UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TESIS PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:
SISTEMA ELECTRÓNICO PARA CONTROL DE ACCESO DE PERSONAS POR RECONOCIMIENTO DE HUELLA DACTILAR, CON AUTENTICACIÓN REMOTA EN BASE DE DATOS A TRAVÉS DE UNA WLAN

AUTORA:
ESTEFANÍA GRACIELA TORRES AZA

DIRECTOR:
ING. JAIME MICHILENA

IBARRA-ECUADOR
OCTUBRE 2012

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación "**Sistema Electrónico para Control de Acceso de Personas por Reconocimiento de Huella Dactilar, con Autenticación Remota en Base de Datos a través de un WLAN**" fue desarrollado en su totalidad por la Srta. Estefanía Graciela Torres Aza portadora de la cédula de identidad número: 1002862801, bajo mi supervisión.

Ing. Jaime Michilena
DIRECTOR DEL PROYECTO

CERTIFICACIÓN

Ibarra, 12 de Agosto de 2012

Señores
UNIVERSIDAD TECNICA DEL NORTE
Presente

De mis consideraciones.-

Siendo auspiciante del proyecto de tesis de la Egresada ESTEFANIA GRACIELA TORRES AZA con CI: 100286280-1 quien desarrolló su trabajo con el tema "**SISTEMA ELECTRÓNICO PARA CONTROL DE ACCESO DE PERSONAS POR RECONOCIMIENTO DE HUELLA DACTILAR, CON AUTENTICACIÓN REMOTA EN BASE DE DATOS A TRAVÉS DE UNA WLAN"**, me es grato informar que se han superado con satisfacción las pruebas técnicas y la revisión de cumplimiento de los requerimientos funcionales, por lo que se recibe el proyecto como culminado y realizado por parte de la egresada ESTEFANIA GRACIELA TORRES AZA. Una vez que hemos recibido la capacitación y documentación respectiva, nos comprometemos a continuar utilizando el mencionado aplicativo en beneficio de nuestra Hostal.

La egresada ESTEFANIA GRACIELA TORRES AZA puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,

Ing. Alejandro Pita
GERENTE PROPIETARIO

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, ESTEFANIA GRACIELA TORRES AZA, con cédula de identidad Nro. 100286280-1, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la ley de propiedad intelectual del Ecuador, articulo 4,5 y 6, en calidad de autor del trabajo de grado denominado: "**SISTEMA ELECTRÓNICO PARA CONTROL DE ACCESO DE PERSONAS POR RECONOCIMIENTO DE HUELLA DACTILAR, CON AUTENTICACIÓN REMOTA EN BASE DE DATOS A TRAVÉS DE UNA WLAN"**, que ha sido desarrollado para optar por el título de Ingeniera en Electrónica y Redes de Comunicación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autora me reservo los derechos morales de la obra antes mencionada, aclarando aquí descrito es de mi autoría y que no ha sido previamente presentado para ningún grado o calificación profesional.

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

Nombre: ESTEFANIA GRACIELA TORRES AZA

Cédula: 100286280-1

Ibarra a los 31 días del mes de agosto del 2012

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	1002862801
Apellidos y Nombres	Torres Aza Estefanía Graciela
Dirección	Calle Tena 6-36 y Machala. Ibarra
Email	estefania_torres86@hotmail.com
Teléfono Fijo	062602725
Teléfono Móvil	0999386708

DATOS DE LA OBRA	
Título	Sistema Electrónico para Control de Acceso de Personas por Reconocimiento de Huella Dactilar, con Autenticación Remota en Base de Datos a través de un WLAN.
Autor	Torres Aza Estefanía Graciela
Fecha	31 de agosto de 2012
Programa	Pregrado
Título por el que se aspira	Ingeniera en Electrónica y Redes de Comunicación
Director	Ing. Jaime Michilena

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Estefanía Graciela Torres Aza, con cédula de identidad Nro. 1002862801, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 143.

_____

Firma
Nombre: Estefanía Graciela Torres Aza
Cédula: 1002862801
Ibarra a los 31 días del mes de agosto de 2012

AGRADECIMIENTO

Agradezco a Dios por haberme dado la fuerza y la entereza para poder llegar a culminar mis estudios; a mis padres y hermanos, por brindarme siempre su incondicional apoyo en cada momento de mi vida.

A mi familia, amigos y demás personas que hicieron de esta etapa, una manera agradable de vivir y compartir.

A mi tutor, Ing. Jaime Michilena por su disciplina y persistencia para que llegue a culminar mi Tesis exitosamente.

A todos y cada uno de ustedes, nuevamente.

Gracias.

Estefanía Graciela Torres Aza

DEDICATORIA

El presente trabajo va dedicado a mi querida madre, quien ha estado siempre a mi lado brindándome su ayuda con el fin de que logre culminar mi carrera.

Lo dedico también a todos los miembros de la Universidad Técnica del Norte, quienes con sus conocimientos supieron orientarme.

Estefanía Graciela Torres Aza

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

CAPITULO IV

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto propone el diseño y construcción de un sistema microprocesado destinado a la administración del acceso de personas a edificaciones. Se basa en el reconocimiento de la huella dactilar del usuario y su verificación en una base de datos remota conectada a través de una red inalámbrica de área local.

El desarrollo del proyecto se encuentra distribuido en cinco capítulos que contienen la información concerniente al diseño, construcción e implementación del mismo.

En el marco teórico se explican conceptos básicos sobre el funcionamiento del sistema, haciendo uso de la teoría científica que se relaciona directa o indirectamente con el trabajo de grado.

Se realiza una descripción del prototipo acorde con las actividades para las que se lo concibió. Ya con una visión clara de lo que se pretende lograr, se efectúa un enfoque general explicando los requisitos y la aproximación del hardware. Esto en el segundo capítulo.

En el tercer capítulo se detallan los criterios y procedimientos tomados en la caracterización del módulo. Se eligen los dispositivos electrónicos que se adaptan a los requerimientos del prototipo. Se define el hardware mediante diagramas esquemáticos; el firmware y software con diagramas de flujo.

Posteriormente, en el cuarto capítulo se detallan los pormenores de la implementación física del sistema. También se describen las pruebas realizadas en la comprobación de su robustez y fiabilidad.

Finalmente, con toda la información obtenida en el desarrollo del proyecto se establecen las conclusiones respectivas y se sugieren las posibles mejoras al sistema.

ABSTRACT

This project proposes the design and construction of a microprocessed system for the management of people access to buildings. It is based on the recognition of the user's fingerprint verification in a remote database connected through a wireless local area network.

Development of the project is divided into five chapters that contain information concerning the design, construction and implementation.

Theoretical framework explains the basics of system operation, using the scientific theory that relates directly or indirectly with the degree work.

A description of the prototype is performed in accordance with the activities for which it was conceived. And with a clear vision of what is sought, is made a general approach to explain the requirements and the hardware approach. This in the second chapter.

In third chapter details the criteria and procedures taken in the characterization of the module. Electronic devices are selected to suit the requirements of the prototype. Is defined hardware through schematics, firmware and software through flowcharts.

Then, in fourth chapter describes details of physical implementation. It also describes tests performed on testing its robustness and reliability.

Finally, with all information from the project, are performed conclusions and suggests possible improvements to the system.

PRESENTACIÓN

En este proyecto se diseña e implementa un sistema de control de acceso, como proceso integrado a la nómina de la Hostal “Las Garzas”. Tiene como fin verificar la identidad de los empleados y proporcionarles un nivel de acceso relativo a su horario de trabajo. Para esto se utilizan módulos de comunicación IEEE802.11 de orientación embebida, módulos de lectura biométrica y microcontroladores.

Existe un software para PC que maneja la base de datos de los movimientos de los usuarios autenticados, realizando reportes de horas de ingreso / salida y períodos de permanencia en la edificación. Además permite limitar el acceso entre varios usuarios, pudiendo asignarse únicamente ciertas horas en las que puedan ingresar.

Luego de construir e implementar el sistema, se puntualizan las pruebas realizadas para condiciones reales de trabajo, dando como resultado un excelente desempeño. Se tienen como características generales, alta fiabilidad en las lecturas biométricas, seguridad en la red inalámbrica y respuesta rápida de la base de datos.

De forma complementaria se presenta una descripción de la funcionalidad de cada una de las opciones de reconocimiento biométrico existentes y se detalla el porqué de la adopción de la huella dactilar. Además se compila la información referente a las redes inalámbricas de área local basadas en IEEE802.11, su funcionalidad y aplicaciones.

CAPÍTULO I

1. MARCO TEÓRICO

Este capítulo describe las características de la tecnología inalámbrica a utilizarse en el desarrollo del sistema. Se indica las áreas de aplicación del protocolo IEEE 802.11, entre ellas en sistemas embebidos. Se establece además el análisis de las tecnologías para reconocimiento biométrico las cuales tales como huella dactilar, iris, retina, geometría de la mano, facial, voz y reconocimiento de la firma, siendo éstas las más utilizadas.

.

1.1. INTRODUCCIÓN A IEEE 802.11

La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN).

Con IEEE 802.11 se pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso. En la práctica, admite ordenadores portátiles, equipos de escritorio, asistentes digitales personales (PDA) o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11Mbps o superior) dentro de un radio de varias docenas de metros en ambientes cerrados (de 20 a 50 metros en general) o dentro de un radio de cientos de metros al aire libre.

El estándar establece los niveles inferiores del modelo OSI (modelo de interconexión de sistemas abiertos) para las conexiones inalámbricas, por ejemplo:

- La capa física (PHY, PHYSICAL LAYER) ofrece tres tipos de transmisión de información los cuales son:

- ✓ FHSS (FRECUENCY HOPPING SPREAD SPECTRUM): Técnica de espectro ensanchado mediante saltos de frecuencia, que consiste en dividir la banda ISM en 79 canales de 1MHz sin superposición y realizar saltos periódicos de un canal a otro siguiendo una secuencia pseudoaleatoria.
- ✓ DSSS (DIRECT SPREAD SPECTRUM): Para que la comunicación sea tolerante al ruido e interferencias, en vez de saltar de una frecuencia a otra como el FHSS, utiliza códigos pseudoaleatorios que distribuyen la potencia de los datos a transmitir en un amplio ancho de banda.
- ✓ Infrarrojo difuso: no ha recibido ninguna aceptación en el mercado y por eso quedará fuera de este estudio.

- La capa de enlace de datos compuesta por dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC).

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos. La capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, y las reglas para la comunicación entre las estaciones de la red.

Cualquier protocolo de nivel superior puede utilizarse en una red inalámbrica IEEE 802.11 de la misma manera que puede utilizarse en una red Ethernet.

1.1.1. LOS DISTINTOS ESTÁNDARES IEEE 802.11

El estándar IEEE 802.11 en realidad es el primer estándar y permite una velocidad de transmisión (V_{Tx}) de 1 a 2Mbps. El estándar original se ha modificado para optimizar el ancho de banda (incluidos los estándares 802.11a, 802.11b, 802.11g y 802.11n, denominados estándares físicos 802.11) o para especificar componentes de mejor manera con el fin de

garantizar mayor seguridad o compatibilidad. La tabla a continuación muestra las modificaciones más difundidas del estándar 802.11 y sus significados:

Tabla 1: Estándares IEEE 802.11 más difundidos

Nombre del Estándar	Descripción
IEEE 802.11ª	Admite una velocidad de transmisión superior de hasta 54Mbps aunque en la práctica es de 30Mbps. Aprovecha 8 canales de radio en la frecuencia de 5Ghz.
IEEE 802.11b	Es el más utilizado en la actualidad, ofrece 11Mbps aunque en la práctica es de 6Mbps. Tiene un alcance de 300m en un espacio abierto. Usa el rango de frecuencia de 2.4Ghz.
IEEE 802.11g	Utiliza la banda de 2,4Ghz pero opera a una velocidad teórica máxima de 54Mbps, que en promedio es de 22Mbps.
IEEE 802.11n	Usa simultáneamente las bandas 2.4Ghz y 5.4Ghz. Suministra velocidades superiores a 100Mbps lo cual duplica la velocidad de 802.11g y 802.11a.

Fuente:http://www.garciagaston.com.ar/verpost.php?id_noticia=121

1.1.2. RANGO Y FLUJO DE DATOS

Los estándares 802.11a, 802.11b y 802.11g, llamados "estándares físicos", son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos.

Tabla 2: Rangos de transmisión y flujo de datos de IEEE 802.11

Estándar	Frecuencia [Ghz]	Velocidad [Mbps]	Alcance [m]
IEEE 802.11a	5	54	10
IEEE 802.11b	2.4	11	100
IEEE 802.11g	2.4	54	100
IEEE 802.11n	2.4 y 5.4	100	100

Fuente:http://www.garciagaston.com.ar/verpost.php?id_noticia=121

1.1.2.1. Estándar 802.11a

Se basa en la tecnología llamada OFDM (multiplexación por división de frecuencias ortogonales). Utiliza 8 canales no superpuestos para la transmisión.

Debido a su diferente frecuencia central de trabajo en relación a 802.11b (5GHz vs. 2.4Ghz), es incompatible con ésta. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de "banda dual".

Tabla 3: Velocidades y alcances de transmisión en ambientes cerrados de IEE802.11a

Velocidad teórica [Mbps]	Alcance [m]
54	10
48	17
36	25
24	30
12	50
6	70

Fuente: http://es.wikipedia.org/wiki/IEEE_802.11

1.1.2.2. Estándar 802.11b

Permite un valor máximo de transferencia de datos de 11Mbps en un rango de 100 metros aproximadamente en ambientes cerrados y de más de 200 metros al aire libre (o incluso más que eso con el uso de antenas direccionales).

Tabla 4: Velocidades y alcances de transmisión en ambientes cerrados de IEE802.11b

Velocidad teórica [Mbps]	Alcance [m]
11	50
5.5	75
2	100
1	150

Fuente: http://es.wikipedia.org/wiki/IEEE_802.11

1.1.2.3. Estándar 802.11g

Permite un máximo de transferencia de datos de 54 Mbps en rangos comparables a los del estándar 802.11b. Además, y debido a que el estándar 802.11g utiliza el rango de frecuencia de 2.4 GHz con codificación OFDM (multiplexación por división de frecuencias ortogonales), es compatible con los dispositivos 802.11b con excepción de algunos dispositivos más antiguos.

Tabla 5: Velocidades y alcances de transmisión en ambientes cerrados de IEE802.11g

Velocidad teórica [Mbps]	Alcance [m]
54	27
48	29
36	30
24	42
18	55
12	64
9	75
6	90

Fuente: http://es.wikipedia.org/wiki/IEEE_802.11

1.1.2.4. Estándar 802.11n

Es una propuesta de modificación al estándar IEEE 802.11 para mejorar significativamente el rendimiento más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps.

1.2. SEGURIDAD EN LAS REDES INALÁMBRICAS

La seguridad es una de las primeras preocupaciones al desarrollar una LAN inalámbrica, para esto el estándar tiene incorporado lo que es llamado WEP (WIRED EQUIVALENT PRIVACY) o privacidad equivalente a la alámbrica, que es un generador de números pseudoaleatorios o PRNG (PSEUDO RANDOM NUMBER GENERATOR). Este PRNG entrega una

secuencia de bits igual en longitud que el paquete más largo posible, la cual es combinada con el paquete saliente o entrante produciendo así el paquete transmitido en el medio.

