

**DISEÑO DE SISTEMA QUE CONTROLE EL ACCESO PEATONAL Y
VEHICULAR EN ZONAS FRANCAS**

ANDRES FELIPE MARÍN LÓPEZ

**UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE AUTOMÁTICA Y ELECTRÓNICA
PROGRAMA INGENIERÍA MECATRÓNICA
SANTIAGO DE CALI
2009**

**DISEÑO DE SISTEMA QUE CONTROLE EL ACCESO PEATONAL Y
VEHICULAR EN ZONAS FRANCAS**

ANDRES FELIPE MARÍN LÓPEZ

**Pasantía para optar al título
de Ingeniero Mecatrónico**

Directores

JORGE IVAN VELANDIA ROMERO

Ingeniero electrónico

OLMES AGUDELO FERNANDEZ

Ingeniero electricista

EDWARD MANJARRES

Teniente retirado

**UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE AUTÓMATICA Y ELECTRÓNICA
PROGRAMA INGENIERÍA MECATRÓNICA
SANTIAGO DE CALI
2009**

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Occidente para optar al título de Ingeniero Mecatrónico

Ing. JIMMY TOMBE

Jurado

Ing. JUAN CARLOS MENA

Jurado

Ing. JORGE IVAN VELANDIA

Director

Santiago de Cali, 4 de Mayo 2009

AGRADECIMIENTOS

Doy gracias a Dios por la fortaleza y ánimo para salir adelante.

A mis padres por brindarme su apoyo incondicional, su amor, paciencia y sobre todo por darme esta oportunidad tan grande de realizar mis sueños de ser un ingeniero mecatrónico.

A mis hermanas por su apoyo, compañía y solidaridad.

A mis maestros tanto en la parte académica como deportiva, al ingeniero Jorge Iván Velandia; ya que con sus conocimientos y sabiduría estuvieron siempre para resolver todas mis inquietudes.

A mis compañeros que siempre estuvieron al mi lado incondicionalmente, en especial a la Ing. Diana Vanessa, Hernández, Ing. Wilmar Andrés Ramírez, Ing. Alejandro Moreno y Julián Andrés Leal.

Al doctor Juan Carlos Luna y a todos los integrantes de la gran familia de la copropiedad Zona Franca del Pacífico especialmente al gerente Ing. Rodrigo Velasco, al Ing. Olmes Agudelo y al teniente retirado Edward Manjarres por su colaboración.

TABLA DE CONTENIDO

	Pág.
RESUMEN	11
INTRODUCCIÓN	13
1. PLANTEAMIENTO DE LA MISION	15
1.1. DESCRIPCION DEL PRODUCTO	15
1.2. PRINCIPALES OBJETIVOS DE MARKETING	15
1.3. PREMISAS Y RESTRICCIONES	15
1.4. PARTES IMPLICADAS	15
2. OBJETIVOS	16
2.1. OBJETIVO GENERAL	16
2.2. OBJETIVOS ESPECIFICOS	16
3. ESPECIFICACIONES DEL PRODUCTO	17
3.1. PLANTEAMIENTO DEL CLIENTE - NECESIDADES	17
3.2. MATRIZ DE CALIDAD	18
4. ESTADO ACTUAL DEL CONTROL DE ACCESO EN LA ZONA FRANCA DEL PACIFICO	22
4.1. ENTRADA PRINCIPAL	22
4.2. ENTRADA SECUNDARIA	24
5. SELECCION DE CONCEPTOS	26

5.1. DOCUMENTACION DE LOS DIFERENTES COMPONENTES QUE CONFORMAN LOS SISTEMAS DE CONTROL DE ACCESO A NIVEL INDUSTRIAL	26
5.1.1. Software para control de acceso.	26
5.1.2. Control de Accesos de Personas Mecanismos.	27
5.1.3. Identificación Automática. Electrónicos Portados. Llaves	34
5.1.4. Biométricos.	45
5.1.5. Equipos combinados: lector o teclado y biométrico.	52
5.2. CONTROL DE ACCESOS DE VEHÍCULOS	55
5.2.1. Medios Pasivos para Control de Accesos de Vehículos.	55
5.3. GENERALIDADES DE LOS DISPOSITIVOS	62
5.4. ESTANDARES DEL SISTEMA AUTOMÁTICO QUE CONTROLA EL ACCESO PEATONAL Y VEHICULAR EN LA ZONA FRANCA DEL PACIFICO	63
5.5. GENERACION DE CONCEPTOS	65
5.6. ESTUDIO DE COSTOS DE LOS CONCEPTOS	67
5.7. MATRIZ DE TAMIZAJE.	71
6. DISEÑO A NIVEL DE SISTEMA.	74
6.1. ANALISIS DE LA ARQUITECTURA DEL PRODUCTO	74
7. DISEÑO INDUSTRIAL.	75
7.1. VALORACIÓN EN EL DISEÑO INDUSTRIAL	75

7.1.1. Necesidades ergonómicas.	75
7.1.2. Necesidades estéticas	75
7.2. NATURALEZA DEL PRODUCTO: TECNOLOGICO O USUARIO	76
8. DISEÑO DE MANUFACTURA	77
8.1. COSTOS DE MANUFACTURA.	77
8.2. ESTRUCTURA CABLEADA.	77
9. ESPECIFICACIONES TECNICAS	79
9.1. REQUERIMIENTOS TECNICOS.	79
9.2. CONSUMO DE POTENCIA.	82
9.2.1. Calculo de UPS.	83
10. CONCLUSIONES	84
11. RECOMENDACIONES	85
BIBLIOGRAFIA	86

LISTA DE TABLAS

	Pág.
Tabla 1. Jerarquización de necesidades de usuario	17
Tabla 2. BenchMarking	18
Tabla 3. Necesidades vs. Métricas	20
Tabla 4. Relación entre métricas	21
Tabla 5 Costos de los módulos	68
Tabla 6 Costos de conceptos	71
Tabla 7. Matriz de tamizaje	73
Tabla 8. Conceptos seleccionados	74
Tabla 9. Costos de manufactura	77
Tabla 10. Estructura Cableada	79
Tabla 11. Requerimientos técnicos	80
Tabla 12. Consumo de potencia	82

LISTA DE FIGURAS

	Pág.
Figura 1. Análisis competitivo	19
Figura 2. Plano portería principal	23
Figura 3. Portería 2	25
Figura 4. Torno	27
Figura 5. Portillo automático	28
Figura 6. Molinete o Tambor rotativo	29
Figura 7. Exclusas	30
Figura 8. Puerta giratoria	31
Figura 9. Puerta deslizante	34
Figura 10. Llaves de proximidad	37
Figura 11. Tarjeta código de barras	39
Figura 12. Tarjeta magnética	40
Figura 13. Tarjeta de Proximidad	42
Figura 14. Tarjetas Inteligentes	43
Figura 15. Reconocimiento de huella	46
Figura 16. Reconocimiento por geometría de mano	48
Figura 17. Reconocimiento de voz	49

Figura 18. Reconocimiento de iris o retina	50
Figura 19. Reconocimiento facial	51
Figura 20. Barreras automáticas	57
Figura 21. Arco detector magnético	59
Figura 22. Generación de conceptos, ingreso peatonal	65
Figura 23. Generación de conceptos, ingreso vehicular	66
Figura 24. Concepto A	66
Figura 25. Concepto B	66
Figura 26. Concepto C	67
Figura 27. Concepto D	67
Figura 28. Estructura cableada	74
Figura 29. Necesidades ergonómicas	75
Figura 30. Necesidades estéticas	76
Figura 31. Naturaleza del producto	76

RESUMEN

La Zona Franca del Pacífico requiere de un control de acceso que funcione de forma automática para sus instalaciones, por diferentes razones, entre las más destacadas se encuentra el mejoramiento continuo de seguridad y calidad, agilidad en los registros, confiabilidad, rapidez y efectividad en el ingreso o salida. Todo esto para brindar mejor servicio a la comunidad que se encuentra en el parque industrial.

Por medio del diseño concurrente se busca llegar a una solución óptima, que genere resultados de forma positiva y real, que satisfaga tanto al usuario como el operador.

En el proyecto se propone dos sistemas diferentes en el cual tanto el software como el hardware sean seguros, robustos y se ejecuten en tiempo real, garantizando la trazabilidad de la información, la optimización de tiempos y costos a largo plazo. Ofreciendo así un ambiente más confiable y asegurando un eficaz flujo continuo del personal y vehículos al ingreso y salida del parque industrial.

Para el desarrollo del proyecto se estudiaron los diferentes equipos, programas y sistemas que se usan a nivel mundial en el sector industrial para el control de acceso, la forma cómo interactúan entre ellos y su entorno. Conociendo esto se escogen dos propuestas de acuerdo con las necesidades y requerimientos de la Zona Franca del Pacífico.

Básicamente el sistema de control de acceso funciona utilizando los siguientes elementos:

- **Software:** Es el que facilita la comunicación entre los usuarios/operadores y los equipos, envía la información en la base de datos, almacena registro y presenta información necesaria a los operadores de la persona que ha ingresado en el parque industrial.
- **Lector:** Son equipos electrónicos que poseen sensores de gran variedad, dependiendo del tipo de lectura que estos ejecuten, se encargan de recibir un dato análogo y real y lo convierten en un dato digital y en lenguaje de máquina para comunicarse con los distintos dispositivos.

- **Mecanismo:** Son equipos que impiden o permiten de forma física el ingreso y/o salida de un recinto.

Las actividades realizadas para desarrollar el documento, se iniciaron con un estudio de necesidades lo cual determino la importancia del sistema de control de acceso para la zona franca del pacifico, estudio de propuestas generadas por empresas que habían cotizado el sistemas automático de control de acceso para el parque industrial, evaluación de sistema de control de acceso actual versus control de acceso propuesto por las empresas, determinando cual cumple de forma más completa las expectativas y necesidades del cliente, se estudian y generan diferentes conceptos, estudio de costos, se evalúan los conceptos con los criterios de selección para generar dos propuestas del sistema de control de acceso.

INTRODUCCIÓN

Desde los inicios de nuestros tiempos el ser humano a buscado proteger sus pertenencias garantizando de esta manera su supervivencia y la de los miembros de su familia; conforme suceda esto se asegura la prosperidad de su linaje y aporta a su descendencia un grano de arena para su progreso. Esta problemática interminable ha llevado a la ciencia a buscar nuevos métodos y sistemas más eficientes, seguros y económicos para brindar dicha protección tan anhelada. Un buen ejemplo de esto son los costosos equipos e investigaciones que pagan los diferentes gobiernos para conocer el estado del clima de sus regiones, también se puede ver en las grandes inversiones a nivel militar por mantener la soberanía de un pueblo, sin ir más allá, el hecho de pensar en la seguridad de nuestros hogares no suena irracional; por esta razón se colocan puertas resistentes, rejas, guardamos el dinero en bancos, nuestras pertenencias en cajas fuertes, nos refugiamos en casas solidas, etc., para que nuestras pertenencias, nuestra integridad y la de los seres queridos, no pase a manos no deseadas o por lo menos a situaciones difíciles de controlar.

La Copropiedad Zona Franca del Pacifico (CZFP), es una empresa dedicada a la administración, mantenimiento y seguridad de la infraestructura del parque industrial existente dentro de la Zona Franca del Pacifico, ubicada en el Km. 6 de la carretera Yumbo-Aeropuerto Alfonso Bonilla Aragón del municipio de Palmira – Valle del Cauca. La Copropiedad interesada en satisfacer las necesidades para reforzar la seguridad de los usuarios y/o copropietarios, solicita el diseño de un sistema de control de acceso que funcione de forma autónoma para el personal y vehículos que ingresen y salgan del parque industrial, para su posterior desarrollo.

Aprovechando los conocimientos adquiridos, la experiencia y sabiduría de los directores y asesores del proyecto, se realiza una propuesta con fundamento que incluye información completa sobre el estado actual de las condiciones e información importante sobre los requerimientos específicos del diseño, de tal manera que los proveedores interesados en el desarrollo del proyecto apliquen bajo las mismas condiciones específicas acordes a las necesidades reales y requerimientos de la Zona Franca del Pacifico.

La importancia de este documento radica en que todas las empresas cotizantes se basen en un sistema de seguridad estudiado, aprobado y estandarizado teniendo en cuenta que las necesidades y requerimientos ya están plenamente identificadas, con lo cual, la empresa cotizante debe encargarse del desarrollo e implementación del sistema de control de acceso.

El diseño concurrente es un diseño en el cual se tienen en cuenta de forma simultánea los sistemas mecánicos, electrónicos y software como parte de todo un sistema y no se ven de forma independiente, de esta manera se disminuyen los costes del producto y el tiempo de producción. Teniendo en cuenta que se debe seguir unos pasos elementales como son el conocimiento de las necesidades del cliente, establecer especificaciones, generar conceptos, seleccionar conceptos, entre otros.

1. PLANTEAMIENTO DE LA MISION

El proceso de diseño, se rige por unas funciones y requisitos, los cuales solo pueden ser orientados por las condiciones del producto.

En el planteamiento de la misión, se enfocan entonces las posibles condiciones del producto.

1.1. DESCRIPCION DEL PRODUCTO

Diseño de sistema que controle el acceso peatonal y vehicular en zonas francas

1.2. PRINCIPALES OBJETIVOS DE MARKETING

Zona Franca del Pacifico.

1.3. PREMISAS Y RESTRICCIONES

- Componentes y subsistemas de fácil adquisición en el país.
- Fácil instalación.
- Autónomo
- Soporte y respaldo local

1.4. PARTES IMPLICADAS

- Usuario
- Normativas del mecanismo
- Operario
- Equipo de desarrollo

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Diseñar el control de acceso peatonal y vehicular para la Zona Franca del Pacífico.

2.2. OBJETIVOS ESPECIFICOS

- Determinar los cambios que se afectan con la implementación del producto.
- Analizar requerimientos desde el punto de vista administrativo, tecnológico y de seguridad propuestos por el personal la Copropiedad Zona Franca del Pacífico.
- Estudiar los ejemplos de sistemas utilizados para el control de acceso, en instalaciones similares, con el fin de proponer esquemas o soluciones más adecuados a este proyecto (BENCHMARKING).
- Realizar un inventario de posibles equipos o software con que cuente la Zona Franca en la actualidad, para determinar la posibilidad de integrarlos al presente proyecto.
- Enmarcar el diseño para que cumpla con los estándares y normas internacionales refiriéndose al control de acceso peatonal y vehicular.
- Proponer las mejores estrategias de mando y control para el monitoreo de las puertas de acceso, tanto peatonales como vehiculares.
- Proponer el diseño de una interfaz de software amigable para los usuarios.
- Plantear un sistema modular y de arquitectura abierta para ofrecer la posibilidad de ampliarlo de acuerdo a las necesidades de la Zona Franca del Pacífico.
- Adquirir experiencia en la forma como se plantea, ejecuta y lleva a cabo el diseño de proyectos de ingeniería.

3. ESPECIFICACIONES DEL PRODUCTO

3.1. PLANTEAMIENTO DEL CLIENTE - NECESIDADES

Para iniciar con el proceso de identificación de las necesidades, el primer paso es escuchar que es lo que desea el cliente, y traducir dichas necesidades o requerimientos, al lenguaje ingenieril y técnico.

Los siguientes requerimientos fueron planteados después de haber realizado un estudio y análisis de las necesidades puntuales que debe abarcar el proyecto de control de acceso para la Zona Franca del Pacífico en cuanto a Seguridad y Sistemas.

Tabla 1. Jerarquización de necesidades de usuario.

#	Necesidad	Importancia.
1	Agilidad de ingreso y salida de forma segura	5
2	Trazabilidad y control de ingreso dentro del parque	3,5
3	Control de activos	4
4	Agilidad de requisas	5
5	Automatización apertura y cierre de puertas	5
6	Generar registro visual del personal que ingresa en vehículo	4,5
7	salvaguardar registro de ingreso de empleados	5
8	Compatible con base de datos Oracle	5
9	Sistema Operativo Linux	5
10	Gran capacidad de almacenamiento	4,5
11	Fácil manejo para los operarios	4
12	Facilidad de mantenimiento	5
13	Interfaz grafica amigable	3,5
14	Robusto	4,5
15	Fácil manejo para usuarios	4
16	Capacidad de modificarse para posibles mejoras	4,5
17	Control al vencimiento de los documentos como EPS, ARP y contratos	4
18	Garantías por defectos de software y/o hardware	5
19	Garantiza evacuación inmediata en caso de posible emergencia	5

Nota: Los valores de importancia son necesarios para la elaboración de la matriz de calidad.

La Zona Franca del Pacífico ha recibido diferentes empresas especializadas en control de acceso, las cuales presentan características diferentes al momento de realizar sus cotizaciones, estas empresas son comparadas entre ellas y el sistema de control de acceso actual, en la matriz de la calidad.

3.2. MATRIZ DE CALIDAD

Es una herramienta que se utiliza para evaluar comparativamente los productos, servicios y procesos de trabajo en organizaciones con las necesidades del cliente, también es utilizada para conocer cuales son los puntos fuertes en los que se enfoca cada empresa para conocer de esta manera los puntos débiles de el producto actual y mejorarlo.

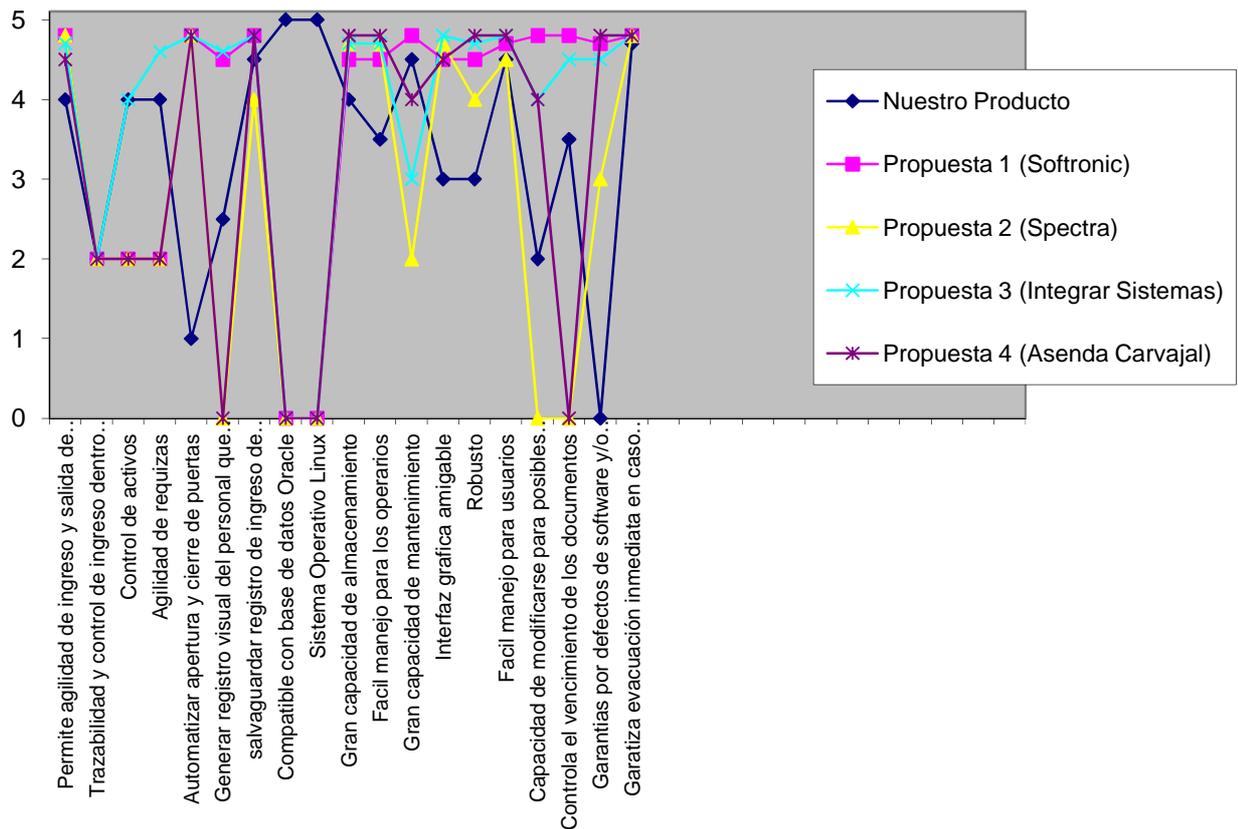
En la siguiente tabla se muestra dicha comparación en donde a cada empresa cotizante se le asigna un valor cuantitativo en un rango de 0 – 5 donde cero es el valor mínimo y cinco el máximo.

