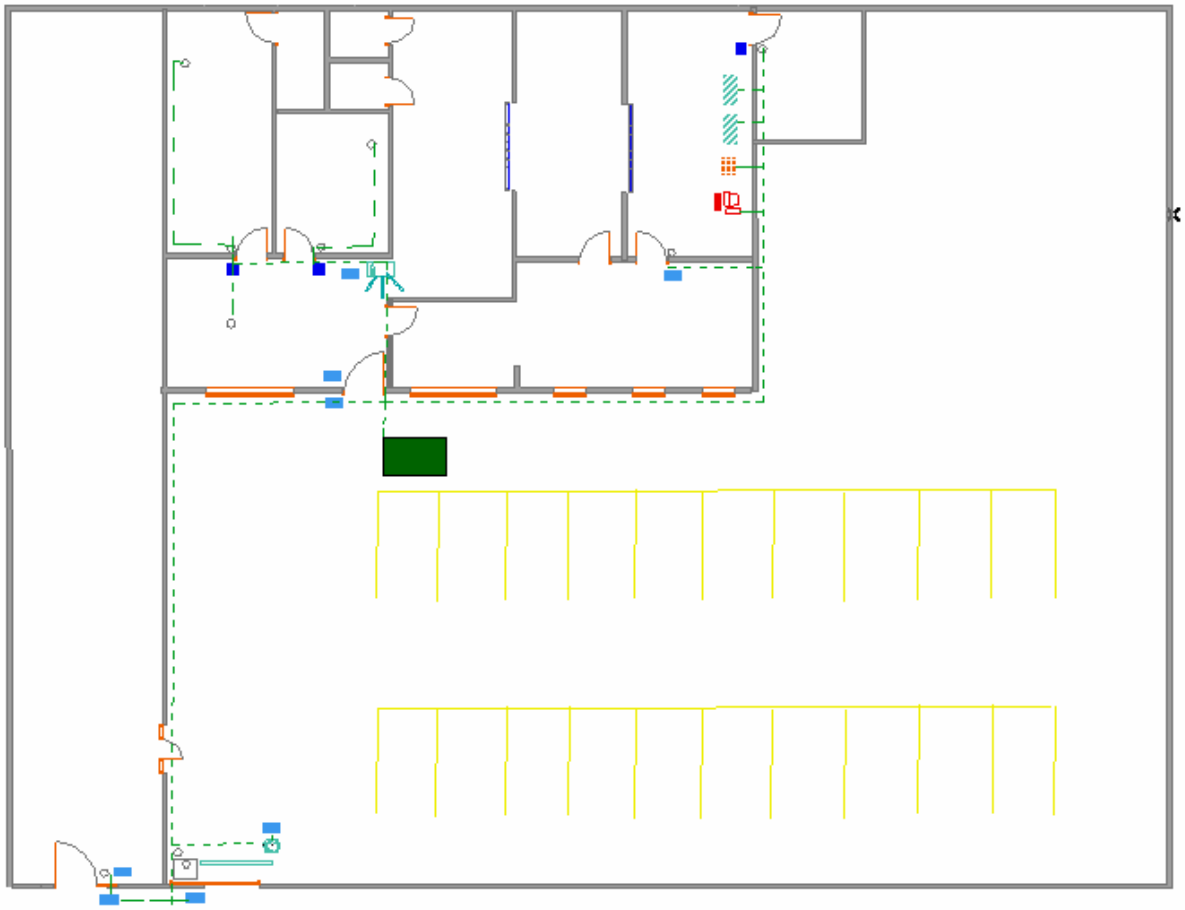
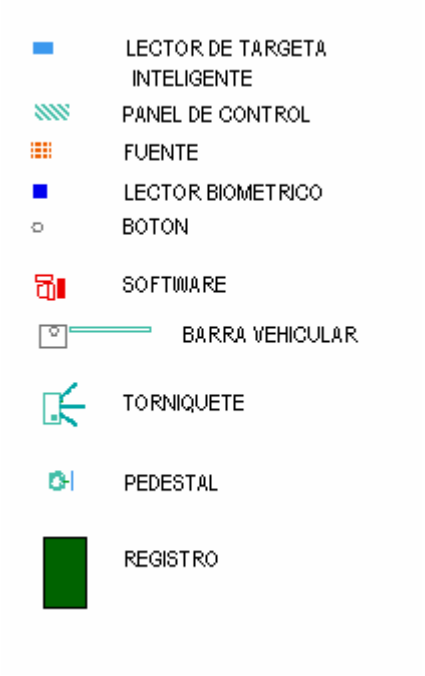


Figura 4.3. Plano de las Oficinas de D.S.C.A con cableado y dispositivos de control de acceso.

SIMBOLOGÍA



o

A continuación mostramos los diagramas de conexiones de los equipos que vamos a instalar. Comenzando con los Paneles que es la base de nuestro sistema. El diagrama representa a un panel IDentipass.

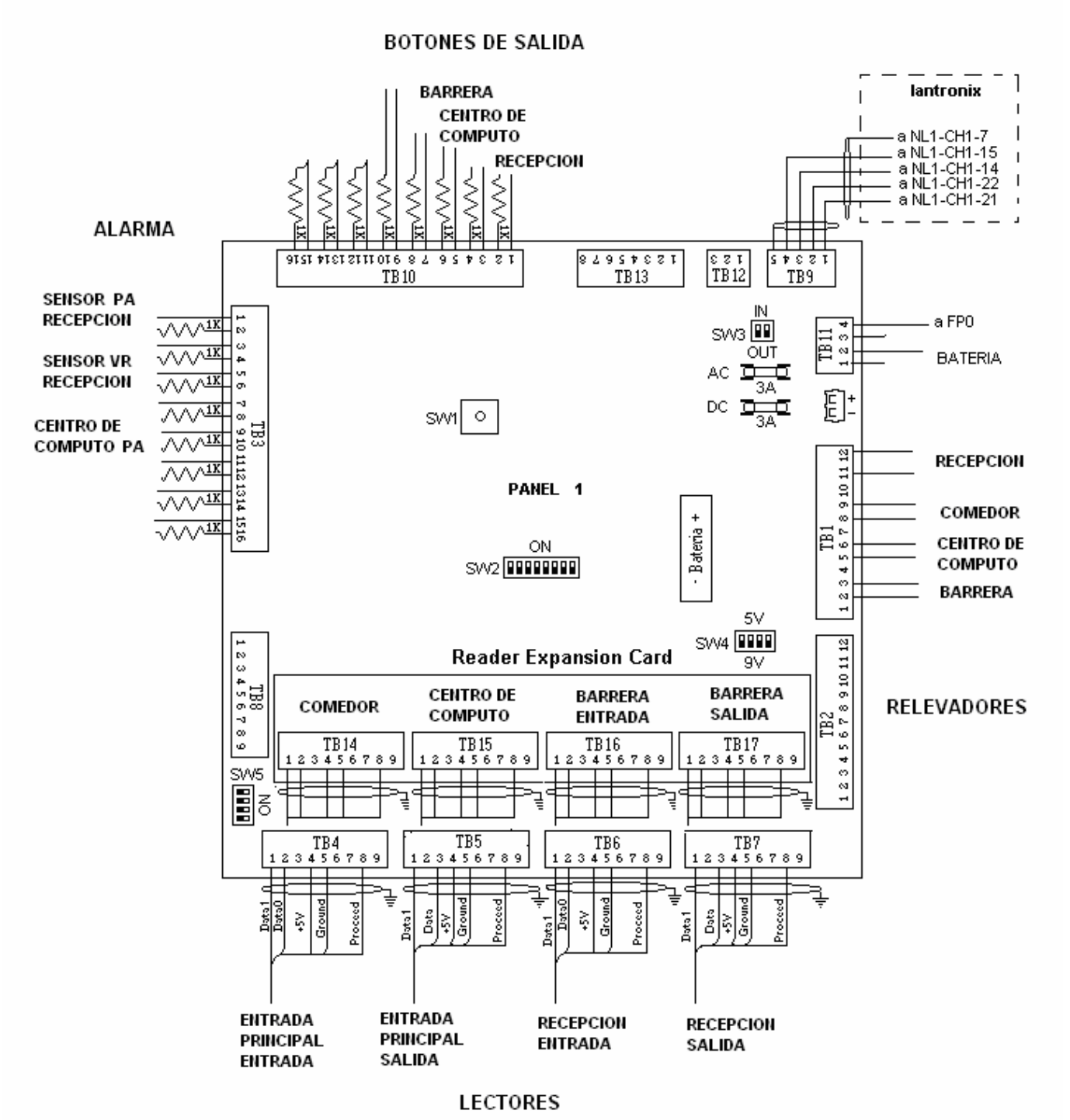


Figura 4.3. Diagrama de conexión del Panel 1

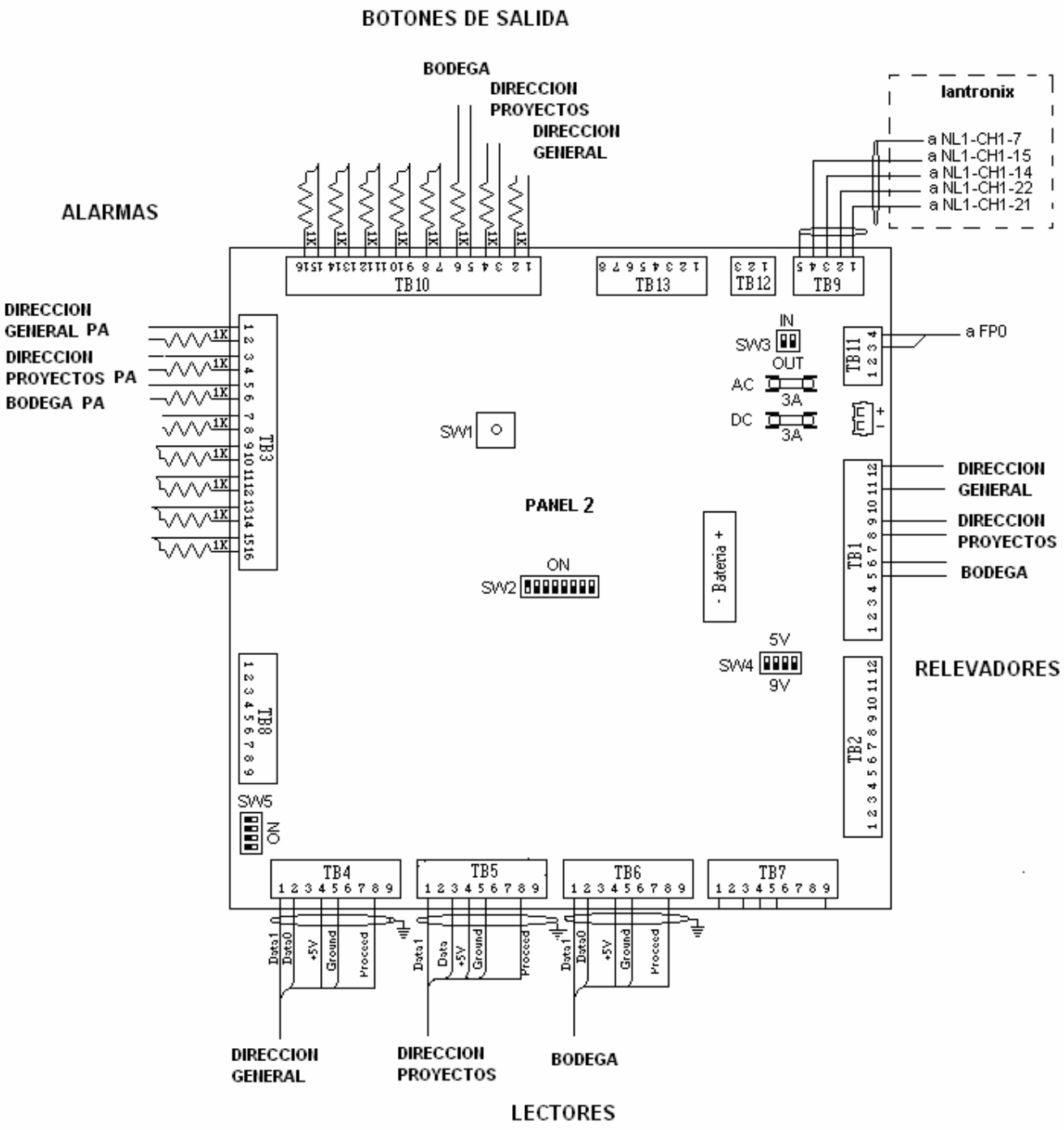


Figura 4.4. Diagrama de conexión del panel 2

Para estos paneles se puede observar que tienen una configuración muy similar el panel 1 (figura 4.3) tiene el control de mayor numero de lectoras pero se dividió así para manejar las tarjetas inteligentes y los biométricos por separado el panel 1 maneja las lectoras de tarjeta inteligente y el panel 2(figura 4.4) maneja las lectoras biométricas, con ello podemos manejar más cómodamente ambas tecnologías. Las demás conexiones de los paneles representan los relevadores, las alarmas y botones de salida de nuestro sistema.

A continuación mostramos en la siguiente tabla la configuración de los paneles de nuestro sistema.

Panel 1	*Panel 2*
Dirección de panel: 1	**Dirección de panel: 2**
Dirección IP: 8.1.3.200	**Dirección IP: 8.1.3.201**
COM: COM5	**COM: COM6**
Lectores:	**Lectores:**
1.- Entrada Principal Entrada	**1.- Dirección General**
2.- Entrada Principal Salida	**2.- Dirección Proyectos**
3.- Recepcion Entrada	**3.- Bodega**
4.- Recepcion Salida	
Relevadores:	**Relevadores:**
1.- Recepción	**1.- Dirección General**
2.- Comedor	**2.- Dirección Proyectos**
3.- Centro de Computo	**3.- Bodega**
4.- Barrera	
Alarmas:	**Alarmas:**
1.- Sensor PA (Puerta Abierta) Recepción	**1.- Dirección General PA (Puerta Abierta)**
2.- Sensor VR (Vidrio Roto) Recepción	**2.- Dirección Proyectos PA (Puerta Abierta)**
3.-Centro de Computo PA (Puerta Abierta)	**3.- Bodega PA (Puerta Abierta)**
Solicitudes de salida (botones):	**Solicitudes de salida (botones):**
1.- Barrera	**1.- Dirección General**
2.- Centro de Computo	**2.- Dirección Proyectos**
3.- Recepción	**3.- Bodega**

Tabla 4.2. Configuración de los paneles.

En la tabla 4.2 se muestra como están repartidas las lectoras las alarmas y los botones de los 2 paneles de control así como la dirección IP que tienen dentro de nuestro sistema.

También se observa que dentro del panel 1 se colocaron solo las lectoras de tarjeta inteligente y en el panel 2 se encuentran las lectoras biométricas esto fue decidido para tener un orden dentro de los paneles y con la ventaja de poder manejarlas con mayor facilidad.

En la figuras 4.5 y figura 4.6 se muestran las conexión de los dispositivos del panel a las chapas y botones del sistema. Y la figura 4.7 y 4.8 son las imagenes del panel de Control instalado.

