INDICE

DESCRIPCION DE FIGURAS

DESCRIPCION DE TABLAS

1. PLANTEAMIENTO DEL PROBLEMA

La pequeña industria colombiana no cuentan con sistemas de control de acceso a sus centros de computo para proteger sus activos más preciados: La información, las diferentes plataformas que contienen estos datos y los esquemas de comunicación con los cuales es transmitida a los diferentes puntos de una organización.

En el mercado colombiano existente diferentes medios y tecnologías para controlar el acceso a un centro de computo como la seguridad física realizada por una persona ó herramientas de autenticación y validación como la biometría, tarjetas magnéticas, teclados matriciales, etc. Algunos con mejores argumentos tecnológicos como los sistemas de control de la retina humana ó la confirmación de la huella dactilar pero que no son de fácil adquisición por cualquier empresa debido a su gran costo económico.

Existente otras tecnologías de control de acceso como la utilización de teclados matriciales, tarjetas de banda magnética ó códigos de barras que por su obsoleto nivel tecnológico han motivado a los impostores ha superar estos sistemas de seguridad con una mayor facilidad, lo que obliga a los usuarios a instalar nuevos sistemas cada vez más potentes y fiables.

Está es la razón por la cual se ha planteado el desarrollar y crear un prototipo que solucione el problema de control de acceso a centros de computo, con herramientas y tecnología de última generación y lo más interesante de todo su reducido valor económico ante los demás sistemas de control de acceso de última generación.

1.1 DESCRIPCION

Se desarrollara una solución global de seguridad, el sistema estará compuesto básicamente de tres fases: El modulo de acceso encargado de manejar autónomamente el ingreso de usuarios a las de pendencias, el servidor de gestión cuya función es centralizar los procesos administrativos del sistema y el tercer modulo una interfase electrónica cuya labor será la de realizar la apertura de las puertas de acceso ó informar al usuario el porque no es posible su ingreso.

El modulo de acceso está conformado por una tarjeta inteligente de contacto que ha sido desarrollado como un sistema de almacenamiento de información, que contiene un modulo de memoria EPROM que facilita las labores de lectura y grabación de datos sobre el ship de la tarjeta. Una unidad lectora que permite obtener la identificación del usuario grabada en el chip de la tarjeta, la cual es transferida al servidor de gestión directamente.

El servidor de gestión será el responsable de llevar a cabo todas las labores de control del sistema y el responsable por validar y guardar todos los accesos solicitados al sistema por los diferentes usuarios. El servidor de gestión estará compuesto por una base de datos que contendrá toda la información pertinente a usuarios, permisos, puertas y otras tablas de utilidad para el buen desenvolvimiento del sistema.

Una interfase electrónica que permitirá la apertura de las puertas después ó el envió de un mensaje al usuario que intenta obtener el ingreso. La transmisión de los datos se realiza utilizando el protocolo eléctrico 232.

1.2 ANALISIS DE VARIABLES

Las variables globales que afectan SCAEC son:

- Costos
- Espacio
- Medios Electrónicos
- Software
- Talento humano

Se hará un análisis de cada una de las variables.

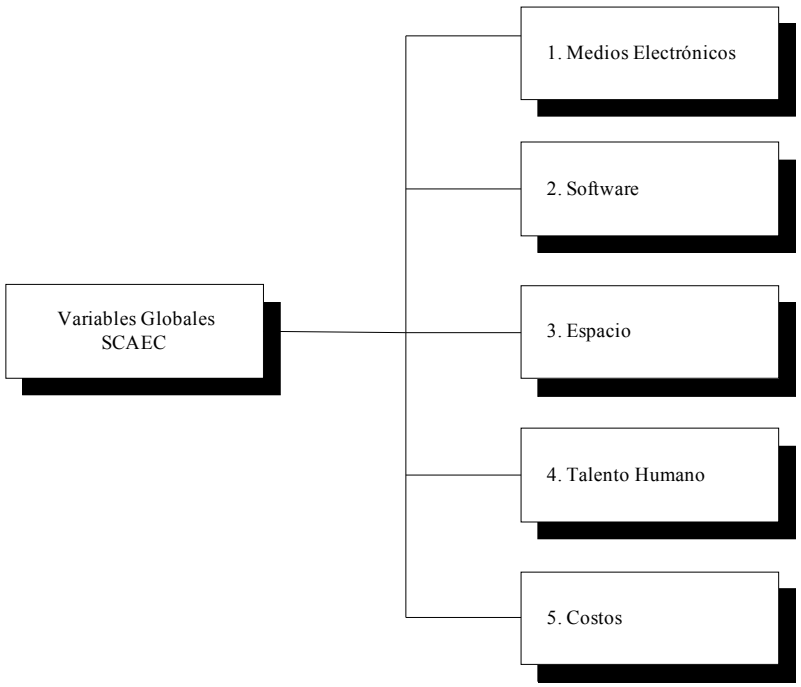


Figura 1 Variables Globales SCAEC

1.2.1 Medios Electrónicos

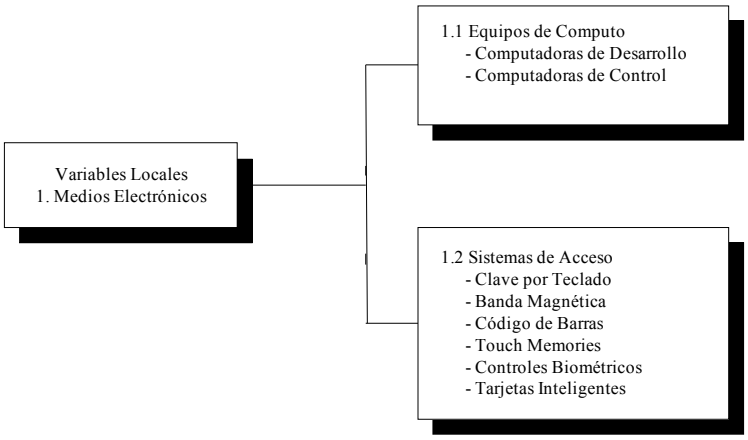


Figura 2 V.L. Medios Electrónicos

1.1.2.1 Equipos de Cómputo

- Computadores de desarrollo
- Computadores de control

1.2.1.2 Sistemas de Control de Acceso

- Claves por teclado:
- Banda magnética:
- Código de barras:
- Touch Memories:
- Sistemas Biométricos:
- Tarjetas inteligentes:

1.2.2 Software

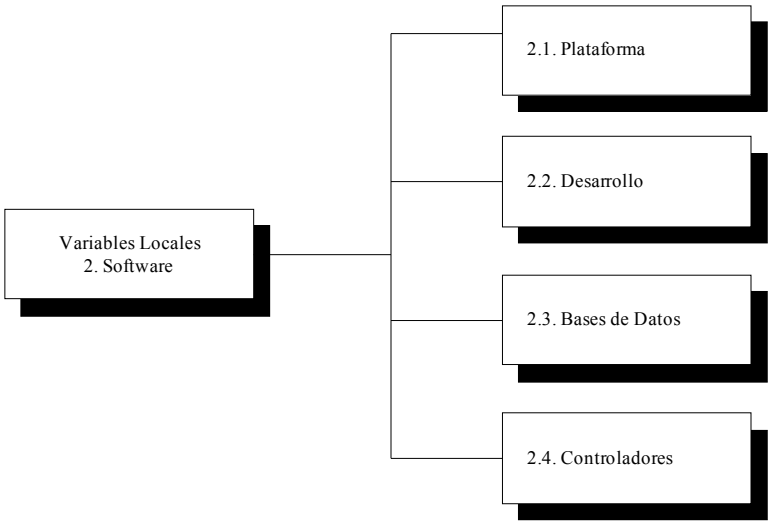


Figura 3 V.L. Software

1.2.2.1. Plataforma

Plataforma	Ventajas	Desventajas
Linux	- Es de libre distribución y bajo costo de adquisición.	- No hay suficiente software de aplicación.
Windows	- Gran cantidad de aplicativos, seguros y fiables.	- Licencias demasiados costosas.

Tabla 1 V.L. Plataforma

1.2.2.2. Herramientas de Desarrollo

Herramienta	Ventajas	Desventajas
C++	- Gran estabilidad - Funciona en Windows y Linux.	- Gran cantidad de líneas de código. Lo que hace sea confuso.
Visual Basic	- Fácil desarrollo - Manejo gráfico del entorno	- No funciona en las dos plataformas. - Demasiado costos el licenciamiento.

Tabla 2 V.L. Herramientas de Desarrollo

1.2.2.3. Motores de Base de datos

Motor B.D.	Ventajas	Desventajas
Access de Microsoft	- No presenta errores de código. - Fácil manejo gráfico	- No sirve para bases de datos de miles de registros.
MySql	- No presenta errores de código. - Estable y fiable	- No es gráfico. - No funciona en ambiente Windows.

Tabla 3 V.L. Motores de Base de Datos

1.2.2.4. Control

Software controlador	Ventajas	Desventajas
Asembler	- Funciona bien a bajo nivel y en chips.	- Instrucciones complicadas

Tabla 4 V.L. Control

1.2.3 Espacio

Figura 4 V.L. Espacio

El lugar donde se llevará a cabo la construcción y desarrollo del prototipo será la ciudad de Bogotá.

1.2.4 Personal

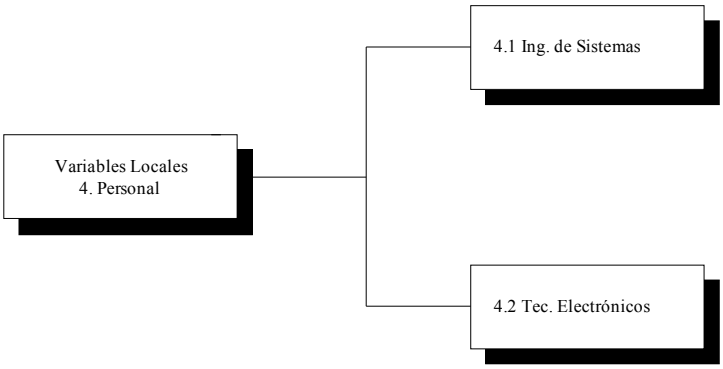


Figura 5 V.L. Personal

1.2.4.1 Ingenieros de Sistemas

Personal con gran capacidad de creación e innovación. Especialistas en el diseño de sistemas de gestión y excelentes programadores.

1.2.4.2 Tecnólogos Electrónicos

Excelentes técnicos con habilidad para el diseño e implementación de circuitos electrónicos.

1.2.5 Costos

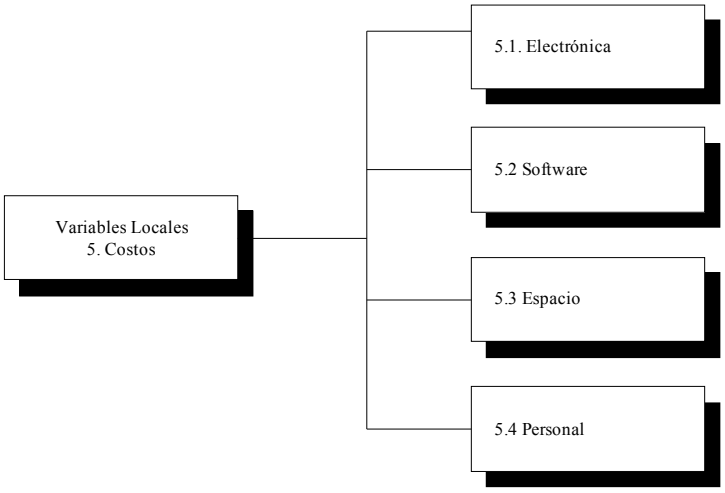


Figura 6 V.L. Costos

1.2.5.1 Costos de componentes electrónicos

Medios Electrónicos	Unidad / Mt	Valor unidad	Valor
Tarjetas inteligentes	3	$ 8.000,00	$ 24.000,00
Unidad Lectora	1	$ 980.000,00	$ 980.000,00
Circuito electrónico de control	1	$ 270.000,00	$ 270.000,00
Cable UTP para redes	12	$ 23.000,00	$ 276.000,00
Quemadora tarjetas	1	$ 145.000,00	$ 145.000,00
Dial Matricial	1	$ 50.000,00	$ 50.000,00
Lector de códigos de barras	1	$ 25.000,00	$ 25.000,00
Tarjetas Inteligentes de memoria	1	$ 5.000,00	$ 5.000,00
Tarjetas Inteligentes de microchip	1	$ 30.000,00	$ 30.000,00
Equipo de computo	1	$ 2.150.000,00	$ 2.150.000,00
Foto lector de huellas	1	$ 600.000,00	$ 600.000,00

Tabla 5 V.L. Costos de Componente electrónicos

1.2.5.2 Costos de adquisición de software

Software	Descripción		Valor
Linux	Red Had 8.0	$	300.000
Windows	Windows 2000 Server	US	640
	Windows 2000 Profesional	US	500
C++		US	250
Visual Basic	Versión 6.0	US	300
Microsoft Access	Version 6.0	US	150
MySql		US	70

Tabla 6 V.L. Costos de Adquisición de Software

1.2.5.3 Costos de Espacio

- Alquiler de oficina

Alrededor de $ 150.000 pesos con los servicios y administración.

1.2.5.4 Costos de Personal

Personal	Valor hora
Ingeniero de Sistemas	$ 25.000,00
Tecnólogo Electrónico	$ 18.000,00
Asesoría Ing. Electrónicos	$ 150.000,00

Tabla 7 V.L. Costos de Personal

1.3 FORMULACION

¿Es posible controlar el acceso de personas a los centros de computo utilizando SCAES?

1.4. DELIMITACION

- El prototipo está diseñado y habilitado solamente para controlar el ingreso de personas a un centro de computo.
- El prototipo requiere para su normal funcionamiento se encuentre habilitado a un sistema de corriente regulada con respaldo de contingencia UPS.
- El prototipo está diseñado para trabajar con el protocolo eléctrico 232 y 434.
- La tarjeta inteligente utilizada para el sistema de gestión SCAEC es de tipo memoria y tendrá la información básica del usuario como es un código de acceso y su respectivo nombre.
- El número de esclavos para el desarrollo de prototipo será de uno.
- El número de esclavos programados dentro del PIC 16F873 A y la unidad del DIR switch es de cuatro.
- El sistema está desarrollado para trabajar solamente en la plataforma Windows.
- La especificaciones mínimas para la instalación de Scaes son:
  Windows 2000 profesional, 64 megas de memoria, 233 MHZ de velocidad de CPU y Monitor súper VGA.

2. OBJETIVOS

2.1. GENERAL

Diseñar e implementar un prototipo de un sistema completo de control de acceso de personas a un centro de computo a través de un mecanismo electrónico de última generación.

2.2. ESPECIFICOS

- Recolectar, tabular y seleccionar información de las nuevas tecnologías de control de acceso de acceso para centros de computo existentes en el mercado.
- Analizar y Diseñar los diferentes elementos que conforman el modelo conceptual para el prototipo del control de acceso SCAEC.
- Implementar e integrar los elementos básicos para el funcionamiento del prototipo SCAEC
- Valorar y modificar la integración funcional de los diferentes módulos que integran el correcto funcionamiento del prototipo SCAES.

3. JUSTIFICACIÓN

La necesidad de asegurar la identificación de los usuarios en los accesos de centros de computo. La importancia y valor de estos datos manejados, motiva a los impostores a superar los sistemas de seguridad existentes, lo que obliga a los usuarios a instalar nuevos sistemas cada vez más potentes y fiables.

Estas necesidades de autenticación y seguridad, unidas a las ya existentes anteriormente en materia de seguridad de accesos físicos, han determinado un interés creciente por los sistemas electrónicos de identificación y autenticación. Su denominador común es la necesidad de que sean medios simples, prácticos y fiables, para verificar la identidad de una persona.

En la actualidad se ha investigado y desarrollado sistemas de control de acceso de personas, utilizando tecnologías de última generación pero de un alto costo monetario y su aplicabilidad ha sido para empresas de un gran poder económico.

Se han realizado estudios de mercado para observar las necesidades en el comercio de estás herramientas de control de acceso y las últimas tendencias tecnológicas hemos hallado una oportunidad de negocio para desarrollar e implementar un sistema de control de accesos a centros de computo utilizando herramientas y tecnología de última generación teniendo como centro de gravedad su bajo valor económico el cual permitirá su fácil adquisición por parte de la mediana y pequeña industria colombiana.

4. MARCO TEORICO

Ya sabemos que unos requerimientos primordiales de los sistemas informáticos que desempeñan tareas importantes son los mecanismos de seguridad adecuados a la información que se intenta proteger; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos activos del sistema, generalmente usuarios) que intentan acceder a los objetos (elementos pasivos, como ficheros o capacidad de cómputo), mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones retínales.

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, sino autenticar que esa persona es quien dice ser realmente. Aunque como humanos seguramente ambos términos nos parecerán equivalentes, para un ordenador existe una gran diferencia entre ellos: imaginemos un potencial sistema de identificación estrictamente hablando, por ejemplo uno biométrico basado en el reconocimiento de la retina; una persona miraría a través del dispositivo lector, y el sistema sería capaz de decidir si es un usuario válido, y en ese caso decir de quién se trata; esto es identificación. Sin embargo, lo que habitualmente hace el usuario es introducir su identidad (un número, un nombre de usuario...) además de mostrar sus retinas ante el lector; el sistema en este caso no tiene que identificar a esa persona, sino autenticarlo: comprobar los parámetros de la retina que está leyendo con los guardados en una base de datos para el usuario que la persona dice ser: estamos reduciendo el problema de una población potencialmente muy elevada a un grupo de usuarios más reducido, el grupo de usuarios del sistema que necesita autenticarlos.

Los métodos de autenticación se suelen dividir en tres grandes categorías, en función de lo que utilizan para la verificación de identidad: (a) algo que el usuario sabe, (b) algo que éste posee, y (c) una característica física del usuario o un acto involuntario del mismo. Esta última categoría se conoce con el nombre de autenticación biométrica. Es fácil ver ejemplos de cada uno de estos tipos de autenticación: un password (Unix) o passphrase (PGP) es algo que el usuario conoce y el resto de personas no, una tarjeta de identidad es algo que el usuario lleva consigo, la huella dactilar es una característica física del usuario, y un acto involuntario podría considerarse que se produce al firmar (al rubricar la firma no se piensa en el diseño de cada trazo individualmente).

Por supuesto, un sistema de autenticación puede (y debe, para incrementar su fiabilidad) combinar mecanismos de diferente tipo, como en el caso de una tarjeta de crédito junto al PIN a la hora de utilizar un cajero automático o en el de un dispositivo generador de claves para el uso de One Time Passwords.

Cualquier sistema de identificación (aunque les llamemos así, recordemos que realmente son sistemas de autenticación) ha de poseer unas determinadas características para ser viable; obviamente, ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros), económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto) y ha de soportar con éxito cierto tipo de ataques (por ejemplo, imaginemos que cualquier usuario puede descifrar el password utilizado en el sistema de autenticación de Unix en tiempo polinomial; esto sería inaceptable). Aparte de estas características tenemos otra, no técnica sino humana, pero quizás la más importante: un sistema de autenticación ha de ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen. Por ejemplo, imaginemos un potencial sistema de identificación para acceder a los recursos de la Universidad, consistente en un dispositivo que fuera capaz de realizar un análisis de sangre a un usuario y así comprobar que es quien dice ser; seguramente sería barato y altamente fiable, pero nadie aceptaría dar un poco de sangre cada vez que desee consultar su correo.

4.1.ANTECEDENTES

Anexo se muestran los principales métodos de autenticación:

4.1.1 Sistemas basados en algo conocido: Contraseñas

El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser simplemente basándonos en una prueba de conocimiento que a priori sólo ese usuario puede superar; y desde Alí Babá y su "Ábrete, Sésamo" hasta los más modernos sistemas Unix, esa prueba de conocimiento no es más que una contraseña que en principio es secreta. Evidentemente, esta aproximación es la más vulnerable a todo tipo de ataques, pero también la más barata, por lo que se convierte en la técnica más utilizada en entornos que no precisan de una alta seguridad, como es el caso de los sistemas Unix en redes normales (y en general en todos los sistemas operativos en redes de seguridad media-baja); otros entornos en los que se suele aplicar este modelo de autenticación son las aplicaciones que requieren de alguna identificación de usuarios, como el software de cifrado PGP o el escáner de seguridad NESSUS. También se utiliza como complemento a otros mecanismos de autenticación, por ejemplo en el caso del Número de Identificación Personal (PIN) a la hora de utilizar cajeros automáticos.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, clave que han de mantener en secreto si desean que la autenticación sea fiable. Cuando una de las partes desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común, y si ésta es correcta se otorga el acceso a un recurso. Lo habitual es que existan unos roles preestablecidos, con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior (en el modelo del acceso a sistemas Unix, tenemos al usuario y al sistema que le permite o niega la entrada).
Como hemos dicho, este esquema es muy frágil: basta con que una de las partes no mantenga la contraseña en secreto para que toda la seguridad del modelo se pierda; por ejemplo, si el usuario de una máquina Unix comparte su clave con un tercero, o si ese tercero consigue leerla y rompe su cifrado (por ejemplo, como veremos luego, mediante un ataque de

diccionario), automáticamente esa persona puede autenticarse ante el sistema con éxito con la identidad de un usuario que no le corresponde.

4.1.2 Sistemas basados en algo poseído:

Mencionaremos los principales sistemas de control de acceso con una muy breve descripción de cada uno de este esquema de control de acceso:

4.1.2.1 Claves por Teclado:

Obviamente esta opción es la más económica, pero la menos segura. Hace tiempo que han caído en desuso y no se han generado hasta el momento nuevas aplicaciones donde puedan resurgir como una opción válida.

4.1.2.2 Banda Magnética:

Es la más conocida y difundida. Su ventaja es su popularidad y el bajo costo, pero en sí es, de todos los medios de identificación, uno de los más vulnerables de todos. Sólo se recomiendan en oficinas o establecimientos administrativos. Su principal problema es el desgaste al que se ven sometidos tanto el lector, como las tarjetas y la posible desmagnetización de la banda, obligando a cambiar o re grabar la tarjeta con todos los problemas que trae aparejado.

4.1.2.3 Wiegand:

Fue uno de los primeros sistemas de lectura que se utilizó. Hoy en día, sólo se usa en ampliaciones de instalaciones viejas, pero no se ofrece en sistemas nuevos.

4.1.2.4 Código de Barras:

La principal ventaja de esta tarjeta, es que permite una construcción rápida y económica por el mismo usuario, no existe rozamiento con un cabezal, pero a pesar de que se las puede proteger contra fotocopias, son las más vulnerables en lo que a seguridad se refiere.

4.1.2.5 Touch Memories:

Es una pastilla electrónica, encapsulada en acero inoxidable que generalmente se transportan con un soporte plástico tipo llavero. Brindan un muy alto nivel de seguridad ya que no se pueden duplicar y son altamente resistentes al desgaste, siendo ideales para ambientes industriales, aunque no son recomendables para ambientes con alto grado de generación de corriente estática (P. Ej.: oficinas con mucha alfombra y ambientes muy secos).

4.1.2.6 Tarjeta Inteligentes:

Son tarjetas de plástico similares en tamaño y otros estándares físicos a las tarjetas de crédito que llevan estampadas un circuito integrado: Este es un circuito que puede ser de una sola memoria o contiene un microprocesador con un sistema operativo que le permite una serie de tareas como: Almacenar, encriptar información, leer y escribir datos, como un ordenador. Es una tarjeta que por su diseño tecnológico, no puede duplicarse. Cada una posee un código distinto y no permite que varios usuarios puedan tener una tarjeta duplicada

4.1.3 Sistemas de autenticación biométrica

A pesar de la importancia de la criptología en cualquiera de los sistemas de identificación de usuarios vistos, existe otra clase de sistemas en los que no se aplica esta ciencia, o al menos su aplicación es secundaria. Es más, parece que en un futuro no muy lejanos estos serán los sistemas que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario: son más amigables para el usuario (no va a necesitar recordar passwords o números de identificación complejos, y, como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o su ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética; las principales razones por la que no se han impuesto ya en nuestros días es su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento.

Estos sistemas son los denominados biométricos, basados en características físicas del usuario a identificar. El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptología se limita aquí a un uso secundario, como el cifrado de una base de datos de patrones retínales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos. La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Obviamente aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes o sistemas Unix el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado recurso.

4.1.3.1 Verificación de voz

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

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique. Como veremos a continuación, estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va `proponiendo' a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales...) Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

4.1.3.2 Verificación de escritura

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

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

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

4.1.3.3 Verificación de huellas

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

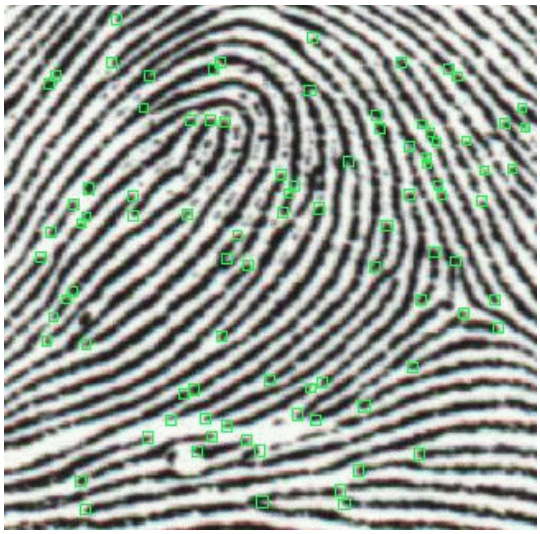


Figura 7 Control de Accesos Verificación de huellas

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

4.1.3.4 Verificación de patrones oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: o bien analizan patrones retínales, o bien analizan el iris. Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos: por un lado, los usuarios no se fían de un haz de rayos analizando su ojo, y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas.

4.1.3.5 Retina

La vasculatura retinal (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura.