Tabla 2. BenchMarking

NUM.	REQUERIMIENTOS DEL CLIENTE	PESO	PESO REL.	ANALISIS COMPETITIVO				
				Nuestro Producto	Propuesta 1 (Softronic)	Propuesta 2 (Spectra)	Propuesta 3 (Integrar Sistemas)	Propuesta 4 (Asenda Carvajal)
1	Permite agilidad de ingreso y salida de forma segura	5	5,81	4	4,8	4,8	4,7	4,5
2	Trazabilidad y control de ingreso dentro del parque	3,5	4,07	2	2	2	2	2
3	Control de activos	4	4,65	4	2	2	4	2
4	Agilidad de requizas	5	5,81	4	2	2	4,6	2
5	Automatizar apertura y cierre de puertas	5	5,81	1	4,8	4,8	4,8	4,8
6	Generar registro visual del personal que ingresa en vehiculo	4,5	5,23	2,5	4,5	0	4,6	4,8
7	salvaguardar registro de ingreso de empleados	5	5,81	4,5	4,8	4	4,8	4,8
8	Compatible con base de datos Oracle	5	5,81	5	0	0	0	0
9	Sistema Operativo Linux	5	5,81	5	0	0	0	0
10	Gran capacidad de almacenamiento	4,5	5,23	4	4,5	4,7	4,7	4,8
11	Facil manejo para los operarios	4	4,65	3,5	4,5	4,7	4,7	4,8
12	Gran capacidad de mantenimiento	5	5,81	4,5	4,8	2	3	4
13	Interfaz grafica amigable	3,5	4,07	3	4,5	4,7	4,8	4,5
14	Robusto	4,5	5,23	3	4,5	4	4,7	4,8
15	Facil manejo para usuarios	4	4,65	4,5	4,7	4,5	4,8	4,8
16	Capacidad de modificarse para posibles mejoras	4,5	5,23	2	4,8	0	4	4
17	Controla el vencimiento de los documentos	4	4,65	3,5	4,8	0	4,5	0
18	Garantias por defectos de software y/o hardware	5	5,81	0	4,7	3	4,5	4,8
19	Garatiza evacuación inmediata en caso de posible emergencia	5	5,81	4,7	0	0	0	4,8

En la **Figura 1**. Se hará un análisis de tendencia del Benchmarking realizado anteriormente.

Figura 1. Análisis competitivo.



Al mismo tiempo que se identifican las necesidades, a partir de las mismas, se generan las métricas las cuales indican las unidades métricas que se utilizan para satisfacer las necesidades mencionadas.

Adicionalmente, en el paso de establecimiento de las métricas, también se relacionan las necesidades.

En la **Tabla 3**. Se relaciona las métricas con las necesidades. En la cual se dan tres valores 1 representa la mínima relación, 3 que es una relación media y 9 que representa una máxima relación.

Tabla 3. Necesidades vs. Métricas

			NUMERO DE COLUMNA							
			1	2	3	4	5	6	7	
			MAX. RELACION DE LA COLUMNA							
			9	9	9	9	9	9	9	
			PESO DEL REQUERIMIENTO							
			524,42	605,61	646,51	623,26	900	346,64	396,64	
			Minimize (▼), Maximize (▲), or Target (X)							
			▲	▲	▲	▲	▲	▲	▲	
			Target or Limit Value							
NUMERO	MAXIMO VALOR DE RELACION	PESO REL.	METRICAS							
			REQUERIMIENTOS							
			Tiempo para ingresar datos al sistema (minutos)	Confiablez (Subjetivo)	Compatibilidad software con base de datos (Lisa)	Comunicación con todo el sistema de seguridad (Lisa)	Normas y estándares de seguridad (Lisa)	Materiales del mecanismo (Lisa)	Medios de transmisión de datos y/o comunicación (Lisa)	
1	9	5,81	Permite agilidad de ingreso y salida de forma segura	9	9	1	9	9	3	9
2	9	4,07	Trazabilidad y control de ingreso dentro del parque	9	9	1	9	9	1	9
3	9	4,65	Control de activos	9	9	9	9	9	1	1
4	9	5,81	Agilidad de requizas	9	3	1	9	9	1	1
5	9	5,81	Automatizar apertura y cierre de puertas	3	9	1	3	9	9	1
6	9	5,23	Generar registro visual del personal que Ingres a en vehiculo	9	9	9	9	9	1	1
7	9	5,81	salvaguardar registro de ingreso de empleados	3	9	9	9	9	1	1
8	9	5,81	Compatible con base de datos Oracle	1	9	9	9	9	1	3
9	9	5,81	Sistema Operativo Linux	1	9	9	9	9	1	3
10	9	5,23	Gran capacidad de almacenamiento	9	9	9	1	9	1	3
11	9	4,65	Facil manejo para los operarios	9	3	9	1	9	3	3
12	9	5,81	Gran capacidad de mantenimiento	1	9	3	9	9	9	9
13	9	4,07	Interfaz grafica amigable	9	9	9	1	9	1	1
14	9	5,23	Robusto	3	9	9	9	9	9	9
15	9	4,65	Facil manejo para usuarios	9	9	9	1	9	1	1
16	9	5,23	Capacidad de modificarse para posibles mejoras	1	3	9	9	9	1	9
17	9	4,65	Controla el vencimiento de los documentos	9	9	9	9	9	1	1
18	9	5,81	Garantias por defectos de software y/o hardware	1	9	9	1	9	9	1
19	9	5,81	Garaliza evacuación inmediata en caso de posible emergencia	1	9	1	1	9	9	9

Posteriormente se evalúan las métricas entre ellas mismas para conocer si su relación es significativa o no.

Tabla 4. Relación entre métricas.

		NÚMERO DE COLUMNA							
NÚMERO DE FILA	MÉTRICAS	1	2	3	4	5	6	7	
		Tiempo para ingresar datos al sistema (minutos)							
		Confiabilidad (Subjetivo)							
		Compatibilidad software con base de datos (lista)							
		Comunicación con todo el sistema de seguridad (Lista)							
		Normas y estándares de seguridad (Lista)							
		Materiales del mecanismo (Lista)							
		Medios de transferencia de datos y/o comunicación (Lista)							
1	Tiempo para ingresar datos al sistema (minutos)								
2	Confiabilidad (Subjetivo)	+							
3	Compatibilidad software con base de datos (lista)	-	-						
4	Comunicación con todo el sistema de seguridad (Lista)	+	+	-					
5	Normas y estándares de seguridad (Lista)	+	+	-	+				
6	Materiales del mecanismo (Lista)	-	+	-	-	+			
7	Medios de transferencia de datos y/o comunicación (Lista)	+	+	-	+	+	-		

En la anterior grafica, el signo (+) representa que hay relación entre las métricas, y el signo (-) que no existe relación.

4. ESTADO ACTUAL DEL CONTROL DE ACCESO EN LA ZONA FRANCA DEL PACIFICO

La Zona Franca del Pacifico posee dos secciones para ingreso y salida, una es la entrada principal, donde acceden contratistas, visitantes y vehículos particulares y de carga y la segunda sección hace parte al ingreso y salida peatonal de los empleados de las diferentes empresas ubicadas dentro del parque industrial.

A continuación se detalla cada una de las entradas.

4.1. ENTRADA PRINCIPAL

En la primera sección encontramos el ingreso de visitantes, contratistas y vehículos particulares y de carga. Es importante notar que para el ingreso de visitantes a las instalaciones, debe estar autorizado con anterioridad por parte de la empresa que va a visitar, esta autorización debe ser registrada en el programa PICIZ (Programa Integral para Control Informático de Zonas Francas) que en este caso funciona como control de acceso de visitantes para verificar los datos por el personal de seguridad que se encuentra en la entrada del parque, ellos se encargan de permitir o restringir el ingreso y salida de las personas a las instalaciones. Adicional a esto inspeccionan si el personal que entra o sale, esta armado o lleva consigo algo que pertenece a las instalaciones del parque industrial (control de activos). Para el ingreso de mercancía, la Zona Franca del Pacifico utiliza el mismo programa PICIZ el cual se encarga de llevar un registro muy detallado del ingreso y salida de productos a la Zona Franca y a las empresas que se encuentran dentro de esta. Este programa presenta dificultades ya que fue diseñado para un control de acceso de mercancías mas no de personal, y como el software no pertenece a la Zona Franca del Pacifico entonces se necesita un permiso para anexarle el modulo de control de acceso de personal. En el momento se encuentra en prueba un programa similar a PICIZ con la gran ventaja que es de propiedad de la Zona Franca del Pacifico llamado PACIFICO al cual se puede anexarle el modulo de control de acceso sin tener mayor dificultad en cuanto a licencias y/o permisos especiales. En el momento PACIFICO se encuentra a prueba en una zona franca que administra el usuario operador llamada AGROINDUSTRIAS DEL CAUCA.

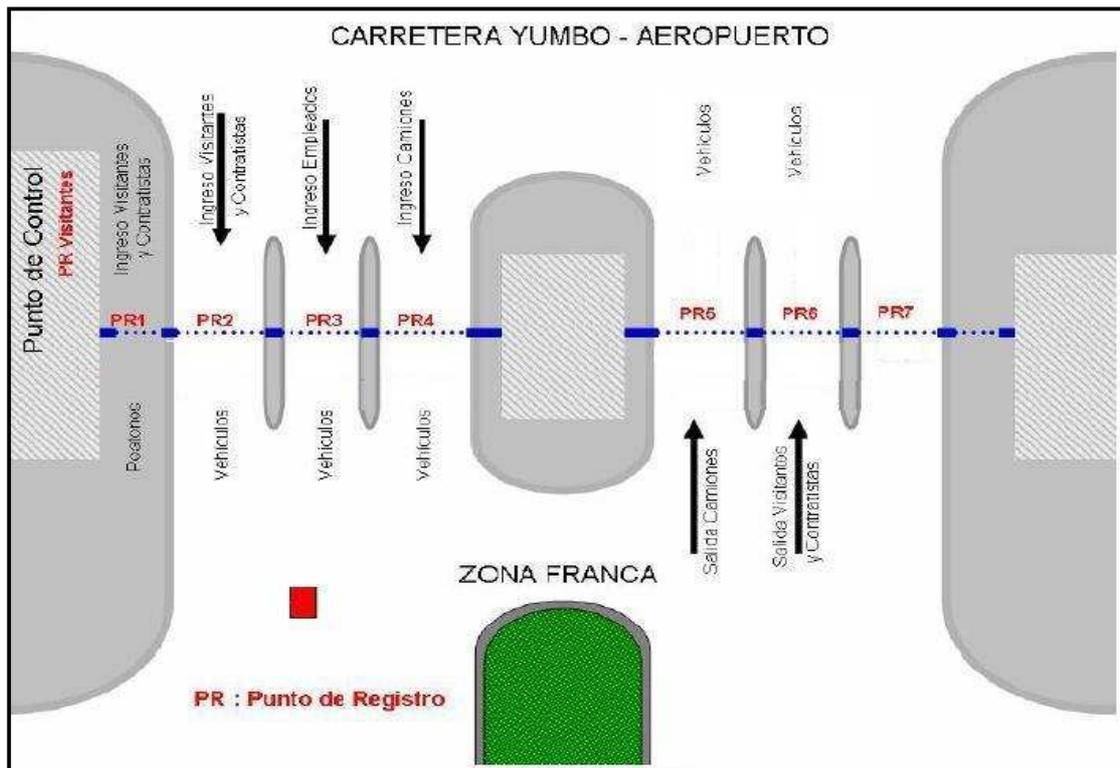
Pero aunque el cambio de software se genere se debe tener en cuenta la infraestructura de la red de datos y licencias

En la entrada principal hay 5 (cinco) personas de seguridad que se encargan del ingreso, autorización, entrega de carné de entrada y de requisar a las personas que ingresan o salen de la Zona Franca; los cargos de dicho personal se encuentran seccionados de la siguiente forma:

- Auxiliar recepción.
- Refuerzo portería 1.
- Guarda control puerta de visitantes.
- Control ingreso vehículos de carga.
- Guarda externo o refuerzo parqueadero.

En la **Figura 2.** se muestra como se encuentra dividida la entrada principal a la Zona Franca del Pacifico desde una vista superior.

Figura 2. Plano portería principal



Fuente: Cotización de sistema de control de acceso de Softronic Solutions S.A. Santiago de Cali, 2008.

En la figura anterior, se aprecia la entrada principal de la Zona Franca tiene 7 (siete) puertas de registro PR las cuales en el momento funcionan seis, de izquierda a derecha, la puerta uno PR1, funciona para el ingreso y salida de peatones (ya sean visitantes y/o contratistas), la puerta dos PR2, es para el ingreso de contratistas o visitantes que se trasladan en vehículo, la puerta tres PR3, es para el ingreso de empleados que se movilizan en vehículo, la puerta cuatro PR4, es para el ingreso de mercancía que es transportada en camiones o tracto mulas, la puerta cinco PR5, es para la salida de los vehículos de carga y la puerta seis PR6, es para la salida de visitantes, contratistas y empleados que se transportan en vehículos.

Las puertas solo son abiertas para el ingreso/salida del personal o mercancía. Esto se realiza de forma manual por parte del personal de seguridad, lo cual en algunas ocasiones amerita de dos o más personas solo para estar abriendo y cerrando puertas y otras tantas requisando vehículos y personal peatonal.

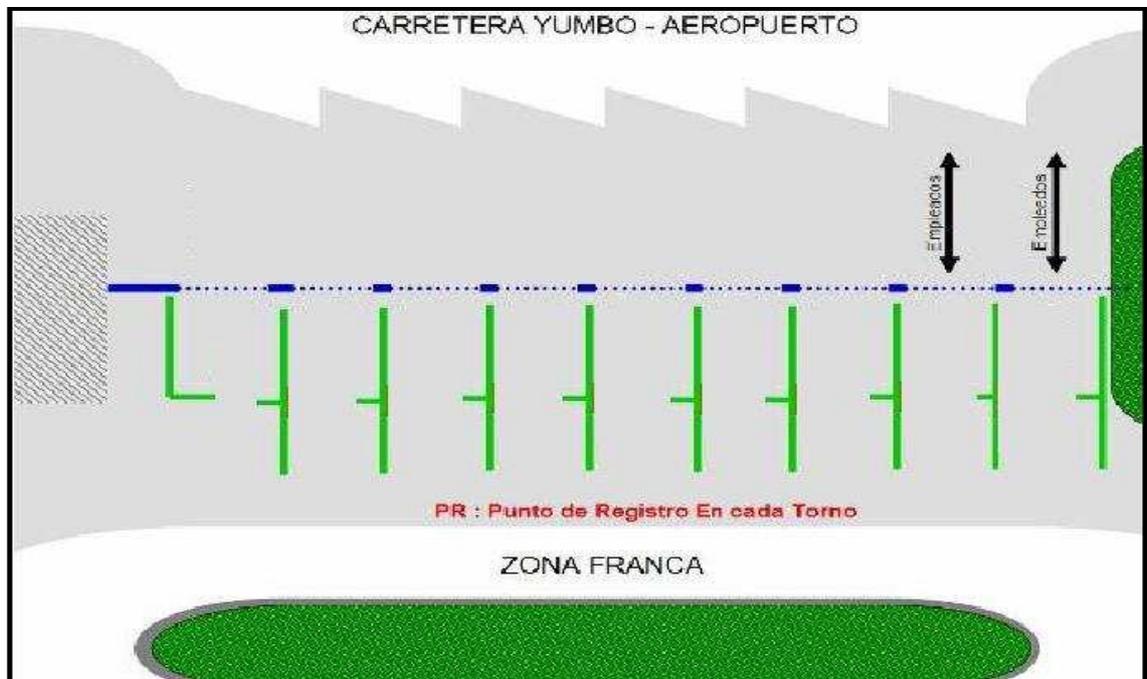
4.2. ENTRADA SECUNDARIA

En la entrada secundaria es el ingreso peatonal de los empleados de las diferentes compañías establecidas dentro del parque industrial.

Para el ingreso por este sector, se exige el carné a los empleados por el personal encargado de la seguridad.

Se encuentran varios tornos los cuales nunca se han usado y se encuentran deteriorados por oxido y falta de mantenimiento.

Figura 3. Portería 2.



Fuente: Cotización de sistema de control de acceso de Softronic Solutions S.A. Santiago de Cali, 2008.

En la **Figura 3.** se observa la entrada secundaria donde se aprecia que hay nueve (9) puertas con tornos de las cuales se usa una puerta, máximo dos dependiendo del flujo del personal.

5. SELECCION DE CONCEPTOS

5.1. DOCUMENTACION DE LOS DIFERENTES COMPONENTES QUE CONFORMAN LOS SISTEMAS DE CONTROL DE ACCESO A NIVEL INDUSTRIAL

A continuación se presentan las posibilidades más conocidas usadas en el área industrial para el control de acceso.

5.1.1. Software para control de acceso.

El software diseñado para aplicaciones de control de accesos se encargará de gestionar las comunicaciones entre los terminales de captura de datos (lectores) y la explotación de esta información almacenada por medio del programa informático diseñado para tal fin.

