ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO Y CONSTRUCCIÓN DE UN MÓDULO DE CONTROL DE ACCESO PARA LOS ARMARIOS DE CNT DE LA CIUDAD DE AMBATO

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y CONTROL

DIEGO FERNANDO LAGOS SALTOS
diegofer544@hotmail.com

DIRECTOR: ING. YADIRA LUCÍA BRAVO NARVAEZ
yadira.bravo@epn.edu.ec

Quito, Junio 2012

DECLARACIÓN

Yo Diego Fernando Lagos Saltos, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Diego Fernando Lagos Saltos

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diego Fernando Lagos Saltos, bajo mi supervisión.

_____

Ing. Yadira Bravo
DIRECTORA DEL PROYECTO

AGRADECIMIENTO

A Dios por guiarme en este duro camino, por darme la fortaleza y el valor en cada uno de los obstáculos que se me han presentado durante toda mi etapa estudiantil.

A mis padres por su apoyo incondicional durante toda mi vida, seguramente no podré pagarles todo lo que ustedes han hecho por mí, pero trataré de hacer todo lo posible para retribuir sus esfuerzos.

A mi hermana que ha estado junto a mí, gracias por escucharme, entenderme y aconsejarme durante los buenos y malos momentos compartidos.

A mis abuelitos, quienes han sido parte fundamental de mi desarrollo emocional como persona, además de guiar mis pasos siempre por el camino correcto.

A la Ing. Yadira Bravo por la ayuda y el tiempo dedicado a la culminación de este proyecto.

Al Ing. Fabián Ortiz y Polivio Onofa, por su valiosa ayuda y consejos en cada una de las etapas de la realización de este proyecto.

Al Ing. Hernán Cortez por brindarme toda la apertura y colaboración en el desarrollo de este proyecto, mismo que sin su aprobación no hubiera sido posible.

DEDICATORIA

A Dios, que sin su ayuda y bendición nada de esto hubiera sido posible.

A mi familia, que siempre han estado presente, mostrando su preocupación y apoyo durante toda mi carrera estudiantil; además de depositar su confianza en mí para enfrentar los retos encontrados en el camino y sobrellevarlos de la mejor manera.

A mi querida EPN que me acogió en sus aulas, brindándome todo el conocimiento adquirido y la satisfacción de poder servir a mi país siendo un profesional de prestigio.

Finalmente a mis amigos y compañeros, por los momentos de alegría vividos durante largas jornadas de trabajo.

CONTENIDO

CAPÍTULO 1

RESUMEN

La realización del presente proyecto, surge a partir de la necesidad de las empresas de telefonía local de implementar seguridad y control en la operación de los armarios telefónicos por parte del personal técnico a cargo de los mismos. Además de precautelar el deterioro de los armarios por una manipulación indebida de personas inescrupulosas.

Para las operadoras de telefonía local, son muchos los problemas causados por el fraude telefónico, los cuales son: violación de la privacidad y el robo de llamadas, robo del cable multipar.

Particularmente en la empresa de telefonía local CNT Ambato, se requería de un sistema que controle la seguridad y el acceso a sus armarios telefónicos, lo cual permitiría tener un mejor funcionamiento de sus operaciones, y a la vez automatizar el sistema de ingreso a los armarios con nuevas tecnologías.

El sistema ofrece un monitoreo en tiempo real de los eventos ocurridos durante las 24 horas del día en el armario, identificando al personal que accede al mismo, almacenando los eventos ocurridos, además facilita la detección de aperturas fraudulentas mediante un mensaje de alarma a un teléfono celular. Para la construcción del mismo se utiliza la tecnología RFID, un microcontrolador como elemento de control, tecnología GSM para transmisión de datos, y una página web que permitirá observar los eventos ocurridos desde cualquier parte del mundo.

PRESENTACIÓN

La tecnología de RFID es un sistema de autoidentificación inalámbrico, el cual consiste de etiquetas que almacenan información y lectores que pueden leer a estas etiquetas a distancia. La tecnología RFID está siendo adoptada cada vez por más industrias debido a que su costo es cada vez menor y sus capacidades son mayores. Esto permite generar grandes beneficios como incrementos en la productividad y administración principalmente en los sectores de cadenas de suministro, transporte, seguridad y control de inventarios.

En el Capítulo 1, se hace una revisión de las diversas tecnologías de control de acceso que actualmente se utilizan. Se profundiza el estudio de la tecnología RFID, en la misma se detalla su historia, frecuencias de funcionamiento, estándares y aplicaciones. Además de los elementos primordiales en un sistema RFID.

La descripción de los dispositivos utilizados en la elaboración del módulo de control de acceso se detalla en el Capítulo 2, además se describe el diseño de los distintos circuitos que conforman el hardware de control, adicional a ello se explica la conexión de los mismosy la alimentación del sistema.

Dentro del Capítulo 3, se explica el desarrollo del software para el microcontrolador como para la interfaz,la cual consta de dos partes: aplicación de control-administración y aplicación web. En lo que se refiere a la programación del microcontrolador se menciona las principales subrutinas desarrolladas para la comunicación con el modem GSM y la memoria EEPROM; incluyendo diagramas de flujo y configuraciones especiales para los mismos. Para el desarrollo de la interfaz se expone los programas utilizados para la creación de la base de datos y las dos aplicaciones; además se describe el funcionamiento de las mismas.

En el Capítulo 4, se realizan las pruebas al módulo, también se explica el procedimiento de selección del armario telefónico en donde se instaló el sistema. Se expone las pruebas realizadas en la interfaz de control y administración; en la

página web se muestran todos los reportes realizados durante los 3 días de prueba.

Las conclusiones y recomendaciones respecto al proyecto, en base a los objetivos y alcances planteados en el tema de tesis, son presentadas en el Capítulo 5.

CAPÍTULO 1

SISTEMAS DE CONTROL DE ACCESO Y ESTUDIO DE LA TECNOLOGÍA RFID

En este capítulo se realiza una descripción de los sistemas de control de acceso, así como sus principales tecnologías más utilizadas en nuestro medio. Además se realiza un estudio detallado de la tecnología RFID.

1.1 SISTEMAS DE CONTROL DE ACCESO

1.1.1 GENERALIDADES Y DESCRIPCIÓN DEL PROYECTO[6]

El control de acceso ha evolucionado considerablemente a lo largo de estos años, actualmente lo podemos identificar como un sistema integrado de políticas y procesos organizacionales que pretende facilitar y controlar el acceso a los sistemas de información y a las instalaciones. Este concepto ha pasado por tanto de estar formado exclusivamente por impedimentos físicos, a ser un concepto que también se relaciona con la informática, medio en el que se ha vuelto cada vez más crítico para proteger la información personal y las bases de datos.

Mediante diferentes tecnologías podemos gestionar la digitalización de la identidad con la que se controla los accesos físicos de personas, como la entrada y salida de edificios e instalaciones, por medio de tarjetas (electrónicas o magnéticas) y dispositivos biométricos. La identificación de las personas se puede realizar a través de diferentes tipos de dispositivos de lectura (lectores) y de identificación (tarjetas, biométricos) que utilizan a su vez distintas tecnologías. La selección del lector debe ser consecuente con la elección de la acreditación de identificación personal.

El presente proyecto de titulación pretende realizar un módulo de control de acceso para un armario telefónico en la ciudad de Ambato. El mismo pretende:

- Detectar en tiempo real cualquier suceso ocurrido en el punto de acceso durante las 24 horas del día.
- Identificar al personal que accede al armario, almacenando los eventos ocurridos.
- Enviar un mensaje de alarma en caso de aperturas no autorizadas.

Su funcionamiento es el siguiente: mediante el lector RFID se lee el código de la tarjeta, y posteriormente el microcontrolador toma la decisión de permitir el acceso si el mismo se lo realiza dentro del horario respectivo, además de que dicho código debe encontrarse almacenado en la memoria; el momento en el que haya una apertura del armario, se va a registrar la hora en que el operador ingresa así como la hora del cierre, y esa información es enviada a través de mensaje de texto mediante un modem GSM hacia la interfaz. Para el respaldo de la información en el microcontrolador se utiliza una memoria EEPROM. La interfaz consiste en 2 partes: la primera es una simple interfaz de control y administración a la que llegan todos los eventos que son almacenados en la base de datos; la segunda parte es una página web, en la que se visualizan eventos, usuarios, realiza búsquedas de eventos y los imprime, facilitando el acceso a la información de los mismos en cualquier parte del mundo.

1.1.2 COMPONENTES DE UN SISTEMA DE CONTROL DE ACCESO

- Tarjeta controladora: Es la parte más importante del control de acceso en la cual se hace la instalación de todos los periféricos y es la que realiza todos los procesos de control.

- Sensor: Este dispositivo es el encargado de notificar el estado de la puerta: cerrada o abierta.

- Cerradura: Este dispositivo eléctrico es el encargado de mantener cerrada o abierta la puerta.

- Lectores: Son los dispositivos que deben sensar el tipo de información presentada en forma de tarjeta para ingresar o salir de algún lugar donde esté presente este dispositivo.

- PC y Software: Es la herramienta que sirve para programar el panel de acceso y revisar el estado del sistema. La PC no necesita estar en línea para que el equipo y el sistema sigan operando.

1.1.3 TECNOLOGÍAS DE CONTROL DE ACCESO

A continuación se presenta una breve descripción de las tecnologías de control de acceso más utilizadas actualmente.

1.1.3.1 Sistemas Biométricos[10]

Un sistema biométrico es un método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento preciso. Las características básicas que un sistema biométrico tiene son: desempeño, aceptabilidad y fiabilidad. Las cuales apuntan a la obtención de un sistema biométrico con utilidad práctica.

En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características. Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

- Rostro.
- Termograma del rostro (Reconocimiento facial que se basa en la luz infrarroja).
- Huellas dactilares.
- Geometría de la mano.

- Venas de las manos.
- Iris.
- Patrones de la retina.
- Voz.
- Firma.

Figura 1.1: Sistema Biométrico basado en huellas dactilares [10]

1.1.3.2 Código de Barras[26]

Conocidos hoy por una buena parte de la humanidad los códigos de barras, son una técnica de entrada de datos (tal como la captura manual, el reconocimiento óptico y la cinta magnética), con imágenes formadas por combinaciones de barras y espacios paralelos, de anchos variables. Representan números que a su vez pueden ser leídos y descifrados por lectores ópticos o scanners.

Figura 1.2: Código de barras [11]

1.1.3.3 Tarjetas Inteligentes[13]

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

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

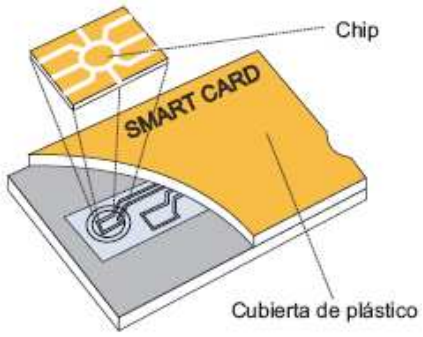


Figura 1.3: Tarjeta Inteligente [13]

1.1.3.4 Tecnología de banda magnética[12]

Es toda aquella banda oscura presente en tarjetas de crédito, abonos de transporte público o carnets personales que está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina (generalmente epoxi) y que almacenan cierta cantidad de información mediante una codificación determinada que polariza dichas partículas. La banda magnética es grabada o leída mediante contacto físico pasándola a través de una cabeza lectora-escritora gracias al fenómeno de la inducción magnética.

Figura 1.4: Tarjetas con banda magnética [12]

1.1.3.5 Tarjetas de Proximidad[14]

Las tarjetas de proximidad son dispositivos que están constantemente enviando señales al lector para saber la posición exacta de cada una en todo momento.

También se denominan dispositivos RFID (*Radio Frequency Identification*) cuyo propósito es el de transmitir la identidad de un objeto mediante ondas de radio.

Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor.

Figura 1.5: Tarjetas de Proximidad [14]

Esta es la tecnología de control de acceso que es utilizada en el presente trabajo, por lo que es explicado posteriormente de manera más amplia.

1.2 TECNOLOGÍA RFID (IDENTIFICACIÓN POR RADIO FRECUENCIA)[8]

La identificación por radiofrecuencia es una tecnología basada en el reconocimiento de información contenida en etiquetas electrónicas. Cuando estas etiquetas entran en el área de cobertura de un lector de radiofrecuencia (RFID), éste envía una señal para que la etiqueta transmita la información almacenada en su memoria, habitualmente un código de identificación.

Una de las claves de esta tecnología es que la recuperación de la información contenida en la etiqueta se realiza vía radiofrecuencia y sin necesidad de que exista contacto físico o visual (línea de vista entre el dispositivo lector y las etiquetas), aunque en muchos casos se exige una cierta proximidad de esos elementos.

1.3 HISTORIA DE LA TECNOLOGÍA RFID[8]

El origen de esta tecnología se remonta a la época de la Segunda Guerra Mundial específicamente cuando los radares permitían la detección de aviones a kilómetros de distancia, más no su identificación. En un comienzo, el ejército alemán descubrió que si los pilotos balanceaban sus aviones al volver a la base cambiaría la señal de radio reflejada de vuelta. Con este método se lograba distinguir a los aviones alemanes de los aliados y se convirtió en el primer dispositivo de RFID pasivo.

Entre la década de 1950 y 1960 hubo un avance tecnológico referente a los radares y sistemas de comunicaciones por radiofrecuencia en el área de identificación de objetos remotamente. Pronto los países avanzados empezaron a

trabajar con sistemas antirrobo que usando ondas de radio determinaban si un objeto había sido pagado o no a la salida de tiendas.

Los primeros dispositivos RFID patentados aparecieron en Estados Unidos en 1973 cuando Mario W. Cardullo presentó una etiqueta RFID activa que portaba una memoria rescribible. Para el mismo año, Charles Walton obtuvo una patente de un sistema RFID pasivo que abría las puertas sin necesidad de llaves.

El gobierno norteamericano en los años 70 instaló sistemas muy parecidos para el manejo de puertas en algunas centrales nucleares, cuyas puertas se abrían al paso de los camiones que portaban materiales para las mismas que iban equipados con un tag (etiqueta) RFID. Paralelamente se desarrolló un sistema para el control del ganado de esa época que consistía en un tag RFID pasivo con el que se identificaba a los animales que habían sido o no vacunados. El mismo era insertado en los animales a través de una vacuna.

Con el tiempo ha existido mejoras tanto de emisión como de recepción lo que ha permitido extender su uso en varios campos de aplicación como por ejemplo el ámbito doméstico, seguridad, transporte, etc. Un claro ejemplo de ello es el pasaporte expedido en la actualidad en los EEUU que lleva asociadas etiquetas RFID.

1.4 SISTEMA RFID

En un sistema RFID, el elemento a identificar (puede ser un objeto, animal o persona) se etiqueta con un pequeño chip de silicio unido a una antena de radiofrecuencia (conocido como tag o etiqueta) de modo que pueda comunicarse y ser identificado, a través de ondas de radiofrecuencia, por un dispositivo transmisor/receptor (conocido como lector) diseñado para ese propósito.

La característica principal que dota a este sistema de identificación de un gran valor añadido, es que el chip de RFID permite almacenar en su interior

información de identificación que confiere a cada uno de los elementos etiquetados de un carácter único.

En un sistema básico RFID vamos a encontrar los siguientes elementos:

- Tag: Compuesta de una etiqueta RFID; consiste en un pequeño circuito integrado con una pequeña antena capaz de transmitir un número de serie único hacia un dispositivo de lectura, como respuesta a una petición. En algunas ocasiones se incluye una batería.

- Lector: El cual puede ser de lectura o lectura/escritura, está compuesto por una antena, un módulo electrónico de radiofrecuencia y un módulo electrónico de control.

- Antena del lector: Es un componente obligatorio. Actualmente algunos lectores tienen las antenas incorporadas.

- Controlador: Conocido comúnmente como una PC o Workstation, en la cual corre una base de datos y algún software de control.

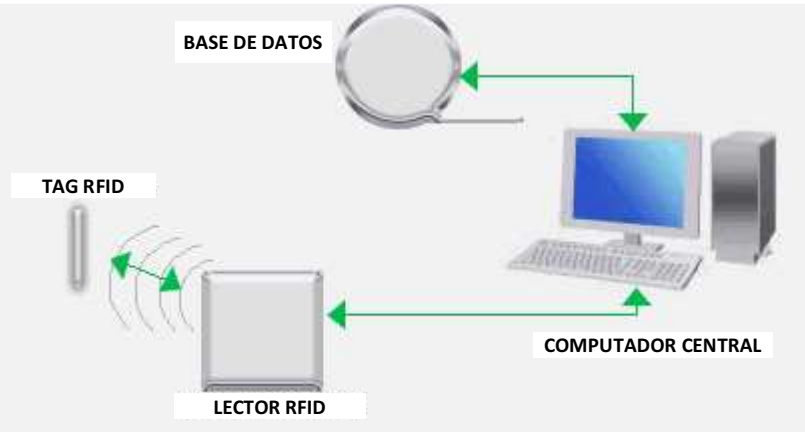


Figura 1.6: Componentes de un sistema RFID [1]

1.5 FRECUENCIAS DE OPERACIÓN DE UN SISTEMA RFID[3]

Hay cuatro clases distintas de clasificación según su frecuencia:

- Baja Frecuencia (9-135 Khz): Los sistemas que utilizan este rango de frecuencia tiene la desventaja de una distancia de lectura de hasta 45cm. Sólo pueden leer un elemento a la vez.

- Alta Frecuencia (13.56 Mhz): Esta frecuencia es muy popular y cubre distancias de 1m a 3m. Típicamente los tags que trabajan en esta frecuencia son de tipo pasivo.

- Ultra Alta Frecuencia (0.3 – 1.2GHz): Este rango se utiliza para tener una mayor distancia entre la tag y el lector (de 3 a 10 metros, dependiendo del fabricante y del ambiente). Estas frecuencias no pueden penetrar el metal ni los líquidos a diferencia de las bajas frecuencias, pero pueden transmitir a mayor velocidad y por lo tanto son buenos para leer más de un tag a la vez.

- Microondas (2.45 – 5.8 Ghz): La ventaja de utilizar un intervalo tan amplio de frecuencias es su resistencia a los fuertes campos electromagnéticos, producidos por motores eléctricos, por lo tanto, estos sistemas son utilizados en líneas de producción de automóviles. Sin embargo, estos tags requieren de mayor potencia y son más costosas, pero es posible lograr lectura a distancias mayores a 10 metros.

1.6 TAG RFID[8]

Es el componente estrella del sistema RFID. Su modo de operación básico, tiene capacidad de recibir y transmitir señales, pero sólo transmite a modo de respuesta ante una posible petición del lector RFID. El tag es un pequeño chip o circuito

integrado, adaptado a una antena de radiofrecuencia (RF) que permite la comunicación vía radio. Estos dos elementos integrados sobre un substrato, forman lo que se conoce como tag. Dependiendo de la aplicación final del sistema de identificación, el substrato donde se encapsula el chip y la antena RF es diferente permitiendo la adaptación de sus características a los requisitos de la aplicación, por ejemplo hay tags especiales para líquidos, metales, libros, etc.

Figura 1.7: Diversos tipos de tags RFID [2]

1.6.1 CONSTRUCCIÓN

Los tags son fabricados en una amplia variedad de formatos. El proceso básico de montaje consta en primer lugar de una base de material de substrato(papel, PVC, PET, etc.), sobre ésta, se encuentra una antena hecha de materiales conductivos, tipo aluminio, cobre, etc. A continuación el chip del tag es conectado a la antena.

Finalmente, se reviste con una capa protectora realizada en diferentes tipos de materiales tales como PVC laminado, resina epóxica o papel adhesivo, según requerimientos que se necesiten por las distintas condiciones finales del entorno.

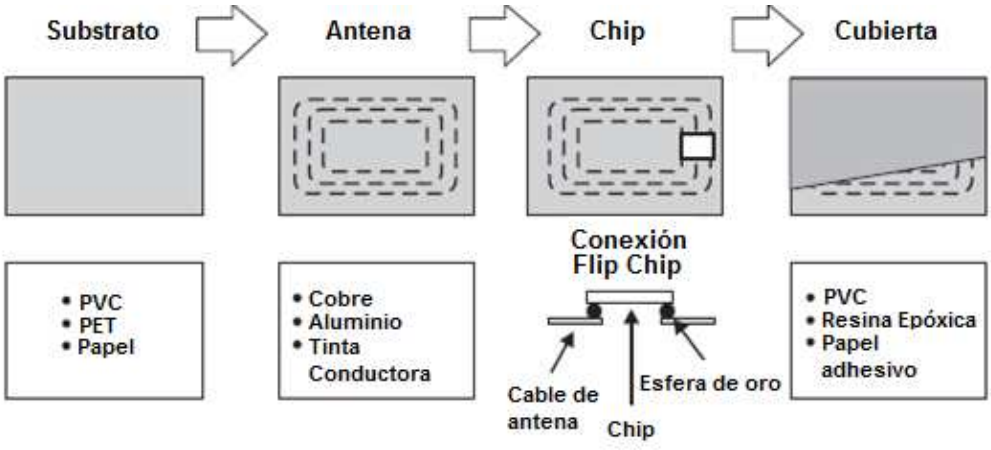


Figura 1.8: Proceso de construcción de los tags RFID [3]

1.6.2 COMPONENTES DE LOS TAGS RFID

Los tags están compuestos principalmente por un microchip y una antena. Adicionalmente puede incorporar una batería para alimentar sus transmisiones o incluso algunos tags más sofisticadas pueden incluir una circuitería extra con funciones adicionales de entrada/salida, tales como registros de tiempo u otros estados físicos que pueden ser monitorizados mediante sensores apropiados (de temperatura, humedad, etc.).

El microchip incluye:

- Una circuitería analógica que se encarga de realizar la transferencia de datos y de proporcionar la alimentación.
- Una circuitería digital que incluye:
  - La lógica de control.
  - La lógica de seguridad.
  - La lógica interna o microprocesador.
- Una memoria para almacenar los datos.

La antena que incorporan los tags para ser capaces de transmitir los datos almacenados en el microchip puede ser de dos tipos:

- Un elemento inductivo (bobina).
- Un dipolo.

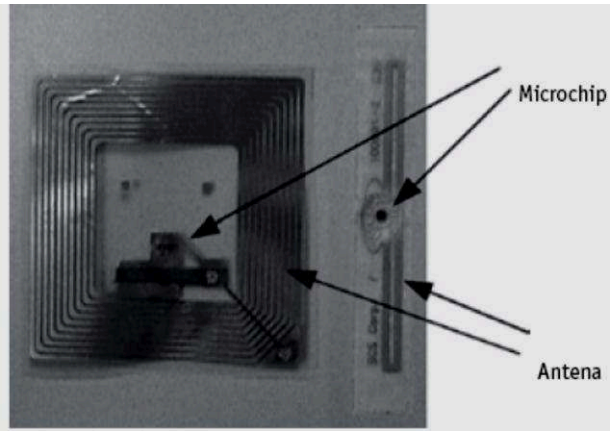


Figura 1.9: Componentes de un tag RFID [6]

1.6.3 TIPOS DE TAGS RFID

Los tags tienen características o capacidades muy diferentes, por lo que tiene múltiples clasificaciones que ayudan a entender cómo afectan a su comportamiento o modo de trabajo. Se clasifican según su topología (activo, pasivo y semipasivo), por su tipo de memoria, capacidad de almacenamiento, frecuencias de trabajo, características físicas, protocolo de interfaz aérea (cómo se comunica con el equipo lector) y así sucesivamente.

Clasificar los tags permite obtener una guía para encontrar el mejor tipo de tag para cada una de las aplicaciones o proyectos. La elección del tag adecuado es un factor clave para garantizar el éxito de la aplicación RFID y su aportación a los procesos productivos.

1.6.3.1 Tags Pasivos[8]

Los tags pasivos no poseen ningún tipo de alimentación. La señal que les llega de los lectores induce una corriente eléctrica mínima que basta para operar el circuito integrado del tag para generar y transmitir una respuesta. La mayoría de tags pasivos utiliza backscatter (reflexión de ondas, partículas o señales de vuelta a la dirección donde vinieron) sobre la portadora recibida. Esto es, la antena está

diseñada para obtener la energía necesaria para funcionar y a la vez para transmitir la respuesta por backscatter. Esta respuesta puede ser cualquier tipo de información, no sólo un código identificador.

Los tags pasivos suelen tener distancias de uso práctico comprendidas entre los 10 cm y llegando hasta unos pocos metros según la frecuencia de funcionamiento, el diseño y tamaño de la antena. Por su sencillez conceptual son obtenibles por medio de un proceso de impresión de las antenas. Como carecen de autonomía energética el dispositivo puede resultar muy pequeño: pueden incluirse en una pegatina o insertarse bajo la piel (tags de baja frecuencia).

Figura 1.10: Tag RFID Pasivo [4]

1.6.3.2 Tags Activos[8]

Los activos poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estos tags son mucho más fiables (tienen menos errores) que los pasivos debido a su capacidad de establecer sesiones con el lector. Gracias a su fuente de energía son capaces de transmitir señales más potentes que las de los tags pasivos, lo que les lleva a ser más eficientes en entornos dificultosos para la radiofrecuencia como el agua (incluyendo humanos y ganado, formados en su mayoría por agua), metal (contenedores, vehículos). También son efectivos a distancias mayores pudiendo generar respuestas claras a partir de recepciones débiles. Por el contrario, suelen ser mayores y más caros, y su vida útil es en general mucho más corta.

Muchos tags activos tienen rangos efectivos de cientos de metros y una vida útil de sus baterías de hasta 10 años. Algunos de ellos integran sensores de registro de temperatura y otras variables que pueden usarse para monitorizar entornos de alimentación o productos farmacéuticos.

Figura 1.11: Tag RFID Activa [5]

1.6.3.3 Tags Semipasivos[8]

Los tags semipasivos poseen una fuente de alimentación propia, aunque en este caso se utiliza principalmente para alimentar el microchip y no para transmitir una señal. La energía contenida en la radiofrecuencia se refleja hacia el lector como en un tag pasivo. Un uso alternativo para la batería es almacenar información propagada desde el lector para emitir una respuesta en el futuro, típicamente usando el método de backscattering (dispersión de un haz lumínico en sentido opuesto al de avance). Los tags sin batería deben responder reflejando energía de la portadora del lector.

La batería permite al circuito integrado del tag estar constantemente alimentado y eliminar la necesidad de diseñar una antena para recoger potencia de una señal entrante. Por ello, las antenas pueden ser optimizadas para utilizar métodos de backscattering. Los tags RFID semipasivas responden más rápidamente, por lo que son más fuertes en el radio de lectura que las pasivas.

Este tipo de tags tienen una fiabilidad comparable a la de los tags activos a la vez que pueden mantener el rango operativo de un tag pasivo. También suelen durar más que los tags activos.

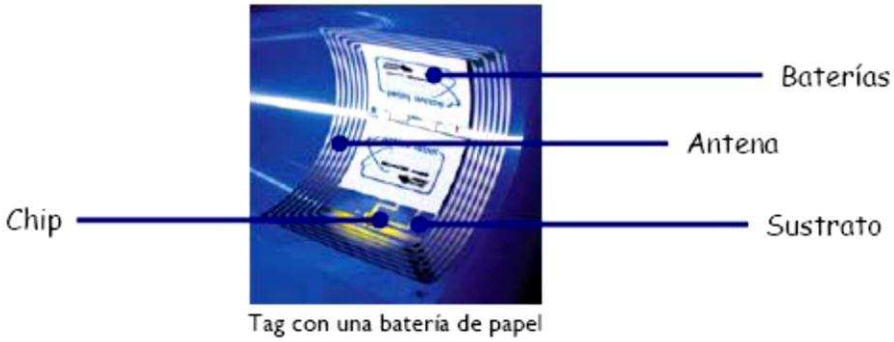


Figura 1.12: Tag RFID Semipasiva [7]

1.7 LECTOR RFID

Es el dispositivo que proporciona energía a los tags, lee los datos que le llegan de vuelta y los envía al sistema de información. Así mismo, también gestiona la secuencia de comunicaciones con el lector.

Con el fin de cumplir tales funciones, está equipado con un módulo de radiofrecuencia (transmisor y receptor), una unidad de control y una antena.

Además, el lector incorpora un interfaz a un PC, *host* o controlador, a través de un enlace local o remoto: RS232, RS485, Ethernet, Bluetooth, etc., que permite enviar los datos del tag al sistema de información.

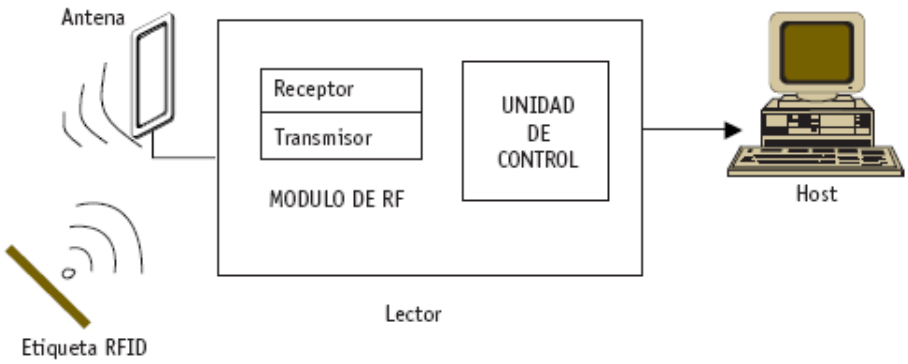


Figura 1.13: Esquema de un lector RFID [6]

El lector puede actuar de tres modos:

- Interrogando su zona de cobertura continuamente, si se espera la presencia de múltiples tags pasando de forma continua.
- Interrogando periódicamente, para detectar nuevas presencias de tags.
- Interrogando de forma puntual, por ejemplo cuando un sensor detecte la presencia de un nuevo tag.

1.7.1 COMPONENTES DEL LECTOR

Los componentes del lector son: el módulo de radiofrecuencia (formado por el receptor y transmisor), la unidad de control y la antena.

1.7.1.1 Módulo de Radiofrecuencia

Consta básicamente de un transmisor que genera la señal de radiofrecuencia y un receptor que recibe, también vía radiofrecuencia, los datos enviados por los tags. Sus funciones por tanto son:

- Generar la señal de radiofrecuencia para activar el tag y proporcionarle energía.
- Modular la transmisión de la señal para enviar los datos al tag.
- Recibir y demodular las señales enviadas por el tag.

1.7.1.2 Unidad de Control

Está constituida básicamente por un microprocesador. En ocasiones, para aliviar al microprocesador de determinados cálculos, la unidad de control incorpora un circuito integrado ASIC (*Application Specific Integrated Circuit*), adaptado a los requerimientos deseados para la aplicación.

La unidad de control se encarga de realizar las siguientes funciones:

- Codificar y decodificar los datos procedentes de los tags.
- Verificar la integridad de los datos y almacenarlos.
- Gestionar el acceso al medio: activar los tags, inicializar la sesión, autenticar y autorizar la transmisión, detectar y corregir errores, gestionar el proceso de multilectura (anticolisión), cifrar y descifrar los datos, etc.
- Comunicarse con el sistema de información, ejecutando las órdenes recibidas y transmitiéndole la información obtenida de los tags.

Una de las funciones más críticas que debe realizar la unidad de control es gestionar el acceso al medio. Cuando se transmite información mediante una tecnología que no requiere contacto físico, existe la posibilidad de que aparezcan interferencias que provoquen cambios indeseados a los datos transmitidos y, en consecuencia, errores durante la transmisión. Para evitar este problema se utilizan procedimientos de comprobación (*checksum*[1]). Los más comunes son la comprobación de bits de paridad, comprobación de redundancia longitudinal (LRC, Longitudinal Redundancy Check) y comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check).

El número de tags que un lector puede identificar en un instante de tiempo depende de la frecuencia de trabajo y del protocolo utilizado. Por ejemplo, en la banda de Alta Frecuencia suele ser de 50 tags por segundo, mientras que en la banda de Ultra Alta Frecuencia puede alcanzar las 200 tags por segundo.

1.7.1.3 Antena[6]

Es el elemento que habilita la comunicación entre el lector y el tag. Las antenas están disponibles en una gran variedad de formas y tamaños. Su diseño puede llegar a ser crítico, dependiendo del tipo de aplicación para la que se desarrolle.

Este diseño puede variar desde pequeños dispositivos de mano hasta grandes antenas independientes. Por ejemplo, las antenas pueden montarse en el marco

[1] Es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corruptos.

de puertas de acceso para controlar el personal que pasa, o sobre una cabina de peaje para monitorizar el tráfico que circula.

La mayor parte de las antenas se engloban en alguna de las siguientes categorías:

- Antenas de puerta (uso ortogonal).
- Antenas polarizadas circularmente.
- Antenas polarizadas linealmente.
- Antenas omnidireccionales.
- Antenas de varilla.
- Dipolos o multipolos.
- Antenas adaptativas o de arrays.

Figura 1.14: Distintos tipos de antenas [6]

1.7.2 LECTORES FIJOS Y MÓVILES[6]

Los lectores pueden variar su complejidad considerablemente dependiendo del tipo de tag que tengan que alimentar y de las funciones que desarrollen. Una

posible clasificación los divide en fijos o móviles dependiendo de la aplicación que se considere.

Los dispositivos fijos se posicionan en lugares estratégicos como puertas de acceso, lugares de paso o puntos críticos dentro de una cadena de ensamblaje, de modo que puedan monitorizar los tags de la aplicación en cuestión.

Los lectores móviles suelen ser dispositivos de mano. Incorporan una pantalla LCD, un teclado para introducir datos y una antena integrada dentro de una unidad portátil. Por esta razón, su radio de cobertura suele ser menor.

Figura 1.15: Lector RFID fijo [6]

Figura 1.16: Lector RFID de mano [6]

1.8 CONECTIVIDAD EN SISTEMAS RFID

Para que el desarrollo de un sistema RFID sea exitoso, se debe tomar en cuenta la conectividad de red para lectores RFID a utilizarse.

Tradicionalmente los lectores RFID han usado las comunicaciones seriales RS-232, RS-485. En la actualidad los fabricantes de lectores están habilitando el uso de nuevas tecnologías como son el Ethernet y Wireless en sus dispositivos.

A continuación se describen brevemente las conectividades de red más utilizadas en sistemas RFID:

- RS-232: Este protocolo provee sistemas de comunicación confiables de corto alcance. Tiene ciertas limitantes como una baja velocidad de comunicación, que va de 9600 bps a 115.2 kbps. El largo del cable está limitado a 30 metros, no cuenta con un control de errores y su comunicación es punto a punto.

- RS-485: El protocolo RS-485 es una mejora sobre RS-232, ya que permite longitudes de cables de hasta 1200 metros. Alcanza velocidades de hasta 2.5 Mbps y es un protocolo de tipo bus lo cual permite a múltiples dispositivos estar conectados al mismo cable.