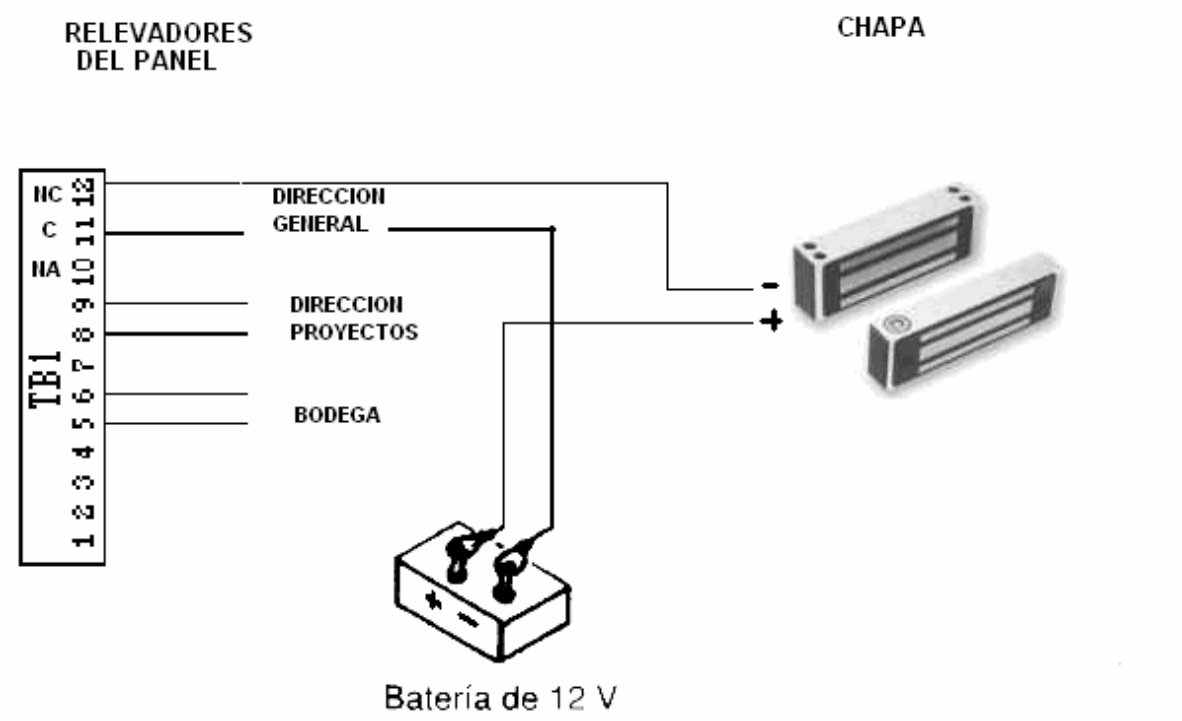


Figura 4.5. Conexión de los magnetos al panel

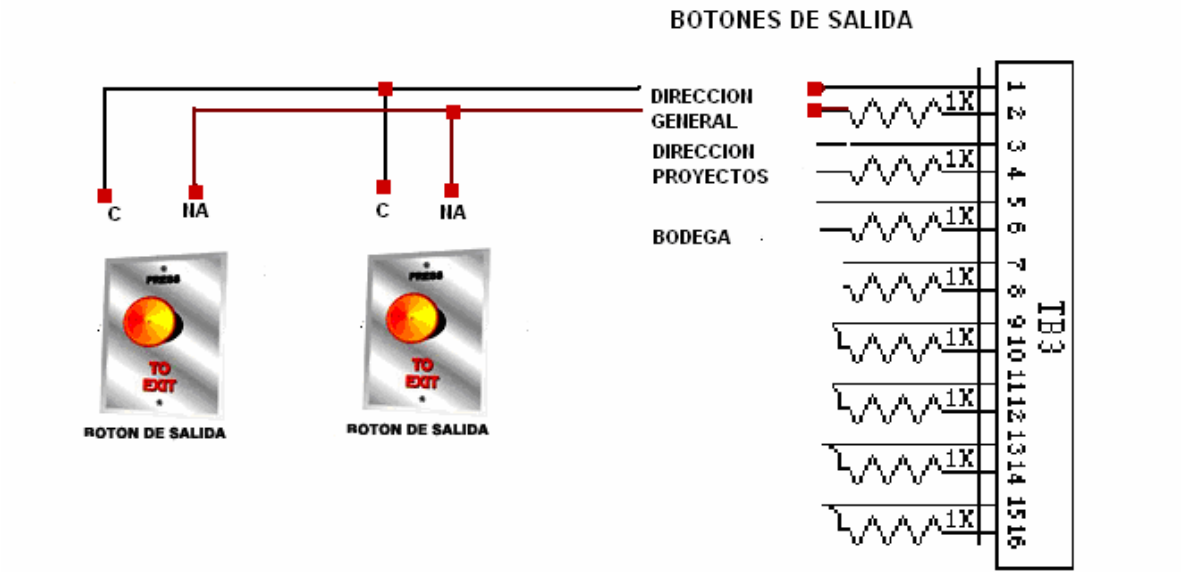


Figura 4.6. Conexión de los botones al panel

Figura 4.7. Panel montado en rack en el área de sistemas

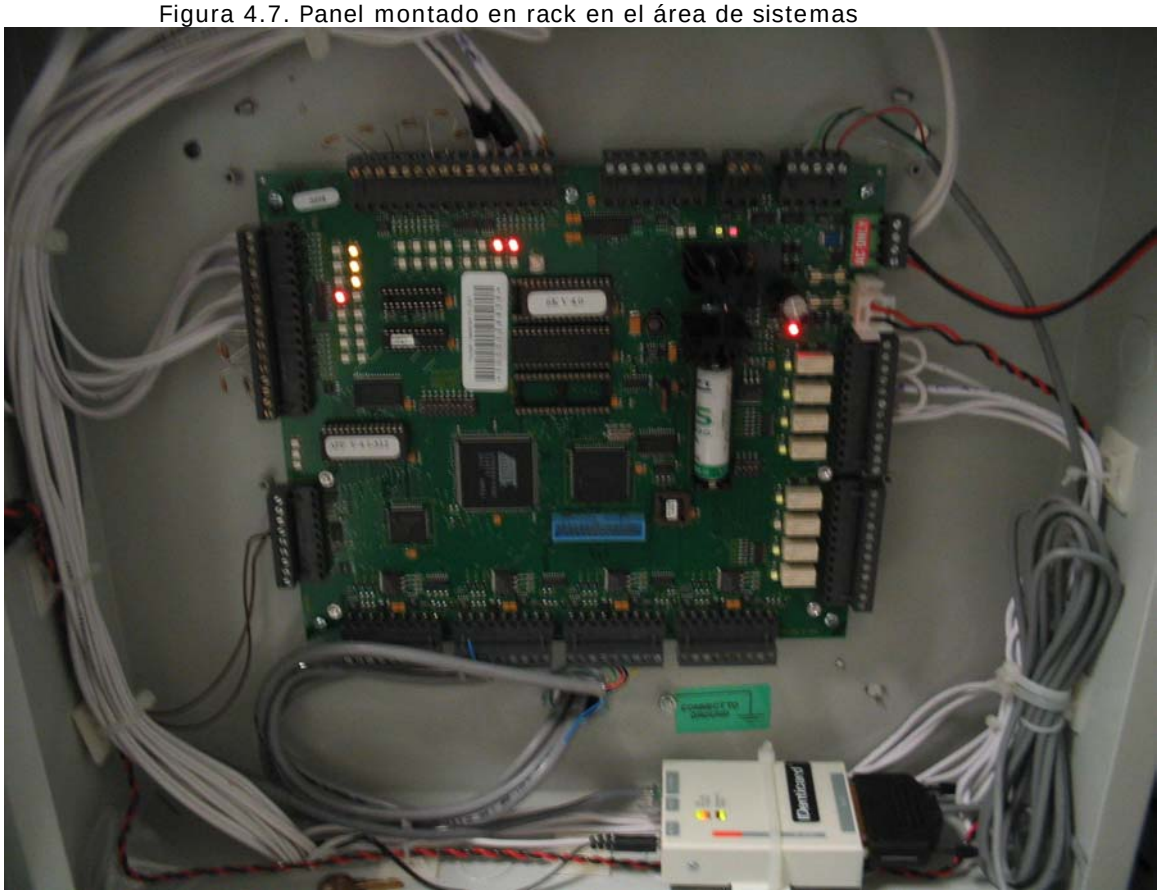
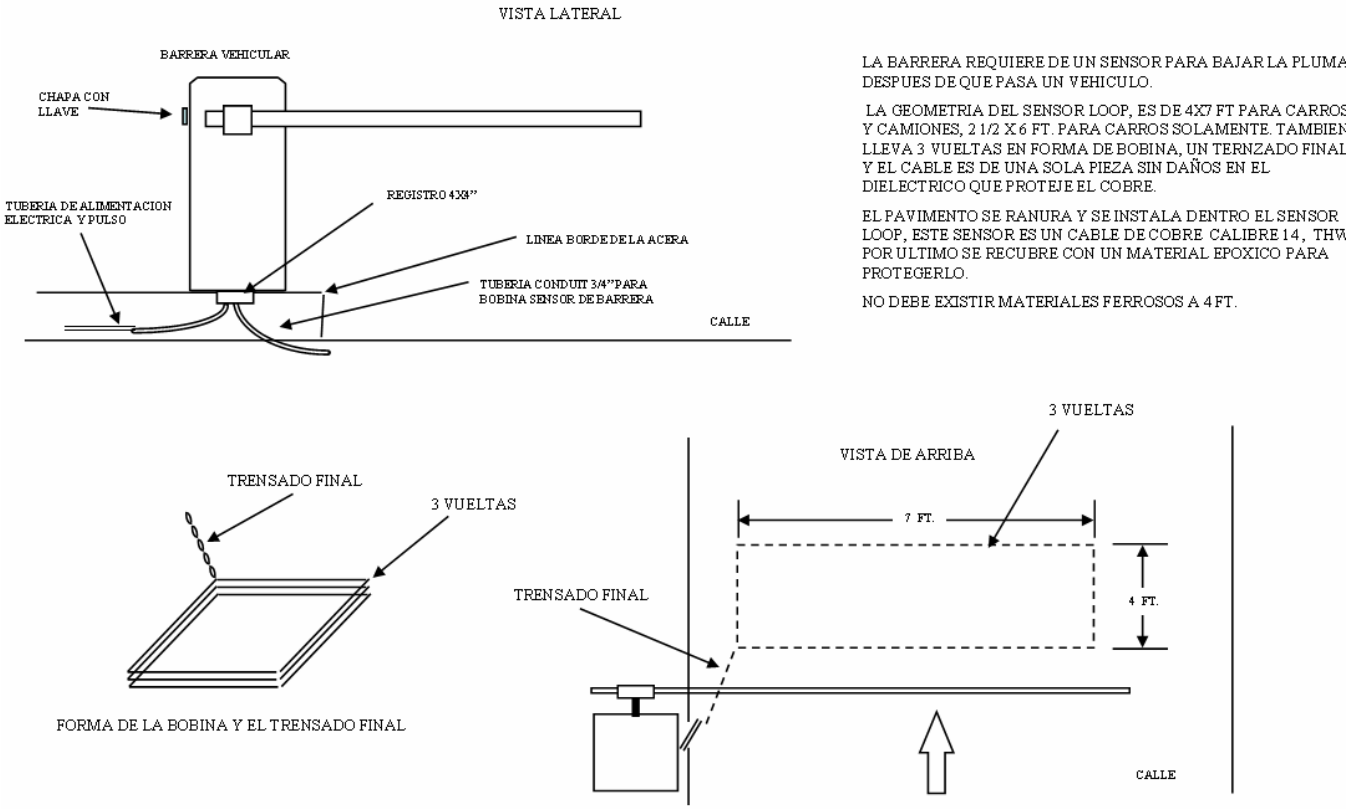


Figura 4.8 Panel 2 con todas las conexiones incluyendo el convertidor Serial/Ethernet Lantronix

En la figura 4.9 y 4.10 se observa los diagramas de los montajes de la barra vehicular y del torniquete.



FIJACION DEL SENSOR LOOP PARA LA BARRERA VEHICULAR APD G-89

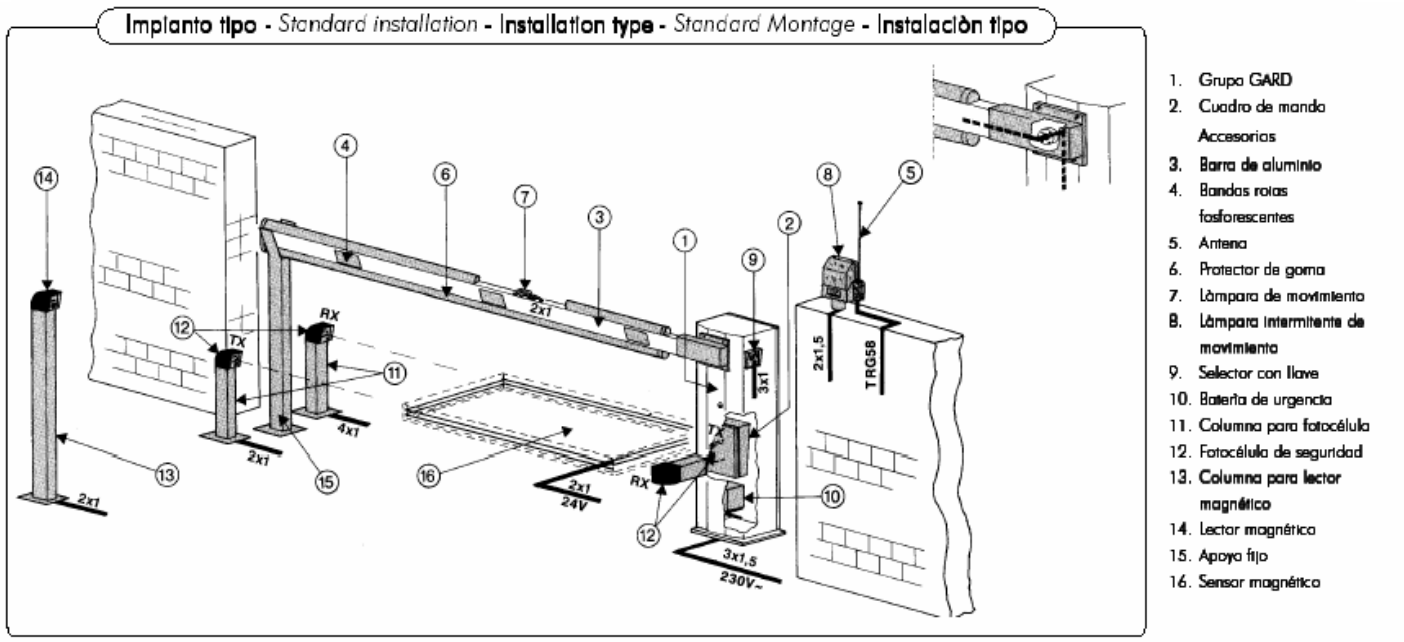


Figura 4.9. Instalación y características de la barrera vehicular a utilizar

o

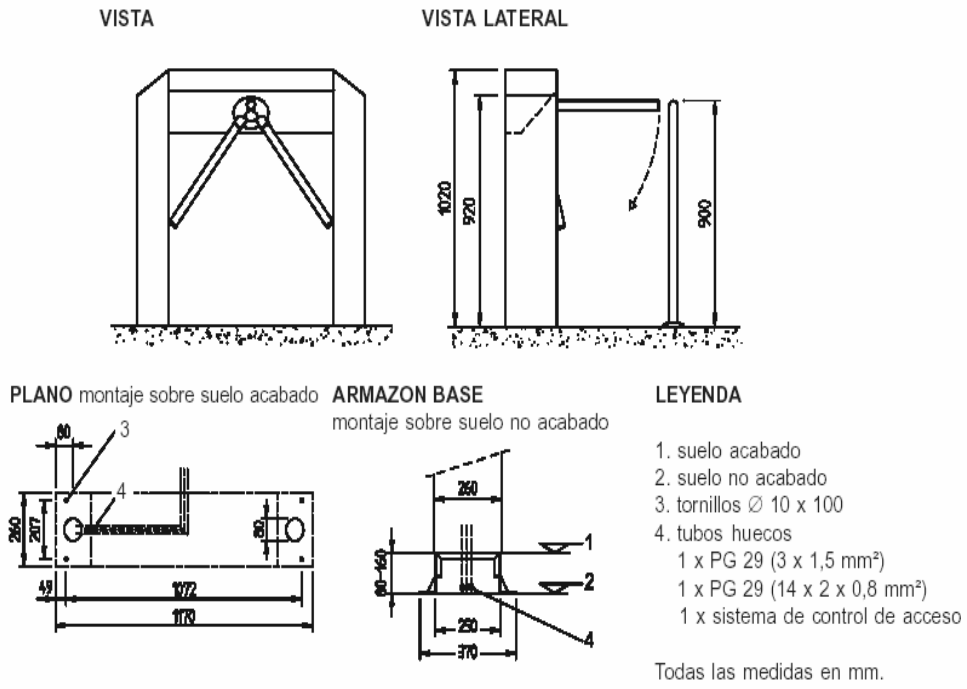


Figura 4.10. Instalación y características del torniquete.

4.3.- Implementación lógica (software) del sistema de control de acceso.

Para esta etapa es necesario haber concluido previamente la instalación de los equipos del sistema y la revisión de los requerimientos para la instalación del software, que son necesarios para la configuración del panel de control Identipass LT, y para configurar el Lantronix .