En los sistemas de autenticación basados en patrones retínales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia ínter ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

4.1.3.6 Iris

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo - de hasta 266 grados de libertad -, inalterable durante toda la vida

de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

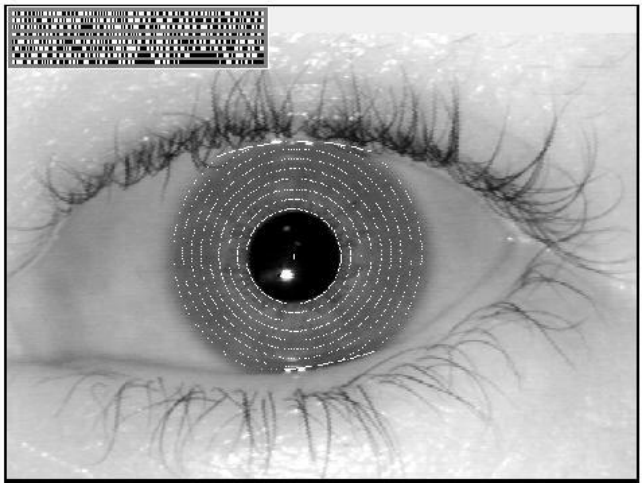


Figura 7 Control de Accesos Iris

4.1.37 Verificación de la geometría de la mano

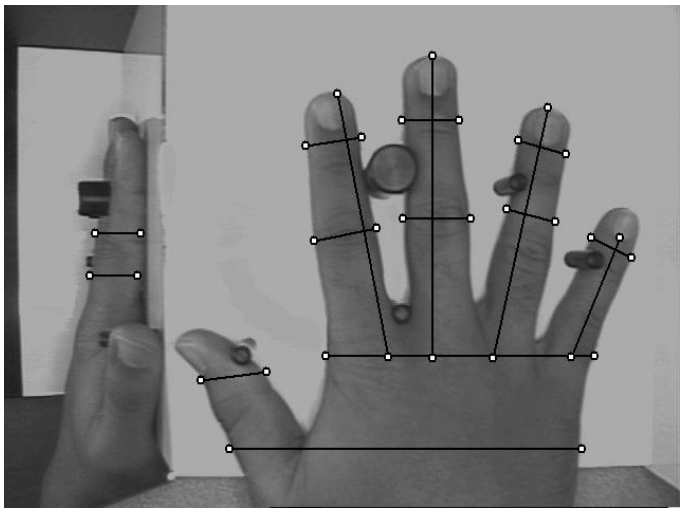


Figura 8 Control de Accesos Verificación de la geometría de la mano

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la

mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura. Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias...) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

4.2. MARCO CONCEPTUAL

4.2.1 Tarjetas Inteligentes

Las tarjetas inteligentes (tarjetas chip) nacieron en el año 1983. Su filosofía es muy sencilla, se trata de almacenar información con una cierta autonomía. Aunque la cantidad de información que pueden almacenar es relativamente pequeña, su autonomía es lo suficientemente importante como para haber producido la expansión de este tipo de tarjetas en el mercado.

La tarjeta inteligente es básicamente un chip, encapsulado en un rectángulo de PVC de aproximadamente 85 x 54 mm. Las tarjetas se suministran habitualmente en color blanco, pero pueden ser impresas utilizando diferentes sistemas. El chip que contiene dispone de unos contactos exteriores que son los que le permiten mantener una comunicación con él, y de esta forma acceder a la información que contiene o grabar nueva información. Estos contactos están bañados en oro para que la tarjeta sea resistente a un uso habitual en cualquier tipo de entorno (alta humedad (incluso con condensación), ambientes químicos). Su pequeño formato hace que sea ideal como sistema de identificación personal. Además, su medida no está limitada por razones técnicas, sino por razones de estandarización, es decir, técnicamente se podrían utilizar tarjetas que fuesen la cuarta parte de las actuales.

4.2.1.1 Utilidades

Las tarjetas chip han sido desarrolladas como sistema de almacenamiento de información inteligente e interactivos. Por tanto su uso abarca desde sistemas de moneda electrónica, hasta sistemas de identificación asociados al almacenamiento de información de los elementos a identificar. Debido a su capacidad de modificar el contenido sin el requerimiento de un grabador excesivamente costoso y la capacidad de realizar múltiples grabaciones sin riesgo de perdida de la información, están desbancando a las tradicionales tarjetas de banda magnética. Además, las tarjetas chip micro procesadas permiten tener un control mucho más seguro sobre la identificación, de forma que tras acuerdos internacionales entre fabricantes, existen identificadores diferentes para todas las tarjetas que circulan por el mundo

4.2.1.2 Tipos de tarjetas

Existen básicamente dos grandes grupos de tarjetas chip:

Tarjetas de memoria:

Sustituyen la complejidad del sistema de seguridad por una mayor capacidad de almacenar datos. Estas tarjetas permiten la lectura y grabación de datos con las funcionalidades que esto comporta. Actualmente se están fabricando tarjetas de hasta 32 Kb. de memoria. Evidentemente, la capacidad de almacenamiento está directamente relacionada con su coste. Al ser gravables en su totalidad, estas tarjetas no garantizan la identificación con absoluta seguridad, por lo que se ha de recurrir a sistemas de encriptación propios de la aplicación con la dicha tarjeta ha de operar.

Tarjetas chip de memoria protegida

Tarjeta de 256 bytes de 8 bits de memoria principal EEPROM y 32 bits de memoria de protección funcional PROM. La memoria principal se borra y escribe byte a byte. Al ser borrado, los 8 bits del byte se colocan en la posición lógica 1. La escritura y el borrado tiene un tiempo de 2.5 ms cada uno. Los primeros 32 bits pueden ser irreversiblemente protegidos contra cambios mediante la escritura del correspondiente bit en la memoria protegida. Cada escritura hecha en la memoria protegida no puede ser borrada. Esta tarjeta, además, tiene un

código lógico de seguridad que controla los accesos de escritura y borrado de la memoria. Para este propósito la tarjeta contiene una memoria de seguridad de 4 bytes con contador de errores.

Figura 10. Tarjeta chip de memoria protegida

Tarjetas micro procesadas:

Tienen como principal utilidad el uso de sistemas de contador (tarjetas monedero, tarjetas de telefonía, etc.) y de identificación de alta seguridad. Su gran uso en la banca ha permitido una rebaja constante en su precio. Normalmente no permiten almacenar mucha información, ya que su uso requiere generalmente poca cantidad de datos. Éstas disponen de una zona de memoria "protegida", solo accesible por el fabricante, que garantiza una identificación única a nivel universal.

La tarjeta chip WG10 es una tarjeta chip con microprocesador. Se trata de una tarjeta diseñada para ofrecer un alto nivel de seguridad e integración requeridos por las operaciones de monedero electrónico. El sistema operativo está basado en la última versión de la norma ISO7816.

En la máscara de la tarjeta se implementan, entre otras, las siguientes funciones:

- Gestión de PIN y claves de seguridad.
- Funciones de crédito y débito seguras.
- Algoritmo DES (Data Encryption Standard).
- Mecanismos de seguridad.
- Claves diversificadas por cada tarjeta.
- Integridad en la gestión de los datos para proteger la transacción.

- Función de búsqueda de transacciones y saldos.
- Cumplimiento de la norma ISO7816 1/2/3/4.
- Capacidad funcional de uso de SAM (Security Access Module).
- Posibilidad de gestión ON line o OFF line.
- Capacidad para multi-operadores y multi-aplicaciones.

Figura 11. Tarjeta chip micro procesada

Tarjeta criptográfica:

Es una tarjeta micro procesada que tiene funciones criptográficas en el propio microprocesador. Anexo hallarán algunas características de seguridad:

- Autenticación interna Tarjeta-Terminal.
- Autenticación externa de usuario y de aplicación
- Validación de PIN de usuario
- Servicios de integridad mediante la generación y verificación de firmas digitales RSA
- Generación de claves RSA en tarjeta
- Mecanismos de confidencialidad para el intercambio seguro de claves de cifrado.
- "Zona de espejo" para evitar pérdida de datos si la tarjeta es extraída durante una operación.

Figura 12. Tarjeta chip criptográfica

4.2.1.3 Utilización de tarjetas inteligentes

Ha habido un claro incremento en la utilización de las tarjetas chip desde su aparición. Hoy en día su utilización es generalizada, aunque muchas veces no se tenga constancia de ello. Por ejemplo, todos los teléfonos móviles digitales (GSM) llevan una. Según estudios actuales el crecimiento del consumo de tarjetas chip es como se muestra a continuación:

Experiencia: Es evidente que su uso está probado y la expansión realizada por estas tarjetas a nivel de tarjetas monedero, telefónicas y sistemas de almacenamiento de información sanitaria, tanto en Francia como en Estados Unidos, son muestras de su utilidad y fiabilidad.

Otra ventaja de adoptar este sistema es el hecho del continuo aumento del uso de estas tarjetas por parte de los usuarios.

Los beneficios que reporta el uso de las tarjetas inteligentes en el entorno de tarjetas monedero son obvios, sino fuera así no hubieran adoptado este sistema ni la Banca ni las grandes multinacionales. Evidentemente, el negocio está en disponer anticipadamente de un capital para cubrir el coste de unos servicios que aún no se han prestado. Esto supone unas ventajas tangibles para el empresario desde el punto de vista de financiación, previsión de gastos, e incluso de disponibilidad de capital para inversiones.

- Aplicaciones: La realización de software asociado a este nuevo entorno permite diversidad de aplicaciones comerciales. Sin embargo actualmente no existen demasiados equipos de desarrollo que trabajen en esta línea debido a la poca expansión del sistema y a la gran tecnología requerida. Aplicaciones tipo con tarjetas inteligentes son:

- Control de acceso y de presencia: Limitan y controlan el acceso a áreas restringidas, edificios, oficinas, clubes, administración, ordenadores.

- Pagos electrónicos: Ofrece una solución ideal para aplicaciones de tarjeta monedero, tarjetas telefónicas, maquinas expendedoras, clubes de clientes, compras electrónicas.

- Transportes: Medio de pago seguro y fácil de utilizar para transportes públicos, billetes de aviones, parquímetros, peajes de autopistas.

- Identificación y seguridad en informática: Control de acceso a ordenadores, terminales, redes, aplicaciones de software, bases de datos, directorios, ficheros confidenciales.

- Sanidad: Almacenamiento de los datos del paciente, incluyendo su historial médico. Para que los profesionales sanitarios puedan utilizarlos.

- Procesos industriales: Control de accesos en procesos de producción, medición de tiempos, seguridad industrial.

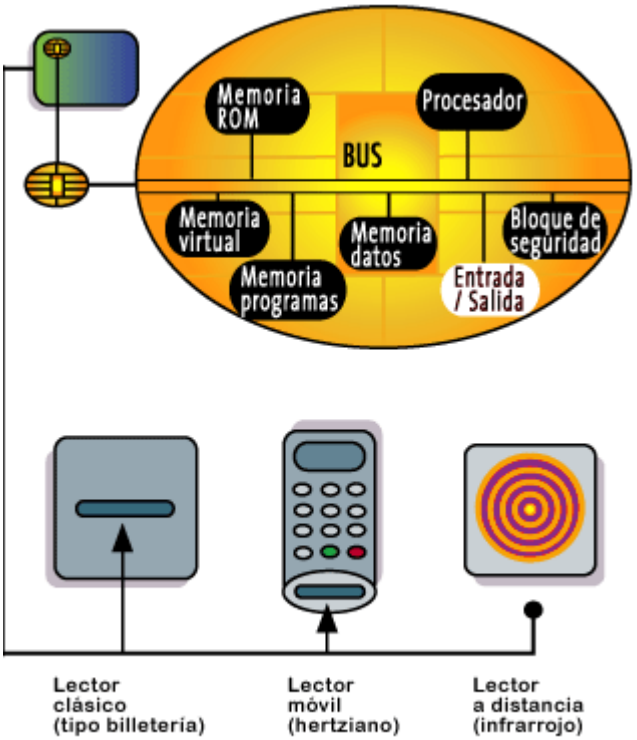


Figura 13. Resumen funcionamiento Tarjeta Inteligente

4.2.2 Unidad Lectora

Aunque habitualmente nos referimos a este dispositivo como "lectora", es frecuente que el mismo dispositivo esté capacitado para realizar la grabación. Existen muchos tipos de lectoras de tarjetas chip, y su elección va asociada, sin duda, a la elección de la tarjeta chip que se utilizará. Es decir, el orden de elección comienza por la tarjeta, y una vez decidido el tipo tarjeta que se utilizará (pueden ser más de uno), se deberá escoger la lectora. Básicamente tenemos dos grandes familias:

Universales: Permiten leer más de un tipo de tarjeta. Estas lectoras acostumbran a ser caras y solo son útiles en entornos en que los diferentes usos de las tarjetas implique la utilización de diferentes tipos de éstas (acceso a zonas, expedición de moneda, ...). Habitualmente incorporan un hardware asociado muy complejo.

Especializadas: Estas lectoras sólo pueden leer unos pocos tipos de tarjetas similares. Su simplificación permite que sean más asequibles. Normalmente van conectadas a un

ordenador, de forma que el control de la lectora y la alimentación eléctrica a menudo se simplifican.

4.2.2.1 Lectoras

MODELO	KMD6000	KMD6000 Plus	Xican
Kimaldi electronics			
	Lector tarjeta smart card, tarjeta chip bancaria para control de acceso.	El KMD6000 con carcasa de acero inoxidable.	Módulo lector / grabador tarjeta chip con display, teclado, relays, etc.
Tarjetas	Tarjeta chip micro procesada – tarjeta inteligente. Protocolo T=0. - Tarjeta chip bancaria tipo Euro 6000, Visa cash, etc.	Tarjeta chip micro procesada – tarjeta inteligente. Protocolo T=0. - Tarjeta chip bancaria tipo Euro 6000, Visa cash, etc.	Tarjeta chip de 256 bytes de memoria.
Características	Lectura código pan, fecha y otros campos del chip	Lectura código pan, fecha y otros campos del chip. Lector de inserción manual muy robusto	Incorpora: display 2x20, teclado 4x4, 2 relays, beeper, 8 entradas digitales y entrada RS-232

Tabla 11. Modelos de lectoras - Características

4.2.2.2 Lectores / Grabadores

MODELO	KMD42	UIC610
	Kimaldi electronics 	Uniform Industrial Corp. 
	Lector / grabador de tarjetas chip de memoria con conexión RS-232	Lector / grabador de tarjeta inteligente PC/SC que cumple estándar EMV
Tarjetas	Lectura y grabación de tarjeta chip SLE 4442 de 256 bytes.	- Para tarjetas CPU protocolos T=0, T=1. - Soporte de tarjetas síncronas, tarjetas de memoria tipo SLE4442, SLE4428, etc.
Características	- 2ª conexión RS-232 que permite la conexión del lector + un periférico a un único COM. - Controles OCX / VCL de Windows. - Comandos código ASCII.	
Interfase	Conexión RS-232 a host	Conexión USB o RS-232

Tabla 12. Modelos de lectoras / grabadores - Características

4.2.2.3 Lectores Híbridos de Inserción

MODELO	HCR330	HCR350
Uniform Industrial Corp.		
	Lector de inserción manual híbrido: lector banda magnética y lector / grabador tarjeta chip.	Lector de inserción manual híbrido: lector banda magnética y lector / grabador tarjeta chip. Tamaño reducido.
Tarjetas	Soporta tarjetas chip de memoria y tarjetas micro procesadas T=0 / T=1	Soporta tarjetas chip de memoria y tarjetas micro procesadas T=0 / T=1
Coercitividad	Lectura de banda magnética de alta y baja coercitividad (300-4,000 oe). Disponible en configuración para 1, 2 y 3 pistas	Lectura de banda magnética de alta y baja coercitividad (300-4,000 oe).
Características	- Bloqueo de la tarjeta mientras está leyendo el chip. Incorpora slot SAM (Security Access Module), opcionalmente ampliación a 4 SAMs. - Expulsión de la tarjeta mediante comando y al interrumpirse la alimentación.	- Diseño delgado. - Frontal de plástico o metálico.
Interfase	Interfase RS-232 y opcionalmente TTL o USB	Interfase RS-232 y opcionalmente TTL

Tabla 13. Lectores Híbridos de Inserción - Características

4.2.3 Microcontroladores

Recibe el nombre de controlador el dispositivo que se emplea para el gobierno de uno o varios procesos. Por ejemplo, el controlador que regula el funcionamiento de un horno dispone de un censor que mide constantemente su temperatura interna y, cuando traspasa los

límites prefijados, genera las señales adecuadas que accionan los efectores que intentan llevar el valor de la temperatura dentro del rango estipulado.

Aunque el concepto de controlador ha permanecido invariable a través del tiempo, su implementación física ha variado frecuentemente. Hace tres décadas, los controladores se construían exclusivamente con componentes de lógica discreta, posteriormente se emplearon los microprocesadores, que se rodeaban con chips de memoria y E/S sobre una tarjeta de circuito impreso. En la actualidad, todos los elementos del controlador se han podido incluir en un chip, el cual recibe el nombre de microcontrolador. Realmente consiste en un sencillo pero completo computador contenido en el corazón (chip) de un circuito integrado.

Un microcontrolador es un circuito integrado de alta escala de integración que incorpora la mayor parte de los elementos que configuran un controlador.

Un microcontrolador dispone normalmente de los siguientes componentes:

- Procesador o UCP (Unidad Central de Proceso).

- Memoria RAM para Contener los datos.

- Memoria para el programa tipo ROM/PROM/EPROM.

- Líneas de E/S para comunicarse con el exterior.

Generador de impulsos de reloj que sincronizan el funcionamiento de todo el sistema.

Los productos que para su regulación incorporan un microcontrolador disponen de las siguientes ventajas:

Aumento de prestaciones: un mayor control sobre un determinado elemento representa una mejora considerable en el mismo.

Aumento de la fiabilidad: al reemplazar el microcontrolador por un elevado número de elementos disminuye el riesgo de averías y se precisan menos ajustes.

Reducción del tamaño en el producto acabado: La integración del microcontrolador en un chip disminuye el volumen, la mano de obra y los stocks.

Mayor flexibilidad: las características de control están programadas por lo que su modificación sólo necesita cambios en el programa de instrucciones.

El microcontrolador es en definitiva un circuito integrado que incluye todos los componentes de un computador. Debido a su reducido tamaño es posible montar el controlador en el propio dispositivo al que gobierna. En este caso el controlador recibe el nombre de controlador empotrado (embedded controller).

4.2.4 Bases de Datos

Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

Las bases de datos proporcionan la infraestructura requerida para los sistemas de apoyo a la toma de decisiones y para los sistemas de información estratégicos, ya que estos sistemas explotan la información contenida en las bases de datos de la organización para apoyar el proceso de toma de decisiones o para lograr ventajas competitivas. Por este motivo es importante conocer la forma en que están estructuradas las bases de datos y su manejo.

Los datos son la Base de Datos propiamente dicha.

Hardware. El hardware se refiere a los dispositivos de almacenamiento en donde reside la base de datos, así como a los dispositivos periféricos (unidad de control, canales de comunicación, etc.) necesarios para su uso.

Software. Está constituido por un conjunto de programas que se conoce como Sistema Manejador de Base de Datos (DMBS: Data Base Management System). Este sistema maneja todas las solicitudes formuladas por los usuarios a la base de datos.

Usuarios. Existen tres clases de usuarios relacionados con una Base de Datos:

1. El programador de aplicaciones, quien crea programas de aplicación que utilizan la base de datos.

2. El usuario final, quien accesa la Base de Datos por medio de un lenguaje de consulta o de programas de aplicación.

3. El administrador de la Base de Datos (DBA: Data Base Administrator), quien se encarga del control general del Sistema de Base de Datos.

Globalización de la información. Permite a los diferentes usuarios considerar la información como un recurso corporativo que carece de dueños específicos.

4.2.5 Cerradura Eléctrica

Este destrabador realiza la apertura de una cerradura estándar liberando el pestillo en forma eléctrica, comandado por los controles de accesos. Es el tipo más común y económico, ofreciendo un grado de seguridad bajo. Es ideal para instalaciones simples donde se utiliza la

cerradura existente. Se instala sobre el marco de la puerta, por lo general embutido; también hay accesorios para montaje aplicado como en el caso de puertas de vidrio.

Los hay de dos tipos de activación:

- Activación con energía: para la apertura necesita ser energizado y traba la puerta sin necesidad de corriente eléctrica.
- Activación sin energía: para la apertura debe quitarse la energía, ya que la traba la realiza estando energizado. La ventaja de este destrabador es que puede utilizarse para casos de emergencia donde hay que asegurar la apertura sin disponer del resto de la instalación, ya que se le puede quitar la energía con un pulsador de corte de emergencia. Su calidad y costo son mayores.

4.3. HIPOTESIS

4.3.1. General

Desarrollar un sistema de control de acceso de personas a un centro de computo utilizando como llave de identificación la tarjeta inteligente la cual es leída por una unidad lectora de contacto. Este lector captura los datos de la tarjeta y los decodifica entregado a un circuito electrónico una señal digital la cual es enviada por hilos de cobre a un servidor de gestión el cual validará y autenticará los datos recibidos permitiendo la habilitación de un censor para permitir la apertura de la puerta de acceso ó proteger al área de accesos no autorizados con la generación de alarmas. Todo el sistema de validación de usuarios estará controlado por servidor de gestión que será soportado por una base de datos la cual tendrá todos los usuarios y controles de nuestro sistema.

4.3.2 De Trabajo:

4.3.2.1 Llave de autenticación:

La utilización de las tarjetas inteligentes de contacto como de medio de autenticación para lograr el acceso a un centro de computo ó un recinto de accedo controlado. Estas tarjetas son

las que necesitan ser insertadas en una terminal con lector inteligente para que por medio de contactos pueda ser leída.

El control de acceso: Es el elemento mas obvio y el que mas se descuida por ejemplo el acceso a la estación de administración de la red o a la sala de servidores, por otro lado es muy importante que exista un sistema de contraseñas que es la única forma de autentificar e identificar a los usuarios en el momento en que acceden al sistema informático.

No existe un sistema seguro al 100%, pero el de las tarjeta inteligentes es teóricamente el que ofrece un mayor grado de seguridad.
La tarjeta inteligente es un mecanismo muy seguro para el almacenamiento de información financiera o transaccional, la tarjeta inteligente es un lugar seguro para almacenar información como claves privadas, numero de cuenta, password, o información personal muy valiosa, esta capacidad se debe a:

- Encriptación.
- Clave segura (PIN).
- Clave secundaria de seguridad.
- Sistema de seguridad redundante.
- Firmas digitales.
- Alta seguridad en el acceso físicos a: recintos, laboratorios, controles, salas informáticas.
- A través de sistemas biométricos, huella dactilar y retina.

4.3.2.2 Circuito electrónico

La elaboración de un circuito electrónico que permita la recepción de una señal eléctrica emitida por el servidor de gestión y la cual le indicará al circuito la realización de un tarea definida previamente. Está tarea programada previamente en un microcontrolador indicará al mecanismo que tipo de acción realizar. A su vez este mecanismo informará al sistema su estado real de servicio.

4.3.2.3 Servidor de Gestión

Es un programa desarrollado en Visual Basic para Windows 2000 Profesional que permite la administración de todo el sistema. Está diseñado para manejar varios hilos de proceso, lo que le permite atender rutinas de comunicación serial con lo módulos de acceso mientras se procesan datos requeridos por el administrador. Toda la información pertinente al sistema es almacenada en una base de datos relacional que incluye las tablas necesarias para la administración del sistema. En el programa el manejo de la información se hace utilizando un lenguaje estándar de búsqueda estructurada en base de datos SQL, que permite hacer poderosas relaciones de información de varias de las tablas.

5. METODOLOGIA

5.1 TIPO DE INVESTIGACION

La investigación se enfocara al crecimiento empresarial y tecnológico con la construcción de un dispositivo electrónico con interfaz a un sistema de cómputo.

5.2 LINEA DE INVESTIGACION

El proyecto esta enfocado al desarrollo empresarial y tecnológico, donde se van a involucrar las siguientes disciplinas:

- Ingenierías del software, ya que el software será un producto eficiente y de calidad.
- Ingeniería electrónica, puesto que el desarrollo involucra el diseño y la construcción de las plaquetas de circuitos para el interfaz del sistema.

5.3. ETAPAS O FASES

5.3.1. Etapa Preliminar

5.3.1.1 Identificación problema

La mediana ó pequeña industria colombiana no cuentan con sistemas de control de acceso a sus centros de computo para proteger sus activos más preciados: La información, las máquinas que contienen estos datos y los medios con los cuales es transmitida a los diferentes puntos de una organización.

En el mercado colombiano existente diferentes medios y tecnologías para controlar el acceso a un centro de computo como la seguridad física realizada por una persona ó herramientas de autenticación y validación como la biometría, tarjetas magnéticas, teclados matriciales, etc. Algunos con mejores argumentos tecnológicos como los sistemas de control de la retina humana ó la confirmación de la huella dactilar pero que no son de fácil adquisición por cualquier empresa debido a su gran valor económico.

Existente otras tecnologías de control de acceso como la utilización de teclados matriciales, tarjetas de banda magnética ó códigos de barras han motivado a los impostores ha superar estos sistemas de seguridad con una mayor facilidad, lo que obliga a los usuarios a instalar nuevos sistemas cada vez más potentes y fiables.

Está es la razón por la cual se ha planteado desarrollar y crear un prototipo que solucione el problema de control de acceso a centros de computo, con herramientas y tecnología de última generación y lo más interesante de todo su bajo valor económico.

5.3.1.2 Evaluación y Selección de alternativas

- Investigación del mercado

La unidad de control de acceso SCAES está dirigida hacia la mediana y pequeña industria, universidades y entidades que requieren un esquema de seguridad para sus lugares más importantes.

- Encuestas y recolección de datos

La forma mas ágil de recolectar información es la encuesta. Se sabe que una investigación de mercados puede ser la clave para el lanzamiento de un nuevo producto o para el relanzamiento de uno que ya existente, también se sabe que diseñar y aplicar una encuesta es una tarea demorada y laboriosa por esta razón muchas personas la dejan para el final.

La única fuente fidedigna de datos es el mismo mercado y el mejor método para recolectar esta información es a través de una investigación de mercado. La investigación arroja datos supremamente importantes no solo para su utilización en el campo financiero si no también en el área de mercado para la estrategia y su implementación: Con los datos se trabaja directamente con certeza, y no con especulaciones.

- Preguntas de investigación

- ¿Sabe que es un control de acceso para centros de computo?
- ¿Saben las empresas colombianas sobre SCAEC?
- ¿Cuentan las empresas colombianas con métodos eficaces y económicos para realizar procesos de control de acceso?
- ¿Por qué es necesario proteger la información?
- ¿Usted sabe que son los métodos de control de acceso por tarjeta inteligente?
- ¿Si la empresa tuviera la oportunidad de adquirir sistemas de control de acceso con está metodología ustedes los compraría?

- Ficha Técnica

- Población 1215 empresas en la capital colombiana
- Nivel de confianza 80%
- Muestreo por convivencia no probalístico
- Dirigido a la mediana y pequeña empresa bogotana
- Encuesta aplicada a 30 empresas.

- Tabulación Información

Análisis gráfica de la información recopilada

Figura 14. Tabulación pregunta - ¿Sabe que es un control de acceso para centros de computo?

Fuente: Pequeña y mediana empresa.

En la anterior grafica se percibe que las personas no conocen los sistemas de control de Acceso en centros de computo en una proporción del 70 %.

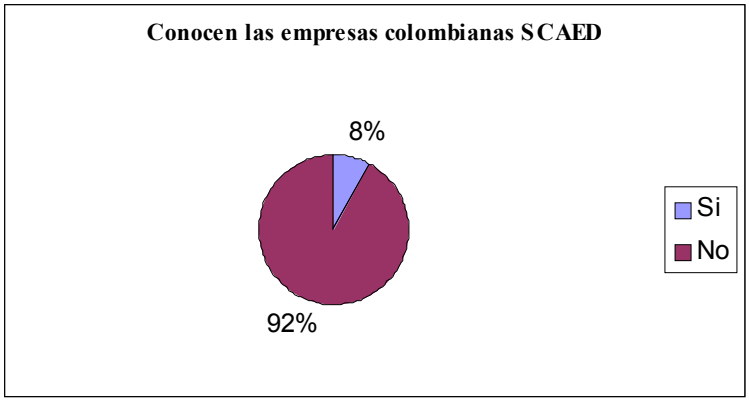


Figura 15. Tabulación pregunta - ¿Conocen las empresas colombianas SCAEC?