Características y prestaciones fundamentales:

- Almacenamiento en memoria de funciones y parámetros de programación así como los de configuración del sistema y de los controladores.
- Definición y programación individual de diferentes puntos de acceso (apertura, bloqueo, incidencias, etc.).
- Configurar perfiles de acceso y asignarlos a cada usuario.
- Recogida de los marcajes desde los puntos de control por medio de lectores de tarjetas, teclados, biométricos.
- Transmisión de los datos a sus respectivos ficheros de tratamiento.
- Habilitar y cancelar los permisos de paso (tarjetas, códigos, etc.) individualmente o en bloque.
- Acceso protegido por contraseña y/o procedimientos de autenticación.
- Integración con programas de control de presencia, de visitas, de vehículos, de rondas, de alarmas, sistemas de CCTV, etc. pudiendo importar y exportar datos entre aplicaciones.
- Arquitectura escalable: capacidad para adaptarse a necesidades futuras de ampliación.
- Supervisión del estado de los dispositivos en tiempo real.
- Posibilidad de funcionamiento en red con protocolo TCP/IP en redes LAN o WAN e Internet.
- Integración en el mismo software o paquete de programas de aplicaciones para el control de visitas, control de presencia, gestión de producción, etc.

- Compatibilidad y funcionamiento bajo entornos de uso generalizado Linux: ventanas, menús desplegados, identificación intuitiva (iconos, botones de selección, etc.), ayuda en línea, etc.
- Adaptación del programa a las necesidades del cliente mediante los cambios, ampliaciones, distintas configuraciones, rediseño, etc.

5.1.2. Control de Accesos de Personas Mecanismos.

- **Torno o torniquete.** Equipo que consta de un mueble donde se hallan los mecanismos necesarios para controlar el funcionamiento de tres barras o brazos en forma de trípode, los cuales giran 120° por impulso para permitir el paso individualizado de las personas, permaneciendo uno de los brazos en posición horizontal con la intención de bloquear el acceso.

Figura 4. Torno.



Fuente: Torno [en línea]. Andalucía: Integración, desarrollo y mantenimiento electrónico, 2003 [Consultado 24 de Octubre de 2008]. Disponible en Internet: http://www.idmesl.com/imagenes/productos/control_accesos/tornos.jpg

Sus características principales son:

- Instalación tanto en el interior como en el exterior de las construcciones, siendo necesario en el segundo caso protegerlo de las inclemencias meteorológicas.
- Requieren mínima vigilancia por medios humanos u ópticos, que permitan actuar ante intentos de fraude.
- Diferentes modelos para un pasillo o doble pasillo.
- Según permitan el paso en uno o dos sentidos se clasifican en unidireccionales o bidireccionales.

- La apertura puede ser automática o vinculada a sistemas electrónicos: teclados, lectores, biométricos.
- Sistema de desbloqueo automático o manual en caso de interrupción del suministro de energía eléctrica o para los casos de emergencia y evacuación.
- El material de construcción, tanto de los brazos como del armazón, suele ser de acero inoxidable, que permitirá su instalación ambivalente, en interior y exterior.
- Algunos equipos incorporan partes de plástico ABS, PVC, fibra de vidrio, etc.
- Protección contra el vandalismo y la intemperie.
- Pueden equiparse con una serie de accesorios emplazados en la estructura del equipo.

• **Portillos automáticos.** Equipo que consta de una estructura en la cual se alojan los paneles o pantallas que cierran el paso hasta que se autoriza un acceso.

En su uso habitual están supeditados a la previa autorización de sistemas de identificación automática: lectores de tarjetas, biométricos o teclados.

Figura 5. Portillo automático



Fuente: Portillo automático [en línea]. Barcelona: IDC Electrónica S.A., 2008. [Consultado 24 de Octubre de 2008]. Disponible en Internet: http://www.idcsa.com/imgprod/terminales/Port3_P.jpg

Entre sus características destaca:

- Empleo frecuente en el interior de las instalaciones, aunque es válido para el exterior, protegido de las inclemencias meteorológicas.
- Requieren mínima vigilancia por medios humanos u ópticos, que permitan actuar ante intentos de fraude.
- Por la forma de alojarse los paneles se clasifican en abatibles, batientes y correderos ocultables.

- Células fotoeléctricas regulan el paso de personas y la apertura de los paneles.
- Según permitan el paso en uno o dos sentidos, los portillos pueden ser unidireccionales o bidireccionales.
- Sistema de desbloqueo automático ante la interrupción del suministro de energía eléctrica o en casos de emergencia o evacuación (anti pánico).
- Se pueden adaptar para el paso de las sillas de ruedas de los minusválidos.
- Protección contra el vandalismo y la intemperie.

Pueden equiparse con una serie de accesorios emplazados en la estructura del equipo.

- **Molinete o tambor rotativo.** Equipo constituido por un eje al que se acoplan tres o cuatro paneles, o filas de barras horizontales superpuestas, que giran 90° o 120° en una estructura envolvente circular para permitir el paso individualizado de personas.

Figura 6. Molinete o Tambor rotativo



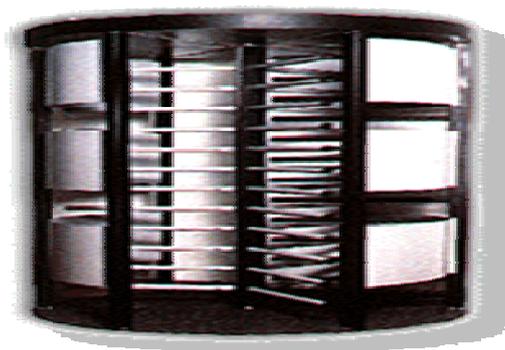
Fuente: Molinete [en línea]. Barcelona: Accesor Applications and Services, S.A., 2003. [Consultado 24 de Octubre de 2008]. Disponible en Internet: http://www.accesor.com/productos/art/106_11.jpg

Estas son algunas de sus características:

- Uso frecuente en exteriores, sin necesidad permanente de vigilancia.
- Los paneles giratorios suelen ser de cristal, metacrilato o plástico, mientras que las barras son de acero inoxidable o aluminio.
- Funcionamiento unidireccional o bidireccional, facilitando el paso en uno o dos sentidos.
- El paso puede ser continuo o supeditado al control de sistemas electrónicos (teclados, lectores, biométricos).

- Los de paneles suelen cubrir alturas de un metro, empleándose mayormente los de tubo metálico para dimensiones superiores.
- Protección contra el vandalismo y la intemperie.
- **Esclusas.** Sistema de colocación de dos puertas entre las cuales se crea un espacio intermedio y se condicionan la apertura de la segunda al cerramiento previo de la anterior (excepto en situaciones de emergencia).

Figura 7. Esclusas



Fuente: Esclusas [en línea]. España: Astra sistemas S.A., 2003. [Consultado 24 de Octubre de 2008]. Disponible en Internet: www.astrasistemas.com/Imagenes/Esclusa.gif

Corrientemente están vinculadas al control de sistemas electrónicos de identificación (lectores, biométricos o teclados), vigilancia óptica, detectores de metales o pulsadores manuales. El accionamiento de las puertas puede estar temporizado o sometido a detectores de presencia o fotocélulas coordinados con indicadores visuales (led o piloto) y/o acústicos que informan del estado.

Se emplea en el interior de inmuebles, permitiendo el diseño y aplicación individualizados en función del nivel de seguridad a conseguir. Los modelos y configuraciones de los conjuntos existentes en el mercado son muy variados, pero a todos ellos hay que exigirles un blindaje resistente y anclaje firme a elementos estructurales del edificio.

Entre sus funciones destacamos la inestimable colaboración en las tareas de control de acceso (entrada, salida, y objetos, si incorporan detector de metales) a los establecimientos permitiendo la identificación y confinamiento de personas sospechosas.

Otros requisitos a considerar: dimensiones del conjunto (ancho, alto, profundidad), materiales de construcción (metálicos, vidriados), flujo de personas, dispositivos

de control, sistema de emergencia (liberación de puertas), iluminación, peso, alimentación principal y secundaria, certificación por entidad reconocida, etc.

De obligada instalación en la mayoría de entidades bancarias, en el conjunto se integra un arco detector de metales que activará el bloqueo de las puertas y, consecuentemente, el confinamiento de las personas que porten objetos metálicos.

La apertura de las puertas puede ser automática o manual, a distancia por personal autorizado o por el usuario previa autorización del sistema.

- **Puerta giratoria.** Equipo convencional formado por un eje al que se acoplan tres o cuatro paneles de una pieza que giran 90° o 120° en una estructura envolvente circular para asegurar el paso individualizado de personas.

Para instalaciones con mucha afluencia de personas (edificios de oficinas, hoteles, centros comerciales, aeropuertos, hospitales) se fabrican equipos con mayor capacidad de tránsito, permitiendo el acceso agrupado y la utilización de sillas de minusválidos, carros de compra, portamaletas, etc.

Figura 8. Puerta giratoria.



Fuente: Puerta Giratoria. [en línea]. [Consultado 5 de Enero de 2009]. España: BoonEdam S.L., 2004. Disponible en Internet: <http://www.boonedam.com/img/products/tw/front-tw.jpg>

Sus características principales son:

- Suelen funcionar por impulso manual aunque también en modo de desplazamiento automático continuo.
- Permiten el paso en dos direcciones (bidireccional) a pesar de mantener un giro permanente en el mismo sentido.
- No es habitual supeditar el paso a sistemas electrónicos de control de accesos.
- Dispositivo anti pánico: abatir las hojas en caso de emergencia.

- Favorecer el aislamiento térmico y acústico.
- Operación de modo silencioso.
- Materiales de composición muy diversos (maderas, vidrio, metales, PVC) y acabados múltiples, considerando la integración en el ambiente estético del entorno.

- **Puertas de Acceso.** Las puertas, podemos afirmar, es el medio de control de accesos de uso generalizado que se halla implantado en multitud de espacios o recintos y sobre el que se implementan medios complementarios de seguridad. La puerta es el componente básico para impedir la intrusión por las aberturas que puedan presentar las paredes. Por ello es imprescindible aplicarles métodos y sistemas para controlar el acceso, ya sea de personas o de vehículos.

Existe gran diversidad de puertas susceptibles de ser utilizadas en el cerramiento de espacios, exteriores o interiores, y que, consecuentemente, colaboran en las tareas de control de acceso de personas a dichos recintos.

Con el objetivo de incrementar su eficacia y fiabilidad en la acción protectora suelen equiparse con medios electrónicos complementarios (contacto magnético, sensor inercial, micro contactos, cerraduras especiales, etc.) encargados de detectar y comunicar las variaciones o modificaciones que produzcan sobre el elemento físico.

Asimismo es factible supeditar las operaciones de apertura y cierre al reconocimiento practicado por sistemas electrónicos de identificación (lectores, biométricos o teclados), vigilancia óptica, detectores de metales, pulsadores manuales, etc.

Los componentes principales de la puerta son:

- **Puertas automáticas.** Referente a éstas, la NBE-CPI 96 determina en el artículo 8.1.b) que "las puertas de apertura automática dispondrán de un sistema tal que, en caso de fallo del mecanismo de apertura o del suministro de energía, abra la puerta e impida que ésta se cierre, o bien que, cuando sean abatibles, permita su apertura manual. En ausencia de dicho sistema, deberán disponerse puertas abatibles de apertura manual que cumplan las condiciones indicadas en el párrafo anterior".

El mercado nos ofrece gran variedad de diseños para los tipos de puertas automáticas (batiente, deslizante) y, con la intención de concretar, se exponen las características principales de estos elementos empleados habitualmente en controles de accesos:

- Control del sistema por medio de controlador electrónico o microprocesador.
- Activación de apertura por detección de presencia, pulsación manual de interruptor, código en teclado, vinculación a tarjeta o biométrico, etc.
- Programación de los ciclos de apertura, permanencia y cierre.
- Cierre automático temporizado tras apertura o vinculado a sensor, manual, cierrapuertas, etc.
- Velocidad de desplazamiento regulable, pudiendo ser distinta en la apertura o cierre.
- Operación de modo silencioso.
- Bloqueo del acceso en casos específicos: código erróneo, detección de intrusos, "anti-passback".
- Posibilidad de apertura manual en caso de fallo en el suministro de energía, avería, emergencia.
- Dispositivo para mantener la apertura en determinados casos: incendio, evacuación, horas de máxima afluencia, etc.
- Supervisión y programación del sistema por medio de terminales portátiles o aplicaciones informáticas.
- Integración con otros sistemas de protección: contra incendio, intrusión, atraco y robo, etc.
- Posibilidad de añadir detección de obstáculos, que provocaría la interrupción instantánea del proceso.
- Los componentes, accesorios y mecanismos de las puertas no deben suponer un riesgo para la circulación y seguridad de los ocupantes.

• **Puerta peatonal deslizante.** Sistema utilizado para facilitar la apertura y cierre de puertas, frecuentemente deslizantes de cristal, en locales de gran afluencia de personas sin requerir una atención constante.

Las puertas correderas pueden ser simples o de doble hoja y telescópicas simples o de doble hoja, etc. en configuración longitudinal, pero también existen modelos de puertas correderas curvas para configuraciones semicirculares.

Entre sus características principales:

- Funcionamiento automático y autónomo.
- Control por microprocesador.
- Programación de la velocidad de apertura y cierre (regulable).
- Fijación del tiempo de permanencia abierto.
- Detección por medio de detector de movimiento, infrarrojo, microondas, fotocélula, etc.
- Sistema de autodiagnóstico continuo.
- Dispositivo de seguridad contra el aplastamiento de usuarios entre dos hojas o puerta y marco.

- Dispositivo de bloqueo/desbloqueo manual y anti pánico en determinadas circunstancias.
- Sistema de alimentación ininterrumpida.
- Operación de modo silencioso.
- Puede integrarse en sistemas de control de acceso y monitorizarse el estado de la puerta.
- Posibilidad de vinculación con detectores, pulsadores, sistemas de alarma, tarjetas, biométricos, etc. para asegurar el bloqueo o desbloqueo del acceso.
- Otros aspectos a considerar: motor, dimensión y altura del acceso, peso de las hojas, materiales de construcción, accesorios (cerradura, llave, pulsadores, mando a distancia), alimentación, consumo, etc.
- Las aplicaciones más habituales han sido en centros comerciales, estaciones, comercios, oficinas, etc.

Figura 9. Puerta deslizante



Fuente: Puerta deslizante. [en línea]. Iran: Manufacturer and Exporter of Automatic Doors, 2004. [Consultado 24 de Octubre de 2008]. Disponible en Internet: <http://achilandoor.20un.com/39-b.jpg>

5.1.3. Identificación Automática. Electrónicos Portados. Llaves

- **Sistemas electrónicos.** Los sistemas electrónicos empleados en el control de accesos de personas se aplican fundamentalmente con dos propósitos:
 - Identificar automáticamente a las personas por medio de:
 - Lectores de medios electrónicos portados:
 - Llaves: magnéticas, de proximidad, etc.
 - Tarjetas: código de barras, magnéticas, proximidad, chip, etc.

- Equipos biométricos analizadores de la huella dactilar, la geometría de la mano, la retina o el iris, la voz, los rasgos faciales, la firma, etc.

Complementar las funciones de los elementos de cerramiento (puertas y cerraduras) mediante automatismos, sensores de estado, accionamientos, etc. Asimismo no se debe olvidar la inestimable colaboración aportada por los sistemas ópticos de vigilancia, en las tareas de identificación, y por los equipos de inspección en las tareas reconocimiento y examen de objetos, además de los medios de comunicación.

- **Identificación automática.** Los sistemas de identificación automática de personas se caracterizan por permitir que se realice dicha función sin la intervención de personas de control o seguridad, disponiéndose los datos preceptivos por grabación en un soporte (electrónicos portados) o por formar parte de la morfología del individuo (biométricos).

Los sistemas electrónicos portados de identificación automática son aquellos elementos (llaves especiales, tarjetas) que se asignan a las personas para su presentación ante dispositivos de reconocimiento (lectores).

Por su forma de utilización pueden ser de tres tipos:

- *De introducción:* Se insertan en aberturas dispuestas en el equipo de lectura
- *De pasada:* Es preciso deslizarlos por ranuras practicadas en el equipo lector.
- *De proximidad:* Basta con acercarlos al elemento de reconocimiento.

Los medios más empleados son:

- Llave magnética.
- Llave de proximidad.
- Teclado numérico.
- Tarjetas.
- Equipo vía radio.

- **Llave magnética.** Llave, generalmente de plástico, que contiene información codificada magnéticamente y se introduce en un lector al efecto, el cual compara y reconoce el código particular procediendo a la apertura de un acceso (puerta, portón, barrera, cierre metálico, etc.) o manteniendo el bloqueo, si es rechazada.

Sus características principales son:

- Las llaves pueden ser planas o disponer de guía central, izquierda o derecha.

- Programación por medio de codificadora específica o, en ciertas llaves, manualmente, modificando la posición de los imanes.
- Los códigos posibles de grabarse son numerosos, por lo que las probabilidades de repetirse son casi nulas.
- Habilitación y cancelación desde el propio lector, unidades especiales o por medio de software específico.
- Diferentes acabados en cuanto a color: negra, gris, azul, crema, blanca, etc.
- Su aplicación es suficiente para espacios con escaso nivel de seguridad ya que no ofrecen muchas garantías contra el copiado de la llave y borrado de la información magnética.
- Su instalación es muy frecuente para controlar el acceso a garajes y aparcamientos de muy diversas dimensiones.
- Representa una solución alternativa para llaves y cerraduras al agilizar las operaciones manuales y de control sobre los accesos.

• **Llave de proximidad.** Esta llave incorpora un emisor de ondas radio que son reconocidas o desestimadas por un equipo receptor, permitiendo o denegando el acceso, respectivamente.

También se les llama de "manos libres" al no ser precisa la introducción o deslizamiento por el lector, incluso, a veces, ni la extracción de la cartera o bolsillo en que se porte.

Entre sus características principales se puede señalar:

- Las llaves se diseñan con muy diferentes formas: llave, botón, llavero, medallón, etc.
- Este medio ofrece una alta fiabilidad, siempre que quien la porte, sea persona autorizada.
- Programación de códigos por medio de codificadora específica equipos informáticos.
- Los códigos posibles de grabarse son numerosos, garantizándose la imposibilidad de copia o duplicados.
- Habilitación y cancelación desde el propio lector, unidades especiales o por medio de software específico.
- La vida útil de este elemento es muy prolongada, se evita el desgaste, tanto del dispositivo como del lector, al no requerir el contacto directo con los equipos de lectura.
- Su aplicación es frecuente para controlar el acceso a espacios con apertura vinculada a este dispositivo.

Figura 10. Llaves de proximidad.



Fuente: Llaves de proximidad [en línea]. España: Casa Domo, el portal del edificio y el hogar digital, 2008 [Consultado 24 de Octubre de 2008]. Disponible en Internet:

http://www.casadomo.com/images/news/20060410_SIMA_Miniatec_acce.jpg

- **Tarjetas.** Las tarjetas de identificación y acreditación se comenzaron a emplear a finales de la década de los sesenta, evolucionando desde la hoja o cartulina recortada con texto impreso (nombre y número) hasta las tarjetas plastificadas que, aparte de los datos personales, podían incluir una fotografía pegada. Este proceso era lento en su elaboración y costoso en cuanto a tiempo dedicado, y si le añadimos facilidad en la falsificación podremos entender la evolución de estos elementos.