- Ehernet: Se considera como una buena opción, ya que su velocidad es más que suficiente para los lectores de RFID. La confiabilidad del protocolo TCP/IP sobre Ehternet asegura la integridad de los datos enviados y finalmente al ser la infraestructura común para las redes. En la mayoría de países desarrollados ya cuentan con una red de este tipo, lo que permite una instalación más sencilla y menos costo de integración.

- Wireless 802.11: Se utiliza en la actualidad en los lectores de RFID móviles. Esta solución reduce los requerimientos de cables y por lo tanto de costos.

1.9 ESTÁNDARES DE LA TECNOLOGÍA RFID

Dentro del proceso de estandarización de la tecnología RFID tienen una gran importancia los organismos que desarrollan los diferentes estándares con los que operan los dispositivos RFID. Los estándares están diseñados para una óptima operación del sistema RFID con respecto a otros equipos eléctricos y de radio, además de garantizar la interoperabilidad entre diferentes lectores y tags. Los estándares de RFID abordan cinco áreas fundamentales:

- Protocolo de comunicación
- Contenido de los datos
- Aplicaciones
- Tipos de modulación de la señal
- Velocidad de transmisión de los datos

Algunos de estos organismos son el Instituto Europeo de Normas de Telecomunicaciones ETSI (*European Telecommunications Standards Institute*), la EPCglobal *(Electronic Product Code)* y la Organización Internacional de Normalización ISO (*International Standarization Organization*), dedicados al desarrollo de estándares como:

- ISO 10536: Mapas de identificación
- ISO 14443: Sistemas de proximidad (tarjetas sin contacto).
- ISO 15693: Tarjetas de vecindad (Vicinity Cards 1-1.5m, 13.56 Mhz). Tarjetas que pueden ser leídas, desde una mayor distancia que las tarjetas de proximidad.
- ISO 18000: Para las etiquetas (Tags de RFID). Interfaz de radio.
- EPC: Código electrónico de producto, estándar que tiene la mayor probabilidad de implementarse a nivel mundial.

1.10 APLICACIONES DE LA TECNOLOGÍA RFID

A continuación se describen en detalle algunas de las aplicaciones más utilizadas en la actualidad y en las que se detecta un mayor beneficio por la aplicación de la tecnología RFID.

1.10.1 GESTIÓN DE ALMACÉN INTELIGENTE

La automatización de la gestión de almacén mediante el uso de la tecnología RFID, implica una mejora substancial en todo el proceso, puesto que está fundamentada en la reducción de los tiempos de inventariado y la optimización de los stocks, lo que facilita las decisiones de producción adecuándolas a las necesidades reales. De esta forma se puede conseguir un importante ahorro de espacio de almacenaje.

Los elementos típicos de la gestión RFID del almacén son:

- Puestos de etiquetado para identificar los productos que no lleven el etiquetado en origen.

- Terminales móviles para identificación de productos con conectividad inalámbrica al sistema de información central.

- Portales fijos para la lectura de tags RFID, ubicados en las zonas de entrada y salida de productos.

Un sistema típico dispone de equipos de lectura RFID móviles, que se encargan de identificar y verificar la correcta localización y estado de los productos almacenados, contrastando la información con las bases de datos correspondientes del sistema de información, y actualizándola en caso necesario.

Las funcionalidades y capacidades que se ven notablemente mejoradas por la aplicación de la tecnología RFID son:

- Identificación de productos
- Identificación de ubicación
- Gestión de ubicación
- Gestión de inventarios
- Localización selectiva del producto
- Gestión dinámica de stock e intercambio de información con los proveedores y clientes.

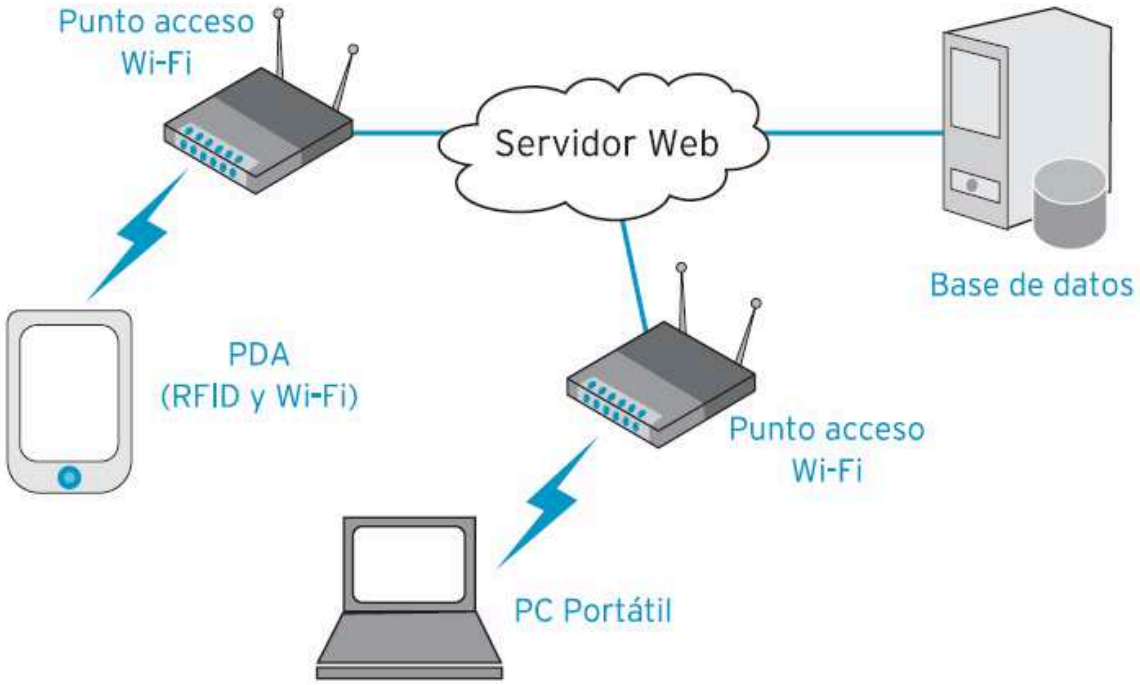


Figura 1.17: Sistema de Gestión basado en RFID [8]

1.10.2 IDENTIFICACIÓN DE PERSONAS[8]

Aunque el tema de privacidad es crítico en este tipo de aplicaciones, existe un gran número de soluciones de identificación de personas, sobretodo enfocadas al aumento de la seguridad.

En el año 2000, la International Civil Aviation Organization (ICAO) comenzó la evaluación de la tecnología RFID en chips sin contacto y su aplicación al pasaporte para identificar personas y evitar la suplantación o falsificación de identidad.

Finalmente Estados Unidos impuso a todos los países del VWP5 la implementación del pasaporte electrónico basado en RFID antes del 26 de Octubre de 2006. Es a partir de estos mandatos de los gobiernos cuando se extiende el uso de la tecnología RFID de forma masiva para la identificación de ciudadanos en tránsito procedentes de otros países. La adopción de la tecnología RFID junto con técnicas de autenticación y cifrado en los documentos de identificación permite identificar personas de forma segura evitando la falsificación y la suplantación de identidad.

Una de las aplicaciones de identificación de personas mediante RFID más utilizada es la identificación de pacientes en centros sanitarios.

Uno de los factores claves para el aumento de la seguridad de los pacientes en el ámbito hospitalario es la identificación correcta. Los eventos adversos asociados a la identificación incorrecta del paciente son un riesgo para la seguridad de los mismos durante su tratamiento. Para dotar al personal sanitario de una herramienta fiable de identificación que ayude a minimizar los riesgos asociados al proceso, se utilizan soluciones basadas en la tecnología RFID, con el que cada paciente es identificado de forma unívoca y segura, por ejemplo mediante pulseras que incorporan un chip RFID que almacena la información del paciente.

Figura 1.18: Identificación de paciente mediante pulsera RFID [8]

1.10.3 EDUCACIÓN

El uso más arquetípico de la RFID en la educación es en las bibliotecas, en donde este tipo de tecnología contribuye a:

- Reemplazar el sistema de código de barras.
- Simplificar los procedimientos para prestar o devolver material.
- Mejorar los sistemas de detección anti robo.
- Agilizar los procesos de inventario y facilitar la identificación de materiales que están fuera de su lugar.

Figura 1.19: Aplicación del sistema RFID en las bibliotecas [9]

CAPÍTULO 2

DISEÑO DEL HARDWARE

En el presente capítulo se realiza una descripción detallada de cada uno de los elementos usados en el diseño y construcción del módulo de control de acceso para los armarios de CNT en la ciudad de Ambato.

2.1 DIAGRAMA DE BLOQUES DEL SISTEMA

En el siguiente esquema se aprecia cómo están distribuidos los dispositivos utilizados en el desarrollo del módulo de control de acceso para los armarios telefónicos:

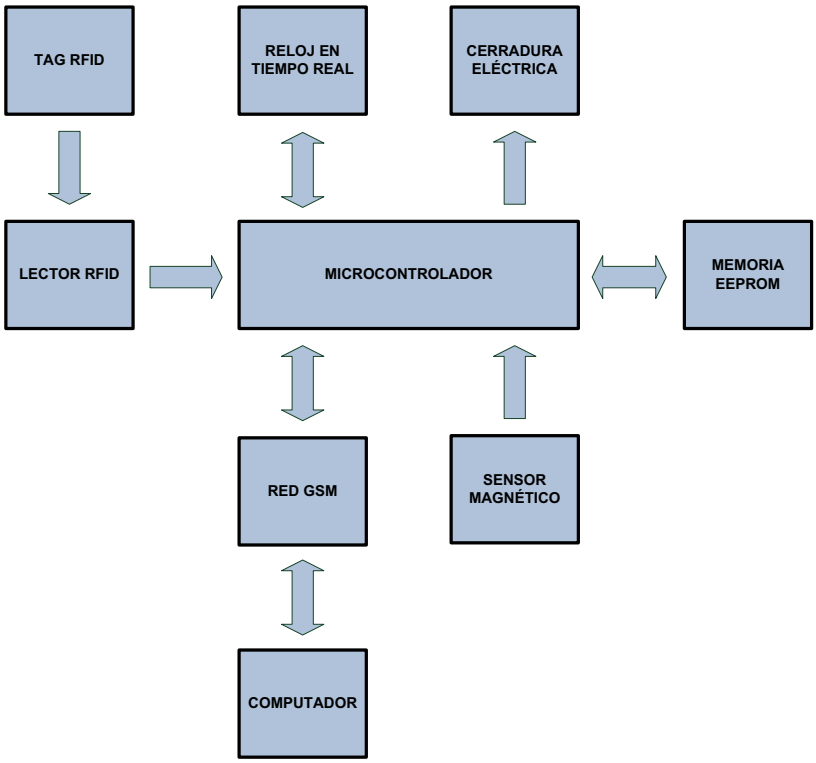


Figura 2.1: Diagrama de bloques

El diagrama de bloques mostrado en la figura 2.1 detalla el funcionamiento del proyecto. Para esto se tiene un elemento de control, el microcontrolador que realiza el manejo de todo el sistema. El reloj en tiempo real entrega la fecha y hora al sistema. El lector RFID entrega al microcontrolador los datos de lectura procedentes de los tags. Se dispone de un sensor magnético para enviar una señal al microcontrolador de apertura de la puerta. La memoria EEPROM recolecta toda la información del acceso como respaldo, la cual posteriormente es transmitida hacia el computador mediante dos modems GSM (transmisor y receptor). También se cuenta con una cerradura eléctrica que es accionada por el microcontrolador.

2.2 DESCRIPCIÓN DE LOS ELEMENTOS UTILIZADOS

2.2.1 LECTOR RFID ID-20

Este es un lector RFID muy sencillo de usar; tiene una antena incorporada. Al alimentar el lector y acercar un tag RFID, devuelve su código de identificación mediante su puerto serial, y además activa un pin al que se le puede conectar un led o un buzzer para indicar que se acaba de hacer una lectura. Es compatible con el puerto serial (UART) de muchos microcontroladores.

Las características más importantes se describen a continuación:

- Alimentación: 5V
- Frecuencia de lectura: 125kHz
- Compatible con tags EM4001
- Conexión serial: 9600bps TTL y RS232
- Distancia de lectura: 12 a 16 cm aproximadamente
- Dimensiones: 38x70x7mm
- Salida de emulación de banda magnética

Figura 2.2: Lector RFID ID-20 [15]

Para mayor detalle, en el anexo A se adjunta el datasheet del lector ID20 respectivamente.

2.2.2 TAG RFID

Como el lector trabaja a 125KHz se necesitan tags que operen a ese valor de frecuencia.

El tag adecuado para este trabajo es el de la serie EM4001. Es de bajo costo y fácil de utilizar. Existe en varios modelos; se puede poner fácilmente en el cinturón con un clip o en el bolsillo; tiene una gama variada de aplicaciones tales como, el control de acceso en oficinas, industrias o complejos de departamentos. Sus principales características son las siguientes:

- Basada en EM4001 ISO
- Frecuencia de 125kHz
- Codificación Manchester
- Resistente plástico PVC
- ID único de 32-bit

Como este tipo de tarjetas se rigen bajo la norma ISO 7816, que es un estándar internacional relacionado con las tarjetas de identificación electrónicas; estas normas tienen un apartado en el cual se garantiza que no existan dos tarjetas con el mismo código aunque sean de diferentes fabricantes.

Figura 2.3: Tag RFID EM4001 [16]

2.2.3 MODEM ZTE MG 3006

Es un tipo de modem GSM/GPRS inalámbrico compatible con cuádruple banda, SMS, funciones de servicios de datos, etc.

Entre sus principales aplicaciones podemos citar las siguientes: transmisión de datos, puntos de venta inalámbricos, supervisión de sistemas centrales de calefacción, administración de flotas, parquímetros, adquisición de datos hidrológicos, máquinas de distribución entre otras.

Figura 2.4: Modem ZTE MG3006 [17]

A continuación se describen las principales características del modem:

- Alimentación típica de 3.9 VDC
- Banda cuádruple GSM: 850/900/1800/1900MHZ
- Soporta comandos AT estándar y extendidos.

- Posee reloj en tiempo real (RTC)
- Fiable conectividad de red GSM, proporcionando un rápido y amplio rango de comunicación inalámbrica.
- Cubierta de acero para evitar interferencia electromagnética.

En el Anexo B se adjunta el datasheet de este elemento.

2.2.4 MICROCONTROLADOR ATMEGA 324P

El Atmega324P es un microcontrolador CMOS de 8 bits a baja potencia basado en arquitectura RISC de AVR. Ejecuta las instrucciones en un solo ciclo de reloj; el ATMEGA324P alcanza un desempeño de 1 MIPS (millones de instrucciones por segundo).

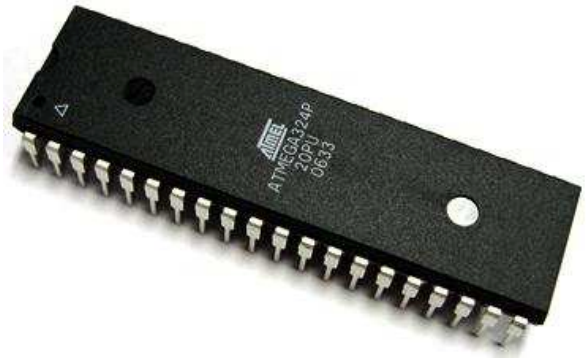


Figura 2.5: Microcontrolador Atmega324P [18]

Las instrucciones en la memoria de programas son ejecutadas con estructura segmentada, al mismo tiempo que una instrucción es ejecutada, se realiza la búsqueda de la próxima instrucción. Este concepto permite habilitar instrucciones para ser ejecutadas con cada ciclo de reloj.

Las características generales del ATMEGA324P son:

- 32K bytes de flash programable con la característica de ser de lectura y escritura.
- 1K byte de EEPROM, 2K bytes de SRAM

- 32 líneas I/O de propósito general
- 32 registros de propósito general
- Interrupciones internas y externas
- 8 canales A/D, de 10 bits
- Un puerto serial SPI
- Dos USART seriales programables
- Voltajes Operables de 2.7 – 5.5 V
- Un watchdog timer con oscilador interno

En la figura 2.5 se muestra la distribución de pines del microcontrolador ATMEGA324P:

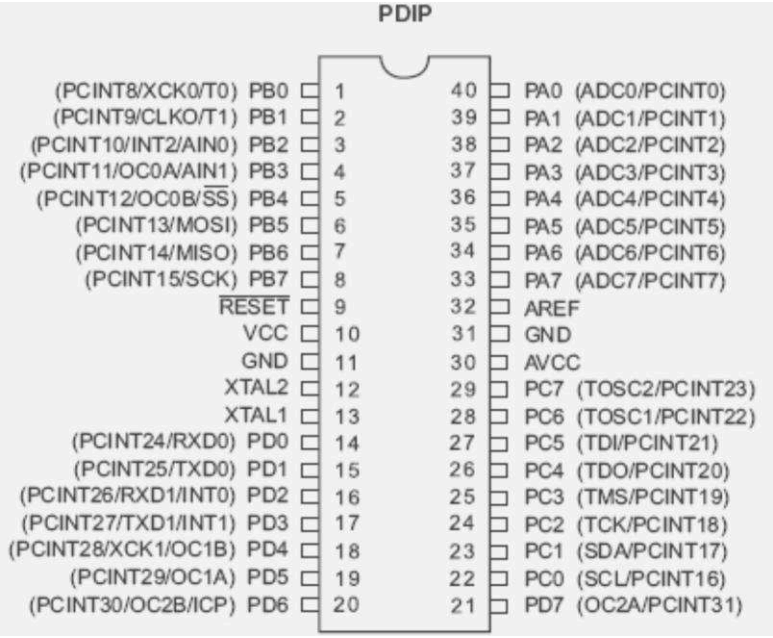


Figura 2.6: Diagrama de pines del Microcontrolador Atmega324P [19]

En el Anexo C se adjunta el datasheet de este elemento.

2.2.5 MEMORIA EEPROM[27]

La memoria EEPROM es programable y borrable eléctricamente y su nombre proviene de la sigla en inglés *Electrically Erasable Programmable Read Only Memory*. Actualmente estas memorias se construyen con transistores de

tecnología MOS (*Metal Oxide Silice*) y MNOS (*Metal Nitride-Oxide Silicon*). Las celdas de memoria en las EEPROM son similares a las celdas EPROM y la diferencia básica se encuentra en la capa aislante alrededor de cada compuesta flotante, la cual es más delgada y no es fotosensible.

Las memorias EEPROM son no volátiles y eléctricamente borrables a nivel de bytes. La posibilidad de programar y borrar las memorias a nivel de bytes supone una gran flexibilidad, pero también una celda de memoria más compleja. La programación requiere de tiempos que oscilan entre 157µs y 625µs. Frente a las memorias EPROM, presenta la ventaja de permitir su borrado y programación en placa, aunque tienen mayor coste debido a sus dos transistores por celda.

Las principales ventajas de estas memorias son:

- Las palabras almacenadas en memoria se pueden borrar de forma individual.
- Para borrar la información no se requiere luz ultravioleta.
- Las memorias EEPROM no requieren programador.
- De manera individual se puede borrar y reprogramar eléctricamente grupos de caracteres o palabras en el arreglo de la memoria.
- Para reescribir no se necesita hacer un borrado previo.
- Una ventaja adicional de este tipo de memorias radica en que no necesitan de una alta tensión de grabado, sirven los 5 voltios de la tensión de alimentación habitual.

Las memorias EEPROM que funcionan bajo el protocolo I2C han ganado poco a poco un espacio en el hardware de los equipos electrónicos hasta transformarse en uno de los medios de almacenamiento de información más populares por su practicidad y sencillez de manejo. Tener la posibilidad de almacenar datos de diversa índole en una memoria no volátil, es una característica importante de los equipos que les permite la desconexión prolongada de cualquier suministro energético y conservar durante mucho tiempo información valiosa que de otro modo, se perdería al desconectar un sistema. También conocidas como

memorias de protocolo “serie” las 24CXX son infaltables en cualquier equipo electrónico de consumo masivo.

Para el presente trabajo se ha elegido la memoria serial 24LC256 de Microchip.

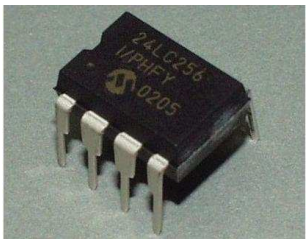


Figura 2.7: Memoria EEPROM 24LC256 [20]

Las principales características de la memoria 24LC256 son las siguientes:

- Tecnología CMOS de bajo consumo
- Corriente máxima para escritura: 3 mA (5V)
- Corriente máxima de lectura: 400 uA (5V)
- Corriente en reposo: 100 nA
- Interfaz de dos cables I2C
- Cascada de hasta 8 memorias
- Control interno automático del ciclo de lectura/escritura
- Paginación de 64-byte para páginas
- Velocidad de escritura: 5 ms máx.
- Protección de escritura por hardware
- Ciclos de borrado/escritura: 1.000.000
- Retención de datos: mayor a 200 años
- Encapsulado: 8-pin PDIP

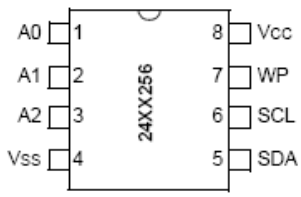


Figura 2.8: Diagrama de la memoria EEPROM 24LC256 [21]

La descripción de los pines son listados en la Tabla 2.1:

Nombre	8 pines PDIP	8 pines SOIC	8 pines TSSOP	8 pines MSOP	8 pines DFN	Función
A0	1	1	1	-	1	Chip configurable seleccionado por usuario
A1	2	2	2	-	2	Chip configurable seleccionado por usuario
(NC)	-	-	-	1,2	-	No conectado
A2	3	3	3	3	3	Chip configurable seleccionado por usuario
Vss	4	4	4	4	4	Tierra
SDA	5	5	5	5	5	Línea de datos
SCL	6	6	6	6	6	Línea de reloj
(NC)	-	-	-	-	-	No conectado
WP	7	7	7	7	7	Entrada de protección de escritura
Vcc	8	8	8	8	8	+1.8V - 5.5V (24AA256) +2.5V – 5.5V (24LC256) +1.8V – 5.5V (24FC256)

Tabla 2.1: Descripción de los pines de la memoria EEPROM 24LC256 [21]

En el Anexo D se adjunta el datasheet de este elemento.

2.2.6 RELOJ EN TIEMPO REAL DS1307

El DS1307 es un reloj de tiempo real exacto, el cual automáticamente, mantiene el tiempo y la fecha actual, incluyendo compensación para meses con menos de 31 días y saltos de año.

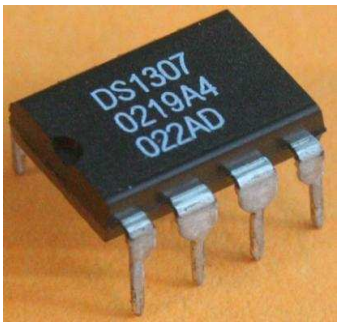


Figura 2.9: Reloj en tiempo real DS1307 [22]

Las principales características del DS1307 son las siguientes:

- Bajo consumo de energía, menos de 500nA en modo de respaldo con batería.
- Reloj en tiempo real que cuenta desde segundos hasta años, válido hasta el 2100.
- Interface serial I2C.
- Voltaje de alimentación de 5Vdc.

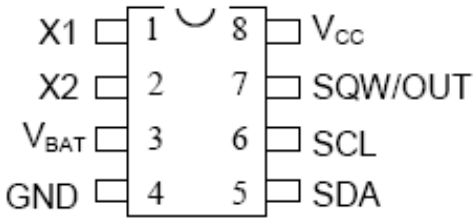


Figura 2.10: Diagrama de pines del Reloj en tiempo real DS1307 [22]

El DS1307 es un dispositivo de 8 pines al que se le conecta un cristal de cuarzo estándar, de bajo costo, a 32768kHz entre los pines 1 y 2 para generar los pulsos necesarios para que el conteo de tiempo sea exacto. Opcionalmente se le puede conectar al pin3 una batería de respaldo de 3 voltios, para asegurar que se mantendrá el tiempo a la fecha aunque se desconecte la fuente de tensión del circuito principal. El circuito integrado automáticamente detecta que se ha removido la energía en el circuito principal y se conecta la batería de respaldo cuando es requerido; la misma que puede durar hasta 10 años.

Adicionalmente el circuito integrado DS1307 tiene dos características interesantes. El pin 7 es una salida de colector abierto, que puede ser programada para hacer “flash” cada 1Hz. Esto permite la colocación de un led como indicador de segundos en aplicaciones de reloj. El circuito integrado también tiene 56 bytes de memoria RAM para propósito general.

Para reconocer al elemento en el bus I2C se utiliza una dirección de esclavo, la cual es fija dada por el fabricante: 11010000. En el Anexo E se adjunta el datasheet de este elemento.

2.2.7 SENSOR MAGNÉTICO

Este dispositivo es un interruptor, que a diferencia de actuar sobre él manualmente, se hace magnéticamente. Es decir; se activa cuando un imán se le aproxima y se desactiva, cuando este se aleja. Consta de dos elementos:

- Soporte electrónico
- Soporte magnético

El soporte electrónico, incorpora en su interior, los mecanismos que harán abrir o cerrar un circuito, algo similar a un relé. El soporte magnético, tiene en su interior dos imanes polarizados de forma que su campo se dirija de forma adecuada.

Figura 2.11: Sensor magnético [24]

2.2.8 CERRADURA ELÉCTRICA

Es el elemento que permite el acceso a la puerta del armario telefónico. Para el presente proyecto se escoge una electrochapa la cual consiste en el accionamiento de un vástago eléctrico. Este tipo de cerradura es la más apropiada, debido a que las cerraduras normales son muy gruesas para la puerta del armario. Además de que el mismo está fabricado de fibra de vidrio, lo que conllevaría un significativo daño al momento de la instalación de una cerradura eléctrica común. Funciona con un voltaje de 12Vdc. La misma se acciona al recibir la señal del relé y posteriormente el vástago retorna a su posición original por efecto del resorte.

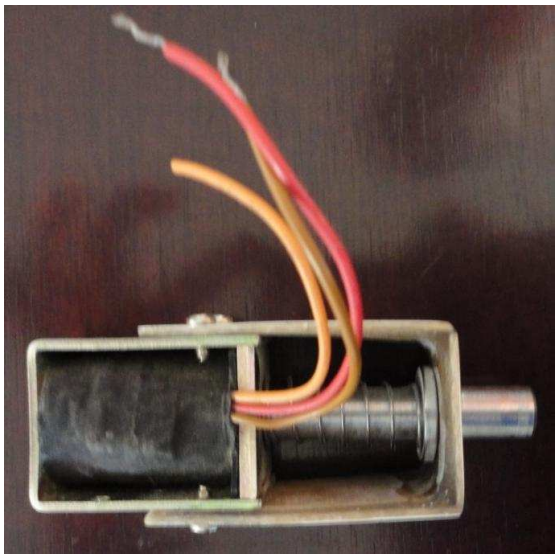


Figura 2.12: Electrochapa

2.3 DISEÑO DE LOS CIRCUITOS

Una vez que se ha descrito las características técnicas de todos los dispositivos utilizados en el proyecto, se diseña el diagrama de los circuitos que conforman el sistema a implementarse. Se explica por partes debido a que cada uno de los dispositivos que componen el sistema requiere una conexión específica.

2.3.1 DISPOSITIVOS I2C

En este bus I2C van a ir conectados la memoria EEPROM 24LC256 y el reloj en tiempo real DS1307. Además en esta sección se usan los pines de línea de datos y reloj (SDA Y SCL respectivamente). Estos respectivos pines deben estar en estado alto para que tenga un adecuado funcionamiento, por ello se debe conectar resistencias de pull-up, que gracias a las mismas permiten conectar en paralelo varias entradas y salidas.

En la práctica se recomienda utilizar un intervalo de valores de las resistencias de pull-up, el cual va desde 4.7KΩ hasta 10KΩ, para el presente proyecto se ha optado colocar resistencias de 4.7KΩ, obteniendo excelentes resultados.

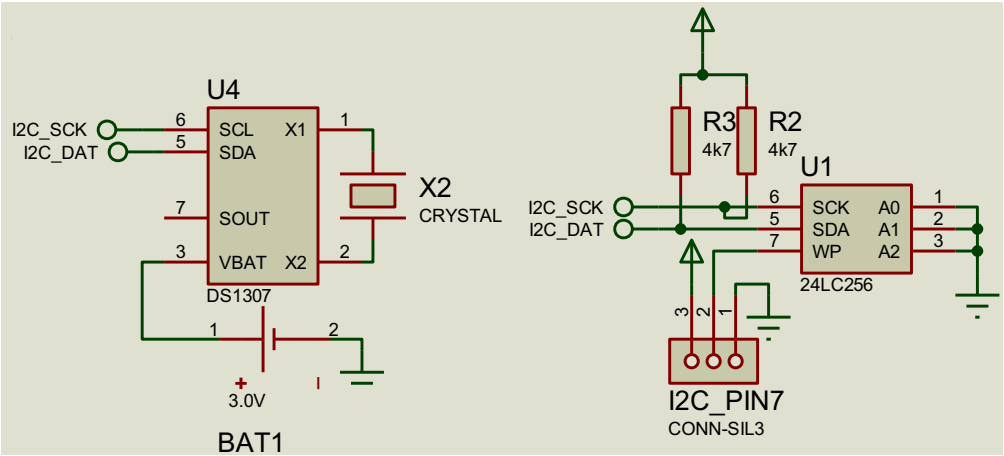


Figura 2.13: Diagrama de conexión de los dispositivos I2C

Para la conexión de la memoria, los pines A0, A1 Y A2 deben estar conectados a tierra porque no se van a usar, debido a que los mismos son utilizados cuando se tiene 2 o más memorias y estos pines sirven para realizar el direccionamiento. El pin WP debe estar conectado en bajo para poder escribir y leer en la memoria. Para el caso del DS1307 se conectan las líneas de datos y de reloj al bus serial I2C; además del cristal de 32768 Khz y la batería de respaldo de litio de 3V.

2.3.2 CONEXIÓN DEL MODEM GSM

La conexión de este dispositivo se da por medio del circuito integrado MAX232 con la configuración dada en la figura 2.14, la cual sugiere el fabricante, los capacitores pueden ser desde 1 a 10uF.

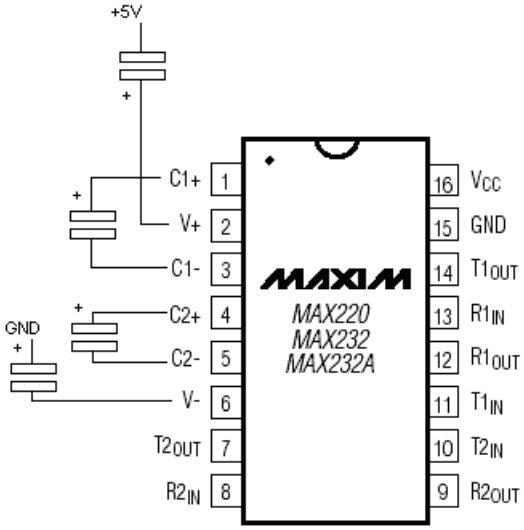


Figura 2.14: Configuración del MAX232[23]

El microcontrolador utiliza los pines de transmisión y recepción para comunicarse con el MAX232, y éste se conecta al modem GSM por medio de sus pines de salida.

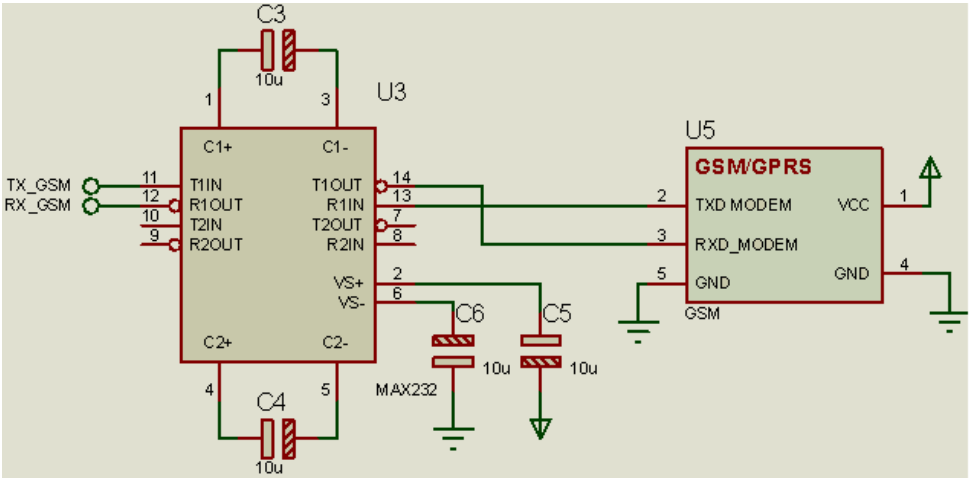


Figura 2.15: Diagrama de la conexión hacia el Modem GSM

2.3.3 CONEXIÓN DEL LECTOR RFID

El hardware del lector RFID está armado de acuerdo a la configuración sugerida por el fabricante, la cual se encuentra en el datasheet de este dispositivo. El mismo está compuesto del lector RFID, resistencias, un transistor, un capacitor, un buzzer y un diodo led, el cual actúa paralelamente al buzzer, indicando si el lector está o no leyendo el tag. El diodo led siempre debe estar conectado a través de una resistencia que limite su corriente, la resistencia R9 se calcula con la corriente de polarización y el voltaje de alimentación. Los valores típicos de corriente directa de polarización están comprendidos entre los 10 y 20mA.

$$R_l = \frac{E}{I_l} = \frac{5V}{10mA} = 500\Omega$$

Se utiliza una resistencia estándar de 470Ω. Para el cálculo de R19 que es la resistencia de base del transistor 2N3904 se la calcula con la corriente mínima en la base y es dato del fabricante:

$$Rb = \frac{Vcc}{Ib} = \frac{5V}{5mA} = 1K\Omega$$

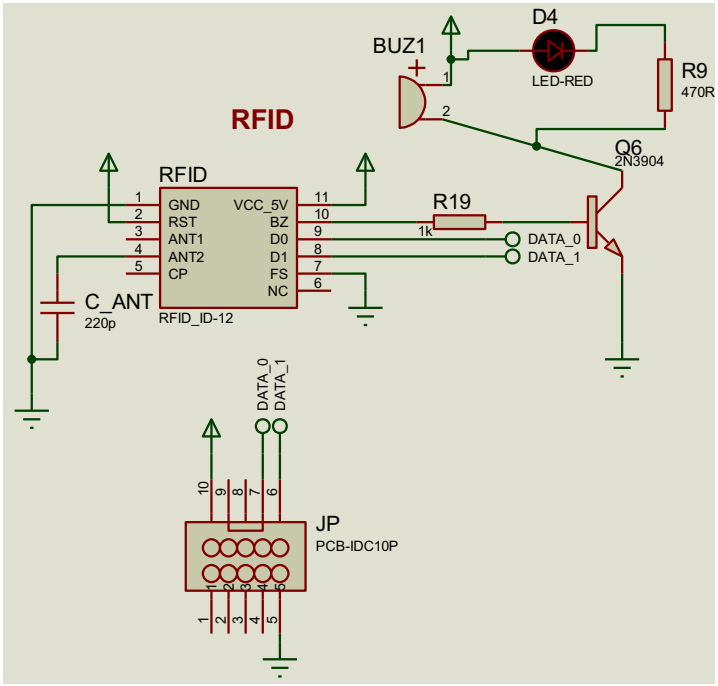


Figura 2.16: Diagrama de conexión del hardware externo del lector RFID

Cabe mencionar que el hardware del lector RFID, es colocado en la puerta del armario, por lo que la placa del mismo es externa y se comunica con la placa principal por medio de un bus de datos y un conector IDC(Conector por desplazamiento de aislante).