La configuración del panel de control y del los demás elementos lógicos se muestran en el apéndice B y se podra observar como se registra una huella al sistema, los pasos para instalar el panel, el MODEM y el lantronix. En esta sección solo mostraremos algunas opciones que presenta el panel de control. Sin embargo la configuración del panel y el registro del la huella al sistema se puede observar en el se puede observar en el apéndice B.

4.3.1.- Configuración del Panel.

En esta parte solo mostraremos algunas e las opciones con la que cuenta el panel de control las otras opciones con las que cuenta el panel como el añadir un lector o botón son presentadas en el apéndice B.

Comenzaremos con el software para el panel de control de acceso, este software está basado en una estructura de cliente-servidor, por lo que es necesario primeramente instalar el software servidor para después conectar a el los clientes.

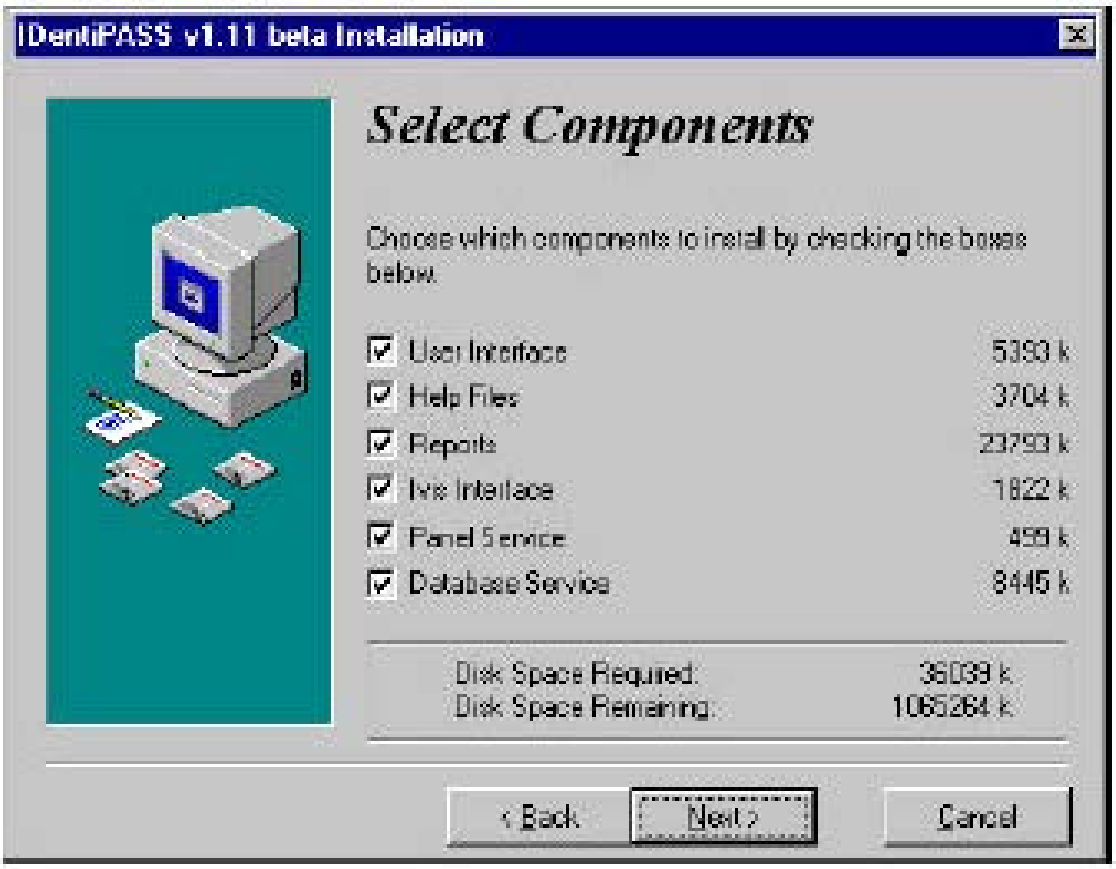


Figura 4.11 Instalación del software para el panel IDentipass.

Dentro del proceso de instalación del servidor es necesario señalar cada una de las opciones mostradas, las cuales son:

- User Interface: Es el programa cliente que permite administrar, configurar y monitorear el sistema.
- Help Files: Son los archivos de ayuda que componen el manual del software.
- Reports: Son todos los tipos de reportes que puede generar el sistema referente al acceso de los usuarios y reportes internos del sistema
- Ivis Interface: Es un pequeño software incluido que permite al usuario del sistema diseñar e imprimir credenciales

Dentro de software podemos tener algunas funciones que nos servirán para poder agregar a los usuarios a sus áreas de trabajo o los lugares en los que pueden tener acceso, así como la capacidad de habilitar un lector dentro del panel o otros elementos o los puertos que van a ser ocupados por la computadora y el panel. A continuación se muestran algunas de las funciones con las que cuenta el software de Identipass LT.

Agregar un site: SITE es la localización de tus base de dato ODBC. Puede ser una computadora o una conexión interna. Identipass LT permite instalar una base de datos, un panel de servicio y 4 interfaces. Para añadir tu Site, la computadora tiene que sostener la base de datos y sondear los paneles, con un

clic izquierdo en el Mouse sobre SITE sobre el menú principal y como seleccionar a la computadora que se va utilizar como SIte.

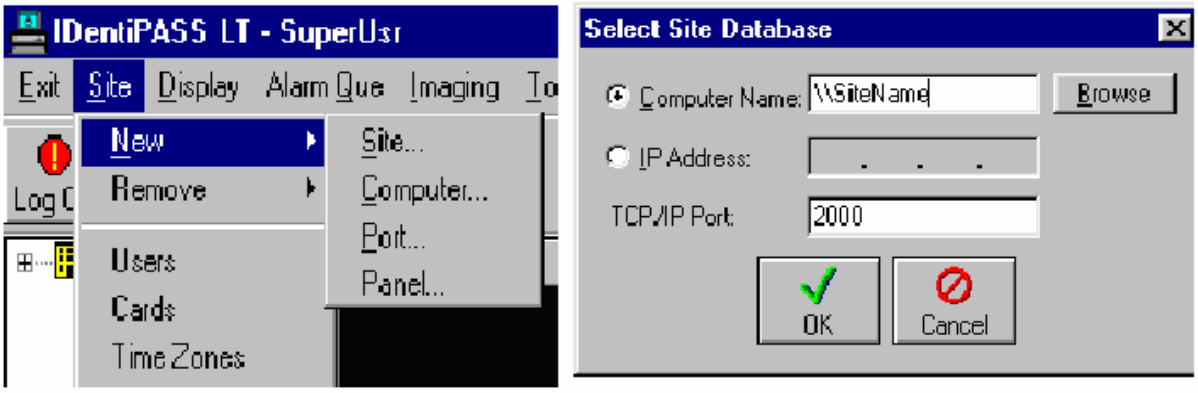


Figura 4.12 Agregar un Site para el panel IDentipass.

Con el menú figura 4.12 también se puede agregar varias computadoras y puertos para la comunicación entre el panel y la computadora.

De la ventana se puede escoger los tipos de dispositivos, puertos y velocidad en la conexión. Los tipos de dispositivos que pueden ser seleccionados son del 9000 panels o NetLink.

Sus opciones son RETRY: Control el número de minutos entre el llamado de volver a intentarlo

TIMEOUT: Este set es el número de segundos que el panel esperara por la respuesta del anfitrión.

THRESHOLDL: Esto pone el porcentaje de la plenitud para el búfer de la transacción que causará que el panel llame a la computadora personal cargar sus transacciones. El búfer de la transacción del entrepaño tiene un máximo de 4000 transacciones.

Dail on card Fail: Si esta opción es escogida, una transacción de tarjeta que falla causará que el panel llame el número de la emergencia para notificar el sistema.

Reinitialize Panel: Un panel remoto es mandado su información de arreglo sólo una vez. sobre el inicio de inicial. Si usted cambia información en esta pantalla, tal como números de teléfono, usted debe escoger "Reinicializa Entrepaño" causar que la nueva información para ser cargada al panel remoto.

Slave Panel: el panel remoto panel: Verifique esto cuando el panel no es el panel al que el módem esta conectado.

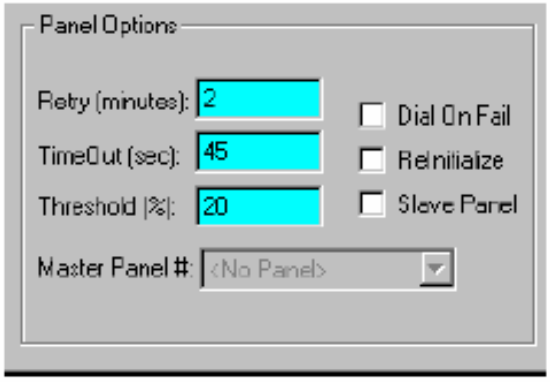


Figura 4.13 Opciones del panel.

4.4.- Capacitación y entrega del proyecto.

Los plazos de implementación deben contar con evaluaciones periódicas que permitan detectar a tiempo problemas, debilidades y limitaciones e iniciar procesos formales para su corrección a tiempo. Y una vez terminado la parte del la implementación es importante capacitar al personal sobre el uso de los equipos para esto agregamos un apéndice el cual nos sirve para explicar como se registra una huella digital.

Es por ello que debe definir un protocolo formal (así como recursos y equipos de trabajo) para la revisión, corrección y adaptación a los equipos y sistema en la fase de capacitación sin que se produzca un impacto negativo significativo en la ejecución global del proyecto.

En ciertos casos se recomienda un equipo de trabajo paralelo al de desarrollo para la incorporación de los resultados de la evaluación a las fases semi-completadas del proyecto y su adecuación para no detener el avance del cronograma central de implementación.

En algunas ocasiones es se presenta una resistencia al cambio y es por ello, que sirve de manera increíble que el personal o usuarios tengan una participación como actores en los diversos sectores. Lo que lleva al individuo a la familiarización con el nuevo sistema ya existente.

Para la capacitación es necesario contar con un manual de usuario o lo que es lo mismo materiales de capacitación, cobertura, sectorial y consideraciones logísticas.

Unidades de Ejecución: Definición de perfiles de grupos de trabajo, líderes y responsables de las distintas secciones y servicios del proyecto, e identificación de quiénes cumplen con esos perfiles.

Definición de Responsabilidades: Delimitación clara de responsabilidades de acción, recursos y participación con conocimiento de las relaciones y dependencias entre el trabajo de las distintas unidades. Prever cómo el

incumplimiento de una unidad puede afectar el resto y cómo podrá detectarse eso a tiempo.

4.4.1.-Definición de Ciclos de Renovación y Actualización

Al definir el presupuesto y los costos de un proyecto, debemos considerar el costo de su mantenimiento, actualización y renovación, para no encontrarnos en una situación de limitaciones operativas e imposibilidad de alcanzar los objetivos en el corto plazo y obsolescencia en el mediano plazo.

Debe hacerse un análisis exhaustivo que permita detectar y prever costos ocultos y costos futuros del proyecto e integrarlos en el presupuesto.

Así mismo deben definirse escenarios cambiantes del entorno y el impacto de dichos cambios para elaborar de antemano planes de contingencia, con costo definido, que permitan lidiar con ellos y evitar que pongan en peligro la consecución de los objetivos del proyecto.

Si bien cada proyecto es único y la infraestructura y tecnologías poseen sus características particulares, se recomienda proyectar un costo de mantenimiento, renovación y actualización anual que ronde por el 25% al 35% del costo inicial del proyecto.

Un buen ejercicio, para evaluar y ver si se justifica la inversión, es estimar los costos totales del proyecto a 3 y 5 años y los beneficios esperados. No vale la pena proyectar más allá ya que la tecnología generalmente supera nuestras expectativas y cambia los entornos, herramientas y paradigmas en formas que hoy no podemos imaginar en plazos tan reducidos como 5 años. Por ello, debe tenerse en cuenta que los proyectos de tecnología, a menos que cuenten con una buena estrategia de renovación y actualización, y aún implementándola, deben renovarse por completo al menos cada 3 años y máximo cada 5.

También sugerimos la adquisición de un contrato de mantenimiento preventivo y correctivo anual con cuatro visitas al año para dar mantenimiento preventivo y las visitas necesarias si es que surge algún problema que requiera de un mantenimiento correctivo. Dicho contrato tendrá un costo anual del 15% del total del proyecto (no incluye refacciones).

CONCLUSIONES

Conclusiones

La tecnología biométrica proporciona muchas ventajas: seguridad, comodidad, variedad de fabricantes, estandarización de equipos, diferentes tipos de biométricos y un aspecto muy importante para este caso de análisis, los costos de implementación, con la implementación del sistema biométrico la empresa CAPTA pudo obtener grandes beneficios en los que podemos destacar el factor comercial, esto es, que se puede mostrar ventajas de estos equipos con una implementación real. La cual esta diseñada expresamente para su optimo funcionamiento, motivos por los cuales se cumple con otro de los objetivos que tenía la empresa que era, utilizar esta división como sujeto de prueba para una implementación de un sistema de control similar en todas las divisiones de la empresa cubriendo así todo el edificio, y con base en los resultados obtenidos la empresa se encuentra analizando actualmente la posibilidad de implementar un sistema de control de acceso a mediano plazo.

Ventaja tecnológica: Con la utilización de las lectoras de biométricos y de tarjeta inteligente. El guardar un template en la tarjeta inteligente (smart card) permitió al sistema ahorrar parte de la memoria porque la base de datos de la huella se convirtió en una base de datos distribuida en el que el usuario lleva su propio registro permanentemente esto permite que la base de datos del sistema de control de acceso pueda crecer en una gran medida sin sobrepasar sus limites propios (en usuarios o mantener más tiempo los eventos ocurridos mediante el registro de reportes.) Lo cual incrementa la capacidad del sistema.

La comunicación entre el servidor y el panel de control de acceso de fabrica es vía serial (RS232 O RS484) y esto proporciona ciertas desventajas como es una velocidad de comunicación más lenta y que el sistema sea controlado por una computadora con la inclusión de l adaptador Ethernet y de la estructura interna de la red (Ventajas de usar tecnología Ethernet: Usa un método de transmisión de datos conocido como Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA / CD). Cuando una estación de trabajo quiere acceder a la red, debe cerciorarse si hay alguna otra maquina transmitido para transferir la información a través de la red. Todas las estaciones de trabajo recibirán el mensaje y la que sea el destino recibirá la información. En caso de que dos estaciones de trabajo traten de enviar datos por la red al mismo tiempo, cada una tendrá un aviso de colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envió, con esto se puede obtener otras ventajas como son: el tener instalado clientes en diferentes en diferentes equipos o (computadoras) aparte del servidor, que en base a permisos establecidos puede monitorear o modificar algunos aspectos del sistema vía remota.

Esto también facilitaría que todo el sistema de control implementado tenga la gran ventaja de poder integrarse a un circuito cerrado de televisión (CCTV) o un sistema de alarmas convencionales por ejemplo si una alarma de incendio se

activa el sistema puede liberar todas las puertas ya se ha internamente o vía remota o tener una lectura con cámaras de seguridad en las zonas más importantes.

En cuanto a la capacitación para el personal que se encargará de administrar el sistema de control de acceso debe ser integral, para el monitoreo de datos, y mantener el sistema en perfectamente condiciones, y con ello evitar en gran medida ser atendidos por los técnicos de soporte y con ello gastos innecesarios. Por otra parte, es conveniente proporcionar a los usuarios información para configuración del sistema y que puedan explotar todas las funciones que estos le ofrecen sin necesidad de levantar un reporte por este motivo. Hasta el momento, la Dirección General cuenta con un tríptico para el uso de los equipos digitales, por lo que se requiere de elaborar un material de características similares del uso del sistema en general.

Por ultimo con la elaboración de este trabajo pudimos observar que la mayor parte de las empresas de seguridad en nuestro país únicamente comercializan e importan tecnología de seguridad empresarial, y que no se tiene la disposición para diseñar y desarrollar sus propios sistemas o elementos de seguridad con lo que se podría reducir los gastos de estos sistemas en gran medida.

APÉNDICES

Apéndices.

A. Equipos para sistemas de control de acceso.

La serie Honeywell permite el control de acceso y teniendo ciertas ventajas. Compatible con versiones previas de WINPAK (2.0 / PRO) así como NSTAR, trabaja con paneles NS2 + (NS2 de NSTAR actualizado), N1000 y Pro2200.