Las necesidades de simplificar el proceso, unidas a la aspiración de identificar y acreditar a las personas por motivos de seguridad en numerosas y variadas instalaciones conllevó la aparición de las tarjetas de plástico o PVC como un elemento fiable, manejable, portable y de reducido coste con posibilidad de disponerse tanto en pequeñas como en grandes empresas, edificios o establecimientos, tanto públicos como privados.

En un principio carecían de la posibilidad de utilizarse con dispositivos de seguridad, pero la necesidad de una identificación personalizada y automática fomentó la incorporación de diversos métodos o tecnologías (código de barras, información magnética, infrarrojos, chips) que facilitaron su integración en los sistemas de control de accesos.

Posteriormente se amplió su rendimiento para establecer las limitaciones de acceso a determinadas áreas y controlar la presencia de personas en las instalaciones.

Con el tiempo las prestaciones de este elemento se han adoptado para ser utilizadas en otras aplicaciones automatizadas relacionadas con el control de acceso y utilización de equipamientos muy diversos:

- Acceso a cajeros automáticos que facilitan la retirada de dinero, adquirir entradas para espectáculos, recargar el teléfono móvil, etc.
- Uso de equipos ofimáticos (fotocopiadora) e informáticos (ordenadores).
- Abono de importes de compras o servicios: estacionamiento, llamar por teléfono, etc.
- Control las entregas y acceso a préstamo de libros (bibliotecas), alquiler de cintas de vídeo (videoclub), etc.
- Monedero electrónico de acceso y pago en máquinas autoservicio.

Asimismo han evolucionado las técnicas de impresión y grabación de datos o códigos con resultados positivos en cuanto a digitalización y personalización de las tarjetas en función de los particulares gustos (colores, logotipos, texto, fotos, medidas de seguridad) y necesidades de los clientes o usuarios.

Por último hay que referirse a la durabilidad de estos elementos, supeditada a la utilización personal del usuario, las limitaciones peculiares de la tecnología integrada y una serie de precauciones básicas como:

- No intentar doblar la tarjeta.
- No practicarle troqueles o aplastamiento.
- Mantenerla alejada de la luz solar y radiaciones ultravioletas.
- No exponerla a temperaturas elevadas y elementos químicos corrosivos.

• **Tarjeta de código de barras.** En la tarjeta se imprime un código de barras, compuesto por una sucesión en paralelo de barras y espacios, que será la referencia de comparación y análisis por el lector para facilitar o impedir la apertura de accesos.

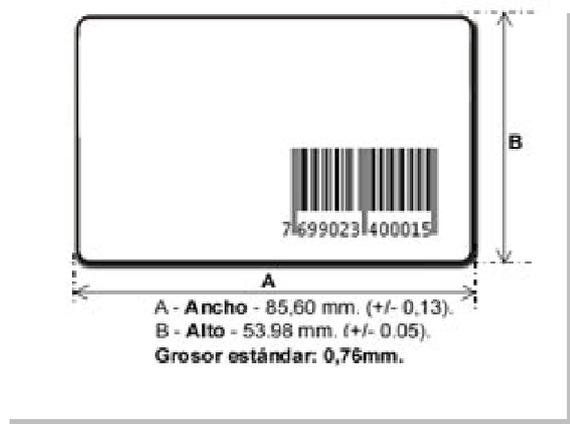
Pueden ser:

- Reflexivas: de carácter pasivo, económicas y bajo nivel de seguridad.
- Transmisivas o emisoras: precio medio y elevada seguridad.

Entre las características básicas de estos elementos se destaca:

- Impresión en blanco y negro o color, tanto del código como de los diferentes aspectos personalizables: logotipos, textos, dibujos, fotografía, fondos, etc.
- Se emplean diversas simbologías (modos de codificar la información en forma de barras y espacios): código 39, código 93, código 128.
- No se produce desgaste en el uso de la tarjeta y el lector ya que la lectura se efectúa por medio de un haz luminoso.
- Esta técnica impide asimismo el posible rayado del código, que podría convertirse en ilegible por el equipo.
- Posibilidad de añadir una banda de protección sobre el código para mantenerlo oculto en previsión de obtener duplicados por fotocopia y practicar rayas superficiales.
- Resistencia a la fractura, humedad y las temperaturas elevadas.
- Es conveniente protegerlas en fundas o bolsas para evitar rozaduras susceptibles de inutilizar el código.
- Su bajo coste es una ventaja a considerar en la adquisición.
- Su aplicación en el control de acceso se ha generalizado para entidades de todo tipo: empresas, instalaciones deportivas, urbanizaciones, estacionamientos, edificios, etc.

Figura 11. Tarjeta código de barras



Fuente: Tarjeta de código de barras [en línea]. [Consultado 24 de Octubre de 2008]. España: Avanze nuevas tecnologías S.A. 2005. Disponible en Internet: www.loyalstudio.com/WLS/images/isobarras.jpg

Pueden ser mixtas, al combinarse con otras tecnologías: banda magnética, proximidad, Wiegand.

Otras aplicaciones del código de barras: comercios, inventarios, facturación, envíos, documentación, control de calidad, etc.

- **Tarjeta magnética.** Tarjetas, cuyo formato se ha extendido en múltiples aplicaciones, que contienen la información codificada en una banda magnética incrustada en el elemento.

Admite dos formas de utilización sobre el lector, introducción o pasada, y opera al comparar y reconocer el código particular procediendo a la apertura de un acceso (puerta, portón, barrera, cierre metálico, torno, portillo, etc.) o manteniendo el bloqueo del paso.

Figura 12. Tarjeta magnética.



Fuente: Tarjeta Magnetica. [en línea]. Barcelona: Accesor Applications and Services, S.A., 2003. [Consultado 24 de Octubre de 2008]. Disponible en Internet: http://www.accesor.com/productos/art/105_1.jpg

Sus características principales son:

- Grabación de códigos por medio de codificadora específica.
- Los códigos posibles de grabarse son numerosos, por lo que las probabilidades de repetirse son casi nulas.
- Habilitación y cancelación desde el propio lector, unidades especiales o por medio de software específico.
- Resistencia a la fractura, humedad y las temperaturas elevadas.
- Representa una solución alternativa y ventajosa frente a las llaves y cerraduras al agilizarse las operaciones manuales e incrementarse las posibilidades de control sobre los accesos.
- Es conveniente protegerlas contra el rayado de la banda magnética y la influencia de campos magnéticos que borrarían o dañarían los datos codificados.

- Su aplicación es frecuente para identificar a las personas que precisan un servicio (cajero automático), para desbloquear una acceso, para controlar la presencia, para autorizar el uso de equipos y maquinaria, etc.
- Su instalación se ha generalizado en gran cantidad de oficinas e instalaciones industriales o comerciales para controlar el acceso y presencia de empleados.

Pueden ser mixtas, al combinarse con otras tecnologías: código de barras, proximidad, Wiegand.

Diferentes acabados en cuanto a formato, grosor y color pudiendo personalizarse mediante la impresión de textos, imágenes, logos, fotos, etc.

Su tecnología es muy conocida debido a la implantación en las abundantemente utilizadas tarjetas de crédito y compra.

- **Tarjeta de proximidad.** Son medios que proporcionan un alto nivel seguridad al permitir la identificación de cada usuario por medio de un código único e irreplicable grabado en fabricación y que no se puede modificar, falsificar o duplicar. Esta tarjeta lleva incorporado emisor de ondas radio que son reconocidas o desestimadas por un equipo receptor, permitiendo o denegando el acceso, respectivamente.

Se puede referir también a éstas como tarjetas de "manos libres" al no ser precisa la introducción o deslizamiento por el lector, incluso, a veces, ni la extracción de la cartera o bolsillo en que se porte.

Sus características más rescatables son:

- Este medio ofrece una alta fiabilidad, siempre que quien la porte, sea persona autorizada.
- La vida útil de este elemento es muy prolongada por no requerir el contacto directo con los equipos de lectura.
- Puede asignarse a nuevos usuarios.
- Grabación de códigos por medio de codificadora específica.
- Los códigos posibles de grabarse son numerosos, garantizándose la imposibilidad de copia.
- Habilitación y cancelación desde el propio lector, unidades especiales o por medio de software específico.
- No precisa de alimentación externa (batería o pila) ni de red ya que la lleva a cabo por la inducción generada por el campo magnético del lector.
- Velocidad de lectura superior a otras tarjetas, incluso sin necesidad de extraerla de bolso, cartera, billetera, etc.
- Resistentes a la fractura, humedad y las temperaturas elevadas.

- Representa una solución alternativa y ventajosa frente a las llaves y cerraduras al agilizarse las operaciones manuales e incrementarse las posibilidades de control sobre los accesos.
- Su instalación se ha generalizado en gran cantidad de oficinas e instalaciones industriales o comerciales para desbloquear elementos de cierre, además de controlar el acceso y presencia de empleados.
- Diferentes acabados en cuanto a formato, grosor y color pudiendo personalizarse mediante la impresión de textos, imágenes, logos, fotos, etc.

Figura 13. Tarjeta de Proximidad



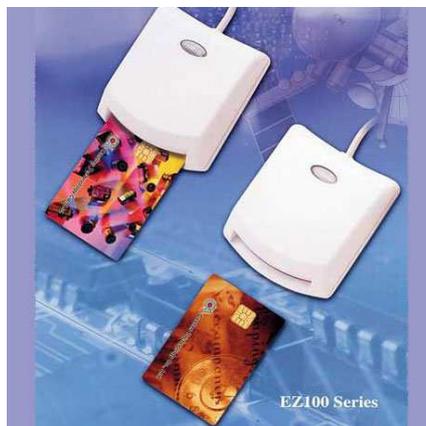
Fuente: tarjeta de proximidad. [En línea]. España: Euroquat, 2006. [Consultado 24 de Octubre de 2008]. Disponible en Internet: <http://www.euroquat.es/Tarjetasplasticas/proximidad.jpg>

Pueden ser mixtas, al combinarse con otras tecnologías: código de barras, banda magnética, Wiegand.

- **Tarjeta inteligente o chip.** Esta tarjeta incorpora un microchip con capacidad de almacenamiento de información (datos, claves, etc.) que son comparados en el equipo lector con códigos predefinidos para facilitar o impedir la apertura de accesos.

Se le considera apropiado para espacios donde se precise un nivel alto de seguridad por ofrecer amplias garantías contra el copiado y utilización por persona ajena ya que, es frecuente, el requerimiento de contraseñas o claves.

Figura 14. Tarjetas Inteligentes



Fuente: Tarjetas inteligentes. [en línea]. Argentina: CopyDat 2005[Consultado 24 de Octubre de 2008]. Disponible en Internet: <http://www.copydat.com.ar/images/products/EZ100NR.jpg>

Estas son algunas de sus características:

- Este medio ofrece una alta fiabilidad, siempre que quien la porte sea persona autorizada.
- Posibilidad de incorporar el microchip a tarjetas existentes.
- Capacidad de almacenamiento y memoria superior a otras tarjetas.
- Permite borrar y volver a grabar datos en la memoria.
- Admite la lectura y grabación de información variada.
- Seguridad de la información almacenada, impidiendo su reproducción.
- Integra diversas aplicaciones en el mismo soporte.
- Capacidad para procesar la información contenida (microprocesador).
- Posibilidad de funcionamiento combinado con otras tecnologías.
- Posibilidad de grabación remota de datos por el usuario.
- Más de diez mil operaciones de grabación y/o borrado.
- Memoria fiable durante más de diez años.

Otras aplicaciones: acceso a servicios bancarios o equipos informáticos, abonar compras, llamadas telefónicas, máquinas autoservicio, transportes, estacionamientos, etc.

Se prevé un considerable incremento del uso de esta tecnología en un futuro próximo.

- **Tarjetas de infrarrojos.** Las tarjetas de infrarrojos contienen un código grabado para su lectura por medio de un haz luminoso emitido por un lector sin requerir un contacto directo.

Entre sus características se puede destacar:

- Este medio ofrece una alta fiabilidad, siempre que quien la porte, sea persona autorizada.
- No se produce desgaste en el uso de la tarjeta y el lector ya que la lectura se efectúa por medio de un haz luminoso.
- La vida útil de este elemento es muy prolongada por no requerir el contacto directo con los equipos de lectura.
- Se añade una capa de protección sobre el código que no impide el paso de los rayos infrarrojos al efectuarse la lectura.
- Grabación de códigos por medio de codificadora específica.
- Los códigos posibles de grabarse son numerosos, garantizándose la imposibilidad de copia.
- Habilitación y cancelación desde el propio lector, unidades especiales o por medio de software específico.
- Velocidad de lectura superior a otras tarjetas.
- Resistencia a la fractura, humedad y las temperaturas elevadas.

• **Tarjetas Wiegand:** Esta tecnología es similar a la empleada por las tarjetas magnéticas ya que también el lector debe identificar el código almacenado en la banda magnética, con las diferencias siguientes:

- El código se graba en unos cables integrados en la banda magnética.
- Cada cable posee unas cualidades magnéticas diferenciadas.
- Estas peculiaridades del código permiten su modificación y borrado.
- También admite la posibilidad de cifrar el código.
- Las tarjetas pueden ser leídas sin requerir el contacto directo con el lector consiguiendo evitar su desgaste y alargar la vida tanto del lector como de la tarjeta.
- Pueden ser mixtas, al combinarse con otras tecnologías: código de barras, banda magnética, proximidad.

Otros tipos de tarjeta factibles de emplear para el control de acceso de personas, y que no vamos a desarrollar por ser utilizadas escasamente, son:

- Tarjetas holográficas.
- Tarjeta electrónica.
- Tarjeta capacitiva.
- Tarjeta mecánica.

5.1.4. Biométricos.

La biometría podría definirse como una tecnología basada en el reconocimiento de ciertos rasgos físicos particulares de las personas. Su aplicación en el ámbito de la seguridad se ha orientado hacia los sistemas de control de acceso de personas con al intención de lograr una identificación fiable y segura.

El principio de funcionamiento de estos sistemas consiste en el reconocimiento de ciertas características específicas de cada persona que son almacenadas en la memoria del equipo para ser comparadas con un patrón (PIN) cuando los usuarios presentan sus rasgos particulares de huellas, voz, palma de la mano, huella, iris, etc.

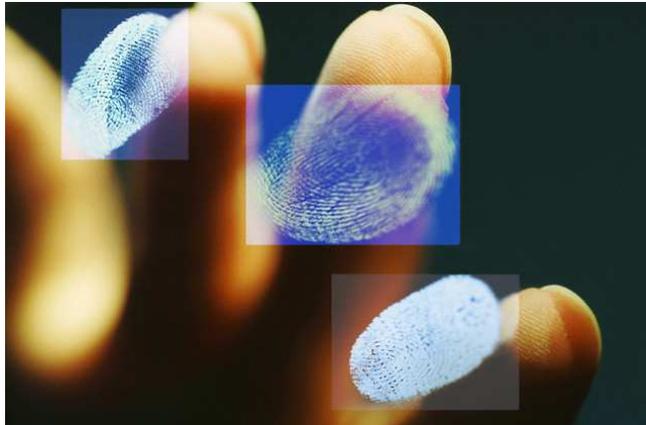
Como ventaja frente a llaves y sistemas de identificación electrónicos portados debemos señalar su imposibilidad de cesión a otros usuarios (delito de suplantación de la personalidad), olvido, extravío o sustracción; asimismo no es preciso memorizar complicados códigos numéricos, claves o contraseñas, fáciles de obtener por intimidación o coacción.

En resumen, se consigue una verificación personalizada y, consecuentemente, una elevada seguridad y fiabilidad en la identificación de personas al basarse en rasgos particulares e irrepetibles.

Debido a estas características tan singulares se han convertido en sistemas imprescindibles para controlar el acceso en áreas de máxima seguridad, siendo frecuente el empleo combinado con otros equipos, como lectores de tarjetas (de banda magnética, de proximidad, de códigos de barras), teclados, etc. con la finalidad de asegurar la identificación de las personas autorizadas.

- **Reconocimiento de la huella dactilar.** Equipo que permite identificar las personas por el reconocimiento de su característica, intransferible y exclusiva huella dactilar que es capturada y analizada al presentarse en el lector, el cual actúa en consecuencia, confirmando o denegando el acceso.

Figura 15. Reconocimiento de huella.



Fuente: [en línea]. México: Compublish magazine, 2006[Consultado 24 de Octubre de 2008]. Disponible en Internet: <http://www.compublish.com/img/CRBR002810.jpg>

Para ello, al dar de alta (escanear) una nueva huella, se crea un perfil biométrico que es memorizado con el fin de verificar posteriores intentos de acceso.

Seguidamente se puede reseñar otras características:

- Posibilidad de trabajar en modo autónomo u off-line (el equipo se encarga de todas las funciones) y on-line o conectado en red y controlados, local o remotamente, por un sistema informático con el correspondiente software de gestión.
- Gran capacidad de almacenamiento de datos (perfil de huellas).
- Velocidad de lectura y verificación aceptable (1 segundo).
- Almacenamiento en memoria de acontecimientos: admisiones, denegaciones, fallos, averías, etc.
- Aceptación del desplazamiento (unos 5 mm.) o rotación del dedo (unos 15 °).
- Integración en otros sistemas de control de acceso implantados (tornos, puertas, barreras) y combinación con otros medios de identificación automática (lectores de tarjetas, teclados).
- Confirmación de operaciones por medio de señales acústicas, ópticas o mensajes hablados.
- Programación de diversos parámetros y condiciones.
- Posibilidad de instalación en red para controlar tanto el acceso como la presencia de numerosas personas en múltiples ubicaciones.
- No hay que preocuparse de portar objetos para identificarse ni de su custodia.
- Posibilidad de montaje superficial o empotrado en paredes o puertas.

- Existen equipos de identificación portátiles, conectables a cualquier toma eléctrica o ensamblados con fuente de alimentación propia.
- Como aplicación alternativa se emplea también para autorizar el acceso y uso en ordenadores.

- **Reconocimiento por la geometría de la mano.** Estos equipos permiten identificación de las personas por el reconocimiento del perfil tridimensional de la mano (exclusivo de cada persona) que es capturado al presentarse en la pantalla del lector.

Para ello, al dar de alta un nuevo perfil de mano, se crea un patrón que es almacenado en memoria para posteriores comprobaciones de acceso. Hay equipos que actualizan el patrón de referencia cada vez que detectan cambios mínimos en el perfil presentado, siendo las causas más frecuentes hematomas, contusiones, cicatrices, etc.