En el hardware de la placa principal se utiliza el conector IDC y una bornera, en la cual van a estar los pines DATA0 y DATA1 que son los encargados de transmitir los distintos datos de información del tag hacia el lector, y el pin RX_RFID que va a transmitir los datos unificados del tag hacia el microcontrolador.

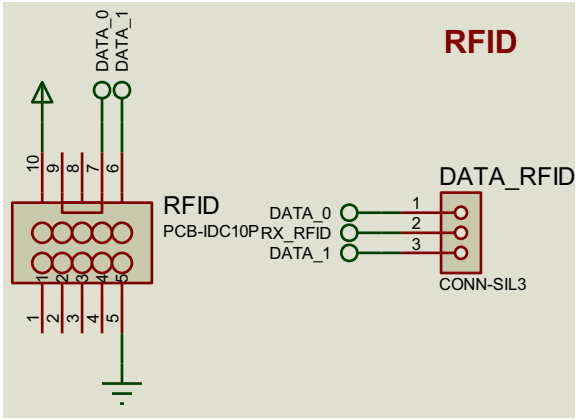


Figura 2.17: Diagrama de conexión del lector RFID

2.3.4 ELEMENTOS EN EL MICROCONTROLADOR

El microcontrolador es el encargado de gobernar todos los procesos que se dan en el circuito, por lo que se realiza la conexión de los siguientes elementos:

Un oscilador externo X1, el cual necesita el modem GSM para su correcto funcionamiento, su frecuencia de oscilación es de 11.0592 Mhz.

Un circuito de reset, en el que se coloca una resistencia de 10kΩ, que lo pone en alta impedancia al pin de reset del microcontrolador hasta que el pulsador sea presionado y envíe 0V, en este momento R1 impide el cortocircuito entre Vcc y tierra.

Un relé el cual permite el accionamiento de la cerradura eléctrica de 12Vdc, el respectivo circuito consta de un diodo paralelo a la bobina del relé, un transistor 2N3904 con su respectiva resistencia de base la cual se la calcula como el procedimiento realizado para la resistencia R1 en el circuito del lector RFID.

Se coloca los pines de transmisión y recepción del modem GSM TX_GSM y RX_GSM; el pin de recepción de datos del lector RFID: RX_RFID y las entradas del bus serial I2C: I2C_DAT y I2C_SCK. Además de tres diodos led; dos de ellos corresponden a la configuración del modem GSM y el tercero indica la apertura de la puerta.

Una entrada para el sensor magnético con una resistencia de pull up de 4.7KΩ, adicionalmente en el microcontrolador se incorpora 6 pines para la entrada del grabador ISP del microcontrolador.

A continuación se muestra el circuito de todos los elementos que intervienen en el microcontrolador:

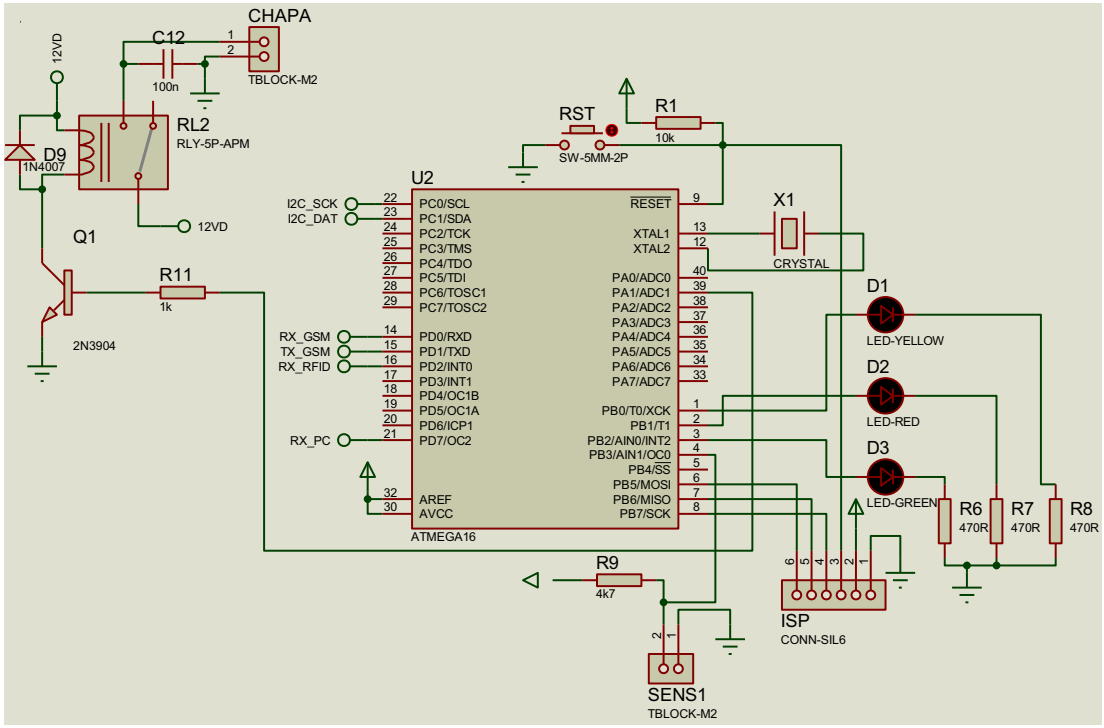


Figura 2.18: Diagrama de conexión de los elementos en el microcontrolador

2.3.5 ALIMENTACIÓN DEL SISTEMA

La fuente de alimentación abastece a todos los dispositivos que conforman el Módulo de control de acceso a los armarios telefónicos, por lo que se tiene en cuenta la energía que consume todo el sistema, para escoger adecuadamente que tipo de fuente utilizar.

A continuación se muestra una tabla en la cual se detalla el consumo de corriente de los diferentes dispositivos que conforman el sistema:

DISPOSITIVO	CANTIDAD	CONSUMO DE CORRIENTE
Microcontrolador ATMEGA 324P	1	200 mA
Memoria EEPROM 24LC256	1	3 mA
Reloj en tiempo real DS1307	1	1.5 mA
Modem GSM ZTE MG3006	1	250 mA
Lector RFID ID-20	1	65 mA
Circuito Integrado MAX232	1	4 mA
Diodo Led	3	30 mA
Otros	-	50 mA
Total		**603.5 mA**

Tabla 2.2: Consumo total de corriente del sistema

Por lo tanto se obtiene como resultado un consumo de aproximadamente 600 mA; entonces se necesita una fuente de alimentación de por lo menos 1 A.

La fuente de alimentación satisface los requerimientos de voltaje y corriente que el sistema necesita, además proporciona el voltaje adecuado para el funcionamiento del circuito de control.

Figura 2.19: Fuente de alimentación

Sus principales características son las siguientes:

- Voltaje de entrada: 120Vac
- Voltaje de salida: 12Vdc
- Corriente: 2A
- Entrega un voltaje estable en la línea, con menos cantidad de ruido.
- Libre de cualquier interferencia y protegida contra transitorios de sobrevoltaje, puesto que posee los filtros y reguladores adecuados.
- Cubierta metálica para evitar cualquier inducción hacia los cables telefónicos.

La fuente tiene una salida de 12Vdc, pero para el circuito de control se necesitan de voltajes en el orden de los 5Vdc, por tal motivo se ha diseñado en la placa de control una pequeña fuente regulable para alimentar todos los dispositivos que se encuentran en la misma.

En el circuito de la fuente regulable consta una bornera que es la entrada de la fuente de 12Vdc, seguida de un puente de diodos que protege al circuito en caso de conectar la polaridad incorrecta; aquí también se ha incluido el circuito de respaldo, el mismo que consta de un relé que conmutará a la batería en caso de interrupción de la energía eléctrica. La fuente regulable consta del circuito integrado LM317T, que se encarga de regular el voltaje proporcionado por la fuente de 12Vdc, además de los capacitores a la entrada y salida para un buen

funcionamiento y absorber posibles picos de corriente. El ajuste se lo realiza por medio de un potenciómetro.

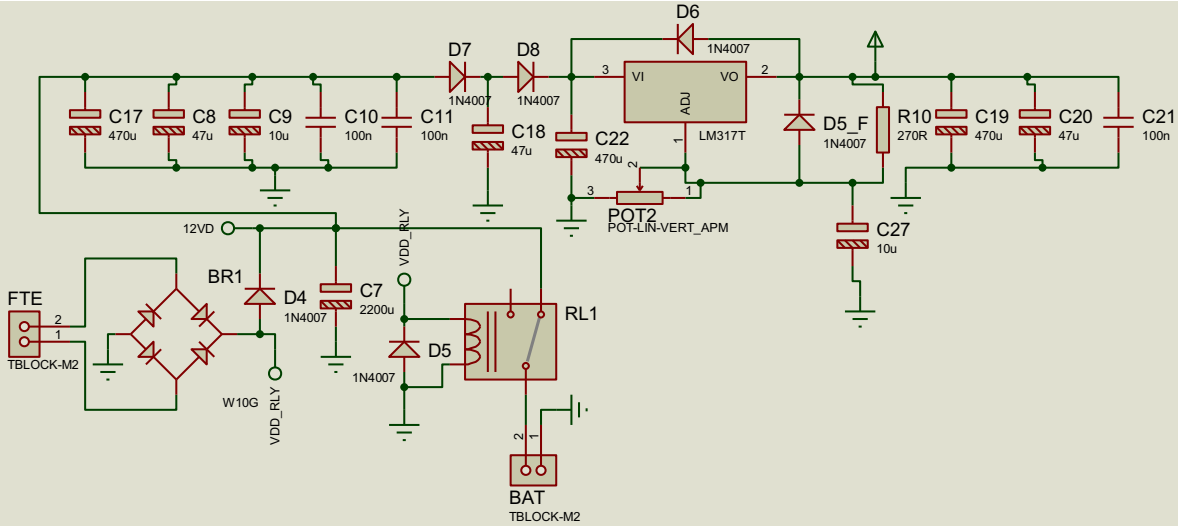


Figura 2.20: Diagrama de conexión de la fuente regulable y circuito de respaldo

2.3.6 DIAGRAMA GENERAL DEL SISTEMA

Una vez indicado la conexión de cada uno de los elementos utilizados en el presente proyecto, se procede a mostrar el circuito completo en la figura 2.21, además en el anexo E se encuentra el circuito impreso y los dispositivos montados en la placa de control.

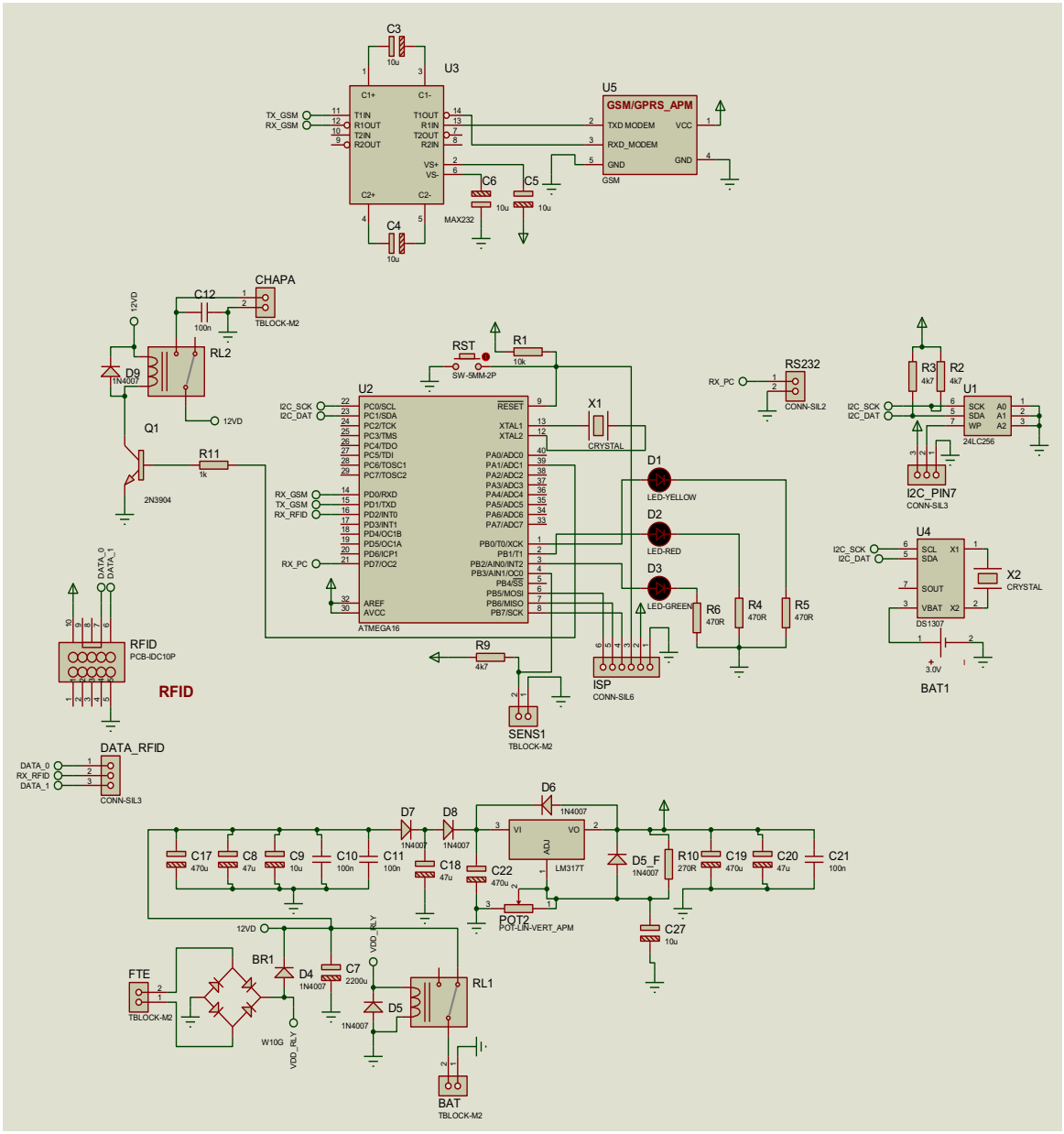


Figura 2.21: Diagrama general de conexiones

CAPÍTULO 3

DISEÑO DEL SOFTWARE

En este capítulo se explica el desarrollo del software utilizado para la interfaz y el microcontrolador.

3.1 PROGRAMACIÓN DEL MICROCONTROLADOR

La programación consiste en el desarrollo de las subrutinas del reloj en tiempo real DS1307, modem GSM, escritura y lectura de la memoria EEPROM. Para el software del microcontrolador se escoge un lenguaje de programación simple, eficaz, de bajo costo, y que se adapte a los requerimientos del proyecto.

La mejor opción seleccionada para el desarrollo de este prototipo, es el compilador BASCOM AVR, pues viene con rutinas elaboradas que facilitan la programación de los microcontroladores ATMEL AVR.

BASCOM AVR es un compilador BASIC en Windows para la familia de microcontroladores AVR. Está diseñado para trabajar en W95/W98/NT/XP/Vista/Seven. Está hecho para trabajar con la serie de microcontroladores de ATMEL AVR, pero BASCOM puede exportar un archivo de extensión hex o bin, con lo cual puede trabajar con microcontroladores que no sean de la familia ATMEL AVR. Para el presente trabajo se utiliza la versión demo de BASCOM-AVR, sin que haya existido problema alguno en la programación.[28]

Figura 3.1: Presentación del compilador BASCOM-AVR

Los comandos utilizados en BASCOM AVR son muy fáciles de recordar, en comparación con compiladores en C o similares. Soporta programadores USB, ISP, Serial; haciendo que este compilador sea muy útil y flexible.

3.1.1 COMUNICACIÓN I2C PARA EL RELOJ EN TIEMPO REAL DS1307

En el microcontrolador no es necesario implementar todo el protocolo I2C, ya que BASCOM AVR realiza esta labor. Por tal razón se debe configurar el bus definiendo los pines SDA (línea de datos) y SCL (línea de reloj) respectivamente.

Una vez que se ha configurado el bus I2C, se procede a configurar las direcciones para escritura y lectura de los datos del reloj calendario DS1307; a más de la librería del mismo.

Se configura el reloj para utilizar las variables Time$ y Date$; se recurre al argumento User para emplear un propio código de lectura y escritura del microcontrolador en combinación con el puerto de comunicación I2C del DS1307 y establecer el formato de la fecha:

```
Config Clock = User
Config Date = Ymd , Separator = /
```

Cada vez que se necesite trabajar con el tiempo y fecha en tiempo real, el compilador BASCOM utiliza subrutinas de temporización, las cuales pueden utilizarse en cualquier momento que se las requiera. Las variables para mostrar el tiempo y fecha son las siguientes:

Time$: Correspondiente al tiempo.
Date$: Correspondiente a la fecha.

A continuación se muestra el diagrama de flujo para la configuración del dispositivo DS1307:

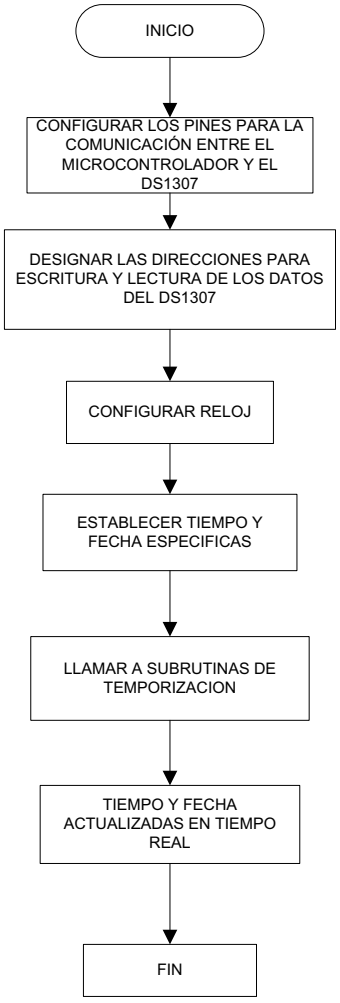


Figura 3.2: Diagrama de flujo de la configuración para el reloj en tiempo real DS1307

3.1.1.1 Subrutinas de Temporización

A continuación se realiza una breve descripción de las subrutinas de temporización utilizadas en la programación del reloj en tiempo real DS1307.

3.1.1.1.1 Subrutina Settime

En ella se transforma las variables establecidas de segundos, minutos y horas a BCD, debido a que para la comunicación I2C es necesario que los datos estén en BCD. A continuación se muestra su respectivo diagrama de flujo:

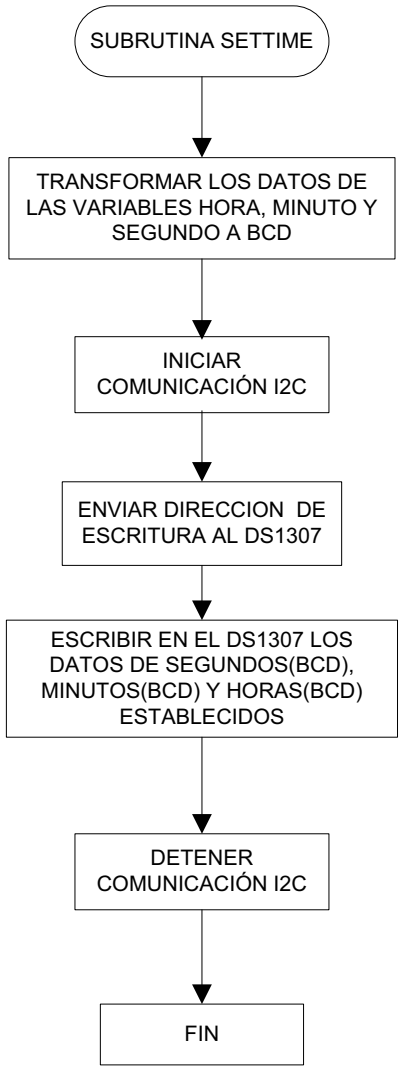


Figura 3.3: Diagrama de flujo de la Subrutina Settime

3.1.1.1.2 Subrutina Setdate

Esta subrutina trabaja con las variables correspondientes a la fecha: día, mes y año; y las transforma a BCD, debido a que para la comunicación I2C es necesario que los datos estén en BCD.

A continuación se muestra su respectivo diagrama de flujo:

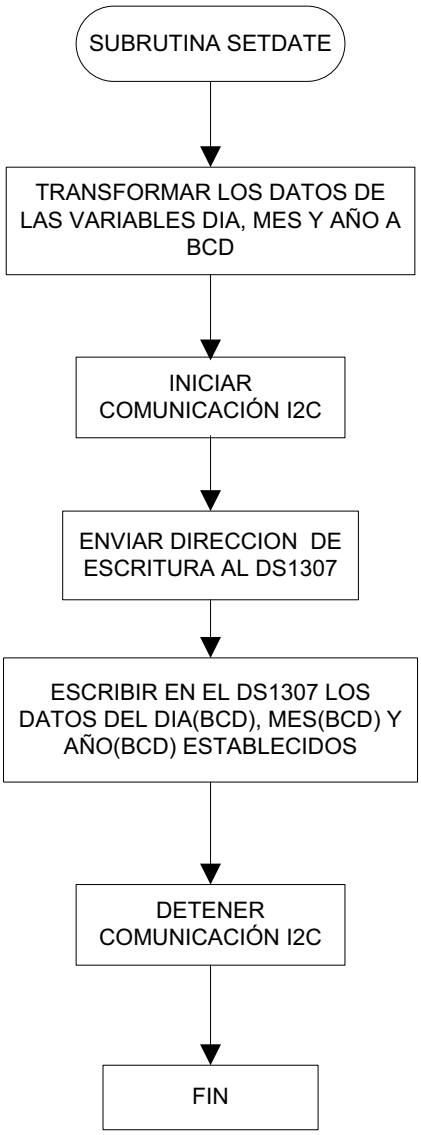


Figura 3.4: Diagrama de flujo de la Subrutina Setdate

3.1.1.1.3 Subrutina Getdatetime

Con esta subrutina se puede trabajar con los datos de la fecha (Date$) y la hora (Time$); ya que transforma las variables de valor BCD a decimal.

A continuación se muestra su respectivo diagrama de flujo:

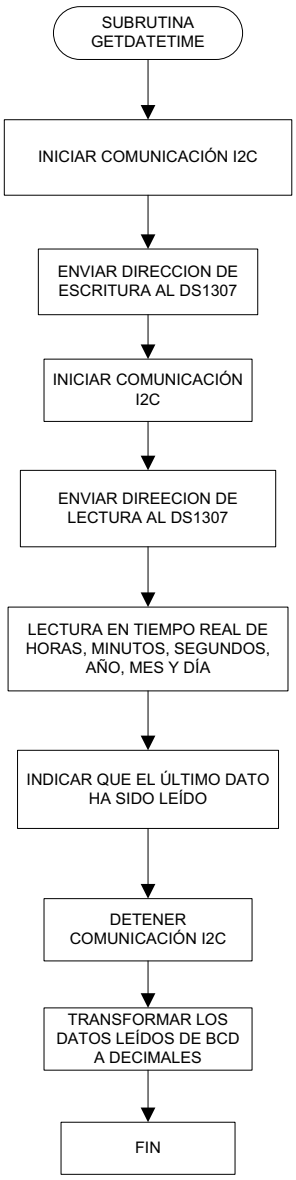


Figura 3.5: Diagrama de flujo de la Subrutina Getdatetime

3.1.2 MEMORIA EEPROM

Para el almacenamiento de la información de los eventos ocurridos durante el acceso al armario telefónico se cuenta con una memoria EEPROM 24LC256 no volátil, descrita en el capítulo anterior.

El modo de funcionamiento de la memoria es el siguiente: cuando este dispositivo envía el dato a través del bus SDA, el mismo es definido como transmisor

mientras que cuando la recibe, el bus es definido como receptor. El bus SDA es controlado por un dispositivo maestro el cual genera un reloj serial (SCL), que controla el acceso al bus y genera las condiciones de inicio y parada, mientras la memoria trabaja como esclavo.

3.1.2.1 Distribución de datos a almacenarse en la memoria

En el dispositivo se guarda la siguiente información:

- Número de evento
- Número asignado al código de la tarjeta.
- Fecha
- Hora de ingreso
- Hora de salida

Por los datos obtenidos en el datasheet de la memoria, la misma cuenta con 32Kbytes de almacenamiento, distribuidos en páginas de 64 bytes; lo que da como resultado 500 páginas de 64 bytes.

De acuerdo a la información que se necesita respaldar, se tiene que detallar la cantidad de bytes requeridos para después calcular el número de eventos que se pueden guardar. Evento es considerado la apertura y posterior cierre del armario; para lo cual en la siguiente tabla se especifican las variables a utilizarse:

Variable	Número de bytes
Número de evento	2
Número de código de la tarjeta	1
Fecha	3
Hora de ingreso	3
Hora de salida	3
Total	12

Tabla 3.1: Distribución de las variables a utilizarse en la memoria

Como se puede observar, se requiere 12 bytes por cada evento ocurrido; pero como las páginas de la memoria están distribuidas cada 64 bytes, se necesita tener un almacenamiento de cada evento con números múltiplos de 64, porque cada vez que se llene una página se debe mandar una señal de stop. Por tal razón se ha visto la necesidad de ocupar 16 bytes por cada evento; estos 4 bytes adicionales van a ser llenados con ceros.

Cabe mencionar que los códigos de las tarjetas son guardados en la memoria EEPROM del microcontrolador, ya que si se guardan en la memoria externa, ocupan mucho espacio en la misma y el historial de la información almacenada no sería significativo. Por ello, el código que tiene cada tarjeta es reemplazado por un número del 1 al 10 de acuerdo a un orden establecido, el mismo que se almacena en la memoria EEPROM 24LC256.

La organización de la memoria EEPROM para guardar los eventos es la siguiente:

NÚMERO DE EVENTO	NÚMERO DE TARJETA	FECHA	HORA DE INGRESO	HORA DE SALIDA	ESPACIO DE CEROS
2 bytes	1 byte	3 bytes	3 bytes	3 bytes	4 bytes

Figura 3.6: Información que se va a guardar en la memoria EEPROM

A continuación se calcula el número de eventos que se pueden guardar en la memoria:

$$\#\text{Eventos} = 500\ \text{pág} * \frac{64\ \text{bytes}}{1\ \text{pág}} * \frac{1\ \text{evento}}{16\ \text{bytes}} = 2000\ \text{eventos}$$

De acuerdo al cálculo realizado, se puede almacenar 2000 eventos de 16 bytes en la memoria EEPROM. En caso de que se supere la cantidad de eventos, el microcontrolador envía un mensaje a la interfaz indicando que se ha llegado a los 2000 eventos e inmediatamente se borra la cuenta de los eventos, para posteriormente borrar los eventos de la página web.

Una vez que se conoce la cantidad de información que se almacena en la memoria; es necesario conocer la manera de cómo se guarda toda esta información.

3.1.2.2 Escritura de la Memoria

La escritura de una memoria EEPROM se la realiza de dos maneras:

- Escribiendo un byte
- Escribiendo varios bytes

Se escoge la segunda opción debido a que se manejan 16 bytes por cada evento, por consiguiente la lectura también se realiza leyendo varios bytes.

Primero hay que configurar las direcciones de escritura y de lectura de la memoria EEPROM 24LC256. Después hay que declarar la subrutina que hace la escritura, en la misma se incluye todas las variables a utilizarse. Se inicia la comunicación I2C y se envía el byte de control y la dirección de 2 bytes a la memoria. Posteriormente se envían todos los datos hacia la misma. Se detiene la comunicación I2C y se realiza una pausa de aproximadamente 100 milisegundos.

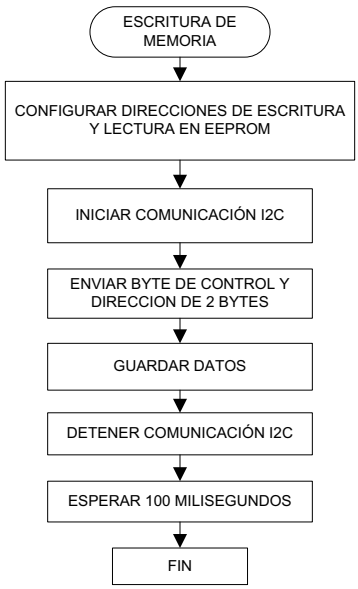


Figura 3.7: Diagrama de flujo de la escritura de la memoria EEPROM

3.1.2.3 Lectura de la Memoria

Para la lectura de datos se procede de una manera similar que la escritura, con la diferencia de que ya no se tiene que configurar las direcciones de escritura y de lectura de la memoria.

Primero se recurre a declarar la subrutina respectiva con todas las variables. Después se inicia la comunicación I2C y se envía el byte de control (correspondiente a la escritura) y la dirección de 2 bytes a la EEPROM. De nuevo se inicia la comunicación I2C y se envía el byte de control de lectura a la EEPROM. Se leen todos los datos, indicando siempre si existen más datos para leer y el último dato de lectura; posteriormente se detiene la comunicación I2C.

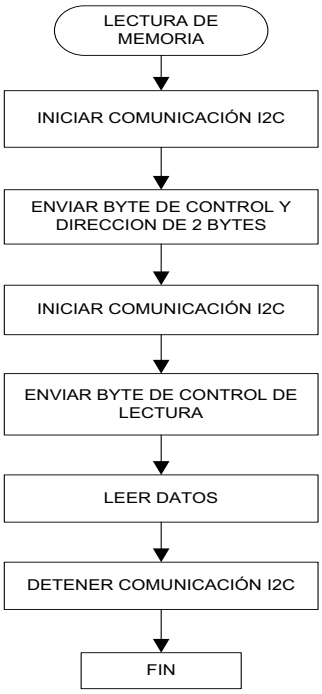


Figura 3.8: Diagrama de flujo de la lectura de la memoria EEPROM

3.1.3 MODEM GSM

A continuación se describen las subrutinas más importantes utilizadas en el programa del microcontrolador para la comunicación con el modem GSM.

3.1.3.1 Limpiar Buffer

Esta función asegura que el buffer de comunicaciones esté vacío para ser utilizado. Se captura el valor decimal del primer caracter ASCII que se encuentra en el buffer de comunicaciones.

Se obtiene el valor decimal del caracter ASCII que se encuentra en el buffer de comunicaciones, se utiliza esta función hasta obtener el valor 0. A continuación se muestra el diagrama de flujo de la función Limpiar Buffer:

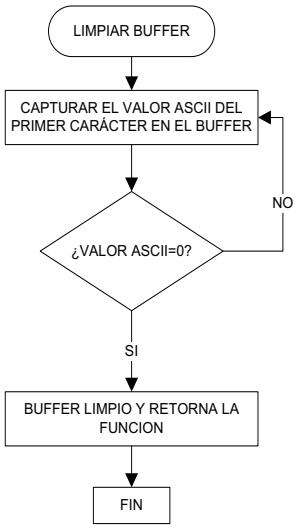


Figura 3.9: Diagrama de flujo de la Función Limpiar Buffer

3.1.3.2 Configuración inicial

Esta función permite configurar los principales parámetros del Modem GSM para su funcionamiento. Primero se limpia el buffer del puerto de comunicaciones y se limpia la variable que contiene la respuesta del buffer de comunicaciones. Se verifica si existe la tarjeta SIM y la correcta conexión a la red GSM del modem. Si los parámetros están correctamente verificados se limpia el buffer del puerto de comunicaciones y la variable que contiene la respuesta del buffer. Se envía el comando AT por el puerto de comunicaciones serial hasta que el modem responda OK, el comando AT permite iniciar la configuración del Modem. Se

llama a la función Limpiar Buffer para verificar que el buffer de comunicaciones se encuentra vacío.

Se envía el comando ATEO por el puerto de comunicaciones serial hasta que el modem responda OK, el comando ATEO sirve para eliminar el eco producido por el Modem. Se llama a la función Limpiar Buffer para verificar que el buffer de comunicaciones se encuentra vacío.

Se envía el comando AT+IPR por el puerto de comunicaciones serial hasta que el modem responda OK, el comando AT+IPR sirve para establecer la velocidad de transmisión del Modem. Se llama a la función Limpiar Buffer para verificar que el buffer de comunicaciones se encuentra vacío.

Se envía el comando AT+CMGF por el puerto de comunicaciones serial hasta que el modem responda OK, el comando AT+CMGF sirve para establecer el modo de SMS como texto. Se llama a la función Limpiar Buffer para verificar que el buffer de comunicaciones se encuentra vacío.

Se envía el comando AT+CNMI por el puerto de comunicaciones serial hasta que el modem responda OK, el comando AT+CNMI sirve para establecer el formato de SMS para ser enviados por el Modem. Se llama a la función Limpiar Buffer para verificar que el buffer de comunicaciones se encuentra vacío.

Se envía el comando AT+CSQ por el puerto de comunicaciones serial hasta que el modem responda OK, el comando AT+CSQ sirve para verificar si el Modem tiene una señal adecuada para el correcto envío de SMS. Se llama a la función Limpiar Buffer para verificar que el buffer de comunicaciones se encuentra vacío.