Las principales preocupaciones de los usuarios es que un intruso no pueda:

- Acceder a los recursos de la red usando un equipo similar para LAN inalámbrica.
- Ser capaz de capturar el tráfico de la LAN inalámbrica, lo que se llama EAVESDROPPING*,* es decir, escuchar secretamente o captar información privilegiada en claro o cifrada.

Según los expertos en seguridad de información, los sistemas de comunicación deben contar con mecanismos de seguridad suficientes para proteger los datos que circulan por la red, sobre todo las redes inalámbricas exigen niveles de seguridad mayores que en una red cableada. Por ejemplo, la autenticación en redes inalámbricas debe ser en doble sentido ya que se debe verificar la identidad del usuario que se asocia a la red y la identidad de la red que se asocia con el usuario. Además se debe contar con ciertas medidas de seguridad como el filtrado SSID, MAC, entre otros.

Actualmente se cuenta con estándares de seguridad de redes inalámbricas que ayudan a cubrir las necesidades para establecer conexiones seguras como se mencionará más adelante.

1.2.1. MEDIDAS DE SEGURIDAD

El filtrado es un mecanismo básico de seguridad que ayuda a determinar qué estaciones pueden ganar acceso a la WLAN.

1.2.1.1. Filtrado SSID

Es un método rudimentario de filtrado y es solamente utilizado como control de acceso. El SSID es un identificador de la red; una estación debe conocer el SSID de la WLAN para poder autenticarse y asociarse. Se lo configura en el AP (ACCESS POINT) o punto de acceso en una red de infraestructura; o en la otra estación en una red AD – HOC.

El problema de este tipo de filtrado es que el SSID se lo emite en texto plano en las tramas de administración de BROADCAST, por tanto es fácil obtenerlo con el uso de un SNIFFER. Se debe evitar utilizar el SSID por defecto o que tenga alguna relación con la empresa. No se debe usar el SSID como mecanismo de seguridad WLAN.

1.2.1.2. Filtrado MAC

Se debe mantener listas de direcciones MAC permitidas y programadas en los APs, ya que la mayoría de éstos tienen una funcionalidad de filtrado. Este filtrado se utiliza en redes pequeñas y es susceptible a los siguientes problemas:

- Robo de tarjeta de un computador en el que está el filtro MAC
- Captación de información de la red para robar direcciones MAC

1.2.1.3. Filtrado de protocolos

Se puede filtrar los paquetes que atraviesan la red basándose en los protocolos de capa 2 hasta 7 del modelo OSI. Por ejemplo se puede permitir el acceso a tráfico SNMP, HTTP, HTTPS, FTP y todos los demás serán bloqueados.

1.2.2. ESTÁNDARES DE SEGURIDAD

1.2.2.1. WIRED EQUIVALENCY PROTOCOL (WEP)

Provee autenticación, confidencialidad e integridad mediante el algoritmo de encriptación simétrico RC-4 con claves de 64 y 128 bits.

La clave de 64 bits se genera a partir de una clave estática de forma automática, aunque es posible introducir esta clave de forma manual. Esta clave debe ser conocida tanto por el AP como por todos los clientes que quieran conectarse utilizando WEP.

De los 64 o 128 bits de la clave secreta, se generan 4 llaves de 40 o 104 bits respectivamente y los 24 bits restantes se añaden en un vector de inicialización (IV). De las cuatro llaves generadas se selecciona sólo una de ellas para la encripción WEP.

1.2.2.1.1. Encripción e integridad con WEP

Para generar una trama encriptada con WEP se deben realizar los siguientes pasos, los mismos que se explican en la siguiente figura:

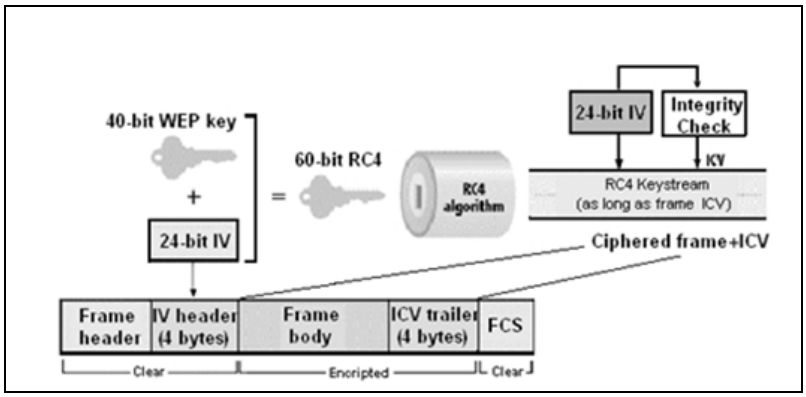


Figura 1: Encripción con WEP

Fuente: http:www.aulaclic.es

- La trama a cifrar está compuesta de HEADER (encabezamiento) y PAYLOAD (carga útil). Se calcula el CRC (código de redundancia cíclica) de 32 bits del PAYLOAD de la trama que se quiere enviar.
- Se añade el CRC a la trama como valor de chequeo de integridad (ICV, INTEGRITY CHECK VALUE).
- Se selecciona una de las cuatro llaves posibles, mediante el KEY NUMBER, que especifica la clave a usar.
- Se añade el vector de inicialización (IV) de 24 bits al inicio de la llave seleccionada.
- Con los 24 bits del IV y los 40 ó 104 bits de la llave se consigue los 64 ó 128 bits respectivamente de la llave total que se usará para encriptar.

1.2.2.1.2. Autenticación con WEP

Se tienen 3 tipos de autenticación:

- ***NONE.*** Es la autenticación por defecto para redes IEEE 802.11. Autentica cualquier cliente que pide acceso a la red, todos los clientes que conozcan el SSID de la WLAN e inicien el proceso de autenticación son registrados por el AP.
- ***SHARED KEY AUTHENTICATION.*** El cliente envía una petición de autenticación al AP, el cual contesta con un desafío no encriptado. Posteriormente el cliente encripta la clave compartida y el desafío (CHALLENGE), y reenvía la información hacia el AP para que éste verifique si la clave es correcta y envíe como respuesta el resultado de autenticación.
- ***OPEN SYSTEM AUTHENTICATION.*** Se acredita a cualquiera que desea asociarse a la WLAN, pero no se permite a la estación transmitir a menos que conozca la clave WEP compartida.

1.2.2.1.3. Ventajas

- Fácil de instalar
- No requiere de una inversión adicional
- No necesita servidores de autenticación, certificados digitales y bases de datos de usuarios
- Compatibilidad con todas las plataformas de clientes
- Compatibilidad con casi todo el hardware de WLAN

1.2.2.1.4. Desventajas

- Usa la misma clave para encriptación y autenticación
- Mecanismo de autenticación, encripción e integridad con varias debilidades
- No es una solución corporativa adecuada
- No protege de intrusiones de usuarios internos

1.2.2.2. IEEE 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente - servidor, que restringe la conexión de equipos no autorizados a una red.

La base fundamental de 802.1x es EAP (EXTENSIBLE AUTHENTICATION PROTOCOL). EAP es una simple encapsulación que define el formato de las tramas para el intercambio de credenciales de las partes. El autenticador envía peticiones a los sistemas que buscan acceso y en función de las respuestas, el acceso puede ser otorgado o denegado.

El protocolo 802.1x involucra tres peticiones que se explican a continuación y que se observa en la siguiente figura:

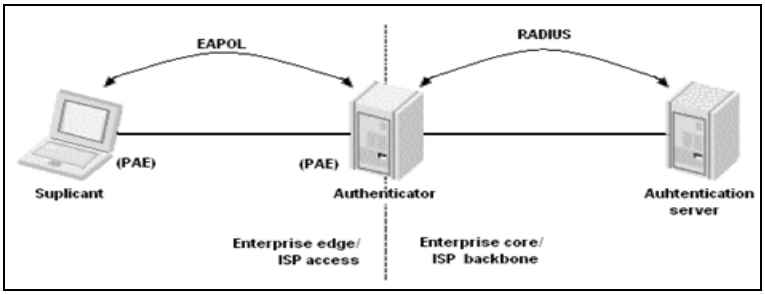


Figura 2: Protocolo IEEE 802.1x

Fuente: http://www.ja.net//

- El equipo del cliente que desea comunicarse con la red.
- El servidor de autorización y autenticación que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-in User Service).
- El autenticador, que es el equipo de red (SWITCH, ROUTER, servidor de acceso remoto) que recibe la conexión del cliente. Éste actúa como intermediario entre el cliente y el servidor de autenticación, y solamente permite el acceso del cliente a la red cuando el servidor de autenticación así lo autoriza.

1.2.2.3. WI-FI PROTECTED ACCESS (WPA)

WPA es básicamente un pre-estándar de IEEE 802.11i que aparece a finales del 2002 y tiene por objetivo garantizar la seguridad en las especificaciones IEEE 802.11b, 802.11a y 802.11g, proponiendo un nuevo protocolo para cifrado TKIP (TEMPORAL KEY INTEGRITY PROTOCOL). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo.

El mecanismo de autenticación usado en WPA es 802.1x y EAP.

1.2.2.3.1. Privacidad e integridad con TKIP

Este protocolo amplía y mejora WEP, dando solución a sus problemas de vulnerabilidad al aumentar la longitud de la clave de 40 a 128 bits y pasa de ser única y estática a ser generada de forma dinámica para cada usuario, para cada sesión, y por cada paquete enviado; además utiliza una función de combinación de claves, que funciona generando claves temporales con un periodo fijo de duración que son reemplazadas de forma frecuente.

Ofrece cuatro mejoras:

- Un código de integridad de mensaje criptográfico y no un simple CRC.
- Reforzamiento del IV.
- Combinación de claves por paquete.
- Generación de nuevas claves.

El código de integridad de mensaje criptográfico (MIC) permite garantizar la integridad del mensaje enviado y añade a la información transmitida un mensaje de autenticación MAC (MESSAGE AUTHENTICATION CODE).

1.3. SISTEMAS EMBEBIDOS

Son sistemas que se diseñan pensando en una aplicación concreta y por esa razón se los desarrolla de manera muy ajustada a las necesidades, implicando un bajo tamaño, reducido costo y alta replicidad.

Estos dispositivos electrónicos son usados para controlar y operar equipos, dispositivos, máquinas, aparatos domésticos, equipos móviles, PDAs, automóviles, instrumentos electrónicos, operar máquinas y hasta plantas industriales.

El término *embebido* indica que estos circuitos integrados son una parte esencial e integral del sistema en que se encuentran. Son elementos que integran intrínsecamente, todos los subsistemas y elementos necesarios para realizar la labor de operación, control e instrumentación definida para el correcto funcionamiento de la maquinaria o dispositivo, siendo éstas desde labores simples hasta de una alta complejidad.

En la actualidad los sistemas embebidos tienen una capacidad de cálculo bastante alta (varios MIPS, millones de instrucciones por segundo) necesaria para realizar labores complejas tales como el cálculo de la FFT (transformada rápida de Fourier), para realizar filtros digitales, análisis de señales y demás cálculos matemáticos complejos. Toman decisiones en tiempo real tan complejas, que eran imposibles de hacer en este tipo de dispositivos electrónicos hace algunos años.

Dentro de las comunicaciones hay muchos aparatos basados en sistemas embebidos como ruteadores y puntos de acceso, sistemas de seguridad informática como cortafuegos, SWITCHES de comunicaciones administrables remotamente, sistemas de filtrado de paquetes TCP/IP, módems alámbricos e inalámbricos, controles de acceso, entre otros.

La comunicación adquiere gran importancia en un sistemas embebido. Lo normal es que el sistema pueda comunicarse mediante interfaces estándar de cable o inalámbricas. Normalmente incorporará puertos de comunicaciones del tipo RS-232, RS-485, SPI, I²C, CAN, USB, IP, Wi-Fi, GSM, GPRS, DSRC, etc.

1.3.1. HARDWARE DE SISTEMAS EMBEBIDOS

Figura 3: Hardware de un sistema embebido
Fuente: http://ocw.um.es/ingenierias/sistemas-embebidos/material-de-clase-1/ssee-t01.pdf

Los sistemas embebidos trabajan sobre una amplia gama de plataformas de hardware que van desde los 8 hasta los 64 bits actualmente y su selección depende exclusivamente de la aplicación final. Es importante por consiguiente saber definir la plataforma de desarrollo y los requerimientos específicos del producto final que se obtendrá.

1.3.2. SOFTWARE DE SISTEMAS EMBEBIDOS

Los programas de desarrollo para sistemas embebidos son propietarios y cerrados. Permiten generar códigos binarios para ser cargados en estos sistemas. Además estas herramientas son de un costo relativamente alto de mantenimiento debido a su licenciamiento.

1.3.3. Sistemas operativos de sistemas embebidos

Se puede decir que no todos los sistemas embebidos usan o requieren de un sistema operativo. Es importante tener esto claro porque en muchos casos es innecesario. Sin embargo, hay otros sistemas que sí requieren un sistema operativo para operar, este es el caso de las PDAs,

algunos modelos de teléfonos móviles o celulares y algunos sistemas industriales.

Los sistemas operativos por su parte requieren de un cierto hardware mínimo para ser ejecutados lo que generalmente implica un mayor desarrollo de hardware. En general los sistemas operativos para sistemas embebidos necesitan un hardware menor a un PC normal.

1.3.4. SISTEMAS EMBEBIDOS DE CONTROL DE ACCESO

Para el control de acceso es importante disponer de mecanismos de seguridad adecuados al medio o información que se intenta proteger; el conjunto de tales mecanismos incluirá al menos un sistema que permita identificar a las entidades (elementos del sistema, usuarios, entre otros) que intentan acceder, mediante procesos tan simples como una clave de seguridad o tan complejos como un dispositivo analizador de patrones biométricos.

El objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, sino autenticar que esa persona es quien dice ser realmente. Aunque como humanos seguramente ambos términos parecerán equivalentes, para un computador existe una gran diferencia entre ellos.

Por un lado, la identificación es el simple proceso de identificar una entidad de otra o determinar la identidad de una entidad con quien se está comunicando; mientras que la autenticación es la prueba de que la entidad es quien dice ser.

Los métodos de autenticación se suelen dividir en tres grandes categorías, en función de lo que utilizan para la verificación de identidad:

- PASSWORD: algo que el usuario conoce
- TOKEN: algo que el usuario tiene

- AUTENTICACIÓN BIOMÉTRICA: algo que el usuario es

1.4. BIOMETRÍA

Cada vez es más frecuente la necesidad de que automáticamente se identifique a una persona para que ésta pueda acceder a un determinado lugar o servicio.

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas. Es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

1.4.1. RECONOCIMIENTO BIOMÉTRICO

Los dispositivos biométricos tienen tres partes principales: por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar; además disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos, y también ofrecen una interfaz para las aplicaciones que los utilizan. El proceso general de autenticación sigue pasos comunes a todos los modelos de autenticación biométrica:

- Captura o lectura de los datos que el usuario a validar presenta.
- Extracción de ciertas características de la muestra.
- Decisión de si el usuario es válido o no.
- Comparación de estas características con las guardadas en una base de datos.