Otras características reseñables son:

- Posibilidad de trabajar en modo autónomo u off-line (el equipo se encarga de todas las funciones) y on-line o conectado en red y controlados, local o remotamente, por un sistema informático con el correspondiente software de gestión.
- Gran capacidad de almacenamiento de datos (patrones).
- Programación de diversos parámetros y condiciones, así como conexión de periféricos.
- Velocidad de lectura y verificación aceptable.
- Discrimina pequeños desplazamientos, desvíos o rotaciones al presentar la mano para su lectura.
- Almacenamiento en memoria de acontecimientos: admisiones, denegaciones, fallos, averías, etc.
- Confirmación de operaciones por medio de señales acústicas, ópticas o mensajes hablados.
- Discrimina la presencia de cambios poco significativos motivados por anillos o alianzas, tiritas o apósitos, heridas o cortes, etc.
- Posibilidad de instalación en red para controlar tanto el acceso como la presencia de numerosas personas en múltiples ubicaciones.
- Integración en otros sistemas de control de acceso implantados (tornos, puertas, barreras) y combinación con otros medios de identificación automática (lectores de tarjetas, teclados).
- No hay que preocuparse de portar objetos para identificarse ni de su custodia.

Figura 16. Reconocimiento por geometría de mano



Fuente: Reconocimiento geometria mano [en línea]. Bogotá: Controles y seguridad S.A. [Consultado 24 de Octubre de 2008]. Disponible en Internet: <http://www.whlcontroles.com/images/HAND.jpg>

- **Reconocimiento de la voz.** Equipo que permite identificar las personas por el reconocimiento de características fónicas (tono, timbre, intensidad) de la voz. El usuario habla a través de un teléfono o micrófono conectado a un controlador que verifica la coincidencia con el perfil almacenado y actúa en consecuencia, confirmando o denegando el acceso.

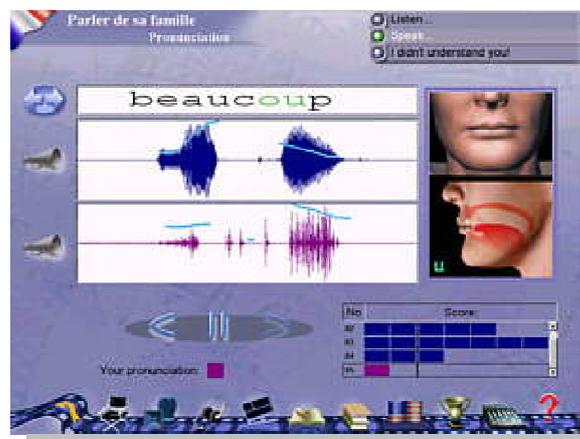
Para ello, al dar de alta una nueva caracterización, se crea un perfil biométrico que es memorizado con el fin de cotejar posteriores intentos de acceso. Estos equipos actualizan el patrón de referencia cada vez que detectan cambios mínimos en el perfil captado.

Otras características de estos equipos son:

- Posibilidad de trabajar en modo autónomo u off-line (el equipo se encarga de todas las funciones) y on-line o conectado en red y controlado, local o remotamente, por un sistema informático con el correspondiente software de gestión.
- Es conveniente utilizar una frase secreta por cada usuario ya que se aumenta la seguridad al desconocer la "longitud" del mensaje.
- Gran capacidad de almacenamiento de datos.
- Velocidad de lectura aceptable.
- Integración en otros sistemas de control de acceso implantados (tornos, puertas, barreras, etc.) y combinación con otros medios de identificación automática (lectores de tarjetas, teclados).

- Almacenamiento en memoria de acontecimientos: admisiones, denegaciones, fallos, averías, etc.
- Confirmación de operaciones por medio de señales acústicas, ópticas o mensajes hablados.
- Programación de diversos parámetros y condiciones.
- Posibilidad de instalación en red para controlar tanto el acceso como la presencia de numerosas personas en múltiples ubicaciones.
- No hay que preocuparse de portar objetos para identificarse ni de su custodia.

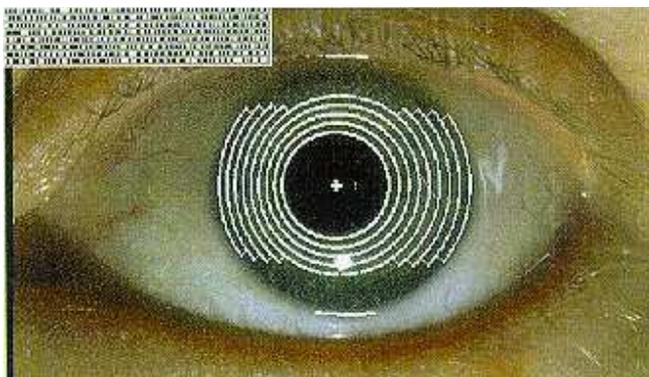
Figura 17. Reconocimiento de voz.



Fuente: Reconocimiento de voz [en línea]. Argentina, Tecnología Educativa S.A., 2006 [Consultado 24 de Octubre de 2008]. Disponible en Internet: <http://www.tecnoedu.com/Soft/img/Tellmerek2.jpg>

- **Reconocimiento por la retina o iris.** Equipo que permite identificar las personas por el reconocimiento de la disposición de los vasos sanguíneos de la retina, cuya forma y número es capturada y analizada al presentarse en el lector, el cual actúa en consecuencia, confirmando o denegando el acceso. Para ello, al dar de alta una nueva forma de retina, se crea un perfil biométrico que es memorizado con el fin de verificar posteriores intentos de acceso. El lector detecta la presencia de usuarios y presenta una abertura desde la cual se debe mirar hacia puntos establecidos mientras el equipo capta los datos a verificar.

Figura 18. Reconocimiento de iris o retina.



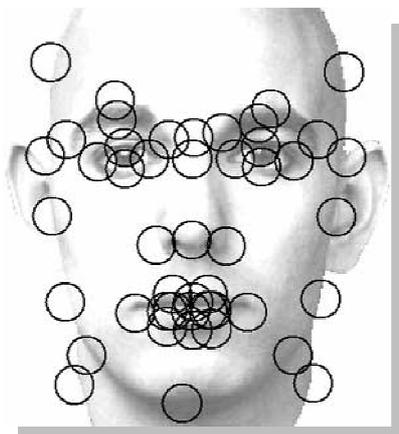
Fuente: Reconocimiento de iris [en línea]. Venezuela: Escuela de Ingeniería Eléctrica Universidad Central de Venezuela, 2008 [Consultado 24 de Octubre de 2008]. Disponible en Internet: http://neutron.ing.ucv.ve/revista-e/No6/Olquin%20Patricio/Mapa_Iris.gif

Entre otras características de estos equipos señalamos:

- Posibilidad de trabajar en modo autónomo u off-line (el equipo se encarga de todas las funciones) y on-line o conectado en red y controlado, local o remotamente, por un sistema informático con el correspondiente software de gestión.
 - Gran capacidad de almacenamiento de datos.
 - Velocidad de lectura aceptable.
 - Integración en otros sistemas de control de acceso implantados (tornos, puertas, barreras, etc.) y combinación con otros medios de identificación automática (lectores de tarjetas, teclados).
 - Programación de diversos parámetros y condiciones.
 - Almacenamiento en memoria de acontecimientos: admisiones, denegaciones, fallos, averías, etc.
 - Confirmación de operaciones por medio de señales acústicas, ópticas o mensajes hablados.
 - No hay que preocuparse de portar objetos para identificarse ni de su custodia.
-
- **Reconocimiento facial.** Equipo que permite identificar las personas por el reconocimiento de sus particulares y únicas características de la cara, que son capturadas por una cámara de televisión y comparadas con las almacenadas en memoria del sistema, el cual actúa en consecuencia, autorizando o denegando el acceso.

Para ello, al dar de alta un nuevo rostro, se crea un perfil biométrico que es memorizado con el fin de verificar posteriores intentos de acceso.

Figura 19. Reconocimiento facial



Fuente: face recognition. [en línea]. Estados Unidos: Worcester Polytechnic Institute. 2008 [Consultado 24 de Octubre de 2008]. Disponible en Internet: <http://www.wpi.edu/News/Transformations/2002Spring/Images/recognition1.jpg>

Estas son algunas de sus características:

- No precisa el contacto físico con el equipo.
 - Reconocimiento desde distintos ángulos e, incluso, con cambios en el aspecto: cortes de pelo, gestos, gafas, prendas para la cabeza, etc.
 - Rechaza automáticamente fotos, fotocopias, caricaturas.
 - Almacenamiento en memoria de acontecimientos: admisiones, denegaciones, fallos, averías, etc.
 - Confirmación de operaciones por medio de señales acústicas, ópticas o mensajes hablados.
 - Posibilidad de grabación de las imágenes de los accesos autorizados y/o denegados.
 - Posibilidad de funcionamiento autónomo o conectado en red.
 - Integración en otros sistemas de control de acceso implantados (tornos, puertas, barreras).
 - No hay que preocuparse de portar objetos para identificarse ni de su custodia.
- **Reconocimiento por la forma del tecleo.** El usuario debe teclear una sucesión determinada de números, sobre la cual se ha creado un PIN en la memoria en función del ritmo de pulsaciones, y el equipo analizará esa peculiar forma de tecleo actuando en consecuencia, confirmando o denegando el acceso.

Este sistema de identificación biométrica mantiene escasa implantación, motivada por las dudosas garantías de seguridad ofrecidas. Algunas de sus características:

- Almacenamiento en memoria de acontecimientos: admisiones, denegaciones, fallos, averías, etc.
- Confirmación de operaciones por medio de señales acústicas, ópticas o mensajes hablados.
- Posibilidad de funcionamiento autónomo o conectado en red.
- Integración en otros sistemas de control de acceso implantados (tornos, puertas, barreras).
- No hay que preocuparse de portar objetos para identificarse ni de su custodia.

• **Reconocimiento por la forma de la firma.** Sistema que permite identificar las personas por el reconocimiento de la forma de la firma. El usuario elabora la firma en una pantalla de digitalización con un lápiz especial mientras un controlador verifica la coincidencia con el perfil (PIN) almacenado y actúa en consecuencia, confirmando o denegando el acceso.

Otras de sus características son:

- Posibilidad de trabajar en modo autónomo o conectado en red.
- Programación de diversos parámetros y condiciones.
- Almacenamiento en memoria de acontecimientos: admisiones, denegaciones, fallos, averías, etc.
- Confirmación de operaciones por medio de señales acústicas, ópticas o mensajes hablados.
- Integración en otros sistemas de control de acceso implantados (tornos, puertas, barreras) y combinación con otros medios de identificación automática (lectores de tarjetas, teclados).
- No hay que preocuparse de portar objetos para identificarse ni de su custodia.

5.1.5. Equipos combinados: lector o teclado y biométrico.

La implantación de los sistemas biométricos se ha concentrado en áreas que exigen un alto nivel de protección, el cual es frecuentemente reforzado al vincularse la operatividad del sistema con otros equipos de identificación automática, como teclados o lectores de tarjetas.

Las exigencias de acatar dos requisitos de identificación, al supeditar la autorización de paso a dos sistemas, han orientado su aplicación hacia actividades y sectores donde prevalezcan los criterios redundantes de seguridad sobre los de reducción de costes.

El resultado es una alta fiabilidad en las operaciones de control de accesos fruto de la combinación integrada o ampliada de las funciones y prestaciones propias de cada equipo. En las tarjetas chip es factible grabar el perfil del rasgo biométrico en la memoria de la tarjeta.

Por lo tanto el sistema reúne y complementa las características propias del sistema de identificación biométrico y las del elemento portado o teclado, anteriormente expuestas en cuanto a:

- Funcionamiento en modo autónomo o conectado en red y control, local o remoto.
- Capacidad de almacenamiento de datos (perfiles).
- Velocidad de lectura y verificación.
- Almacenamiento en memoria de acontecimientos.
- Integración en otros sistemas de control de acceso implantados.
- Confirmación de operaciones por medio de señales.
- Programación de diversos parámetros y condiciones.
- Aplicaciones informáticas compatibles con sistemas operativos de uso generalizado.

• **Equipo vía radio.** El equipo consta de un emisor de ondas radio, en una frecuencia determinada, que activa los mecanismos de apertura de acceso al ser captadas por un receptor que las analiza.

Entre sus características destacamos:

- Este medio ofrece una alta fiabilidad, siempre que quien lo porte sea persona autorizada.
- La vida útil de este elemento es muy prolongada por no requerir el contacto directo con los equipos de lectura.
- No requiere la aproximación a distancias de lectura relativamente cortas.
- Velocidad de lectura superior a muchas tarjetas, incluso sin necesidad de extraerla de bolso, cartera, billetera, etc.
- Habilitación y cancelación desde el propio equipo o por medio de unidades especiales.
- Proporciona un nivel de seguridad elevado en la identificación automática.
- Posibilidad de ocultar o disimular en el entorno de ubicación tanto el equipo receptor como la antena.
- Representa una solución alternativa y ventajosa frente a las llaves y cerraduras al agilizarse las operaciones manuales e incrementarse las posibilidades de control sobre los accesos.

• **Equipos combinados: lector y teclado.** La implantación de los sistemas de control de acceso es obligatoria en áreas que exigen un nivel aceptable de

protección, el cual se pretende conseguir a menudo con la implantación de equipos que integran dos tipos diferentes de tecnologías de identificación. La combinación más utilizada es el lector de tarjetas magnéticas y un teclado numérico con funcionamiento vinculado al cumplimiento de las exigencias comunes de estos dos sistemas de identificación.

Las prestaciones de estos equipos han orientado su aplicación hacia actividades y sectores donde prevalecen criterios redundantes de seguridad sobre los de reducción de costes.

El resultado es una alta fiabilidad en las operaciones de control de accesos fruto de la combinación integrada de las funciones propias de cada tecnología. Por lo tanto el sistema reúne y complementa las características propias del teclado y las del elemento portado, anteriormente expuestas en cuanto a:

- Funcionamiento en modo autónomo o conectado en red y control, local o remoto.
- Capacidad de almacenamiento de datos (perfiles).
- Velocidad de lectura y verificación.
- Almacenamiento en memoria de acontecimientos.
- Integración en otros sistemas de control de acceso implantados.
- Confirmación de operaciones por medio de señales.
- Programación de diversos parámetros y condiciones.
- Implantación en espacios interiores o exteriores.
- Aplicaciones informáticas compatibles con sistemas operativos de uso generalizado.

• **Teclado numérico.** Este dispositivo posibilita la introducción de un código numérico mediante la pulsación de los dígitos correspondientes en el terminal de captación. Esos números son comparados con los almacenados en la memoria del equipo, procediendo a la apertura de accesos si coinciden con los códigos cargados, desechándolos en caso contrario.

Características generales de estos medios de control de acceso son:

- Posibilidad de funcionamiento autónomo (off-line) o conectado en red (on-line).
- Posibilidad de conexión local o remota a PC, que asumirá las funciones de recepción y tratamiento de la información recogida.
- Programación desde el propio teclado o desde unidades centrales para los equipos en red.
- Autocomprobación del estado de equipos y medios de transmisión.
- Confirmación de las operaciones mediante display, led y/o señal acústica.
- Conservación de datos y últimos eventos ante la falta de suministro eléctrico.

- Cuentan con salidas de relé para apertura de accesos, activación de alarmas, sirenas, etc. además de entradas para detectar puertas abiertas y otras funciones adicionales.
- Integración en otros equipos: torniquetes, portillos, esclusas, etc. y sistemas de control de acceso.
- Montaje tanto en interior como exterior, en superficie o empotrado, pared o poste.
- Conexión habitual por cable, aunque también existen equipos inalámbricos.
- Teclado de membrana, alfanumérico, retroiluminado, con display o visor, indicadores luminosos, puerto de comunicaciones, etc.
- Instalación y disposición anti vandalismo del equipo.
- Autoprotección contra sabotajes, el polvo, la intemperie, el agua, etc.
- Sus funciones son controladas por una unidad de control que almacena los códigos de usuario, facilita altas y bajas, alimenta los teclados, etc.
- Código de amenaza: genera una alarma silenciosa cuando el usuario está amenazado, posibilitando la ayuda de terceros.

• **Identificación óptica. CCTV.** La implantación de sistemas de vigilancia óptica electrónica en los controles de accesos ha supuesto un considerable aumento cualitativo de las prestaciones de los equipos empleados para tales funciones al permitir la identificación visual de las personas que acceden a las instalaciones o recintos sin riesgo físico para el personal encargado del control, que puede efectuarse tanto desde puestos locales como remotos.

Las características y prestaciones que ofrecen son:

- El procedimiento de identificación puede ser por visualización continua de monitores por parte del personal encargado o vinculada a la presencia detectada por un sensor o fotocélula, video-sensor, la utilización de una tarjeta, la pulsación de dispositivo, etc.
- Las identificaciones, tanto positivas como negativas, se almacenarán en dispositivos de grabación para su posterior tratamiento o consulta.
- Esta técnica de identificación facilita la toma de decisiones al personal responsable, sin exponerse a riesgos que conlleva la identificación directa.
- Dependiendo de la magnitud de la instalación es factible efectuar un seguimiento de los movimientos interiores de las personas y controlarles mientras permanecen en el recinto.

5.2. CONTROL DE ACCESOS DE VEHÍCULOS

5.2.1. Medios Pasivos para Control de Accesos de Vehículos.

En este apartado se hace referencia a elementos físicos muy empleados para el control de accesos de vehículos, aunque frecuentemente se les incorporan

mecanismos o sistemas electrónicos con el fin de conseguir una mayor efectividad y operatividad en las operaciones que realizan.

Alguno de estos medios pasivos, que habitualmente se instalan para el control de acceso de vehículos son:

- Canalización.
- Barreras.
- Puertas.
- Puertas o portones pivotantes o abatibles.
- Puertas o portones suspendidos.
- Puertas basculantes.
- Puertas enrollables.
- Puertas seccionales.
- Puertas o portones deslizantes o correderos.
- Elementos de cierre: cerraduras.
- Obstáculos escamoteables.
- Esclusas para vehículos.

• **Canalización.** Este concepto se refiere a la disposición de los medios adecuados para obligar a los vehículos a acceder y circular por los itinerarios específicos, con el objetivo de dirigirlos hacia equipos o personal de control. Según los medios anteriormente mencionados puede ser:

- Canalización arquitectónica: emplea elementos constructivos para encaminar los vehículos: muros, muretes, barandillas, etc.
- Canalización por medios físicos: se colocan estratégicamente pivotes, conos, bolardos, vallas móviles, jardineras, maceteros, para dirigir los vehículos hacia el punto de control.

• **Barreras automáticas.** Elemento rígido o articulado consistente en una barra cuya longitud se adapta a la anchura del vial de paso, permaneciendo en posición horizontal para detener los vehículos y elevándose para facilitar el acceso.