Se envía el comando AT+W por el puerto de comunicaciones serial hasta que el modem responda OK, el comando AT+W sirve para guardar la configuración actual del Modem. Se llama a la función Limpiar Buffer para verificar que el buffer de comunicaciones se encuentra vacío. A continuación se muestra el diagrama de flujo de la configuración inicial del modem GSM:

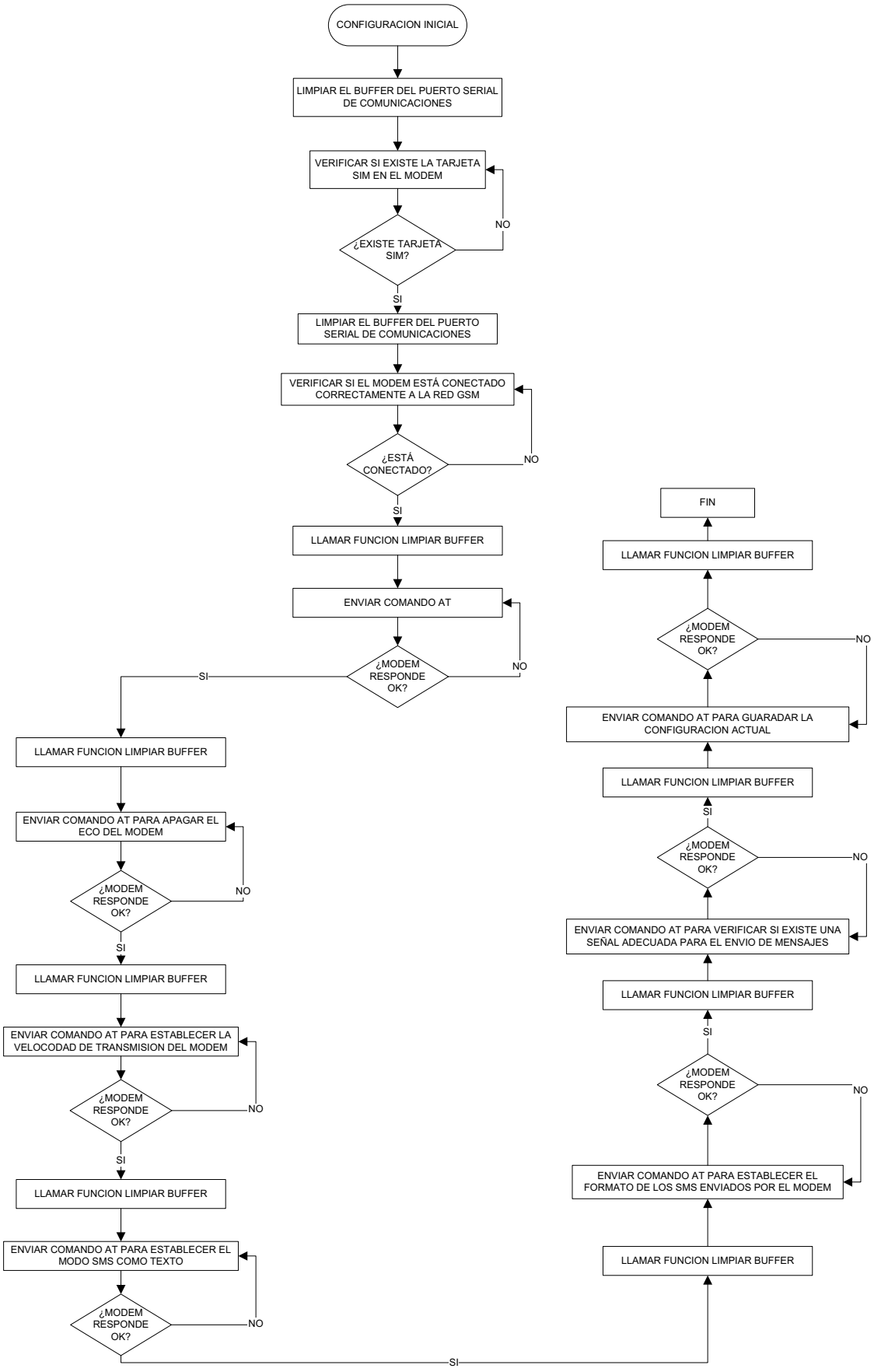


Figura 3.10: Diagrama de flujo de la configuración inicial del modem gsm

3.1.3.3 Obtener OK

Esta función permite obtener la respuesta OK del Modem. Se verifica si existen datos en el buffer de comunicaciones. Si lo hay, se captura el valor decimal del primer caracter y se verifica si devuelve el dato OK; si dato es válido se devuelve una variable con el dato OK, caso contrario se vuelve a verificar hasta encontrar el dato OK.

A continuación se muestra el diagrama de flujo del envío de mensajes:

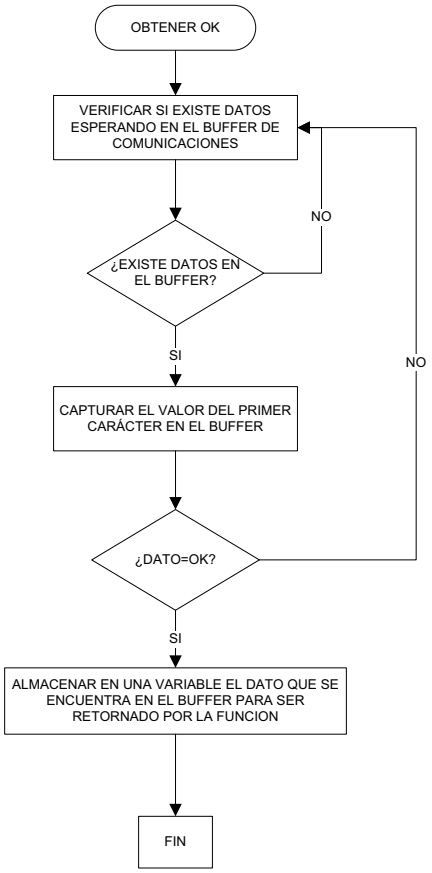


Figura 3.11: Diagrama de flujo de la Función Obtener OK

3.1.3.4 Enviar mensaje

Esta función permite enviar SMS a través del Modem. Primero se limpia el buffer de comunicaciones, y se realiza un retardo de 500 ms. A continuación se envía el comando AT+CMGS, seguido de la variable que almacena el número de celular al

que se desea enviar el mensaje; se envía este comando hasta obtener como respuesta en el buffer el carácter “>”. Si la respuesta en el buffer es el carácter “>” positiva, se llama a la función Limpiar Buffer, después se envía el texto del mensaje. Se llama a la función Obtener OK hasta obtener la respuesta OK del modem. Finalmente se limpia el buffer de comunicaciones. A continuación se muestra el diagrama de flujo del envío de mensajes:

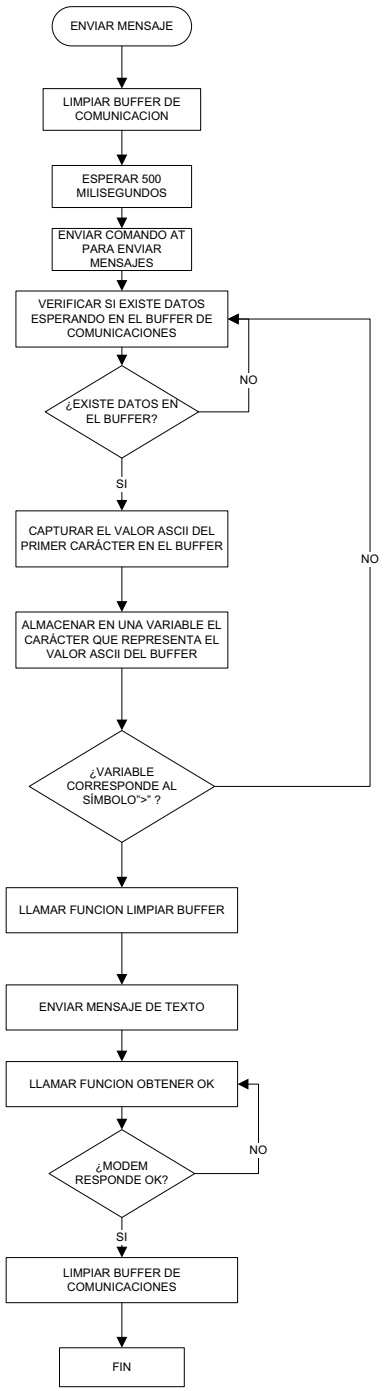


Figura 3.12: Diagrama de flujo del envío de mensajes

3.1.3.5 Recibir Mensaje

Esta función permite recibir los SMS que llegan al Modem. Se crea una variable de tipo string que almacenará los datos del buffer. Se obtienen los valores ASCII de los caracteres en el buffer. Luego se almacena en la variable creada los caracteres que se encuentran en el buffer hasta que devuelva el valor ASCII 10(representa salto de línea).

Se limpia la variable para almacenar los caracteres del buffer de comunicaciones, y nuevamente se obtienen los valores ASCII de los caracteres en el buffer. Se almacena en la variable creada los caracteres que se encuentran en el buffer hasta que devuelva el valor ASCII 10. Se almacena los datos de la variable de caracteres en la variable de tipo string. Finalmente se limpia el buffer. A continuación se muestra el diagrama de flujo de la función Recibir Mensaje:

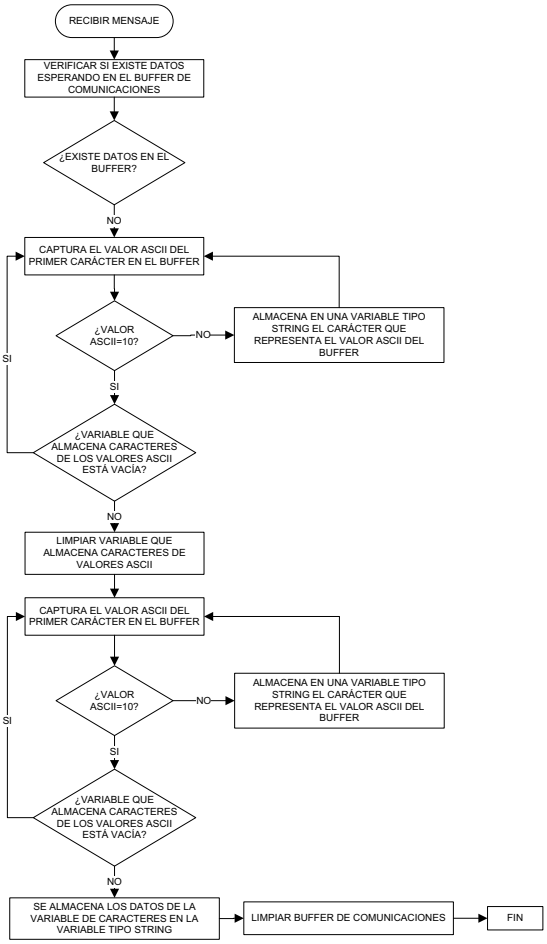


Figura 3.13: Diagrama de flujo de la Función Recibir Mensaje

3.1.3.6 Validar Mensaje

Esta función permite validar los SMS, dependiendo del número del que son enviados y el texto que poseen. Para ello se crea una variable la cual va a albergar el número del celular del cual provenga un mensaje

Posteriormente se compara si el número del cual proviene el mensaje es válido, si lo es, entonces, se valida el texto SMS que contiene.

Para el presente trabajo existen cuatro tipos de mensajes de texto válidos:

1. **ALARM OFF**: Desbloqueo de programa principal, en el cual se procede a desbloquear el programa principal, ya que al ocurrir una apertura no autorizada del armario se bloquea el programa principal, envía un SMS de alarma hacia un celular (“PUERTA ABIERTA – ALARMA ENCENDIDA”) y no hace ninguna acción hasta no recibir el mensaje anteriormente indicado. Las únicas acciones que realiza el programa son recibir y validar mensajes.

2. **ABRIR PUERTA**: Acciona la cerradura eléctrica que permite la apertura de la puerta del armario telefónico.

3. **MEMPED**: Pedido por parte de la Interfaz de Control y Administración sobre algún evento perdido; aquí se procede con el envío de un evento solicitado, ya que el mismo no consta en la base de datos. Cabe indicar que seguido de la instrucción MEMPED se añaden cuatro caracteres que toman un valor desde 0000 hasta 1999 según el orden del evento.

4. **COD**: Almacenamiento de los tags en la memoria EEPROM del microcontrolador, seguido de los números correspondientes a cada tag.

A continuación se muestra el diagrama de flujo de la función Validar Mensaje:

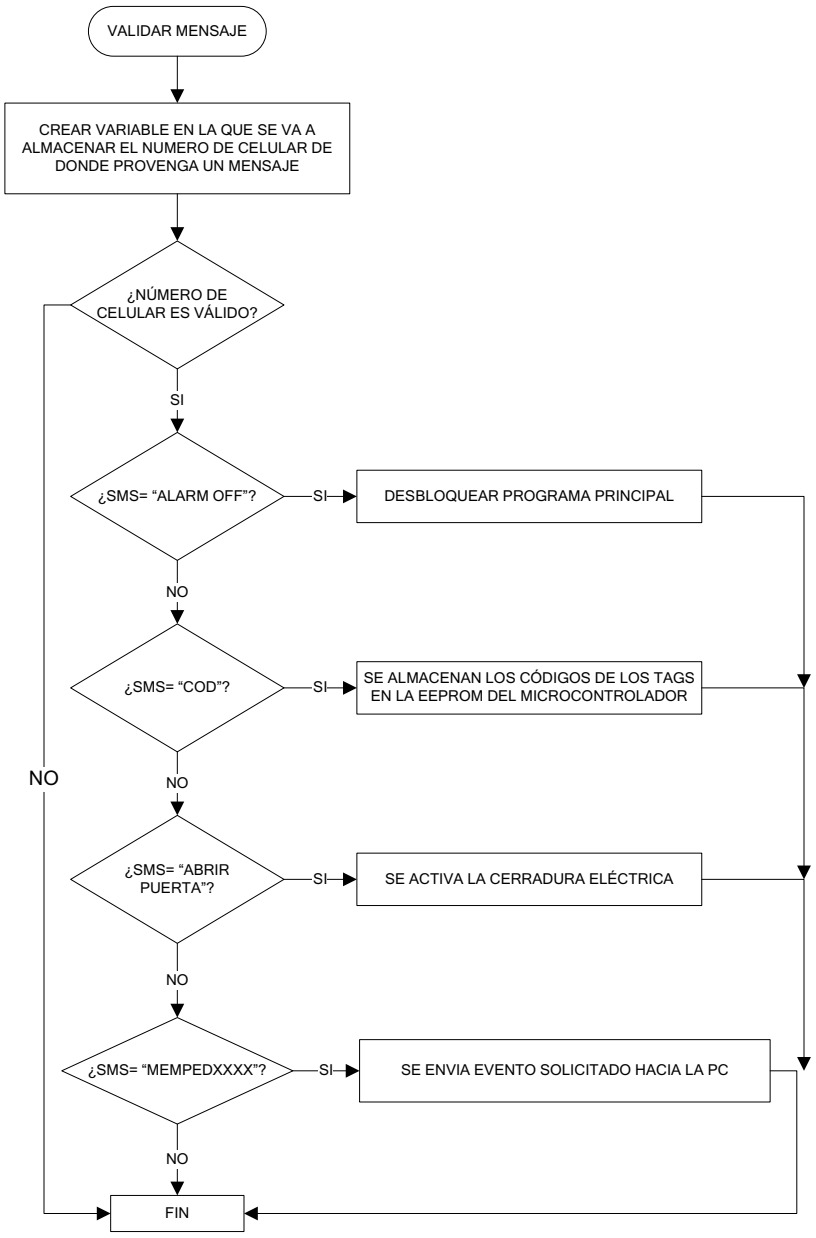


Figura 3.14: Diagrama de flujo de la Función Validar Mensaje

3.1.4 PROGRAMA PRINCIPAL

Como todo programa realizado en el compilador BASCOM-AVR, una vez que se ha configurado los parámetros iniciales como son: cristal, variables, registros, puertos, etc.; el microcontrolador está encargo de realizar las siguientes tareas:

- Revisa si se realiza la apertura no autorizada del armario telefónico, de ser así, el microcontrolador envía inmediatamente un mensaje de texto hacia un teléfono celular indicando que el programa del microcontrolador se ha bloqueado y proseguirá así hasta que no reciba un mensaje en el cual se indique el desbloqueo del mismo. Cabe mencionar que en este estado el sistema podrá únicamente recibir y validar mensajes.

- Cada vez que el microcontrolador reciba un mensaje de texto, se valida el número de teléfono del cual se recibe el mensaje, esto quiere decir que se aceptan mensajes únicamente de números previamente guardados en el microcontrolador, posterior a eso, se va realizar la respectiva acción de control dependiendo del contenido del mensaje que haya llegado, los cuales pueden ser: desbloquear el programa, almacenar tags en la EEPROM, petición de envío de eventos o activar la cerradura eléctrica. Además se actualiza la hora y fecha del sistema.

- Revisa si el lector RFID ha detectado un tag, si es así, primeramente verifica que el acceso se lo realice dentro del horario programado en el microcontrolador el cual es desde las 08h00 hasta las 16h59, luego compara si el tag detectado coincide con los almacenados en la EEPROM; si cumple las dos condiciones, activa la cerradura eléctrica, y después va a detectar la apertura y cierre de la puerta con el posterior almacenamiento del evento respectivo.

- Borra la cuenta de eventos y la memoria EEPROM cuando excede 2000 eventos, enviando un mensaje a la página de la interfaz.

En la siguiente figura se muestra el diagrama de flujo del programa realizado en el microcontrolador ATMEGA324P:

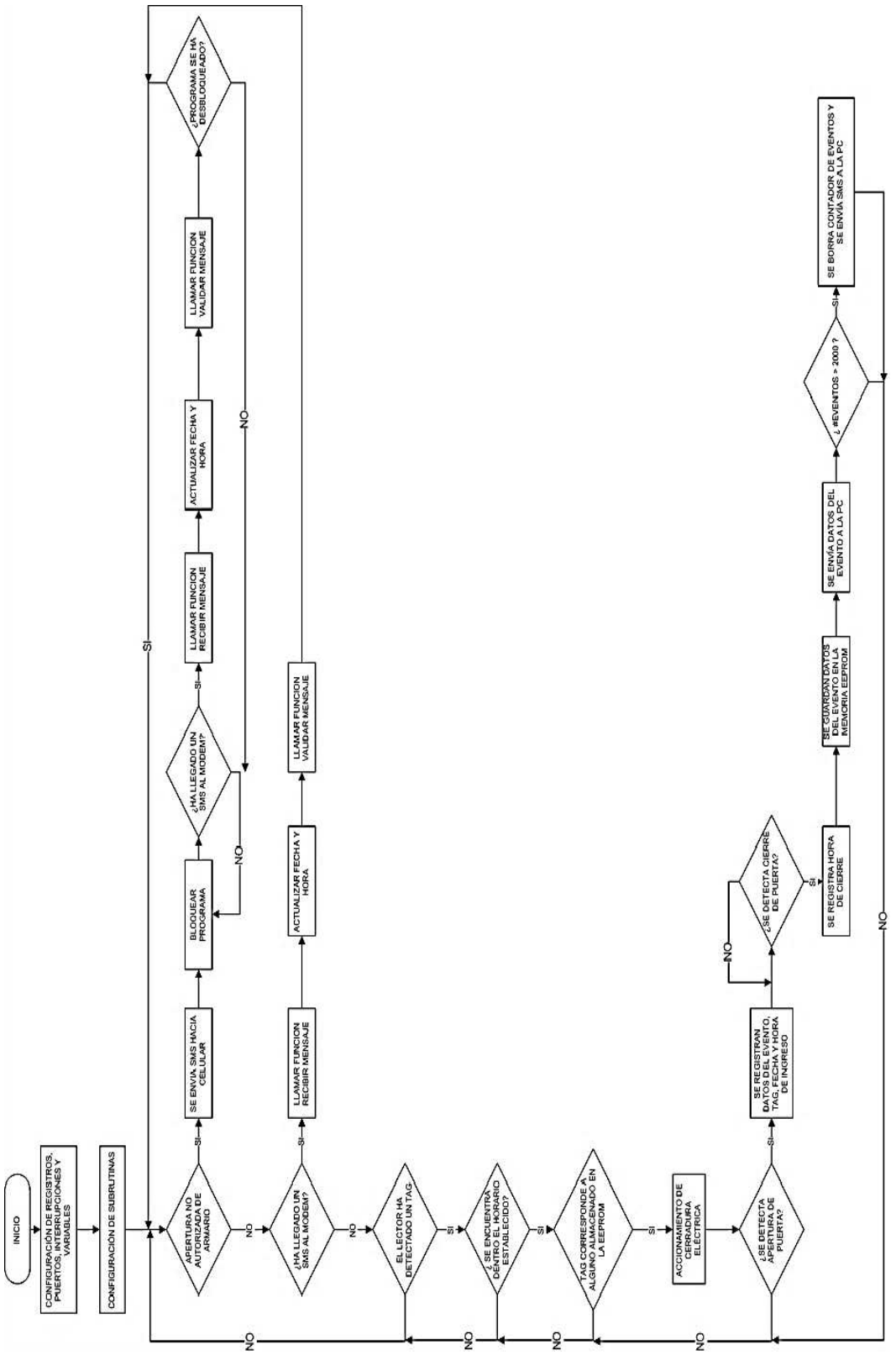


Figura 3.15: Diagrama de Flujo del Programa realizado en el microcontrolador

3.2 PROGRAMACIÓN DE LA INTERFAZ

La interfaz tiene dos aplicaciones: la primera para el control y administración; y la segunda es la aplicación web.

Para la aplicación de control y administración se utiliza el software SharpDevelop, y la página web se usa el software Delphi.

Las dos aplicaciones van a estar enlazadas a través de la base de datos como se indica en la figura:

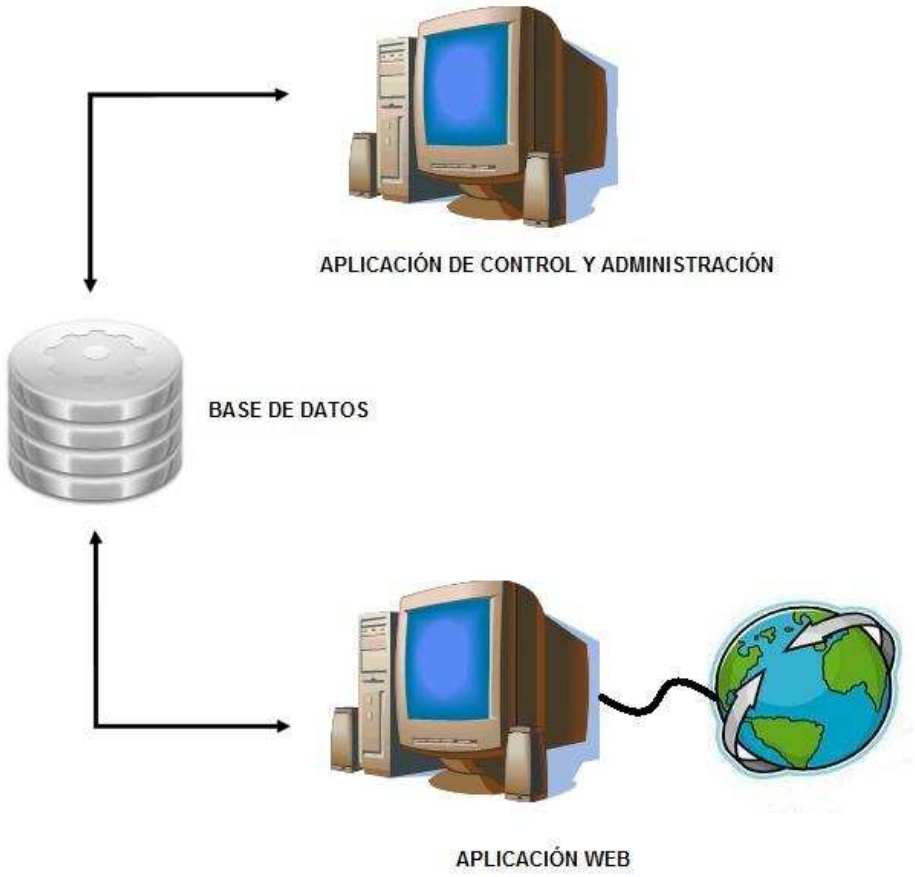


Figura 3.16: Esquema general de la interfaz a implementarse

En la figura 3.16 se puede observar como la base de datos, es el elemento fundamental para el funcionamiento de la interfaz. La actualización de la información en la página web depende de la recepción de datos en la aplicación

de control y administración, y posteriormente del almacenamiento en la base de datos.

3.2.1 BASE DE DATOS

Antes de comenzar a trabajar con las aplicaciones anteriormente mencionadas se crea la base de datos, la cual alberga los distintos datos que se necesitan para el diseño de las dos aplicaciones.

El siguiente paso es escoger el tipo de base de datos; en este caso se escoge una base de datos relacional; siendo ésta la más utilizada en la actualidad para implementar aplicaciones web.

Una base de datos relacional cumple con el modelo relacional, el cual consiste en representar al mundo real mediante tablas relacionadas entre sí por columnas comunes.

Num_empleado	Nombre	Sección
33	Pepe	25
34	Juan	25

Num_sección	Nombre
25	Textil
26	Pintura

Figura 3.17: Ejemplos de modelos relaciones mediante tablas [25]

La base de datos relacional necesita de un sistema de gestión, el cual es un software dedicado a tratar con bases de datos relacionales. En la actualidad existe una variedad de programas; para el presente trabajo se va a utilizar MySQL; ya que es uno de los más utilizados en aplicaciones web.

Como la base de datos trabaja conjuntamente con una página web se necesita de un servidor, el cual tenga soporte de base datos MySQL y de lenguaje para

páginas web; por tal razón se ha escogido el servidor XAMPP 1.6.6, ya que cumple con todos los requerimiento anteriormente citados.

Xampp es un servidor independiente de plataforma, software libre, que consiste en la base datos MySQL, el servidor web Apache y los intérpretes para los lenguajes de script: PHP y Perl.

El programa está liberado bajo la licencia GNU y actúa como un servidor web libre, fácil de usar y capaz de interpretar páginas dinámicas. Actualmente XAMPP está disponible para Microsoft Windows, GNU/Linux, Solaris y MacOS X.

La versión que se utiliza para el presente proyecto de titulación es el XAMPP1.66a. Para instalarlo, se siguen los pasos de la propia instalación. Una vez que se instala el servidor, se procede a configurar el panel de control de XAMPP, el cual se lo muestra en la figura 3.19, el mismo sirve para administrar y detener en cualquier momento las aplicaciones que se quieran. Se debe tener en cuenta, que para iniciar tanto el servidor Apache como el de MySQL, se tiene que tener desocupados los puertos que estos utilizan, pero normalmente estos puertos no se ocupan por ningún otro programa, por lo que no se tiene que tocar nada.

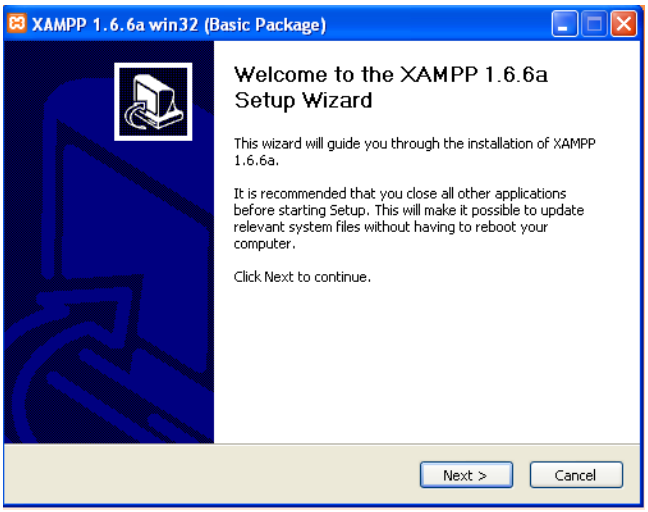


Figura 3.18: Proceso de instalación de Xampp

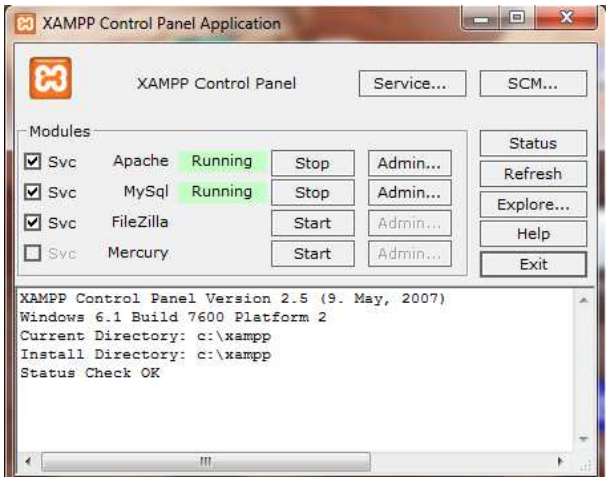


Figura 3.19: Panel de control de XAMPP

Ahora que ya se tiene instalado y configurado el servidor XAMPP, la página web del presente trabajo se aloja en la dirección: C:\xampp\htdocs.

En el anexo F se adjunta el procedimiento para la creación de la base de datos con sus respectivas tablas y campos en MySQL.

Una vez que ya se tiene la nueva base de datos, se debe crear las tablas, y posteriormente los campos con los cuales se va a trabajar. Para el presente trabajo se ha creado las siguientes tablas con sus respectivos campos:

Administradores: Esta tabla almacena toda la información referente a las personas que administran las dos aplicaciones de la interfaz, y contiene los siguientes campos:

- Nombre
- Apellido
- Código de identificación
- Clave, para el acceso a la página web y asignar los permisos a los usuarios.

Eventos: En esta tabla se registra toda la información referente al acceso por parte de los usuarios, con los siguientes campos:

- Código del tag
- Número del evento
- Nombre
- Apellido
- Fecha
- Hora de ingreso
- Hora de salida
- Armario

Historial: En esta tabla se almacenan todos los eventos que se borren de la página web, en caso de cualquier consulta, el administrador podrá ingresar a la base de datos y verificar cualquier evento anterior al borrado de la web. Va a tener los mismos que campos que la tabla Eventos, con la diferencia que se le añade otro campo llamado ingreso, el cual empieza desde cero, y se incrementa cada 2000 eventos.

Ordenado: En ésta tabla, se ordena la numeración de los eventos, para mostrar en la página web. En la misma se tiene los mismos campos que la tabla Eventos.

Usuarios: La tabla almacena toda la información referente a los usuarios asignados para el acceso al armario telefónico. Los campos son los siguientes:

- Código del tag
- Nombre
- Apellido
- Cargo
- Clave, que es el mismo campo de la tabla administradores, pero el objetivo de colocarle en esta tabla es para saber cuál administrador le asignó el permiso al usuario.

Índice: Esta es una tabla de un campo, el cual se encarga de llevar la cuenta del campo ingreso que está en la tabla historial.

3.2.2 APLICACIÓN DE CONTROL Y ADMINISTRACIÓN

Esta aplicación es la encargada de receptar y transmitir toda la información desde y hacia el microcontrolador, y luego almacenarla en la base de datos.

La aplicación de control y administración envía y recibe los mensajes de texto a través del modem. Los mensajes de envío conciernen a:

- Asignación de permisos de acceso que son los tags que se almacenan en el módulo.
- Petición de eventos perdidos, en caso de que alguno de ellos no haya sido almacenado en la base de datos.

Los mensajes de recepción conciernen a:

- Información del evento, el cual va ser almacenado en la base datos, para su publicación en la página web.
- Confirmación de algún proceso realizado por el administrador, el cual puede ser: asignación de tags o petición de evento perdido.
- Notificación de memoria llena, que inmediatamente va a borrar los eventos de la página web.

Para la decodificación de estos mensajes se ha escogido el software SharpDevelop, debido a que éste es gratuito y trabaja excelentemente con la transmisión y recepción serial.

SharpDevelop es un entorno de desarrollo integrado libre para los lenguajes de programación C, C#, Visual Basic.NET y Boo.

Figura 3.20: Presentación de SharpDevelop

3.2.2.1 Recepción de datos

Cada vez que llegue un mensaje a la aplicación, se valida la cadena de caracteres de la misma, para ello se crea una variable tipo string en la cual se almacena el mensaje que llegó al modem.

Posteriormente si la cadena es válida se procede a evaluar los siguientes casos:

- Si la cadena corresponde a los almacenamientos de eventos, se procede a separar cada uno de los elementos de la cadena como son: evento, tag, fecha, hora de ingreso y salida, para posteriormente almacenarlos en la base de datos.

- Si la cadena corresponde a confirmación de recepción de mensaje, en la aplicación se muestra un cuadro en el que se indica que el proceso se realizó correctamente.

- Si la cadena corresponde al borrado de la memoria EEPROM, inmediatamente se borra los eventos de la página web.

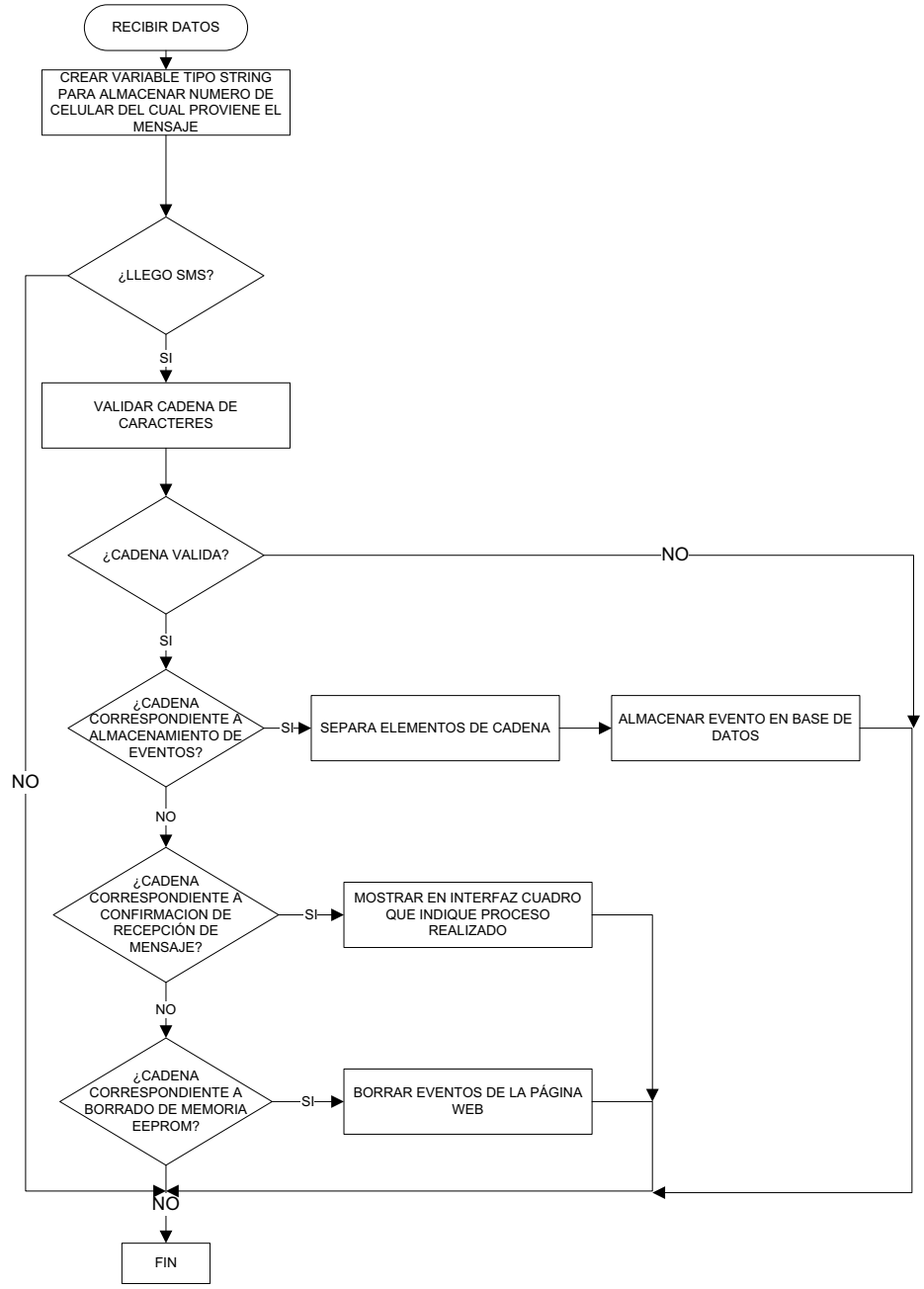


Figura 3.21: Diagrama de flujo de la recepción de datos en la aplicación de control y administración.