Es en la decisión donde principalmente entran en juego las dos características básicas de la habilidad de todo sistema biométrico: las tasas de falso rechazo y las de falsa aceptación.
Por tasa de falso rechazo (FALSE REJECTION RATE, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (FALSE ACCEPTANCE RATE, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo.

Evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad ya que se está proporcionando acceso a un recurso a personal no autorizado para acceder a él.

1.4.2. MÉTODOS BIOMÉTRICOS

Los métodos de tipo fisiológico incluyen los siguientes:

- Identificación de huellas dactilares
- Reconocimiento del iris
- Reconocimiento de la retina
- Identificación de la geometría de la mano
- Reconocimiento facial
- Reconocimiento mediante el uso de termogramas faciales
- Análisis de ADN
- Reconocimiento auricular
- Exploración del patrón venoso en la muñeca

Entre los métodos basados en comportamiento se tiene:

- Identificación por la voz
- Reconocimiento de la firma

- Dinámica de pulsación en teclado
- Análisis del patrón de marcha

Tabla 6: Comparativa de sistemas biométricos

	Ojo (iris)	**Ojo (retina)**	**Huellas dactilares**	**Vascular dedo**	**Geometria de la mano**	**Escritura y firma**	**Voz**	**Cara**
Fiabilidad	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Muy Alta	Alta	Alta	Alta	Alta
Prevencion de ataques	Muy Alta	Muy Alta	Alta	Muy Alta	Alta	Media	Media	Media
Aceptacion	Media	Baja	Alta	Alta	Alta	Muy Alta	Alta	Muy Alta
Estabilidad	Alta	Alta	Alta	Alta	Media	Baja	Media	Media

Fuente:http://www.securetech.com.uy/servicios/info/biometria_2.htm

1.4.3. RECONOCIMIENTO DE HUELLA DACTILAR

Figura 4: Reconocimiento de huella dactilar

Fuente: http://www.eleconomista.es

El reconocimiento de huella dactilar es el método de identificación biométrica por excelencia debido a que es fácil de adquirir, fácil de usar y por ende goza de gran aceptación por parte de los usuarios. El nacimiento de las técnicas de identificación a través de las huellas dactilares, a pesar de transcurrido el tiempo es la herramienta más eficaz para la identificación de personas.

Todos los sistemas dactiloscópicos se basan en cuatro principios fundamentales:

- Perennidad: se sabe que las huellas dactilares se manifiestan a partir del sexto mes del desarrollo del embrión y que están presentes a lo largo de toda la vida de los seres humanos y hasta la descomposición del cadáver.
- Inmutabilidad: Las huellas dactilares no se ven afectadas en sus características por el desarrollo físico de los individuos ni por enfermedades de ningún tipo.
- Diversidad infinita: Las huellas dactilares son únicas e irrepetibles, cada ser humano posee huellas dactilares con características individuales.
- A simple vista toda persona puede observar que la piel no es enteramente lisa o uniforme, sino que está cubierta de rugosidades, protuberancias y depresiones en la dermis.

CAPÍTULO II

2. DESCRIPCIÓN DEL SISTEMA

Este capítulo detalla la concepción general del sistema en base a sus requerimientos. Se utiliza la determinación de subsistemas para facilitar la posterior caracterización de todos los elementos del hardware, y la programación del firmware y software.

2.1. PROBLEMA

Actualmente en la Hostal “Las Garzas” se tiene una escasa infraestructura tecnológica para el control de acceso de los empleados a la bodega de insumos. Esto ha ocasionado grandes pérdidas económicas para los propietarios debido a que el personal no correspondiente al turno de trabajo, sustrae las pertenencias de sus compañeros y los insumos del lugar.

2.2. JUSTIFICACIÓN

Las tecnologías de autenticación biométrica hoy en día se han convertido en la principal solución para evitar la suplantación de identidad. Dentro de éstas, la lectura de huella dactilar se consolida como un medio seguro, rápido y práctico para la acreditación de usuarios, prescindiendo del uso de medios clonables como tarjetas codificadas o llaves.

Por otro lado, el bajo consumo de potencia, el gran nivel de integración, el bajo costo, la relativa facilidad de implementación y la movilidad, son características que han convertido a los equipos inalámbricos en la mejor opción para la transmisión de datos.

Con la fusión de las dos tecnologías detalladas anteriormente, resulta factible e interesante implementar un sistema de autenticación de usuarios

por lectura de su huella dactilar. El proyecto se orienta a utilizar WLAN en la transmisión de datos desde varios terminales hacia una sola base, a fin de permitir la entrada y salida de personas a través de diversos puntos de acceso.

Existen en el mercado dispositivos de autenticación biométrica que no manejan bases de datos para reportes de accesos ni tampoco están diseñados para trabajar en conjunto. Así, no permiten controlar el tránsito de personas a través de diversas entradas / salidas en una misma edificación.

2.3. DESCRIPCIÓN GENERAL DEL SISTEMA

- El dispositivo es un sistema digital de control de acceso de personas a edificaciones mediante reconocimiento de su huella dactilar y verificación en una base de datos remota con conexión a una WLAN de infraestructura.

  Los diversos mecanismos implementados en el sistema permiten:

- Sensar de manera precisa y con alta velocidad, los parámetros implicados en el acceso de personas a edificaciones.
- Verificar la legitimidad de los usuarios mediante autenticación biométrica de su huella dactilar para permitir o restringir su acceso hacia lugares determinados
- Establecer comunicación inalámbrica remota con una computadora personal en la que se encuentra una base de datos correspondiente a los usuarios autenticados y los horarios de ingreso.
- Utilizar una interfaz amigable con el usuario para administrar la base de datos.

2.4. REQUISITOS DEL SISTEMA

Los requisitos se detallan teniendo en cuenta las condiciones del ambiente de trabajo, las especificaciones de potencia y las funciones que realiza el dispositivo.

2.4.1. REQUISITOS EN BASE AL AMBIENTE DE TRABAJO

- Potencia de transmisión y sensibilidad de recepción adecuada para permitir la mayor distancia de separación entre los nodos de la red inalámbrica.
- Capacidad de coexistencia con otros dispositivos inalámbricos que trabajen en la misma banda con la mínima interferencia posible.
- Inmunidad al ruido eléctrico generado por elementos inductivos conectados a la acometida.

2.4.2. REQUISITOS EN BASE A ESPECIFICACIONES DE POTENCIA

- Manejo de potencia suficiente para conmutar las cargas eléctricas administradas por el sistema.
- Consumo eléctrico reducido en estado de espera.
- Entrega de potencia eficiente por parte de los reguladores de voltaje, para permitir el funcionamiento seguro de todos los dispositivos electrónicos que forman parte del dispositivo.
- Protección contra conexión invertida y picos de voltaje, para evitar daños prematuros y permanentes en el dispositivo.

2.4.3. REQUISITOS EN BASE AL DESEMPEÑO SOLICITADO

- Alta velocidad de adquisición, procesamiento y ejecución.
- Interfaz gráfica, explícita y legible para el manejo de la base de datos.

- Exactitud en la base de tiempo utilizada como referencia para los períodos de muestreo de variables y para la conmutación de los dispositivos eléctricos.
- Vida útil larga con mantenimiento mínimo.
- Seguridad en la lectura biométrica de huella dactilar, que asegure que el sistema sea inmune a posibles fraudes de autenticación.
- Robustez en el manejo de datos y eventos que impida que el sistema se congele.
- Seguridad en la comunicación inalámbrica para evitar intrusiones.

2.5. APROXIMACIÓN EN BLOQUES

La concepción básica del dispositivo se basa en bloques agrupados en subsistemas, de acuerdo a sus funciones generales (sensado, procesamiento y visualización, autenticación, respuesta), tal como se muestra en el siguiente diagrama:

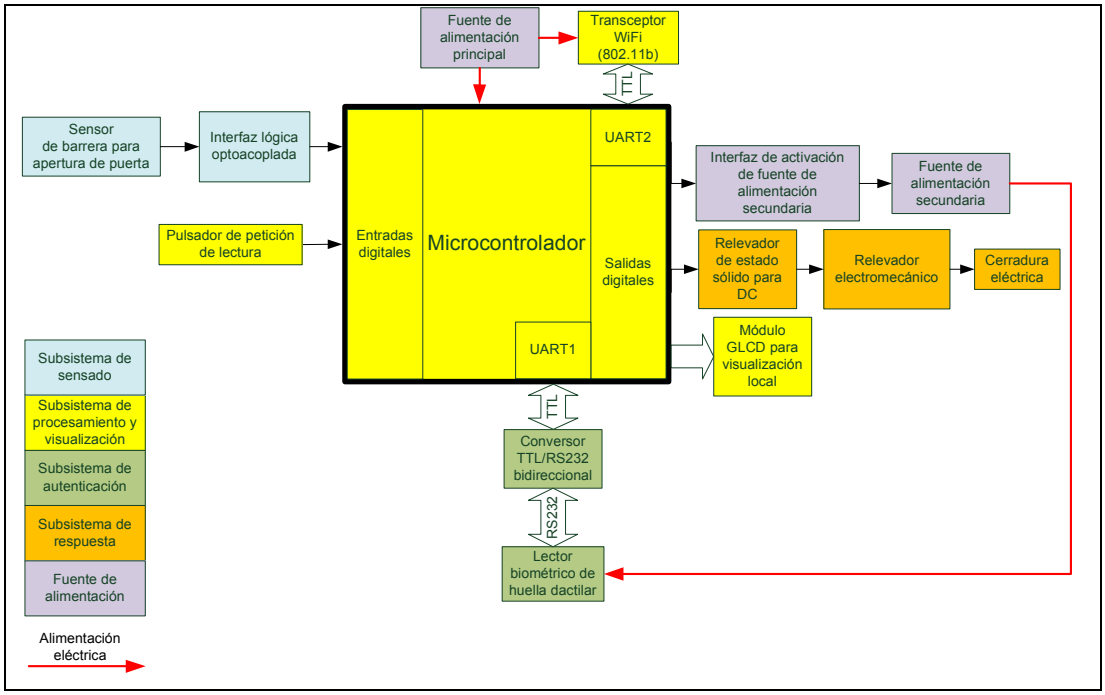


Figura 5: Diagrama de bloques del sistema

Fuente: Autor

2.5.1. SUBSISTEMA DE SENSADO

Se encarga básicamente de la adquisición y acondicionamiento de la variable implicada en el evento de apertura – cierre de la puerta. La señal lógica manejada proviene de un sensor dispuesto para monitorear la posición de la puerta de acceso a la bodega.

2.5.2. SUBSISTEMA DE PROCESAMIENTO Y VISUALIZACIÓN

Un microcontrolador, base fundamental del mecanismo, maneja dos puertos de comunicación serial bidireccional para la transferencia de información con el lector biométrico y con la base de datos en PC.

Para la comunicación remota con la PC, existe un transceptor IEEE802.11b en topología punto a punto que se convierte en un puente inalámbrico entre el microcontrolador y el computador.

El módulo de visualización GLCD permite al usuario verificar lo siguiente:

- Estado del enlace inalámbrico.
- Nombre del usuario autenticado.
- Autorización / derogación de acceso.
- Estado de la puerta (abierta / cerrada).
- Estado de la lectura biométrica.

Las siguientes, son algunas subfunciones agregadas del mecanismo:

- Procesar las peticiones de lectura biométrica al leer el estado del pulsador de petición.
- Encender y apagar la fuente de alimentación del lector biométrico.
- Interpretar la información recibida desde el lector biométrico para enviarla por vía inalámbrica a la PC.

- Interpretar los comandos recibidos desde la PC para permitir o no el acceso de un usuario.

2.5.3. SUBSISTEMA DE AUTENTICACIÓN

Consiste básicamente en un lector biométrico de huella dactilar, con procesador incorporado y comunicación serial. El acceso a este dispositivo se hace a través de comunicación serial.

Según lo anterior, se puede indicar que los algoritmos de autenticación y la grabación y remoción de usuarios, son procesos realizados localmente por el lector. El microcontrolador se limita a enviar comandos hacia el módulo de lectura biométrica y recibir información desde éste.

Es importante resaltar que si bien el lector biométrico realiza localmente la autenticación de los usuarios, quien permite o no el acceso de ellos es la base de datos remota en la PC.

El lector biométrico se puede conectar además a un computador personal mediante interfaz serial. De esta manera se puede configurar sus parámetros de funcionamiento, e ingresar o retirar las lecturas biométricas de ciertos usuarios.

2.5.4. SUBSISTEMA DE RESPUESTA

Comprende la interfaz usada para manejar consumidores de potencia. Su función es transformar cierta salida digital proveniente del microcontrolador, en un suministro de corriente considerable para activar la cerradura eléctrica.

CAPÍTULO III

3. DESARROLLO

A continuación se realiza la determinación de los componentes y su configuración vinculada, de manera que puedan regirse a los requisitos del sistema y a las funciones concebidas mediante el diagrama de bloques.

Posteriormente se utiliza diagramas de flujo para indicar el funcionamiento del firmware del microcontrolador y el software de la base de datos.

3.1. CARACTERIZACIÓN DEL HARDWARE

3.1.1. SUBSISTEMA DE SENSADO

3.1.1.1. Sensor de barrera para apertura de puertas

Este sensor detecta el estado de la puerta. Su alimentación se hace directamente con 12V y consiste internamente de un diodo LED infrarrojo y un fotodiodo. Cuando la puerta se cierra, una película opaca de plástico se interpone en la barrera emisor – receptor y la salida del sensor se coloca en alta impedancia. Cuando la puerta se abre, el sensor envía una señal de 0V.

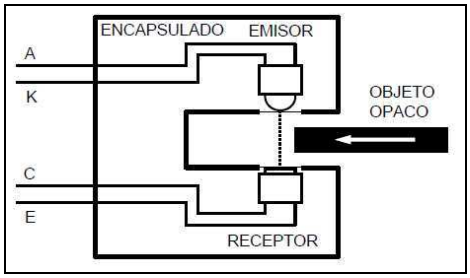


Figura 6: Sensor óptico de barrera

Fuente: Autor

3.1.1.2. Interfaz lógica optoacoplada

Este circuito es usado para leer el estado del sensor de barrera. Consiste en un circuito negador sencillo basado en un transistor BJT polarizado por divisor de voltaje y un optoacoplador.

Cuando el sensor de barrera envía 0V (señal de puerta abierta), se coloca un voltaje bajo en el transistor PNP, permitiendo que derive tierra y polarice al optoacoplador. Éste último, coloca un 0L en la salida hacia el microcontrolador.

La resistencia R12 limita la corriente de alimentación del sensor de barrera. Ante alta impedancia (señal de puerta cerrada), la resistencia R13 coloca un voltaje alto que asegura que Q2 y por lo tanto IC7 no se polaricen. Entonces, la resistencia PULLUP interna de la entrada del microcontrolador coloca un 1L.