Figura 20.Barreras automáticas



Fuente: Barreras automáticas. [en línea]. Barcelona: Accesor Applications and Services, S.A., 2003. [Consultado 24 de Octubre de 2008]. Disponible en Internet: http://www.accesor.com/noticias/img_not/68_1mig.jpg

Características básicas de estos medios son:

- Fijación a soporte oculto en una caja con otros mecanismos.
 - Sistema de apertura automática por control remoto (botonera), a distancia (telemando) o vinculada a lectores de llaves o tarjetas, teclados, biométricos, detector de
 - lazo magnético, etc.
 - Sistema de apertura/cierre manual para maniobrar en casos de ausencia de corriente.
 - Diferentes usos (residencial o intensivo), tanto para interior como exterior.
 - Material de construcción en aluminio o fibras de escaso peso, pintadas por ambos lados en franjas de color rojo y blanco reflectante, con imprimación anticorrosión para resistir las inclemencias meteorológicas.
 - Posibilidad de adaptación de la barra a la longitud del acceso.
 - Regulación de la velocidad de elevación, descenso y de finales de carrera, sin vibraciones.
 - Posibilidad de añadir accesorios para mejorar su seguridad: soporte de apoyo en el extremo, avisadores ópticos luminosos, franjas reflectantes, sistema de seguridad anti aplastamiento, control centralizado, etc.
 - Incorporación de sistema detección de obstáculos (fotocélulas, infrarrojos, lazo magnético o inductivo), procediendo a la interrupción inmediata de la operación y actuar inversamente.
-
- **Obstáculos escamoteables.** Estos medios se implantan para controlar el acceso de vehículos a zonas o áreas que lo tienen restringido: áreas

residenciales, centros y edificios oficiales, instalaciones industriales, cascos históricos, zonas peatonales, etc. Pueden ser de diferentes tipos:

- Estructura metálica en forma de cuña inversa que se eleva 45º grados sobre el suelo para obligar a la detención de los vehículos.
- Dados metálicos o pivotes alineados que se elevan verticalmente para impedir el paso de los vehículos.
- Pilón o bolardo retráctil: cuando supera el nivel de superficie impide el paso el paso de vehículos y lo facilita al descender.

Características comunes a estos equipamientos son:

- Todos ellos se ocultan en el suelo para facilitar el acceso.
- Su uso más frecuente es obligar a la detención de vehículos con el fin de realizar las oportunas operaciones de inspección y control.
- La activación puede estar vinculada a la identificación individual de personas por lector de tarjetas, teclados, biométricos, etc.
- El accionamiento puede realizarse mediante dispositivos electromecánicos, apertura automática, remota o a distancia.
- Materiales de construcción resistentes (acero, hierro, aleaciones, etc.), capaces de soportar impactos a velocidad de 100 Km/h.
- Tiempos de subida y de bajada del obstáculo regulable, así como el de permanencia en posición oculta.
- Ocultación automática o por fuerza de gravedad en casos de suspensión del suministro eléctrico, emergencias, evacuación, etc. También es posible mediante un interruptor para emergencias.
- Posibilidad de personalizarse añadiendo escudos, anagramas, logotipos, de empresas, entidades, ayuntamientos, organismos, etc.

• **Esclusas para vehículos.** El objetivo de este sistema de control de entradas y salidas es el mismo que para las personas, al habilitar un espacio entre dos o más puertas, portones u otras barreras que tienen supeditada su apertura al cerramiento previo de la anterior.

Por ello, su aplicación primordial es para realizar las inspecciones de cargas y vehículos a fin de poder detectar la presencia de explosivos, armas, drogas, objetos u mercancías de la propia instalación, etc. En caso afirmativo el vehículo queda confinado entre dichas puertas o barreras para facilitar el tratamiento de la incidencia: requisar, avisar a el responsable de seguridad o las fuerzas policiales, etc.

Estos medios también se les considera de autorización automática por facilitar el paso tras un proceso de identificación positiva sin la intervención de personal operativo.

- **Arco Detector magnético.** Dispositivo que capta la presencia de masas metálicas, abundantes en los componentes de personas y vehículos (turismos, motocicletas, camiones), para informar a un controlador de accesos o aplicación informática que efectuarán las acciones establecidas: apertura de puerta, levantamiento de barrera, expedición de ticket, detección del obstáculo, etc.

Figura 21. Arco detector magnético.



Fuente: Arco detector magnético [en línea]. México: APRINSA, 2008 [Consultado 18 de Diciembre de 2008]. Disponible en Internet: http://www.aprinosa.com/shop/view_product.php?product=CS%205000

Algunas de sus características son:

- Sensibilidad ajustable.
- Capacidad de detección permanente en un tramo: con ello se evita la activación de cierres antes de abandonar el espacio.
- Mínimo tiempo de respuesta.
- Protección contra rayos, otras descargas eléctricas e interferencias.
- Integración en sistemas implantados o de nueva creación.
- Las aplicaciones más corrientes se centran en la activación de puertas motorizadas, barreras automáticas, expendedores de tickets, etc. en el acceso a garajes, estacionamientos, recintos, peajes, etc. y como detector de obstáculos.
- Posibilidad de identificar vehículos (turismo, camión, motocicleta) al determinar y comparar su masa metálica.
- Capacidad para identificar el sentido de circulación del móvil, mediante la colocación de dos detectores contiguos.

- **Detector por radiofrecuencia.** El vehículo porta un microchip o tag con su número de identificación particular que será captado por las ondas de radiofrecuencia emitidas por el lector cuando dicho móvil se encuentra en las

proximidades, procediendo a realizar la operación programada: apertura de puerta, levantamiento de barrera, liberar peaje, activar semáforo, etc.

Como características reseñables se consideran:

- El lector realiza las funciones de transmisor y receptor ya que envía una señal de radio en una frecuencia determinada, la cual activa el microchip a una distancia cercana y éste remite el número de identificación individual.
- Los componentes básicos del sistema son el lector, los microchip y las antenas, aunque pueden formar parte de otros sistemas controlados por ordenadores equipados con el software correspondiente y formar redes unidas por diferentes sistemas de comunicación.
- Esta tecnología permite la automatización de los procesos al identificar inmediatamente, sin necesidad de contacto físico con el equipo lector, facilitando el acceso del vehículo sin detenerse para introducir o pasar una tarjeta, marcar un código, pulsar un botón. Por ello esta generalizando su implantación en estacionamientos, áreas residenciales o industriales, peaje de autopistas, etc.
- La distancia de lectura no es la misma para todos los modelos, siendo frecuentemente eficaz entre los 5 y 20 cm; la velocidad del vehículo también puede ser muy variable.
- Validación y cancelación de las tarjetas o tags por medio de software específico.
- Otros datos a considerar: software de gestión, frecuencia de trabajo, alimentación, salidas de relé, temperatura de trabajo, etc.

- **Barrera de rayos infrarrojos.** Aunque no es muy frecuente, si es factible instalar estos equipos, que emplean la tecnología de infrarrojos, como detectores de presencia de vehículos al aproximarse a puertas, portones o barreras.

Son apropiadas en controles de acceso alejados de puestos de control o vigilancia constante, complementados con la supervisión por medios de captación de imágenes (identificación) vinculados a la detección realizada por los equipos. En función de las necesidades de cobertura se emplearían barreras de uno o dos haces abarcando el ancho total del vial de paso.

Muy empleados como detector del obstáculo en una zona específica: peaje, control de acceso, zona de pago, etc.

- **Captación de imágenes.** La implantación de sistemas de vigilancia óptica electrónica en los controles de accesos permite la identificación de las personas y vehículos que acceden a las instalaciones o recintos desde puestos de control remotos. Esta técnica de identificación, por visualización en un monitor, facilita la toma de decisiones al personal responsable ya que no se expone a una intervención directa que conllevaría más riesgos contra su persona.

El procedimiento de identificación se realiza mediante la visualización continua de monitores por parte del personal encargado o vinculada a la presencia detectada por un sensor, la utilización de una tarjeta, la pulsación de dispositivo, etc. Las identificaciones, tanto positivas como negativas, se almacenarán para su posterior tratamiento.

Ciertas aplicaciones específicas para aparcamientos públicos o comunitarios toman varias imágenes del vehículo para combatir los intentos de fraude por parte de usuarios que denuncian agresiones al automóvil durante el estacionamiento. Asimismo se puede disponer del video sensor, cuya aplicación práctica al control de accesos de vehículos permite detectar la aproximación y movimientos de vehículos dentro de su campo de alcance convirtiéndose en un detector de extraordinaria fiabilidad, que, además, proporciona imágenes reales de la situación.

- **Sistemas de reconocimiento de placas.** Conjunto de equipos gobernados por aplicaciones informáticas e implantados con la finalidad de automatizar las tareas propias de los controles de acceso de vehículos.

El procedimiento se puede resumir:

1. Detección de la presencia del vehículo (lazo magnético, habitualmente).
2. Identificación: una cámara capta la imagen frontal o posterior del vehículo (incluso sin detenerse) y el programa extrae los datos de la matrícula.
3. Registro de datos: los caracteres de la matrícula son almacenados en memoria o base de datos de la aplicación informática.
4. Autorización: el sistema compara la información extraída con la almacenada, autorizando el acceso en caso de coincidencia y denegándolo en el contrario.
5. Ejecución de acciones programadas: activar barreras o puertas, encender luces, entregar tickets, etc.

Admite su instalación tanto en interior como en exterior y no precisa la atención permanente de personal de vigilancia u operadores.

Permite la gestión integral de los vehículos: control de acceso y de presencia (nivel de ocupación), almacenamiento de fotogramas, elaboración de informes, listados, estadísticas, etc.

El sistema es capaz de reconocer las matrículas de vehículos de los países extranjeros de nuestro entorno más próximo.

Opcionalmente puede asociarse la captación de una imagen del conductor a la lectura de la matrícula e incluirla en las presentaciones en pantalla. También es posible la captación de imágenes de la morfología del vehículo con el fin de evitar fraudes.

Posibilidad de conexión de varios puestos de control a un solo servidor e integración con otros sistemas de seguridad y de control de acceso o presencia.

Nota: La información de los dispositivos fue extraída de una pagina electrónica, fuente: <http://www.guiadelaseguridad.com.ar/control-de-accesos.htm>

5.3. GENERALIDADES DE LOS DISPOSITIVOS

Todos los elementos, materiales y equipos suministrados deben ser nuevos, sin uso y de primera calidad, de fácil montaje, reemplazo libre de defectos e imperfectos.

Aquellos equipos que tengan una misma función deben ser iguales en esquema, diseño, elaboración y modelo.

El color de los equipos debe ser armonioso con las instalaciones del parque industrial.

Los materiales y equipos indicados deben estar sujetos a normas y especificaciones vigentes a ello, igualmente, realizar los montajes y obras necesarios para la correcta operación del sistema. Materiales y equipos deben corresponder a marcas homologadas por ICONTEC o en su defecto con normas internacionales de amplio reconocimiento.

El sistema debe ofrecer las siguientes cualidades:

- Funcionamiento durante las 24 horas del día, durante los siete días de la semana.
- Medio físico de transmisión por Fibra Óptica proyectada.
- Alimentación de equipos con AC regulada para la totalidad del sistema, evitando daños a éste por fallas de alimentación eléctrica
- Toda la información debe ser administrada directamente desde el centro de control del sistema.

5.4. ESTANDARES DEL SISTEMA AUTOMÁTICO QUE CONTROLA EL ACCESO PEATONAL Y VEHICULAR EN LA ZONA FRANCA DEL PACIFICO

Para la estandarización del proyecto se tiene un enfoque a la prevención de embotellamiento que realmente tengan que ver con la causa; que se debe mantener y controlar con relación a los equipos, personal involucrado, y métodos. El resultado para mantener y controlar, se debe clasificar de la siguiente manera:

- **Estándares relativos a los equipos:**

- Máxima eficiencia de los equipos
- Construcción de un sistema que logre:
 - Cero averías
 - Cero accidentes

- ***Estándares de limpieza, inspección y lubricación.***

- Programas de mantenimientos de hardware y software.
- Maximización de la eficiencia en cuanto a las especificaciones del WBO (World Basc Organization) referente al sistema de calidad de servicio y de seguridad en el parque industrial.

- ***Estándares relativos al personal***

- Manual de procedimientos y labores.
- Campañas de capacitación al personal involucrado.
- Aprovechamiento total de los recursos existentes.

- ***Estándares de métodos:***

- Los métodos de control de acceso implican:
 - **Identificación:** Qué presentamos para demostrar nuestra identidad.
 - **Autenticación:** Como se comprueba nuestra identidad.
 - **Autorización:** Que podemos hacer después.

Para la estandarización de la metodología World Basc Organitation; la cual es una organización que se encarga de los estándares internacionales de seguridad en la que se menciona la importancia de poseer un sistema de control de acceso para las diferentes empresas.

Donde hace referencia a puntos como los siguientes:

- En áreas críticas, debe disponerse de sistemas de alarmas, dispositivos de detección de intrusos, y de revisión de personas, equipajes, cargas y equipos de vigilancia, monitoreados y controlados permanentemente.
- Debe llevarse un registro de vehículos que ingresan y salen de las instalaciones de la empresa.
- Deben inspeccionar los vehículos al ingresar y salir de áreas críticas.
- Debe disponerse un procedimiento para el control de acceso adecuado, de empleados, contratistas y vigilantes elaborado y conservando registros de las personas que ingresan a las instalaciones, donde estuvieron, a quien visitaron, a qué horas ingresaron y a qué horas salieron de las mismas.
- Todo personal que ingresa a la instalación debe tener a la vista una identificación. Debe revisarse una verificación de la identificación de la persona que ingresa.
- El control de acceso a las instalaciones debe prever la supresión rápida y completa de la identificación otorgada por la empresa a un empleado en causa de caducidad, así como la supresión de acceso a los locales del sistema informático.
- Se debe disponer de un programa de implementación del sistema CCTV para la vigilancia perimetral de las instalaciones para las áreas críticas.
- **Estándar Wiegand.** Para el manejo de datos de los dispositivos; es importante que estos cumplan con el estándar Wiegand que es el encargado de normalizar las comunicaciones de los diferentes dispositivos sin importar la marca. La importancia de este protocolo radica en la posibilidad que presta para las compañías en determinado momento de cambiar el equipo lector sin necesidad de cambiar el resto del sistema por incompatibilidad de comunicación. También es importante mencionar que es el que se encarga de la detección de errores en la comunicación del sistema haciéndolo por medio de la paridad de los datos enviados y recibidos.
- **Estándar NISTIR 6529** También conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en 1999 por NIST y Biometrics Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.
- **Normas para instalaciones eléctricas.** En cuanto a la conexión de los equipos, se debe ceñir según las especificaciones del fabricante; teniendo en cuenta las normas del código eléctrico nacional en su última versión en ICONTEC y el Reglamento Técnico de Instalaciones Eléctricas y la ANSI.

En caso de que se presente conflicto entre las normas señaladas anteriormente, prevalecerá “Reglamento Técnico de Instalaciones Eléctricas – RETIE ”.

- **Estándar ANSI / INCITS 358** Estándar creado en 2002 por ANSI y BioApi Consortium, que presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.

5.5. GENERACION DE CONCEPTOS

Los conceptos generados a continuación se realizarán teniendo en cuenta la viabilidad de adquisición y el funcionamiento de cada uno de sus componentes. Se examinó la disponibilidad tecnológica y la forma en la cual se implementa esta tecnología en las diferentes empresas a nivel regional, nacional e internacional.

Cada uno de los conceptos serán evaluados con varios criterios de selección extraídos del estudio de necesidades del cliente, las cuales se identificaron previamente; de esta manera se conocerá cual de los conceptos generados suple de una forma completa los requerimientos y necesidades de la Zona Franca del Pacífico.