IDenticard® ha hecho que el control de acceso confiable sea simple y económico para cualquier negocio con la introducción de Centurión, un sistema independiente con capacidad para 2 lectoras. Centurión es ideal para ser usado en aplicaciones pequeñas que requieran control de acceso a 1 o 2 puertas.

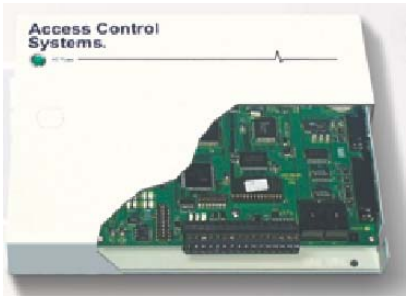
Equipo	Ventajas	Imagen y Costo
Centurión	**Características principales** **• Capacidad para 2,500 usuarios en la base de datos del panel** **• Compatible con la mayoría de las lectoras estándar de la industria** **• Bloqueo automático habilitado / deshabilitado** **• Control de zonas de tiempo con opción de exclusión** **• Antipassback** **• Control de parqueaderos que mantiene cuenta de tarjetas en el área** **• Regla de supervisor**	 $950.00 Dls

Tabla A.1.- Equipos de Centurión para sistemas de control de acceso.

Equipo	Ventajas	Imagen y Costo
IDENTIPASS	**Características principales SERIES IDentiPASS** **. Registro de los acontecimientos ocurridos** **. Ilimitados grupos de acceso virtuales asignados a un usuario** **. puerta flexibles y configuración de grupos de puertas** **. Acontecimientos y registros de los eventos realizados por los usuarios** **. Capacidad para 64.000 Tarjetas**	 $2045 Dls $1650 Dls (tarjeta de expansión para 4 de lectores)

Tabla A.2.- Equipos de IDentipass para sistemas de control de acceso.

Cuando hablamos de los sistemas de Control de Accesos, una parte importante cuando se instala un Sistema de Control de Acceso, todos los equipos están conectados entre sí y se centraliza todo el manejo y supervisión del sistema en una computadora, que tendrá instalado un Software de Gestión, Administración, Control y Supervisión de todos los accesos. Generalmente en estos casos, la información de lo que está sucediendo en cada acceso (es indistinto que sean puertas, molinetes, barreras, etc.), se estará viendo en ese mismo momento en la PC de Gestión, teniendo en cuenta el panel elegido, el software será elegido dependiendo de nuestro panel.

Software para el panel del control

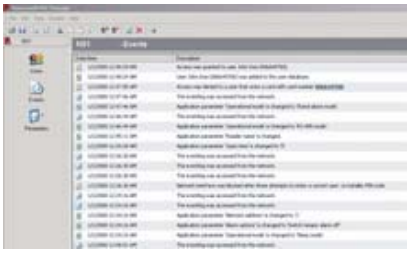
Equipo	Ventajas	Imagen y Costo
NS1CU. Software para NS1	**Software.** *** Lleva a cabo todas las funciones de sistema. configuración y monitoreo** *** Control de hasta 8 unidades / red RS485** *** Reporte de eventos opción de impresión o exportación** *** Administración de usuarios, agregar y borrar, clasificar usuarios y antipassback por tiempo de 1 a 254 minutos.**	 $275.00 Dls
Equipo	Ventajas	Imagen y Costo
Software de Integración WIN - PAK 2005.	**Razones para adquirir WinPak 2005:** *** Incluye todo lo necesario para sistemas sencillos o completos** *** Integración con DVRs (Fusión y Rapid Eye)** *** Administración de uno o varios sitios** *** Módulo de credencialización integrado** *** Configuración rápida y fácil** *** Gran base instalada** *** Reducción de tiempo de instalación** *** Tecnología de punta** *** Programación flexible** *** Nuevas características que satisfacen las necesidades de sus clientes y proyectos.**	

Tabla A.3.- software para los paneles de los sistemas de control de acceso.

Lectoras

Muchos sistemas de Control de Acceso, además de permitir usar uno o dos lectores (no importa con qué tecnología), nos permiten combinar dichas tecnologías para facilitar y adecuar nuestras necesidades. Decimos que este es el punto, quizás, más importante, porque en realidad define la característica "visible" de todo el equipamiento instalado, que estará dada según el perfil del cliente, del ambiente de trabajo y el presupuesto asignado a la obra.

bioscrypt ***Sistema Biométrico con Lectora de Proximidad Integrada.***

Equipo	Ventajas	Imagen y Costo
VProx, VFlex y VPass. **Para instalación en interiores. Estos tres modelos son similares en su forma física, con las diferencias propias de cada una, como se muestra a continuación:** **V-PROX: Lectora de huella con lectora de proximidad HID integrada en el cuerpo de la V-Prox. Enrolamiento de 4,000 plantillas de huellas.** **Compatible con Controladores Serie IQ Indispensable una excelente conexión a tierra física de este equipo para su correcta operación y garantía. Proporcionar número de serie de la lectora al pedir tarjetas adicionales.** **V-FLEX: Provee autentificación con huella y se integra con otras lectoras como las de banda magnética, las de proximidad, o de código de barras entre otras(dispositivo externo Wiegand). Enrolamiento de 4,000**	**Comunicación:** **Puerto RS232, RS485, Wiegand.** **Voltaje:** **9-24V DC** **Temperatura de operación:** **0 a 60 grados centígrados** **Altura 130 mm** **Anchura 50 mm** **Profundidad 65.5 mm** **Tiempo de enrolamiento menos de 3 segundos** **Tiempo de verificación entre 1 y 2 segundos** **Tamaño de plantilla de huella 350 bytes en VProx y VFlex, y de 2400 bytes en VPass** **Tasas de error:** **VProx y VFlex: Tasa de Falsa** **Aceptación y de Falso Rechazo iguales 0.1%** **VPass: Tasa de Falsa Aceptación 0.2%, Tasa de Falso Rechazo 1.0%**	 **$1077.00 Dls**

plantillas de huellas. **V-PASS: Identificación automática y sencilla del usuario únicamente con su huella dactilar. Capacidad máxima de 500 plantillas de huellas, 300 es el número óptimo.** **Pueden ser utilizadas en ambientes de desarrollo cuando se utiliza el kit de desarrollo (SDK) de Bioscrypt dando así mayor flexibilidad.** **Se administra con el software VeriAdmin para enrolamiento y administración de huellas y usuarios.**	**Niveles de seguridad** **VProx: Credencial & Huella con lector de proximidad HID integrado.** **VFlex: Credencial & Huella con lector externo conectado a VFlex.** **VPass: Huella sola.**	 **$1,108.00 Dls.**
V_Smart. **Para instalación en interiores. El modelo V-Smart permite a un usuario autentificarse utilizando su credencial inteligente -sin contacto- tipo MiFARE (modelo V-Smart-A) o iCLASS (modelo V-Smart-A-H), para luego colocar su huella dactilar y así contar con una autentificación doble.** **Estas tarjetas inteligentes almacenan la huella dactilar del usuario -misma que se registra en el enrolamiento de dicho usuario- y es muy útil cuando se cuenta con cientos o miles de usuarios.** **Prácticamente puede tener número ilimitado de usuarios. La huella NO se almacena en el dispositivo, solamente en la credencial inteligente sin contacto.**	**Comunicación :** **Puerto RS232, RS485, Wiegand.** **Voltaje : 9-12V DC** **Temperatura de operación 0 a 60 grados centígrados** **Altura 130 mm** **Anchura 118 mm** **Profundidad 63.5 mm** **Tiempo de enrolamiento menos de 5 segundos** **Tiempo de verificación entre 1 y 2 segundos** **Tamaño de plantilla de huella 350 bytes** **Tasas de error** **Tasa de Falsa Aceptación y de Falso** **Rechazo iguales: 0.1%** **Niveles de seguridad** **Credencial inteligente sin contacto & Huella**	 **$1200 Dls**

V-Station. **Para instalación en interiores. El modelo V-Station permite a un usuario autentificarse con su número de empleado para colocar posteriormente su huella dactilar, o si se prefiere, puede autentificarse primero con una tarjeta o credencial de proximidad para posteriormente colocar su huella.** **Es un equipo robusto que puede conectarse a la red de la institución/empresa con un cableado Ethernet pues puede asignársele una dirección IP.** **Puede contener desde 1 hasta 3,550 plantillas de huella y alojar más de 4,000 eventos.** **Cuenta con un software de administración Veriadmin incluido que permite el enrolamiento, administración y explotación de datos desde una PC de la red.** **Produce un archivo de eventos que deberá ser explotado por el cliente para su análisis posterior.** **Con su tecnología de relevador interconstruida puede activar la apertura de dispositivos de acceso como electroimanes, torniquetes y otros.**	**Comunicación** **Puerto Ethernet, RS232, RS485, Wiegand.** **Voltaje 9-12V DC** **Temperatura de operación 0 a 60 grados centígrados** **Altura 130 mm** **Anchura 118 mm** **Profundidad 63.5 mm** **Tiempo de enrolamiento menos de 5segundos** **Tiempo de verificación entre 1 y 2 segundos** **Tamaño de plantilla de huella** **350 bytes** **Tasas de error** **Tasa de Falsa Aceptación y de Falso Rechazo iguales: 0.1%** **Niveles de seguridad:** **V-Station-A (Base) Múltiple: PIN solo, PIN & Huella, PIN & Huella & Password, PIN & Password** **V-Station-AP (Proximidad) Múltiple: PIN solo, PIN & Huella, PIN & Huella & Password, PIN & Password. La credencial de proximidad toma el lugar del PIN.** **V-Station-AG (Tarjeta inteligente) Múltiple** **V-Station-AH (Tarjeta inteligente) Múltiple** **V-Station-AS (Search) Huella sola.**	 **$1,450.00 Dls.**  **$2300 Dls**

Tabla A.4.- Lectoras Bioscript para sistemas de control de acceso.

Lectores HID.

<table>
<tr><th>Equipo</th><th>Ventajas</th><th>Imagen y Costo</th></tr>
<tr>
<td>iClass R10.

Ideal para aplicaciones de control de acceso pues combina el mayor rango de lectura de proximidad de 13.56MHz de las credenciales iClass con la tecnología de credencial inteligente.

Lectoras y credenciales requieren llaves que empaten para operar. Toda transmisión entre lectora y credencial es cifrada utilizando un algoritmo seguro.</td>
<td>Frecuencia de transmisión

13.56MHz

Distancia de lectura

<table>
<tr><th>Credencial</th><th>Distancia máx.</th></tr>
<tr><td>iClass Card</td><td>7.6 cm</td></tr>
<tr><td>iClass Key</td><td>2.5 cm</td></tr>
<tr><td>iClass Tag</td><td>2.5 cm</td></tr>
<tr><td>iClass Prox</td><td>3.8 cm</td></tr>
<tr><td>MiFARE Card</td><td>5.0 cm</td></tr>
</table>
Tamaño 4.83 X 10.26 X 2.03 cm

Alimentación 10 a16 VCD

Corriente

80mA promedio/300mA pico a 12VDC

Seguridad

Llaves de autentificación de 64 bits.

Instalación Interiores & exteriores Interfases Wiegand

Temperatura de operación -35° a 65° C
Humedad de operación 5-95% humedad relativa no condensada
Distancia de cable Wiegand: 150m</td>
<td> 
$250 Dls</td>
</tr>
<tr>
<td>iClass R30.

Ideal para aplicaciones de control de acceso pues combina el mayor rango de lectura de proximidad de 13.56MHz de las credenciales iClass con la tecnología de</td>
<td>
<table>
<tr><th>Distancia de lectura</th><th>Credencial</th><th>Distancia máx.</th></tr>
<tr><td>iClass Card</td><td>11.4 cm</td></tr>
<tr><td>iClass Key</td><td>2.5 cm</td></tr>
<tr><td>iClass Tag</td><td>2.5 cm</td></tr>
<tr><td>iClass Prox</td><td>5.0 cm</td></tr>
<tr><td>MiFARE Card</td><td>5.0 cm</td></tr>
</table>
</td>
<td> 
$700 Dls</td>
</tr>
</table>

<table>
<tr>
<td>credencial inteligente.

Lectoras y credenciales requieren llaves que empaten para operar. Toda transmisión entre lectora y credencial es cifrada utilizando un algoritmo seguro. análisis posterior.

iClass R40

Ideal para aplicaciones de control de acceso pues combina el mayor rango de lectura de proximidad de 13.56MHz de las credenciales iClass con la tecnología de credencial inteligente.

Lectoras y credenciales requieren llaves que empaten para operar. Toda transmisión entre lectora y credencial es cifrada utilizando un algoritmo seguro.

iClass RK40.

Autentificación dual con credencial y PIN personal. Configurable a utilizar PIN solo o credencial sola.

El modelo RK40 es lectora solamente de</td>
<td>Tamaño 8.38 X 12.19 X 2.16 cm

Llaves de autentificación de 64 bits.

Instalación Interiores & exteriores

Interfases Wiegand

Distancia de cable Wiegand: 150m.

Distancia de lectura

<table>
<tr><th>Credencial</th><th>Distancia máx.</th></tr>
<tr><td>iClass Card</td><td>11.4 cm</td></tr>
<tr><td>iClass Key</td><td>2.5 cm</td></tr>
<tr><td>iClass Tag</td><td>2.5 cm</td></tr>
<tr><td>iClass Prox</td><td>5.0 cm</td></tr>
<tr><td>MiFARE Card</td><td>5.0 cm</td></tr>
</table>

Tamaño 8.38 X 12.19 X 2.16 cm

Seguridad

Llaves de autentificación de 64 bits.

Instalación Interiores & exteriores

Interfases Wiegand

Distancia de lectura

<table>
<tr><th>Credencial</th><th>Distancia máx.</th></tr>
<tr><td>iClass Card</td><td>10.1 cm</td></tr>
<tr><td>iClass Key</td><td>3.8 cm</td></tr>
<tr><td>iClass Tag</td><td>3.8 cm</td></tr>
<tr><td>iClass Prox</td><td>6.3 cm</td></tr>
<tr><td>MiFARE Card</td><td>5.0 cm</td></tr>
</table>
</td>
<td> 
$700 Dls</td>
</tr>
</table>

credencial HID iClass y/o PIN. **El modelo RWK400 tiene además la habilidad de escribir datos en la credencial HID iClass del usuario.**	**Tamaño 8.38 X 12.19 X 2.286 cm** **Corriente** **72mA promedio/244mA pico a 12VDC** **Instalación Interiores & exteriores** **Interfases Wiegand** **Puerto configurable RS232 o RS485** **Distancia de cable** **Wiegand: 150m** **RS232: 15m** RS485: 1,220m	 $750 Dls
Equipo	Ventajas	Imagen y Costo
Proxpro y teclado **Entryprox.**	**Radiofrecuencia 125KHz** **Tamaño 12.7 X 12.7 X 2.54 cm** **Alimentación 10-28.5 VCD** **Corriente** **100mA promedio/120mA pico a 24VDC** **Color de cubiertas Gris y beige** **Seguridad** **Reconoce formatos de credencial de hasta 84 bits** **Instalación Interiores & exteriores** **Interfases Wiegand** **Clock & Data (magnetic stripe)** **RS232** **RS422** **Temperatura de operación -30° a 65° C** **Humedad de operación 0-95% humedad relativa no condensada**	 $750 Dls

	Distancia de cable Wiegand: 150m **Clock & Data: 152m** **RS232: 15m** **RS422: 1,219m** **Radiofrecuencia 125KHz** **Tamaño 13.33 X 6.98 X 4.1 cm** **Alimentación 10-15 VCD** **Corriente 150mA promedio/120mA pico a 12VDC** **Seguridad** **Permite hasta 2,000 credenciales o TAGs HID con formatos de hasta 37 bits Se digita un número de empleado, luego se presenta la credencial o TAG.** **Interfases Wiegand** **Clock & Data (magnetic stripe)** **RS232** **RS422** **Temperatura de operación -35° a 66° C** **Humedad de operación 5-95% humedad relativa no condensada** **Distancia de cable Wiegand: 152m**	 $400 Dls

Tabla A.5.- Lectoras HID para sistemas de control de acceso.