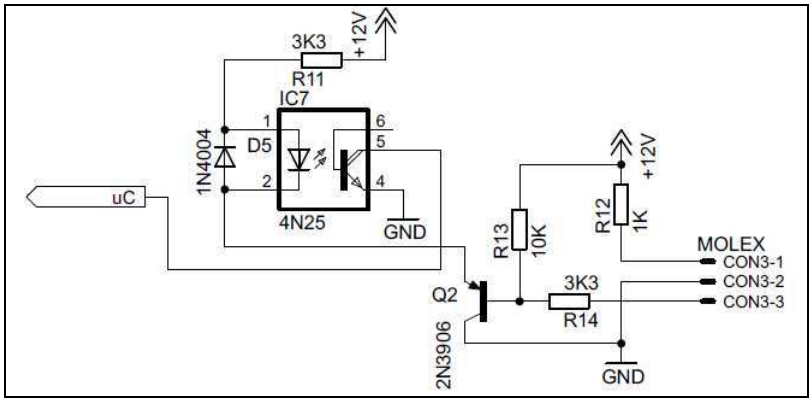


Figura 7: Interfaz lógica optoacoplada

Fuente: Autor

Cuando el sensor deriva tierra (señal activada), Q2 se polariza colocando 0V en el cátodo de IC7. Esto provoca que se polarice el LED del optoacoplador y que éste a la vez excite al fototransistor, derivando así un 0L en la entrada del microcontrolador.

3.1.2. SUBSISTEMA DE PROCESAMIENTO Y VISUALIZACIÓN

3.1.2.1. Microcontrolador

Los microcontroladores son los dispositivos más utilizados en el desarrollo de sistemas embebidos. Dentro de decenas de marcas de semiconductores, la familia AVR de ATMEL posee ciertas características que la hace idónea para aplicaciones específicas debido a su reducido consumo, reloj interno, altos MIPS, bajo costo, entre otros.

El ATMEGA644 es un microcontrolador de alta inmunidad a la interferencia eléctrica y gran memoria de programa. Las siguientes son varias características importantes de este dispositivo:

- Memoria FLASH de 64Kbytes.
- Memoria RAM de 4Kbytes.
- Tres módulos temporizadores (TIMER0 a TIMER2).
- Módulo UART (Transmisor receptor asincrónico universal), con registros de trabajo independientes para transmisión y recepción.
- Conversor análogo – digital de hasta 8 canales con resolución de 10bits y tiempo de adquisición programable.
- Oscilador interno RC calibrado de 8Mhz con un THROUGHPUT de 8MIPS.
- Multiplicación en hardware en un ciclo de instrucción.
- Niveles de prioridad para las interrupciones.
- Arquitectura optimizada para compilación en lenguaje C, con set extendido de instrucciones.
- Rango de voltaje de operación entre 2.7V y 5.5V.
- Capacidad de retención de datos de 100 años a 25°C.

El siguiente diagrama de bloques, detalla su estructura interna:

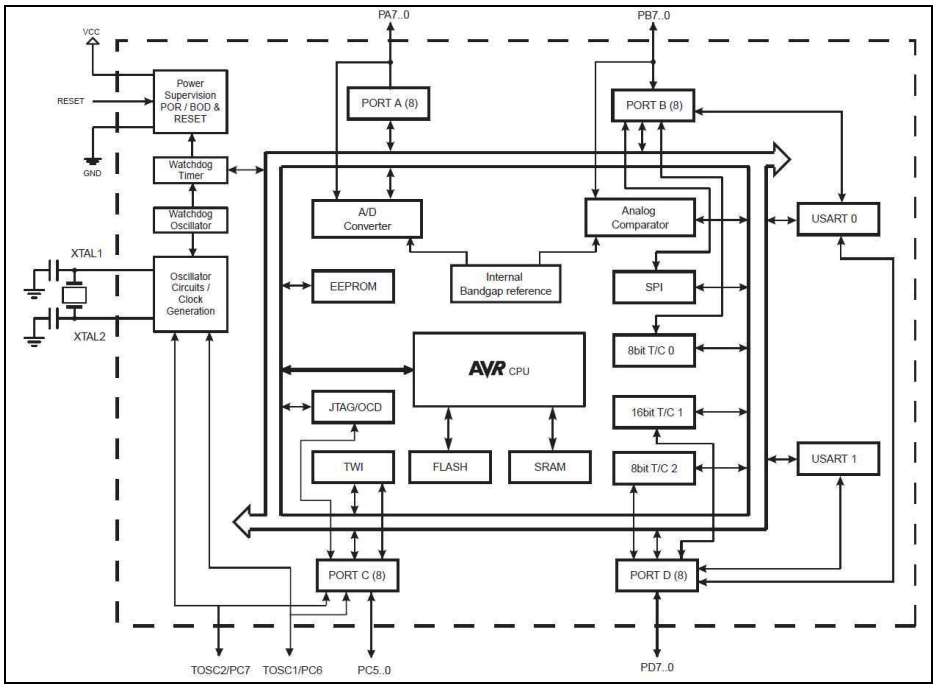


Figura 8: Diagrama de bloques del ATmega644

Fuente: http://www.atmel.com//

El ATMEGA644P se encarga del procesamiento de la información, al adquirir todos los datos de las variables externas e interpretarlos. De esta manera se asegura el control de los dispositivos eléctricos, el envío remoto de datos y la ejecución de comandos.

Una característica especial de configuración del hardware del microcontrolador es que el voltaje de alimentación, al igual que en el resto del circuito, es de 5V. También es importante mencionar que la mayoría de los pines utilizados como entradas digitales, tienen una resistencia PULL UP interna que mantiene un nivel lógico alto cuando no hay presencia de señales.

La siguiente tabla resume el destino de conexión de cada uno de los pines del microcontrolador. Define además si son entradas o salidas, y en el caso de ser entradas, si éstas son análogas o digitales

Tabla 7: Configuración de puertos del microcontrolador

CONFIGURACIÓN DE PUERTOS DEL MICROCONTROLADOR ATMEGA644P					
	NOMBRE	***PIN***	***E/S***	***A/D***	***FUNCIÓN / OBSERVACIÓN***
	PA0/ADC0	40	E	D	PETICIÓN DE LECTURA
	PA1/ADC1	39	E	D	SENSOR DE BARRERA
	PA2/ADC2	38	-	-	-
	PA3/ADC3	37	-	-	-
	PA4/ADC4	36	-	-	-
	PA5/ADC5	35	-	-	-
	PA6/ADC6	34	-	-	-
PORTB	PB0/ICP	1	S	D	DB0 GLCD
	PB1/OC1A	2	S	D	DB1 GLCD
	PB2/OC1B	3	S	D	DB2 GLCD
	PB3/MOSI	4	S	D	DB3 GLCD
	PB4/MISO	5	S	D	DB4 GLCD
	PB5/SCK	6	S	D	DB5 GLCD
	PB6/XTAL1	7	S	D	DB6 GLCD
	PB7/XTAL2	8	S	D	DB7 GLCD
PORTC	PC0/ADC0	22	S	E	PIN 30 GLCD
	PC1/ADC1	23	S	E	ACTIVACION RELE
	PC2/ADC2	24	S	E	FUENTE PRIMERIA
	PC3/ADC3	25	-	-	-
	PC4/ADC4	26	-	-	-
	PC5/ADC5	27	-	-	-
	PC6/RESET	28	-	-	-
PORTD	PD0/RXD	2	E	D	TX WIFLY
	PD1/TXD	3	S	D	RX WIFLY
	PD2/INT0	4	S	D	RS GLCD
	PD3/INT1	5	S	D	RW GLCD
	PD4/XCK	6	S	D	E GLCD
	PD5/T1	11	S	D	CS1 GLCD
	PD6/AIN0	12	S	D	CS2 GLCD
	PD7/AIN1	13	S	D	RST GLCD

Fuente: http://www.atmel.com//

3.1.2.2. Módulo de visualización

Se maneja un visualizador gráfico de 128x64 píxeles con procesador SAMSUNG KS0108 que permite al usuario observar en tiempo real, gráfica y alfanuméricamente los mensajes y eventos del sistema.

Tal como se observa en la siguiente figura, las patitas RD<2:6> del ATMEGA644P, configuradas como salidas, manejan los pines de control; el bus de datos está implementado en las salidas RB<0:7>.

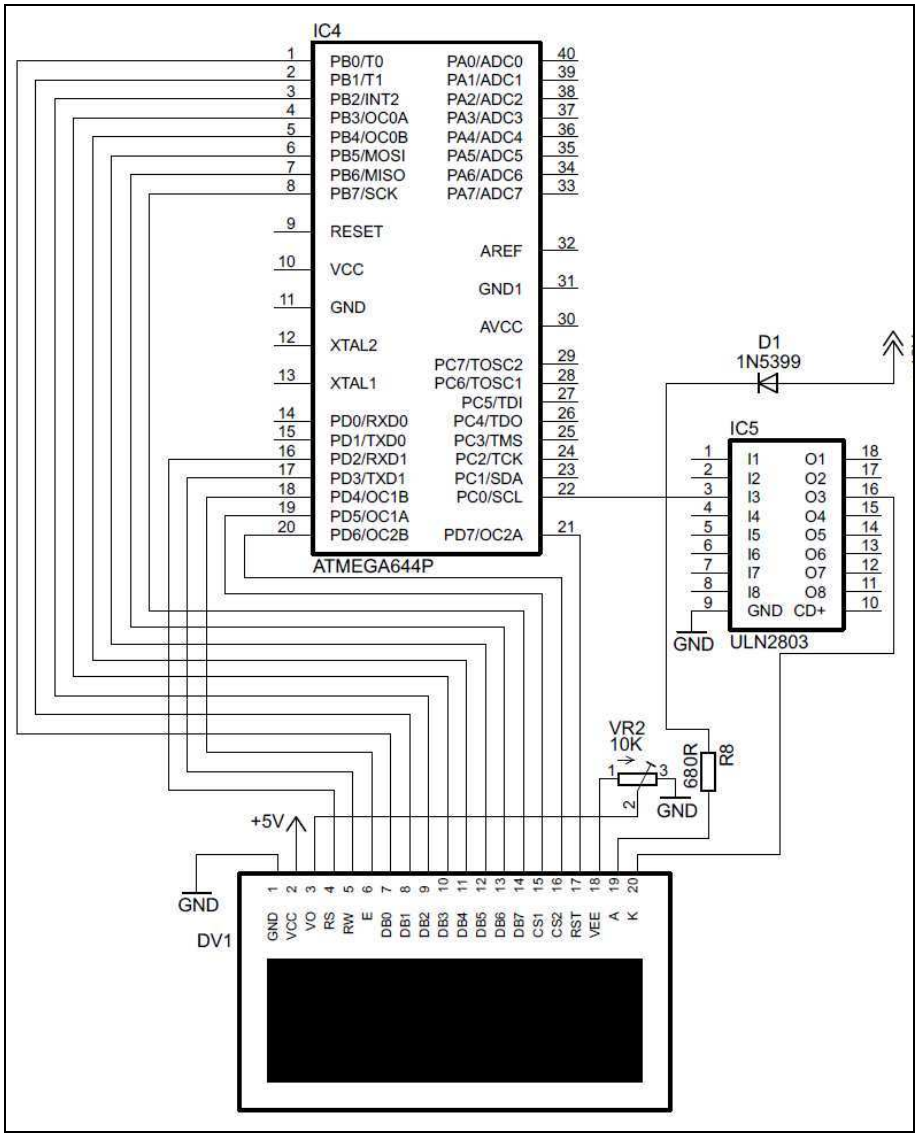


Figura 9: Conexión del módulo GLCD

Fuente: Autor

Los LEDs de retroiluminación de la pantalla GLCD, son alimentados desde el suministro de corriente principal y a través de la resistencia limitadora de corriente R8. Esto se hace debido a que el consumo relativamente alto de los LEDs, provocaría sobrecalentamiento en los reguladores lineales de voltaje. Uno de los buffers del ULN2803 permite el encendido y apagado de la luz, según lo ordenado por el microcontrolador.

El ajuste de contraste se realiza al regular el voltaje que polariza al pin VO, mediante el potenciómetro VR2. Es importante resaltar que el voltaje negativo necesario para el contraste, es generado por el propio módulo GLCD a través del pin VEE.

3.1.2.3. Transceptor IEEE 802.11b

La comunicación se implementó sobre el módulo WIFLY RN111B debido a la disponibilidad de este transceptor en el mercado local.

Debido a su pequeño tamaño y consumo de energía extremadamente bajo, es útil para aplicaciones embebidas móviles inalámbricas, tales como sistemas de monitoreo, seguimiento GPS, entre otras. Posee manejo de la pila TCP / IP a bordo, además de programas de aplicación en redes tales como TELNET y FTP. El hardware requiere solamente cuatro conexiones (PWR, TX, RX, GND) para crear una conexión básica.

Puede ser configurado a través de un conjunto de instrucciones en ASCII, luego de lo cual se incorpora automáticamente en una red inalámbrica.

Tabla 8: Características del transceptor WIFLY RN111B

ÍTEM	CARACTERÍSTICAS
RADIO	802.11b infraestructura
POTENCIA	Recepción: -82 a -93 [dBm] Transmisión: 12 [dBm]
ANTENA	Dipolo
DIMENSIÓN	43 x 60 [mm²]
ALIMENTACIÓN	3 ~ 16 [V]
CONSUMO DE CORRIENTE	(Idle) 40 ~(Op.) 120 [mA]
TEMPERATURA DE OPERACIÓN	-40 ~ 85 [°C]
HUMEDAD	90 [% RH]
SOPORTE DE COMUNICACIONES	TCP/UDP/IP, ICMP, Telnet, TFTP, DHCP, FTP, UDP Time
CANAL DE COMUNICACIÓN AUXILIAR	UART, 1200 ~ 921000 [bps]
SEGURIDAD	WEP128, WPA, WPA2
ENTRADAS – SALIDAS EXTERNAS	8 propósito general

Fuente: http://www.sparkfun.com//

El siguiente diagrama de bloques describe su estructura:

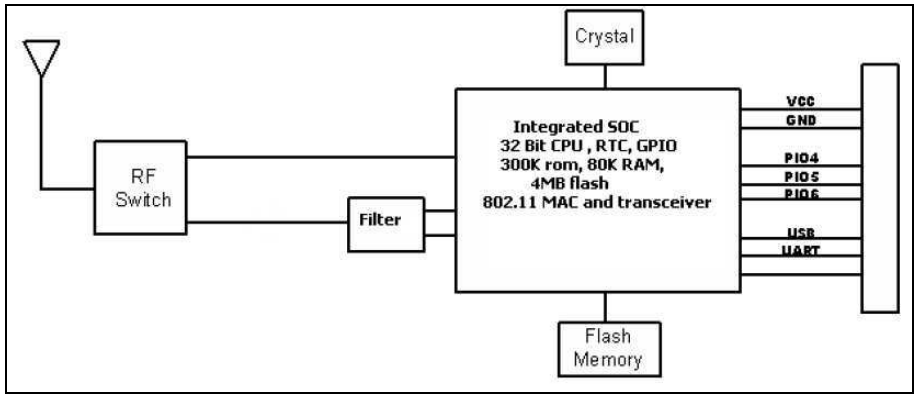


Figura 10: Diagrama de bloques del módulo WIFLY RN111B

Fuente: http://www.sparkfun.com//

La siguiente figura muestra la conexión entre el módulo WIFLY y el microcontrolador. Las resistencias R5, R6 y R7, forman un divisor de voltaje de 2/3. Su propósito es adecuar la señal lógica de alrededor de 5V proveniente del pin Tx del microcontrolador, en una señal de 3.3V apta para

el módulo inalámbrico. R4 y R5 limitan la corriente que circula en los canales de comunicación.