Figura 22. Generación de conceptos, ingreso peatonal

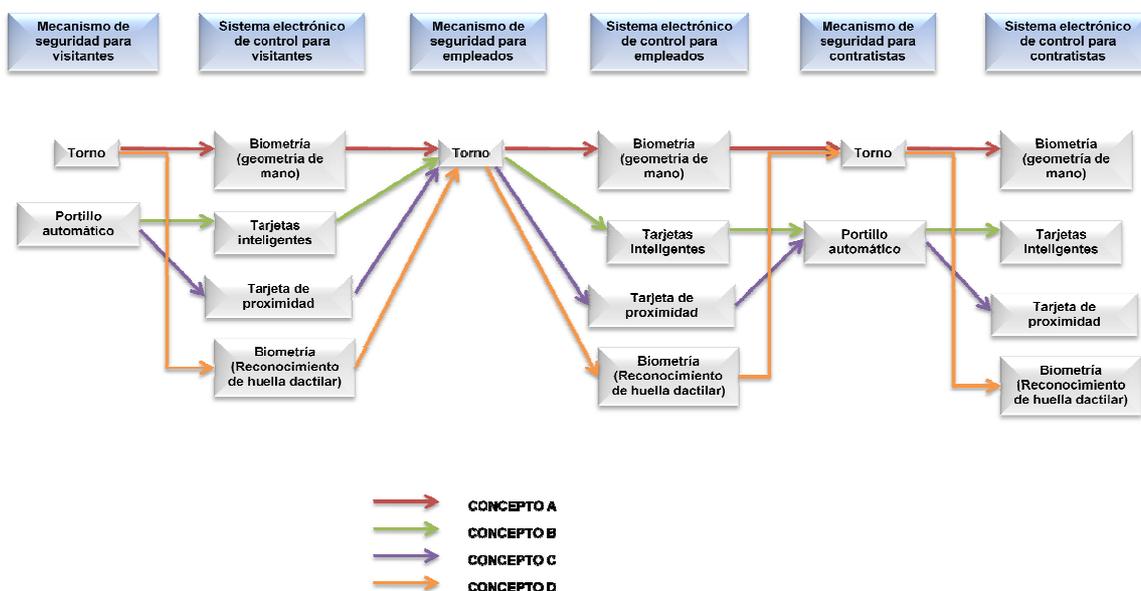


Figura 23. Generación de conceptos, ingreso vehicular

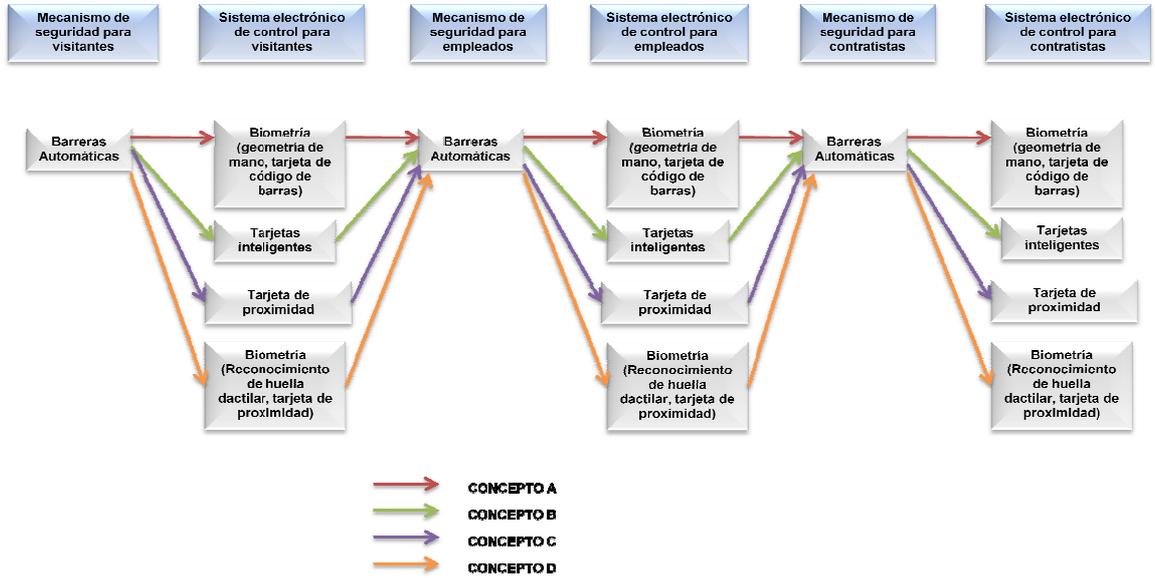


Figura 24. Concepto A

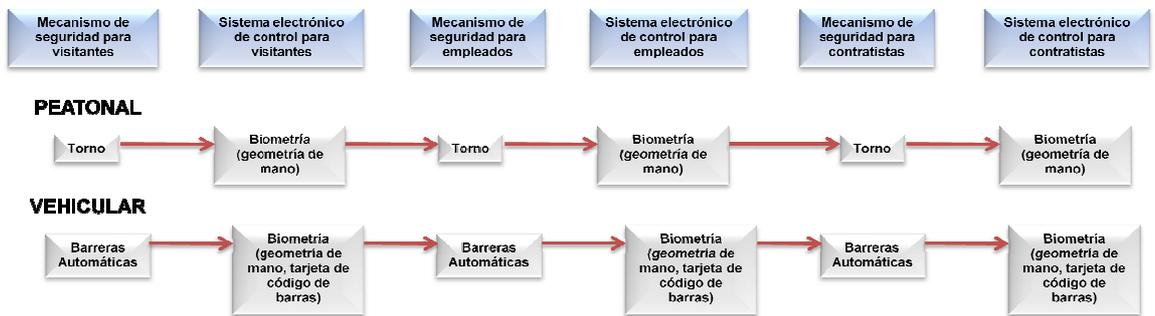


Figura 25. Concepto B

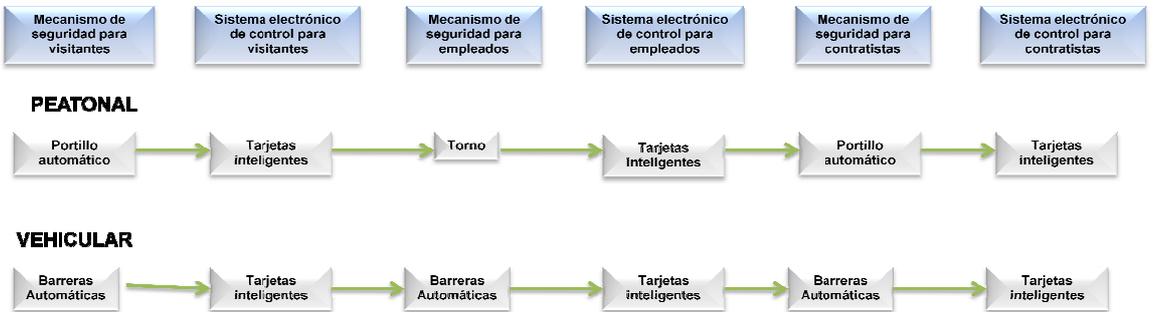


Figura 26. Concepto C

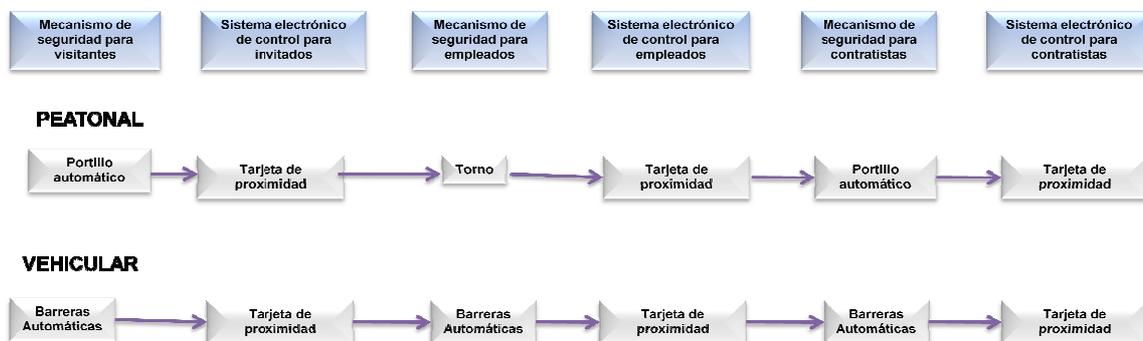
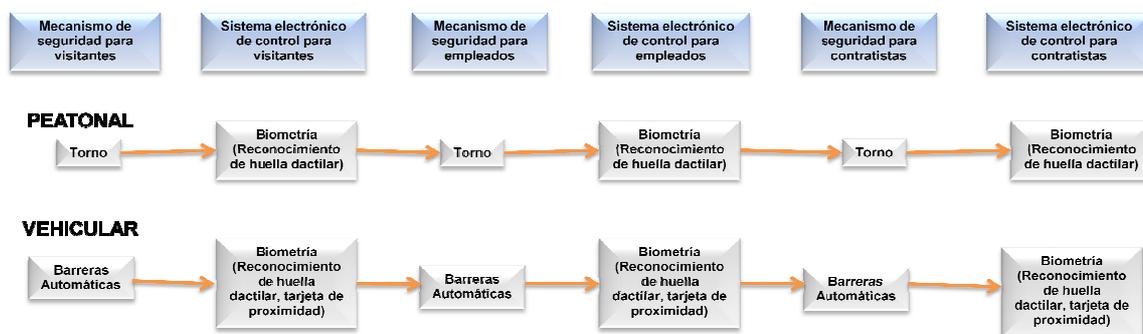


Figura 27. Concepto D



5.6. ESTUDIO DE COSTOS DE LOS CONCEPTOS

Los costos que se presentan a continuación; fueron obtenidos a través de páginas de internet de empresas conocidas y recomendadas por personas que trabajan en el medio de la seguridad electrónica, también fueron obtenidas de algunas empresas que han cotizado este proyecto a la Zona Franca del Pacífico.

El estudio de costos fue obtenido a finales de Diciembre de 2008 por lo tanto varía dependiendo del cambio de divisas, ya que muchas de las empresas cotizantes y las páginas de los fabricantes, presentan sus precios en dólares americanos.

Se presenta un promedio aproximado de los precios de los conceptos y sus respectivos elementos; no se tiene en cuenta los costos de manufactura, IVA ni costos de importación.

En la **Tabla 5** se muestra los costos de los componentes que pertenecen a los conceptos de forma independiente.

Tabla 5. Costos de los módulos.

Item	Marca	Equipo	Costo (COP)	Costo promedio Equipo (COP)
1	--	Lectora huella digital	--	4.014.666,67
1.1	Bosch	--	8.364.000,00	--
1.2	Softronic (marca no especificada)	--	2.200.000,00	--
1.3	F4 frax	--	1.480.000,00	--
2	--	Torno bidireccional	--	10.091.333,33
2.1	Spectra (3004D)	--	11.000.000,00	--
2.2	Softronic (marca no especificada)	--	9.000.000,00	--
2.3	Assenda (catrax master)	--	10.274.000,00	--
2.4	Colombian Security	Rediseño	660.000,00	
3	--	Barreras Automáticas	--	6.201.000,00
3.1	Jomaf 2350	--	1.500.000,00	--
3.2	Softronic (marca no especificada)	--	6.950.000,00	--
3.3	Colombian Security	--	4.574.000,00	--
3.4	Assenda (MIB 30*C100)	--	8.181.000,00	--

Tabla 5. Continuación

Item	Marca	Equipo	Costo (COP)	Costo promedio Equipo (COP)
3.5	Spectra (marca no especificada)	--	9.800.000,00	--
4	--	lectora tarjeta de proximidad	--	558.333,33
4.1	Kimaldi (Lector/grabador)	--	553.000,00	--
4.2	Assenda (ProxPro)	--	396.000,00	--
4.3	Bosch 18 cm.	--	726.000,00	--
5	--	Tarjetas de proximidad (lectores y tarjetas)	--	695.000,00
5.1	ProxPro Plus (50 unidades)	--	240.000,00	--
5.2	Bosch d8238 (50 unidades)	--	1.150.000,00	--
6	--	Lector código de barras	--	745.000,00
6.1	USB Metrologic 9520N	--	490.000,00	--
6.2	QS6000 PSC	--	1.000.000,00	--
7	--	Software	--	1.595.000,00
7.1	Assenda	--	2.000.000,00	--
7.2	Spectra	--	1.385.000,00	--

Tabla 5. Continuación

Item	Marca	Equipo	Costo (COP)	Costo promedio Equipo (COP)
7.3	Softronic	--	1.400.000,00	--
8	--	Lector de geometría de mano	--	4.173.333,33
8.1	Asistencia HandPunch 2000E/512	--	5.520.000,00	--
8.2	Assenda (HandKey)	--	4.200.000,00	--
8.3	Hand Punch 2000	--	2.800.000,00	--
9	--	Arco detector de metales	--	17.138.666,67
9.1	Cmm 05626	--	19.530.000,00	--
9.2	LAS 1252	--	14.758.000,00	--
9.3	Syscom (Intell 218z51)	--	17.128.000,00	--
10	--	Lector tarjetas inteligentes	--	58.666,67
10.1	Lector grabador Towtoko RS 232	--	40.000,00	--
10.2	Lector /grabador essential USB	--	72.000,00	--
10.3	Lector grabador DNI	--	64.000,00	--

En la **Tabla 6** se presentan los costos de los conceptos.

Tabla 6. Costos de conceptos.

Evaluación costo dispositivo vs concepto	Costo mecanismo (peatonal)	#	Costo dispositivo lector (peatonal)	#	Costo mecanismo (Vehicular)	#	Costo dispositivo lector (vehicular)	#	Costo Software	#	Costo detector magnético	#	Costo total proyecto
Concepto A	10.091.333	3	4.173.333	7	6.201.000	4	745.000	4	1.595.000	1	17.138.000	3	140.280.330
Concepto B	8.750.000	3	58.666	7	6.201.000	4	58.666	4	1.595.000	1	17.138.000	3	104.708.326
Concepto C	10.091.333	3	1.253.333	7	6.201.000	4	1.253.333	4	1.595.000	1	17.138.000	3	121.873.662
Evaluación costo dispositivo vs concepto	Costo mecanismo (peatonal)	#	Costo dispositivo lector (peatonal)	#	Costo mecanismo (Vehicular)	#	Costo dispositivo lector (vehicular)	#	Costo Software	#	Costo detector magnético	#	Costo total proyecto
Concepto D	10.091.333	3	4.000.000	7	6.201.000	4	695.000	4	1.595.000	1	17.138.000	3	138.866.999

NOTA: Los signos # se refieren a la cantidad de equipos que se requieren para el sistema.

5.7. MATRIZ DE TAMIZAJE.

En la matriz de tamizaje se evalúan los conceptos con algunos criterios de selección, que son normalmente las necesidades, de tal forma que se evalúa cual de los conceptos se adecua a las necesidades de la Zona Franca del Pacifico.

En la **tabla 7** se presenta la matriz de tamizaje, donde se tomo como referencia al concepto A, y se evalúa con todos los conceptos contra los criterios de selección; a la referencia se le da un valor neutro, en caso tal que algún concepto supere a la referencia se le da un valor positivo (+) en caso contrario se da un valor negativo (-). Al final se suman los puntos positivos y negativos y se le da un valor a cada concepto.

Tabla 7. Matriz de tamizaje.

CRITERIO DE SELECCION	B	C	D	A (REF)
<i>Permite agilidad de ingreso y salida de forma segura</i>	0	0	0	0
<i>Automatizar apertura y cierre de puertas</i>	0	0	0	0
<i>Gran capacidad de almacenamiento</i>	+	+	+	0
<i>Fácil manejo para los operarios</i>	+	+	+	0
<i>Gran capacidad de mantenimiento</i>	-	+	+	0
<i>Robusto</i>	0	0	+	0
<i>Fácil manejo para usuarios</i>	0	0	0	0
<i>Capacidad de modificarse para posibles mejoras</i>	0	0	0	0
<i>Garantiza evacuación inmediata en caso de posible emergencia</i>	0	0	0	0
<i>Que soporte intemperie</i>	0	0	0	0
<i>Funcionalidad</i>	0	0	+	0
<i>Costos</i>	+	+	0	0
<i>Que posea mas de una forma de comunicación</i>	0	0	0	0
<i>Representación comercial en cuanto a: personal capacitado, tiempo respuesta, suministro de repuestos</i>	+	+	+	0
POSITIVOS	4	5	6	
IGUALES	9	1	8	
		0		
CRITERIO DE SELECCION	B	C	D	
NEGATIVOS	2	0	0	
TOTAL	2	5	6	
ORDEN	3	2	1	
CONTINUAN	N	SI	SI	
	O			

Teniendo en cuenta los resultados obtenidos en la tabla anterior, se puede concluir que los conceptos **C** y **D** son los que cumplen con todos los requerimientos del cliente. Por lo tanto son los más probables para llegar a ser los proyectos a desarrollar.

La **Tabla 8** que se presenta a continuación explica que tiene cada concepto.

Tabla 8. Conceptos seleccionados.

ELEMENTO	CONCEPTO	
	C	D
PEATONAL	--	--
Mecanismo de seguridad para visitantes y contratistas	Portillo automático	Torno
Sistema Electrónico de Control para visitantes y contratistas	Tarjeta de proximidad	Biometría de huella dactilar
Mecanismo de seguridad para empleados	Torno	Torno
Sistema Electrónico de Control para empleados	Tarjeta de proximidad	Biometría de huella dactilar
VEHICULAR	--	--
Mecanismo de seguridad para visitantes y contratistas	Barreras automáticas	Barreras automáticas
Sistema Electrónico de Control para visitantes y contratistas	Tarjeta de proximidad	Biometría de huella dactilar/Tarjeta de proximidad
Mecanismo de seguridad para empleados	Barreras automáticas	Barreras automáticas
Sistema Electrónico de Control para empleados	Tarjeta de proximidad	Biometría de huella dactilar/Tarjeta de proximidad

El cliente solicita que se presenten las dos mejores propuestas de control de acceso, dichas propuestas son extraídas de los mejores puntajes en la matriz de tamizaje, por esta razón se presentó el concepto C y D en la anterior tabla.

El concepto C presenta características como la rapidez de respuesta (agilidad) y los bajos costos de los dispositivos lectores; el concepto D se caracteriza por la alta confiabilidad que este ofrece y tiene una orientación de control de acceso más enfocada hacia el individuo en relación a los empleados.

6. DISEÑO A NIVEL DE SISTEMA.

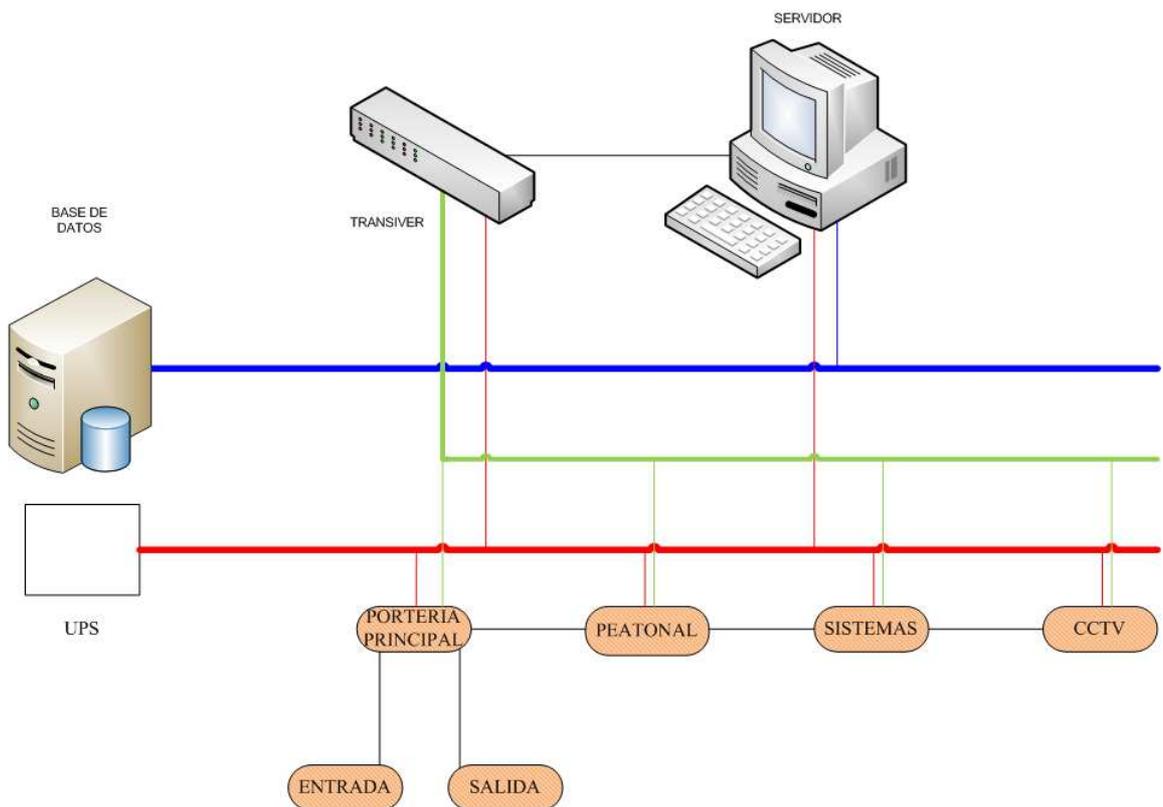
6.1. ANALISIS DE LA ARQUITECTURA DEL PRODUCTO

Se puede definir la arquitectura del producto como una arquitectura modular, ya que la relación entre los elementos funcionales y físicos es mínima, de hecho se puede decir que son independientes.

La modularidad es de tipo mixta, esto se debe a las especificaciones del cliente.

En la **Figura 28.** Se muestra la estructura cableada del sistema de control de acceso para la Zona Franca de Pacifico.

Figura 28. Estructura cableada.