- **Lectoras honeywell**

Equipo	Ventajas	Imagen y Costo
OP10HONE. Mini lectora.	**Mini Lectora.** *** Rango de lectura 2" - 5"** *** Alternativa a la HID ProxPoint** *** Salida de tamper, se activa cuando la lectora se retira de la pared o superficie de montaje** *** Tornillos de montaje**	 **$127.00 Dls.**

	ocultos *** Viene con 3 caratulas de color negro, blanco y gris.**	
OP40HONE. Mini lectora.	**Lectora Tradicional.** *** Rango de lectura 2" - 5"** *** Alternativa a la HID ProxPoint** *** Salida de tamper, se activa cuando la lectora se retira de la pared o superficie de montaje** *** Tornillos de montaje ocultos** *** Viene con 3 caratulas de color negro, blanco y gris.**	 **$154.00 Dls.**
OP30HONE. Mini lectora.	**Mini para instalación en Caja Eléctrica.** *** Rango de lectura 2" - 5"** *** Alternativa a la HID ProxPoint** *** Salida de tamper, se activa cuando la lectora se retira de la pared o superficie de montaje** *** Tornillos de montaje ocultos** *** Viene con 3 caratulas de color negro, blanco y gris.**	 **$184.00 Dls.**
OP90HONE. Mini lectora.	**Lectora Resistente, Anti vandálica.** *** Alternativa Keri y PAC** *** Aleación de Zinc** *** Utiliza tornillos de seguridad** *** Aprobación UI294 pendiente.**	 **$442.00 Dls.**

Tabla A.6.- Lectoras Honeywell para sistemas de control de acceso.

POW-R-MAG™

Equipo	Ventajas	Imagen y precio
Chapa magnética de uso rudo, ahorra energía al absorber menos corriente **PMG-1200** **PM-600.** **PM-400PM** **Seleccione el módulo de acuerdo las chapas eléctricas que instale.** **SYSM-4L. Montaje tipo L para PM-400DM** **SYSM-4Z. Montaje tipo Z para PM-400DM.** **SYSM-6L. Montaje tipo L para PM-600.** **SYSM-6Z. Montaje tipo Z para PMG-600 .** **SYSM-6PC. Montaje tipo L para PMG-600PC.** **SYSMG-8Z. Montaje tipo Z para PM-1200.**	**Construcción sellada con materiales de alta calidad. Con componentes de estado sólido, sin partes movibles, una vez instalada olvídese del mantenimiento.** *** También en interiores por su presentación y apariencia.** *** Montaje universal para ser colocada en posición vertical, horizontal.** *** Aluminio anodizado resiste a la corrosión.** *** Desempeño continuo en cualquier voltaje desde 12VCD a 24VCD/CA.** *** Tiempo de apertura 0.3 segundos.** *** Fabricado 100% en Estados Unidos.** **Chapa magnética con fuerza de sujeción de 544 Kgs. Voltaje desde 12VCD a 24VCD/CA. Dimensiones: 26x6.35x3.5 cm.** **Chapa magnética con fuerza de sujeción de 272 Kgs. Voltaje desde 12VCD a 24VCD/CA Dimensiones: 21x6.35x3.5 cm.** **Chapa magnetica con fuerza de sujeción de 181 Kgs. Voltaje desde 12VCD a 24VCD/CA. Dimensiones: 16x5.1x2.5 cm.**	 **$293.00 Dls.** **$191.00 Dls.** **$169.00 Dls** **$9.00 Dls.**

Tabla A.7.- Chapas POW R MAG para sistemas de control de acceso.

Equipo	Ventajas	Imagen y precio
S6514LMKM32D. **Cerradura eléctrica.**	*** Ajustable en campo sin necesidad de herramientas especiales** *** Para puertas de marco de aluminio madera y metal** *** Ideal para centros comerciales, industrias, instituciones médicas, oficinas, etc.** *** Seleccionable en campo el modo de operación (abierto o cerrado).** *** Selección de operación de voltaje de 12VCD o 24VCD y de 12-24VCA** *** Ajuste horizontal para alineamiento en la puerta** *** Switch de monitoreo del estado de la puerta** *** Listada UL 1034.**	 **$185.00 Dls**
14BS-0526D. **Contrachapa eléctrica.**	*** Operación de 12 VCD / VCA.** *** Consumo máximo de 250m Amp.** *** Dimensiones 3.17 x 14.9 cm.**	 **$79.00 Dls.**
11BS-0526D. **Contrachapa eléctrica.**	*** Operación de 12 VCD / VCA.** *** Consumo máximo de 250m Amp.** *** Dimensiones 3.5 x 8.9 cm.**	 **$65.00 Dls.**
8371. Chapa magnetica 750 lbs (340kg).	**Chapa Magnética.** *** Sin magnetismo residual.** *** Acabado eficiente (bien pulido para mejorar abrasión entre sí).** *** Terminal de conexión de tornillo para cable hasta calibre 16 en el interior** *** Fabricada en aluminio anodizado claro** *** Fuerza de retección de la chapa confiable** *** Voltaje de operación y**	 **$232.00 Dls.**

	consumo de 12 VCD, 520 mAmp. o 24 VDC 260 mAmp. (seleccionable por jumper) * Tornillos de seguridad incorporados para facilitar la instalación en el montaje * Bracket ajustable * Dimensiones 23.8 x 4.3 x 2.5 cm.	
GB8112. Para puertas de ½" de grosor utilizando chapa con fuerza de sujeción de 1200 Lbs. GB7112. Para puertas de ½" de grosor utilizando chapa con fuerza de sujeción de 600 Lbs. GB8134. Para puertas de ¾" de grosor utilizando chapa con fuerza de sujeción de 1200 Lbs	**Bracket para Puertas de Vidrio. * Para utilizarse con chapas magnéticas (no incluida) * Acabado pulido para mejorar sujeción entre si. * Tornillos de seguridad para facilitar la instalación en el montaje. * Bracket ajustable. * Dimensiones: 23.8 x 4.3 x 2.5cm.**	 **$128.00 Dls. $128.00 Dls. $113.00 Dls.**

Tabla A.8.- Equipos RCI para sistemas de control de acceso.

- Tarjetas HID.

Equipo	Ventajas	Imagen y Costo
ISOProx II Credencial de acceso programable con proximidad por radiofrecuencia .	**Radiofrecuencia 125KHz Distancia de lectura** **Lectora / Distancia máx.** **MiniProx 12.5 cm ThinLIne II 12.5 cm ProxPoint Plus 6.25 cm ProxPro 17.5 cm MaxiProx 50 cm Tamaño 5.4 X 8.57 X 0.084 cm Material Laminado de polivinilo - Polyvinyl chloride (PVC)**	 **$2.5 Dls**

ProxCard II

Números de ID

Definibles por el cliente

Compatibilidad
Con todas las lectoras de proximidad HID
Formato
Soporta hasta 85 bits, para más de 137,000 millones de códigos.
Imprimible Sí

Radiofrecuencia 125KHz

Distancia de lectura

Lectora	Distancia máx.
MiniProx	14 cm
ThinLIne II	14 cm
ProxPoint Plus	7.5 cm
ProxPro	20 cm
MaxiProx	60 cm

$2.0 Dls

iClass Card.

Credencial de acceso programable con proximidad por radiofrecuencia. Más económica que la ISOProx II.

Compatibilidad
Con todas las lectoras de proximidad HID
Número impreso
En el exterior de la credencial para facilidad de administración
Formato
Soporta hasta 85 bits, para más de 137,000 millones de códigos.
Imprimible No
Radiofrecuencia 13.56MHz
Transmisión de datos
Cifrada entre la lectora y la credencial iClass

Distancia de lectura

Lectora	Distancia máx.
R10	7.6 cm
R30	8.9 cm
R40	11.4 cm
RK40	10.1 cm

$4.00 Dls

	RWK400 10.1 cm **Seguridad** **Con técnica de encriptación estándar se reduce el riesgo de credenciales duplicadas. Se pude incrementar la seguridad con encripción DES o triple DES.** **Almacenamiento** **Múltiples áreas de aplicación separadas, cada una protegida por llaves de lectura/escritura de 64 bits.** **Credenciales de 2Kbit (256bytes) y de 16Kbits (2K bytes)** **Material** **Laminado de polivinilo - Polyvinyl chloride** **Formato** **Soporta hasta 85 bits, para más de 137,000 millones de códigos.** **Opciones Banda magnética** **Grabado de numeración externa** **Slot vertical** **Diseño (texto o gráfico)**	

Tabla A.9.- Tarjetas HID para sistemas de control de acceso.

Torniquetes

Equipo	Ventajas	Imagen y Costo
Torniquet box	**Especificaciones técnicas** **. Equipo en acero carbono, con acabado en pintura epoxi de alta resistencia.** **. Sistema con tres brazos en tubo de acero inoxidable pulido** **. Display de cristal liquido con 2 líneas y 16 columnas** **. Teclado numerico y de funciones** **. Memoria no volátil que**	

Kerberos TPB-E01/E02	**mantiene los datos colectados por un año . Comunicación RS232 para distancia de hasta 15 metros. RS485 para distancia de hasta 1,500 metros TCP/IP (opcional) . Permite conectar hasta 32 equipos en una misma puerta serial del microcomputador. . Alimentación 110v o 220 v 50/60 Hz . Consumo 20 W . Dimensiones 283 mm de ancho 1045 mm de longitud 970 mm de altura 745 mm total de ancho (tapa y brazo)**	
Molinete Informatizado		 $3,600 Dls
Molinete Electromecánico 1	**• Gabinete de Acero Inoxidable o Acero Carbono. - • Soporta diversas configuraciones: Biometría, Código de barras, proximidad o magnético. Identificación exacta de usuarios • Mantenimiento simplificado**	

El modelo TOMSED TUT 60S	**• Bajo Costo** **• Gran durabilidad** **• Plataforma Opcional** **• Pedestal de sustentación en acero tratado con pintura en E-POX**	 $1,850 Dls $2,000 Dls (con lector prox)
El modelo TOMSED TUT-60	**Opera en forma mecánica o electrónica. El mecanismo de uso rudo es ideal para las condiciones de alto volumen y a usos que se relacionan con estadios, arenas y otras aplicaciones para admisión de multitudes. Cada torniquete mecánico cuenta con un registro de 5 dígitos para poder dar un control preciso y confiable de los asistentes.** **Opera en forma electrónica y está diseñado para hacer interfase en forma sencilla con cualquier instrumento de control de accesos. El sistema de control incluye una fuente de voltaje de 24 VDC. El torniquete puede ser: para ingreso controlado, control de ingreso sin salida, salida libre o entrada y salida controladas. Se puede tener cualquier combinación de cerrado o abierto en caso de falla.**	 
Barrera Vehicular Armex 3 mts.	***mecanismo*: motor a reductor por medio de banda con opción a cadena; transmisión por medio de brazos tipo biela a eje con chumaceras** ***gabinete* : lamina de acero al carbón calibre 11 tapas superior y trasera cal 18** **Acabado galvanizado mas pintura electrostática poliuretano o poliéster color amarillo llama y crema con opción a otras combinaciones sobre pedido.** **Gabinete opcional en acero inoxidable.**	 $ 1850 Dls

	tamaño: **alto 105 cm , ancho 35 cm, largo 32 cm, brazo: 3.0 – 3.5 m.** ***peso*****: 50 kg aprox.** **características *eléctricas:*** ***Alimentación:*** **110 volts a.c.** ***Motor:*** **monofasico 110 volts 1/4 h.p.** ***control:*** **control lógico programable crouzet millenium 3 con display iluminado con fecha, hora, conteo de vehículos, y diagnostico en pantalla. relevador de estado sólido accionamiento de motor** **salidas: 24 volts 1.9 amp. para fotoceldas, lectora, camara de cctv buzer, loop de piso etc.** **entradas: n/a para recibir pulso de activacion desde dispositivo ya sea, lectora, teclado, boletera, etc.** **n/a para recibir pulso de push bottom para activación manual o de emergencia.** **n/a para fotocelda o loop de piso** **n/a pulso de dispositivo de seguridad como fotocelda auxiliar** **Tiempo de apertura: 1.8 segundos aprox.** **características *mecánicas:*** ***mecanismo*****: motoreductor con usillo a brazo retractil tipo tijera** ***carcaza*** **: acero al carbón con aplicaciones de acero inoxidable con opción a otros materiales y**	

Barrera Retractil CIDEP 3 mts	**acabados de acuerdo a pedido.** **con montaje independiente al mecanismo** ***tamaño:*** **alto 105 cms , ancho 32 cms, largo 50 cms, brazo: 2.5 – 2.9 mts** ***peso*****: 45 kgs aprox. (dependiendo de la carcaza)** **características *eléctricas:*** ***alimentación:*** **110 volts** ***motor:*** **1/4 h.p.** ***control:*** **control lógico programable crouzet millenium 3** **salidas: 12 volts 1.9 A. para foto celdas, lectora, cámara de cctv etc.** **entradas: n/a para recibir pulso de activación desde dispositivo ya sea, lectora, teclado, boletera, etc.** **n/a para recibir pulso de push bottom para activación manual o de emergencia.** **n/a para foto celda o loop de piso** **Tiempo de apertura: 3.5 segundos aprox.**	

Tabla A.10.- Torniquetes y barreras vehiculares para sistemas de control de acceso.

- **BOTONES**

Equipo	Ventajas	Imagen y Costo
SD-7201GCPE1. Botón de salida	**La cara de la placa es de acero inoxidable. Ambas palabras "EXIT" y "SALIDA" están escritas en la placa. Se adapta a cualquier caja de cuadrilla sencilla standard. Botón para presionar en forma de hongo de color verde. Contacto NO/NC con**	 **$ 41.00 Dls**

	capacidad 5A, 125 VAC.	
SD-7101KBPE1. Botón de Salida tipo Push	**Botón de control de acceso normalmente cerrado (terminales tipo ojo). Tapa de aluminio con leyenda de salida y botón fabricado en plástico. Voltaje de operación 12.5 Volts..**	 **$ 12.00 Dls**
940HP-MO. Botón de salida.	**Bóton de Pulso Switch de apertura decorativo. Usado en escritorios y salidas de acceso. Montaje de superficie, de acción momentánea Color beige, discreto y de uso rudo Switch NO / NC con rango de contacto de 10 A 24V. Botón Económico**	 **$ 36.00 Dls**
980-MO. Botón económico.	**Para aplicaciones comerciales donde se requiere pedido de salida con botón sin iluminación.** • **Placa de pared de acero inoxidable calibre 20 para uso en cajas eléctricas estándar** • **Incluye piezas de ferretería para montaje** • **Acción momentánea** • **Switch NO / NC**	 **$ 85.00 Dls**

Tabla A.11.- Botones de acceso para sistemas de control de acceso.

- **FUENTES DE ALIMETACIÓN**

Equipo	Ventajas	Imagen y Costo
ELK-960. Módulo de relevador.	**Módulo económico de relevadores con retardo de tiempo.** *** Alimentación de 12 a 24 VCD** *** Relevador de tipo industrial de 7 A 30VCD / 10 A. 125VCA**	

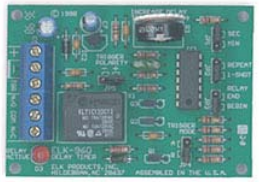
ELKP624. Fuente de alimentación con cargador de batería.	*** Estado inicial del relevador seleccionado por ON/OFF** *** Tiempo de retardo del relevador de 1 a 60 s y de 1 a 60 min** *** El triger puede soportar hasta 4.5 Volts.** **Fuente de alimentación 1.2 A con Cargador de Batería.** *** Protección de sobrecarga autoreseteable** *** Indicadores de alimentación visual de CA y CD** *** Entrada de alimentación de 12, 16.5 y 24VCA de 40VA para obtener una salida seleccionable de 6, 12 ó 24VCD** *** El cargador de baterías tiene una salida de 12VCD y de 1.2 Ah a 10Ah** *** Supresión de flujos de voltaje de CA o CD.**	 **$30.00 Dls.**
Baterías para Respaldo. **WP712.** **WP4512.** **WP1.212.**	**12 VCD, libres de mantenimiento a base de plomo ácido.**	 **$24.00 Dls.** **$17.00 Dls.** **$13.00 Dls.** **$8.00 Dls.**

Tabla A.12.- Fuente de alimentación para sistemas de control de acceso.