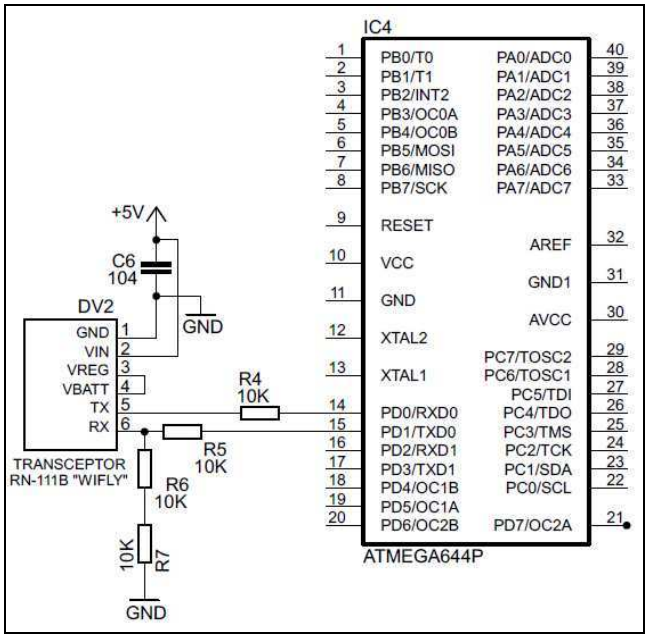


Figura 11: Conexión del módulo de comunicación inalámbrica

Fuente: Autor

La comunicación se basa en un enlace punto a punto entre el sistema electrónico y la PC mediante IP (Protocolo de Internet). La red inalámbrica ya establecida y debidamente configurada, sobre la cual el sistema se comunica con el software en el computador es de tipo infraestructura (a través de un punto de acceso AP). Esto se debe a que el módulo WIFLY únicamente soporta esta configuración y no AD-HOC.

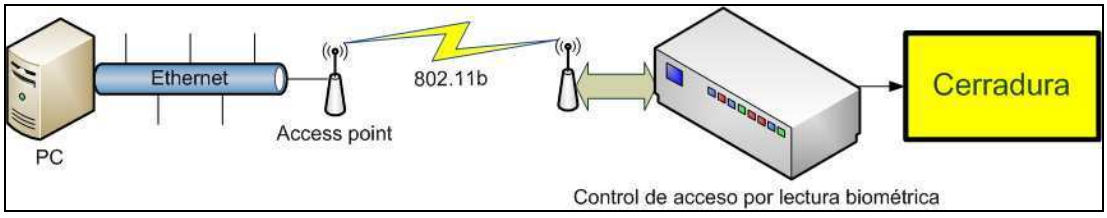


Figura 12: Infraestructura del sistema de comunicación

Fuente: Autor

La inclusión del sistema no altera el rendimiento de cualquier infraestructura existente, ya que el consumo de ancho de banda digital para el enlace bajo IP es mínimo. De esta manera la red puede trabajar

normalmente para el fin original para el que fue instalada, o se pueden incluir otras funciones que la aprovechen de mejor manera como por ejemplo vía de acceso a internet, voz sobre IP, entre otros.
Los parámetros básicos que permiten realizar lo indicado son los siguientes:

Tabla 9: Resumen de configuración de la red

ELEMENTO	CONFIGURACIÓN
Módulo WIFLY	DIRECCIÓN IP: 192.168.0.3 DIRECCIÓN DEL GATEWAY: 192.168.0.50 PUERTO: 2000 MÁSCARA DE SUBRED: 255.255.255.0 DIRECCIÓN DE HOST: 192.168.0.2
ACCESS POINT	MODO DE TRABAJO: AP DIRECCIÓN IP: 192.168.0.50 SEGURIDAD: ABIERTO SSID: control_acceso CANAL: 6 (2.437GHZ) DHCP: NO (IP ESTÁTICA) MÁSCARA DE SUBRED: 255.255.255.0
ETHERNET PC	DIRECCIÓN IP: 192.168.0.2 DIRECCIÓN DEL GATEWAY: 192.168.0.50 PUERTO: 2000 MÁSCARA DE SUBRED: 255.255.255.0 DIRECCIÓN DE HOST: 192.168.0.3

Fuente: Autor

3.1.2.3.1. Configuración del módulo de comunicación inalámbrica

Para realizar la configuración de los parámetros básicos de funcionamiento del transceptor, se lo debe conectar a través de comunicación serial a una PC (cable USB/RS232, transceptor TTL/RS232, terminal serial).

Los parámetros de configuración del módulo se observaron en la tabla anterior. Las siguientes imágenes, son capturas de la configuración a través de consola.

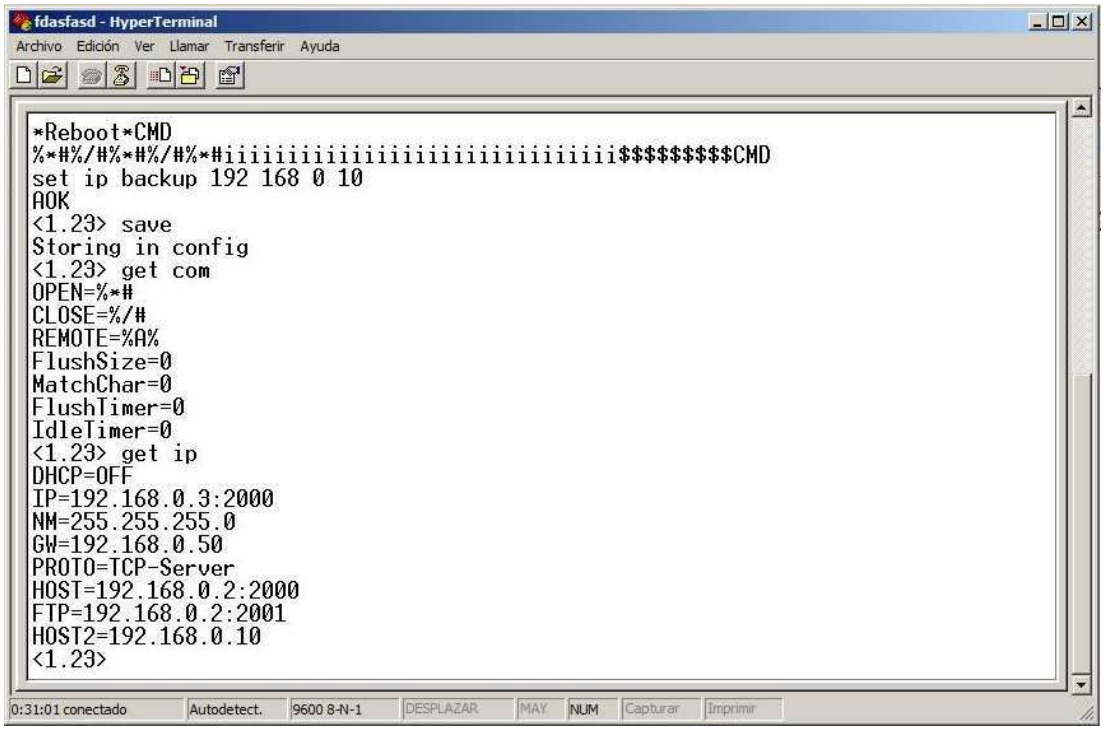


Figura 13: Captura de la consola de configuración del módulo WIFLY

Fuente: Autor

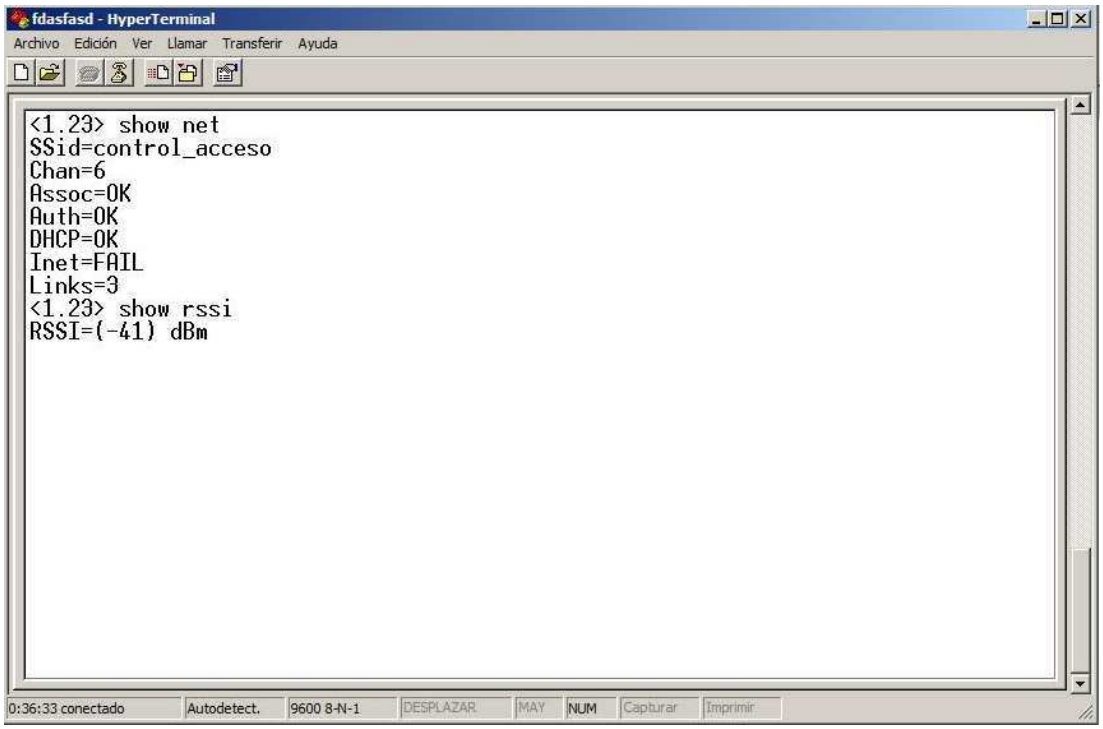


Figura 14: Captura que indica el estado de funcionamiento del módulo WIFLY

Fuente: Autor

3.1.2.4. ACCESS POINT

El punto de acceso AP es un DLINK AIR PLUS EXTREME G DWL-2100. Se lo escogió debido a su bajo costo y disponibilidad en el mercado local. Este dispositivo tiene un módulo de configuración gráfico (WIZARD) que permite ponerlo a funcionar fácilmente y en pocos instantes. En la tabla 9 se indicaron los parámetros básicos configurados en él.

La siguiente imagen indica la interfaz gráfica utilizada para la configuración del AP, así como los datos ingresados en ella.

Figura 15: Captura de la interfaz gráfica de configuración del AP

Fuente: Autor

3.1.2.5. Botón de petición de lectura

El circuito es usado para solicitar al microcontrolador la lectura de la huella dactilar. Se usa un capacitor para absorber los rebotes provocados por la conmutación del pulsador. La figura siguiente indica su configuración:

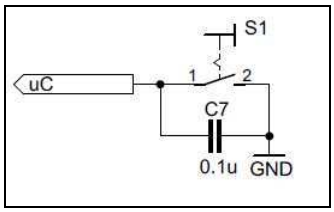


Figura 3.11: Botón de petición de lectura

Fuente: Autor

3.1.3. SUBSISTEMA DE AUTENTICACIÓN

Una de las particularidades del circuito radica en que el identificador de huellas permanece sin alimentación, a menos que el microcontrolador encienda el regulador de voltaje secundario. Esta característica evita el consumo excesivo de corriente.

El microcontrolador envía los comandos de petición de identificación biométrica a través del bus de comunicación serial RS232. Una vez que se ha realizado una lectura, el lector biométrico envía información de vuelta al microcontrolador.

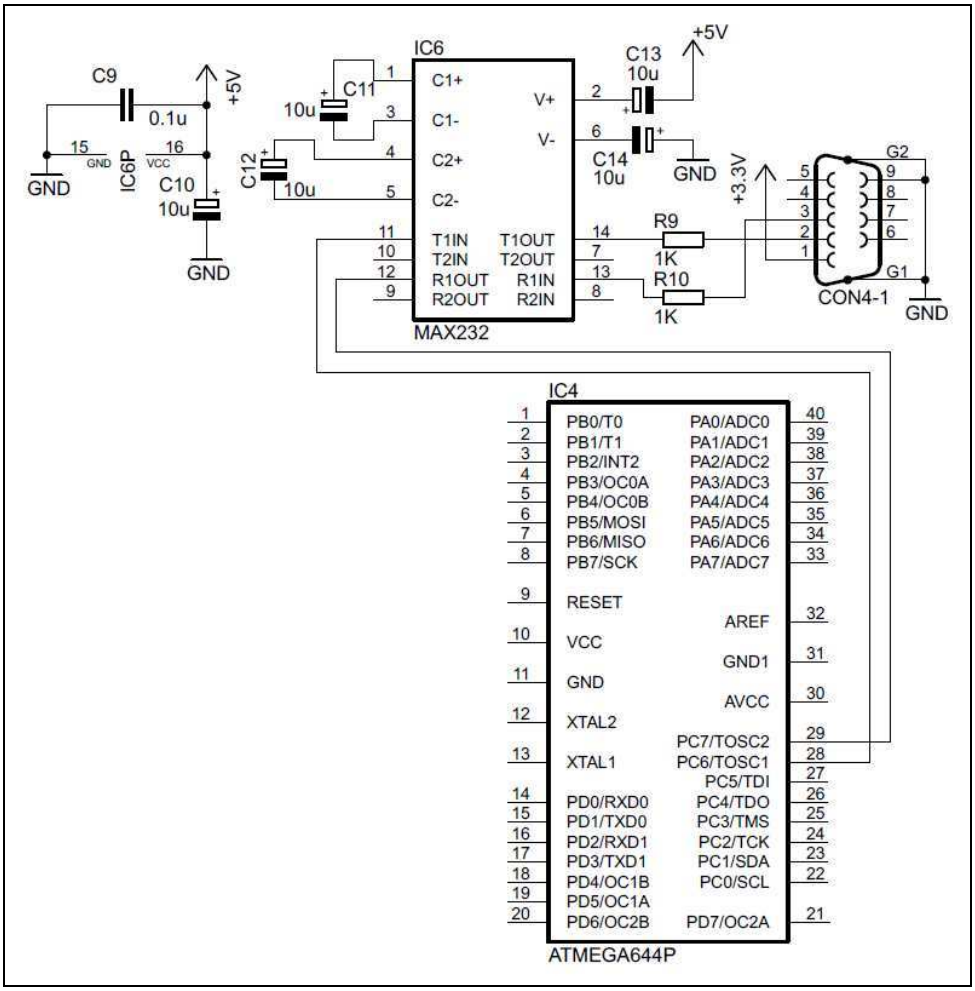


Figura 16: Conexión entre el microcontrolador y el transceptor RS232

Fuente: Autor

La tarea de grabación y remoción de nuevos usuarios, así como también la configuración del programa interno del lector biométrico, se realiza a través de una computadora personal. CON4 permite la conexión mediante protocolo RS232 entre la PC y el lector.