Fuente: Pequeña y mediana empresa.

La gran mayoría de las empresas no conocen el significado de SCAEC en una amplia Proporción del 92 %.

Figura 16. Tabulación pregunta - ¿Cuentan las empresas colombianas con un método seguro de control de acceso de personas a centros de computo?

Fuente: Pequeña y mediana empresa.

En la grafica se percibe claramente que no se poseen métodos seguros de acceso de personas en los centros de computo, con un porcentaje del 77 %.

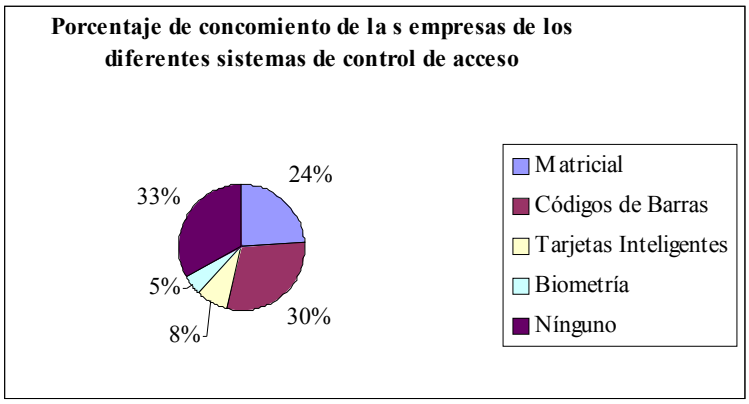


Figura 17. Análisis encuesta - Porcentaje de conocimiento de las empresas de los diferentes sistemas de control de acceso.

Fuente: Pequeña y mediana empresa.

Las empresas no conocen en un 33 % ningún sistema de control, con un 30 % los códigos de barras, con un 24 % los sistemas matricial, con un 8 % las tarjetas inteligentes que son las que nos ocupan y finalmente con 5% los sistemas de biometría.

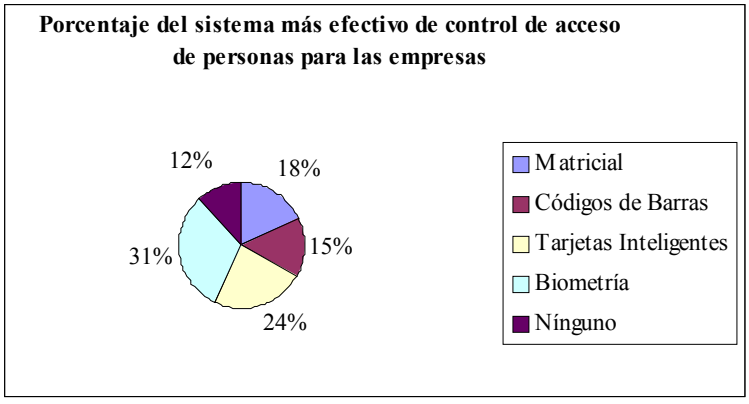


Figura 18. Análisis encuesta - Porcentaje del sistema más efectivo de control de acceso de personas para las empresas.

Fuente: Pequeña y mediana empresa.

En la grafica anterior se percibe que el sistema más efectivo para el acceso de personas es la biometría con un 31 %, que tiene un alto costo, seguido de las tarjetas inteligentes con un 24 % y de los sistemas matricial y del códigos de barras.

- Modelos de control de acceso del mercado

Claves por Teclado:
Obviamente esta opción es la más económica, pero la menos segura. Hace tiempo que han caído en desuso y no se han generado hasta el momento nuevas aplicaciones donde puedan resurgir como una opción válida.

Banda Magnética:
Es la más conocida y difundida. Su ventaja es su popularidad y el bajo costo, pero en sí es, de todos los medios de identificación, uno de los más vulnerables de todos. Sólo se recomiendan en oficinas o establecimientos administrativos. Su principal problema es el desgaste al que se ven sometidos tanto el lector, como las tarjetas y la posible desmagnetización de la banda, obligando a cambiar o re grabar la tarjeta con todos los problemas que trae aparejado.

Wiegand:
Fue uno de los primeros sistemas de lectura que se utilizó. Hoy en día, sólo se usa en ampliaciones de instalaciones viejas, pero no se ofrece en sistemas nuevos.

Código de Barras:
La principal ventaja de esta tarjeta, es que permite una construcción rápida y económica por el mismo usuario, no existe rozamiento con un cabezal, pero a pesar de que se las puede proteger contra fotocopias, son las más vulnerables en lo que a seguridad se refiere.

Touch Memories:
Es una pastilla electrónica, encapsulada en acero inoxidable que generalmente se transportan con un soporte plástico tipo llavero. Brindan un muy alto nivel de seguridad ya que no se

pueden duplicar y son altamente resistentes al desgaste, siendo ideales para ambientes industriales, aunque no son recomendables para ambientes con alto grado de generación de corriente estática (P. Ej.: oficinas con mucha alfombra y ambientes muy secos).

Biométricos:

Su funcionamiento se basa en la lectura de alguna parte del cuerpo humano, eliminando por completo el uso de las tarjetas y por tal motivo son muy seguros, pero a su vez, son los más caros y requieren de un cuidado bastante especial, con lo cual hasta el momento no son utilizados en aplicaciones de uso masivo.

Tarjeta Inteligentes:

Son tarjetas de plástico similares en tamaño y otros estándares físicos a las tarjetas de crédito que llevan estampadas un circuito integrado: Este es un circuito que puede ser de una sola memoria o contiene un microprocesador con un sistema operativo que le permite una serie de tareas como: Almacenar, encriptar información, leer y escribir datos, como un ordenador. Es una tarjeta que por su diseño tecnológico, no puede duplicarse. Cada una posee un código distinto y no permite que varios usuarios puedan tener una tarjeta duplicada.

Cuadro comparativo

Habiendo detallado las características de cada sistema por separado, podemos resumir lo expuesto en este cuadro comparativo.

Tecnología de Lectura	**Seguridad / Inviolabilidad**	**Desgaste Tarjeta**	**Desgaste Lector**	**Costo Man-tenimiento**	**Precio Tarjeta**	**Precio Lector**
Clave Tec.	Muy Baja	No Posee	Alto	Medio	No posee	Bajo
Magnética	Media	Alto	Muy Alto	Alto	Muy Bajo	Bajo
Wiegand	Alta	Medio	Bajo	Bajo	Medio	Medio
Cód. Barras	Baja	Medio	Bajo	Medio	Bajo	Medio
Touch Mem.	Alta	No Posee	No Posee	No Posee	Medio-Alto	Muy Bajo
Tarjetas Inteligentes	Alta	No Posee	No Posee	No Posee	Medio-Bajo	Medio
Biométrico	Muy Alta	No Posee	Bajo	Medio-Alto	No Posee	Muy Alto

Tabla 13. Cuadro comparativo modelos de control de acceso

<u>- Planificación proyecto</u>

a. Identificación problema

- Elección problema
- Identificación problema

b. Evaluación y Selección de alternativas

- Investigación del mercado
- Encuestas y recolección de datos
- Tabulación Información
- Estudiar modelos de accesos
- Formulación hipótesis
- Fijación de Objetivos
- Planificación proyecto
- Evaluación financiera

c. Análisis y diseño prototipo

- Análisis prototipo
- Diagramas de flujo de información
- Diagrama general de proceso
- Diagrama procesos de hardware
- Diagrama procesos de software
- Explotación procesos
- Diseño base de datos MER
- Diagrama de bloques
- Diseño Circuito electrónico

d. Implementar e integrar los módulos del prototipo

- Configuración unidad lectora
- Configuración quemadora tarjetas
- Configuración quemadora de tarjetas pasivas
- Elaboración circuito electrónico
- Implementación base de datos relacional
- Desarrollo software visual
- Implementación interfases de comunicación
- Integración módulos
- Puesta en marcha prototipo

e. Valorar y modificar integración prototipo

- Valoración integral del sistema
- Revisión entradas y salidas de datos
- Corrección de fallas de los módulos
- Validación final del sistema
- Pruebas usuario final
- Documentación sistema

- Evaluación financiera

Los principales elementos que se requieren para el desarrollo del proyecto son:

	Unidad / Mt	Valor unidad
Tarjetas inteligentes	3	$ 8.000
Unidad Lectora	1	$ 300.000
Circuito electrónico de control	1	$ 270.000
Elementos adicionales electrónicos	1	$ 100.000

Tabla 14. Principales componentes de SCAES

5.3.2 Análisis

El prototipo del control de acceso electrónicos y sistematizados estará conformado e integrado por los siguientes elementos:

- Tarjetas inteligentes de contacto de memoria protegida
- Unidad lectora de tarjetas inteligentes de contacto
- Un servidor de gestión, el cual integrará el siguiente software:
    - Visual Basic como herramienta de programación
    - Manejador de Base de Datos Access
- Una interfase electrónica regulada por un microcontrolador que ejecutará las ordenes emitidas por el servidor de gestión y que informará al mismo su estado real.
- Una cerradura eléctrica de control de pistillo

5.3.2.1 Análisis visual de acceso

Figura 19.

Análisis visual de acceso

5.3.2.2 Análisis de localización de las unidades lectoras

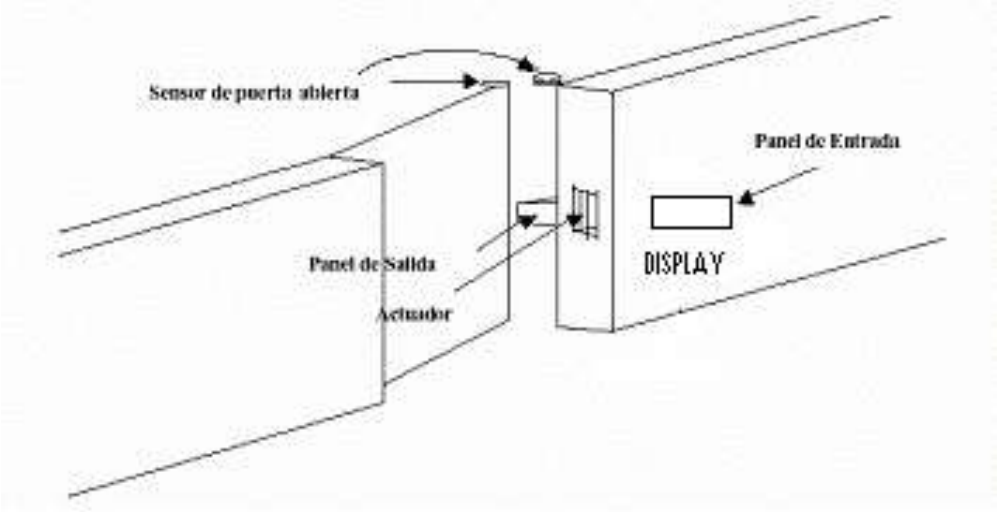


Figura 20.