- **Cable para Sistemas de Control de Acceso.**

Equipo	Ventajas	Imagen y Costo
COMPOSITE-CABLE. **COMPOSITE-CABLE/1000**	**Cable multiconductor para sistemas de control de acceso. 5 pares de conductores calibre 22 para lectora, sensores, chapas y un par calibre 18 para alimentación.**	**$3.85 Dls./Mt** **$1,019.00 Dls.**

	Caja de 305 m. de cable multiconductor para sistemas de control de acceso.	

Tabla A.13.- Cable para sistemas de control de acceso.

B. Configuración del panel.

Comenzaremos con el software para el panel de control de acceso, este software está basado en una estructura de cliente-servidor, por lo que es necesario primeramente instalar el software servidor para después conectar a el los clientes.

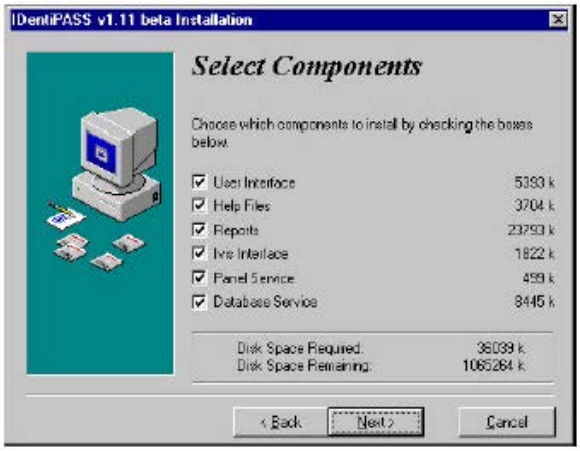


Figura B.1 Instalación del software para el panel IDentipass.

Dentro del proceso de instalación del servidor es necesario señalar cada una de las opciones mostradas, las cuales son:

- User Interface: Es el programa cliente que permite administrar, configurar y monitorear el sistema.
- Help Files: Son los archivos de ayuda que componen el manual del software.
- Reports: Son todos los tipos de reportes que puede generar el sistema referente al acceso de los usuarios y reportes internos del sistema
- Ivis Interface: Es un pequeño software incluido que permite al usuario del sistema diseñar e imprimir credenciales

Dentro de software podemos tener algunas funciones que nos servirán para poder agregar a los usuarios a sus áreas de trabajo o los lugares en los que pueden tener acceso, así como la capacidad de habilitar un lector dentro del panel o otros elementos o los puertos que van a ser ocupados por la computadora y el panel. A continuación se muestran algunas de las funciones con las que cuenta el software de Identipass LT.

Agregar un site: SITE es la localización de tu base de dato ODBC. Puede ser una computadora o una conexión interna. Identipass LT permite instalar una base de datos, un panel de servicio y 4 interfaces. Para añadir tu Site, la computadora tiene que sostener la base de datos y sondear los paneles, con un clic izquierdo en el Mouse sobre SITE sobre el menú principal y como seleccionar a la computadora que se va utilizar como SIte.

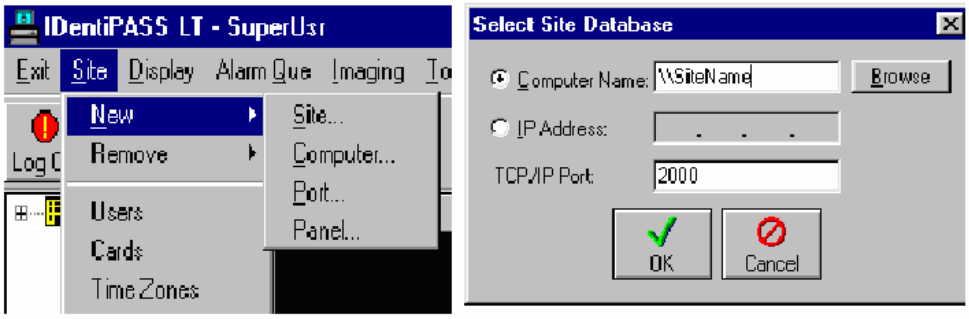


Figura B.2 Agregar un Site para el panel IDentipass.

Con el menú figura 4.13 también se puede agregar varias computadoras y puertos para la comunicación entre el panel y la computadora.

De la ventana se puede escoger los tipos de dispositivos, puertos y velocidad en la conexión. Los tipos de dispositivos que pueden ser seleccionados son: 9000 paneles o NetLink.

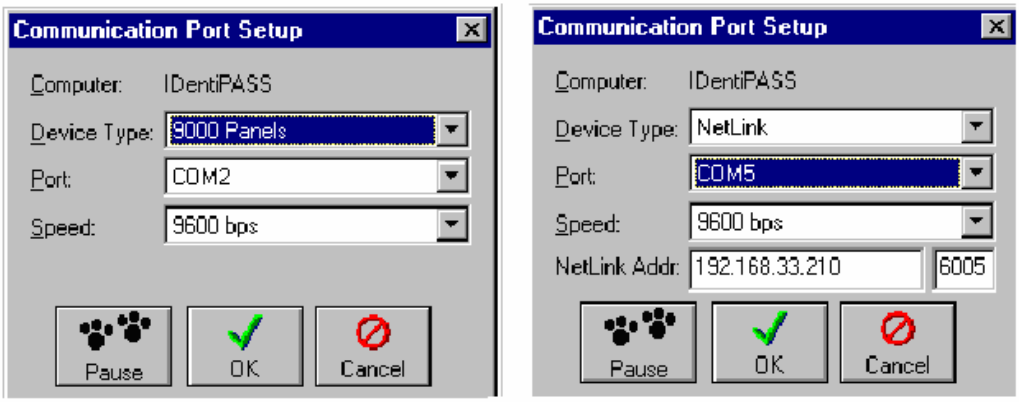


Figura B.3 Comunicación y configuración del puerto del panel.

Un puerto puede ser removido con un clic derecho en el nombre del puerto sobre el árbol del Site, y abre el menú del site después seleccionar Remove Port de este menú. Es el mismo procedimiento para añadir un panel.

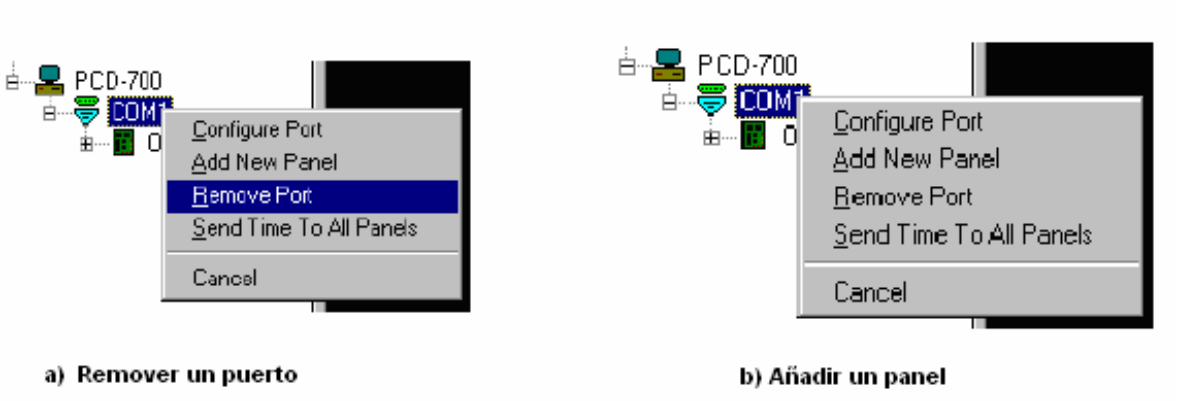


Figura B.4 Añadir y Remover un puerto del Site.

O también un panel puede ser añadido a través del menú principal

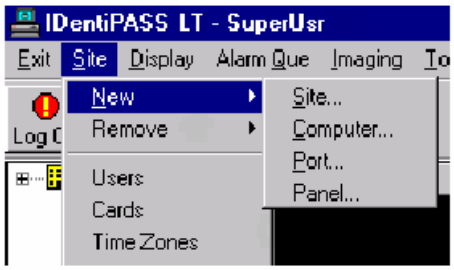


Figura B.5 Añadir un puerto a través del menú principal.

Rellenar en el nombre de panel y la comunicación apropiada para el panel, por default. Y salvar la configuración del panel.

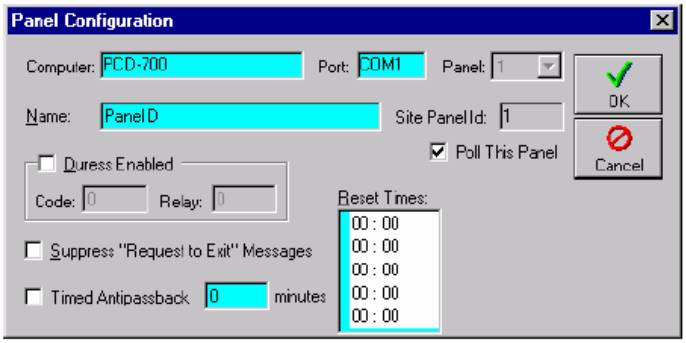


Figura B.6 Configuración del panel.

B.1.- Configuración de MODEM

EL MODEM Identipass MODEM es utilizado por cualquier panel de la serie 9000 o siguientes. Y antes de poder usar este software necesita tener:

- Cable (RS- 232) para el MODEM
- El cable para el puerto serial
- Este software instalado en su computadora

Instrucciones de programación.

1. Instalar el IDenticard MODEM programmer en su sistema de la computadora.
2. Conectar cada MODEM con su respectivo cable (RS- 232)

3. Conecte los MODEM a su cable de toma de corriente.
4. Encienda el interruptor del MODEM
5. Abra el software de IDenticard MODEM. La pantalla principal aparecerá como se muestra abajo.
6. Determine que MODEM este bien conectado en la computadora al igual que el panel.
7. Conecte el cable del MODEM que desea programar al puerto serial.

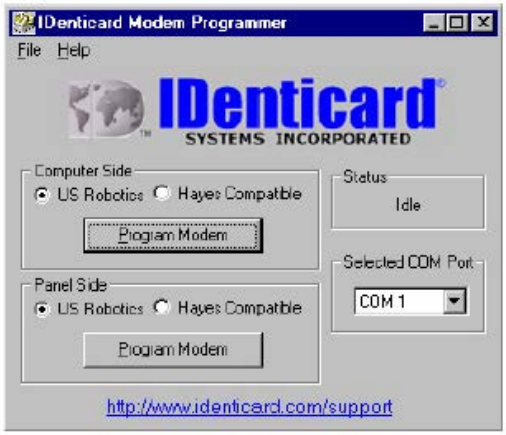


Figura B.7 Configuración del MODEM.

B.2.- Configuración de panel Dial-UP

Rellena en el nombre del panel Dial- Up. Añadir un número telefónico al panel: Las siguientes ventas son requeridas para añadir un MODEM en el panel.

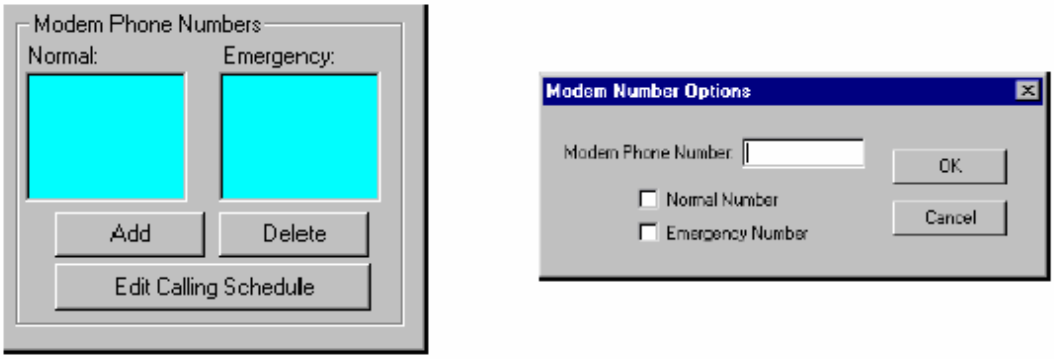


Figura B.8 Añadir número telefónico al panel.

Añadir un lector: Para añadir un lector, se da doble clic sobre el nombre del panel en el Site Tree cuando el lector ese conectado o un click izquierdo sobre el Plus Sign siguiente al nombre del panel para expandir el panel.

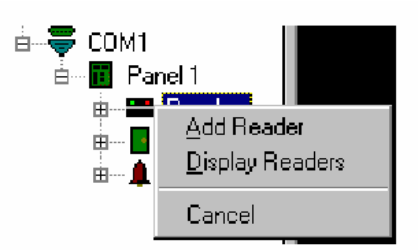


Figura B.9 Añadir un lector a la Configuración del Panel DIAL - UP.

Un click derecho sobre el lector y después un click izquierdo para añadir el lector. Esto te llevara a la ventana de lectores. Con esta ventana tienes la habilidad de ajustar las características de tu lector.

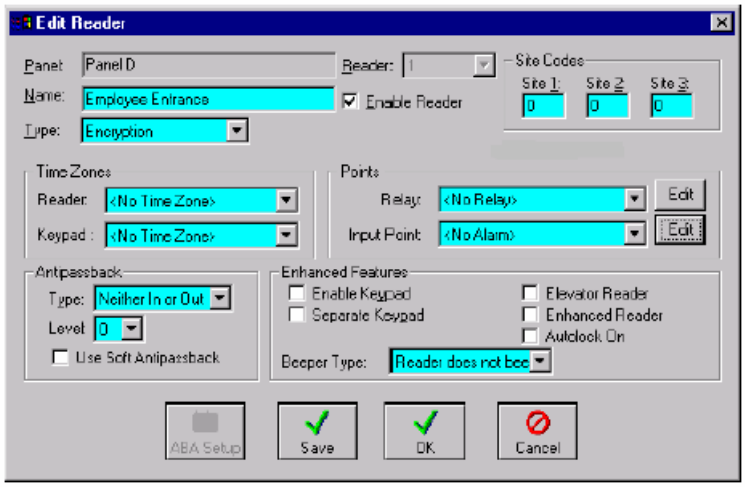


Figura B.10 Configuración del Lectoras.

Añadir un RELAY: Para añadir un relay al panel, expandir el Site Tree para el nivel del panel, Dar un click derecho sobre Relays y escoger añadir el panel. Esto te llevara a ala ventana de relay para poner sus características

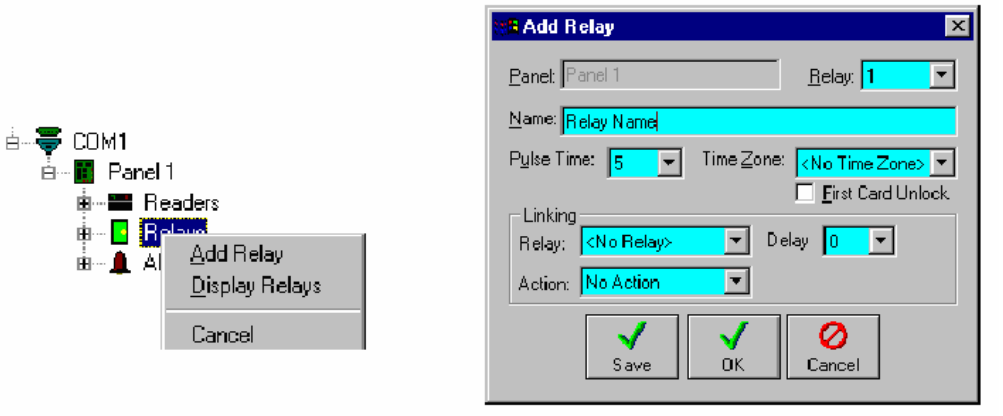


Figura B.11 Configuración del RELAY Panel DIAL - UP.

Añadir una alarma: Para añadir una alarma, se da un click derecho sobre alarmas bajo el nombre del panel y escoger “ADD INPUT POINT”. Este te llevara a la ventana añadir alarma.

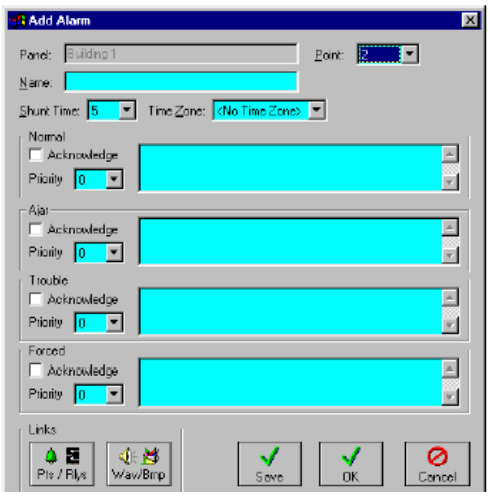


Figura B.12 Configuración de la alarma para el Panel DIAL - UP.