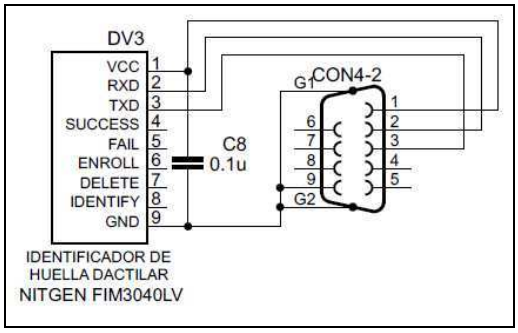


Figura 17: Conexión entre el identificador de huella dactilar y el terminal DB9

Fuente: Autor

3.1.3.1. Lector de huella dactilar FIM3040

El FIM3040 es un dispositivo de identificación de huellas dactilares de bajo costo y excelentes características. Ofrece beneficios tales como alto rendimiento en la identificación, baja potencia de consumo e interfaz serial a RS-232 a través de comandos propietarios para su fácil integración en una amplia gama de aplicaciones.

Pertenece a la marca NITGEN y puede ser conectado a un ordenador o directamente a cualquier sistema embebido entrenado con su protocolo de comunicación propietario. La siguiente tabla resume sus características principales:

Tabla 10: Características del lector FIM3040 de NITGEN

ÍTEM	FIM3040
CPU	ADSP-BF531
DRAM	8Mbyte SDRAM
FLASH ROM	1Mbyte
DIMENSIÓN	43 x 60 [mm²]
SENSOR	NITGEN OPP03
ALIMENTACIÓN	3.3 ± 0.3 [V]
CONSUMO DE CORRIENTE	(Idle) 55 ~(Op.) 210 [mA]
TEMPERATURA DE OPERACIÒN	20 ~ 60 [°C]
HUMEDAD	90 [% RH]
TOLERANCIA A DESCARGAS ESTÁTICAS	± 8 [KV] (indirecto)
CANAL DE COMUNICACIÓN	RS-232, 9600 ~ 115200 [bps]
ENTRADAS – SALIDAS EXTERNAS	3 entradas, 2 salidas

Fuente: http://www.sparkfun.com//

En el proceso de identificación los rasgos biométricos se comparan con los de un conjunto de patrones ya guardados, este proceso se conoce

también como uno-para-muchos (1: N). Este proceso implica no conocer la identidad presunta del individuo, la nueva muestra de datos biométricos es tomada del usuario y comparada una a una con los patrones ya existentes en el banco de datos registrados.

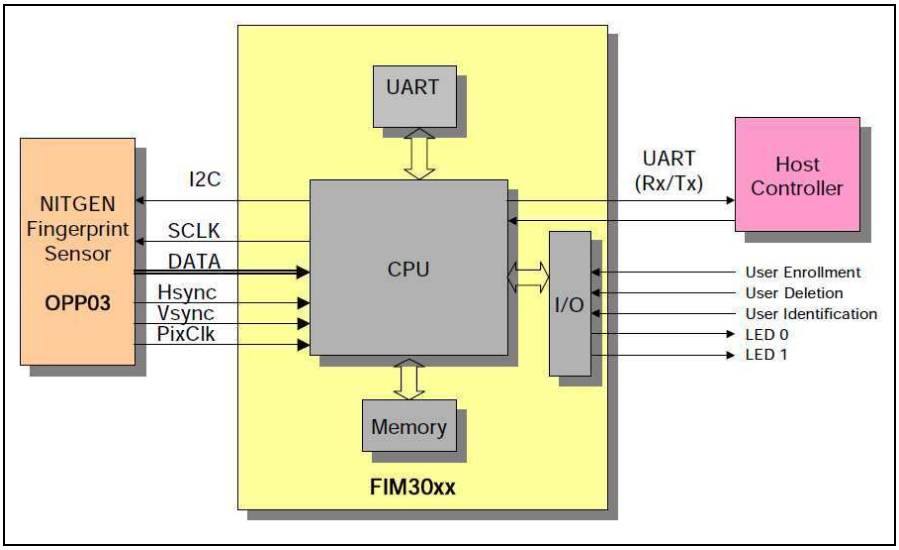


Figura 18: Diagrama de bloques del lector biométrico

Fuente: http://www.sparkfun.com//

3.1.3.1.1. Configuración del lector

La siguiente figura muestra el dispositivo utilizado para dar alimentación al lector biométrico y permitir su conexión con la PC, en el momento de configuración.

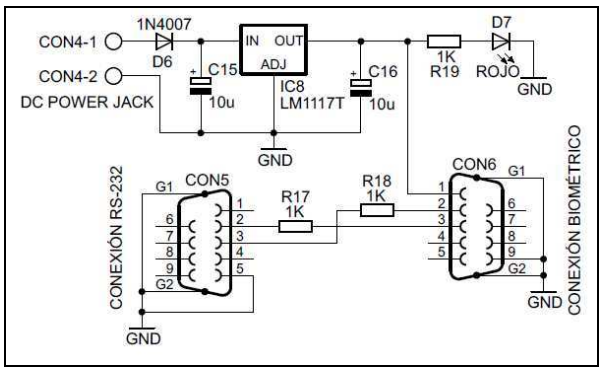


Figura 19: Dispositivo para conexión entre el módulo biométrico y la PC

Fuente: Autor

3.1.4. SUBSISTEMA DE RESPUESTA

El arreglo UNL2803 permite al mecanismo tener la corriente necesaria para manejar la BACKLIGHT del módulo GLCD, la señal de encendido del regulador de voltaje secundario, y en este caso, el relé electromecánico que conmutará la cerradura eléctrica.

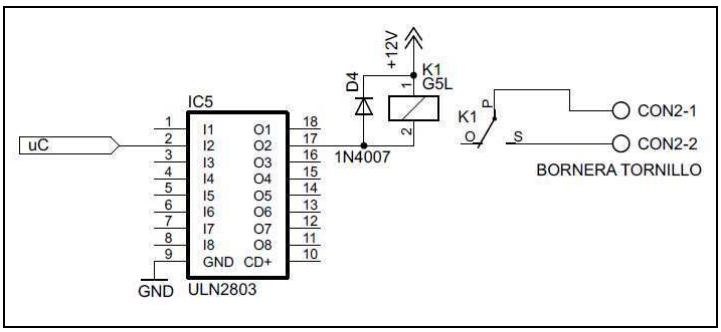


Figura 20: Relevador de potencia para manejo de la cerradura eléctrica

Fuente: Autor

Cuando la salida del microcontrolador se pone en alto, el ULN2803 coloca 0V de hasta 500mA en su salida conectada al relé. Esto provoca que el elemento electromecánico se active y pueda conmutar cargas de hasta 1500W en corriente alterna. El diodo D4 protege a IC5 de voltajes reversos inducidos en la bobina del relé cuando éste se apaga.

3.1.5. ALIMENTACIÓN DEL SISTEMA

Es importante resaltar que existen dos fuentes de voltaje. La primera es usada para la alimentación constante de todo el sistema. La segunda soporta al lector biométrico y su encendido es controlado y temporizado por el microcontrolador.

3.1.5.1. Fuente de alimentación principal

La tensión de alimentación se obtiene de un adaptador inteligente, se filtra y se aplica regulada al resto del circuito. La fuente convierte el voltaje de 12V de entrada en una tensión constante de 5.0V.

En la figura, la fuente de alimentación consta de un rectificador (D1), una protección por sobretensión (R1, D2), un filtro (C1, C2, C3), un regulador lineal fijo de 9V (IC1) y un regulador variable calibrado a 5V (IC2).

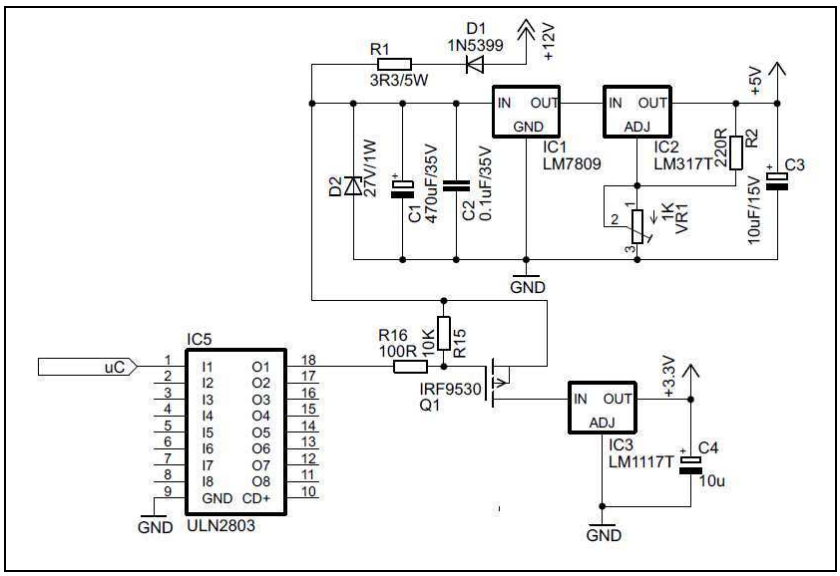


Figura 21: Circuito de alimentación principal y secundario

Fuente: Autor

El rectificador recorta picos negativos de voltaje y protege al circuito cuando por error, se invierte la polaridad de la batería. La resistencia R1 y el zener D2, resguardan al circuito de sobrevoltajes instantáneos.

La regulación se hace en etapas: primero se regula a 9V y luego a 5V. De esta manera, la caída de voltaje de 9V (considerando un voltaje de entrada de 12V), se disipa en algunos integrados. Así, los reguladores de voltaje se calientan menos.

La corriente que pueden suministrar los reguladores según las hojas de datos, es de máximo 1A. Este valor es suficiente para satisfacer las necesidades de potencia del circuito.

3.1.5.2. Fuente de alimentación secundaria

Esta fuente de alimentación es similar a la principal. Su diferencia radica en que el microcontrolador controla el encendido, a través de la interfaz de potencia formada por uno de los transistores de IC5 y Q9.

3.2. DIAGRAMA ESQUEMÁTICO GENERAL

El diagrama esquemático general agrupa a todos los circuitos estudiados, más ciertos componentes de igual importancia como son los condensadores de desacople. Así se evita que corrientes parásitas afecten a los dispositivos. Además se incluyen conectores necesarios en su implementación física.

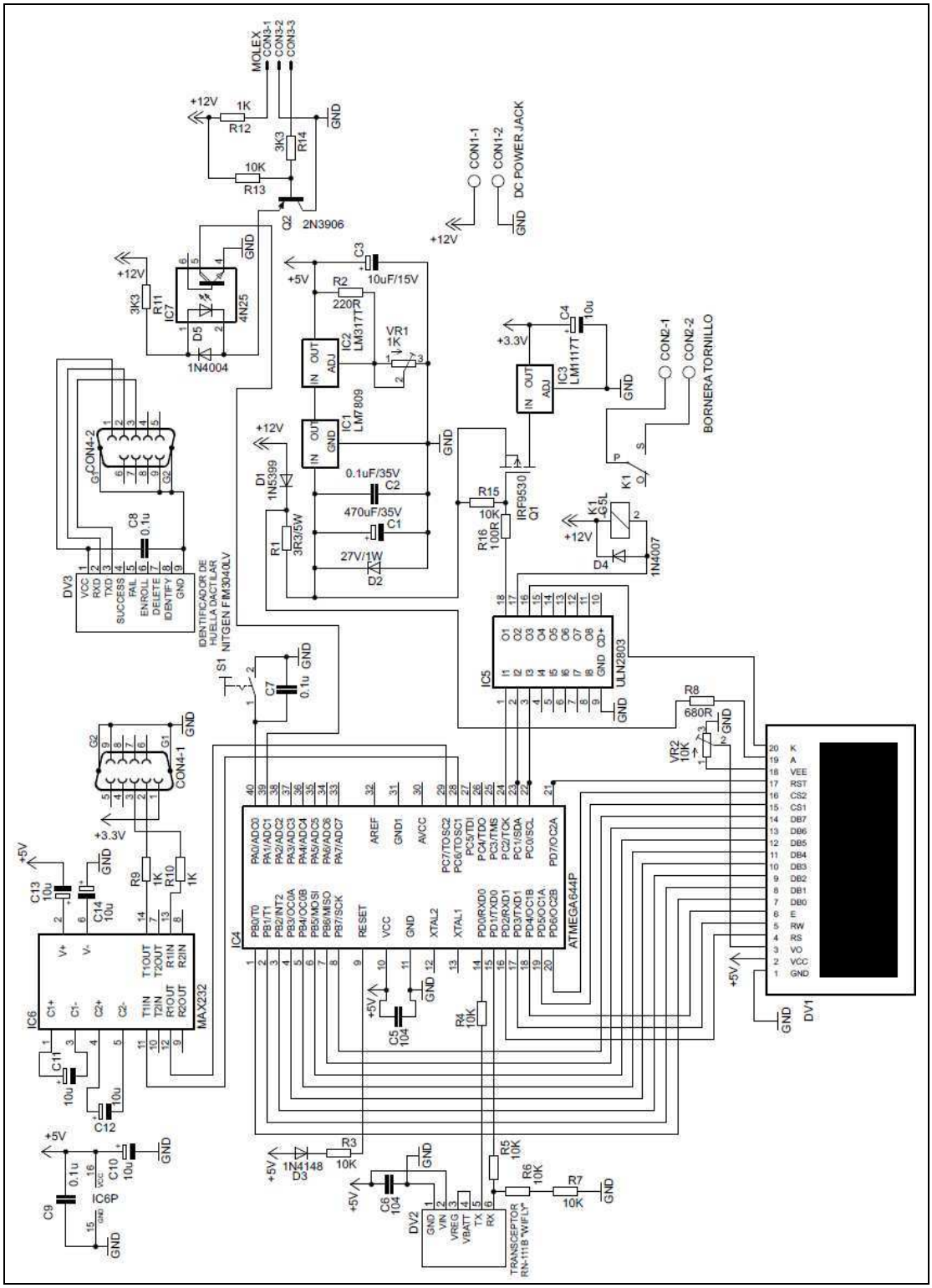


Figura 21: Diagrama esquemático general

Fuente: Autor

3.3. DISEÑO DE LAS PLACAS DE CIRCUITO IMPRESO

El diseño de las placas se realizó cuidando que los circuitos de potencia estén lo suficientemente lejos de los integrados; además, dibujando los condensadores de desacople lo más cerca posible a éstos. Todo para disminuir el efecto de la interferencia.