Análisis de localización de las unidades lectoras

5.3.2.3 Análisis del modelo del servidor de gestión

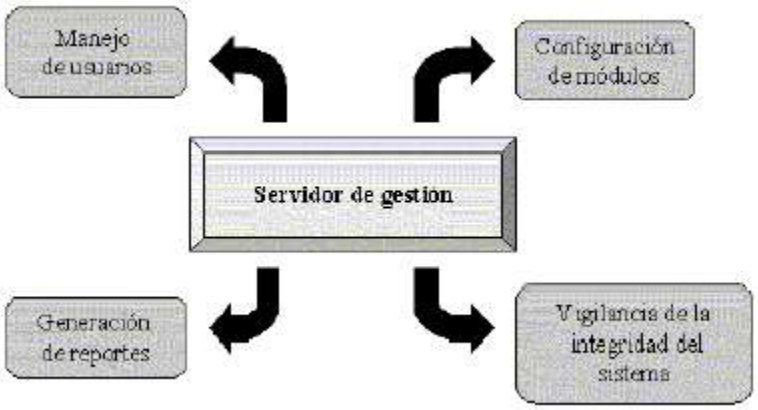


Figura 21. Análisis del modelo del servidor de gestión

5.3.2.4 Análisis modelo integral con el servidor de gestión

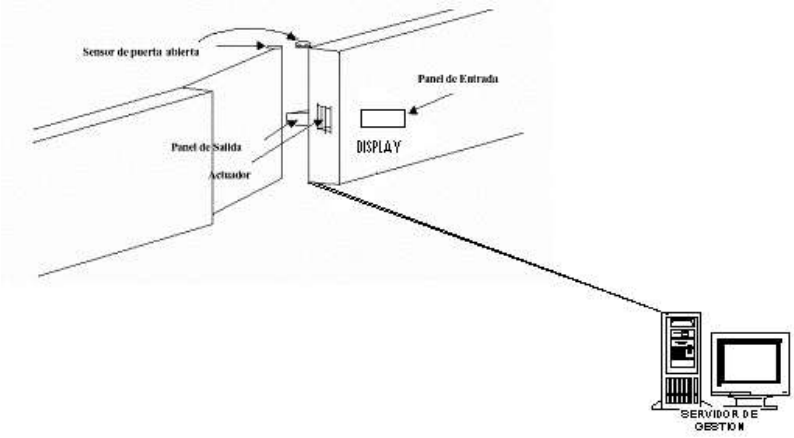


Figura 22. Análisis modelo integral con el servidor de gestión

5.3.2.5 Análisis modelo lógico del sistema

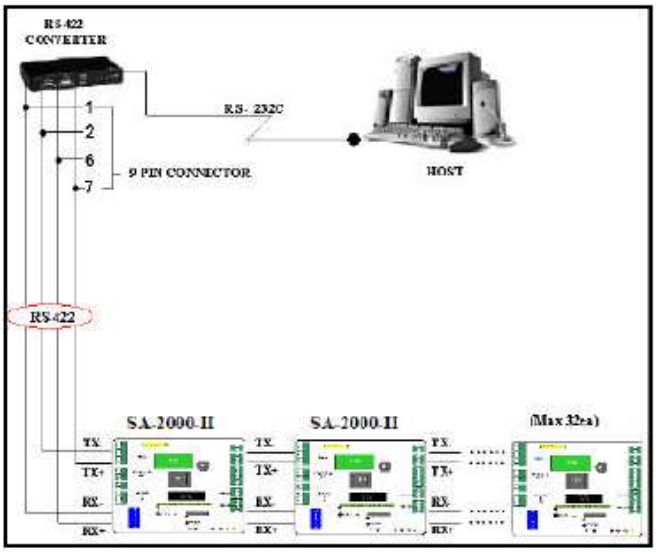


Figura 23. Análisis modelo lógico del sistema

5.3.3 Diseño

5.3.3.1 Diagrama general de proceso

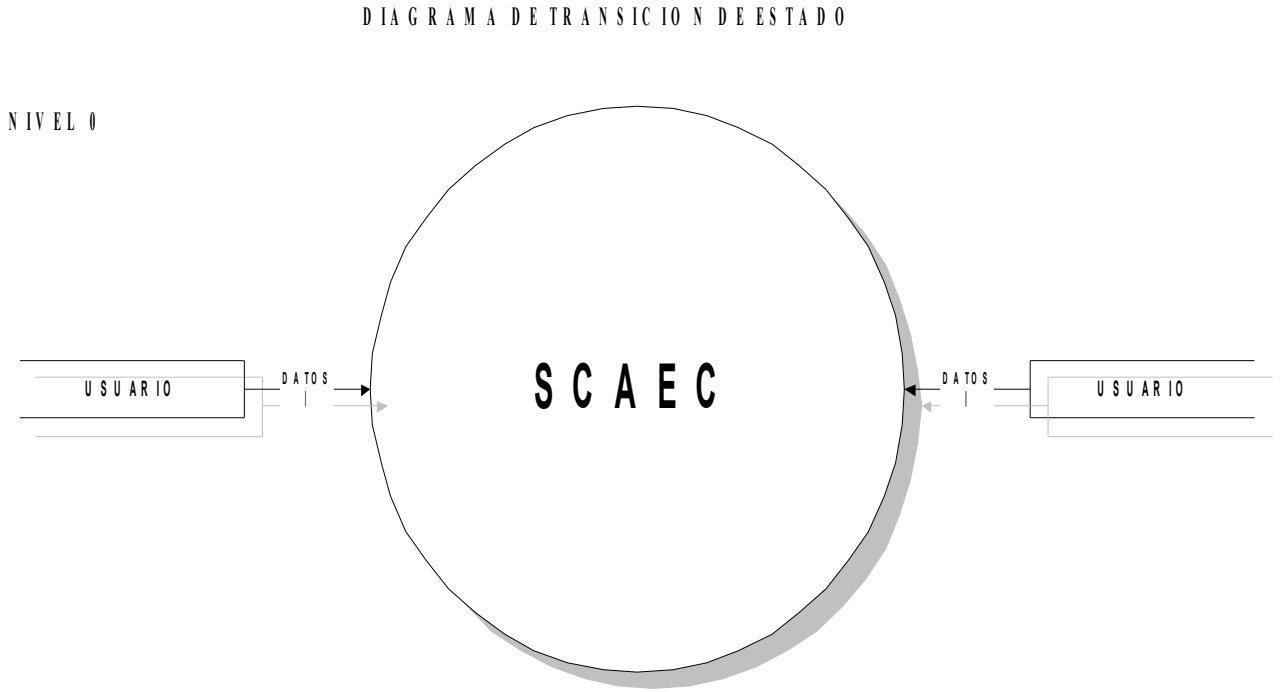


Figura 24. Diagrama general de proceso

5.3.3.2 Diagrama general de transición de estado del sistema

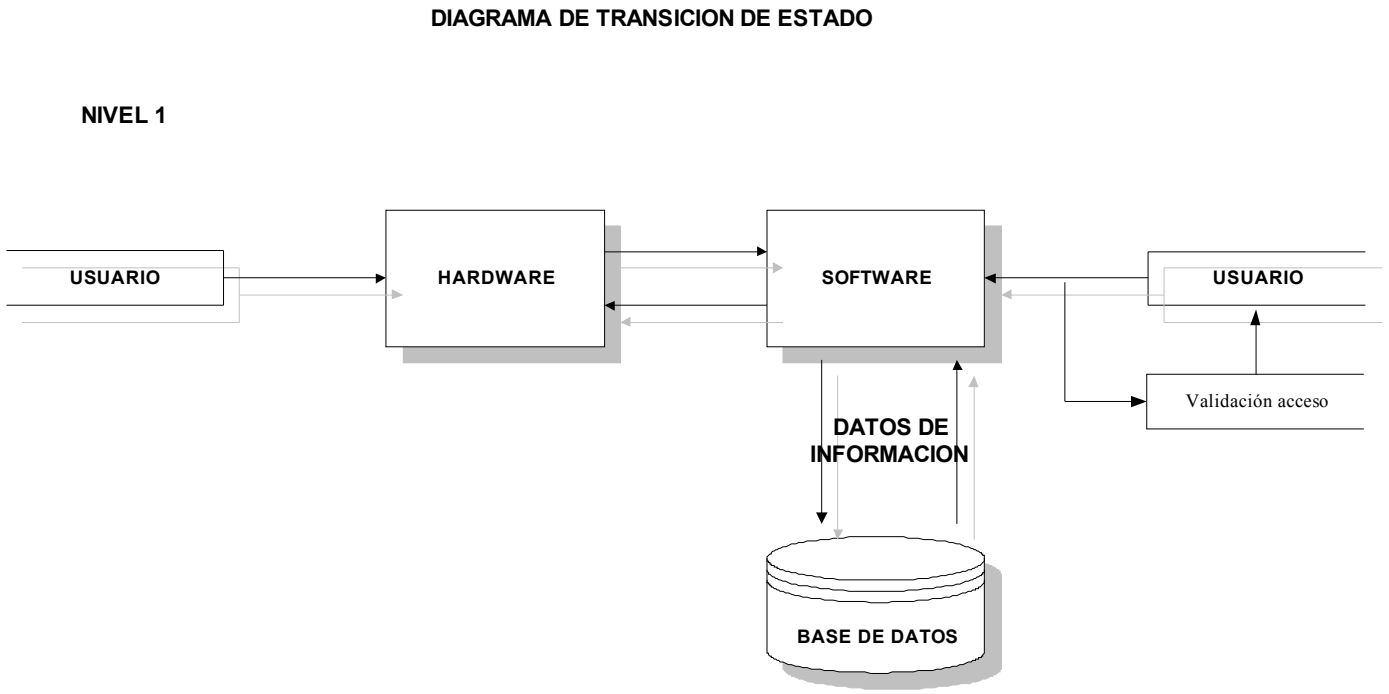


Figura 25. Diagrama general de transición de estado del sistema

5.3.3.3 Diagrama general de transición de estado en el hardware

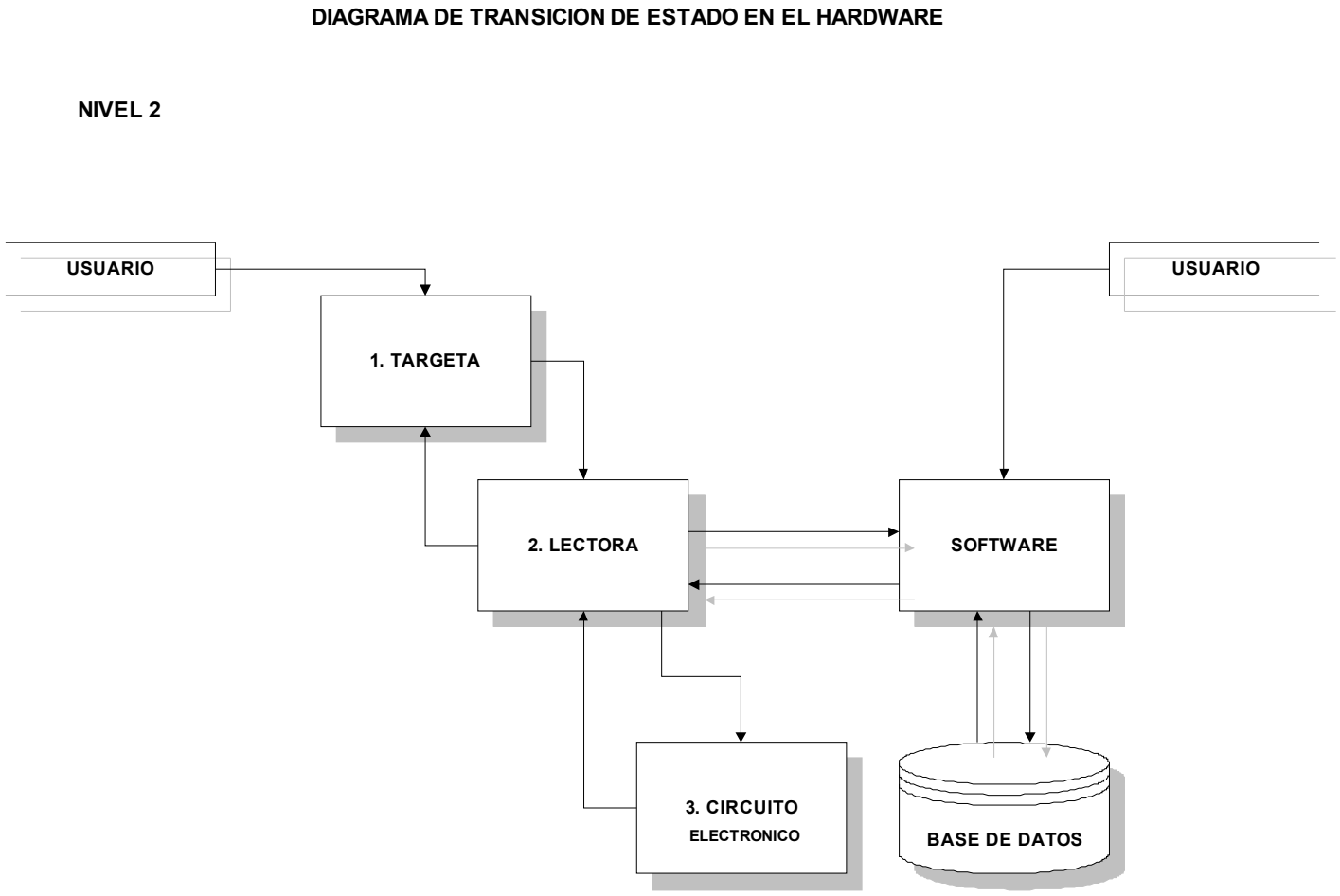


Figura 26. Diagrama general de transición de estado en el hardware nivel 2

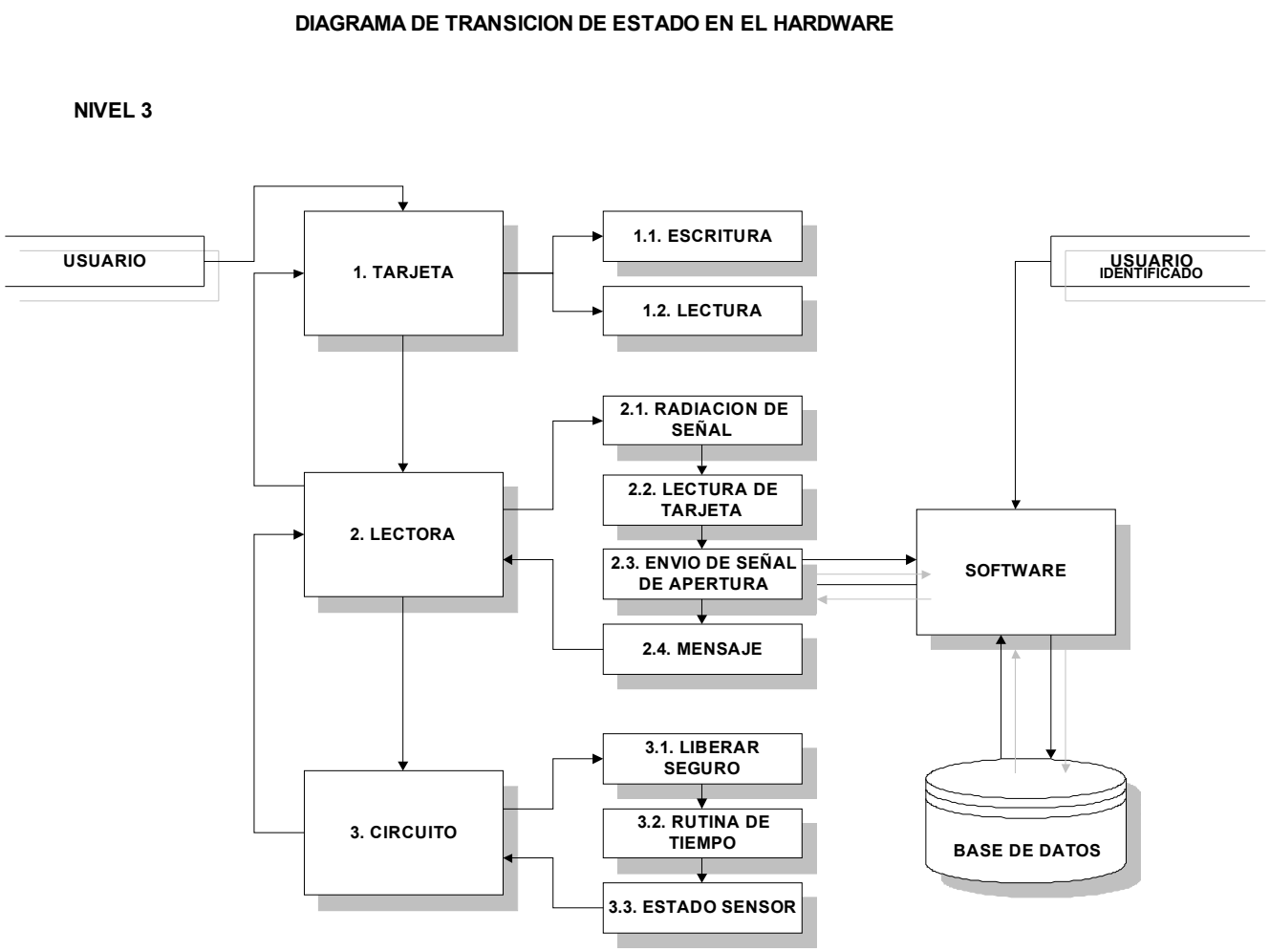


Figura 27. Diagrama general de transición de estado en el hardware nivel 3

5.3.3.4 Explotación procesos

Modelo Explotación procesos: Modulo de Seguridad

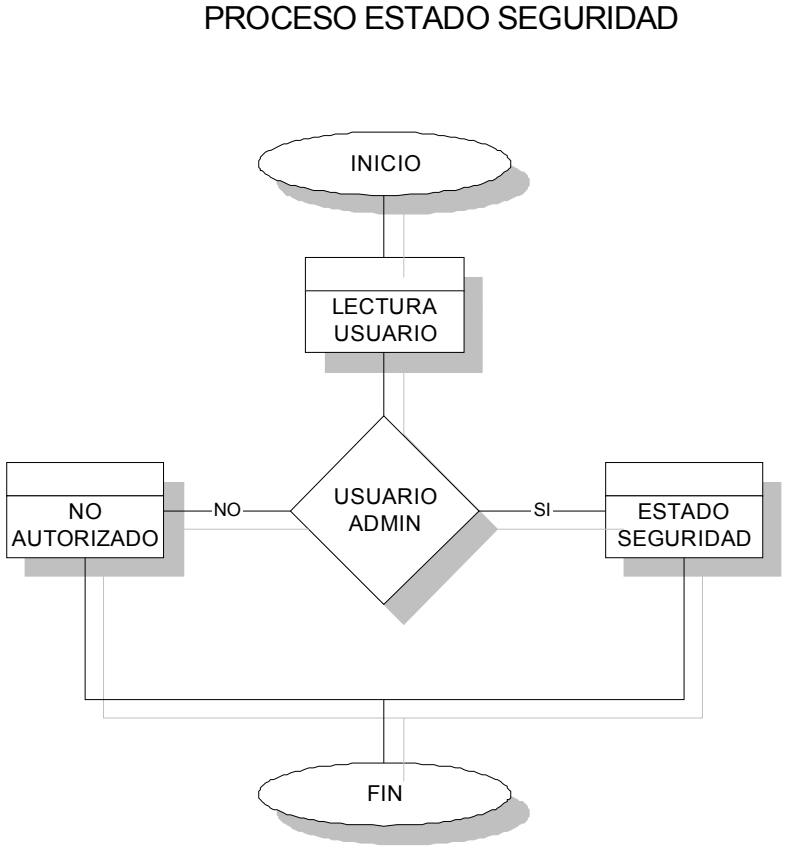


Figura 28. Modelo Explotación de procesos – Modulo de Seguridad

Modelo Explotación procesos: Nivel 0

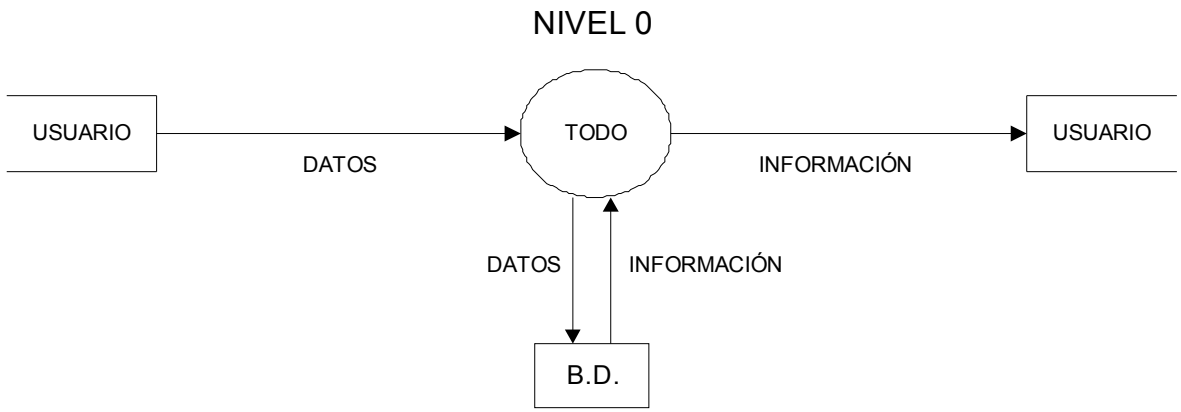


Figura 29. Modelo Explotación de procesos – Nivel 0

Modelo Explotación procesos: Nivel 1

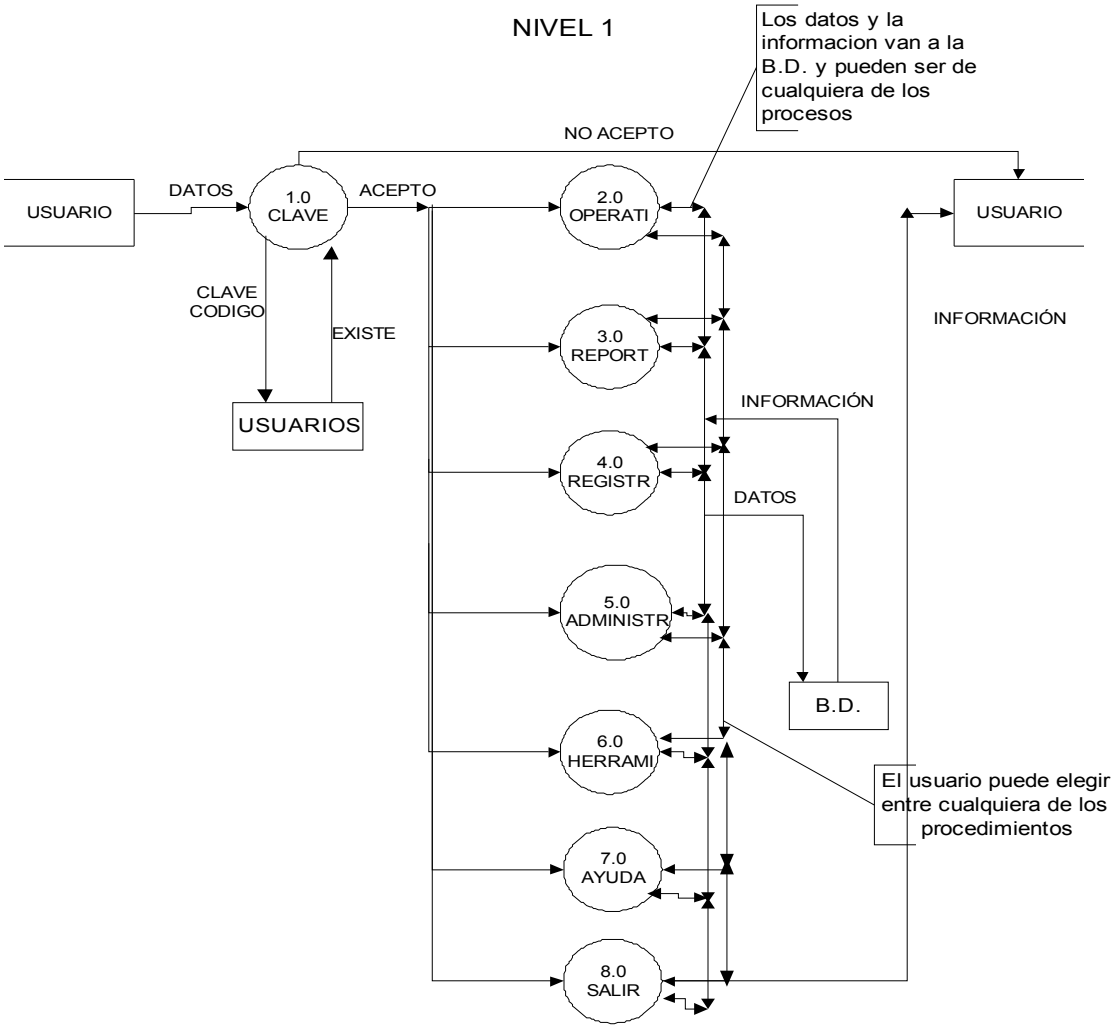


Figura 30. Modelo Explotación de procesos – Nivel 1

Modelo Explotación procesos: Nivel 2

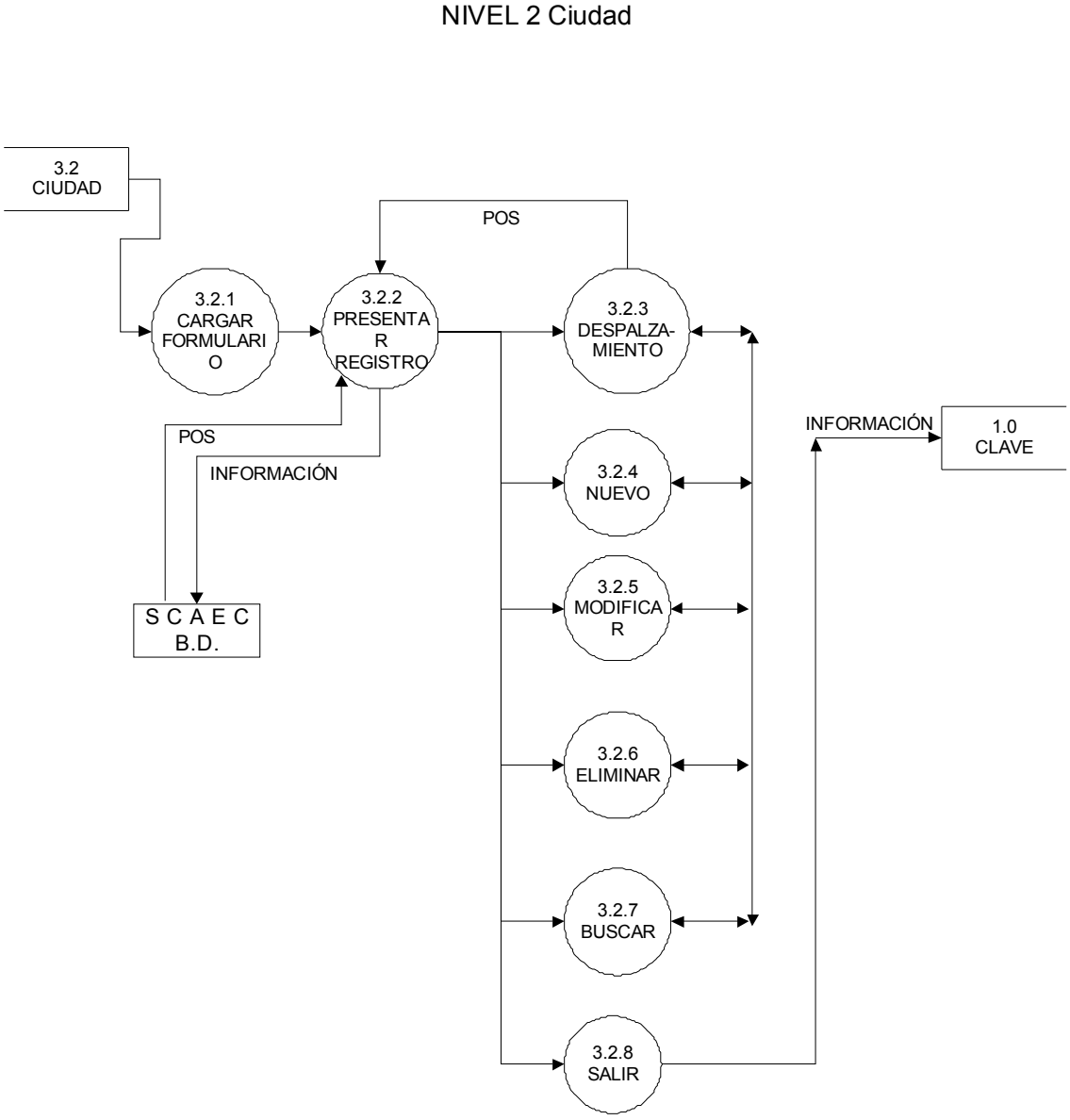


Figura 31. Modelo Explotación de procesos – Nivel 2

Modelo Explotación procesos: Nivel 3

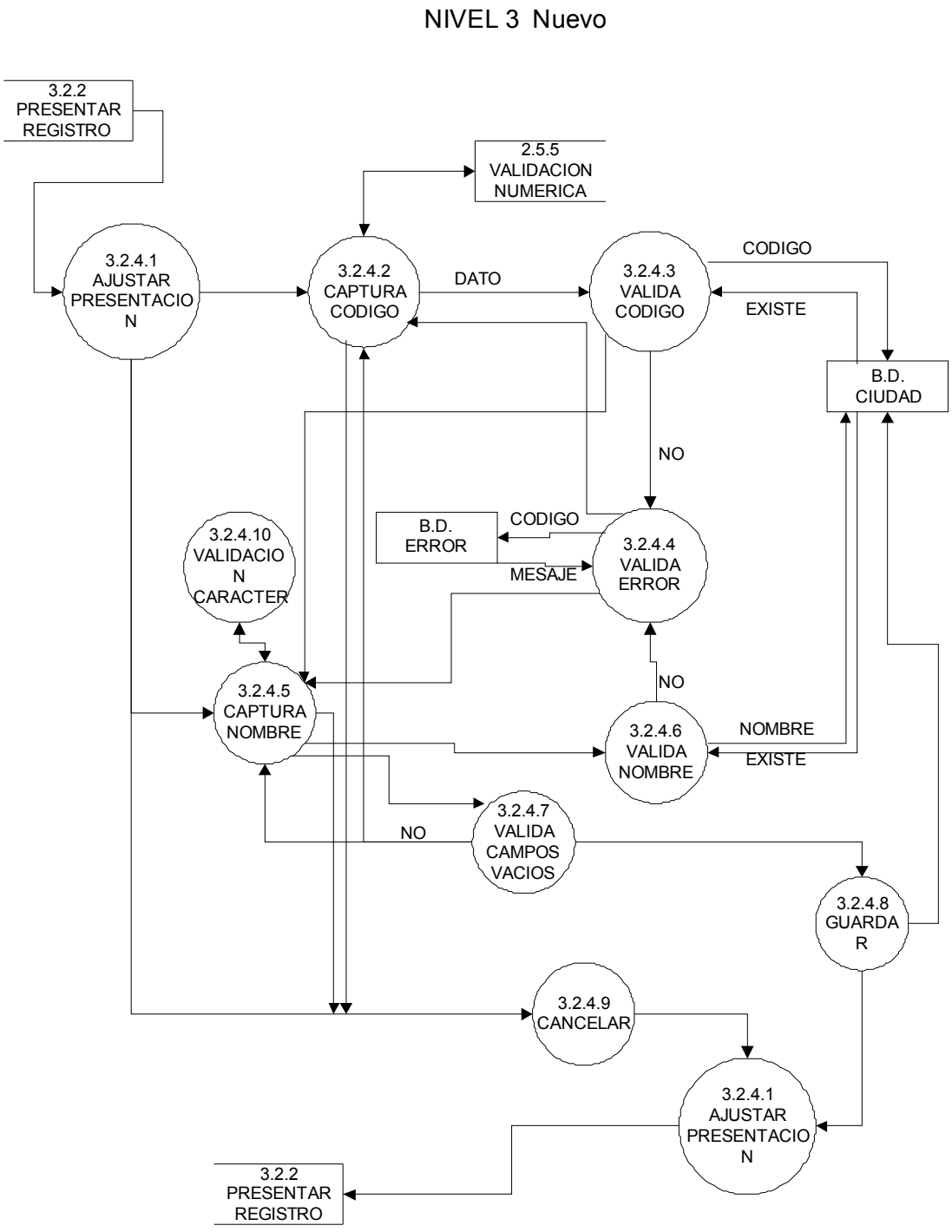


Figura 32. Modelo Explotación de procesos – Nivel 3

Modelo Explotación procesos: Nivel 4

Nível 4 - Eliminar

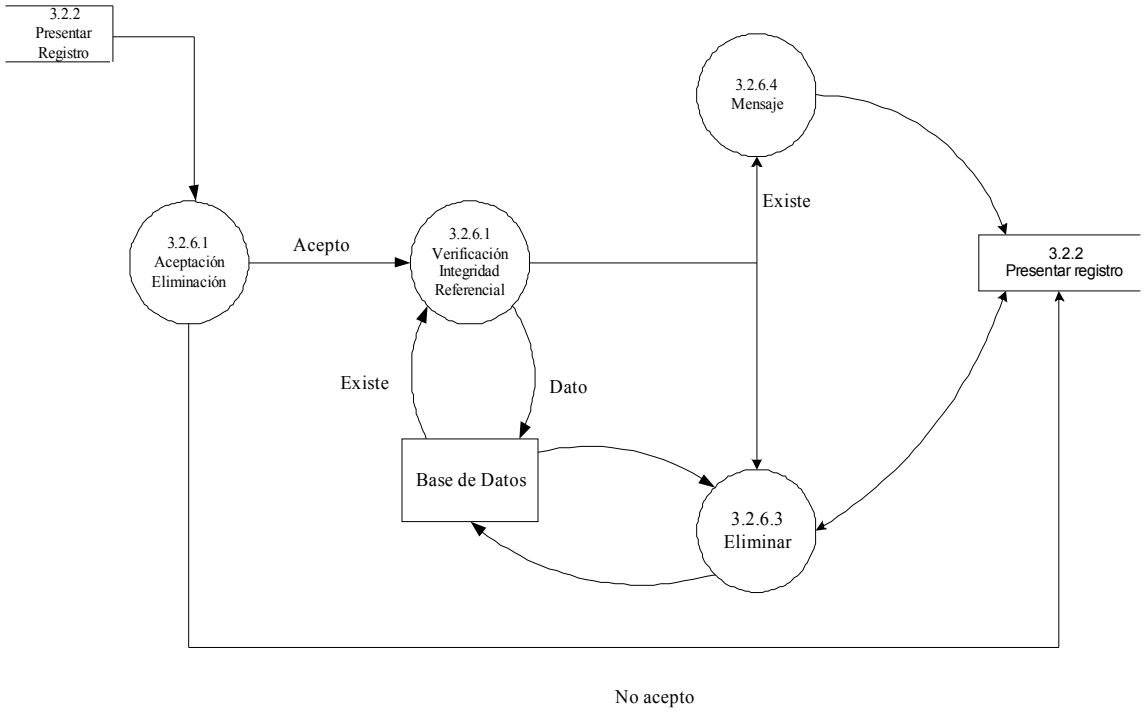


Figura 33. Modelo Explotación de procesos – Nivel 4 Eliminar

Nível 4 - Buscar

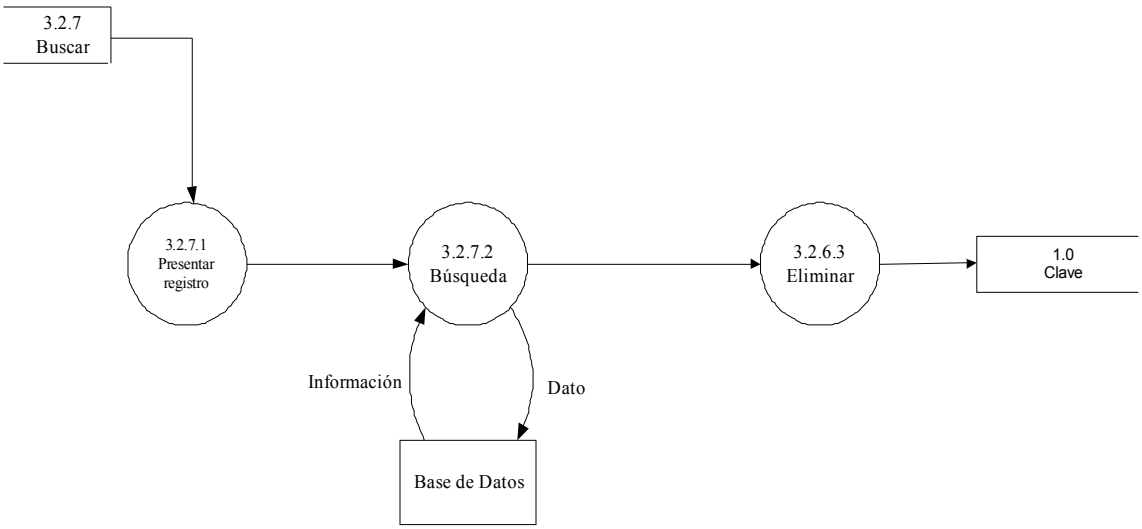


Figura 34. Modelo Explotación de procesos – Nivel 4 Buscar

NIVEL 4 Guardar

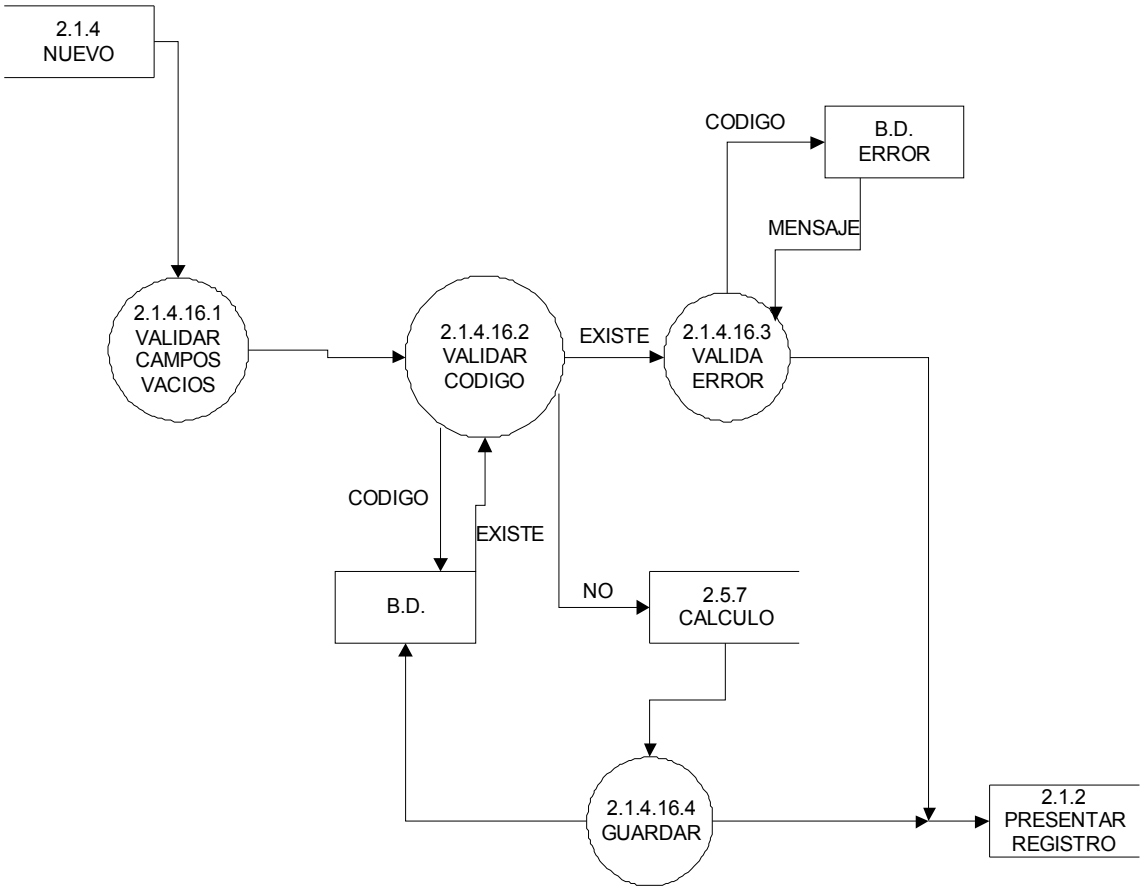


Figura 35. Modelo Explotación de procesos – Nivel 4 Guardar

5.3.3.5 Diagrama de bloques

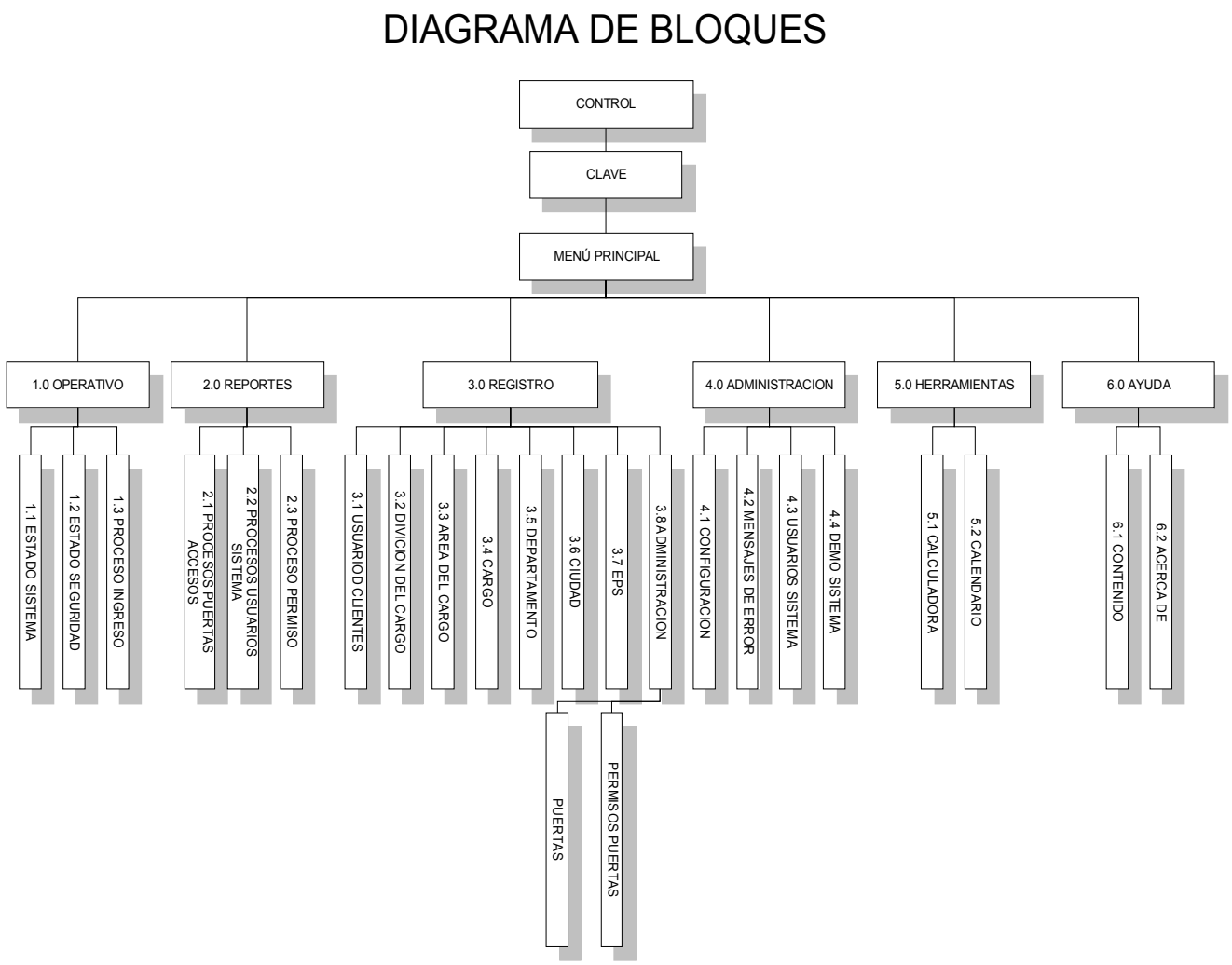


Figura 36. Diagrama de bloques

5.3.5.6 Tabla visual del diagrama de bloques

1.0 Operativo: se manejan las puertas

2.0 Reportes: salidas del sistema

3.0 Registro: Entrada de información a la aplicación

- 3.1 Usuarios Clientes: entrada para los usuarios de las puestas o accesos
- 3.2 División: grupo de trabajo
- 3.3 Área: subgrupo de trabajo
- 3.4 Cargo: labor que desempeña
- 3.5 Departamento
- 3.6 Ciudad
- 3.7 EPS: salud prepagada
- 3.8 Administración: manejo de las puertas o accesos
  - 3.8.1 Permisos: entradas
  - 3.8.2 Puertas: accesos

4.0 Administración: mantenimiento del aplicativo

- 4.1 Configuración: para cambiar los atributos de la configuración del aplicativo
- 4.2 Mensajes de Error: Cambiar los letreros de los mensajes
- 4.3 Usuarios del Sistema: las personas que pueden acceder al aplicativo
- 4.4 Demo Sistema: Demostración de la interfaz del aplicativo con los dispositivos

5.0 Herramientas: opciones extras del aplicativo

- 5.1 Calculadora: calculadora del sistema
- 5.2 Calendario:

6.0 Ayuda: información del aplicativo

- 6.1 Contenido: datos específicos del aplicativo e interfaz
- 6.2 Acerca de: información del desarrollo

7.0 Salir: Sirve para cambiar de sesiones de usuarios o para terminar el aplicativo.

5.3.5.7 Descripción de procedimientos y de formularios

Procedimientos

Prlicam:	Limpia los textos.
Prbot:	Configura los botones.
Prvalva:	Valida si existen campos vacíos.
Prgrafic:	Carga los iconos y los gráficos.
Prmensa:	Mensajes de ayuda en línea.
Prclave:	Carga la clave.
Prcargar:	Carga los cuadros de texto.
Prmovi:	Movimientos o botones de navegación.
Prmen:	Mensajes de error en la base de datos.
Prexi:	Verifica que existan o no en nombre para ver si es repetido.
Prayu:	Cargar la ayuda del programa.
Prmenli:	Mensajes de error en los botones.
Prbous:	Cambia la configuración de los botones de los usuarios.
Prus:	Carga los usuarios y los permisos.
Prestr:	Bloquea los cuadros de texto.
Prlidbc:	Cargar los permisos de los usuarios.
Prpermisos:	Activa las diferentes opciones de permisos.