7. DISEÑO INDUSTRIAL.

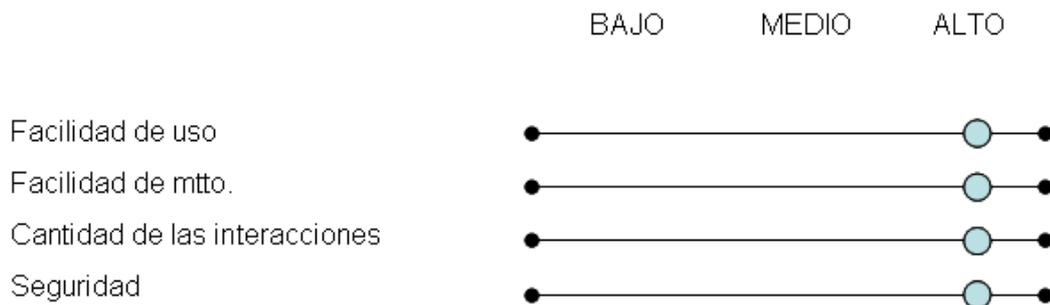
7.1. VALORACIÓN EN EL DISEÑO INDUSTRIAL

La valoración del diseño industrial del Sistema de Control de Acceso Automático para la Zona Franca del Pacífico nos ayudará a optimizar las respectivas funciones, valor y apariencia del mismo. Para esto nos basaremos en las necesidades ergonómicas y estéticas del sistema.

7.1.1. Necesidades ergonómicas.

En la **figura 29** podemos encontrar las necesidades del proyecto a nivel ergonómico; que son aquellas que tienen que ver con la interacción con el usuario.

Figura 29. Necesidades ergonómicas

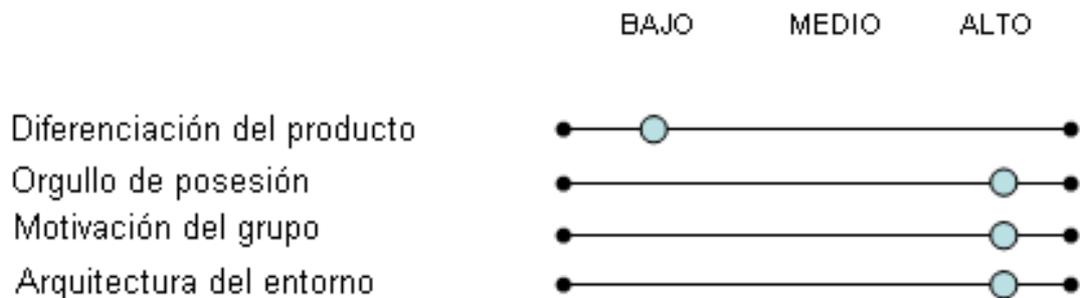


En las necesidades ergonómicas podemos observar que las valoraciones en facilidad de uso, facilidad de mantenimiento, cantidad de interacciones y seguridad tienen una valoración alta, debido a que el sistema de control de acceso estará sometido a prueba constantemente esto requiere una alta seguridad; la facilidad y la cantidad de interacciones que se necesitan para que el sistema funcione están ligadas y se consideran de alta importancia para aumentar la agilidad de ingreso y disminuir los tiempos y la facilidad de mantenimiento es representativo para los costos y tiempos de mantenimiento.

7.1.2. Necesidades estéticas

En la **figura 30** se indican las necesidades estéticas; que son aquellas que tienen que ver con la parte visual del producto.

Figura 30. Necesidades estéticas.

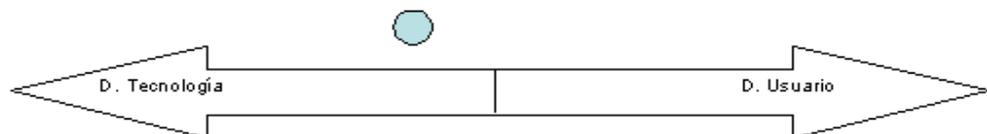


En las necesidades estéticas en la parte de la diferenciación del producto se obtuvo una baja calificación ya que no es indispensable para la Zona Franca del Pacífico que el sistema sea diferente a los sistemas de control de acceso actuales, en cuanto al orgullo de posesión, motivación del grupo y arquitectura del entorno obtuvieron una calificación alta, ya que se hace necesario que el producto se vea bien con las instalaciones del parque y no genere contaminación visual, esto conlleva a presentar un orgullo de posesión por ende la motivación del grupo en cuanto a la parte estética y la seguridad que ofrece va a ser alta.

7.2. NATURALEZA DEL PRODUCTO: TECNOLÓGICO O USUARIO

Es muy importante establecer el sistema será dominado por la tecnología o por el usuario, por tal motivo establecemos que el sistema de control de acceso es un sistema dominado más por la tecnología ya que está basado en acometer una tarea técnica, y su poco dominio de usuario es debido a que solo interviene en la interfaz en donde la persona tendrá una visualización e ingresará los datos al software del sistema de control de acceso; el resto se encarga el producto.

Figura 31. Naturaleza del producto



8. DISEÑO DE MANUFACTURA

Para el diseño de manufactura se tiene en cuenta que todos los componentes y piezas del sistema de Control de acceso son estándares, buscando que su mantenimiento sea más económico, fácil y reduzca su tiempo.

8.1. COSTOS DE MANUFACTURA.

Los costos de manufactura referentes a mano de obra, se adquirieron obteniendo un promedio de las empresas que cotizaron en Zona Franca del Pacifico como se muestra en la **Tabla 9**. En donde se tiene en cuenta la instalación de los diferentes equipos, configuraciones, capacitaciones y puesta en marcha del sistema en los datos no se incluye materiales de instalación.

Tabla 9. Costos de manufactura.

Empresa	Costo de Manufactura
Spectra	6.171.500
Softronics	6.420.000
ColombianSecurity	4.600.000
Assenda	10.000.000
Promedio	6.797.875

8.2. ESTRUCTURA CABLEADA.

En la **Tabla 10**. Se presenta la cantidad de cable (metros) necesario para la instalación del sistema del control de acceso.

Tabla 10. Estructura Cableada.

Punto de inicio	Punto final	distancia (metros)	Potencia 3 #12 (metros)	Datos cable UTP AT 5E/Fibra Optica (metros)
Recepción	Dispositivos Peatonal empleados	215	645	215
Recepción	Portería II	35	105	35
Recepción	Portería I	20	60	20
Servidor/UPS	Recepción	6	54	18
Servidor/UPS	Sistemas	40	--	40
Servidor/UPS	Monitoreo/Seguridad	50	--	50
Servidor/UPS	Sub-Estación	90	27	--
TOTAL			891	378

Como se puede apreciar en la anterior tabla se muestran los puntos en los cuales irán los terminales.

9. ESPECIFICACIONES TECNICAS

9.1. REQUERIMIENTOS TECNICOS.

En la **Tabla 11** se presenta los requerimientos técnicos mínimos que deben cumplir los diferentes elementos del sistema para garantizar el buen funcionamiento del sistema.

Tabla 11. Requerimientos técnicos.

ITEM	DESCRIPCIÓN	REQUERIMIENTO
1	Lectora de huella dactilar	
1.1	Tiempo de identificación	1-2 Segundos.
1.2	Comunicación	RS 232/485, Ethernet
1.3	% Falsa aceptación	0,50%
1.4	% Falso rechazo	1%
1.5	Tipo de identificación	Capacitiva o laser
1.6	Capacidad de almacenamiento	9000 usuarios
1.7	Voltaje lógico	5-12 VDC
1.8	Puerto de almacenamiento	USB 2.0
1.9	Temperatura	-30 a 50 °C.
2	lectora de tarjetas de Proximidad	
2.1	Tiempo de Identificación	1 Segundos
2.2	Comunicación	Rs 232/485, Wiegand Ethernet
2.3	% Falsa aceptación	1%
2.4	% Falso rechazo	1%
2.5	Distancia aprox. de lectura	10 cm
2.6	Capacidad de almacenamiento	1500 usuarios

Tabla 11. Continuación

ITEM	DESCRIPCIÓN	REQUERIMIENTO
2.7	Voltaje lógico	5-12 VDC
2.8	Puerto de almacenamiento	USB 2.0
2.9	Temperatura	-30 a 50 °C.
3	Torno o torniquete	
3.1	Tiempo de acción	1-2 Segundos.
3.2	Material	Acero inoxidable o semejante su color debe contrastar con la fachada del parque
3.3	Dirección de paso	Bidireccional
3.4	Suministro energía	110 VAC 60 Hz
3.5	Voltaje lógico	12-24 VDC
3.6	Transito	Alto
3.7	Comunicación	Rs 232/485
3.8	Sistema anti pánico	Si
3.9	Temperatura	-30 a 50 °C.
4	Talanquera	
4.1	Tiempo de reacción	Menor a 8 Segundos.
4.2	Material de lanza	Resistente y liviano
4.3	Suministro de energía	110 VAC 60 Hz
4.4	Pintura	Intemperie amarillo trafico
4.5	Longitud lanza	3.2 mts aprox. Empleados ; 2.2 mts aprox. Visitantes aprox.
4.6	Sistema anti pánico	Si
4.7	Temperatura	-30 a 50 °C.
5	Software de control de acceso	

Tabla 11. Continuación

ITEM	DESCRIPCIÓN	REQUERIMIENTO
5.2	Comunicación	Rs 232/485, Wiegand
5.3	Numero de unidades lectoras	11 unidades
5.4	Gestión transito peatonal	Si
5.5	Gestión transito vehicular	Si
5.6	Gestión anti-pass back	Por área total
5.7	Software para exportar datos	Formato tipo Excel, Block de notas.
5.8	Almacenamiento de imágenes	Fotos del personal que ingresa.
5.9	Control de tiempo	Personal que visita tanto como el que labora.
5.10	Control de empleados y contratistas	Control de ARP y EPS para empleados y contratistas
5.11	Interfaz grafica	Interfaz amigable con el operario
5.12	Idioma	Español
5.13	Escalabilidad	Permitir actualizar el software con el transcurrir del tiempo
5.14	Lenguaje de programación	compatible con base de datos Oracle
5.15	Compatibilidad	Software de control de acceso actual de el parque industrial
5.16	Operación	Fácil y puntual para operarios
6	Arco detector magnético	
6.1	Suministro de energía	110 VAC

Tabla 11. Continuación

ITEM	DESCRIPCIÓN	REQUERIMIENTO
6.2	Material	Resistente a intemperie con protección a interferencias eléctricas
6.3	Sensibilidad	Alta
6.4	Tiempo de respuesta	<= 0,5 Segundos.

9.2. CONSUMO DE POTENCIA.

En la **Tabla 12** se presenta el consumo del consumo eléctrico representado en Watts; de cada uno de los equipos del control de acceso.

Tabla 12. Consumo de potencia.

Equipo	Cantidad	Watts C/U (aprox)	Watts total (aprox)
Dispositivo lector (Peatonal)	7	4	28
Torno	3	2	6
Dispositivo lector (vehicular)	4	1	4
Computador	1	260	260
Talanquera	4	250	1000
Arco detector magnético	3	35	105
TOTAL	--	--	1403

Los lectores biométricos de huella digital se distribuyen de la siguiente manera:

- 1 Entrada peatonal.
- 2 Entrada vehicular.
- 2 Salida vehicular.
- 2 Entrada peatonal empleados.

Los lectores de huella digital son necesarios para el ingreso/salida del personal peatonal así como el que se moviliza en vehículos dentro del parque, ya que es preciso registrar a todo el personal que ingresa en el parque industrial y es necesario que se tenga un sistema de identificación estándar para todos.

- Los tornos se distribuyen:
- 1 Entrada vehicular.
- 2 Entrada peatonal visitantes.

Los tornos son bidireccionales, de esta manera se ocupa menos espacio y no se hace necesario comprar otro torno para la otra dirección.

- Los lectores de tarjetas son ubicados en el ingreso y salida de los vehículos. Los lectores de tarjetas se emplean para controlar el ingreso de los vehículos; a cada vehículo se le entrega una tarjeta con la cual se identifica y verifica que el vehículo esta en el parque industrial. Y se puede conocer quien es la persona que ingresa en el vehículo y quien es que sale.
- El computador sirve para funcionar como periférico entre el usuario y el software, también tiene como función de puerto de almacenamiento y verificación de datos.
- Las talanqueras se ubican en la entrada y salida vehicular tanto de empleados como de contratistas y visitantes.
- El transductor es el que se encarga de cambiar as señales recibidas de la fibra óptica en señales legibles para el computador.

9.2.1. Calculo de UPS.

Para determinar el consumo real de los dispositivos ya que estos no se encuentran en constante uso, se multiplica el total de Watts presentados anteriormente por 0.8, los datos que arroja este calculo es con el que se trabaja para determinar la capacidad de UPS.

$$1403 * 0.8 = 1122.4 \text{ Watts.}$$

Para determinar el tipo de UPS que se debe usar para el control de acceso; se toma el dato arrojado anteriormente y se divide en 900 de esta forma determinamos los KVA.

$$1122.4 / 900 = 1.25 \text{ KVA.}$$

Por factor de seguridad se considera que la capacidad de la UPS debe ser de 2 KVA con autonomía de 30 minutos.

10. CONCLUSIONES

Conocer y estudiar de forma minuciosa las necesidades del cliente es la base fundamental en todo diseño, en este caso, la Zona Franca del Pacífico tiene unas necesidades que son sobresalientes y muy importantes, pero otras que no son tan relevantes, son de igual importancia. Es así como sucede en el caso del software, su compatibilidad, la modularidad del sistema y la robustez entre otros.

La matriz de la calidad (QFD) juegan un papel muy importante, ya que en ella se estudian las necesidades, se hace el Benchmarking que es una evaluación con otras empresas que trabajan con el mismo producto y analizar las ventajas y desventajas de este y se puede estudiar si la relación entre los requerimientos es significativa o no lo cual es de gran importancia en el momento de darle un peso a la selección de las métricas.

Conocer el estado actual en cuanto a la parte de seguridad del parque industrial es importante para saber cuáles son los puntos que se deben reforzar y cuáles deben mantenerse.

Estudiar todos los elementos que forman parte de un sistema de control de acceso en el sector industrial a nivel mundial permite, proponer nuevas ideas viables para la realización del proyecto.

La matriz de tamizaje brinda datos importantes en el momento de escoger un proyecto, permite escoger dicho proyecto, por sus fortalezas, y no por preferencias.

Tener una idea global, basada en promedios de los costos del proyecto de forma individual y general permite aterrizarlo y establece una línea comparativa para las propuestas que se realicen.

11. RECOMENDACIONES

- En el momento del desarrollo del sistema de control de acceso es necesario que el montaje se haga de forma modular, ya que por la complejidad del proyecto se afecta el funcionamiento normal de la Zona Franca del Pacífico.
- Se recomienda conservar las puertas existentes que se encuentran ubicadas en la entrada/salida de la Zona Franca del Pacífico; a pesar que se instalen los mecanismos de seguridad es importante que dichas puertas permanezcan en el parque industrial, ya que sirven como soporte en caso de averías, mantenimiento, etc. También se pueden emplear en horas nocturnas en las cuales el flujo del personal es mínimo, y la inseguridad aumenta notoriamente.
- La redundancia en la seguridad juega un papel importante en momentos críticos; por tal razón se recomienda instalar una cámara rotacional o domo de tres grados de libertad en el sector del acceso de empleados, teniendo en cuenta que la Zona Franca del Pacífico tiene instalados este tipo de cámaras en otros sectores del parque, sobra resaltar el excelente papel que cumple a diario en el parque industrial este tipo de tecnologías. Se hace necesario colocar una de estas cámaras en este punto específico por el flujo de personal que se presenta a diario en horas pico.
- Para el acceso del parque industrial es significativo identificar y diferenciar plenamente el personal de empleados con el personal de visitantes y contratistas, por seguridad y la disminución del congestionamiento y embotellamiento en las horas pico.
- Se recomienda cambiar el medio de comunicación de línea telefónica a fibra óptica, ya que el parque industrial, se presenta en una zona abierta y se corre el riesgo de posibles daños por descargas eléctricas las cuales pueden generar daños en la comunicación de los dispositivos involucrados en este proyecto.

BIBLIOGRAFIA

Acces Control & Security Management Solutions [en línea]. Santa Ana, CA: Hirsch Electronics Corp, 2009 [Consultado 19 de Julio de 2008]. Disponible en Internet: www.hirschelectronics.com/

AMWATCH Sistemas de Control de Acceso [en línea]. Florida: Amtel Security System Inc, 2005 [Consultado 03 de Septiembre de 2008]. Disponible en Internet: <http://www.amtel-security.com/Spanish/products/ACS.html>

CASTRO OSPINA, Diego Fernando. Ingeniería concurrente, una estrategia de operaciones orientada al mejoramiento continuo en el diseño de productos [CD-ROM]. Santiago de Cali, 1999. 1 CD-ROM. Trabajo de grado (Ingeniero de Producción). Universidad Autónoma de Occidente. División de Ingenierías.

Control de acceso basado en reconocimiento de iris [en línea]. Cartagena: Universidad Tecnológica de Bolívar, 2006 [Consultado 25 de Junio de 2008]. Disponible en Internet: <http://biblioteca.unitecnologica.edu.co/notas/2004-03-08/0024820.pdf>

Control de accesos [en línea]. Argentina: Guia de la seguridad, 2008 [Consultado 20 de Agosto de 2008]. Disponible en Internet: <http://www.guiadelaseguridad.com.ar/control-de-accesos.htm>

Geocities [en línea]. USA: Yahoo Inc, 2009. [Consultado 18 de Octubre de 2008]. Disponible en Internet: <http://www.geocities.com/jhdezsan/norma.htm>
http://www.amtel-security.com/Spanish/products/proximity_card_readers.html

Lectoras Biométricas [en línea]. Florida: Amtel Security System Inc, 2005 [Consultado 20 de Octubre de 2008]. Disponible en Internet: http://www.amtel-security.com/Spanish/products/acs_biometric_devices.html

Lectoras de código de barras de largo alcance [en línea]. Florida :Amtel Security System Inc, 2005 [Consultado 20 de Octubre de 2008]. Disponible en Internet: http://www.amtel-security.com/Spanish/products/amlazer_barcode.html

Lectoras de tarjetas de proximidad y tarjetas AMTEL [en línea]. Florida :Amtel Security System Inc, 2005 [Consultado 22 de Octubre de 2008]. Disponible en Internet: http://www.amtel-security.com/Spanish/products/rfid_tags.html
Lectoras y Tarjetas RF [en línea]. Florida :Amtel Security System Inc, 2005 [Consultado 22 de Octubre de 2008]. Disponible en Internet: http://www.amtel-security.com/Spanish/products/rfid_tags.html

Norma NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de Información [en línea]. Bogotá: CRA Comisión de regulación de agua potable y saneamiento básico, 2009 [Consultado 17 de Noviembre de 2008]. Disponible en Internet: http://www.cra.gov.co/portal/www/resources/lzy_iso27001.pdf

Proximidad inteligente [en línea]. Florida: Amtel Security System Inc, 2005 [Consultado 22 de Octubre de 2008]. Disponible en Internet: http://www.amtel-security.com/Spanish/products/acs_smart_proximity.html