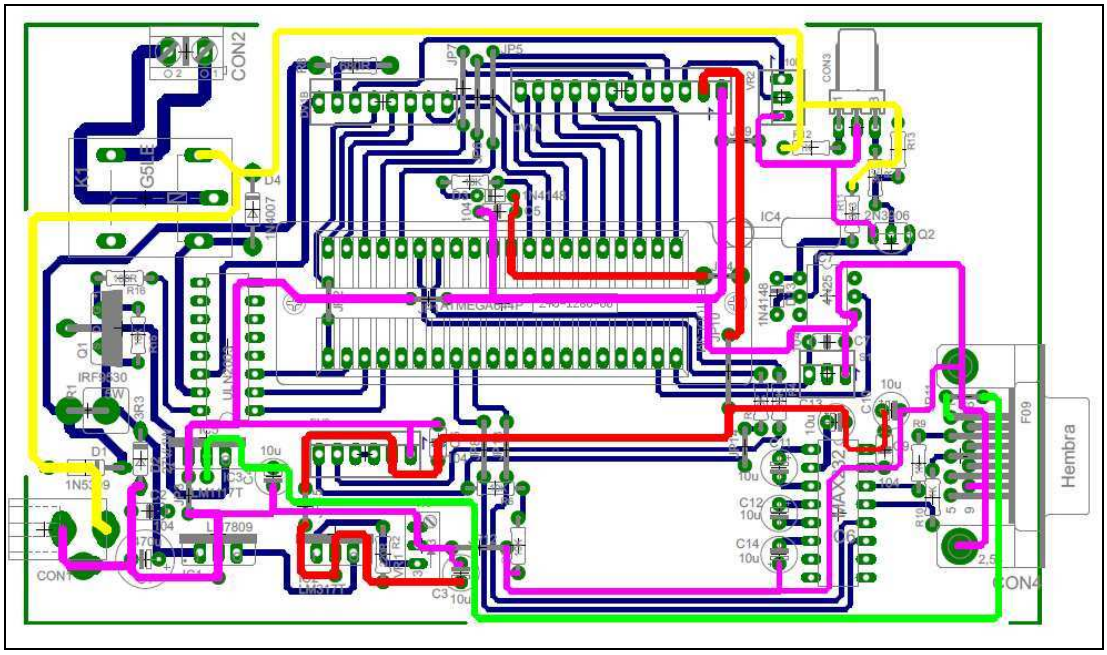


Figura 22: PCB de la placa principal

Fuente: Autor

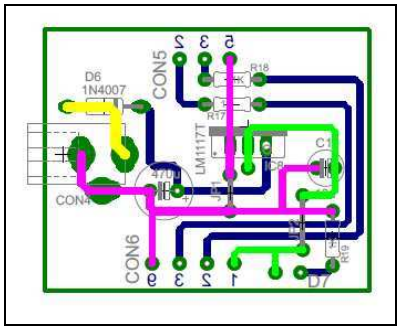


Figura 23: PCB del circuito para conexión entre el biométrico y la PC

Fuente: Autor

3.4. DESCRIPCIÓN DEL FIRMWARE

La tendencia actual, en lo que respecta a la programación de microcontroladores de cualquier marca y tipo, es el uso de compiladores en lenguaje C para el desarrollo de aplicaciones.

C es un lenguaje de nivel intermedio que incorpora muchos elementos propios del ensamblador, puede acceder a los registros del sistema y trabajar con direcciones de memoria, con la particularidad de que permite realizar las operaciones mucho más legibles, utilizar estructuras de datos y otras características propias de los lenguajes de alto nivel.

Este lenguaje permite un manejo abstracto independiente del hardware, a diferencia del ensamblador, pero sin perder mucho del poder y eficiencia que tienen los lenguajes de bajo nivel. Así, es aplicable para desarrollos que necesiten alto grado de optimización.

Algunas de las características más importantes que definen al lenguaje son:

- Tamaño pequeño
- Uso extensivo de llamadas a funciones
- Comandos breves (poco tecleo)
- Lenguaje estructurado
- Programación de bajo nivel (nivel bit)
- Implementación de apuntadores para la memoria, arreglos, estructuras y funciones.

El compilador uC FOR AVR se utiliza para la programación del firmware de este dispositivo. Se lo ha escogido ya que incluye librerías y ejemplos que permiten al programador acceder a la información necesaria para configurar el hardware de los microcontroladores AVR de una manera eficaz.

3.4.1. FIRMWARE DEL MICROCONTROLADOR

Se describen de manera general los algoritmos usados en el microcontrolador.

3.4.1.1. Programa principal

El siguiente diagrama de flujo detalla el funcionamiento del programa principal. Es importante resaltar que varios de los mensajes observados en la pantalla gráfica no se los pormenoriza en este diagrama debido a que se sobreentienden de acuerdo a las acciones tomadas por el sistema microprocesado.

Las siguientes son características importantes del programa:

- El microcontrolador tiene dentro de su hardware un solo módulo UART, el cual está configurado para conectarse con el módulo IEEE802.11b a nivel TTL. Luego de la autenticación biométrica, se envía el número de identificación del usuario y se espera la respuesta, por interrupción, del nombre del usuario y su posible entrada según la hora de la PC.
- Existe un segundo UART virtual (a través de librería) que permite la comunicación entre el microcontrolador y el lector biométrico. La recepción de datos se hace dentro del programa principal, por lo tanto el microcontrolador esclaviza el programa a la espera de datos recibidos.
- La autenticación biométrica de cada usuario es revisada en forma local, dentro de los patrones almacenados previamente en el lector biométrico. La base de datos remota proporciona la correspondiente cadena de caracteres para cada número de usuario, que posteriormente será visualizada en la GLCD.
- La administración del tiempo (hora y fecha) se realiza en la base de datos de la PC, por lo tanto se toma del sistema operativo.

- Existe un usuario maestro (ID 0000) cuyo acceso a la infraestructura es libre, sin necesidad de que el módulo tenga conexión con la base de datos.

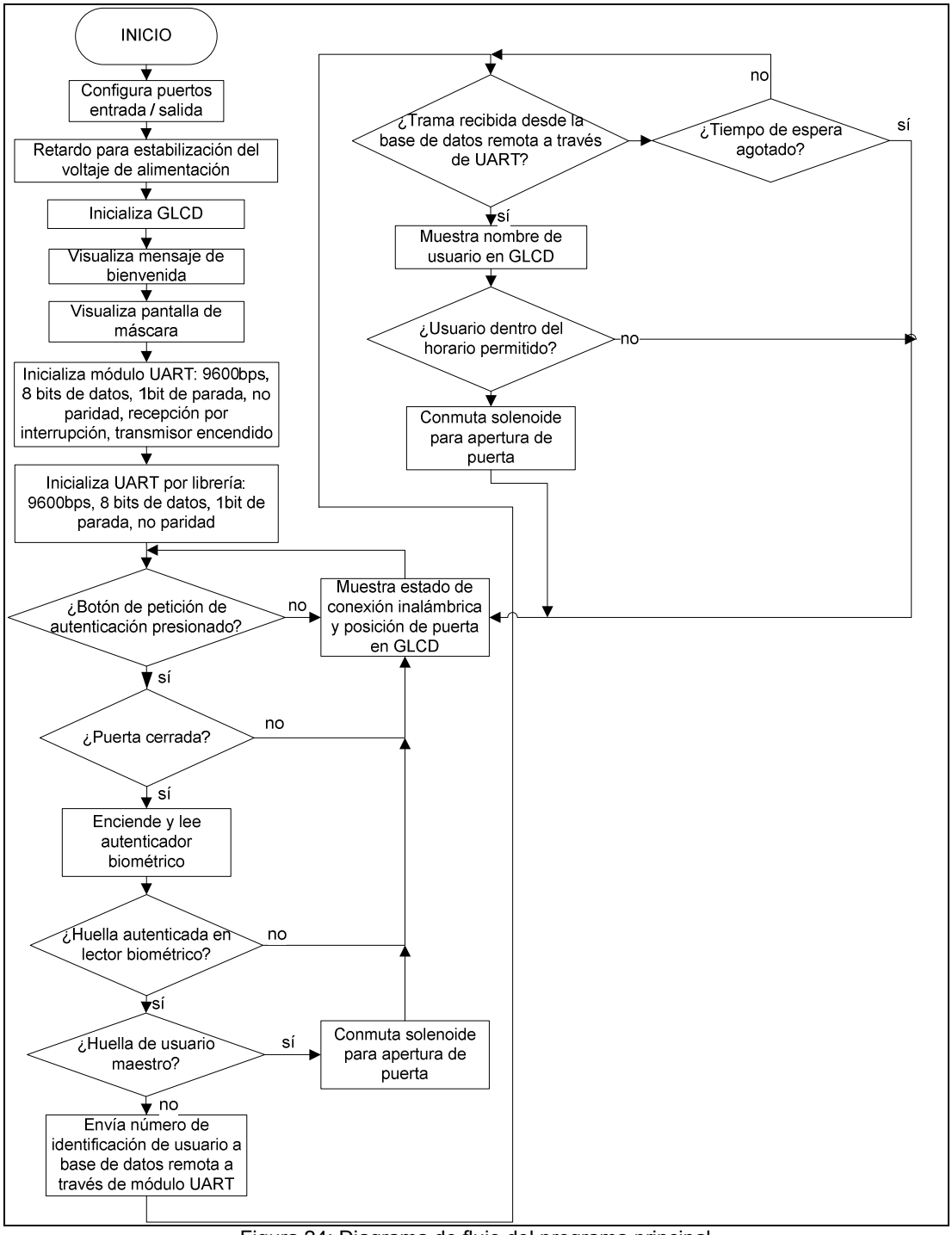


Figura 24: Diagrama de flujo del programa principal

Fuente: Autor

3.4.1.2. Subrutinas especiales

A continuación se detallan los procesos manejados por las subrutinas más relevantes.

3.4.1.2.1. Actualización de estado de conexión y de posición de puerta

Esta subrutina es ejecutada en el programa principal. Se usa para monitorear si se encuentra establecida la conexión inalámbrica entre el módulo WIFLY y el AP a través de un enlace punto a punto bajo TCP/IP. Se usa también para conocer el estado de la puerta al leer la entrada digital conectada al sensor de barrera. Es importante destacar que esta subrutina hace uso tanto de la GLCD como del puerto UART.

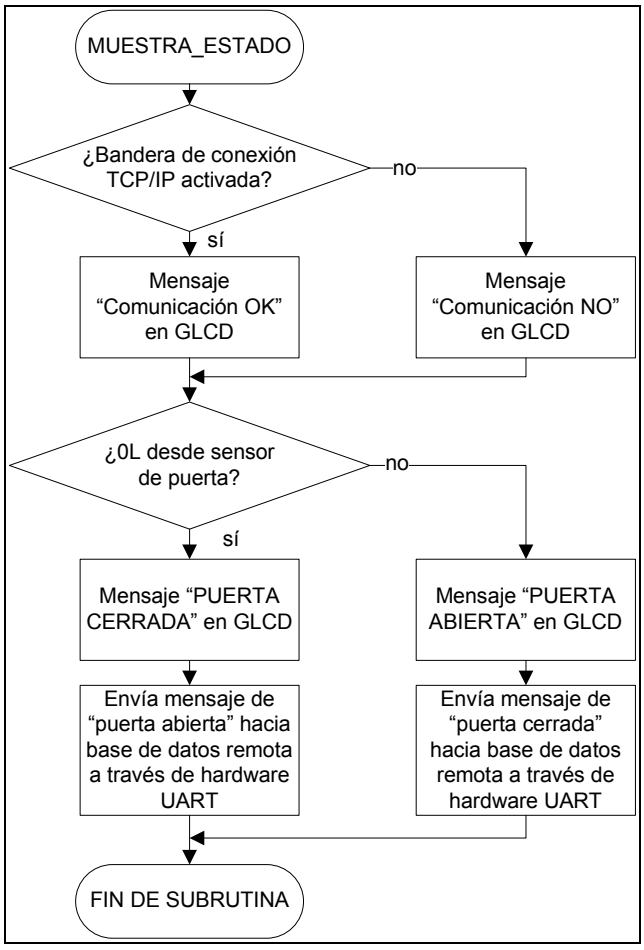


Figura 25: Diagrama de flujo de la subrutina de actualización de estado de conexión y de posición de puerta Fuente: Autor

Como se puede observar en el diagrama anterior, cada vez que se actualiza el estado de la puerta, además de visualizarse el mensaje localmente, se utiliza el puerto UART para enviar el mensaje hacia el módulo WIFLY, y a través de éste, hacia la base de datos en la PC. Lo anterior se realiza para que el programa en la PC anexe cada evento a la base de datos.

3.4.1.2.2. Comunicación con lector biométrico a través de librería UART

Se utilizó un UART emulado por programa además del hardware incluido en el microcontrolador, debido a que se tenían que realizar dos comunicaciones seriales asincrónicas simultáneas.

El inconveniente del uso de esta comunicación por software radica en que se la debe manejar en el programa principal. Así, el programa espera a recibir datos seriales, sin poder realizar mientras tanto, otro proceso en el flujo principal.

En el siguiente diagrama de flujo, se observa la secuencia de envío / recepción de tramas de datos entre el microcontrolador y el lector biométrico.

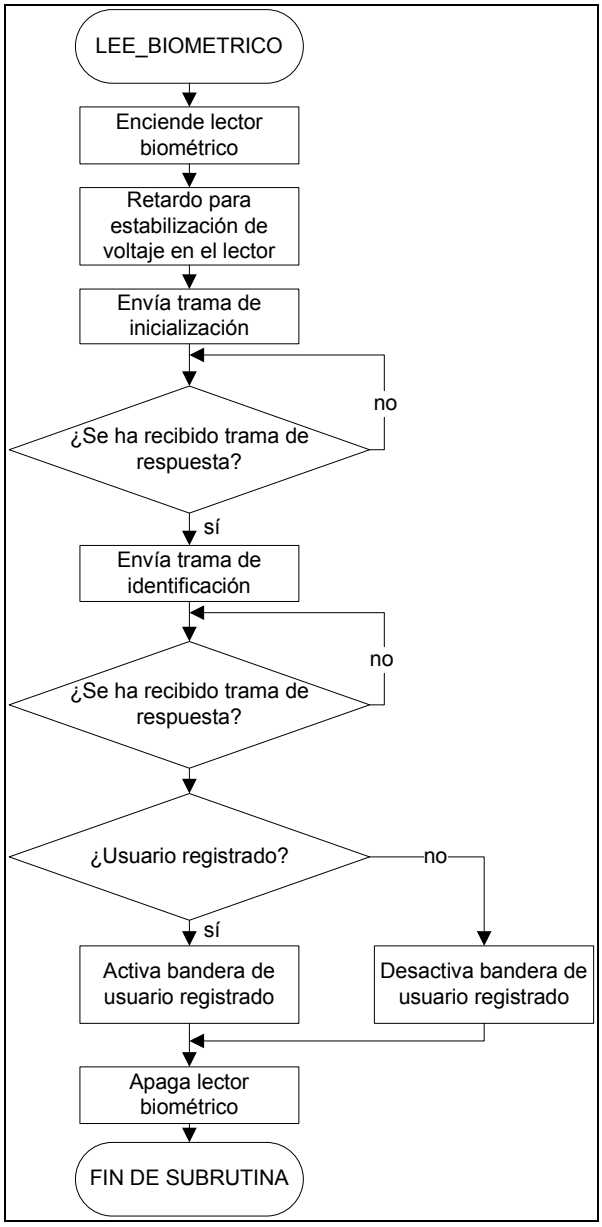


Figura 26: Diagrama de flujo de la subrutina de comunicación con el lector biométrico

Fuente: Autor

La siguiente tabla muestra en detalle las tramas de datos manejadas en la comunicación con el lector biométrico.