Funciones

Fuconfig: Configuración de fondo y textos.

Fuval: Validación de caracteres.

Fucote: Configuración de los usuarios en fondo y letra.

Fuconfidbc: Configuración de los combos y dbcombos.

Fucon: Configura los cuatros de texto.

Variables

Pruta: Almacena la ruta donde se encuentra el programa.

Pcon, Pvan, Pva, Pkey: Banderas y contadores.

Pclave: Almacena la clave dada por el usuario.

Pori, Pdes: Para la copia de seguridad.

Pwork: Espacio de trabajo para el insert y demás.

Psql, Peli, Pm, Pme, Pmes: Para valores en consultas.

Losmpt: Para la base de datos en el insert y demás.

Loreco: Para el recordset del insert y demás.

5.3.3.8 Modelo MER de SCAEC

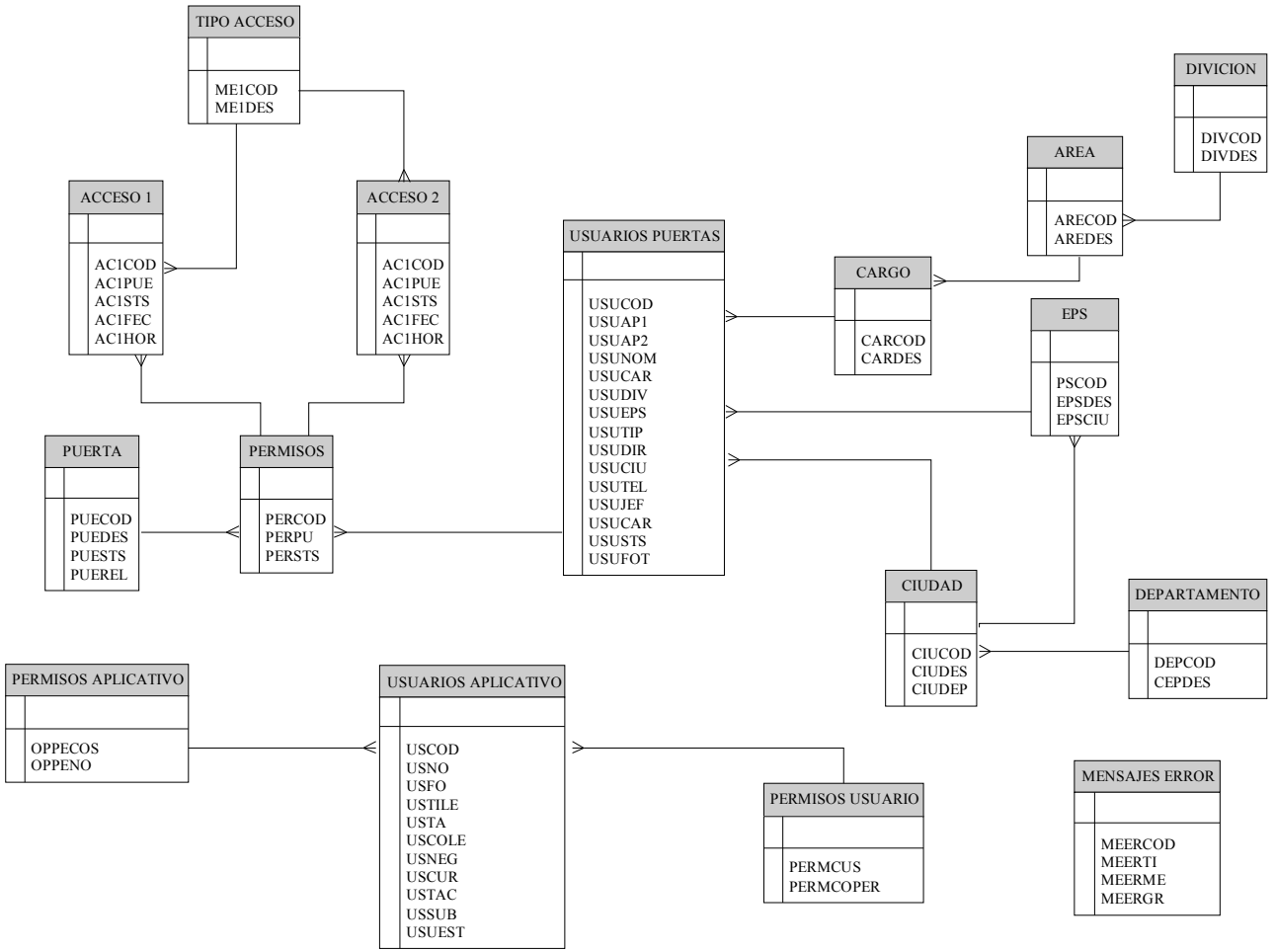


Figura 37. Modelo Entidad Relación SCAEC

5.3.3.9 Diccionario de Datos SCAEC

ENTIDAD: USUARIOS DEL SISTEMA

NEMONICO: ACCUSU
OBJETIVO: TABLA MAESTRA DE USUARIOS DEL SISTEMA
FINALIDAD: CONTIENE LOS DATOS BASICOS DE UN USUARIO DEL SISTEMA AL CUAL SE LE ASIGNA CARNET DE INGRESO.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
USUCOD	Char	Código	Ident. llave primaria consecutivo
USUAP1	Char	Apellido 1	Primer apellido del usuario
USUAP2	Char	Apellido 2	Segundo apellido del usuario
USUNOM	Char	Nombre	Nombre del usuario
USUCAR	Char	Cargo	Indicador cargo del usuario
USUEPS	Char	EPS	Indicador EPS usuario
USUTIP	Char	Tipo de Sangre	Descripción tipo de sangre del usuario
USUDIR	Char	Dirección	Dirección de la vivienda del usuario
USUCIU	Char	Ciudad	Indicador de la ciudad de habitación usuario
USUTEL	Char	Telefono	Número telefónico del usuario
USUJEF	Char	Nombre del Jefe	Nombre del jefe del usuario
USUCAJ	Char	Cargo del Jefe I.	Indicador del cargo del jefe inmediato
USUSTS	Char	Estado del Usu.	Estado del usuario A ó R
USUFOT	Char	Foto Usuario	Número de la foto del usuario

Tabla 15. B.D. - Tabla maestra de usuarios del sistema

ENTIDAD: PUERTAS

NEMONICO: ACCPUE

OBJETIVO: MAESTRO DE PUERTAS Ó ACCESOS QUE TIENE EL SISTEMA

FINALIDAD: CONTIENE LA INFORMACIÓN DE PUERTAS QUE EL SISTEMA ESTARÁ MONITOREANDO.

ATRIBUTOS

Nemónico	**Dato**	**Nombre**	**Observación**
PUECOD	Char	Código	Ident. llave primaria consecutivo
PUEDES	Char	Nom. de la puerta	Descripción de la puerta
PUESTS	Char	Status	Estado de la puerta
PUEREL	Char	Puerta Relación	Indicador de la puerta de acceso

Tabla 16. B.D. - Tabla maestra de accesos del sistema

ENTIDAD: TIPO DE ACCESOS

NEMONICO: ACCMEN

OBJETIVO: TIPO DE ACCESOS A LAS PUERTAS DEL SISTEMA

FINALIDAD: CONTIENE UNA TABLA DE MENSAJES COMO RESPUESTA A UN TIPO DE ACCESO.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
MENCOD	Char	Código	Identificación llave primaria
MENDES	Char	Descripción	Descripción del tipo de acceso

Tabla 17. B.D. - Tabla maestra de tipos de accesos del sistema

ENTIDAD: REGISTRO DE ACCESOS

NEMONICO: ACCAC1

OBJETIVO: TABLA DEL CONTROL DE ACCESOS AL SISTEMA

FINALIDAD: OBJETO DE REGISTRO TEMPORAL DEL PRIMER INGRESO A UNA PUERTA POR PARTE DE UN UUSARIO DEL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
AC1COD	Char	Código	Identificación llave primaria
AC1PUE	Char	Puerta	Identificación llave primaria
AC1STS	Char	Cod. De Acceso	Ind. del tipo de acceso
AC1FEC	Datemine	Fecha	Fecha de ingreso al sistema
AC1HOR	Datemine	Hora	Hora de ingreso al sistema

Tabla 18. B.D. - Tabla maestra de control de accesos del sistema

ENTIDAD: REGISTRO DE ACCESOS HISTORIA

NEMONICO: ACCAC2

OBJETIVO: TABLA DEL CONTROL DE ACCESOS AL SISTEMA HISTORIA

FINALIDAD: OBJETO DONDE QUEDAN REGISTRADOS TODOS LOS MOVIMIENTOS DE ACCESO AL SISTEMA, BLOQUEOS Ó HABILITACIONES POR PARTE DE LOS ADMINISTRADORES DEL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
AC2COD	Char	Código	Identificación llave primaria
AC2PUE	Char	Puerta	Identificación llave primaria
AC2STS	Char	Cod. De Acceso	Ind. del tipo de acceso
AC2FEC	Datemine	Fecha	Fecha de ingreso al sistema
AC2HOR	Datemine	Hora	Hora de ingreso al sistema

Tabla 19. B.D. - Tabla maestra de registro de accesos historia

ENTIDAD: TIPO DE ACCESOS

NEMONICO: ACCME1

OBJETIVO: MAESTRO DEL TIPO DE CONTROL DE ACCESOS AL SISTEMA

FINALIDAD: OBJETO DE MENSAJES DE RESPUESTA A LA VALIDACION DE UN INGRESO AL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
ME1COD	Char	Código	Identificación llave primaria
ME1DES	Char	Descripción	Descripción del tipo de acceso

Tabla 20. B.D. - Tabla maestra de tipo de control de accesos

ENTIDAD: TIPO DE CARGOS

NEMONICO: ACCCAR

OBJETIVO: MAESTRO DEL TIPO DE CARGOS DE USUARIOS

FINALIDAD: OBTETO CON LA DESCRIPCIÓN DE LOS TIPOS DE CARGOS EXISTENTES EN LA COMPAÑÍA DONDE SE INSTALARÁ EL SOFTWARE.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
CARCOD	Char	Código	Identificación llave primaria
CARDES	Char	Descripción	Descripción del tipo de cargo

Tabla 21. B.D. - Tabla maestra de tipo de cargos

ENTIDAD: TIPO DE AREA

NEMONICO: ACCARE

OBJETIVO: MAESTRO DEL TIPO AREAS DE LA EMPRESA

FINALIDAD: OBTETO CON LA DESCRIPCIÓN DE LAS AREAS DE GESTION DE UNA EMPRESA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
ARECOD	Char	Código	Identificación llave primaria
AREDES	Char	Descripción	Descripción del tipo de cargos

Tabla 21. B.D. - Tabla maestra de tipo de áreas

ENTIDAD: TIPO DE DIVISION

NEMONICO: ACCDIV

OBJETIVO: MAESTRO DEL TIPO DE DIVISIONES DEL SISTEMA

FINALIDAD: OBTETO CON LA DESCRIPCIÓN DE LOS TIPOS DE DIRECCIONES QUE CONFORMA LA EMPRESA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
DIVCOD	Char	Código	Identificación llave primaria
DIVDES	Char	Descripción	Descripción del tipo de acceso

Tabla 22. B.D. - Tabla maestra de tipo de divisiones

ENTIDAD: TIPO DE EPS

NEMONICO: ACCEPS

OBJETIVO: MAESTRO DEL TIPO DE EPS

FINALIDAD: OBTETO CON LA DESCRIPCIÓN DE LAS DIFERENTES EPS A LAS CUALES HACEN PARTE LOS USUARIOS DEL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
epsCOD	Char	Código	Identificación llave primaria
epsDES	Char	Descripción	Descripción del tipo de EPS
epsCIU	Char	Ciudad	Indentificador de la ciudad

Tabla 23. B.D. - Tabla maestra de tipo de E.P.S.

ENTIDAD: TIPO DE PERMISOS

NEMONICO: ACCPER

OBJETIVO: MAESTRO DEL TIPO DE PERMISOS PARA LOS USUARIOS

FINALIDAD: OBTETO CON LA INFORMACIÓN DE ACCESOS PERMITIDOS QUE PUEDE TENER UN USUARIO DEL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
perCOD	Char	Código	Identificación llave primaria
perpu	Char	Puerta	Identificación llave primaria
persts	Char	Status permiso	Status de permisos

Tabla 24. B.D. - Tabla maestra de tipo de permisos usuarios

ENTIDAD: MAESTRO DE CIUDADES

NEMONICO: ACCCIU

OBJETIVO: MAESTRO DE CIUDADES

FINALIDAD: OBTETO CON LA DESCRIPCIÓN DE LAS DIFERENTES CIUDADES CAPITAL DEL PAÍS.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
CIUCOD	Char	Código	Identificación llave primaria
CIUDES	Char	Descripción	Descripción de la ciudad
CIUDEP	Char	Ciudad	Indentificador ciudad

Tabla 25. B.D. - Tabla maestra de tipo de ciudades

ENTIDAD: MAESTRO DE DEPARTAMENTOS

NEMONICO: ACCDEP

OBJETIVO: MAESTRO DE DEPARTAMENTOS DEL PAIS

FINALIDAD: OBTETO CON LA DESCRIPCIÓN DE LOS DIFERENTES DEPARTAMENTOS DEL PAÍS.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
DEPCOD	Char	Código	Identificación llave primaria
DEPDES	Char	Descripción	Nombre del departamento

Tabla 26. B.D. - Tabla maestra de tipo de departamentos

ENTIDAD: USUARIOS DEL APLICATIVO

NEMONICO: US

OBJETIVO: TABLA MAESTRA DE USUARIOS DEL APLICATIVO

FINALIDAD: OBTETO CON LOS DATOS BÁSICOS DE LOS USUARIOS DE CONTROL DEL SOFTWARE DEL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
USCOD	Char	Código	Ident. llave primaria consecutivo
USNO	Char	Nombre	Nombre de Usuario
USFO	Num	Fondo	Color de fondo
USTILE	Char	Tipo de Letra	Tipo de Letra
USTA	Char	Tamaño	Tamaño de Letra
USCOLE	Num	Color Letra	Color de la Letra
USNEG	Char	Negrita	Negrita
USCUR	Char	Cursiva	Cursiva
USTAC	Char	Tachado	Tachado de Letra
USUSUB	Char	Subrayado	Subrayado de la Letra

Tabla 27. B.D. - Tabla maestra de usuarios aplicativo

ENTIDAD: PERMISOS DE APLICATIVO

NEMONICO: OPPE

OBJETIVO: TIPO DE PERMISO

FINALIDAD: OBTETO CON LOS DIFERENTES TIPOS DE PERMISOS QUE PUEDE TENER UN USUARIO DECONTROL DEL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
OPPECOD	Char	Código	Identificación llave primaria
OPPENO	Char	Descripción	Nombre del permiso

Tabla 28. B.D. - Tabla maestra de tipo de permisos

ENTIDAD: PERMISOS PARA ENTRADA AL APLICATIVO

NEMONICO: PERM

OBJETIVO: PERMISOS DE CADA OPCION DEL APLICATIVO

FINALIDAD: OBTETO CON LA ASIGNACIÓN DE PERMISOS QUE TIENE UN USUARIO DE CONTROL.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
PERMCUS	Char	Código	Identificación llave primaria
PERMCOPER	Char	Descripción	Nombre del permiso

Tabla 29. B.D. - Tabla maestra de permisos menús

ENTIDAD: MENSAJES DE ERRORES DEL APLICATIVO

NEMONICO: MEER

OBJETIVO: MENSAJES INFORMATIVOS DEL APLICATIVO

FINALIDAD: OBTETO CON LOS DIFERENTES MENSAJES DE EERROR QUE SE PUEDEN PRESENTAR EN LA GESTION DEL SISTEMA.

ATRIBUTOS

Nemónico	Dato	Nombre	Observación
MEERCOD	Char	Código	Identificación llave primaria
MEERTI	Char	Descripción	Nombre del mensaje
MEERME	Char	Mensaje	Mensaje a mostrar
MEERGR	Char	Icono	Icono mostrado

Tabla 30. B.D. - Tabla maestra de mensajes del sistema

5.3.3.10 Estándares

El Software se guarda en una carpeta llamada (SCAEC), se divide en subcarpetas que tienen los siguientes nombres:

Formularios: Contiene todas las ventanas del programa.

Instalación: Almacena los archivos para la instalación del programa.

Manuales: Tienen los textos que sirven como información del programa.

Módulos: Contiene los procesos y funciones del programa

Proyecto: Almacena los gráficos, los reportes, la base de datos, la ayuda y los ejecutables del proyecto.

Los nombre de los reportes se reconocen por sus dos primeras letras (re), y luego el tipo de reporte con las iniciales del mismo, los gráficos principales tienen el nombre que los identifica, la ayuda tiene el nombre "ayuda".

La base de datos se llama (SCAEC), y las tablas tendrán las iniciales del nombre que la identifica en el MER, las tablas tienen las iniciales del nombre que las identifica en el modelo entidad relación.

Los iconos y gráficos tienen un nombre descriptivo.

Las variables se identificaran con (gl) globales, (lo) locales, con un nombre o iniciales descriptivas de la función que cumple. Las constantes cumplirán los mismos estándares con la adición de las letras (co).

Todos los reportes tienen en la parte superior izquierda el logo presentado en la figura 38 y la fecha se que fuera realizado dicho reporte por el usuario.