3.2.2.2 Envío de datos

El envío de información por medio del modem GSM funciona de la siguiente manera:

Se debe escribir el comando: AT+CMGS=”número de teléfono al cual se va enviar”+carácter enter.

Una vez escrito lo anterior se tiene que esperar el carácter prom(>), una vez que llegó, se procede a escribir el mensaje entre comillas y finalmente se lo envía.

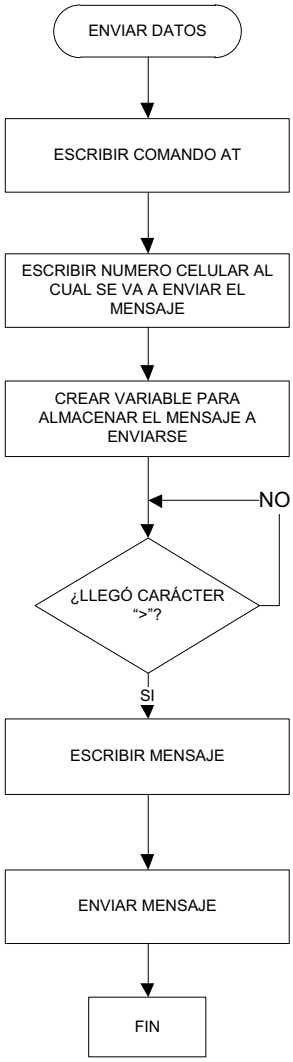


Figura 3.22: Diagrama de flujo del envío de datos en la aplicación de control y administración.

3.2.2.3 Diseño del formulario

El formulario contiene toda la parte visual con todas las opciones que tiene el administrador para el control de la aplicación, las cuales son:

- Recepción y envío de datos del modem GSM.
- Operaciones de ingreso, las cuales comprenden: creación de usuarios para el acceso al armario, crear administradores para la aplicación, eliminación de usuarios y administradores.
- Petición de eventos perdidos.

Para el desarrollo del mismo se procede de la siguiente manera:

Se procede a abrir la aplicación creada anteriormente y se pulsa sobre el botón diseño para ver la ventana del proyecto:

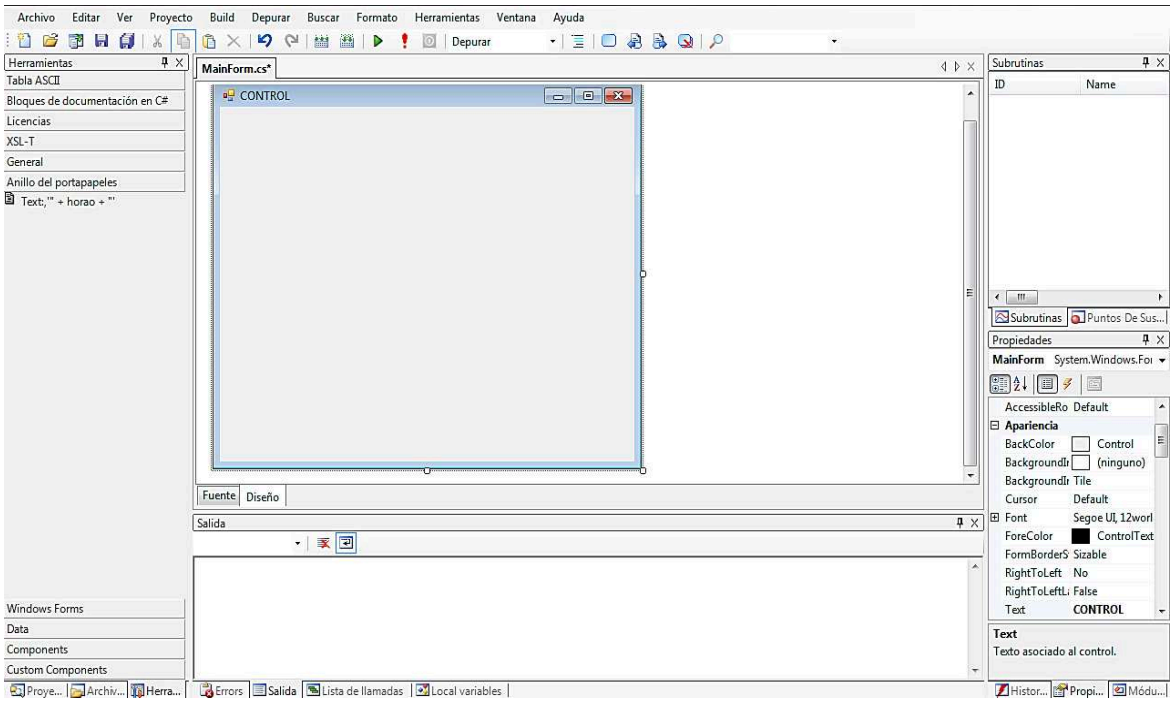


Figura 3.23: Vista previa de la aplicación visual a diseñarse

Al hacer click sobre herramientas se pueden ver los controles disponibles para arrastrarlos sobre el formulario y así poder incorporarles código.

Además se puede ver la ventana Propiedades en donde se puede modificar la apariencia física del formulario, como por ejemplo color de fondo, tipo de cursor, estilo de borde, etc.

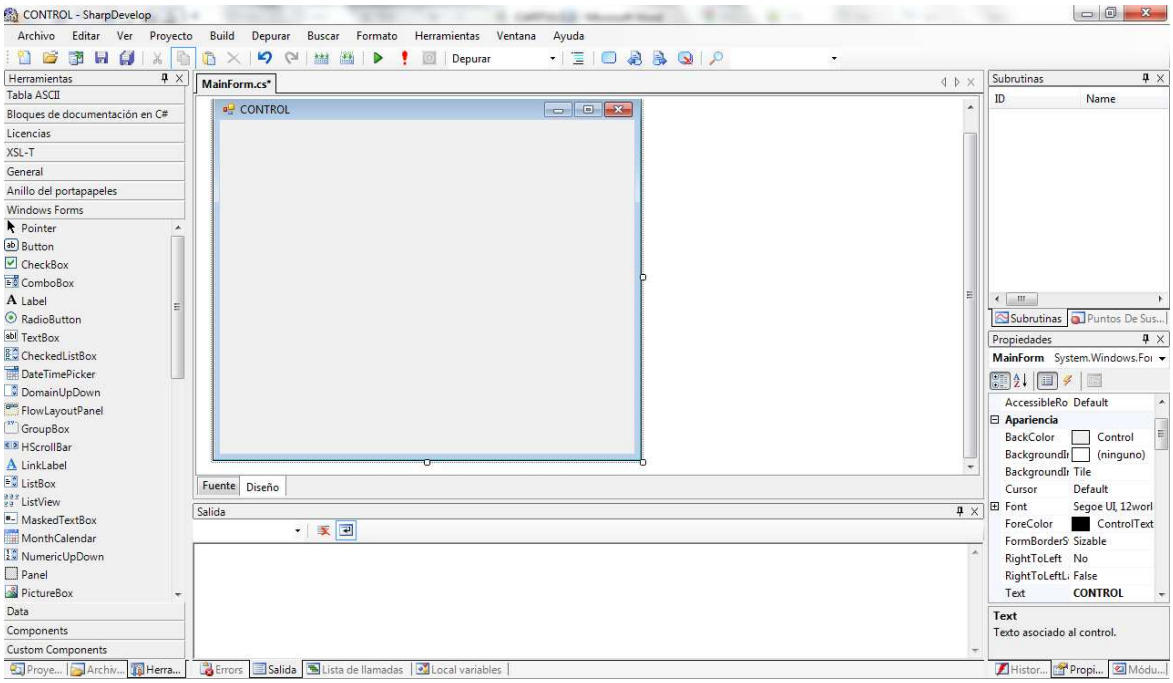


Figura 3.24: Vista previa de la opción herramientas y propiedades

3.2.2.3.1 Lectura de datos

La recepción de datos se encarga de mostrar el mensaje proveniente del módulo de control de acceso.

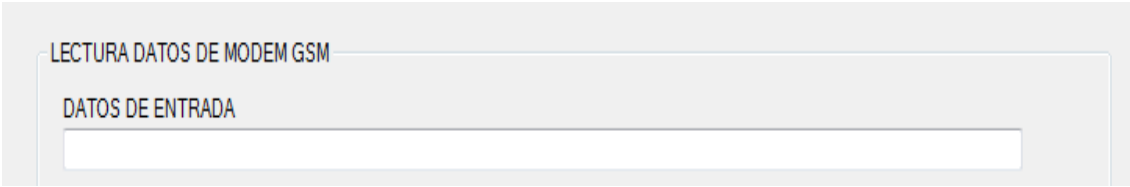


Figura 3.25: Presentación de la lectura de datos del modem

El momento que se reciba un mensaje de algún evento ocurrido aparecerá lo siguiente:

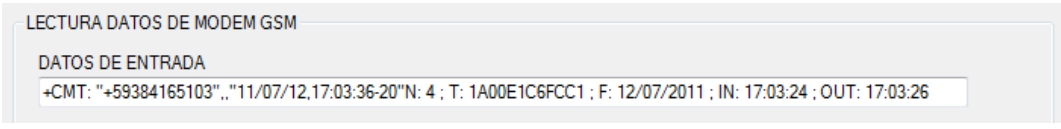


Figura 3.26: Mensaje correspondiente a un evento recibido

3.2.2.3.2 Operaciones de ingreso

Se ha colocado esta opción debido a que la aplicación requiere un manejo adecuado de la misma, por tal razón este menú permite a los administradores:

- Crear usuarios
- Crear administradores
- Eliminar usuarios
- Eliminar administradores

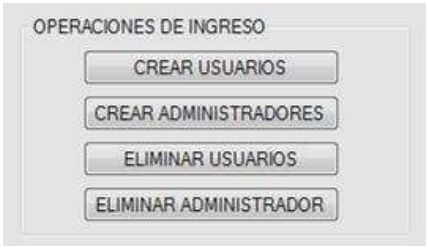


Figura 3.27: Presentación de las operaciones de ingreso

En el momento que se quiera crear usuarios se desplegará los campos concernientes a la tabla usuarios creada en la base de datos:

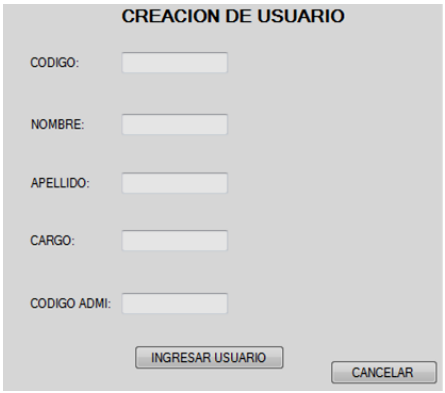


Figura 3.28: Creación de Usuario

En la opción crear administrador, se va a desplegar los campos concernientes a la tabla administradores:

Figura 3.29: Creación de administrador

Al momento de seleccionar la opción eliminar usuarios, se van a borrar todos los usuarios que habían sido almacenado en la base de datos, debido a que los permisos hacia el microcontrolador se envía en un solo mensaje.

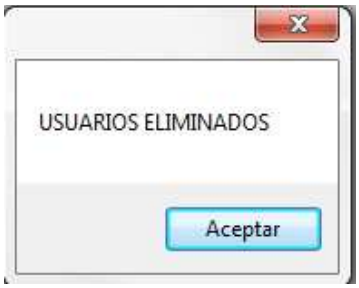


Figura 3.30: Mensaje de conformación de eliminación de usuario

La eliminación de administradores va a ser individualmente, pero primeramente se debe ingresar su código de identificación para poder borrarlo de la base de datos.

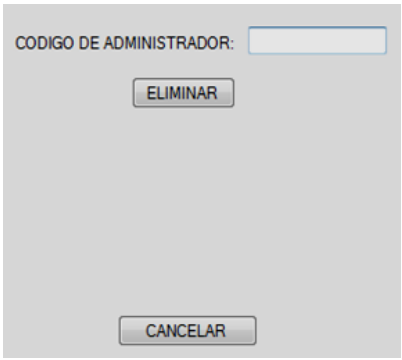


Figura 3.31: Validación de la eliminación de administrador

Figura 3.32: Mensaje de confirmación de eliminación de administrador

3.2.2.3.3 Petición de eventos perdidos

Esta opción está diseñada debido a que en algún momento puede fallar la cobertura de la operadora de la red GSM y no puede llegar algún mensaje respecto al evento ocurrido.

Figura 3.33: Petición de eventos perdidos

La misma funciona de la siguiente manera:

1. El momento de que se seleccione la opción “VER EVENTOS PERDIDOS”, inmediatamente se desplegará todos los eventos que no hayan sido almacenados en la base datos:

Figura 3.34: Lista de eventos perdidos

2. Al seleccionar la opción “SOLICITAR EVENTOS” aparecen dos mensajes: el primero corresponde al evento que se va a solicitar; y el segundo es el mensaje que se envía al microcontrolador, el cual tiene el siguiente formato: MEMPED + cuatro caracteres que toman un valor desde 0000 hasta 1999, debido a que en la memoria EEPROM tenemos un máximo de 2000 eventos que se pueden almacenar.

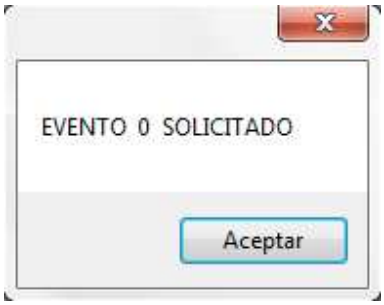


Figura 3.35: Evento que se va a solicitar

Figura 3.36: Mensaje que se envia al microcontrolador

3. Posteriormente llega el mensaje del evento solicitado:

Figura 3.37: Mensaje del evento solicitado

4. Después del envío de cada evento aparece un mensaje en el cual se indica que el proceso se realizó correctamente.

Figura 3.38: Mensaje que confirma que el envío del evento se ha realizado con éxito

5. Cuando se finalice con la petición de todos los eventos perdidos, al momento de solicitar más eventos, aparece un mensaje indicando que finalizó el proceso.

Figura 3.39: Mensaje de finalización del proceso

6. En el caso de que el administrador solicite la petición de eventos y no exista ninguno, se muestra un mensaje indicando que no hay eventos perdidos.

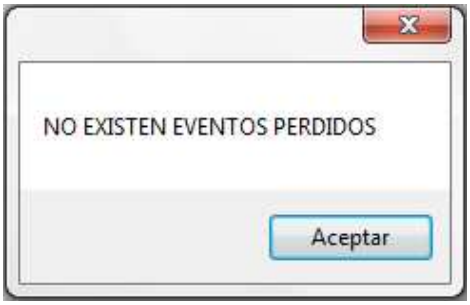


Figura 3.40: Mensaje en caso de no existir eventos perdidos

3.2.2.3.4 Asignación de tags

Esta opción se refiere al envío de los códigos de los tags, lo que permite el acceso a los usuarios, y la presentación de la misma se muestra en la siguiente figura:

Figura 3.41: Asignación de tags

El momento de ir creando usuarios, los códigos de los tags de cada uno de ellos aparecen en el listbox respectivo.

Figura 3.42: Ingreso de los diferentes tags que se envian al microcontrolador

La asignación de tags al microcontrolador se realiza a un máximo de 10 usuarios. Si se desea dar una nueva asignación, primeramente se debe ir a la opción “ELIMINAR USUARIOS” del menú Operaciones de ingreso y volver a crear los nuevos usuarios a los que se desea asignar los permisos de ingreso.

En el caso de tener los tags correspondientes a todos los usuarios asignados para el ingreso al armario, se procede a enviar al microcontrolador los tags; después de un momento llega un mensaje confirmando que el mismo ha sido recibido.

Figura 3.43: Confirmación de que el envío de los tags se ha realizado con éxito

La presentación final del diseño de la aplicación de control y administración es la siguiente:

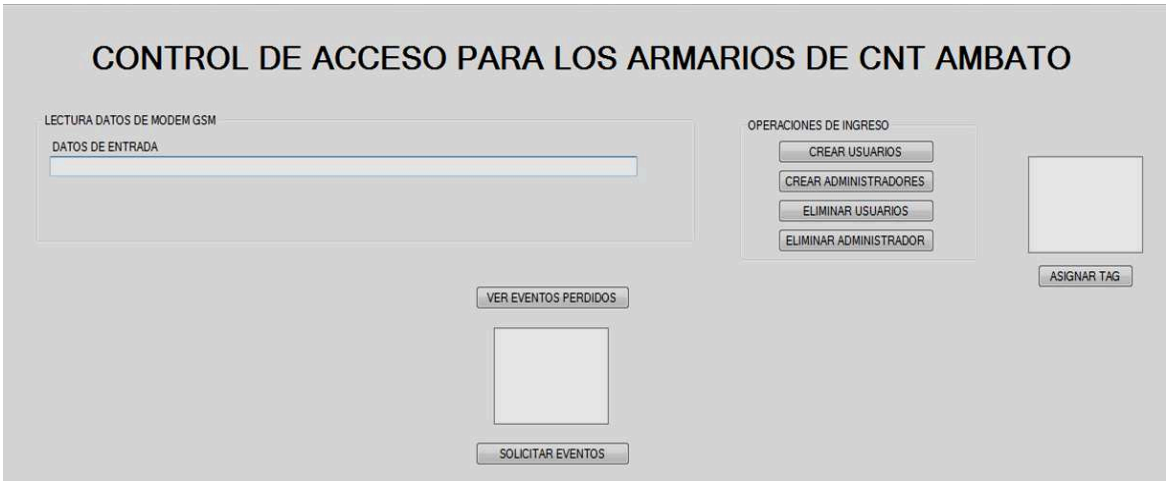


Figura 3.44: Presentación final de la aplicación de Control y Administración

3.2.3 APLICACIÓN WEB

Esta aplicación se refiere a la página web que muestra toda la información referente al acceso al armario. La misma contiene la siguiente información:

- Usuarios asignados para el ingreso al armario.
- Muestra la lista de todos los eventos, en la cual se visualiza: número del evento, tag, nombre y apellido del usuario, fecha, número de armario, hora de ingreso y salida.
- Búsqueda de eventos, las cuales son por: nombre, fecha y armario.

- Impresión de la lista de eventos.

El software con el que se diseña la página web es Delphi for PHP, debido a que está diseñado para llevar el desarrollo en PHP facilitando y agilizando el desarrollo de aplicaciones web centradas en bases de datos.

Delphi for PHP es un software con una estructura conceptual y tecnológica de soporte definida. La biblioteca de componentes visuales incluye muchos componentes que pueden ser usados dinámicamente los unos con los otros. Se integra bien con la base de datos MySQL. Además de que este software puede ser desplegado en la mayoría de servidores web y en casi todos los sistemas operativos y plataformas. Se ha utilizado la versión libre ya que permite realizar páginas web de pequeño tamaño. La versión licenciada tiene la capacidad de realizar páginas complejas en las que incluyen videos, imágenes en alta resolución, animaciones en flash, etc.[29]

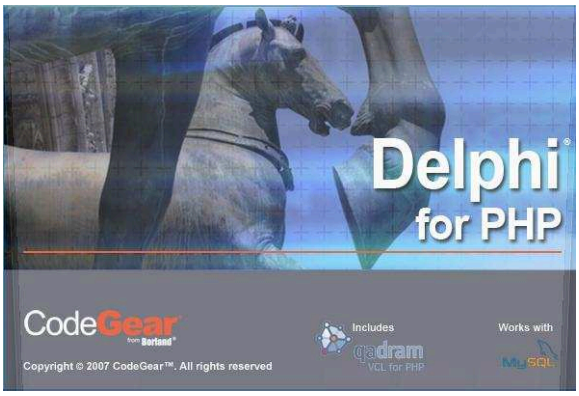


Figura 3.45: Presentación del software Delphi for PHP

3.2.3.1 Diseño de la parte visual de la página web

La misma contiene toda la información que el administrador puede consultar, la cual contiene:

- Un ingreso a la página mediante clave.
- Visualización de usuarios y eventos.
- Búsquedas de los eventos.

- Impresión de eventos.

3.2.3.1.1 Ingreso

Se valida la clave del administrador la cual está almacenada en la base datos. Al momento de presionar el botón ingresar se establece una conexión hacia la base de datos.

Después se valida el texto de la clave a través de una variable creada para este procedimiento y se realiza una búsqueda si la clave ingresada coincide con la clave almacenada en la base de datos.

Figura 3.46: Validación de la clave para el ingreso a la página web

Si la clave es correcta, aparece el nombre del administrador que accede a la página.

Figura 3.47: Mensaje con el nombre del administrador que ingresó a la página

El menú general que aparece es: usuarios, visualizar eventos, imprimir en pdf, búsquedas y la opción de cerrar sesión.

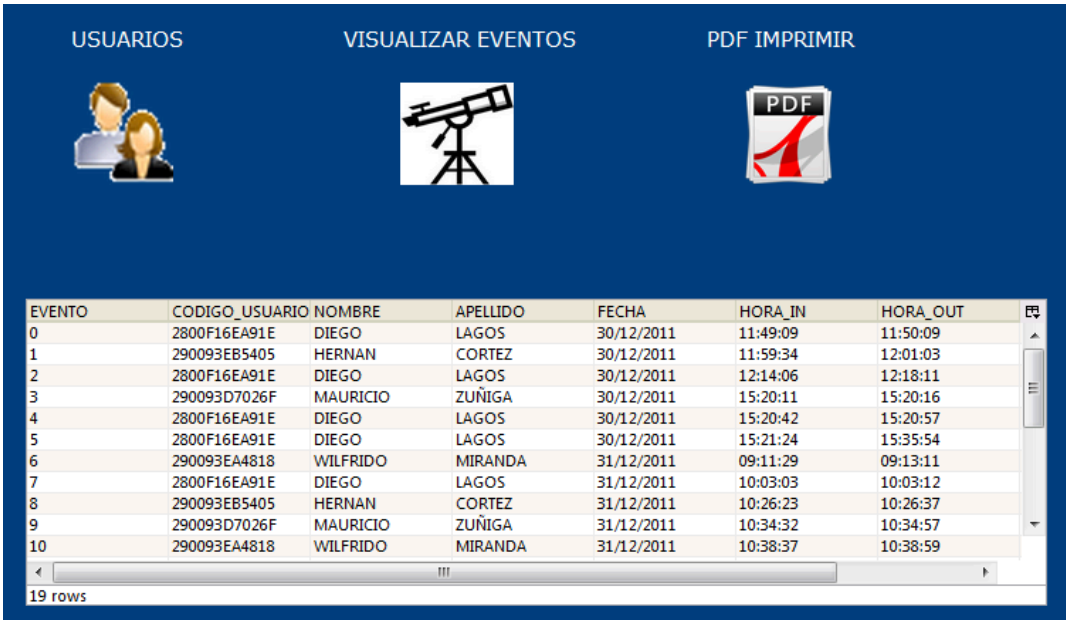
Figura 3.48: Presentación inicial de la página

3.2.3.1.2 Visualización de usuarios y eventos

Se puede realizar la consulta de los usuarios que se encuentran asignados al acceso al armario y ver todos los eventos que han ocurrido. Si se selecciona la opción USUARIOS se va a desplegar una tabla en la cual consta el código del tag, nombre, apellido, cargo que desempeña, y el código del administrador que realizó la asignación.

Figura 3.49: Lista de usuarios

Si se selecciona VISUALIZAR EVENTOS la tabla que se observa contiene: número del evento, código del tag, nombre, apellido, fecha, hora de ingreso y salida, además del número del armario telefónico.



EVENTO	CODIGO_USUARIO	NOMBRE	APELLIDO	FECHA	HORA_IN	HORA_OUT
0	2800F16EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09
1	290093EB5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03
2	2800F16EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11
3	290093D7026F	MAURICIO	ZUÑIGA	30/12/2011	15:20:11	15:20:16
4	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57
5	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54
6	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11
7	2800F16EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12
8	290093EB5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37
9	290093D7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57
10	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59

19 rows

Figura 3.50: Lista de eventos

3.2.3.1.3 Búsquedas

Se puede realizar la búsqueda de acuerdo a los siguientes criterios:

- Por nombre
- Por fecha
- Por armario

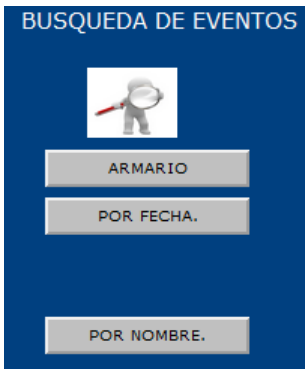


Figura 3.51: Búsqueda de eventos

Cada una de las búsquedas despliega un reporte en formato pdf para su impresión con los siguientes parámetros:

- Evento
- Código de la tarjeta
- Nombre del usuario
- Fecha
- Hora de entrada y salida
- Número del armario

En caso de seleccionar la búsqueda por nombre se tiene que llenar los campos nombre y apellido.

Figura 3.52: Búsqueda de eventos por nombre

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR NOMBRE

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
0	2800F16EA 91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09	119
2	2800F16EA 91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11	119
4	2800F16EA 91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57	119
5	2800F16EA 91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54	119
7	2800F16EA 91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12	119
13	2800F16EA 91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20	119

Figura 3.53: Resultados de la búsqueda por nombre

En la búsqueda por armario, se tiene que digitar el número del mismo, y posteriormente se tiene su reporte en formato pdf.

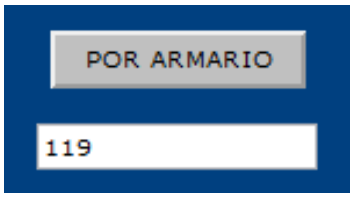


Figura 3.54: Búsqueda por número de armario

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR ARMARIO

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
0	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09	119
1	290093E B5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03	119
2	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11	119
3	290093D 7026F	MAURICIO	ZUÑIGA	30/12/2011	15:20:11	15:20:16	119
4	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57	119
5	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54	119
6	290093E A4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11	119
7	2800F16 EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12	119
8	290093E B5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37	119
9	290093D 7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57	119
10	290093E A4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59	119
11	290093E 3DB82	GEOVANNY	BARRENO	31/12/2011	10:39:32	10:39:56	119
12	290093E 3DB82	GEOVANNY	BARRENO	31/12/2011	10:43:23	10:43:46	119
13	2800F16 EA91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20	119
14	290093E 3DB82	GEOVANNY	BARRENO	02/01/2012	15:55:36	15:55:51	119
15	290093D 7026F	MAURICIO	ZUÑIGA	02/01/2012	15:56:13	15:56:46	119
16	290093E A4818	WILFRIDO	MIRANDA	02/01/2012	16:02:57	16:03:34	119
17	290093E A4818	WILFRIDO	MIRANDA	02/01/2012	16:03:46	16:04:06	119
18	290093E B5405	HERNAN	CORTEZ	02/01/2012	16:05:30	16:05:58	119

Figura 3.55: Resultado de la búsqueda por armario

Para la búsqueda por fecha, se tiene que llenar la misma con el siguiente formato: día/mes/año.

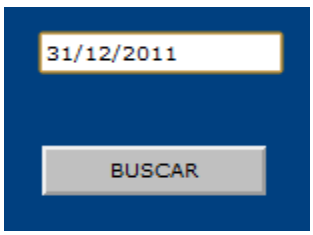


Figura 3.56: Búsqueda de eventos por fecha

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR FECHA

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
6	290093E A4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11	119
7	2800F16 EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12	119
8	290093E B5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37	119
9	290093D 7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57	119
10	290093E A4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59	119
11	290093E 3DB82	GEOVANNY	BARRENO	31/12/2011	10:39:32	10:39:56	119
12	290093E 3DB82	GEOVANNY	BARRENO	31/12/2011	10:43:23	10:43:46	119

Figura 3.57: Resultado de la búsqueda por fecha

3.2.3.1.4 Impresión de reporte de eventos

Realiza la impresión de los todos los eventos ocurridos, y muestra los mismos parámetros que el menú de búsquedas a excepción del número de armario; al igual que en el caso de las búsquedas el documento es en formato pdf.

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA
0	2800F16EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09
1	290093EB5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03
2	2800F16EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11
3	290093D7026F	MAURICIO	ZUÑIGA	30/12/2011	15:20:11	15:20:16
4	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57
5	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54
6	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11
7	2800F16EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12
8	290093EB5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37
9	290093D7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57
10	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59
11	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:39:32	10:39:56
12	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:43:23	10:43:46
13	2800F16EA91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20
14	290093E3DB82	GEOVANNY	BARRENO	02/01/2012	15:55:36	15:55:51
15	290093D7026F	MAURICIO	ZUÑIGA	02/01/2012	15:56:13	15:56:46
16	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:02:57	16:03:34
17	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:03:46	16:04:06
18	290093EB5405	HERNAN	CORTEZ	02/01/2012	16:05:30	16:05:58

Figura 3.58: Presentación de los eventos en formato pdf

CAPÍTULO 4

IMPLEMENTACIÓN Y PRUEBAS

4.1 SITUACIÓN ACTUAL DE LOS ARMARIOS TELEFÓNICOS

En la ciudad de Ambato al realizar la respectiva observación de algunos armarios telefónicos previo a la selección del armario donde se instaló el prototipo modelo del presente proyecto de titulación, se constató que la mayoría de armarios de CNT no gozan de una presentación y seguridad aceptable como lo demuestra la siguiente figura, lo cual no da muchas garantías para que dichos armarios no sean vulnerados y a la vez manipulados por gente extraña a la empresa con fines maliciosos, causando perjuicio a la corporación como también a los usuarios.

Figura 4.1: Armarios que no presentan las garantías necesarias de seguridad y presentación

4.2 SELECCIÓN DEL ARMARIO TELEFÓNICO

Para la selección del armario en donde se instaló el módulo de control de acceso, se considera los siguientes parámetros:

- Cercanía a la Empresa telefónica CNT, para verificar cualquier falla técnica del funcionamiento del prototipo.
- Buen estado del armario.
- Que preste las garantías adecuadas de seguridad para la instalación.
- Que disponga el espacio suficiente para la instalación, ya que algunos armarios están saturados de regletas, razón por la cual dificulta la instalación.
- Que el armario sea de un material amigable para la detección de los tags RFID.

Por las razones expuestas anteriormente se escogió el armario número 119 ubicado en las calles Shyrys y Duchicela, ya que cumple con la mayoría de estas características.

Figura 4.2: Armario escogido para la instalación del módulo

Además se solicitó un permiso a la Empresa Eléctrica Ambato (E.E.A.S.A.) para la instalación provisional de la energía eléctrica.

Figura 4.3: Manguera de conexión de la energía eléctrica hacia el armario

4.3 IMPLEMENTACIÓN DEL SISTEMA

Primeramente se instaló la energía eléctrica, el módulo de control de acceso conjuntamente con la placa del lector RFID, la batería de respaldo y la cerradura eléctrica, como se muestra en la siguiente figura:

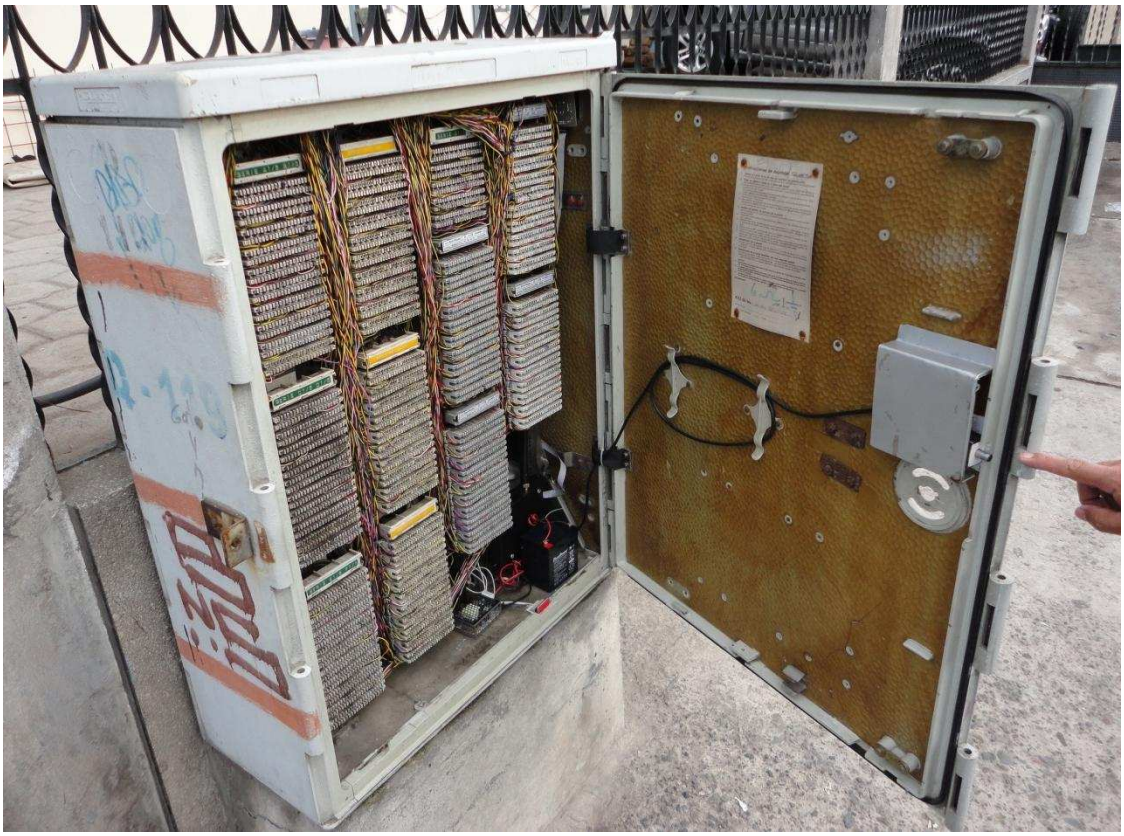


Figura 4.4: Instalación general del módulo

El módulo conjuntamente con la fuente de alimentación, y la batería fueron colocados en la parte inferior interna del armario. Para lograr una lectura cómoda de los tags, el lector RFID fue colocado en el extremo superior del armario.