Añadir a los Usuarios: Para añadir un usuario debes dar un doble click izquierdo sobre usuarios en el Site Tree el menú del site y escogerás botón de usuarios hasta arriba de la pantalla. Esto te llevara a la ventana de User Manager. Del lado izquierdo de la pantalla estar una lista de usuarios y del lado derecho de la pantalla una lista de los grupos. Un usuario del mismo grupo tiene los mismos derechos

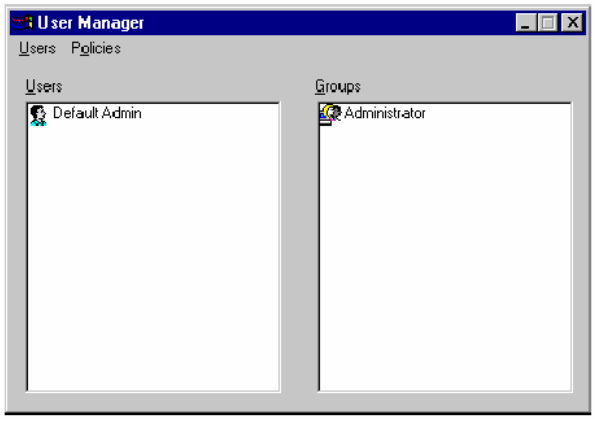


Figura B.13 Añadir Usuarios.

Para añadir un usuario a un grupo: escoge un grupo de o un nuevo grupo. Esto te llevara a la ventana de añadir grupos. Y seleccionaras las características del usuario

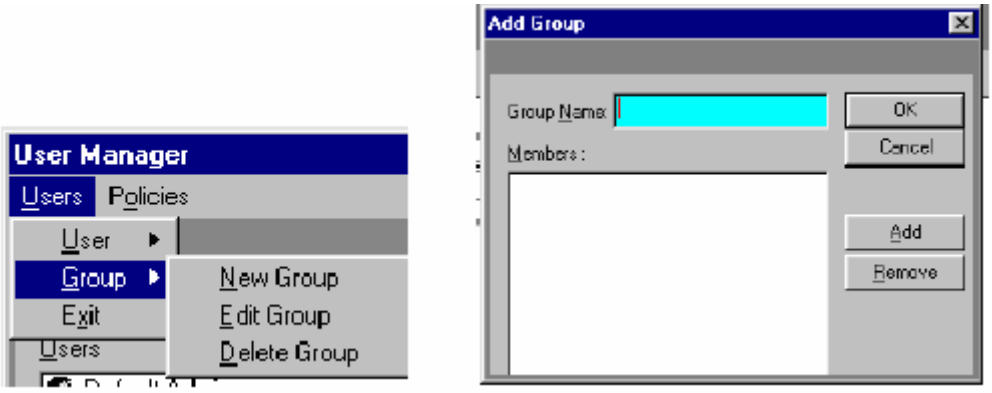


Figura B.14 Añadir a un usuario a un Grupo.

Con el siguiente menú se puede asignar los derechos con los que va a contar el usuario.

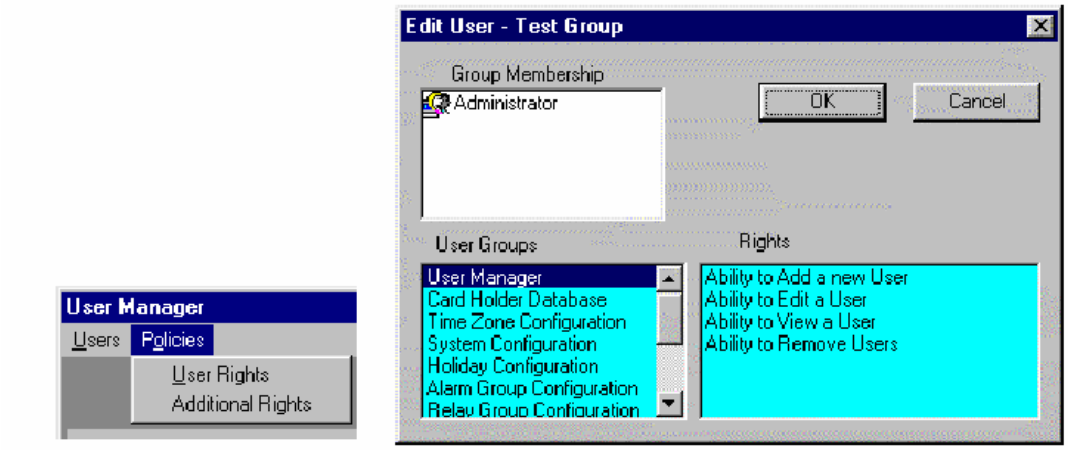


Figura B.15 Añadir Derechos a un usuario.

También se puede agregar a un usuario a un cierto grupo y agregarle más o menos derechos dependiendo de las condiciones que se desea tener.

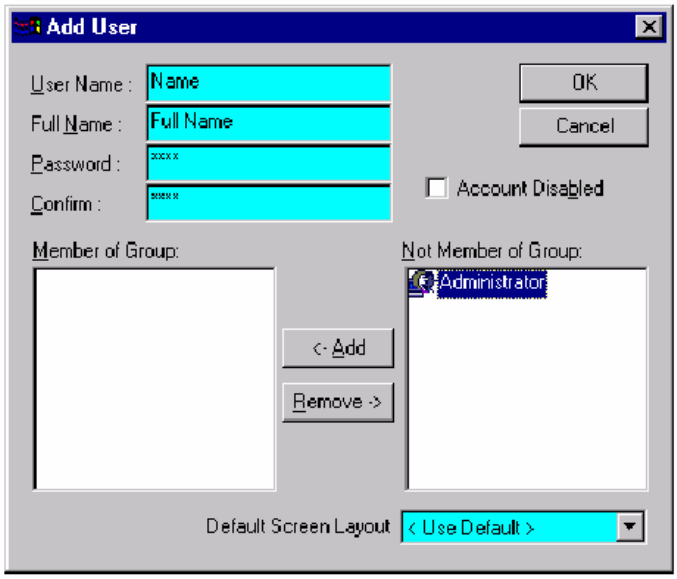


Figura B.16 Añadir a un usuario a un Grupo.

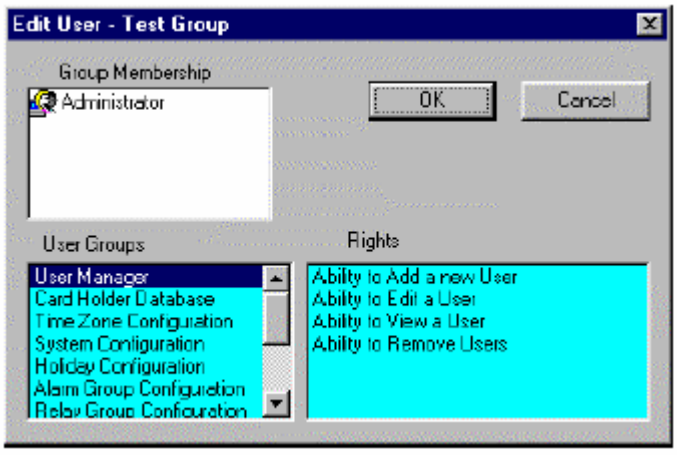


Figura B.17 Añadir a un Grupo ciertos derechos.

B.3.- Configuración de LANTRONIX

El dispositivo Lantronix UDS 10/00 es un convertidor serial/ethernet que utilizaremos para integrar los paneles de control de acceso a la red interna de DSCA, lo que permitirá una mejor administración.

Antes de comenzar es necesario que se haya instalado en la computadora en la que se desea configurar el lantronix el software Device Installer que viene en el disco de instalación del lantronix y/o en el disco que yo deje. También es necesario que se instale la versión 1.1 de Microsoft NET Frameworks o la versión más actual que viene incluida en el disco que deje en caseta 2.

RECOMENDACIÓN: Que el Device Installer y el Frameworks se instalen en el mismo servidor en el que esta el software identipass.

Una vez instalado el Device Iinstaller se ejecuta y aparecerá una ventana como la siguiente:

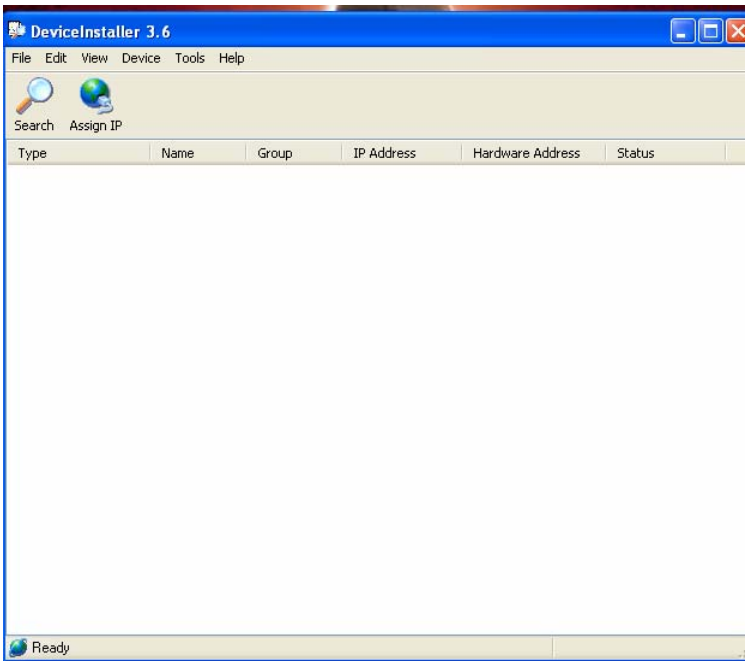


Figura B.18 Configuración del Lantronix.

Una vez que aparece esta ventana se da un click en el icono de Assign IP (el que tiene un mundo). Inmediatamente después aparecerá la siguiente pantalla:

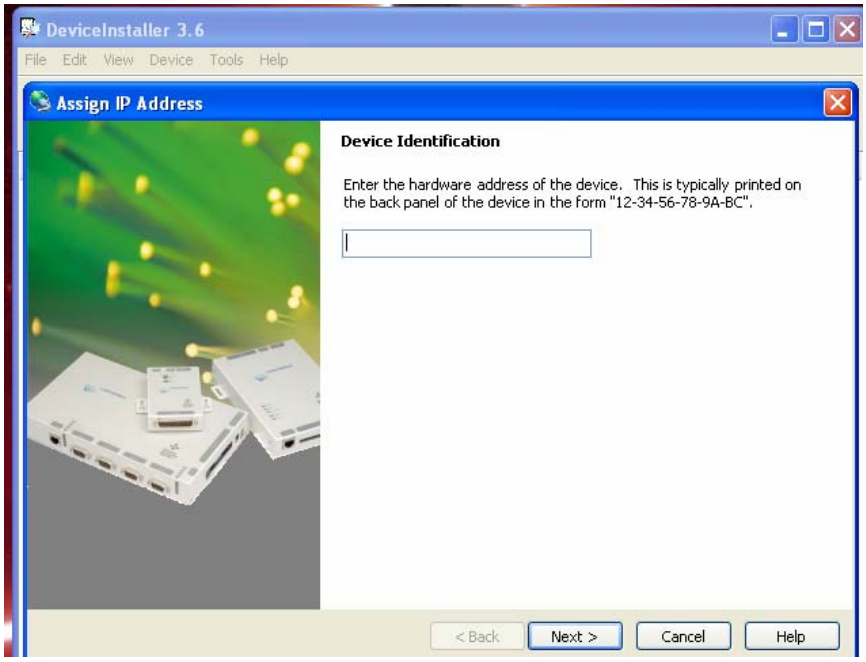


Figura A.19 Dirección del lantronix.

En el renglón en blanco hay que teclear la dirección física del lantronix (su MAC Address); dicha dirección se puede observar en una etiqueta que se encuentra atrás del lantronix, ejemplo: 00-20-4A-67-99 (se debe teclear la dirección completa con todo y guiones).

Después se da un click en next; aparecerá otra ventana en donde hay que seleccionar Assign a specific IP Address. Después de un click en siguiente y aparecerá la siguiente ventana:

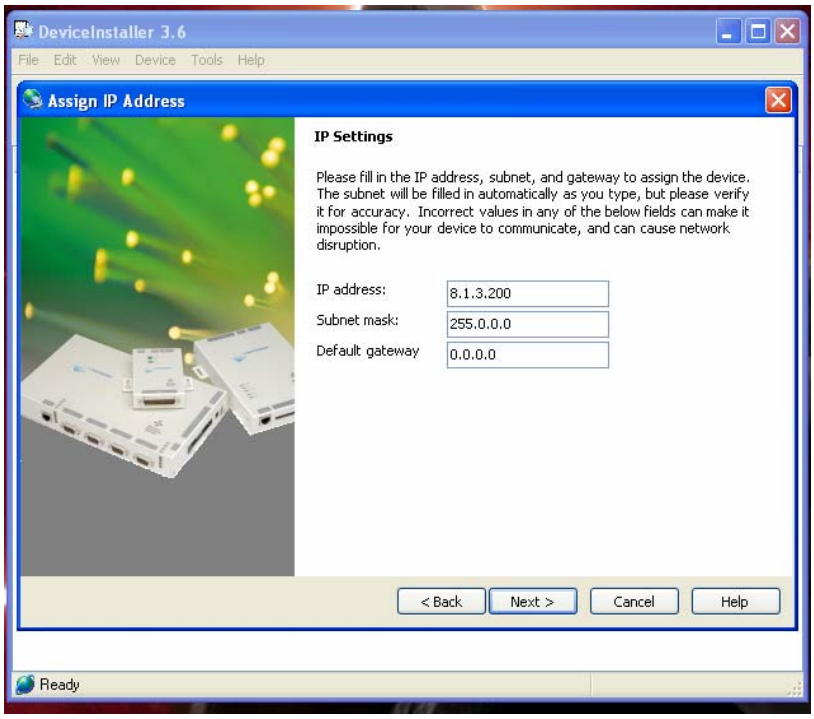


Figura B.20 Dirección IP del Lantronix

Hay que llenar los espacios con la dirección IP que va a tener el dispositivo, en este caso la dirección es 8.1.3.200 para el panel 1 y 8.1.3.201 para el panel 2. La máscara es 255.255.255.0 y el gateway es 8.1.3.1

Si se da ahora un clic al botón de search aparecerá el dispositivo con la dirección IP que se le dio y el status de online.

Después para finalizar hay que seleccionar el dispositivo y dar un click al icono de telnet y sin mover nada dar un click en Ok.

Aparecerá una ventana de entorno de MS-Dos como la siguiente (hay que teclear Enter).

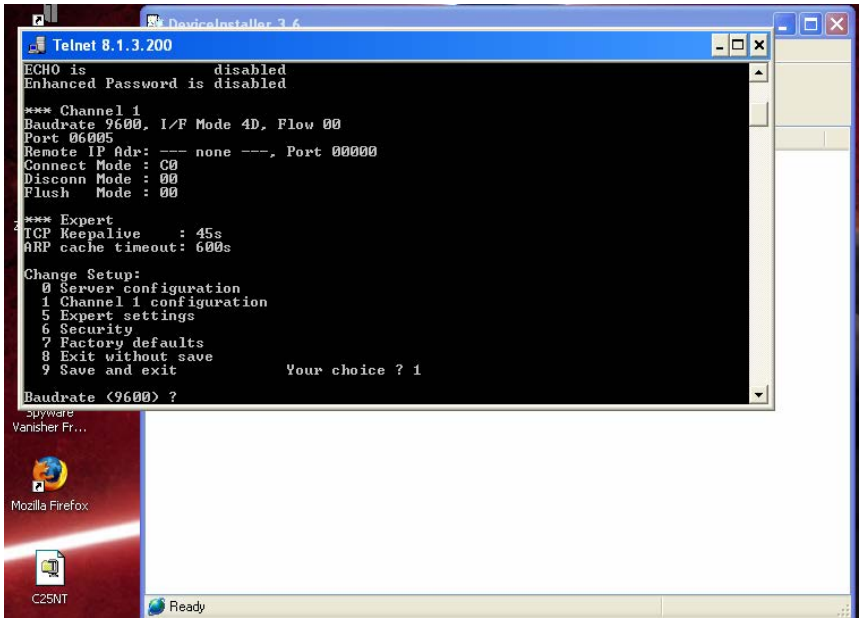


Figura B.21 Seleccionamos el equipo LANTRONIX.