5.3.3.11 Estándares de pantallas

Logo de insignia de SCAES

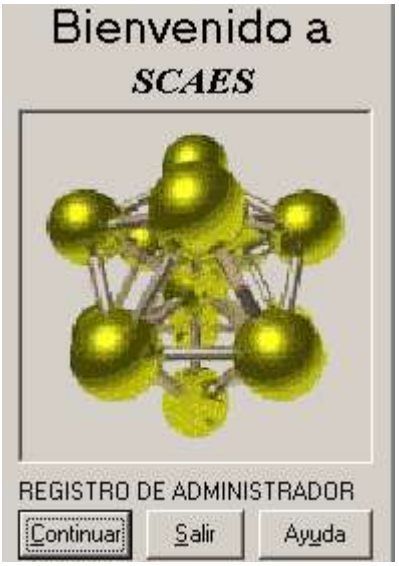


Figura 38. Estándares de pantallas - Logo insignia de Scaes

Pantalla para el ingreso al sistema

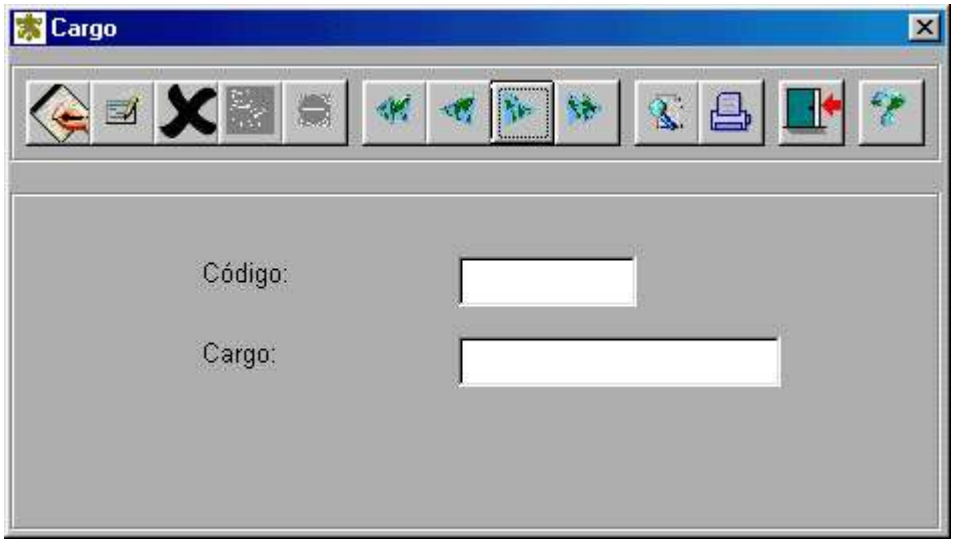


Figura 39. Estándares de pantallas - Ingreso al sistema

Pantalla de la Ventana Principal

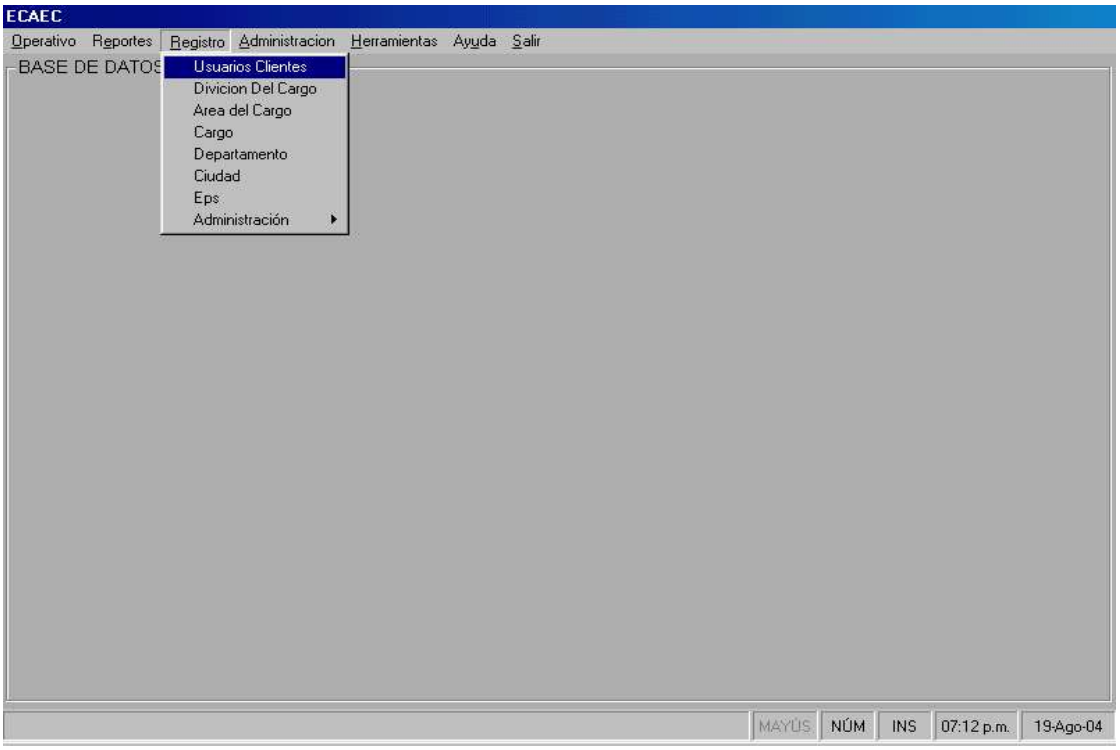


Figura 40. Estándares de pantallas - Pantalla menú principal

Pantalla de la Ventana de Usuarios

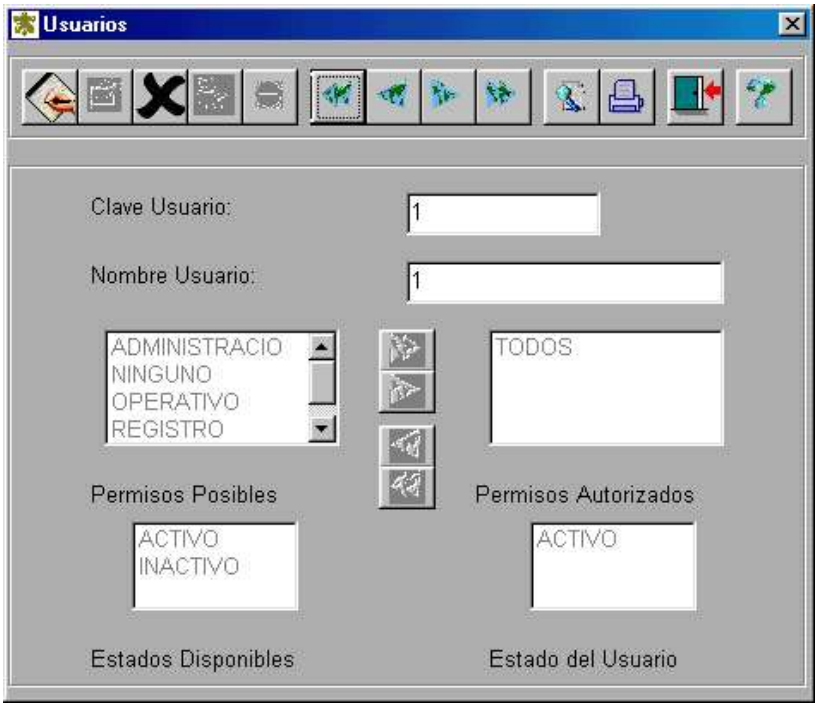


Figura 41. Estándares de pantallas - Control de usuarios

5.3.3.12 Diagrama de procesos intercambios del sistema

- Diagrama de flujo del estado del sistema

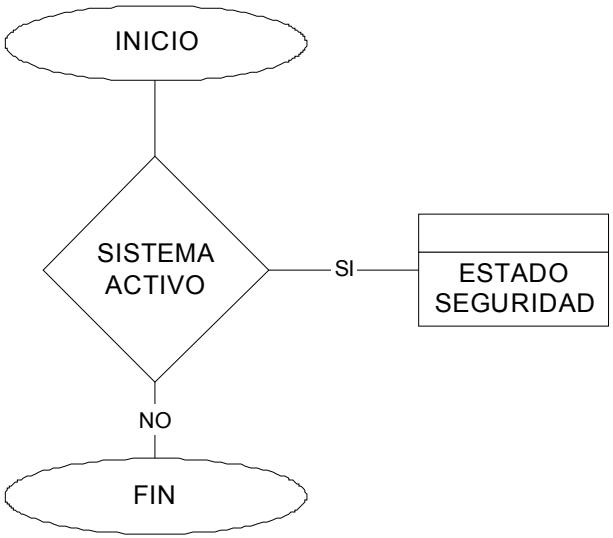


Figura 42. Procesos de intercambio del sistema – Flujo de estado

- Diagrama de Flujo del proceso de seguridad del sistema

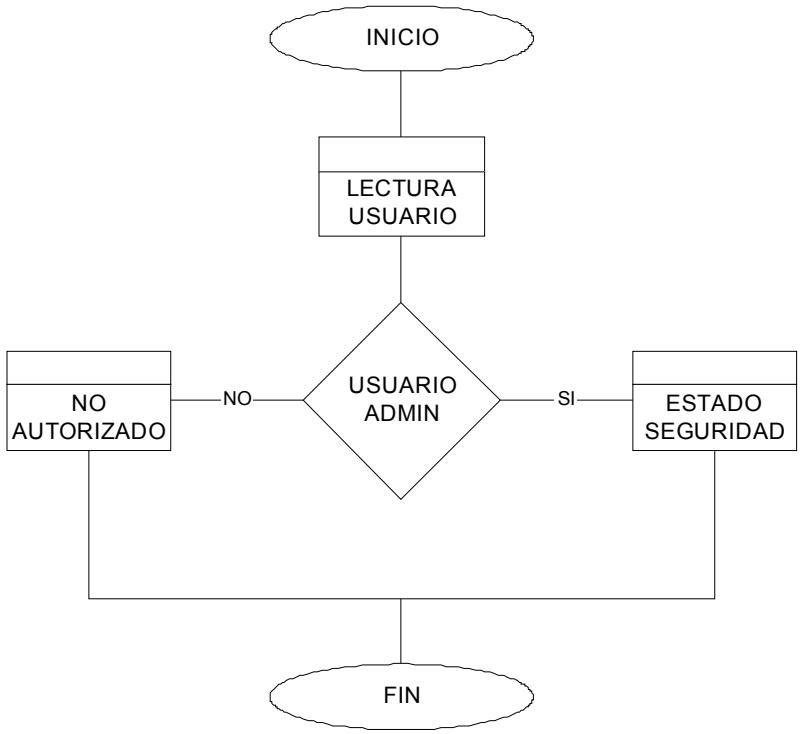


Figura 43. Procesos de intercambio del sistema – Seguridad

- Diagrama de flujo del proceso de ingreso al sistema

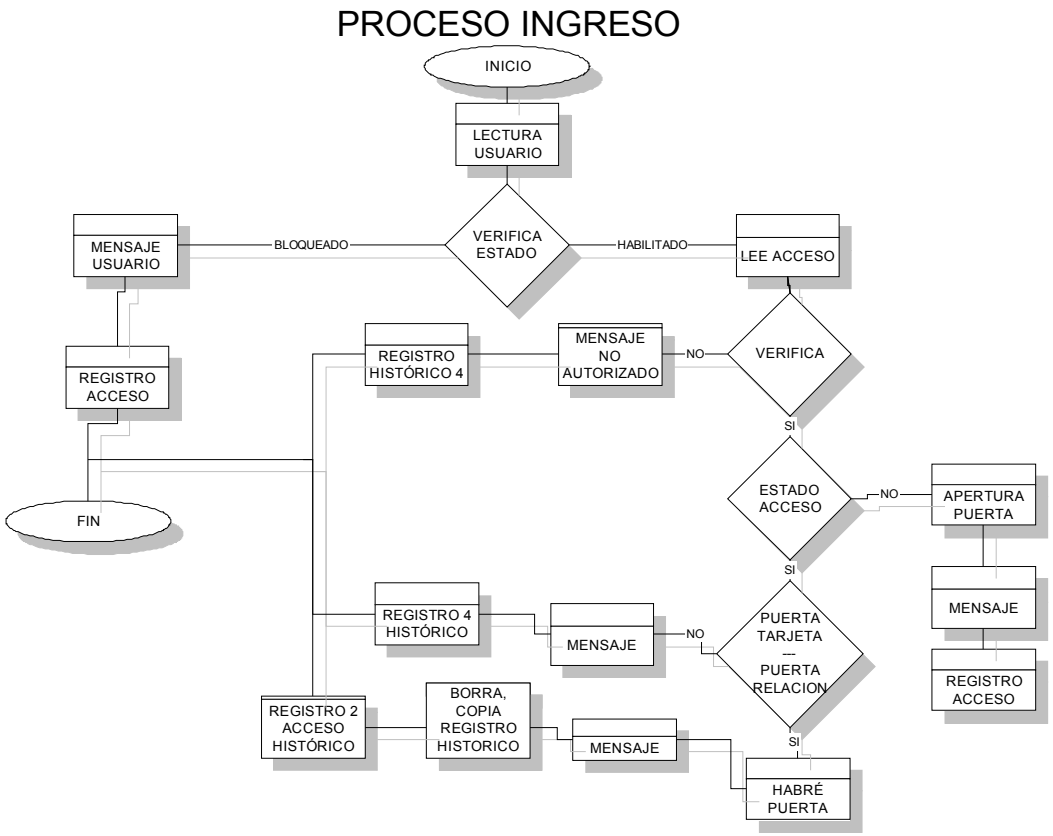


Figura 44. Procesos de intercambio del sistema – Ingreso al sistema

- Diagrama flujo del proceso de acceso a las puertas

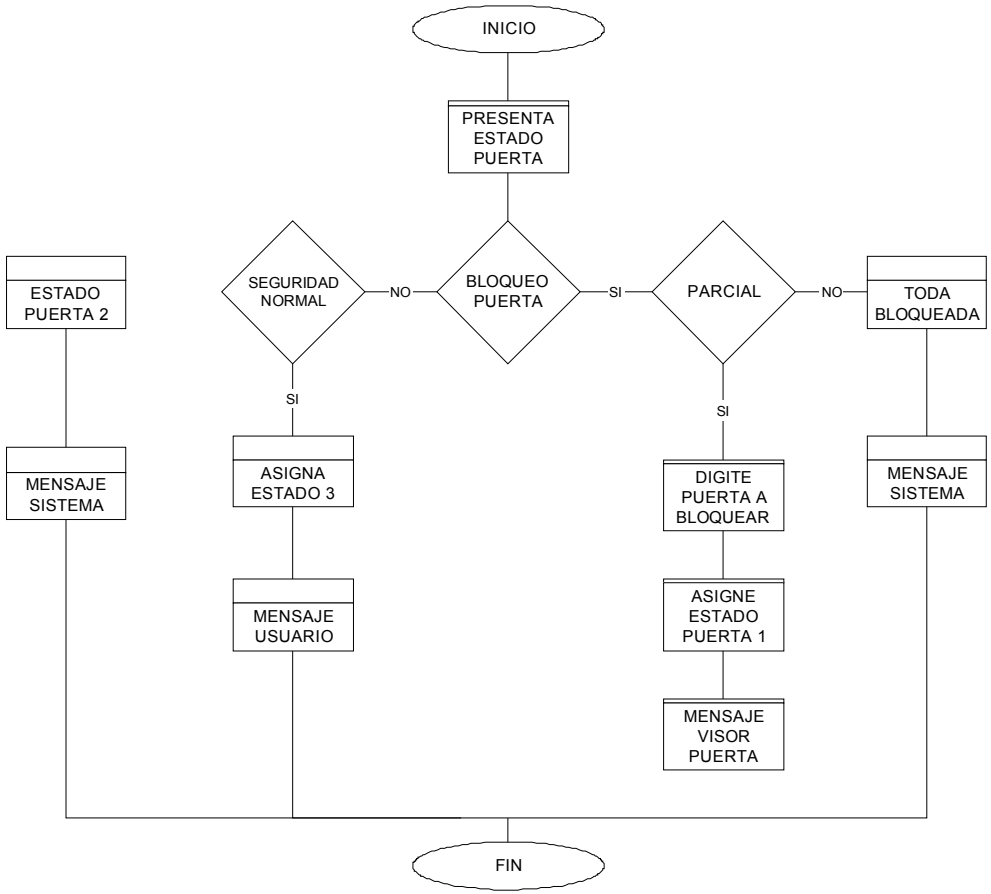


Figura 45. Procesos de intercambio del sistema – Acceso de puertas

5.3.3.13 Diseño lógico de la interfase electrónica

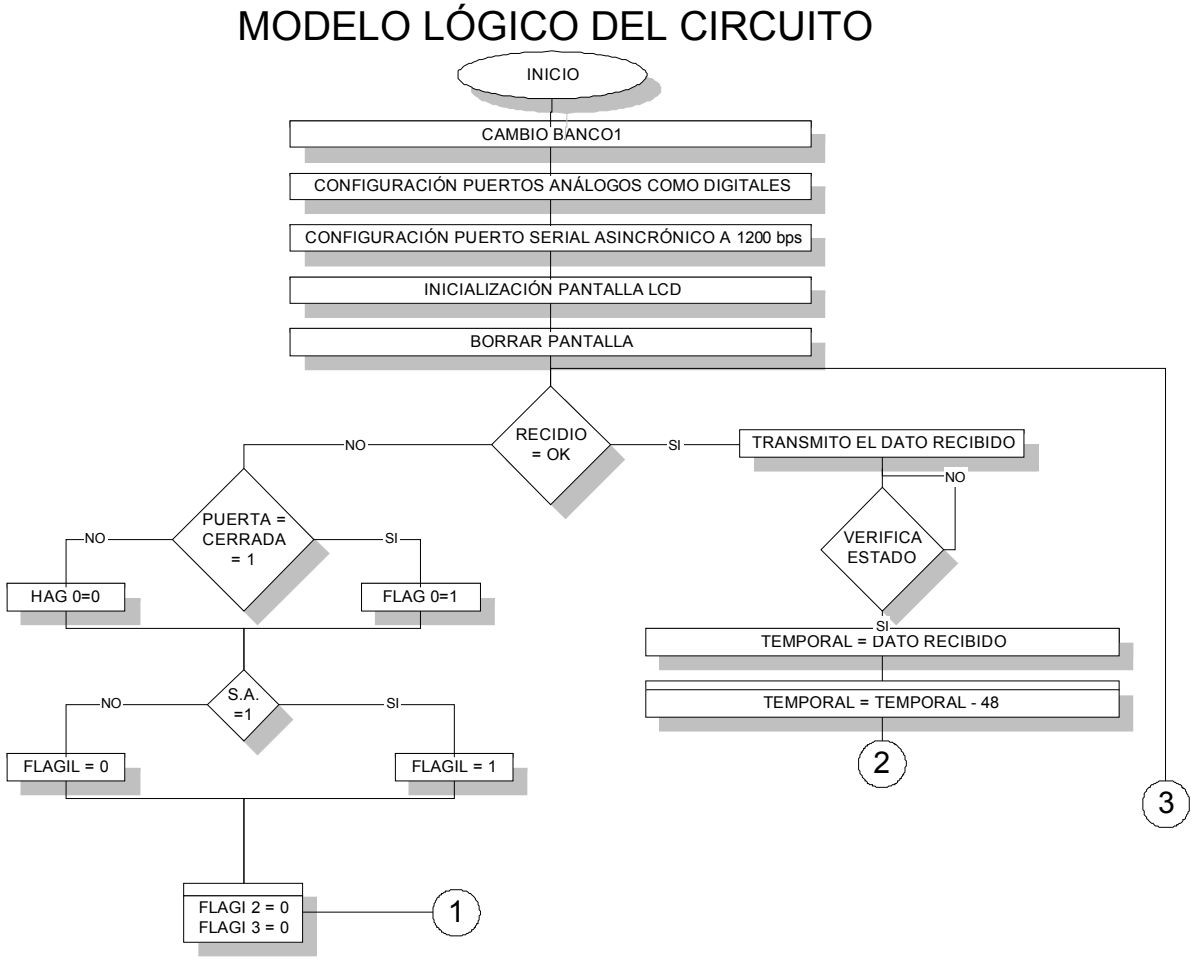


Figura 46. Diseño lógico de la interfase electrónica parte 1

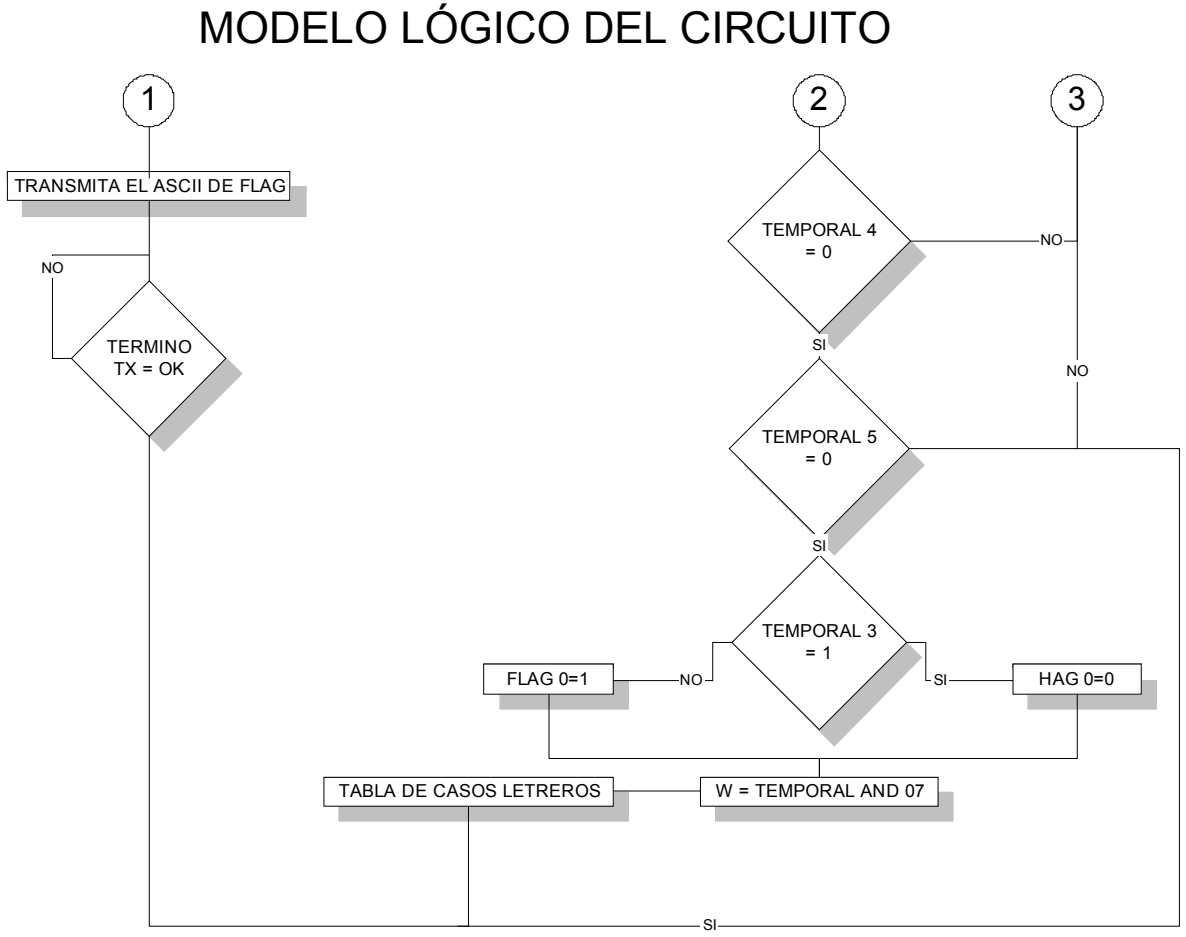


Figura 47. Diseño lógico de la interfase electrónica parte 2

5.3.3.14 Diseño circuito electrónico de la interfase electrónica

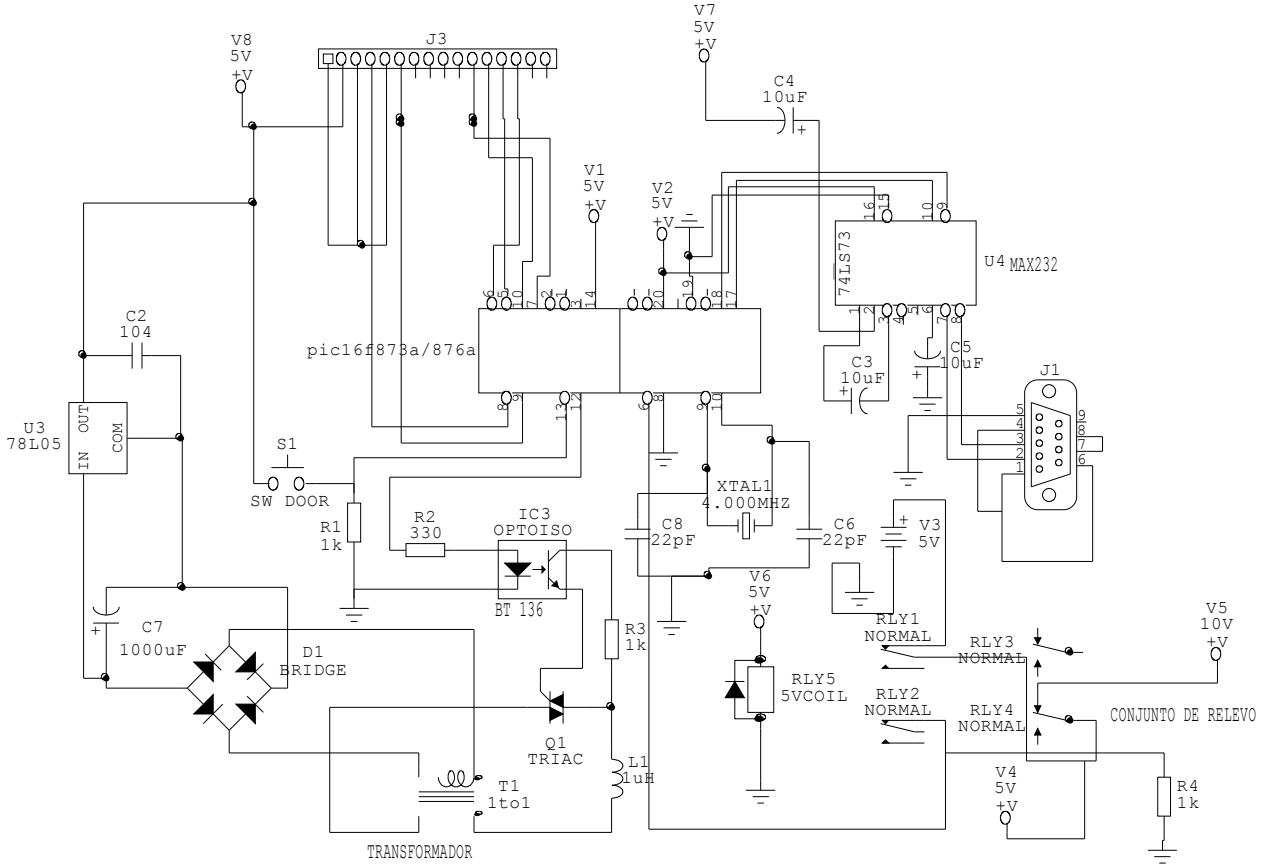
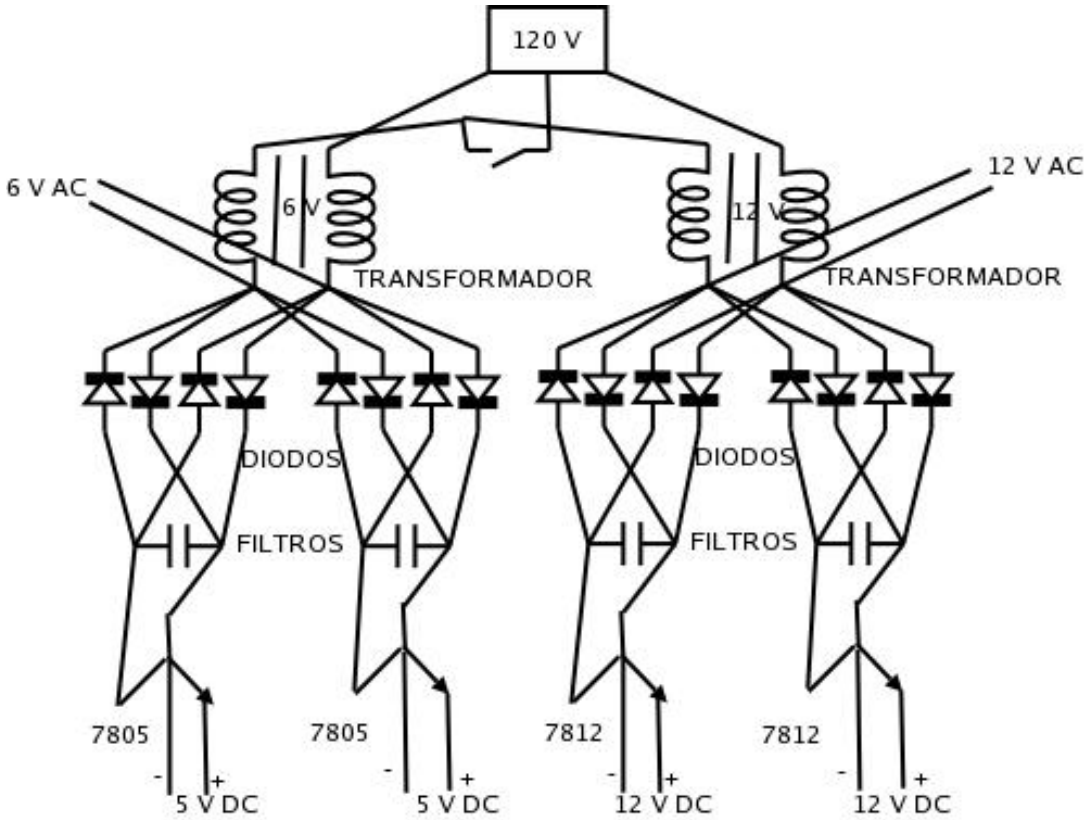


Figura 48.

Diseño circuito electrónico de la interfase electrónica

5.3.3.15 Descripción de los elementos electrónicos

Diagrama de la fuente de poder



BT136

GENERAL DESCRIPTION

Passivated triacs in a plastic envelope, intended for use in applications requiring high bidirectional transient and blocking voltage capability and high thermal cycling performance. Typical applications include motor control, industrial and domestic lighting, heating and static switching.

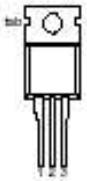
QUICK REFERENCE DATA

SYMBOL	PARAMETER	MAX.	UNIT
	BT136- BT136-	600 600F	
V_{DRM}	Repetitive peak off-state voltages	600	V
$I_{T(RMS)}$	RMS on-state current	4	A
I_{TSM}	Non-repetitive peak on-state current	25	A

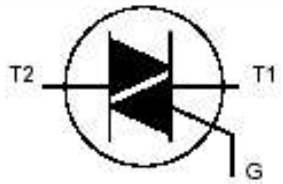
PINNING - TO220AB

PIN	DESCRIPTION
1	main terminal 1
2	main terminal 2
3	gate
tab	main terminal 2

PIN CONFIGURATION



SYMBOL



LIMITING VALUES

Limiting values in accordance with the Absolute Maximum System (IEC 134).

SYMBOL	PARAMETER	CONDITIONS	MIN.	MAX.	UNIT
V_{DRM}	Repetitive peak off-state voltages		-	600[1]	V
$I_{T(RMS)}$	RMS on-state current	full sine wave; $T_{mb} \leq 107$ °C	-	4	A
I_{TSM}	Non-repetitive peak on-state current	full sine wave; $T_j = 25$ °C prior to surge			
		t = 20 ms	-	25	A
		t = 16.7 ms	-	27	A
I^2t	I^2t for fusing	t = 10 ms	-	3.1	A^2s
dI_T/dt	Repetitive rate of rise of on-state current after triggering	$I_{TM} = 6$ A; $I_G = 0.2$ A; $dI_G/dt = 0.2$ A/µs			
		T2+ G+	-	50	A/µs
		T2+ G-	-	50	A/µs
		T2- G-	-	50	A/µs
		T2- G+	-	10	A/µs
I_{GM}	Peak gate current		-	2	A
V_{GM}	Peak gate voltage		-	5	V
P_{GM}	Peak gate power		-	5	W
$P_{G(AV)}$	Average gate power	over any 20 ms period	-	0.5	W
T_{stg}	Storage temperature		-40	150	°C
T_j	Operating junction temperature		-	125	°C

1 Although not recommended, off-state voltages up to 800V may be applied without damage, but the triac may switch to the on-state. The rate of rise of current should not exceed 3 A/µs.