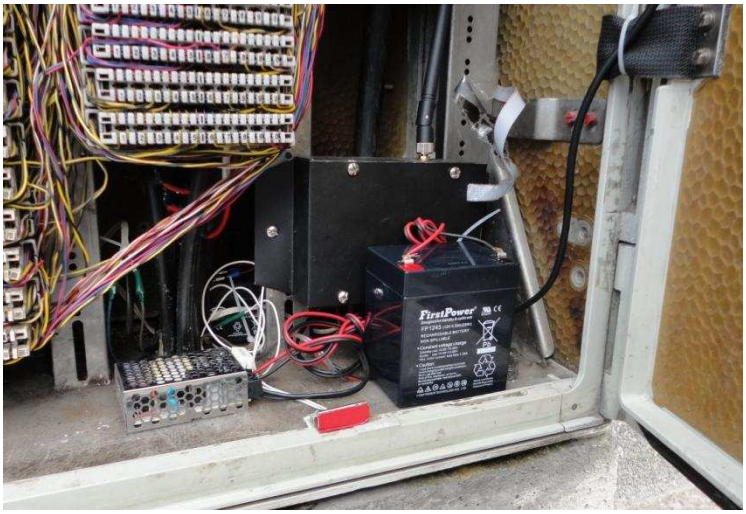


Figura 4.5: Módulo, fuente de alimentación y batería colocados en el armario

Figura 4.6: Placa externa del lector RFID colocado en el extremo superior del armario.

La cerradura, encargada de la apertura del armario se colocó en el borde central de la puerta, lo cual permite que el vástago se deslice libremente en la apertura y cierre de la misma.

Figura 4.7: Instalación de la cerradura eléctrica

4.4 PRUEBAS REALIZADAS AL PROTOTIPO

4.4.1 CREACIÓN DE ADMINISTRADOR, USUARIO Y ASIGNACIÓN DE PERMISOS

Para ello primero se escogió asignar 5 tags RFID para el acceso a los armarios, de los cuales 4 son destinados para el personal de CNT y el restante para el tesista.

Como primer paso se crea a los administradores que son los que tienen el acceso a la página web y son los responsables de crear a los usuarios para los permisos de acceso al armario. Para las pruebas al prototipo se creó un administrador para realizar el control total de la interfaz.

Figura 4.8: Creación del administrador

Posteriormente se creó los usuarios a los cuales se les asigna el código del tag, datos personales, cargo que ejercen en la empresa y el código del administrador:

Figura 4.9: Creación de usuario

Se repite el procedimiento de la figura 4.10 para los cuatro usuarios restantes. Luego de este paso se tienen los 5 tags que se envían hacia el módulo de control de acceso.

Figura 4.10: Tags que van a ser enviados hacia el módulo de control de acceso

Después del envío, llega un mensaje a la aplicación de control y administración de que los códigos han sido enviados correctamente.

Figura 4.11: Mensaje de confirmación de que los códigos han sido recibidos correctamente.

4.4.2 VISUALIZACIÓN DE LA PÁGINA WEB

En la página web se observa toda la información referente a los eventos ocurridos así como los usuarios asignados.

Para que la página web pueda publicarse en el internet, se requiere de un servidor y una dirección IP. El servidor que se utiliza es un computador personal común en conexión con un modem provisto por CNT, en el cual también consta del modem GSM en donde se reciben los diversos eventos que se almacenan en la base de datos.

Para la asignación de la dirección IP, CNT concedió la siguiente dirección pública: 200.107.19.32.

Figura 4.12: Computador que actúa como servidor, junto con los módems respectivos para la conexión a internet y red GSM.

Para acceder a la página web se debe ingresar la siguiente dirección IP en el navegador:

http://200.107.19.32/diego_lagos/cntdatos.php

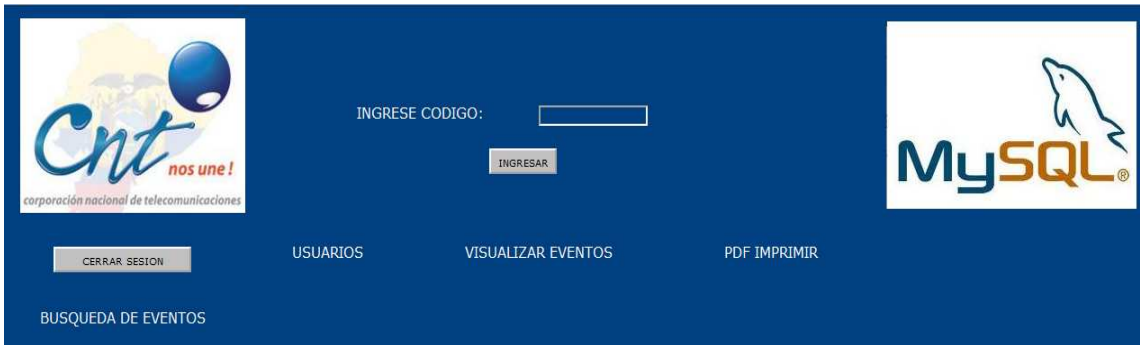


Figura 4.13: Presentación inicial de la página web

Para tener acceso a la información de la página se ingresa la clave de acceso que solo la tiene el administrador, la cual se valida al ingreso. En caso de ingresar la clave incorrecta, la página indica dicho error:

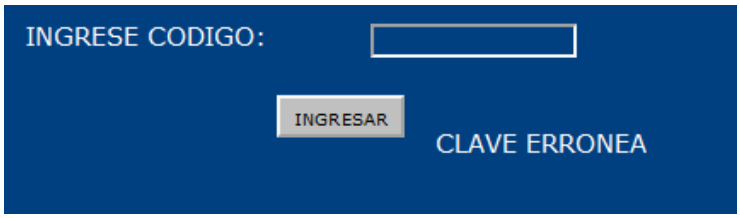


Figura 4.14: Ingreso incorrecto a la página web

Cuando se digita la clave correcta del administrador se despliega el nombre del administrador y el menú principal:

Figura 4.15: Ingreso correcto en donde se muestra el nombre del administrador y menú principal.

4.4.2.1 Prueba del menú visualizar eventos

Para el prototipo del módulo de control de acceso a los armarios telefónicos se realizaron 3 días de pruebas, los cuales fueron el 30, 31 de Diciembre de 2011 y 2 de Enero de 2012 a distintas horas del día; todo la información se observa en la opción VISUALIZAR EVENTOS:

EVENTO	CODIGO_USUARIO	NOMBRE	APELLIDO	FECHA	HORA_IN	HORA_OUT
0	2800F16EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09
1	290093EB5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03
2	2800F16EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11
3	290093D7026F	MAURICIO	ZUÑIGA	30/12/2011	15:20:11	15:20:16
4	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57
5	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54
6	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11
7	2800F16EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12
8	290093EB5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37
9	290093D7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57
10	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59

Figura 4.16: Eventos de los días 30 y 31 de Diciembre de 2011

EVENTO	CODIGO_USUARIO	NOMBRE	APELLIDO	FECHA	HORA_IN	HORA_OUT
9	290093D7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57
10	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59
11	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:39:32	10:39:56
12	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:43:23	10:43:46
13	2800F16EA91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20
14	290093E3DB82	GEOVANNY	BARRENO	02/01/2012	15:55:36	15:55:51
15	290093D7026F	MAURICIO	ZUÑIGA	02/01/2012	15:56:13	15:56:46
16	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:02:57	16:03:34
17	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:03:46	16:04:06
18	290093EB5405	HERNAN	CORTEZ	02/01/2012	16:05:30	16:05:58

Figura 4.17: Eventos de los días 31 de Diciembre de 2011 y 2 de Enero de 2012

4.4.2.2 Prueba del menú usuarios

Aquí se observa todos los usuarios que han recibido el permiso para acceder al armario telefónico. En el mismo se visualiza el código del tag, nombre del usuario, cargo y código del administrador que concedió el permiso. Para el presente trabajo se tiene 5 usuarios.

CODIGO_USUARIO	NOMBRE	APELLIDO	CARGO	COD_ADMIN
290093EB5405	HERNAN	CORTEZ	JEFE DE OPERACIONES	19865
290093D7026F	MAURICIO	ZUÑIGA	RESPONSABLE DE ACCESOS	19865
290093EA4818	WILFRIDO	MIRANDA	ANALISTA DE ACCESOS	19865
290093E3DB82	GEOVANNY	BARRENO	ANALISTA DE ACCESOS	19865
2800F16EA91E	DIEGO	LAGOS	TESISTA	19865

Figura 4.18: Usuarios asignados para el acceso al armario

4.4.2.3 Prueba del menú pdf imprimir

Esta opción permite obtener una lista de reporte en formato pdf de todos los eventos que han sucedido hasta la fecha de su consulta. Contiene los siguientes parámetros:

- Número del evento
- Código del tag
- Nombre del usuario
- Fecha
- Hora de entrada y salida

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA
0	2800F16EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09
1	290093EB5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03
2	2800F16EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11
3	290093D7026F	MAURICIO	ZUÑIGA	30/12/2011	15:20:11	15:20:16
4	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57
5	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54
6	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11
7	2800F16EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12
8	290093EB5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37
9	290093D7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57
10	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59
11	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:39:32	10:39:56
12	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:43:23	10:43:46
13	2800F16EA91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20
14	290093E3DB82	GEOVANNY	BARRENO	02/01/2012	15:55:36	15:55:51
15	290093D7026F	MAURICIO	ZUÑIGA	02/01/2012	15:56:13	15:56:46
16	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:02:57	16:03:34
17	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:03:46	16:04:06
18	290093EB5405	HERNAN	CORTEZ	02/01/2012	16:05:30	16:05:58

Figura 4.19: Reporte de eventos de los 3 días de pruebas

4.4.2.4 Prueba del menú búsquedas de eventos

Como ya se ha mencionado en el capítulo anterior, se tiene tres criterios de búsqueda, y para este caso se procede de la siguiente manera:

- Se realiza la búsqueda de los tres días de pruebas, mostrando sus respectivos reportes.
- Para la búsqueda por nombre se realiza dos búsquedas de usuario con sus respectivos reportes.
- Como se tiene un solo armario se muestra un solo reporte.

Las búsquedas contienen la siguiente información:

- Número del evento
- Código del tag
- Nombre del usuario
- Fecha
- Hora de entrada y salida
- Número del armario

A continuación se muestra todos los reportes referentes a búsquedas:

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR FECHA

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
0	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09	119
1	290093E B5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03	119
2	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11	119
3	290093D 7026F	MAURICIO	ZUÑIGA	30/12/2011	15:20:11	15:20:16	119
4	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57	119
5	2800F16 EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54	119

Figura 4.20: Reporte de búsqueda del 30 de Diciembre de 2011

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR FECHA

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
6	290093E A4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11	119
7	2800F16 EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12	119
8	290093E B5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37	119
9	290093D 7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57	119
10	290093E A4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59	119
11	290093E 3DB82	GEOVANNY	BARRENO	31/12/2011	10:39:32	10:39:56	119
12	290093E 3DB82	GEOVANNY	BARRENO	31/12/2011	10:43:23	10:43:46	119

Figura 4.21: Reporte de búsqueda del 31 de Diciembre de 2011

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR FECHA

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
13	2800F16 EA91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20	119
14	290093E 3DB82	GEOVANNY	BARRENO	02/01/2012	15:55:36	15:55:51	119
15	290093D 7026F	MAURICIO	ZUÑIGA	02/01/2012	15:56:13	15:56:46	119
16	290093E A4818	WILFRIDO	MIRANDA	02/01/2012	16:02:57	16:03:34	119
17	290093E A4818	WILFRIDO	MIRANDA	02/01/2012	16:03:46	16:04:06	119
18	290093E B5405	HERNAN	CORTEZ	02/01/2012	16:05:30	16:05:58	119

Figura 4.22: Reporte de búsqueda del 2 de Enero de 2012

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR NOMBRE

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
1	290093EB5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03	119
8	290093EB5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37	119
18	290093EB5405	HERNAN	CORTEZ	02/01/2012	16:05:30	16:05:58	119

Figura 4.23: Reporte de búsqueda del Usuario 1

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR NOMBRE

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
0	2800F16EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09	119
2	2800F16EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11	119
4	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57	119
5	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54	119
7	2800F16EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12	119
13	2800F16EA91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20	119

Figura 4.24: Reporte de búsqueda del Usuario 2

CORPORACION NACIONAL DE TELECOMUNICACIONES
INFORME DE EVENTOS BUSCADOS POR ARMARIO

EVENTO	TARJETA	NOMBRE	APELLIDO	FECHA	HORA ENTRADA	HORA SALIDA	ARMARIO
0	2800F16EA91E	DIEGO	LAGOS	30/12/2011	11:49:09	11:50:09	119
1	290093EB5405	HERNAN	CORTEZ	30/12/2011	11:59:34	12:01:03	119
2	2800F16EA91E	DIEGO	LAGOS	30/12/2011	12:14:06	12:18:11	119
3	290093D7026F	MAURICIO	ZUÑIGA	30/12/2011	15:20:11	15:20:16	119
4	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:20:42	15:20:57	119
5	2800F16EA91E	DIEGO	LAGOS	30/12/2011	15:21:24	15:35:54	119
6	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	09:11:29	09:13:11	119
7	2800F16EA91E	DIEGO	LAGOS	31/12/2011	10:03:03	10:03:12	119
8	290093EB5405	HERNAN	CORTEZ	31/12/2011	10:26:23	10:26:37	119
9	290093D7026F	MAURICIO	ZUÑIGA	31/12/2011	10:34:32	10:34:57	119
10	290093EA4818	WILFRIDO	MIRANDA	31/12/2011	10:38:37	10:38:59	119
11	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:39:32	10:39:56	119
12	290093E3DB82	GEOVANNY	BARRENO	31/12/2011	10:43:23	10:43:46	119
13	2800F16EA91E	DIEGO	LAGOS	02/01/2012	15:53:27	15:54:20	119
14	290093E3DB82	GEOVANNY	BARRENO	02/01/2012	15:55:36	15:55:51	119
15	290093D7026F	MAURICIO	ZUÑIGA	02/01/2012	15:56:13	15:56:46	119
16	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:02:57	16:03:34	119
17	290093EA4818	WILFRIDO	MIRANDA	02/01/2012	16:03:46	16:04:06	119
18	290093EB5405	HERNAN	CORTEZ	02/01/2012	16:05:30	16:05:58	119

Figura 4.25: Reporte de búsqueda por armario

4.5 COSTOS DEL PROYECTO

A continuación se detalla el costo de los materiales, equipos, diseño y programación utilizados para el presente proyecto.

No se incluye el costo de uso de la IP por cuanto CNT cuenta con sus propias direcciones.

Debido a que los chips utilizados funcionan con líneas de Movistar inicialmente para la realización de pruebas se contrató:

- Un paquete de 30 mensajes con un valor de $1,12 para el modem GSM que se encuentra en el armario.
- Un paquete de 30 mensajes con un valor de $1,12 para el modem GSM que se encuentra junto al servidor.

Por ser un modelo de prototipo que no consume demasiada energía eléctrica, el costo por el uso de la misma no está considerado en el presupuesto gracias a que la Empresa Eléctrica Ambato facilitó su uso gratuito.

Lo que tiene que ver a licencias de los programas utilizados, como se mencionaron en capítulos anteriores, por ser versiones libres o demo que funcionaron adecuadamente, están exentos de costo.

ITEMS			
CANT.	**PRODUCTO**	**V. UNIT**	**V. TOTAL**
14	Resistencia	0,02	0,28
5	Bornera 2 pines	0,25	1,25
2	Relé 12V	0,65	1,3
1	Condensador 3330µF	0,78	0,78
2	Condensador 1000µF	0,25	0,5
5	Condensador 470µF	0,15	0,75
7	Condensador 100nF	0,08	0,56
1	Condensador 2200µF	0,4	0,4
6	Diodo 1N4007	0,08	0,48
1	LM317	0,65	0,65
1	ATMEGA 324P	11,8	11,8
1	MAX232	2,15	2,15
1	DS1307	3,5	3,5
1	Memoria EEPROM 24LC256	1,9	1,9
2	Zócalo 8 pines	0,08	0,16
1	Zócalo 16 pines	0,15	0,15
1	Zócalo 40 pines	0,25	0,25
1	Zócalo para pila	1,15	1,15
1	Pila 3.3V	0,75	0,75
2	Conector IDC - 10 P	0,55	1,1
1	Potenciómetro de precisión 5KΩ	0,55	0,55
2	2N3904	0,08	0,16
1	Cristal 11,0592 Mhz	0,45	0,45
1	Cristal 32768 Khz	0,45	0,45
1	Disipador TO220	0,85	0,85
1	RFID ID-20	55	55
2	MODEM GSM (Transmisor y Receptor)	135	270
1	Fuente 12V – 2A	35	35
1	Caja Metálica	35	35
1	Placa Panel Doble Lado	75	75
1	Placa Simple	4,5	4,5
	Otros materiales	5	5
	Diseño y programación	600	600
2	Paquete de 30 mensajes	1,12	2,24
TOTAL		$ 1114,06	

Tabla 4.1: Presupuesto del proyecto

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Con la realización del proyecto se solucionó a un requerimiento de la empresa CNT Ambato al realizar el diseño de un módulo de control de acceso a sus armarios utilizando herramientas tales como tecnologías RFID y GSM, un microcontrolador, una interfaz de control y administración, además de una interfaz web.

- Para un mejor desempeño del modem interno fue necesario utilizar en el diseño un cristal de 11.0592 Mhz, ya que al realizar las pruebas iniciales del mismo, y probar con otros valores de frecuencia, éstos no permitían su correcto funcionamiento, con el valor mencionado anteriormente se comprobó que el modem trabaja adecuadamente y con las condiciones requeridas para este proyecto.

- La velocidad de transmisión de los mensajes de texto, por medio del módem GSM depender del tráfico de la red GSM operadora (Movistar, Claro o Alegro) que éste prestando los servicios.

- El compilador BASCOM AVR permite un desarrollo más fácil y eficaz de la programación, ya que cuenta con instrucciones y comandos que son compatibles con algunos dispositivos usados en el presente proyecto como son: el reloj en tiempo real DS1307 o la comunicación serial utilizada para el manejo del modem y el lector RFID.

- Para acceder al módulo el operador no requiere que su tag esté en línea de vista o contacto físico con el lector, únicamente necesita estar a una distancia máxima de 10cm. para que lector reconozca el tag.

- En el Ecuador, la tecnología RFID está alcanzando acogida considerable debido a que muchas empresas están invirtiendo en el uso de ésta para obtener un excelente rendimiento y eficiencia de sus procesos, lo que conlleva un ahorro y optimización de recursos.

- El uso de los sistemas RFID va a tener un impacto importante sobre la actividad diaria de industrias, instituciones e inclusive de personas cuando cada vez más productos sean etiquetados y lleguen a los clientes finales propiciando la aparición de nuevas aplicaciones y servicios basados en RFID.

- Una de las desventajas de la tecnología RFID es que al momento de trabajar con objetos producidos con materiales metálicos, materiales absorbentes (como el agua) o embalados dentro de un material de estas características, puede generar fallas parciales o totales al intentar leer datos del tag. En la actualidad existen tags y lectores especialmente diseñados para operar con este tipo de materiales, pero el costo es demasiado elevado.

- El desarrollo de este sistema es una herramienta innovadora y útil a nivel nacional pues hace aportes importantes a la industria electrónica del país.

- El uso de los sistemas de control de acceso no están únicamente enfocados hacia las empresas, sino que poco a poco están usándose en los hogares dentro del campo de la domótica o incluso dentro de edificios residenciales, ya que su costo se ha ido reduciendo.

5.2 RECOMENDACIONES

- Para un correcto funcionamiento de la base de datos, es necesario conocer ciertos parámetros del lenguaje SQL, como son: comandos, clausulas,

operadores lógicos, operadores de comparación; los mismos que sirven para actualizar, crear y manipular cualquier base de datos.

- La base de datos desarrollada en MYSQL, es de fácil acceso por parte de la o las personas encargadas de la página dedicada a la interfaz de administración, lo que conlleva a que pueda ser modificada, provocando un mal funcionamiento de toda la interfaz. Por lo mismo se recomienda que se escoja minuciosamente la persona que maneje la interfaz.

- En la actualidad, la comunicación por el puerto serial de la PC ya no es muy utilizada, debido a que los computadores portátiles ya no vienen con este dispositivo, que ahora es reemplazado por el puerto USB, por tanto se recomienda que si se van a utilizar computadores portátiles con el modem GSM, se adquiera el respectivo conversor de RS-232 a USB.

- Se recomienda tener activado el plan tarifario de todos los chips de los módems GSM para que la información sea enviada mediante mensajes de texto sin inconvenientes.

- Antes de realizar la adaptación definitiva al lector RFID; es recomendable realizar pruebas de lectura al lector RFID utilizado en este proyecto, porque según el datasheet del mismo indicaba una distancia máxima de lectura de 16cm; pero en la práctica esto no se cumple; ya que la distancia real máxima de lectura fue de 10cm.

- Para una mejor explotación de estos recursos tecnológicos se sugiere realizar una investigación más amplia a cerca de las tecnologías aplicadas en este proyecto: RFID, GSM, ya que los mismos tiene una vasta aplicación en el campo de la Automatización y las Comunicaciones.

- Se recomienda que este proyecto se expanda a todos los armarios telefónicos del país, puesto que esto garantizará un mejor funcionamiento de éstos además de un mayor prestigio para la empresa.

REFERENCIAS BIBLIOGRÁFICAS

[1] http://mironlogistikos.blogspot.com/2007/03/funcionamento-de-um-sistema-rfid.html

[2] http://blog.pucp.edu.pe/item/73623/rfid-radio-frequency-identificator

[3] HUNT Daniel V. PULGIA Albert Mike – RFID A Guide to Radio Frequency Identification.

[4] http://foro.prodescargas.com/showthread.php?t=44682

[5] http://www.dipolerfid.es/productos/RFID_tag/Clasificacion_RFID_tags.aspx

[6] PORTILLO J., BERMEJO A., BERNADOS A.; Tecnología de Identificación por Radio frecuencia (RFID): Aplicaciones en el ámbito de la salud.

[7] bibdigital.epn.edu.ec/bitstream/15000/1779/1/CD-2365.pdf

[8] AETIC; La Tecnología RFID: Usos y oportunidades.

[9] http://www.maestrosdelweb.com/editorial/aplicaciones-de-la-tecnologia-rfid-la-educacion/

[10] http:// redyseguridad.fip.unam.mx/proyectos/biometria/basesteoricas.html

[11] http://cuestiondedinero.wordpress.com/2009/11/20/%C2%BFa-donde-se-saca-el-codigo-de-barras-y-cual-es-el-tramite/

[12] http://www.accesor.com/esp/detail_product.php?id_article=105

[13] http://tecnologicodominicano.blogspot.com/2010_05_01_archive.html

[14] http://www.intelektron.com/tecnologias/identificacion_intro.htm

[15] http://www.sparkfun.com/products/8628

[16] http://www.olimex.cl/product_info.php?cPath=50_87&products_id=504

[17] http://creativeelectron.net/shop/index.php/gsm-gprs-modem-forwell-m12z111-1.html

[18] http://www.icgate.com/mall/m_mall_list.php

[19] http://www.datasheetdir.com/ATMEGA324P+AVR-microcontrollers

[20] http://www.5hz-electronica.com/generalic.aspx

[21] http://learning.media.mit.edu/projects/gogo/parts_pdf/EEPROM%20-%2024LC256.pdf

[22] http://picaxe.electronicasimple.com/2009/03/reloj-tiempo-real-ds1307.html

[23] http://arduino.cc/forum/index.php?topic=51562.0

[24] http://www.electroalarma.com.ar/productos/intrusion.php

[25] http://www.monografias.com/trabajos11/basda/basda.shtml

[26] http://www.etimundo.com.mx/informacion/codigo_barras.html

[27] http://memorias-digtelecomii.es.tl/Memoria-EEPROM.htm

[28] http://www.dmd.es/bascom-a.htm

[29] http://es.wikipedia.org/wiki/Delphi_for_PHP

ANEXOS

ANEXO A

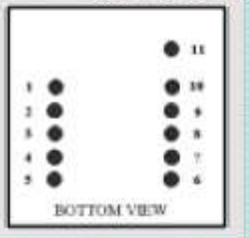
DATASHEET LECTOR RFID ID-20

ID SERIES DATASHEET MAR 01, 2005

ID-2/ID-12 Brief Data

The ID2. ID12 and ID20 are similar to the obsolete ID0, ID10 and ID15 MK(ii) series devices, but they have extra pins that allow Magnetic Emulation output to be included in the functionality. The ID-12 and ID-20 come with internal antennas, and have read ranges of 12+ cm and 16+ cm, respectively. With an external antenna, the ID-2 can deliver read ranges of up to 25 cm. All three readers support ASCII, Wiegand26 and Magnetic ABA Track2 data formats.

ID2 / ID12 / ID20 PIN-OUT



1. GND
2. RES (Reset Bar)
3. ANT (Antenna)
4. ANT (Antenna)
5. CP
6. Future
7. +/- (Format Selector)
8. D1 (Data Pin 1)
9. D0 (Data Pin 0)
10. LED (LED / Beeper)
11. +5V

Operational and Physical Characteristics

Parameters	ID-2	ID-12	ID-20
Read Range	N/A (no internal antenna)	12+ cm	16+ cm
Dimensions	21 mm x 19 mm x 6 mm	26 mm x 26 mm x 7 mm	40 mm x 40 mm x 9 mm
Frequency	125 kHz	125 kHz	125 kHz
Card Format	EM 4001 or compatible	EM 4001 or compatible	EM 4001 or compatible
Encoding	Manchester 64-bit, modulus 64	Manchester 64-bit, modulus 64	Manchester 64-bit, modulus 64
Power Requirement	5 VDC @ 13mA nominal	5 VDC @ 30mA nominal	5 VDC @ 65mA nominal
I/O Output Current	+/-200mA PK	-	-
Voltage Supply Range	+4.6V through +5.4V	+4.6V through +5.4V	+4.6V through +5.4V

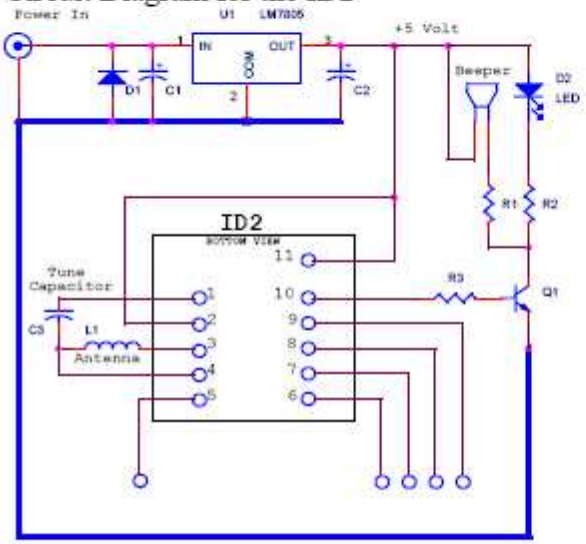
Pin Description & Output Data Formats

Pin No.	Description	ASCII	Magnet Emulation	Wiegand26
Pin 1	Zero Volts and Tuning Capacitor Ground	GND 0V	GND 0V	GND 0V
Pin 2	Strap to +5V	Reset Bar	Reset Bar	Reset Bar
Pin 3	To External Antenna and Tuning Capacitor	Antenna	Antenna	Antenna
Pin 4	To External Antenna	Antenna	Antenna	Antenna
Pin 5	Card Present	No function	Card Present *	No function

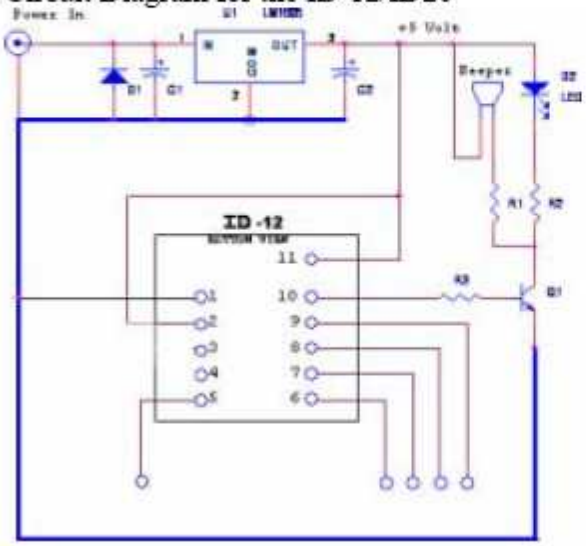
Pin 6	Future	Future	Future	Future
Pin 7	Format Selector (+/-)	Strap to GND	Strap to Pin 10	Strap to +5V
Pin 8	Data 1	CMOS	Clock *	One Output *
Pin 9	Data 0	TTL Data (inverted)	Data *	Zero Output *
Pin 10	3.1 kHz Logic	Beeper / LED	Beeper / LED	Beeper / LED
Pin 11	DC Voltage Supply	+5V	+5V	+5V

* Requires 4K7 Pull-up resistor to +5V

Circuit Diagram for the ID2



Circuit Diagram for the ID-12/ID20



DATA FORMATS

Output Data Structure – ASCII

STX (02h)	DATA (10 ASCII)	CHECK SUM (2 ASCII)	CR	LF	ETX (03h)

[The 1byte (2 ASCII characters) Check sum is the "Exclusive OR" of the 5 hex bytes (10 ASCII) Data characters.]

Output Data Structure – Wiegand26

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
P	E	E	E	E	E	E	E	E	E	E	E	E	O	O	O	O	O	O	O	O	O	O	O	O	P
Even parity (E)													Odd parity (O)												

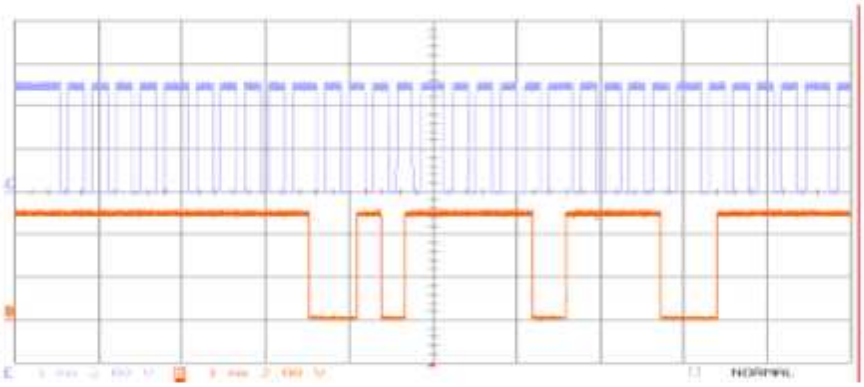
P = Parity start bit and stop bit

Output Data Magnetic ABA Track2

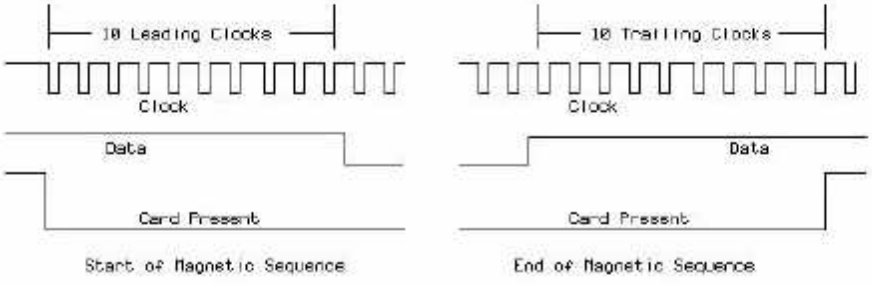
10 Leading Zeros	SS	Data	ES	LCR	10 Ending Zeros

[SS is the Start Character of 11010, ES is the end character of 11111, LRC is the Longitudinal Redundancy Check.]

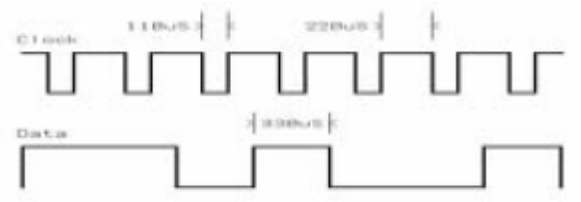
Magnetic Emulation Waveforms



Start and End Sequences For Magnetic Timing

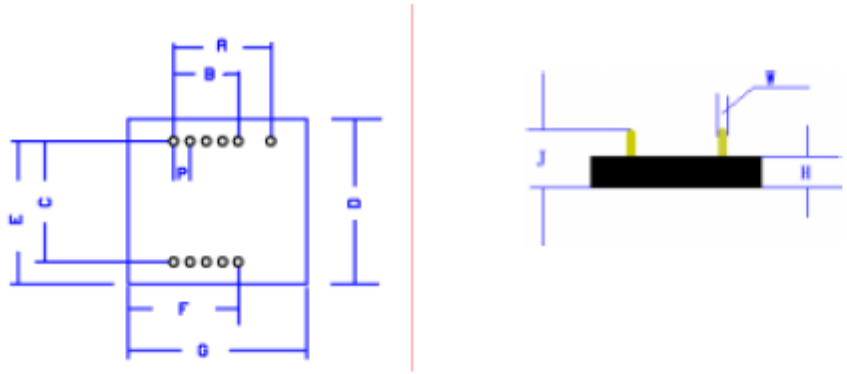


DATA TIMINGS FOR MAGNETIC EMULATION



The magnetic Emulation Sequence starts with the Card Present Line going active (down). There next follows 10 clocks with Zero '0' data. At the end of the 10 leading clocks the start character (11010) is sent and this is followed by the data. At the end of the data the end character is sent followed by the LCR. Finally 10 trailing clocks are sent and the card present line is raised.
The data bit duration is approximately 330uS. The approximate clock duration is 110uS. Because of the symmetry data can be clocked off either the rising or falling edge of the clock.

Dimensions (Top View) (mm)



	ID-0/ID-2wr			ID-10/ID-12wr			ID-15/ID-20wr		
	Nom.	Min.	Max.	Nom.	Min.	Max.	Nom.	Min.	Max
A	12.0	11.6	12.4	12.0	11.6	12.4	12.0	11.6	12.4
B	8.0	7.6	8.4	8.0	7.6	8.4	8.0	7.6	8.4
C	15.0	14.6	15.4	15.0	14.6	15.4	15.0	14.6	15.4
D	20.5	20.0	21.5	25.3	24.9	25.9	40.3	40.0	41.0
E	18.5	18.0	19.2	20.3	19.8	20.9	27.8	27.5	28.5
F	14.0	13.0	14.8	16.3	15.8	16.9	22.2	21.9	23.1
G	22.0	21.6	22.4	26.4	26.1	27.1	38.5	38.2	39.2
P	2.0	1.8	2.2	2.0	1.8	2.2	2.0	1.8	2.2
H	5.92	5.85	6.6	6.0	5.8	6.6	6.8	6.7	7.0
J	9.85	9.0	10.5	9.9	9.40	10.5	9.85	9.4	10.6
W	0.66	0.62	0.67	0.66	0.62	0.67	0.66	0.62	0.67

Note – measurements do not include any burring of edges.
NOTICE - Innovated Devices reserve the right to change these specifications without prior notice.

Designing Coils for ID2

The recommended Inductance is 1.08mH to be used with an internal tuning capacitor of 1n5. In general the bigger the antenna the better, provided the reader is generating enough field strength to excite the tag. The ID-2 is relatively low power so a maximum coil size of 15x15cm is recommended if it is intended to read ISO cards. If the reader is intended to read glass tags the maximum coil size should be smaller, say 10x10cm.