Se escoge la opción 1 y se da Enter a las opciones que aparecen (sin modificar nada) hasta que aparezca la siguiente opción: Port No ahí se escribe el siguiente número 6005 y se da enter, a las siguientes opciones se les da enter

hasta que aparezca de nuevo el menú, se selecciona la opción 9 y el lantronix ha sido configurado correctamente, ya se pueden cerrar la ventana de MS-Dos y la ventana del Device Installer.

Con la instalación del Latronix hemos finalizado la parte de instalación del software con lo que concluimos la tercera parte de la implementación del sistema de control y se procede a dar la capacitación y entrega del proyecto.

B.4.- Resetear panel del control.

Existe una consideración importante en caso de un problema mayor y es; si es necesario resetear el panel

El reseteo de un panel de control de acceso debe hacerse con cuidado y solo en el caso de que el panel no responda (no se comunique con la red o con la pc) o que haga alguna cosa extraña (que los led's parpadeen de manera intermitente, por ejemplo).

Dar un reset a un panel involucra que el panel pierda toda información que tenía guardada anteriormente, toda la configuración de lectores, credenciales y puertas se pierde, en pocas palabras, lo deja en blanco como salido de fábrica. Por ello es importante que después de que se resetee un panel se le haga una carga (download) desde el software identipass.

Para resetear el panel lo primero que hay que hacer es presionar una vez el botón de reset que se encuentra en la parte superior del panel; si con esto no se soluciona el problema por el cual se le dio el reset al panel se procede entonces a resetear por completo el panel. Para hacerlo se requiere desconectar el eliminador que alimenta al panel, y también se debe desconectar la(s) batería(s) de respaldo que alimenta al panel; una vez hecho esto se tiene que quitar una batería que se encuentra en el panel y que tiene el tamaño de una batería AA. Después hay que esperar de 20 a 30 minutos antes de volver a colocar la batería tamaño AA y conectar la batería de respaldo y el eliminador. Con esto el panel ha sido reseteado y toda la información ha sido borrada.

Inmediatamente después se tiene que hacer una carga al panel de la siguiente manera: se entra en el software Identipass Client y se firma como SuperUsr. Después se selecciona en Options la opción Download; una vez ahí se palomean todos los cuadrados, se selecciona el panel Asistencia en la siguiente columna y después se le da en Start u Ok.

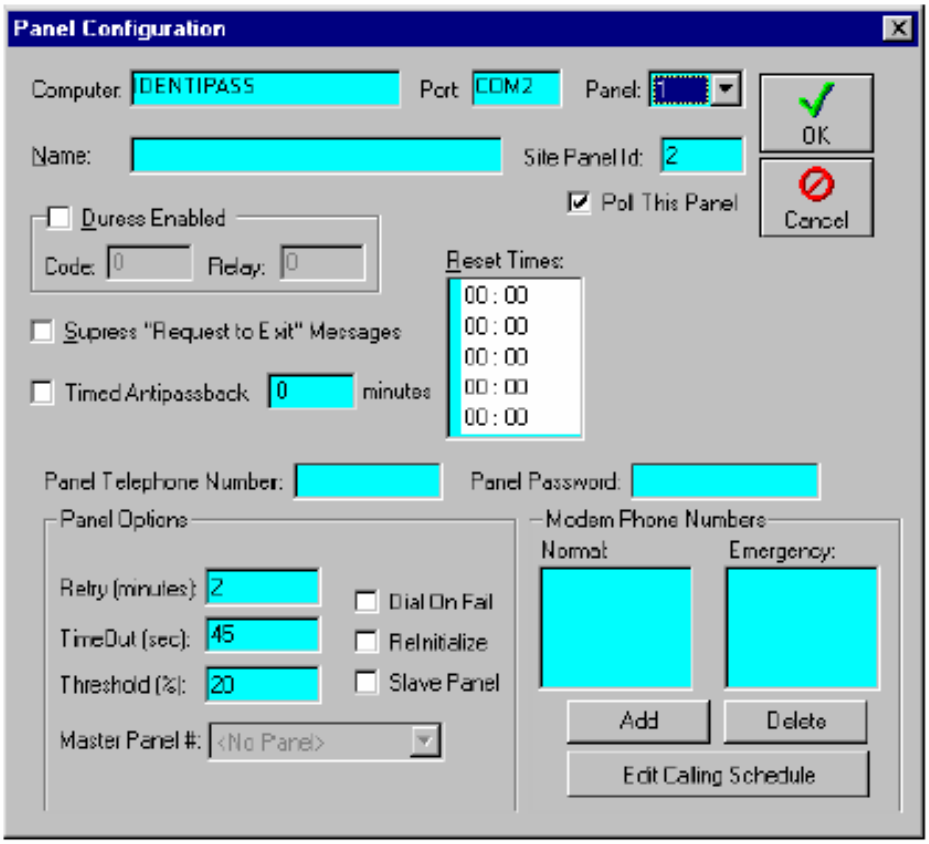


Figura B.4.17 Configuración del Panel DIAL - UP.

Aviso: el password no puede ser cambiado si desea cambiarlo necesita retirar toda la energía de la batería por lo menos 1 minuto. Y resetear el sistema puede resetear todos antipassback.

C. Enrolamiento de huellas del personal.

Para el registro de las huellas digitales de cada usuario dentro del sistema se utilizará el lector biométrico montado en las afueras de la oficina del Director General y el software para el registro de la huella será instalado en la computadora de la recepcionista, quien bajo previa capacitación se encargará de este proceso. En un futuro se evaluará la posibilidad de adquirir un lector biométrico extra con una base para escritorio, para que sea colocado en el escritorio de la recepcionista.

Para enrolar será necesario conectar uno de los lectores biométricos a través de su salida ethernet a la red interna de la empresa, por lo que se le pidió a la empresa colocar un nodo de red cercano al lector. La dirección IP estática con la que será identificada este lector es: 8.1.3.202 (esta dirección se configura en el mismo dispositivo a través de su menú). No es necesario conectar a la red los otros dos lectores biométricos ni asignarles una dirección IP, ya que no se va a transmitir las huellas a estos lectores; porque como se vio en anteriores capítulos,

el registro digital de cada huella se encuentra en la tarjeta inteligente correspondiente a cada usuario.Para enrolar huellas en el sistema se tienen que seguir los siguientes pasos:

1.- Iniciar el software Veriadmin

2.- Dentro del software se configura el lector biométrico (se coloca la dirección IP asignada al dispositivo y se selecciona el tipo de lector: V-smart iClass)

3.- Se selecciona el icono marcado como “Quick enrollment” y aparecerá una ventana como la mostrada en la figura c.1.

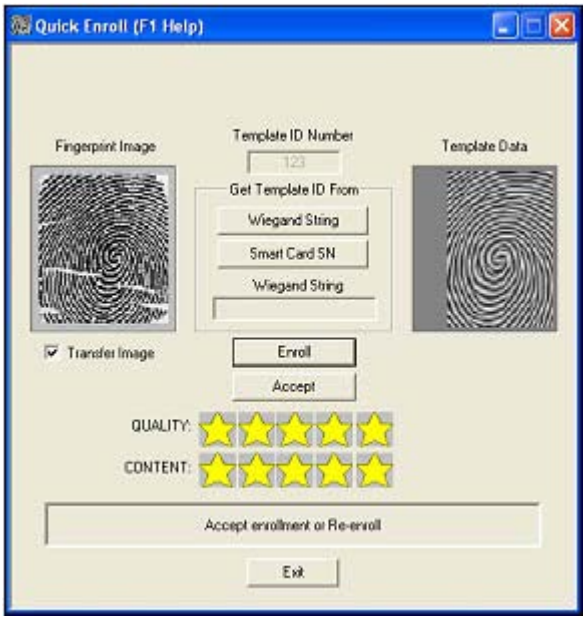


Figura c.1.- Ventana Quick enroll.

4.- Se coloca el dedo en el sensor del lector siguiendo las siguientes recomendaciones:

* Se recomienda el uso del dedo índice, medio y anular; el pulgar y el meñique, ya que el pulgar tiende a ejercer demasiada presión en el sensor y el meñique tiende a ejercer una presión mínima. Si se ejerce demasiada presión se ocasionan manchas en la huella y si se ejerce poca presión el sensor puede no detectar la presencia de un dedo. En cualquiera de ambos casos, la imagen obtenida de la huella tiende a no ser consistente ni confiable. (Figura c.2)

Figura c.2.- Dedos recomendados para el enrolamiento.

* El dedo debe ser colocado tratando de abarcar el área máxima del sensor como se muestra en la figura c.3. Tocar el sensor como si se fuera a presionar un botón crea una imagen del dedo deficiente en información en la representación digital de la huella.

Figura c.3.- Posición correcta e incorrecta del dedo sobre el sensor para el proceso de enrolamiento y verificación.

5.- En la ventana quick enroll se selecciona el botón de Smart card SN para obtener el número de serie de la smartcard. Este número es el que es leído por un lector de tarjeta inteligente convencional y es con el cual se registrará al usuario en el sistema de control de acceso. De esta manera se evita tener a un usuario registrado con dos números diferentes en el sistema de control de acceso.

6.- Después de que aparece el número de serie de la smartcard en la ventana quick enroll, se selecciona el botón enroll y se le pide al usuario mantenga el dedo en el sensor por unos segundos. Una vez hecho esto, el sistema habrá capturado una imagen de la huella digital del usuario y una plantilla o template de la misma huella obtenida a través del algoritmo del lector (Figura c.4).

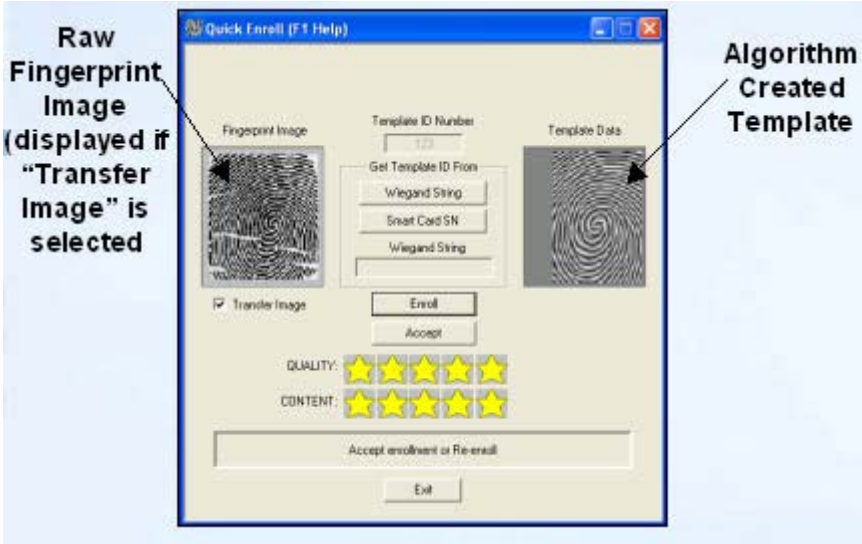


Figura c.4.- Imagen RAW de la huella digital (izquierda de la imagen). Plantilla creada a través del algoritmo (derecha de la imagen).

7.- Antes de aceptar el registro de la huella es necesario checar dos parámetros Calidad (Quality) y Contenido (Content) representados por estrellas en la ventana de quick enroll. La calidad se ve afectada debido a que el dedo no fue centrado correctamente en el sensor o que no abarca la mayor área posible en el sensor; también se ve afectada la calidad debido a la pobre definición de arcos, valles y líneas de la huella digital de la persona, ocasionada por el trabajo, heridas y cortadas. En este caso se recomienda utilizar otro dedo en el registro.

El contenido es la cantidad de información obtenida a través de la imagen que sirve como entrada al algoritmo de creación de la plantilla.

Para obtener una imagen aceptable de una huella digital, se recomienda que por lo menos se tenga 3 estrellas o más en calidad y contenido, si una imagen de la huella tiene 2 estrellas o menos en cualquiera de estos dos parámetros se recomienda volver a enrolar la huella.

8.- Una vez que se obtiene una huella aceptable se da clic en el botón Accept. Se le preguntará al usuario donde desea guardar la plantilla de la huella, teniendo las siguientes opciones: en la computadora, en el lector, o en una smartcard. Se selecciona esta última y se acerca la tarjeta inteligente al lector de smartcard que se encuentra al lado derecho del sensor biométrico. Una vez hecho esto, la plantilla de la huella digital ha quedado guardada en la tarjeta.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

1. Mariano Tapiador Mateos, Juan A. Sigüenza Pizarro , **Tecnologías biométricas aplicadas a la seguridad**, Ed. Alfaomega Ra-Ma, 2005.
2. J. Ashbourn Biometrics: **Advanced Identity Verification,** Springer Verlag, London 2000.
3. A.M. Bazen and S:H Gerz., **Directional field computation for fingerprints Based on the principal Component Analysis of Local Gradients.** In Proc of ProISC2000.
4. Biometric solution for authentication in an E world.
5. Practical Biometrics.
6. Intelligent biometric techniques in fingerprint and face recognition.
7. Biometrics: advanced identity verification: the complete, **Julian Ashbevrn Edit Springer.**
8. Implementing Biometric Security, **John Chirillo, Scout Blaul** Editorial Wiley 1a edición 2003.
9. Access Control Systems: Security, Identity Management and Trust Models ,**Messaoud Benatar** Editorial Springer 1a edición 2005.
10. Administración professonal de proyectos La guía: Una guía práctica para programar el éxito de sus proyectos, **Yamal Chamoun,** Editorial McGraw-Hill Interamericana 2004.
11. Catálogo “Guía de Productos Enero – Junio 2006, **Corporativo INALARM S.A. de C.V.,** Edición no. 3, México D.F.
12. Catálogo de equipos de seguridad Primavera 2006 **Sistemas y Servicios de Comunicación S.A. de C.V. (Syscom),** Talleres Gráficos de Syscom, Chihuahua, México

INTERNET

- http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIOMETRICOS.html (sistemas biométricos)
- http://neutron.ing.ucv.ve/revista-e/No6/Lopez%20Gustavo/Biomert%C3%ADa.html (sistemas biométricos huella)
- http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm (sistemas biométricos)
- http://www.revistasic.com/revista39/agorarevista_39.htm (Biometría)
- www.tiendacapta.com/cat_torniquetes_tomsed.cfm - 64k - (torniquetes)
- http://www.id-digital.com.mx/modules.php?name=Content&pa=showpage&pid=6 (equipos)
- http://www.securitybmg.com/identipass.htm (identipass)
- http://www.identicard.com/e-catalog/SpanishBrochures/CenturionSp.pdf (paneles)
- http://www.hidcorp.com/espanol/products/mifare/ (tarjetas mifare)
- http://www.solucionesbiometricas.com/ (compañías de equipos en general importante)
- http://www.kimaldi.com/ (Equipo de seguridad)
- http://www.intelektron.com/sitioacc/indeacc.htm (Equipo en general)
- http://www.criminalistaenred.com.ar/Lectores%20de%20huellas.html (huella)
- http://www.intelektron.com/sitio/noticias/notas%20de%20%20interes/huellas%20vs%20proximidad.htm (proximidad vs Huella)
- http://www.intelektron.com/sitio/noticias/notas%20de%20%20interes/4.htm (importante viene el cuadro comparativo de las tecnologías)
- http://porsche.ls.fi.upm.es/ProtInfo/Temario/clase2.pdf
- www.biometricgroup.com
- www.cidepsa.com.mx
- www.kimaldi.com/aplicaciones/control_de_acceso
- www.alas-la.org/
- www.monografias.com
- www.biometrics.org
- es.wikipedia.org/wiki/Portada

CD´S

1. - “Bioscrypt Technical Seminar I y II”

Cd de memoria y documentación técnica del curso del mismo nombre impartido en la Ciudad de México en 2005

2. - “HID iclass Certification First level”

Cd de memoria y documentación técnica del curso de certificación del mismo nombre impartido en la Ciudad de México en 2005