Tabla 31. Descripción técnica del BT136 parte 1

MECHANICAL DATA

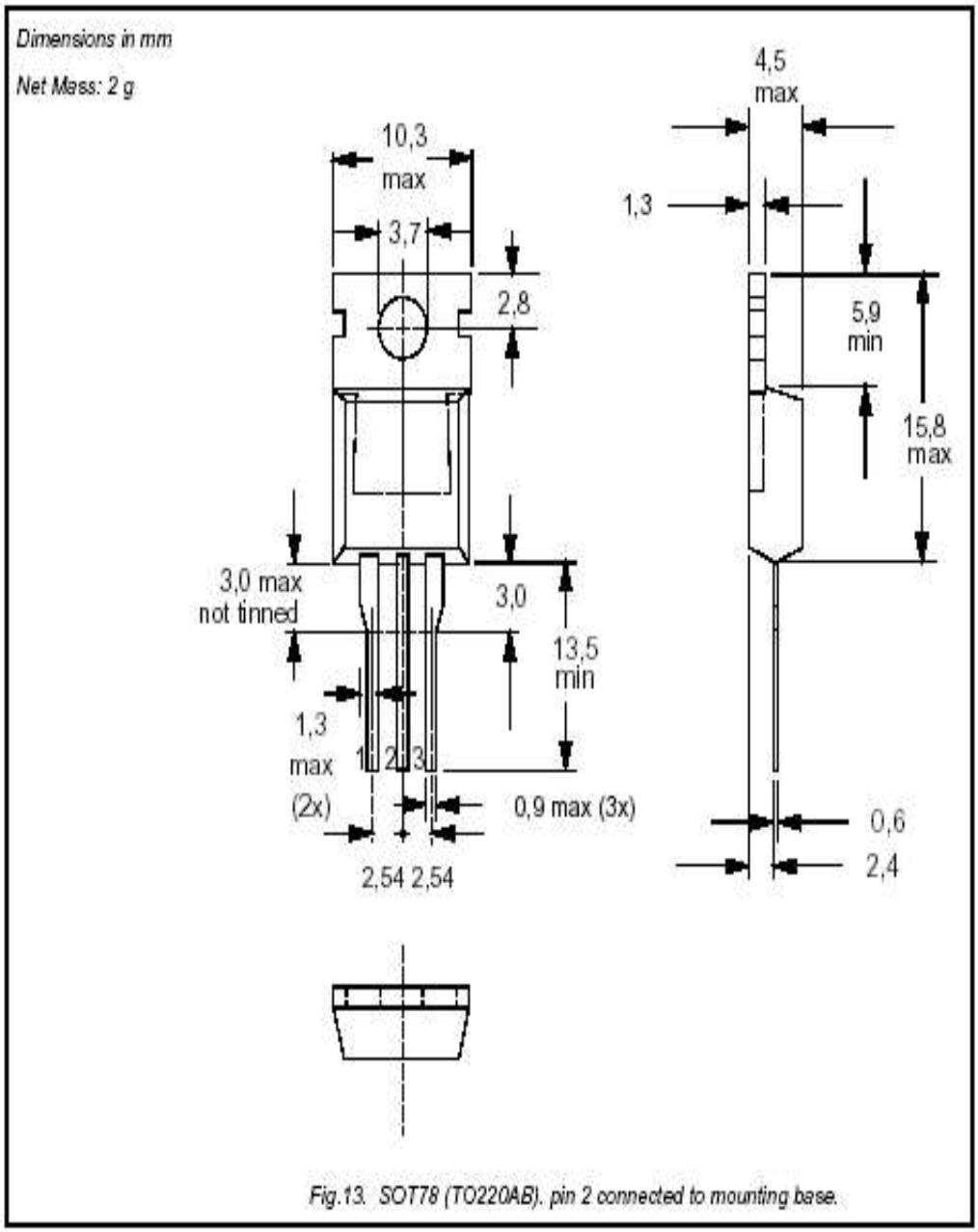


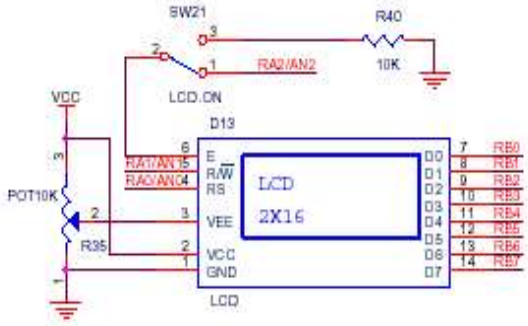
Fig.13. SOT78 (TO220AB). pin 2 connected to mounting base.

Notes
1. Refer to mounting instructions for SOT78 (TO220) envelopes.
2. Epoxy meets UL94 V0 at 1/8".

Tabla 32. Descripción técnica del BT136 parte 2

Display LCD

El esquema correspondiente al circuito de este display se encuentra en la siguiente figura:



Los displays LCD son mayoritariamente estándar y se controlan de formas muy parecidas, incluso cuando no coincide el número de caracteres. En la figura podemos ver los elementos básicos de un display LCD estándar. Por un lado se tiene el bus de datos D0..D7 que en este caso está conectado al puerto B del PIC. Este bus de datos puede ser de entrada al LCD (para escribir caracteres y enviar instrucciones) o puede ser de salida del LCD (para poder leer el estado por ejemplo). El LCD tiene tres señales de control: E es la de habilitación y está conectada al bit 2 del puerto A del PIC, sirve para habilitar el LCD y como vemos está conectada a un interruptor para deshabilitar permanentemente el LCD; la señal R/W sirve para indicar operación de lectura o escritura; por último se la señal RS es la de sincronismo de datos e instrucciones y está conectada al bit 1 del puerto A. Además el LCD tiene señales para alimentación y una señal (VEE) que sirve para controlar el contraste de la pantalla.

Para simplificar las operaciones de escritura y control en el LCD, se provee un fichero (`lcd.h`) disponible en la página web de la asignatura. Este fichero contiene varias rutinas muy útiles entre las que destacan las siguientes:

- `LCD_Prepara()` Esta rutina prepara los puertos A y B de forma adecuada y pone las señales de control en un estado de preparado.
- `LCD_Ini()` Esta rutina envía al LCD la secuencia de inicialización. Esta rutina es necesaria al encender el LCD y debe venir siempre después de la rutina anterior.
- `LCD_Comando(char)` Esta rutina permite enviar cualquier comando o instrucción al LCD. Hay numerosas instrucciones, todas ellas se pueden consultar en el manual del LCD que se puede encontrar en la página web de la asignatura. Por ejemplo, la instrucción `LCD_Comando(00111100b)` indica que el bus de datos es de 8 bits, que se van a utilizar las 2 líneas del LCD con una fuente 5x10. La instrucción

Tabla 33. Descripción técnica del Display LCD parte 1

`LCD_Comando(00001110b)` enciende el LCD para que se vea, enciende el cursor y le dice que no parpadee. Estas dos instrucciones, o algunas parecidas, son necesarias para que aparezca por el LCD lo que se vaya escribiendo.

- `LCD_Dato(char)` Si todo se ha iniciado bien, esta instrucción muestra por pantalla el carácter que se le pase en la posición actual del cursor.

En principio basta con estas cuatro funciones para operar con el LCD. Es bastante aconsejable tener cerca el manual del LCD para ver los comandos de control, ya que son muy útiles. Estos comandos permiten apagar y encender la pantalla, mostrar el cursor, llevar el cursor a una determinada posición, limpiar la pantalla, etc.

Es importante que los conmutadores de la placa EduPIC que sirven para elegir Analógico o Digital estén en su posición central (LIBRE) de esta manera los periféricos no interfieren con la operación sobre los bits RA0, RA1 y RA2 que son los que utiliza el LCD. Como el RA3 se utiliza en la práctica de hoy como entrada digital, deberá ponerse a la derecha (DIGITAL).

Tabla 34. Descripción técnica del Display LCD parte 2

MOC3010

El MOC301XM y la serie MOC302XM aíslan óptimamente los dispositivos de conductor de triac. Estos dispositivos contienen un GaAs que emite un diodo infrarrojo y una luz activa de silicio como interruptor bilateral, que funciona como un triac. Ellos son diseñados para comunicar señales electrónicas y poder de controlar resistencias y cargas inductivas para 115 operaciones de VAC.

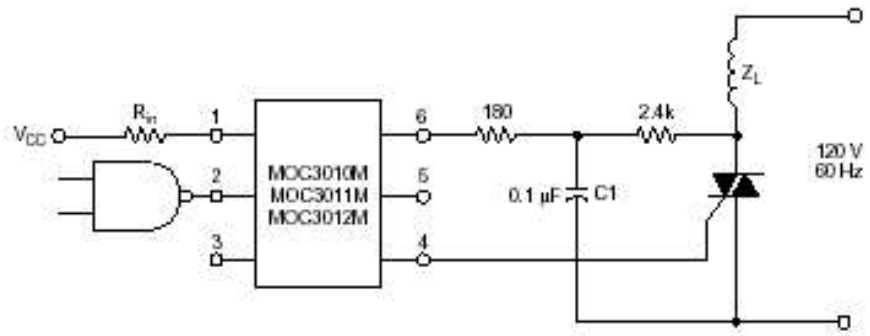


Figure 7. Inductive Load with Sensitive Gate Triac ($I_{GT} \leq 15$ mA)

DESCRIPTION

The MOC301XM and MOC302XM series are optically isolated triac driver devices. These devices contain a AlGaAs infrared emitting diode and a light activated silicon bilateral switch, which functions like a triac. They are designed for interfacing between electronic controls and power triacs to control resistive and inductive loads for 115/240 VAC operations.

FEATURES

- Excellent I_{FT} stability—IR emitting diode has low degradation
- High isolation voltage—minimum 5300 VAC RMS
- Underwriters Laboratory (UL) recognized—File #E90700
- Peak blocking voltage
  - -250V-MOC301XM
  - -400V-MOC302XM
- VDE recognized (File #94766)
  - -Ordering option V (e.g. MOC3023VM)

APPLICATIONS

- European applications for Triac driver 240 VAC (MOC302X only)
- Industrial controls
- Traffic lights
- Vending machines
- Solid state relay
- Lamp ballasts
- Solenoid/valve controls
- Static AC power switch
- Incandescent lamp dimmers
- Motor control

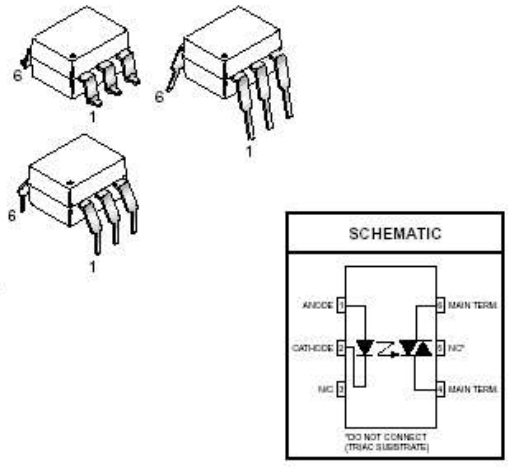


Tabla 35. Descripción técnica del MOC3010

PIC 16F873 A

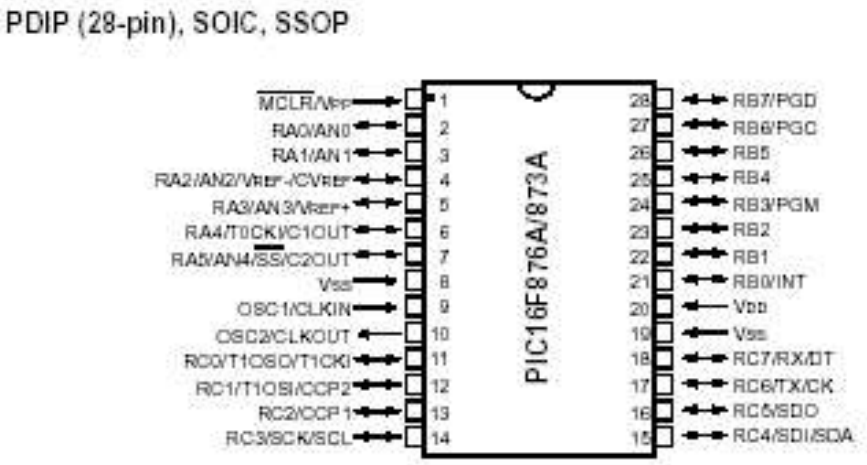


Figura 49. Descripción de pines PIC 16F873 A

Un Micro controlador es un circuito integrado o mas comúnmente llamado chip, que cumple las funciones de cerebro de cualquier aplicación, que puede ser desde encender un led hasta telecontrol y es responsable de la buena funcionalidad del circuito que gobierna. Como todo cerebro, este chip tiene que procesar alguna información que tiene en su memoria y de esta maneta decidir que hacer. A esta información que debe tener el chip se le llama software o programa de aplicación.

Todo el funcionamiento interno del PIC se trata de manejo y configuración de bits de archivos. Estos archivos se encuentran implementados en la memoria RAM y cada uno tiene una longitud de 8 bits, cada BIT de cada archivo cumple una función, por esta razón a estos archivos que ocupan las primeras posiciones de la memoria RAM se les llama Registros de función específica o SFR (Special Function Register).

También existen posiciones de la memoria RAM que no están ocupados por los SFR, y nos sirven para implementar nuestros propios registros, por esto se les llama Registros de propósito general GPR (General Purpose Register).

Microchip Technology Inc. Ha ampliado su familia de microcontroladores Flash de 8 bits PIC16F87X con el PIC16F873 de 28 pines y el PIC16F874 de 40 pines, que ofrecen diversas opciones de memoria para aumentar el rendimiento de los sistemas y la flexibilidad de su diseño.

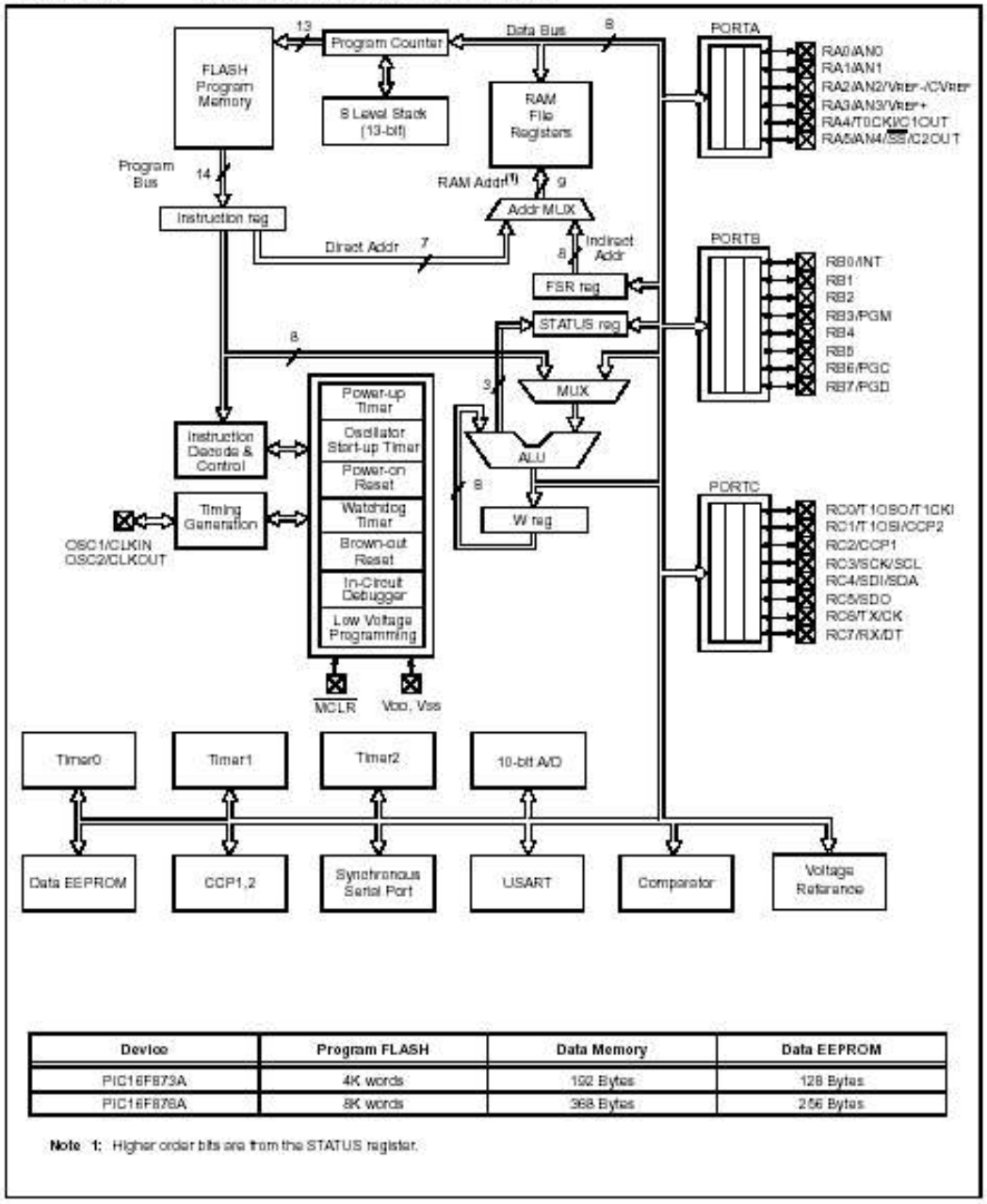
Con 4 K x 14 bits de memoria Flash y 128 bytes de memoria de datos EEPROM, el PIC16F873 y el PIC16F874 se caracterizan por un intervalo de tensión de funcionamiento entre 2,0 y 5,5 V, lo que les hace muy adecuados para aplicaciones alimentadas por batería. Estos dispositivos también proporcionan un convertidor A/D de 5 a 8 canales de 10 bits (± 1 BIT menos significativo), una USART para aplicaciones de adquisición de datos multipunto, un rendimiento de hasta 5 MIPS a 20 MHZ, una capacidad de comunicaciones I2C™ o SPI™, dos temporizadores de 8 bits y uno de 16 bits.

Las interfaces de sincronización de precisión se regulan mediante dos módulos CCP: Captura, de una precisión máxima de 12,5 nanosegundos con la resolución de 16 bits, Comparación, de una precisión máxima de 200 nanosegundos con la resolución de 16 bits y modulación de ancho de Pulso con una resolución de ciclo de carga de 10 bits a una frecuencia de 20 kHz. La tecnología Flash de Microchip tiene la mayor duración del mercado, con 1.000 ciclos de borrado y escritura para memoria de programa y 100.000 ciclos de borrado y escritura para memoria de datos EEPROM.

Los microcontroladores flash PICmicro y los microcontroladores One-Time-Programmable de Microchip se caracterizan por su capacidad In-Circuit Serial Programming™, que permite programarles después de su montaje en un circuito impreso. Esta capacidad ICSP™ también reduce el coste de actualización y hace posible la calibración del sistema durante la fabricación y la inclusión de los códigos de identificación. El PIC16F87X también permite la auto programación a baja tensión, con lo que el usuario puede programar el dispositivo en circuito a la tensión de funcionamiento

que esté empleando. Estas utilidades de programación sólo exigen dos pines I/O para la mayoría de los dispositivos.

FIGURE 1-1: PIC16F873A/876A BLOCK DIAGRAM



Device	Program FLASH	Data Memory	Data EEPROM
PIC16F873A	4K words	192 Bytes	128 Bytes
PIC16F876A	8K words	368 Bytes	256 Bytes

Note 1: Higher order bits are from the STATUS register.

Figura 50. Descripción en diagrama de bloques del PIC 16F873 A

TABLE 1-2: PIC16F873A/876A PINOUT DESCRIPTION

Pin Name	Pin#	I/O/P Type	Buffer Type	Description
OSC1/CLKI	9		ST/CMOS(3)	Oscillator crystal or external clock input.
OSC1		I		Oscillator crystal input or external clock source input. ST buffer when configured in RC mode. Otherwise CMOS.
CLKI		I		External clock source input. Always associated with pin function OSC1 (see OSC1/CLKI, OSC2/CLKO pins).
OSC2/CLKO	10		—	Oscillator crystal or clock output.
OSC2		O		Oscillator crystal output. Connects to crystal or resonator in Crystal Oscillator mode.
CLKO		O		In RC mode, OSC2 pin outputs CLKO, which has 1/4 the frequency of OSC1 and denotes the instruction cycle rate.
$\overline{MCLR}$/VPP	1		ST	Master Clear (Input) or programming voltage (output)
$\overline{MCLR}$		I		Master Clear (Reset) input. This pin is an active low RESET to the device.
VPP		P		Programming voltage input.
				PORTA is a bi-directional I/O port.
RA0/AN0	2		TTL	
RA0		I/O		Digital I/O.
AN0		I		Analog input 0.
RA1/AN1	3		TTL	
RA1		I/O		Digital I/O.
AN1		I		Analog input 1.
RA2/AN2/VREF-/CVREF	4		TTL	
RA2		I/O		Digital I/O.
AN2		I		Analog input 2.
VREF-		I		A/D reference voltage (Low) input.
CVREF		O		Comparator VREF output.
RA3/AN3/VREF+	5		TTL	
RA3		I/O		Digital I/O.
AN3		I		Analog input 3.
VREF+		I		A/D reference voltage (High) input.
RA4/T0CKI/C1OUT	6		ST	
RA4		I/O		Digital I/O – Open drain when configured as output.
T0CKI		I		Timer0 external clock input.
C1OUT		O		Comparator 1 output.
RA5/$\overline{SS}$/AN4/C2OUT	7		TTL	
RA5		I/O		Digital I/O.
$\overline{SS}$		I		SPI slave select input.
AN4		I		Analog input 4.
C2OUT		O		Comparator 2 output.

Legend: I = input O = output I/O = input/output P = power
— = Not used TTL = TTL input ST = Schmitt Trigger input

Note 1: This buffer is a Schmitt Trigger input when configured as the external interrupt.
2: This buffer is a Schmitt Trigger input when used in Serial Programming mode.
3: This buffer is a Schmitt Trigger input when configured in RC oscillator mode and a CMOS input otherwise.

Tabla 36. Descripción técnica del PIC16F 873 A parte 1

TABLE 1-2: PIC16F873A/876A PINOUT DESCRIPTION (CONTINUED)

Pin Name	Pin#	I/O/P Type	Buffer Type	Description
				PORTB is a bi-directional I/O port. PORTB can be software programmed for internal weak pull-up on all inputs.
RB0/INT	21		TTL/ST(1)	
RB0		I/O		Digital I/O.
INT		I		External interrupt.
RB1	22	I/O	TTL	Digital I/O.
RB2	23	I/O	TTL	Digital I/O.
RB3/PGM	24		TTL	
RB3		I/O		Digital I/O.
PGM		I/O		Low voltage ICSP programming enable pin.
RB4	25	I/O	TTL	Digital I/O.
RB5	26	I/O	TTL	Digital I/O.
RB6/PGC	27		TTL/ST(2)	
RB6		I/O		Digital I/O.
PGC		I/O		In-Circuit Debugger and ICSP programming clock.
RB7/PGD	28		TTL/ST(2)	
RB7		I/O		Digital I/O.
PGD		I/O		In-Circuit Debugger and ICSP programming data.
				PORTC is a bi-directional I/O port.
RC0/T1OSO/T1CKI	11		ST	
RC0		I/O		Digital I/O.
T1OSO		O		Timer1 oscillator output.
T1CKI		I		Timer1 external clock input.
RC1/T1OSI/CCP2	12		ST	
RC1		I/O		Digital I/O.
T1OSI		I		Timer1 oscillator input.
CCP2		I/O		Capture2 input, Compare2 output, PWM2 output.
RC2/CCP1	13		ST	
RC2		I/O		Digital I/O.
CCP1		I/O		Capture1 input/Compare1 output/PWM1 output.
RC3/SCK/SCL	14		ST	
RC3		I/O		Digital I/O.
SCK		I/O		Synchronous serial clock input/output for SPI mode.
SCL		I/O		Synchronous serial clock input/output for I^2C mode.
RC4/SDI/SDA	15		ST	
RC4		I/O		Digital I/O.
SDI		I		SPI data in.
SDA		I/O		I^2C data I/O.
RC5/SDO	16		ST	
RC5		I/O		Digital I/O.
SDO		O		SPI data out.
RC6/TX/CK	17		ST	
RC6		I/O		Digital I/O.
TX		O		USART asynchronous transmit.
CK		I/O		USART 1 synchronous clock.
RC7/RX/DT	18		ST	
RC7		I/O		Digital I/O.
RX		I		USART asynchronous receive.
DT		I/O		USART synchronous data.
VSS	8, 19	P	—	Ground reference for logic and I/O pins.
VDD	20	P	—	Positive supply for logic and I/O pins.

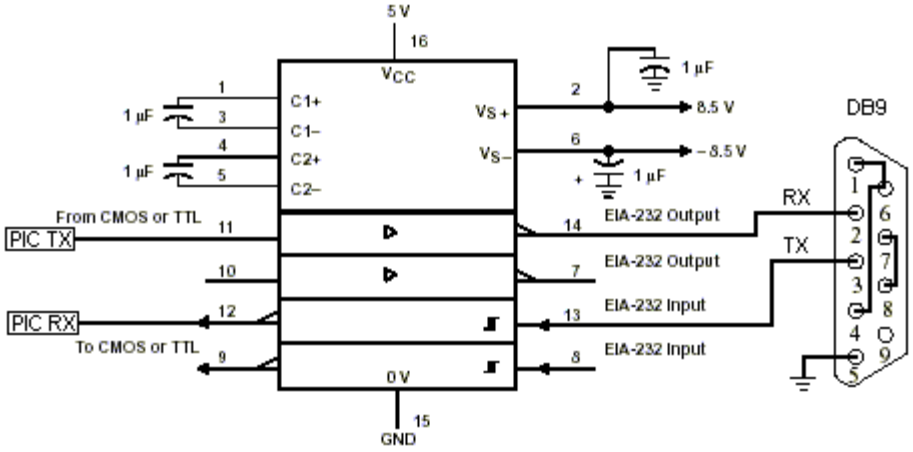
Legend: I = input O = output I/O = input/output P = power
— = Not used TTL = TTL input ST = Schmitt Trigger input

Note 1: This buffer is a Schmitt Trigger input when configured as the external interrupt.
2: This buffer is a Schmitt Trigger input when used in Serial Programming mode.
3: This buffer is a Schmitt Trigger input when configured in RC oscillator mode and a CMOS input otherwise.