There is a science to determine the exact size of an antenna but there are so many variables that in general it is best to get a general idea after which a degree of 'Try it and see' is unavoidable.

If the reader is located in a position where there is a lot of heavy interference then less range cannot be avoided. In this situation the coil should be made smaller to increase the field strength and coupling.

It is difficult to give actual examples of coils for hand wounding because the closeness and tightness of the winding will significantly change the inductance. A professionally wound coil will have much more inductance than a similar hand wound coil.

For those who want a starting point into practical antenna winding it was found that 63 turns on a 120mm diameter former gave an inductance of 1.08mH. For those contemplating adding an additional tuning capacitor it was found that 50 turns on a 120mm diameter former gave 700uH. The wire diameter is not important.
Anybody who wishes to be more theoretical we recommend a trip to the Microchip Website where we found an application sheet for Loop Antennas.
http://ww1.microchip.com/downloads/en/AppNotes/00831b.pdf

The Tuning Capacitor

It is recommended that the internal 1n% capacitor is used for tuning, however a capacitor may be also be added externally. The combined capacitance should not exceed 2n7. Do not forget that the choice of tuning capacitor can also substantially affect the quality of your system. The Id12 is basically an ID2 with an internal antenna. The loss in an ID12 series antenna is required to be fairly high to limit the series current. A low Q will hide a lot of the shortcomings of the capacitor, but for quality and reliability and repeatability the following capacitors are recommend.

Polypropylene	Good Readily available. Ensure AC voltage at 125kHz is sufficient.
COG/NPO	Excellent. Best Choice
Silver Mica	Excellent but expensive
Polycarbonate	Good Readily available. Ensure AC voltage at 125kHz is sufficient.

Voltage Working.

A capacitor capable of withstanding the RMS voltage at 125KHz MUST be chosen. The working voltage will depend on the coil design. I suggest the designer start with rugged 1n5 Polypropylene 630v capacitor to do his experiments and the come down to a suitable size/value. The capacitor manufacturer will supply information on their capacitors. Do not simply go by the DC voltage. This means little. A tolerance of 2% is preferable. A tolerance of 5% is acceptable.

Fine Tuning

We recommend using an oscilloscope for fine-tuning. Connect the oscilloscope to observe the 125KHz AC voltage across the coil. Get a sizeable piece of ferrite and bring it up to the antenna loop. If the voltage increases then you need more inductance (or more capacitance). If the voltage decreases as you bring the ferrite up to the antenna then the inductance is too great. If you have no ferrite then a piece of aluminum

sheet may be used for testing in a slightly different way. Opposing currents will flow in the aluminum and it will act as a negative inductance. If the 125kH AC voltage increases as the aluminum sheet approaches the antenna then the inductance is too high. Note it may be possible that the voltage will first maximize then decrease. This simply means that you are near optimum tuning. If you are using ferrite then the coil is a little under value and if you are using an aluminum sheet then the coil is a over under value.

ANEXO B

DATASHEET MODEM GSM ZTE MG3006

ZTE MG3006 Module Technical Specifications

VERSION：V1.3

ZTE CORPORATION

1 Summary

ZTE MG3006 modules is a type of GSM/GPRS wireless module supports Quad Band, with abundant voice, SMS, data service functions and so on. The modules can be applied in data transmission, wireless POS, security, lottery machine, auto-metering, wireless fax, small switch, tobacco machine, information machine, wireless AD, wireless media, medical ward, remote monitoring, railway terminals, intelligent electronic products and vehicle-tracking systems etc.

This document take MG3006 module as an example, introduces the appearance, hardware framework, functions, technical specifications and relevant test standards for module in detail.

2 Abbreviation

Abbr.	Full name
ADC	Analog-Digital Converter
AFC	Automatic Frequency Control
AGC	Automatic Gain Control
ARFCN	Absolute Radio Frequency Channel Number
ARP	Antenna Reference Point
ASIC	Application Specific Integrated Circuit
BER	Bit Error Rate
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CDG	CDMA Development Group
CS	Coding Scheme
CSD	Circuit Switched Data
CPU	Central Processing Unit
DAI	Digital Audio interface
DAC	Digital-to-Analog Converter
DCE	Data Communication Equipment
DSP	Digital Signal Processor
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
DTR	Data Terminal Ready
EFR	Enhanced Full Rate
EGSM	Enhanced GSM
EMC	Electromagnetic Compatibility
EMI	Electro Magnetic Interference
ESD	Electronic Static Discharge
ETS	European Telecommunication Standard
FDMA	Frequency Division Multiple Access

FR	Full Rate
GPRS	General Packet Radio Service
GSM	Global Standard for Mobile Communications
HR	Half Rate
IC	Integrated Circuit
IMEI	International Mobile Equipment Identity
ISO	International Standards Organization
ITU	International Telecommunications Union
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MCU	Machine Control Unit
MMI	Man Machine Interface
MS	Mobile Station
PCB	Printed Circuit Board
PCL	Power Control Level
PCS	Personal Communication System
PDU	Protocol Data Unit
PLL	Phase Locked Loop
PPP	Point-to-point protocol
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read-only Memory
RMS	Root Mean Square
RTC	Real Time Clock
SIM	Subscriber Identification Module
SMS	Short Message Service
SRAM	Static Random Access Memory
TA	Terminal adapter
TDMA	Time Division Multiple Access
TE	Terminal Equipment also referred it as DTE
UART	Universal asynchronous receiver-transmitter
UIM	User Identifier Management
USB	Universal Serial Bus
VSWR	Voltage Standing Wave Ratio
ZTE	ZTE Corporation

3 Appearance and framework

Appearance of MG3006 is as following figure 3-1:

Figure 3-1 appearance of MG3006 module

- Dimension（length x width x height）：44.0 mm x 28.0mm x 7.6mm
- Weight：8g

4 Functions and interfaces

The basic functions of module are as below:

- Support Quad Band：*GSM 850/EGSM 900/DCS 1800/PCS 1900*
- Support packet data service
- Support circuit switched data service
- Support SMS service
- Support standard AT commands and extended AT commands
- Support standard UART interface
- Support dual-path audio interface
- Supplementary service functions：incoming call display, call forward, call maintenance, call stand by, triple call service and so on.
- Support TCP/IP protocol

5 Technical specifications

5.1 Communication protocols and technical specifications

The communication protocols and technical specifications of MG3006 modules is as following table 5-1:

Table 5-1 communication protocols and technical specifications

Access mode	GSM
Tech-spec	GSM phase 2/2+

Rx/Tx frequency interval	45MHz for GSM 850 45MHz for EGSM 900 95MHz for DCS 1800 80MHz for PCS 1900
Voice encoding	- Half rate (HR) - Full rate (FR) - Enhanced Full rate (EFR) - Adaptive Multi-Rate (AMR)

- MG3006 frequency band：GSM 850/EGSM 900/DCS 1800/PCS 1900 MHz. There frequency bands are shown in table 5-2. Data transmission rate depends on interval assignment and channel encoding of GPRS.

Table5-2 frequency band

name	Tx frequency band(MHz)	Rx frequency band (MHz)
GSM 850	824~849 MHz	869~894MHz
EGSM 900	880~915 MHz	925~960MHz
DCS 1800	1710~1785MHz	1805~1880MHz
PCS 1900	1850~1910MHz	1930~1990MHz

MG3006 module supports CLASS 10，the interval assignment is as following tableTable5-3:

Table5-3 interval assignment

down	up	Maximum supported interval at the same time
4	2	5

GPRS encoding modes supported by MG3006 module are as following table 5-4:

Table5-4 encoding modes

Encoding modes	Data rate(kbps)
CS-1	9.05
CS-2	13.4
CS-3	15.6
CS-4	21.4

The maximum theoretic data rate supported by MG3006 module is as following table5-5:

Table5-5 data rate

Encoding mode	Download (kbps)	Upload(kbps)
CS-1	36.2	18.1
CS-2	53.6	26.8
CS-3	62.4	31.2
CS-4	85.6	42.8

MG3006 module supports Class B，but when GPRS and GSM service exist at the same time, GPRS breaks off, on the other hand, voice and SMS service of GSM is prior. After that GPRS

5.4 Recommendation of antenna specs

The recommended antenna specs are as following table 5-18:

Table5-18 recommended antenna specs

VSWR	1.5:1 maximum
gain	At least 0 dBi in one direction
Input impedance	50Ω
Polarized form	Vertical polarizing

The requirements for antenna's gain are different in different environment. Commonly, in used frequency range, the larger gain, the better capability; otherwise, out of this range, the smaller gain, the better capability.

The antenna seat's type of MG3006 module is MM9329-2700B.

5.5 Power supply

5.5.1 Input voltage

The input voltage is shown in table 5-19:

Table5-19 input voltage

state	Max. voltage	Typical voltage	Min. voltage
Power supply	4.25 VDC	3.90 VDC	3.30 VDC

5.6 Working conditions

- Working temperature:-20℃ ~ +80℃
- Storage temperature:-40℃ ~ +85℃
- humidity：0% ~ 95%

6 Reliability test standard

6.1 Low temperature running experiment

- Required Temperature: -20℃
- Duration Time: 16H
- Reference standard：GB/T 2423.1-2001

6.2 Low temperature storage experiment

- Required Temperature: -40℃
- Duration Time: 24H
- Reference standard：GB/T 2423.1-2001

6.3 High temperature running experiment

- Required Temperature: +80℃
- Duration Time: 16H
- Reference standard：GB/T 2423.2-2001

6.4 High temperature storage experiment

- Required Temperature: +85℃
- Duration Time: 24H
- Reference standard：GB/T 2423.2-2001

6.5 High temperature, high humidity experiment

- Required Temperature: +40℃
- Required Humidity: 85%RH
- Duration Time: 48H
- Reference standard：GB/T 2423.2-2001

6.6 High-low temperature striking experiment

- Cycles: 5
- Temperature Range: -20℃～+80℃
- Duration Time: 2h
- recovery time: 2h
- Reference standard：GB/T 2423.3-2001

ANEXO C

DATASHEET MICROCONTROLADOR ATMEGA 324P

Features

- High-performance, Low-power AVR® 8-bit Microcontroller
- Advanced RISC Architecture
  - 131 Powerful Instructions – Most Single-clock Cycle Execution
  - 32 x 8 General Purpose Working Registers
  - Fully Static Operation
  - Up to 20 MIPS Throughput at 20 MHz
  - On-chip 2-cycle Multiplier
- High Endurance Non-volatile Memory segments
  - 16/32/64K Bytes of In-System Self-programmable Flash program memory
  - 512B/1K/2K Bytes EEPROM
  - 1/2/4K Bytes Internal SRAM
  - Write/Erase Cycles: 10,000 Flash/ 100,000 EEPROM
  - Data retention: 20 years at 85°C/100 years at 25°C
  - Optional Boot Code Section with Independent Lock Bits
    In-System Programming by On-chip Boot Program
    True Read-While-Write Operation
  - Programming Lock for Software Security
- JTAG (IEEE std. 1149.1 Compliant) Interface
  - Boundary-scan Capabilities According to the JTAG Standard
  - Extensive On-chip Debug Support
  - Programming of Flash, EEPROM, Fuses, and Lock Bits through the JTAG Interface
- Peripheral Features
  - Two 8-bit Timer/Counters with Separate Prescalers and Compare Modes
  - One 16-bit Timer/Counter with Separate Prescaler, Compare Mode, and Capture Mode
  - Real Time Counter with Separate Oscillator
  - Six PWM Channels
  - 8-channel, 10-bit ADC
    Differential mode with selectable gain at 1x, 10x or 200x
  - Byte-oriented Two-wire Serial Interface
  - Two Programmable Serial USART
  - Master/Slave SPI Serial Interface
  - Programmable Watchdog Timer with Separate On-chip Oscillator
  - On-chip Analog Comparator
  - Interrupt and Wake-up on Pin Change
- Special Microcontroller Features
  - Power-on Reset and Programmable Brown-out Detection
  - Internal Calibrated RC Oscillator
  - External and Internal Interrupt Sources
  - Six Sleep Modes: Idle, ADC Noise Reduction, Power-save, Power-down, Standby and Extended Standby
- I/O and Packages
  - 32 Programmable I/O Lines
  - 40-pin PDIP, 44-lead TQFP, and 44-pad QFN/MLF
- Operating Voltages
  - 1.8 - 5.5V for ATmega164P/324P/644PV
  - 2.7 - 5.5V for ATmega164P/324P/644P
- Speed Grades
  - ATmega164P/324P/644PV: 0 - 4MHz @ 1.8 - 5.5V, 0 - 10MHz @ 2.7 - 5.5V
  - ATmega164P/324P/644P: 0 - 10MHz @ 2.7 - 5.5V, 0 - 20MHz @ 4.5 - 5.5V
- Power Consumption at 1 MHz, 1.8V, 25°C for ATmega164P/324P/644P
  - Active: 0.4 mA
  - Power-down Mode: 0.1µA
  - Power-save Mode: 0.6µA (Including 32 kHz RTC)

8-bit AVR® Microcontroller with 16/32/64K Bytes In-System Programmable Flash

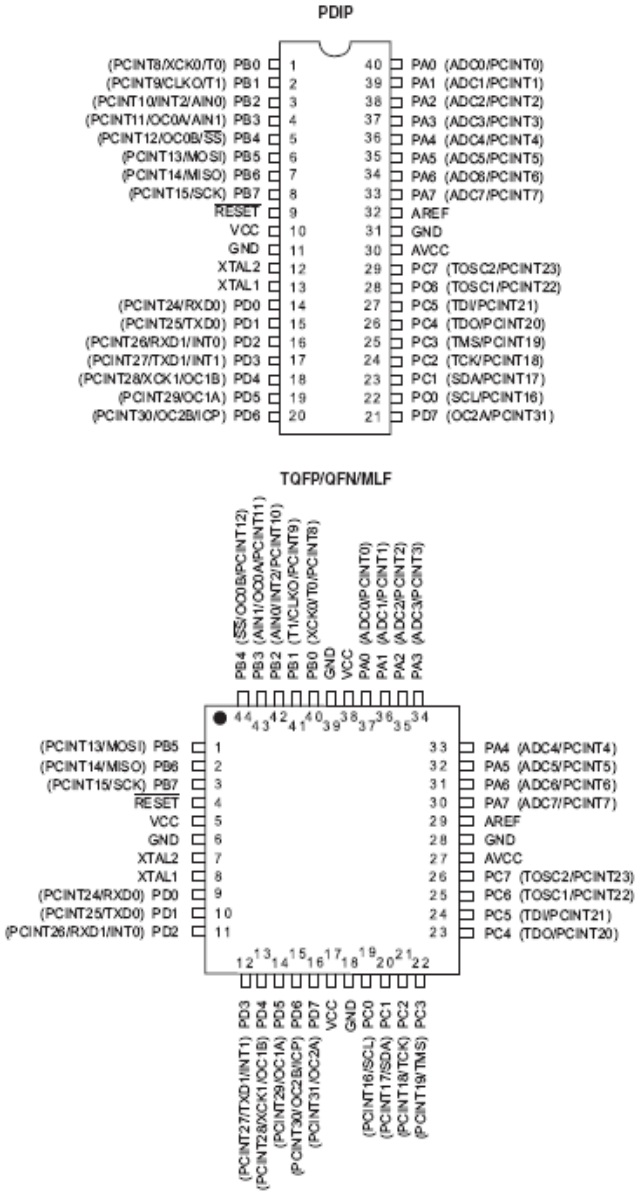
ATmega164P/V
ATmega324P/V
ATmega644P/V

Preliminary

8011G–AVR–08/07

1. Pin Configurations

Figure 1-1. Pinout ATmega164P/324P/644P



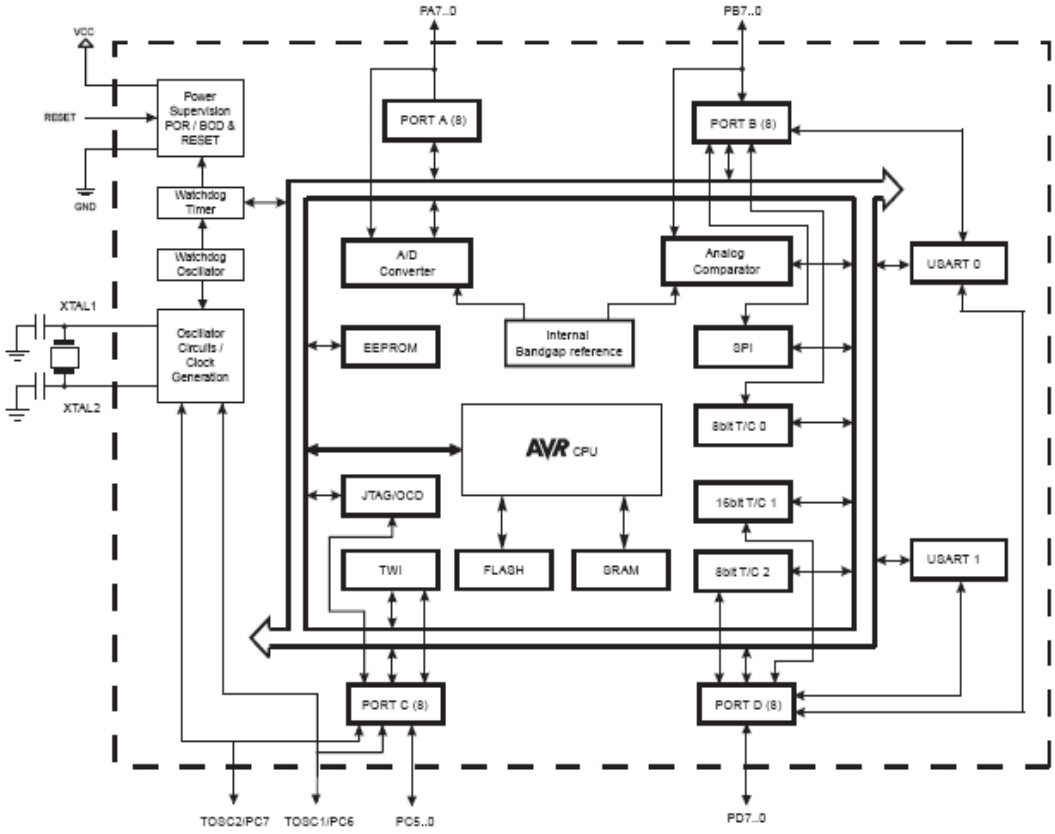
Note: The large center pad underneath the QFN/MLF package should be soldered to ground on the board to ensure good mechanical stability.

2. Overview

The ATmega164P/324P/644P is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega164P/324P/644P achieves throughputs approaching 1 MIPS per MHz allowing the system designer to optimize power consumption versus processing speed.

2.1 Block Diagram

Figure 2-1. Block Diagram



The AVR core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers.

The ATmega164P/324P/644P provides the following features: 16/32/64K bytes of In-System Programmable Flash with Read-While-Write capabilities, 512B/1K/2K bytes EEPROM, 1/2/4K bytes SRAM, 32 general purpose I/O lines, 32 general purpose working registers, Real Time Counter (RTC), three flexible Timer/Counters with compare modes and PWM, 2 USARTs, a byte oriented 2-wire Serial Interface, a 8-channel, 10-bit ADC with optional differential input stage with programmable gain, programmable Watchdog Timer with Internal Oscillator, an SPI serial port, IEEE std. 1149.1 compliant JTAG test interface, also used for accessing the On-chip Debug system and programming and six software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, SPI port, and interrupt system to continue functioning. The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next interrupt or Hardware Reset. In Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules except Asynchronous Timer and ADC, to minimize switching noise during ADC conversions. In Standby mode, the Crystal/Resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low power consumption. In Extended Standby mode, both the main Oscillator and the Asynchronous Timer continue to run.

The device is manufactured using Atmel's high-density nonvolatile memory technology. The On-chip ISP Flash allows the program memory to be reprogrammed in-system through an SPI serial interface, by a conventional nonvolatile memory programmer, or by an On-chip Boot program running on the AVR core. The boot program can use any interface to download the application program in the application Flash memory. Software in the Boot Flash section will continue to run while the Application Flash section is updated, providing true Read-While-Write operation. By combining an 8-bit RISC CPU with In-System Self-Programmable Flash on a monolithic chip, the Atmel ATmega164P/324P/644P is a powerful microcontroller that provides a highly flexible and cost effective solution to many embedded control applications.

The ATmega164P/324P/644P AVR is supported with a full suite of program and system development tools including: C compilers, macro assemblers, program debugger/simulators, in-circuit emulators, and evaluation kits.

2.2 Comparison Between ATmega164P, ATmega324P and ATmega644P

Table 2-1. Differences between ATmega164P and ATmega644P

Device	Flash	EEPROM	RAM
ATmega164P	16 Kbyte	512 Bytes	1 Kbyte
ATmega324P	32 Kbyte	1 Kbyte	2 Kbyte
ATmega644P	64 Kbyte	2 Kbyte	4 Kbyte

2.3 Pin Descriptions

2.3.1 VCC

Digital supply voltage.

2.3.2 GND

Ground.

2.3.3 Port A (PA7:PA0)

Port A serves as analog inputs to the Analog-to-digital Converter.

Port A also serves as an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port A output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port A pins that are externally pulled low will source current if the pull-up resistors are activated. The Port A pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port A also serves the functions of various special features of the ATmega164P/324P/644P as listed on page 80.

2.3.4 Port B (PB7:PB0)

Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port B also serves the functions of various special features of the ATmega164P/324P/644P as listed on page 82.

2.3.5 Port C (PC7:PC0)

Port C is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port C output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port C also serves the functions of the JTAG interface, along with special features of the ATmega164P/324P/644P as listed on page 85.

2.3.6 Port D (PD7:PD0)

Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port D pins that are externally pulled low will source current if the pull-up resistors are activated. The Port D pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port D also serves the functions of various special features of the ATmega164P/324P/644P as listed on page 87.

2.3.7 $\overline{\text{RESET}}$

Reset input. A low level on this pin for longer than the minimum pulse length will generate a reset, even if the clock is not running. The minimum pulse length is given in "System and Reset Characteristics" on page 331. Shorter pulses are not guaranteed to generate a reset.

2.3.8 XTAL1

Input to the inverting Oscillator amplifier and input to the internal clock operating circuit.

2.3.9 XTAL2

Output from the inverting Oscillator amplifier.

2.3.10 AVCC

AVCC is the supply voltage pin for Port F and the Analog-to-digital Converter. It should be externally connected to V_{CC}, even if the ADC is not used. If the ADC is used, it should be connected to V_{CC} through a low-pass filter.

2.3.11 AREF

This is the analog reference pin for the Analog-to-digital Converter.

27. Electrical Characteristics

Absolute Maximum Ratings*

Operating Temperature	-55°C to +125°C
Storage Temperature	-65°C to +150°C
Voltage on any Pin except $\overline{\text{RESET}}$ with respect to Ground	-0.5V to V_{CC}+0.5V
Voltage on $\overline{\text{RESET}}$ with respect to Ground	-0.5V to +13.0V
Maximum Operating Voltage	6.0V
DC Current per I/O Pin	40.0 mA
DC Current V_{CC} and GND Pins	200.0 mA

*NOTICE: Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

27.1 DC Characteristics

T_A = -40°C to 85°C, V_{CC} = 1.8V to 5.5V (unless otherwise noted)

Symbol	Parameter	Condition	Min.(5)	Typ.	Max.(5)	Units
V_{IL}	Input Low Voltage,Except XTAL1 and Reset pin	V_{CC} = 1.8V - 2.4V V_{CC} = 2.4V - 5.5V	-0.5 -0.5		$0.2V_{CC}$(1) $0.3V_{CC}$(1)	V
V_{IL1}	Input Low Voltage, XTAL1 pin	V_{CC} = 1.8V - 5.5V	-0.5		$0.1V_{CC}$(1)	V
V_{IL2}	Input Low Voltage, RESET pin	V_{CC} = 1.8V - 5.5V	-0.5		$0.1V_{CC}$(1)	V
V_{IL3}	Input Low Voltage. RESET pin as I/O	V_{CC} = 1.8V - 5.5V	NA	NA	NA	V
V_{IH}	Input High Voltage, Except XTAL1 and RESET pins	V_{CC} = 1.8V - 2.4V V_{CC} = 2.4V - 5.5V	$0.7V_{CC}$(2) $0.6V_{CC}$(2)		V_{CC} + 0.5 V_{CC} + 0.5	V
V_{IH1}	Input High Voltage, XTAL1 pin	V_{CC} = 1.8V - 2.4V V_{CC} = 2.4V - 5.5V	$0.8V_{CC}$(2) $0.7V_{CC}$(2)		V_{CC} + 0.5 V_{CC} + 0.5	V
V_{IH2}	Input High Voltage, RESET pin	V_{CC} = 1.8V - 5.5V	$0.9V_{CC}$(2)		V_{CC} + 0.5	V
V_{IH3}	Input High Voltage, RESET pin as I/O	V_{CC} = 1.8V - 2.4V V_{CC} = 2.4V - 5.5V	NA		NA	V
V_{OL}	Output Low Voltage(3),	I_{OL} = 5 mA, V_{CC} = 3V I_{OL} = 10 mA, V_{CC} = 5V			0.9 0.6	V
V_{OH}	Output High Voltage(4),	I_{OH} = -20 mA, V_{CC} = 5V I_{OH} = -10 mA, V_{CC} = 3V	4.2 2.3			V
V_{OL3}	Output Low Voltage Reset pin as I/O	NA	NA		NA	V
V_{OH3}	Output High Voltage RESET pin as I/O	NA	NA		NA	V
I_{IL}	Input Leakage Current I/O Pin	V_{CC} = 5.5V, pin low (absolute value)			1	µA

T_A = -40°C to 85°C, V_{CC} = 1.8V to 5.5V (unless otherwise noted) (Continued)

Symbol	Parameter	Condition	Min.[5]	Typ.	Max.[5]	Units
I_{IH}	Input Leakage Current I/O Pin	V_{CC} = 5.5V, pin high (absolute value)			1	µA
R_{RST}	Reset Pull-up Resistor		30		60	kΩ
R_{PU}	I/O Pin Pull-up Resistor		20		50	kΩ
V_{ACIO}	Analog Comparator Input Offset Voltage	V_{CC} = 5V V_{in} = V_{CC}/2		<10	40	mV
I_{ACLK}	Analog Comparator Input Leakage Current	V_{CC} = 5V V_{in} = V_{CC}/2	-50		50	nA
t_{ACID}	Analog Comparator Propagation Delay	V_{CC} = 2.7V V_{CC} = 4.0V		750 500		ns

Notes:
1. "Max" means the highest value where the pin is guaranteed to be read as low
2. "Min" means the lowest value where the pin is guaranteed to be read as high
3. Although each I/O port can sink more than the test conditions (20mA at VCC = 5V, 10mA at VCC = 3V) under steady state conditions (non-transient), the following must be observed:
   1.)The sum of all IOL, for ports PB0-PB7, XTAL2, PD0-PD7 should not exceed 100 mA.
   2.)The sum of all IOL, for ports PA0-PA3, PC0-PC7 should not exceed 100 mA.
   If IOL exceeds the test condition, VOL may exceed the related specification. Pins are not guaranteed to sink current greater than the listed test condition.
4. Although each I/O port can source more than the test conditions (20mA at VCC = 5V, 10mA at VCC = 3V) under steady state conditions (non-transient), the following must be observed:
   1.)The sum of all IOH, for ports PB0-PB7, XTAL2, PD0-PD7 should not exceed 100 mA.
   2.)The sum of all IOH, for ports PA0-PA3, PC0-PC7 should not exceed 100 mA.
   If IOH exceeds the test condition, VOH may exceed the related specification. Pins are not guaranteed to source current greater than the listed test condition.
5. These numbers are valid for ATmega164P and ATmega324P. They are preliminary values for ATmega644P representing design target.

ANEXO D

DATASHEET MEMORIA 24LC256

MICROCHIP 24AA256/24LC256/24FC256

256K I²C™ CMOS Serial EEPROM

Device Selection Table

Part Number	Vcc Range	Max. Clock Frequency	Temp. Ranges
24AA256	1.8-5.5V	400 kHz(1)	I
24LC256	2.5-5.5V	400 kHz	I, E
24FC256	1.8-5.5V	1 MHz(2)	I

Note 1: 100 kHz for Vcc < 2.5V.
2: 400 kHz for Vcc < 2.5V.

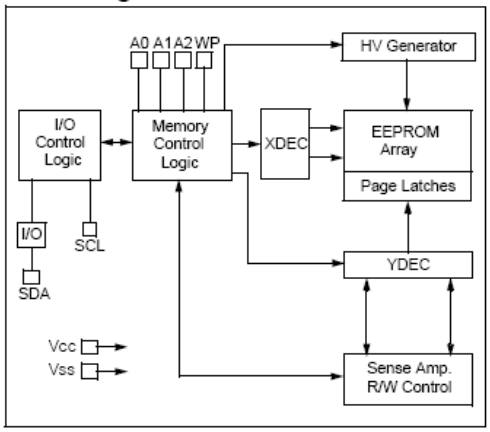
Features:

- Low-power CMOS technology:
  - Maximum write current 3 mA at 5.5V
  - Maximum read current 400 µA at 5.5V
  - Standby current 100 nA, typical at 5.5V
- 2-wire serial interface bus, I²C™ compatible
- Cascadable for up to eight devices
- Self-timed erase/write cycle
- 64-byte Page Write mode available
- 5 ms max. write cycle time
- Hardware write-protect for entire array
- Output slope control to eliminate ground bounce
- Schmitt Trigger inputs for noise suppression
- 1,000,000 erase/write cycles
- Electrostatic discharge protection > 4000V
- Data retention > 200 years
- 8-pin PDIP, SOIC, TSSOP, MSOP and DFN packages, 14-lead TSSOP package
- Pb-free finishes available
- Temperature ranges:
  - Industrial (I): -40°C to +85°C
  - Automotive (E): -40°C to +125°C

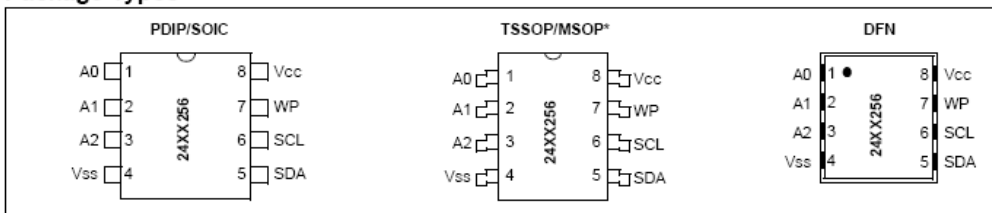
Description:

The Microchip Technology Inc. 24AA256/24LC256/24FC256 (24XX256*) is a 32K x 8 (256 Kbit) Serial Electrically Erasable PROM, capable of operation across a broad voltage range (1.8V to 5.5V). It has been developed for advanced, low-power applications such as personal communications or data acquisition. This device also has a page write capability of up to 64 bytes of data. This device is capable of both random and sequential reads up to the 256K boundary. Functional address lines allow up to eight devices on the same bus, for up to 2 Mbit address space. This device is available in the standard 8-pin plastic DIP, SOIC, TSSOP, MSOP and DFN packages.

Block Diagram



Package Types



Note: * Pins A0 and A1 are no connects for the MSOP package only.

*24XX256 is used in this document as a generic part number for the 24AA256/24LC256/24FC256 devices.

24AA256/24LC256/24FC256

1.0 ELECTRICAL CHARACTERISTICS

Absolute Maximum Ratings(†)

Vcc.....6.5V

All inputs and outputs w.r.t. Vss ..... -0.6V to Vcc +1.0V

Storage temperature .....-65°C to +150°C

Ambient temperature with power applied.....-40°C to +125°C

ESD protection on all pins .....≥ 4 kV

† NOTICE: Stresses above those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational listings of this specification is not implied. Exposure to Absolute Maximum Rating conditions for extended periods may affect device reliability.

TABLE 1-1: DC CHARACTERISTICS

DC CHARACTERISTICS			**Electrical Characteristics:** Industrial (I): Vcc = +1.8V to 5.5V TA = -40°C to +85°C Automotive (E): Vcc = +2.5V to 5.5V TA = -40°C to +125°C			
Param. No.	**Sym.**	**Characteristic**	**Min.**	**Max.**	**Units**	**Conditions**
D1	—	A0, A1, A2, SCL, SDA and WP pins:	—	—	—	—
D2	VIH	High-level input voltage	0.7 Vcc	—	V	—
D3	VIL	Low-level input voltage	—	0.3 Vcc 0.2 Vcc	V V	Vcc ≥ 2.5V Vcc < 2.5V
D4	VHYS	Hysteresis of Schmitt Trigger inputs (SDA, SCL pins)	0.05 Vcc	—	V	Vcc ≥ 2.5V **(Note)**
D5	VOL	Low-level output voltage	—	0.40	V	IOL = 3.0 ma @ Vcc = 4.5V IOL = 2.1 ma @ Vcc = 2.5V
D6	ILI	Input leakage current	—	±1	µA	VIN = Vss or Vcc, WP = Vss VIN = Vss or Vcc, WP = Vcc
D7	ILO	Output leakage current	—	±1	µA	VOUT = Vss or Vcc
D8	CIN, COUT	Pin capacitance (all inputs/outputs)	—	10	pF	Vcc = 5.0V **(Note)** TA = 25°C, FCLK = 1 MHz
D9	Icc Read	Operating current	—	400	µA	Vcc = 5.5V, SCL = 400 kHz
	Icc Write		—	3	mA	Vcc = 5.5V
D10	ICCS	Standby current	— —	1 5	µA µA	TA = -40°C to +85°C SCL = SDA = Vcc = 5.5V A0, A1, A2, WP = Vss TA = -40°C to +125°C SCL = SDA = Vcc = 5.5V A0, A1, A2, WP = Vss

Note: This parameter is periodically sampled and not 100% tested.

2.0 PIN DESCRIPTIONS

The descriptions of the pins are listed in Table 2-1.

TABLE 2-1: PIN FUNCTION TABLE

Name	8-pin PDIP	8-pin SOIC	8-pin TSSOP	8-pin MSOP	8-pin DFN	Function
A0	1	1	1	—	1	User Configurable Chip Select
A1	2	2	2	—	2	User Configurable Chip Select
(NC)	—	—	—	1, 2	—	Not Connected
A2	3	3	3	3	3	User Configurable Chip Select
Vss	4	4	4	4	4	Ground
SDA	5	5	5	5	5	Serial Data
SCL	6	6	6	6	6	Serial Clock
(NC)	—	—	—	—	—	Not Connected
WP	7	7	7	7	7	Write-Protect Input
Vcc	8	8	8	8	8	+1.8V to 5.5V (24AA256) +2.5V to 5.5V (24LC256) +1.8V to 5.5V (24FC256)

2.1 A0, A1, A2 Chip Address Inputs

The A0, A1 and A2 inputs are used by the 24XX256 for multiple device operations. The levels on these inputs are compared with the corresponding bits in the slave address. The chip is selected if the compare is true.

For the MSOP package only, pins A0 and A1 are not connected.