Tabla 37. Descripción técnica del PIC16F 873 A parte 2

MAX232

El circuito integrado MAX232 cambia los niveles TTL a los del estándar RS-232 cuando se hace una transmisión, y cambia los niveles RS-232 a TTL cuando se tiene una recepción. El circuito típico se muestra en la siguiente figura:



Circuito básico con el MAX232

Figura 51. Descripción técnica MAX232

Conversor de protocolos

Modelo 285 - Conversor de Interfase RS-232 a RS-422/RS-485

El Modelo 285 "superverter" es un convertidor de interfaz que puede ser configurado para comunicarse con equipo de acuerdo a las normas de RS-422 o RS-485 a RS-232. Cuando opera como convertidor a RS-485, el Modelo 285 tiene un modo inteligente para controlar las líneas de RS-485. Cuando está configurado para operar de RS-422 a RS-232, el Modelo 285 convierte data "Full Duplex", TD y RD entre los dos protocolos. El Modelo 285 puede ser configurado para convertir la información a RS-485 de dos o cuatro alambres. Porque el protocolo RS-485 es "Half Duplex", esta unidad tiene la capacidad de controlar la transmisión por una de dos maneras. La primera es con la línea de control, RTS, pin 4 del puerto de RS-232. En este caso, cuando la línea RTS está en voltaje positivo, comunicación procede de RS-232 a RS-485. Cuando la línea RTS baja a voltaje negativo, comunicación se permite de RS-485 a RS-232. La Segunda manera de controlar el transmisor es con la línea TD de data.

Cuando no hay transmisión hacia el Puerto RS-232, la unida está automáticamente preparada para recibir información del puerto RS-485. El receptor de RS-485 opera diferente dependiendo en el modo de operación. En RS-485 de 4 alambres, el receptor siempre está activo y el transmisor se controla con la línea RTS o TD. En el modo de dos alambres, el receptor y el transmisor están controlados con la línea RTS o TD. Cuando uno está activo el otro no. El Modelo 285 viene equipado con un conmutador de cinco posiciones para seleccionar lo siguiente: Modo RS-422 (4 alambres), RS-485 (2 o 4 alambres), modo RS-485 transmisor controlado por RTS o TD. En el modo RS-485 de 2 alambres se puede seleccionar la resistencia de terminación (220 ohmios) para el receptor. Este modelo también viene con el conmutador DTE/DCE, que invierte los pines 2 y 3 en el Puerto RS-232 para acomodar cualquier equipo.

Adaptador RJ45 a DB9 hembra

Usado para conectar dispositivos tipo DB9, por ejemplo Cable Cat-5, dispositivos Seriales, consolas de CISCO, equipo de telecomunicaciones, etc.

Está es la manera de armar y colocar los cables, ya listos para presionarlos en el conector DB9.

Código de Colores

Color del Pin	
1 (No conectado)	
2 Amarillo	
3 Negro	
4 Naranja	
5 Verde	Rojo
6 Cafe	
7 Azul	
8 Blanco	
9 (No conectado)	

Figura 52. Descripción de colores DB9

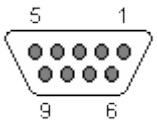


Figura 53. Descripción forma conector DB9

Baquelita circuito de cerradura

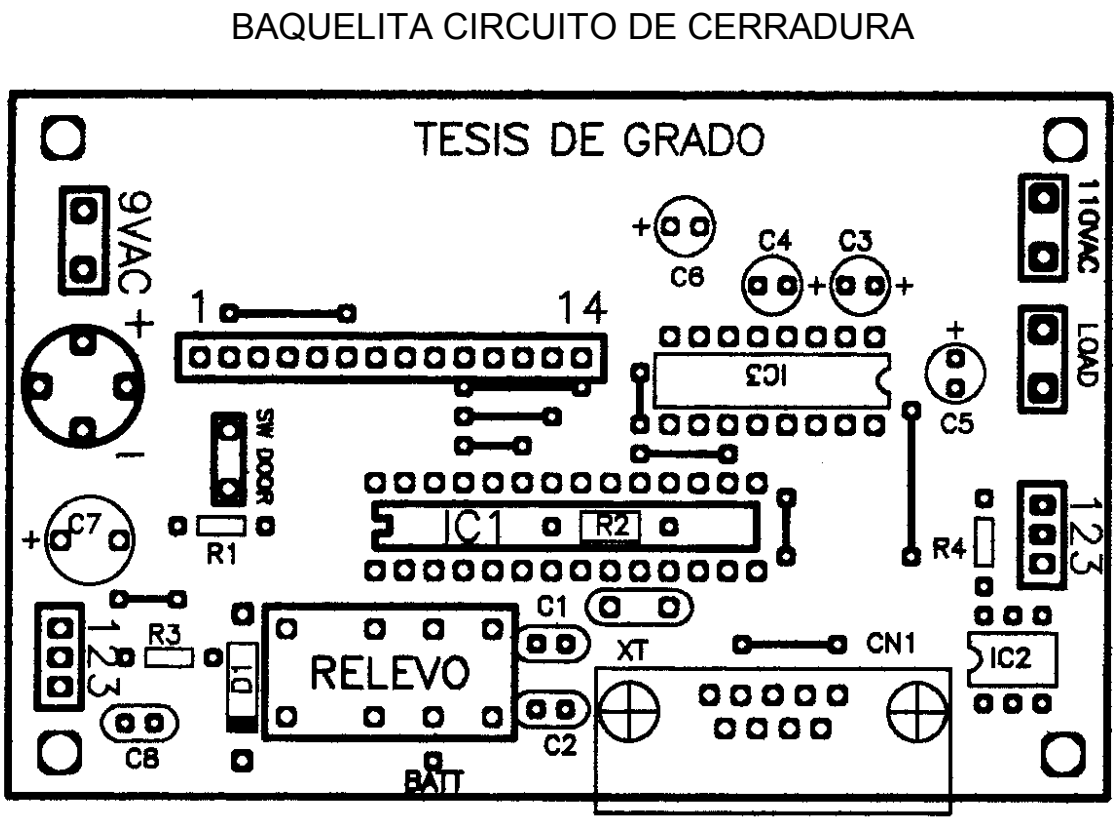


Figura 54. Baquelita circuito de cerradura vista 1

BAQUELITA CIRCUITO DE CERRADURA

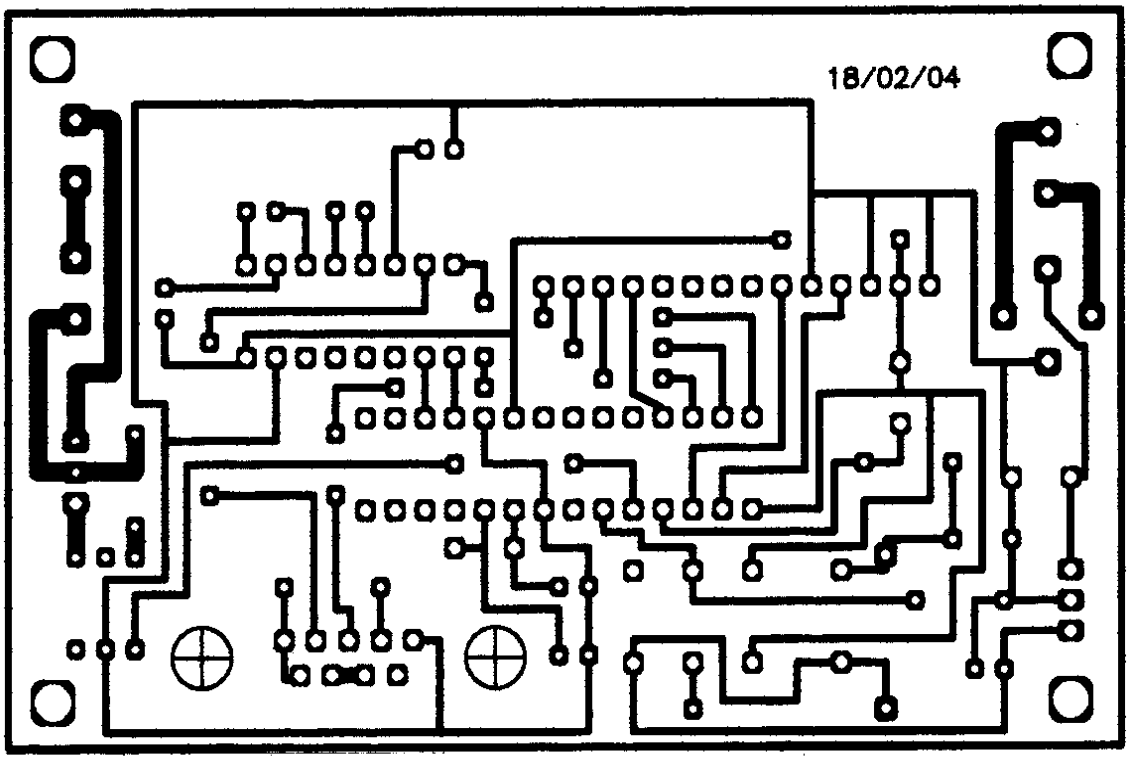


Figura 55. Baquelita circuito de cerradura vista 2

5.3.3.16 Seguro Electrónico

Abre puestas Eléctricos Assel

En la actualidad, la gama de abre puertas eléctricas de Assel es una de las más completas del mercado, ofreciendo en nuestro catálogo mas de 9.000 referencias distintas. De esta forma conseguimos adaptarnos siempre a cada necesidad del cliente, ofreciéndole diversas opciones en los mecanismos y variedad en las armaduras.

Para el mecanismo de apertura, Assel ofrece múltiples combinaciones en cada uno de sus componentes. Así nuestro pestillo puede ser normal, ajustable o con micro ruptor. Además estas opciones pueden llevar automático y/o desbloqueo manual. Nuestras bobinas pueden ser tanto para corriente alterna (8-12V y 110V), continua (12V y 24V) o ambas (12V AC/DC y 24V AC/DC) y validas para funcionamientos en acción invertida y desbloqueo eléctrico. Además todos los componentes pueden estar especialmente reforzados para incrementar la seguridad (ver serie 80).

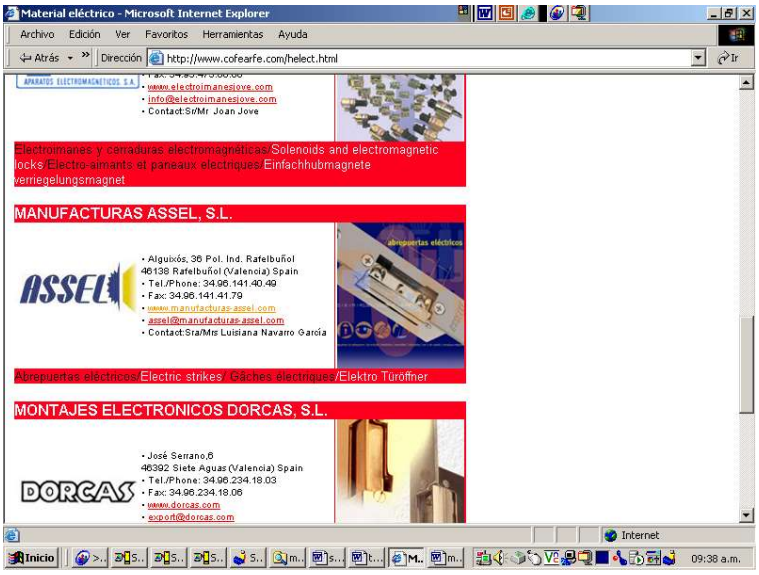


Figura 56. Presentación Abre puertas Eléctricos Assel

5.3.3.17 Tarjeta Inteligente

Tarjeta Inteligentes C3PO

Figura 57. Tarjeta de inteligente C3PO

Tarjeta de Memoria Protegida

Tarjeta de 256 bytes de 8 bits de memoria principal EEPROM y 32 bits de memoria de protección funcional PROM. La memoria principal se borra y escribe byte a byte. Al ser borrado, los 8 bits del byte se colocan en la posición lógica 1. La escritura y el borrado tiene un tiempo de 2.5 ms cada uno. Los primeros 32 bits pueden ser irreversiblemente protegidos contra cambios mediante la escritura del correspondiente bit en la memoria protegida. Cada escritura hecha en la memoria protegida no puede ser borrada.

Esta tarjeta, además, tiene un código lógico de seguridad que controla los accesos de escritura y borrado de la memoria. Para este propósito la tarjeta contiene una memoria de seguridad de 4 bytes con contador de errores.

Funcionamiento

Las tarjetas se activan al introducirlas en un lector de tarjetas. Un contacto metálico, o

incluso una lectura láser, como en un CD-ROM, permite la transferencia de información entre el lector y la tarjeta, actualmente comienzan a existir casas comerciales cuyos productos permiten leer una tarjeta inteligente desde el propio ordenador personal.
Las comunicaciones de las tarjetas inteligentes se rigen por el estándar ISO 7816/3, la tasa de transferencia de datos es de 9600 baudios en modo asincrónico.

Características Técnicas

- 256 x 8-bit de organización de EEPROM.
- Direccionamiento de byte inteligente.
- Protección irreversible contra escritura de los primeros 32 bits.
- 32 x 1-bit de organización de la memoria de protección.
- ATR según norma ISO 7816-3.
- Tiempo de programación de 2.5 ms por byte.
- Mínimo de 10.000 ciclos de escritura / borrado.
- Retención de datos por un mínimo de 10 años.
- Los datos sólo pueden ser modificados después de introducir los tres bytes correctos del código de seguridad programable (memoria de seguridad).

5.3.3.18 Lectora de Tarjetas Inteligentes

Modelo PTI-02

Dispositivo de lectura y escritura por contacto para tarjetas inteligentes tipo E2PROM

Figura 58. Unidad lectora PTI-02

Características

Trabaja bajo cualquier plataforma utilizando puerto serial.
Modulo esclavo de PC.
Comunicación serial.
Almacenamiento confiable de la información.

Especificaciones.

Modelo: PTI-02

Tipo de tarjetas: ISO-7816
Protocolo: I2C
Alimentación: DC 9-12V/500mA
Interfaz: RS232
Velocidad de transmisión: 9600, 8, n, 1.

Información

Sistema que puede ser utilizado para:
Dispositivos control de acceso.
Sistemas prepago.
Sistemas de identificación.
Captura automática de información

5.3.3.14 Transmisión serie RS232.

Las comunicaciones serie se utilizan para enviar datos a través de largas distancias, ya que las comunicaciones en paralelo exigen demasiado cableado para ser operativas. Los datos serie recibidos desde un módem o otros dispositivos son convertidos a paralelo gracias a lo cual pueden ser manejados por el bus del PC.

Los equipos de comunicaciones serie se pueden dividir entre simplex, half-duplex y full-duplex. Una comunicación serie simplex envía información en una sola dirección (p.e. una emisora de radio comercial). Half-duplex significa que los datos pueden ser enviados en ambas direcciones entre dos sistemas, pero en una sola dirección al mismo tiempo. En una transmisión full-duplex cada sistema puede enviar y recibir datos al mismo tiempo.

Hay dos tipos de comunicaciones: síncronas o asíncronas. En una transmisión síncrona los datos son enviados en bloques, el transmisor y el receptor son sincronizados por un o más caracteres especiales llamados caracteres sync.

El puerto serie del PC es un dispositivo asíncrono, luego empezaremos describiendo este tipo de sistemas. En una transmisión asíncrona, un bit identifica su bit de comienzo y 1 o 2

bits identifican su final, no es necesario ningún carácter de sincronismo. Los bits de datos son enviados al receptor después del bit de start. El bit de menos peso es transmitido primero. Un carácter de datos suele consistir en 7 o 8 bits. Dependiendo de la configuración de la transmisión un bit de paridad es enviado después de cada bit de datos. Se utiliza para corregir errores en los caracteres de datos. Finalmente 1 o 2 bits de stop son enviados.

5.3.4 Implementación e Implantación.

SOFTWARE

El desarrollo del aplicativo se realizo utilizando como manejador de base de datos "Access 2000" y como herramienta de programación "Microsoft Visual Studio 6.0".

En la versión original del proyecto fue necesario realizar cambios drásticos frente a la elección del software de programación en el cual se iba ha realizar, pues en el estudio preliminar la plataforma de la base de datos era SQL Server con una interfase gráfica HTLM.

Pero en la medida que se fue desarrollando el estudio de factibilidad, se noto que la plataforma de base de datos era demasiado costosa y no ameritaba la implementación, él numero de registros en su face de prototipo no superaría los 10.000, por consiguiente se decidió la utilización de Access.

En cuanto a la interfase, HTML no proporciono de una manea adecuada la versatilidad de conexión con el puerto, por lo tanto, se opto por Visual Basic, pues este aplicativo proporciona una interfase sencilla y fácil de utilizar.
Pero también nos ha limitado a la utilización de aplicativo y toda sus librerías, por lo tanto no es totalmente portable así como fue le idea original, por lo tanto nos limita a dicha utilización.

El software que se diseño ha sido demarcado por un estándar, que es la utilización de botones de navegación, menús, colores y tipos de fuentes, los cuales son escogidos por el usuario del aplicativo.

TARJETA INTELIGENTE

Se utilizó la tarjeta inteligente de memoria protegida C32PK por su fácil adquisición en el mercado y adaptación a las lectoras disponibles en Colombia.

LECTORA TARJETA INTELIGENTE

La unidad lectora más económica y reconocida en Colombia es PLINTEC LEC la cual tiene un valor aproximado de 250 dólares sin IVA por estos altos valores hemos decidido utilizar una diseña y manufacturada en Colombia por señor Fredy Ortiz Ingeniero Electrónico de la Universidad Distrital de Colombia. Por requerimiento nuestro fue posible adaptar a está unidad un DIR swicht para poder conocer y controlar el lugar donde se instale el dispositivo.

CIRCUITO ELECTRONICO

Uno de los eslabones más duros de desarrollar por nuestras deficiencias en conocimientos en electrónica. Los primeros prototipos del circuito fueron realizados mediante la utilización de los siguientes software MPLAB, CIRCUIT MARKET y TERMINAL MONITOR. Finalizados los diseños y probados los diferentes componentes del circuito se integraron en protoboard por más de 5 veces. Finalmente se tomo la decisión de quemar el circuito en una baquelita para evitar daños de los elementos, desconexiones no deseadas ó corto circuitos por la variedades de voltajes utilizadas y evitar el incremento de los costos por el reemplazo de estos elementos.

5.3.5 Puesta en Marcha y Pruebas.

Como el prototipo se encuentra implementado en una maqueta se consideran cuatro pasos a seguir.

- Prueba del software diseñado
- Pruebas de Comunicación
- Pruebas del circuito
- Prueba general de gestión.

Prueba del software diseñado

- Se verifica la comunicación que existe en el ingreso de información con la base de datos, el manejo de esta y su administración de almacenamiento.

- Examina claves de acceso que permiten a los usuarios el acceso al aplicativo implementado.

- Inspecciona el ambiente grafico y la presentación del usuario, para que sea acorde con los requerimientos.

- Se realizan pruebas de integridad en los diferentes campos de entrada de datos para evitar errores por falta de validaciones.

- Verificación de la exactitud de los reportes establecidos dentro de la aplicación y como fuente de información para el usuario.

Realizadas estas pruebas se llega a la conclusión que el sistema funciona adecuadamente con lo esperado después de haber realizado 5 pruebas y ratificar validaciones.

Prueba de Comunicación

Se envían señales del software implementado a los puertos y se confirma la recepción de señal en estos.

En esta prueba se presentaron inconvenientes mientras se adecua el manejo del componente de Visual Basic para el manejo de comunicaciones Microsoft COMM Control 6.0.

- Las pruebas de software se realizan en un PC con dos puertos seriales de COM1 y COM2. El COM1 se utiliza se configura como el puerto de recepción de datos de la unidad lectora y el puerto COM2 como puerto de intercambio de datos con el circuito electrónico. Las pruebas de comunicación con estos puertos tienen un resultado satisfactorio.

Pruebas del circuito

Al implementar el circuito se presentan inconvenientes con las conexiones realizadas, ya que los pines de salida programados no fueron bien reconocidos en el montaje del PIC 16F873A. Se generan pruebas hasta lograr el objetivo propuesto.

Prueba general de Gestión

Se reúnen todos los diferentes componentes electrónicos en una maqueta para facilitar su movilización y la realización de las pruebas. Se realiza la integración de todos los componentes del sistema de control de acceso SCAEC para observar su comportamiento. Al implementarlo se efectuaron pruebas de la comunicación con el circuito, la recepción de información de la unidad lectora al PC, comprobación interna de datos en la base de datos y validación dentro del sistema.

5.3.5.1 Selección de la Prueba

Es una de las fases más importantes del proceso y a la que se debe destinar el tiempo adecuado y las revisiones oportunas. Como en cualquier desarrollo, se comienza por las unitarias, donde se realiza pruebas muy detalladas modulo por modulo y su correcta integración. La prueba se realiza ejecutando un check list que reúna todas las características vitales del sistema.

5.3.5.2 Sitio de Prueba

Las diferentes pruebas realizadas se realizan en las oficinas alquiladas para le desarrollo del proyecto y se toma como objeto de la prueba la maqueta prototipo que reúne todos los elementos que conforma el proyecto SCAEC.

5.3.5.3 Procedimiento de la Prueba.

- Encendemos todos los componentes del sistema

- Verificación de acceso al software, validaciones e integridad en su funcionamiento.

- Incorporación de un usuario dentro de la base de datos del sistema y se le otorgan permisos de acceso con limitaciones.

- Se realizan los procesos de generación de documento de acceso y verificación de permisos para el usuario de la prueba.

- Activamos los servicios de monitoreo de los puertos seriales del PC COM1 y COM2 y validamos su correcta comunicación con el circuito electrónico y ella unidad lectora.

- Se modifica en la unidad lectora el valor del dir switch de 0 a 1 y se introduce el carnet recién generado para validar lectura y permisos de acceso.

- Se regresa el valor original del esclavo en la unidad lectora y nuevamente se realizan los procesos de validación.

- Verificamos los monitores de control ante los anteriores sucesos y su registro en la base de datos.

- Generamos reportes de permanencia y movimientos del sistema y revisamos los datos obtenidos.

5.3.5.4 Personal de Prueba

Se requiere un tecnólogo electrónico para realizar el check lisa de verificación sobre los diferentes componentes electrónicos, el administrador del sistema, los ingenieros desarrolladores de software, y un usuario para realizar la prueba.

Intervienen en la prueba Javier Rodríguez como tecnólogo electrónico, Ricardo Pinilla como analista e ingeniero desarrollador del software SCAEC y Humberto Pineda como desarrollador de las interfaces de comunicación.

5.3.5.5 Prueba y equipo de Soporte.

Se preparara toda la documentación, tanto del sistema como para usuarios y facilitar las modificaciones posteriores en el primer caso y el inicio de su utilización en el segundo. Las metodologías de desarrollo generalmente aceptadas especifican la información y estructuración de esta documentación.

5.3.5.6 Conclusión de la Prueba

Al efectuar las pruebas correspondientes especificadas en el check list de integridad funcional se observa un buen funcionamiento del sistema. Se detectan algunas deficiencias de presentación y diseño en los reportes de salida los cuales son solucionados.

5.3.5.7 Mantenimiento

El prototipo se dona a la universidad para ser tomado como base para futuras investigaciones y mejoras al respecto. Por lo anterior requiere una operación periódica para verificar el funcionamiento de la unidad lectora, el circuito y las tarjetas de memoria.

5.4 CONCLUSIONES IMPLEMENTACION

- La utilización de "Access 2000" como manejador de bases de datos por su fácil integración con Visual Basic.
- "Visual Basic Studio 6.0" como herramienta de programación.
- La inclusión de la tarjeta inteligente de memoria protegida C32PK.
- El reconocimiento a la creatividad colombiana en el desarrollo de soluciones electrónicas como el de la unidad lectora / escritora de tarjetas inteligentes.

- La incorporación al proyecto de otras herramientas tecnológicas como MPLAB, CIRCUIT MARKET y TERMINAL MONITOR.
- La integración de exitosa de un desarrollo de un software visual con elementos electrónicos y puertos de comunicación.

6. CONCLUSIONES

- Se ha presentado ante la sociedad un nuevo esquema de control de acceso a centro de computo ó cualquier lugar que amerite seguridad utilizando elementos de última tecnología.

- El costo de fabricación de este prototipo promete hacia el futuro que en su fabricación en línea puede ofrecer a la industria colombiana un producto de buena calidad a bajo costo que era uno de los objetivos principales del proyecto.

- Por ser un prototipo se presenta muchos ítem de mejoramiento que pueden ser resueltos con un buen patrocinio económico, cambios de integración electrónica y búsqueda de otras alternativas del lenguaje de programación.

- El proyecto abre la puerta para el desarrollo de nuevas aplicaciones con la utilización de tarjetas inteligentes y puertos seriales que pueden ayudar a solucionar muchas necesidades del mercado como el de la salud. “Podremos llegar a tener nuestra hoja clínica en una tarjeta y poderla llevar a todas partes”.

- El desarrollar el circuito electrónico nos permite conocer este amplio mundo y poder llegar a presentar soluciones integrales que mezclen software y hardware a la vez.

- Se cumplió con el objetivo inicial, diseñando e implementando una maqueta que nos permite el control de acceso a un centro de computo.

7. CRONOGRAMA

Anexamos a continuación los diagramas mencionados

8. BIBLIOGRAFÍA

D. W. Davies and W. L. Price.
Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer.
John Wiley and Sons, New York, 1984

David Everett.
Identity verification and biometrics.
In Keith M. Jackson and Jan Hruska, editors, Computer Security Reference Book, chapter 10, pages 37-73. Butterworth-Heinemann, 1992.

Andrew Tanenbaum.
Operating Systems: Design and Implementation.
Prentice Hall, 1991.

Louis Claude Guillou, Michel Ugon, and Jean-Jacques Quisquater.
The smart card - a standardized security device dedicated to public cryptology.
In Contemporary Cryptology - The Science of Information Integrity, pages 561-614. IEEE Press, 1992.

Roger Merckling and Anne Anderson.
RFC 57.0: Smart Card Introduction, Marzo 1994.

Jesús Pita.

La tarjeta inteligente como medio de identificación electrónica y acceso a servicios de seguridad: La experiencia de la FNMT-RCM.
Seguridad en Informática y Comunicaciones, (39), Abril 2000.

Dirk Balfanz and Edward W. Felten.
Hand-held computers can be better smart cards.
In Proceedings of the 8th USENIX Security Symposium. The USENIX Association, Agosto 1999.

H. Gobioff, S. Smith, J.D. Tygar, and B. Yee.
Smart cards in hostile environments.
In Proceedings of the 2nd USENIX Workshop on Electronic Commerce. The USENIX Association, Noviembre 1996.

Ross J. Anderson.Tamperproofing of Chip Cards.
Enviado a la lista cypherpunks@cyberpass.net por William H. Geiger III en septiembre, 1997.

Ross J. Anderson and Markus Kuhn.
Tamper resistance - a cautionary note.
In Proceedings of the 2nd USENIX Workshop on Electronic Commerce, pages 1-11. The USENIX Association, Noviembre 1996.

David Everett.
Identity verification and biometrics.
In Keith M. Jackson and Jan Hruska, editors, Computer Security Reference Book, chapter 10, pages 37-73. Butterworth-Heinemann, 1992.

Simo Huopio.
Biometric Identification.

In Seminar on Network Security: Authorization and Access Control in Open Network Environment, 1998.

Ken Phillips.
Biometric identification comparison chart.
PC Week, Marzo 1997.