Up to eight devices (two for the MSOP package) may be connected to the same bus by using different Chip Select bit combinations. These inputs must be connected to either Vcc or Vss.

In most applications, the chip address inputs A0, A1 and A2 are hard-wired to logic '0' or logic '1'. For applications in which these pins are controlled by a microcontroller or other programmable device, the chip address pins must be driven to logic '0' or logic '1' before normal device operation can proceed.

2.2 Serial Data (SDA)

This is a bidirectional pin used to transfer addresses and data into and out of the device. It is an open drain terminal. Therefore, the SDA bus requires a pull-up resistor to Vcc (typical 10 kΩ for 100 kHz, 2 kΩ for 400 kHz and 1 MHz).

For normal data transfer, SDA is allowed to change only during SCL low. Changes during SCL high are reserved for indicating the Start and Stop conditions.

2.3 Serial Clock (SCL)

This input is used to synchronize the data transfer to and from the device.

2.4 Write-Protect (WP)

This pin must be connected to either Vss or Vcc. If tied to Vss, write operations are enabled. If tied to Vcc, write operations are inhibited but read operations are not affected.

3.0 FUNCTIONAL DESCRIPTION

The 24XX256 supports a bidirectional 2-wire bus and data transmission protocol. A device that sends data onto the bus is defined as a transmitter and a device receiving data as a receiver. The bus must be controlled by a master device which generates the Serial Clock (SCL), controls the bus access, and generates the Start and Stop conditions while the 24XX256 works as a slave. Both master and slave can operate as a transmitter or receiver, but the master device determines which mode is activated.

4.0 BUS CHARACTERISTICS

The following **bus protocol** has been defined:

- Data transfer may be initiated only when the bus is not busy.
- During data transfer, the data line must remain stable whenever the clock line is high. Changes in the data line, while the clock line is high, will be interpreted as a Start or Stop condition.

Accordingly, the following bus conditions have been defined (Figure 4-1).

4.1 Bus Not Busy (A)

Both data and clock lines remain high.

4.2 Start Data Transfer (B)

A high-to-low transition of the SDA line while the clock (SCL) is high, determines a Start condition. All commands must be preceded by a Start condition.

4.3 Stop Data Transfer (C)

A low-to-high transition of the SDA line, while the clock (SCL) is high, determines a Stop condition. All operations must end with a Stop condition.

4.4 Data Valid (D)

The state of the data line represents valid data when, after a Start condition, the data line is stable for the duration of the high period of the clock signal.

The data on the line must be changed during the low period of the clock signal. There is one bit of data per clock pulse.

Each data transfer is initiated with a Start condition and terminated with a Stop condition. The number of the data bytes transferred between the Start and Stop conditions is determined by the master device.

4.5 Acknowledge

Each receiving device, when addressed, is obliged to generate an Acknowledge signal after the reception of each byte. The master device must generate an extra clock pulse which is associated with this Acknowledge bit.

Note:	The 24XX256 does not generate any Acknowledge bits if an internal programming cycle is in progress.

A device that acknowledges must pull down the SDA line during the acknowledge clock pulse in such a way that the SDA line is stable low during the high period of the acknowledge related clock pulse. Of course, setup and hold times must be taken into account. During reads, a master must signal an end of data to the slave by NOT generating an Acknowledge bit on the last byte that has been clocked out of the slave. In this case, the slave (24XX256) will leave the data line high to enable the master to generate the Stop condition.

5.0 DEVICE ADDRESSING

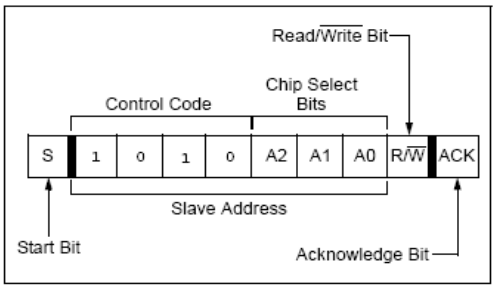
A control byte is the first byte received following the Start condition from the master device (Figure 5-1). The control byte consists of a 4-bit control code. For the 24XX256, this is set as '1010' binary for read and write operations. The next three bits of the control byte are the Chip Select bits (A2, A1, A0). The Chip Select bits allow the use of up to eight 24XX256 devices on the same bus and are used to select which device is accessed. The Chip Select bits in the control byte must correspond to the logic levels on the corresponding A2, A1 and A0 pins for the device to respond. These bits are, in effect, the three Most Significant bits of the word address.

For the MSOP package, the A0 and A1 pins are not connected. During device addressing, the A0 and A1 Chip Select bits (Figures 5-1 and 5-2) should be set to '0'. Only two 24XX256 MSOP packages can be connected to the same bus.

The last bit of the control byte defines the operation to be performed. When set to a one, a read operation is selected. When set to a zero, a write operation is selected. The next two bytes received define the address of the first data byte (Figure 5-2). Because only A14...A0 are used, the upper address bits are a "don't care." The upper address bits are transferred first, followed by the Less Significant bits.

Following the Start condition, the 24XX256 monitors the SDA bus checking the device type identifier being transmitted. Upon receiving a '1010' code and appropriate device select bits, the slave device outputs an Acknowledge signal on the SDA line. Depending on the state of the R/$\overline{W}$ bit, the 24XX256 will select a read or write operation.

FIGURE 5-1: CONTROL BYTE FORMAT

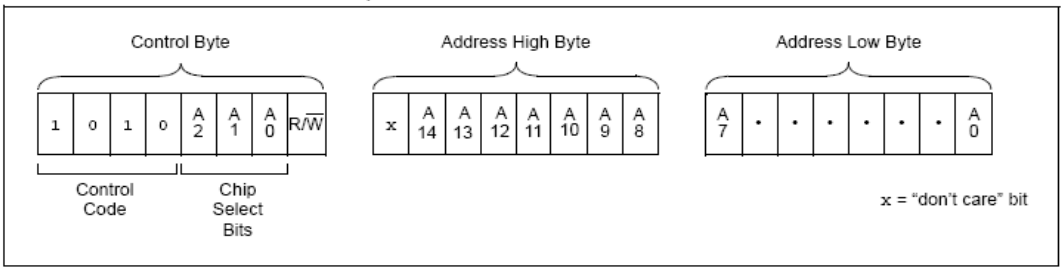


5.1 Contiguous Addressing Across Multiple Devices

The Chip Select bits A2, A1 and A0 can be used to expand the contiguous address space for up to 2 Mbit by adding up to eight 24XX256 devices on the same bus. In this case, software can use A0 of the **control byte** as address bit A15; A1 as address bit A16; and A2 as address bit A17. It is not possible to sequentially read across device boundaries.

For the MSOP package, up to two 24XX256 devices can be added for up to 512 Kbit of address space. In this case, software can use A2 of the control byte as address bit A17. Bits A0 (A15) and A1 (A16) of the **control byte** must always be set to a logic '0' for the MSOP.

FIGURE 5-2: ADDRESS SEQUENCE BIT ASSIGNMENTS



6.0 WRITE OPERATIONS

6.1 Byte Write

Following the Start condition from the master, the control code (four bits), the Chip Select (three bits) and the R/$\overline{W}$ bit (which is a logic low) are clocked onto the bus by the master transmitter. This indicates to the addressed slave receiver that the address high byte will follow after it has generated an Acknowledge bit during the ninth clock cycle. Therefore, the next byte transmitted by the master is the high-order byte of the word address and will be written into the Address Pointer of the 24XX256. The next byte is the Least Significant Address Byte. After receiving another Acknowledge signal from the 24XX256, the master device will transmit the data word to be written into the addressed memory location. The 24XX256 acknowledges again and the master generates a Stop condition. This initiates the internal write cycle and during this time, the 24XX256 will not generate Acknowledge signals (Figure 6-1). If an attempt is made to write to the array with the WP pin held high, the device will acknowledge the command but no write cycle will occur, no data will be written, and the device will immediately accept a new command. After a byte Write command, the internal address counter will point to the address location following the one that was just written.

6.2 Page Write

The write control byte, word address and the first data byte are transmitted to the 24XX256 in much the same way as in a byte write. The exception is that instead of generating a Stop condition, the master transmits up to 63 additional bytes, which are temporarily stored in the on-chip page buffer, and will be written into memory once the master has transmitted a Stop condition. Upon receipt of each word, the six lower Address Pointer bits are internally incremented by one. If the master should transmit more than 64 bytes prior to generating the Stop condition, the address counter will roll over and the previously received data will be overwritten. As with the byte write operation, once the Stop condition is received, an internal write cycle will begin (Figure 6-2). If an attempt is made to write to the array with the WP pin held high, the device will acknowledge the command, but no write cycle will occur, no data will be written and the device will immediately accept a new command.

6.3 Write-Protection

The WP pin allows the user to write-protect the entire array (0000-7FFF) when the pin is tied to Vcc. If tied to Vss the write protection is disabled. The WP pin is sampled at the Stop bit for every Write command (Figure 1-1). Toggling the WP pin after the Stop bit will have no effect on the execution of the write cycle.

Note:	Page write operations are limited to writing bytes within a single physical page, **regardless** of the number of bytes actually being written. Physical page boundaries start at addresses that are integer multiples of the page buffer size (or 'page size') and end at addresses that are integer multiples of [page size – 1]. If a Page Write command attempts to write across a physical page boundary, the result is that the data wraps around to the beginning of the current page (overwriting data previously stored there), instead of being written to the next page, as might be expected. It is, therefore, necessary for the application software to prevent page write operations that would attempt to cross a page boundary.

FIGURE 6-1: BYTE WRITE

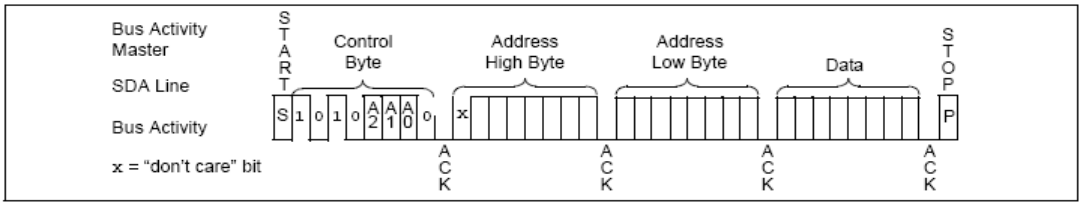
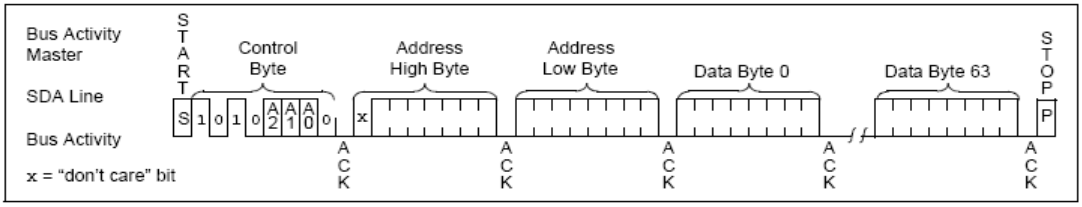


FIGURE 6-2: PAGE WRITE



8.0 READ OPERATION

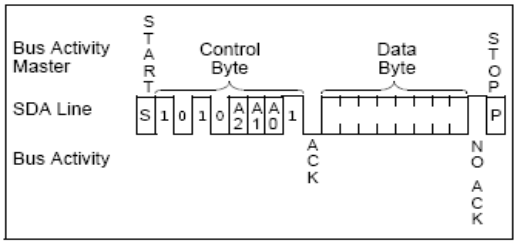
Read operations are initiated in much the same way as write operations, with the exception that the R/$\overline{W}$ bit of the control byte is set to '1'. There are three basic types of read operations: current address read, random read and sequential read.

8.1 Current Address Read

The 24XX256 contains an address counter that maintains the address of the last word accessed, internally incremented by '1'. Therefore, if the previous read access was to address 'n' (n is any legal address), the next current address read operation would access data from address n + 1.

Upon receipt of the control byte with R/$\overline{W}$ bit set to '1', the 24XX256 issues an acknowledge and transmits the 8-bit data word. The master will not acknowledge the transfer, but does generate a Stop condition and the 24XX256 discontinues transmission (Figure 8-1).

FIGURE 8-1: CURRENT ADDRESS READ



8.2 Random Read

Random read operations allow the master to access any memory location in a random manner. To perform this type of read operation, the word address must first be set. This is done by sending the word address to the 24XX256 as part of a write operation (R/$\overline{W}$ bit set to '0'). Once the word address is sent, the master generates a Start condition following the acknowledge. This terminates the write operation, but not before the internal Address Pointer is set. The master then issues the control byte again, but with the R/$\overline{W}$ bit set to a one. The 24XX256 will then issue an acknowledge and transmit the 8-bit data word. The master will not acknowledge the transfer, though it does generate a Stop condition, which causes the 24XX256 to discontinue transmission (Figure 8-2). After a random Read command, the internal address counter will point to the address location following the one that was just read.

8.3 Sequential Read

Sequential reads are initiated in the same way as a random read except that after the 24XX256 transmits the first data byte, the master issues an acknowledge as opposed to the Stop condition used in a random read. This acknowledge directs the 24XX256 to transmit the next sequentially addressed 8-bit word (Figure 8-3). Following the final byte transmitted to the master, the master will NOT generate an acknowledge, but will generate a Stop condition. To provide sequential reads, the 24XX256 contains an internal Address Pointer which is incremented by one at the completion of each operation. This Address Pointer allows the entire memory contents to be serially read during one operation. The internal Address Pointer will automatically roll over from address 7FFF to address 0000 if the master acknowledges the byte received from the array address 7FFF.

FIGURE 8-2: RANDOM READ

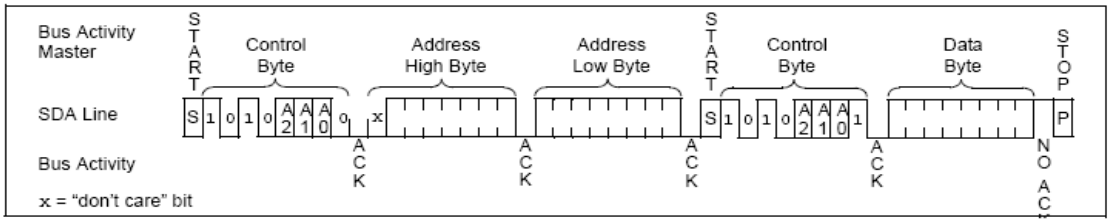
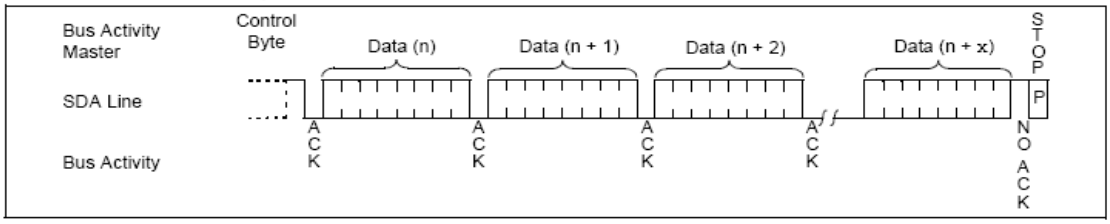


FIGURE 8-3: SEQUENTIAL READ



ANEXO E

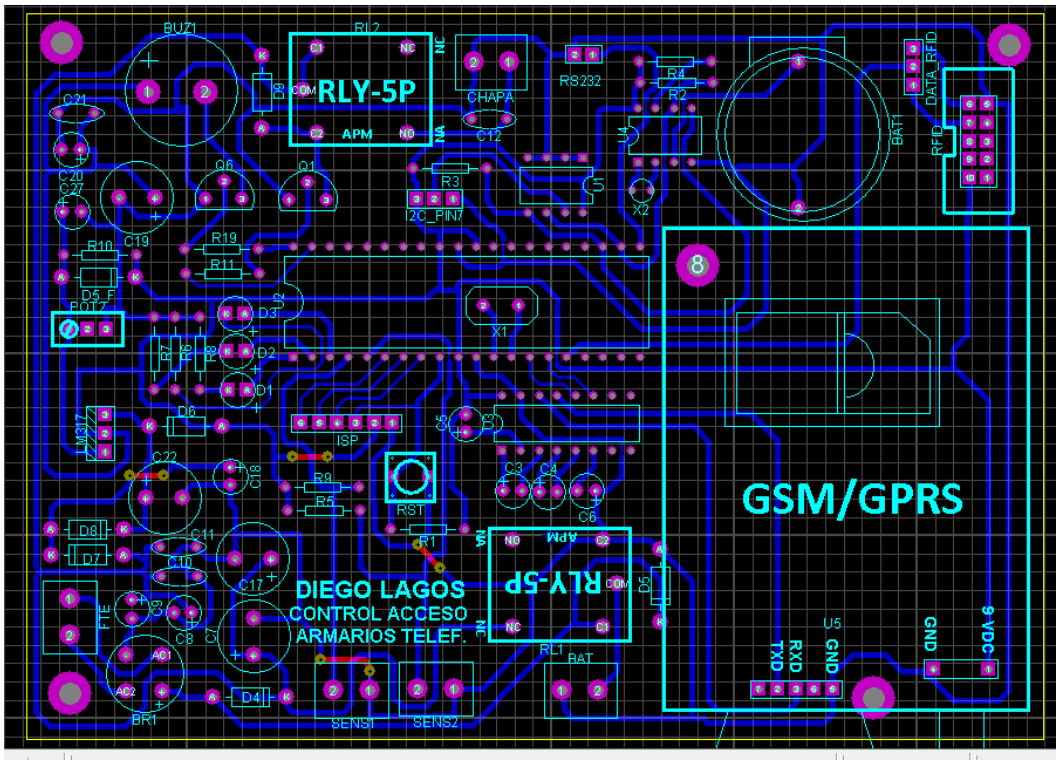
CIRCUITO IMPRESO Y DISPOSITIVOS EN LA PLACA DE CONTROL

CIRCUITO IMPRESO

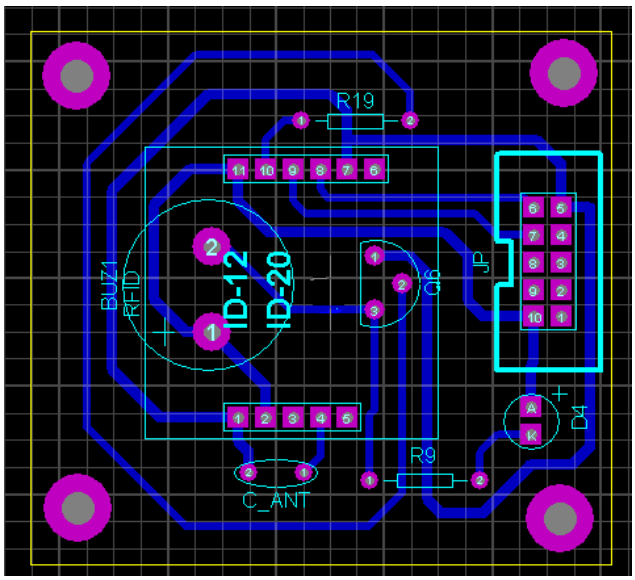
Una vez que se tiene el diseño general de todos los elementos que conforma el módulo de control de acceso a los armarios telefónicos, se procede a elaborar el circuito impreso correspondiente.

Para el diseño del circuito impreso se utilizó el Software Proteus, específicamente el programa ARES, el cual permite realizar el ruteo de circuitos electrónicos. El software Proteus es de gran ayuda ya que permite exportar todos los componentes electrónicos de un circuito determinado, desde el ISIS hacia el ARES, de esta forma permite tener grandes ventajas al momento de realizar el ruteo de circuitos.

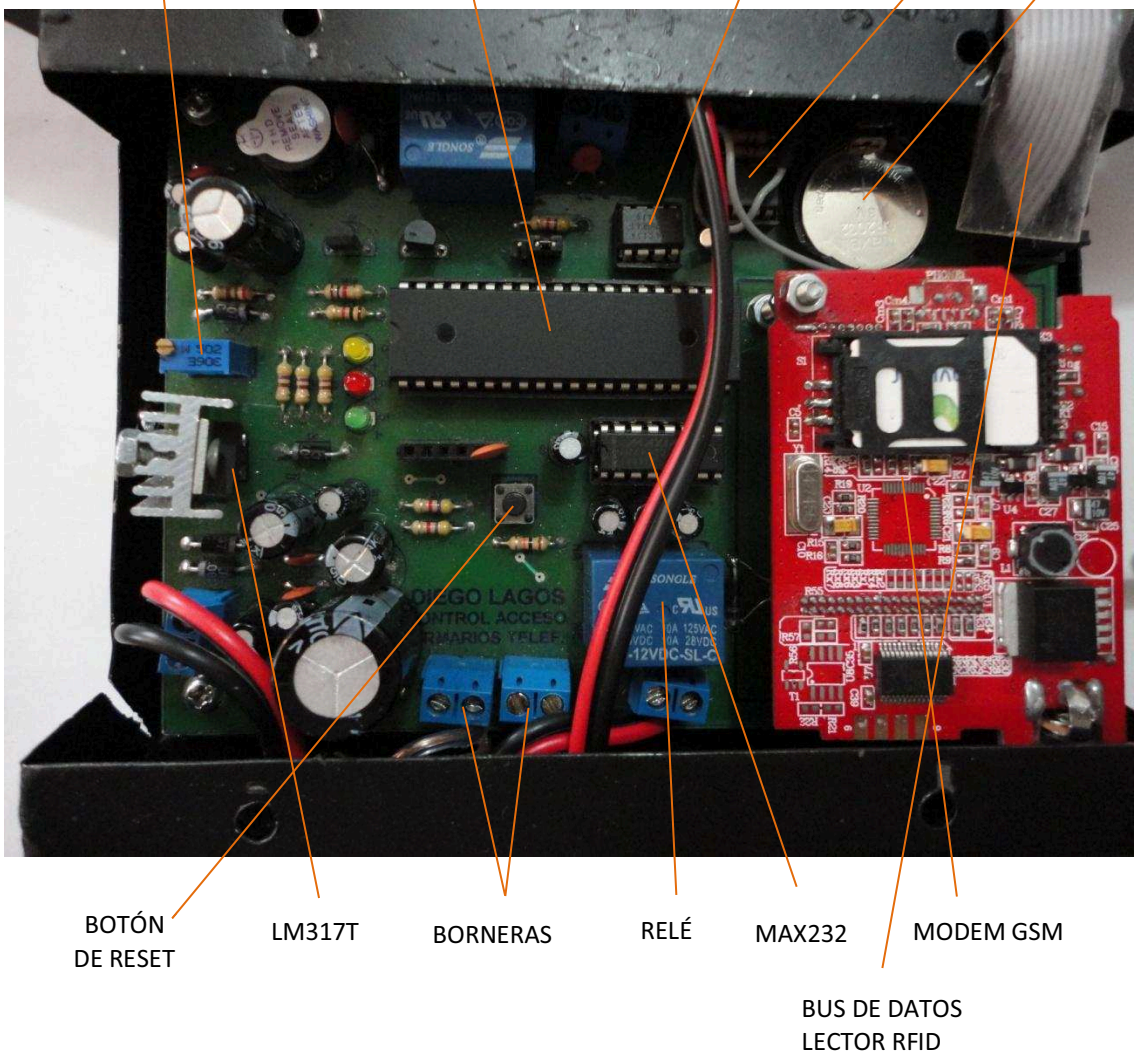
En la siguiente figura se muestra el diagrama del circuito impreso del sistema:



Además se muestra la placa del lector RFID:



En la siguiente imagen, se muestran los dispositivos armados en la placa de control:

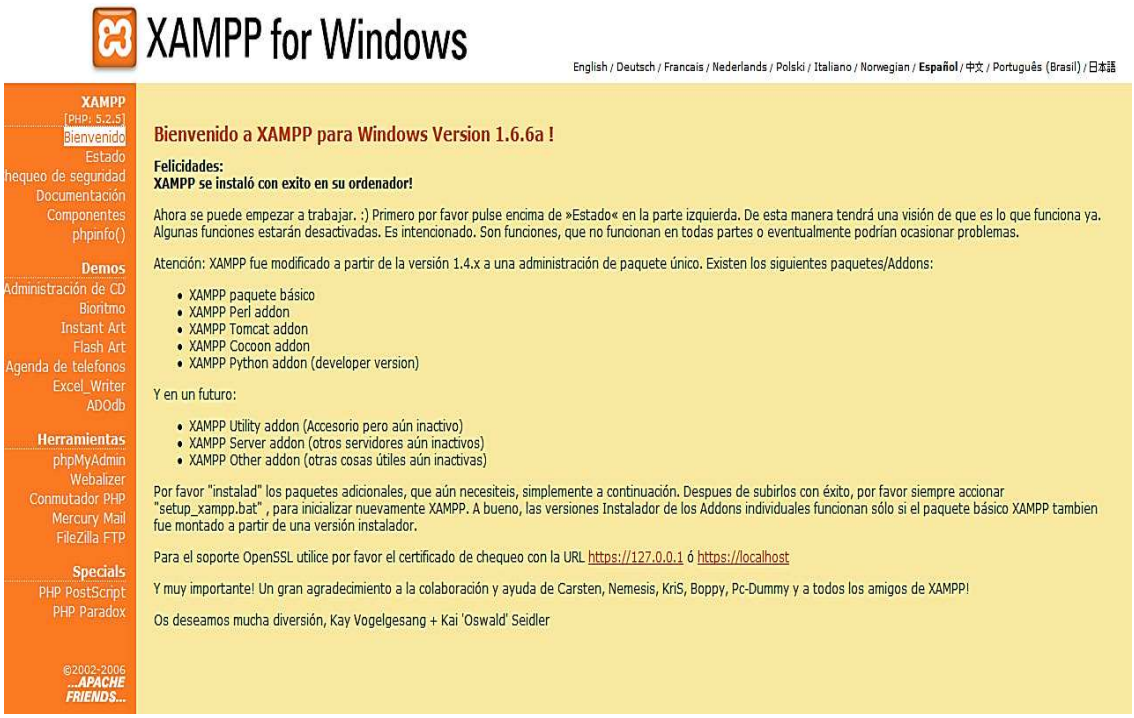

POTENCIÓMETRO DE PRECISIÓN
MICROCONTROLADOR
MEMORIA EEPROM
DS1307
PILA 3.3V
BOTÓN DE RESET
LM317T
BORNERAS
RELÉ
MAX232
MODEM GSM
BUS DE DATOS LECTOR RFID

ANEXO F

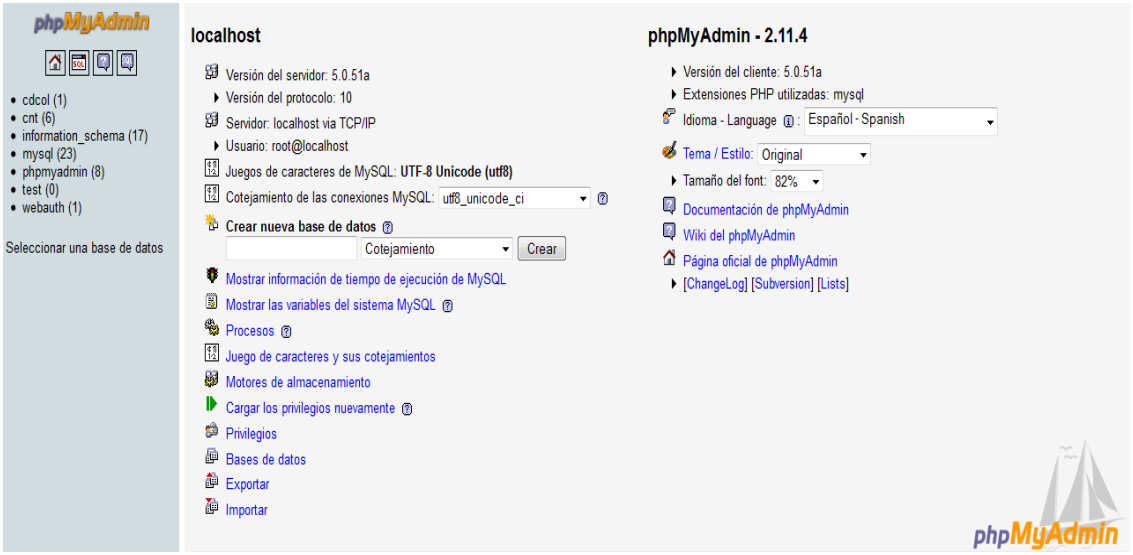
CREACIÓN DE BASE DE DATOS EN MYSQL

PROCESO PARA LA CREACIÓN DE LA BASE DE DATOS

Como ya se tiene el gestor MySQL instalado con XAMPP, se va a elaborar la base de datos, para ello, se procede a abrir el navegador de internet y se escribe en la barra de direcciones: http://localhost/xampp/ y va aparecer la pantalla de inicio del servidor XAMPP:



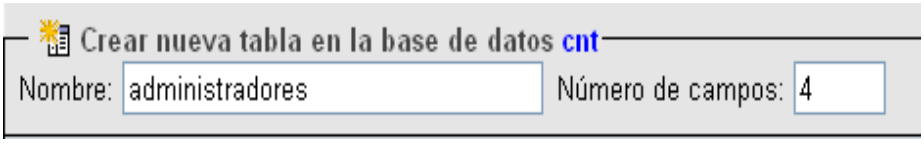
Después en el menú herramientas, se ingresa en la opción phpMyAdmin, en el cual se encuentra MySQL, que se encarga de la creación, administración y modificación de la base de datos:



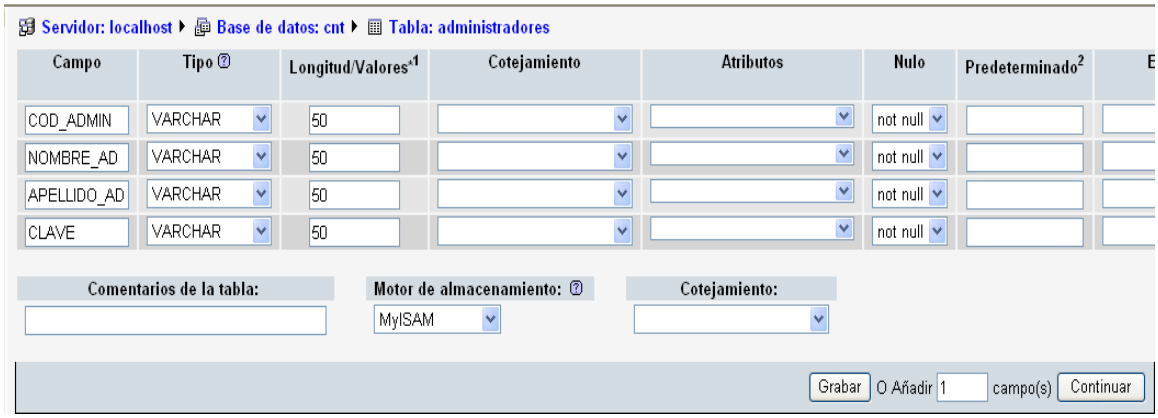
En el apartado Crear nueva base datos, se debe ingresar el nombre de la base de datos a utilizarse y se pulsa el botón Crear:

El proceso para la creación de estas tablas en el módulo MySQL de PhPMyAdmin es el siguiente:

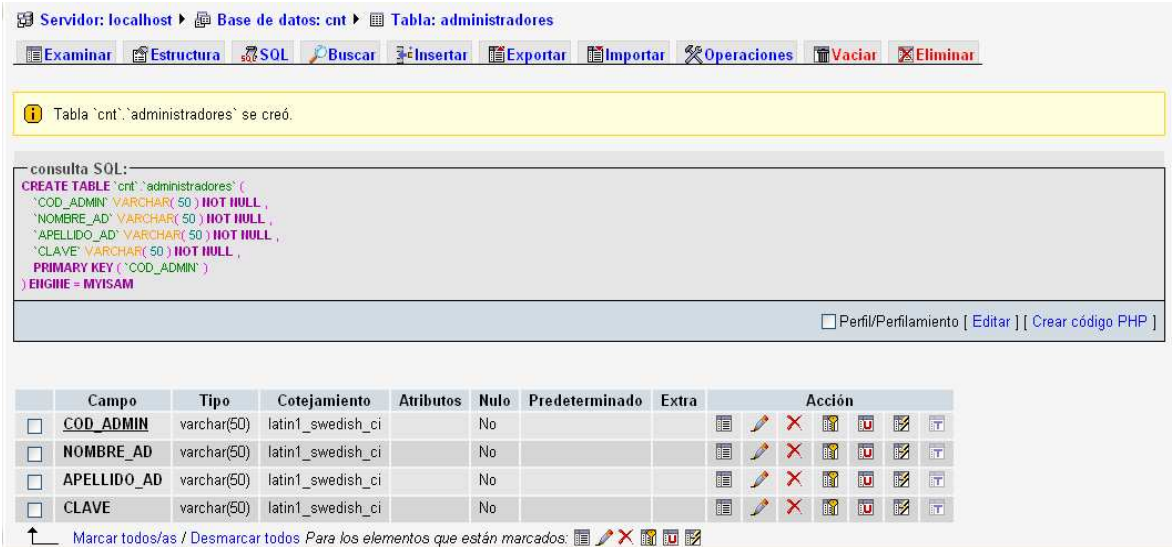
Se introduce el nombre que se va a asignar y el número de campos:



Después se presiona continuar, y aparece la configuración de los campos de la tabla, en donde se dan los nombres y se asignan los tipos de variable de los campos:



Después de presionar grabar se muestra el resultado de los campos generados en la tabla:



Una vez que se ha procedido a crear la primera tabla, se realiza el mismo procedimiento para las 5 tablas restantes. Una vez que se ha concluido este paso, la presentación de la base de datos es la siguiente:


phpMyAdmin
Base de datos
cnt (6)
cnt (6)
administradores
eventos
historial
indice
ordenado
usuarios
Servidor: localhost ▸ Base de datos: cnt
Estructura
SQL
Buscar
Generar una consulta
Exportar
Importar
Diseñador
Operaciones
Privilegios
Eliminar
Tabla
Acción
Registros
Tipo
Cotejamiento
Tamaño
Residuo a depurar
administradores 1 MyISAM latin1_swedish_ci 2.1 KB 60 Bytes
eventos 3 MyISAM latin1_swedish_ci 1.2 KB -
historial 1 MyISAM latin1_swedish_ci 2.2 KB 116 Bytes
indice 1 MyISAM latin1_swedish_ci 1.1 KB 20 Bytes
ordenado 1 MyISAM latin1_swedish_ci 1.1 KB -
usuarios 1 MyISAM latin1_swedish_ci 2.2 KB 188 Bytes
6 tabla(s) Número de filas 8 MyISAM latin1_swedish_ci 9.8 KB 384 Bytes
Marcar todos/as / Desmarcar todos / Marcar las tablas con residuo a depurar
Para los elementos que están marcados:
Vista de impresión
Diccionario de datos
Crear nueva tabla en la base de datos cnt
Nombre:
Número de campos:
Continuar