Tabla 11: Tramas de datos manejadas en la comunicación entre el microcontrolador y el lector biométrico

TIPO DE TRAMA	FLUJO	TRAMA
Inicialización (petición de conexión)	uC - Lector	0x7E,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01
Respuesta a la inicialización	Lector - uC	0x7E,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x0A,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0C
Petición de identificación	uC - Lector	0x7E,0x00,0x00,0x00,0x12,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x12
Respuesta de usuario registrado	Lector - uC	0x7E,0x00,0x00,0x00,0x12,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0A,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x1D,0x31,0x32,0x33,0x34,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xCA
Respuesta de usuario no registrado	Lector - uC	0x7E,0x00,0x00,0x00,0x12,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x13

Fuente: Autor

Los valores resaltados 0x31 0x32 0x33 0x34 forman el número de identificación del usuario y por lo tanto no son fijos. Esta trama posee dos campos más que las demás, ya que contiene información. Las siguientes figuras indican los campos que forman parte de las tramas de comandos y datos utilizadas en la comunicación con el lector biométrico.

Command (1 byte)	Param1 (4 bytes)	Param2 (4 bytes)	Data Size (4 bytes)	Error Code (4 bytes)	Header Checksum (4 bytes)

Figura 27: Modelo de trama de comando usada para el acceso al lector biométrico Fuente: Autor

Command (1 byte)	Param1 (4 bytes)	Param2 (4 bytes)	Data Size (4 bytes)	Error Code (4 bytes)	Header Checksum (4 bytes)	Data (10 bytes)	Data Checksum (4 bytes)

Figura 28: Modelo de trama de datos usada para el acceso al lector biométrico Fuente: Autor

La información detallada sobre el significado de los campos se puede revisar en el manual del desarrollador, anexo al presente trabajo escrito.

3.4.1.2.3. Comunicación con módulo WIFLY a través de hardware UART

Para el acceso al dispositivo de comunicación inalámbrica se usa el módulo UART interno del microcontrolador. La transmisión de datos se

realiza en el programa principal y por lo tanto no necesita de un análisis exhaustivo. Sin embargo, la recepción de datos se maneja por interrupción y por esta razón es preciso un estudio más profundo.

La rutina especial de interrupción se ejecuta cada vez que un byte ha sido recibido. El diagrama de flujo de la interrupción se muestra en la figura 29. Una vez que la rutina recibe el carácter especial “&” (fin de trama), coloca la carga útil del búfer en los registros de trabajo. Así, es el programa principal el encargado de interpretar los comandos recibidos.

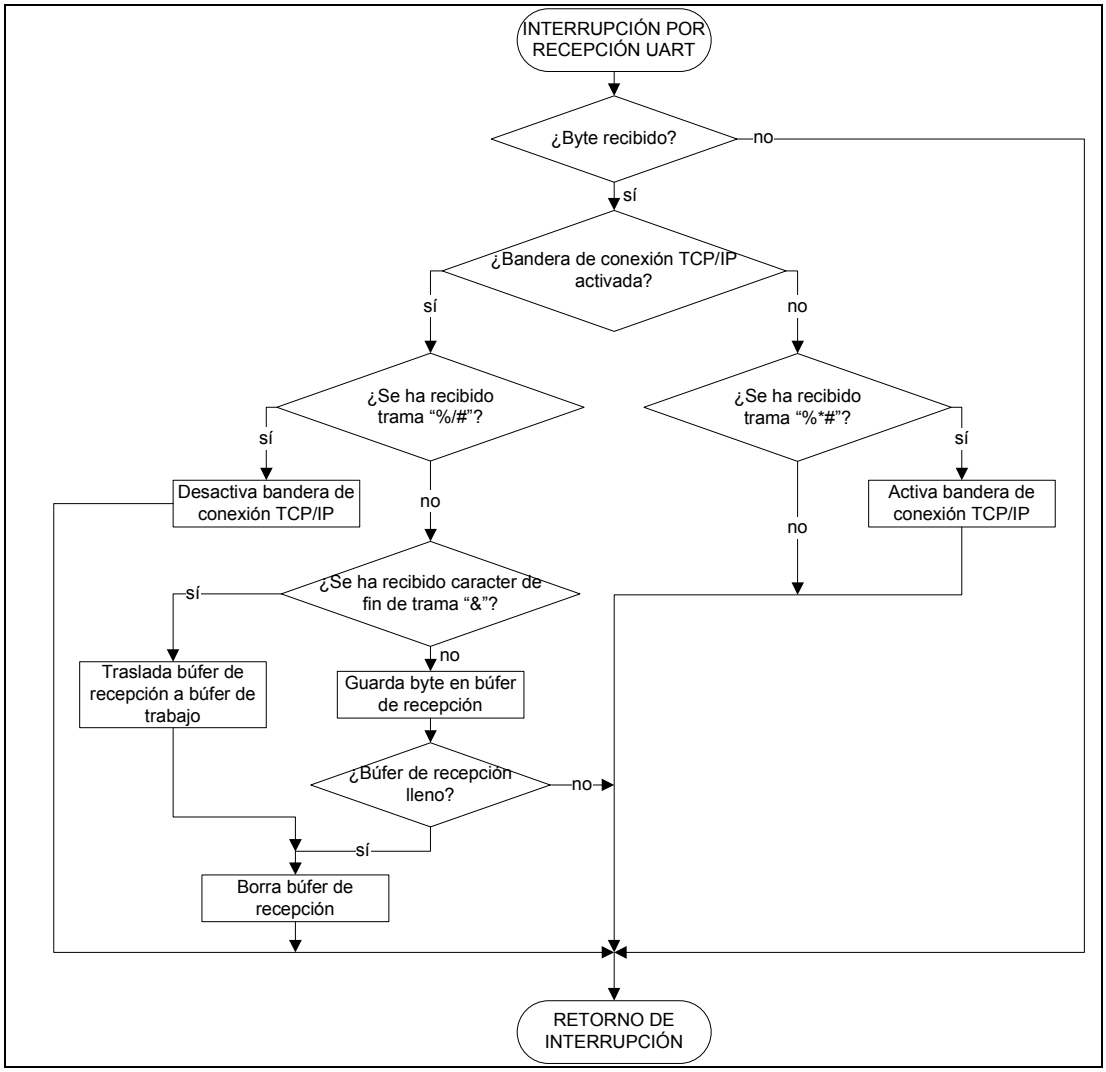


Figura 29: Rutina especial de interrupción por recepción UART Fuente: Autor

La información es recibida a nivel de bytes y cada mensaje enviado y adquirido en formato ASCII empieza con el caracter de inicio de dato, seguido de la carga útil, terminando con el caracter de final de dato.

Tabla 12: Tramas de datos desde el microcontrolador hacia la base de datos

TIPO DE TRAMA	TRAMA
Puerta abierta	$AAAA&
Puerta cerrada	$CCCC&
Petición de verificación en base de datos	$0202&

Fuente: Autor

En la tabla anterior, el valor resaltado pertenece a la identificación de usuario proporcionada previamente por el lector biométrico, por lo tanto, puede cambiar.

Por otro lado, el tráfico de información desde la PC hacia el dispositivo se realiza utilizando un solo modelo de trama.

Tabla 13: Modelo de trama enviada desde la PC hacia el microcontrolador

CAMPOS	INICIO DE TRAMA	CADENA DE CARACTERES DE NOMBRE DE USUARIO	SEÑALIZADOR	CADENA DE CARACTERES DE APELLIDO DE USUARIO	SEÑALIZADOR	COMANDO DE ACCESO	FIN DE TRAMA
TAMAÑO [BYTES]	1	13	1	13	1	1	2
EJEMPLO DE ACCESO AUTORIZADO	$	ESTEFANIA_GRA	$	TORRES_AZA___	$	A	$&
EJEMPLO DE ACCESO NO AUTORIZADO	$	ESTEFANIA_GRA	$	TORRES_AZA___	$	B	$&

Fuente: Autor

3.5. DESCRIPCIÓN DEL SOFTWARE

3.5.1. SOFTWARE EN PC

El software de la computadora personal está realizado en Visual Basic 6.0. Se lo escogió debido a su simplicidad de uso y gran robustez. Es un lenguaje orientado a eventos, sus controles e indicadores se pueden personalizar gráficamente y existe bastante información disponible en la red para los programadores novatos.

Las características más importantes de esta aplicación son:

- Maneja el puerto Ethernet de la PC a través del componente WINSOCK. Este elemento permite realizar conexiones cliente / servidor a través del protocolo TCP/IP.
- Utiliza las referencias *Microsoft Data Formatting Object Library* y *Microsoft ActiveX Data Objects*, lo que le permite trabajar en conjunto con MYSQL y administrar la base de datos.
- Los campos de la base de datos que manejan la información del usuario son: nombres, apellidos, hora de entrada, hora de salida, fecha de inicialización del turno.
- Los reportes que puede imprimir el administrador del sistema son: autenticaciones (usuario, hora, fecha, acceso), apertura de la puerta (fecha, hora de apertura, hora de cierre).
- La primera interfaz gráfica indica el estado de la conexión, la IP del módulo remoto, un botón para entablar y terminar la comunicación y una tabla que contiene información de la nómina de empleados.

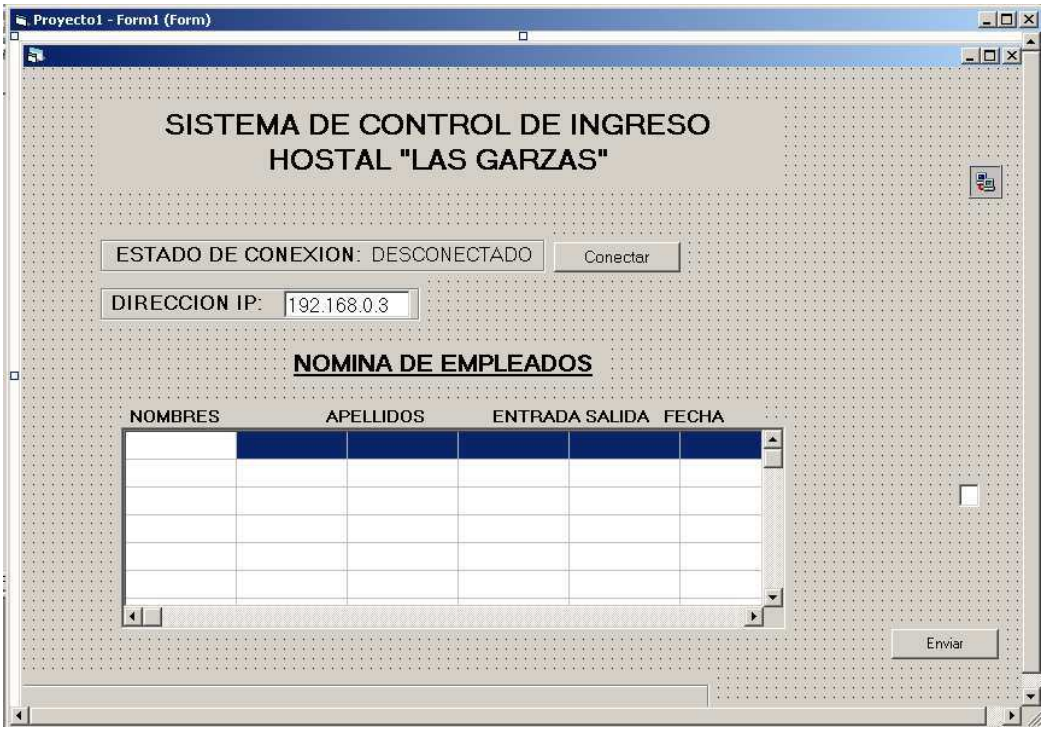


Figura 30: Pantalla principal del programa

Fuente: Autor

- La segunda interfaz gráfica permite ingresar los empleados, previamente autenticados en el lector biométrico, en la base de datos. Es importante resaltar la necesidad de coincidencia entre la clave asignada en la base de datos y el número de usuario grabado en la memoria interna del lector biométrico.

Figura 31: Pantalla de ingreso de datos del empleado

Fuente: Autor

Se puede encontrar información más detallada en el programa de manejo de la base de datos, disponible en el anexo escrito y digital.

3.5.2. SOFTWARE DE CONFIGURACIÓN DEL LECTOR BIOMÉTRICO

Para configurar el hardware del lector e ingresar nuevos usuarios se utiliza el software EVTOOLS de NITGEN, proporcionado por esta empresa sólo a desarrolladores de dispositivos. Este programa mantiene una comunicación serial con el lector biométrico y permite identificar, agregar y borrar las huellas dactilares.

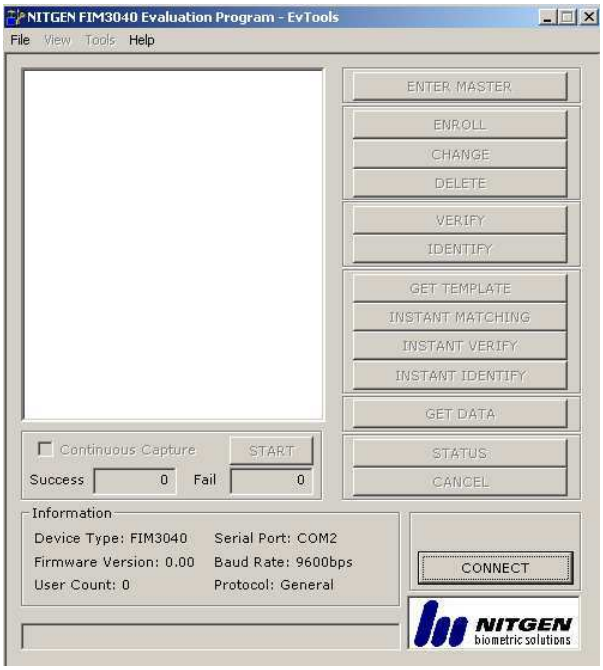


Figura 32: Software EVTOOLS de NITGEN

Fuente: Autor

CAPÍTULO IV

4. IMPLEMENTACIÓN Y PRUEBAS

Este capítulo realiza la descripción del montaje físico del dispositivo y puesta en funcionamiento del equipo al configurar los parámetros eléctricos y de red necesarios. Posteriormente se determina la fiabilidad en la adquisición de datos y la transmisión inalámbrica de los mismos, observando del desempeño general del sistema.

4.1. MONTAJE DEL SISTEMA

4.1.1. MONTAJE FÍSICO

Luego de terminadas las placas, se colocó el sistema en cajas para darle una estructura modular. Las siguientes imágenes muestran los distintos dispositivos que forman parte del mecanismo.

- Lector biométrico:

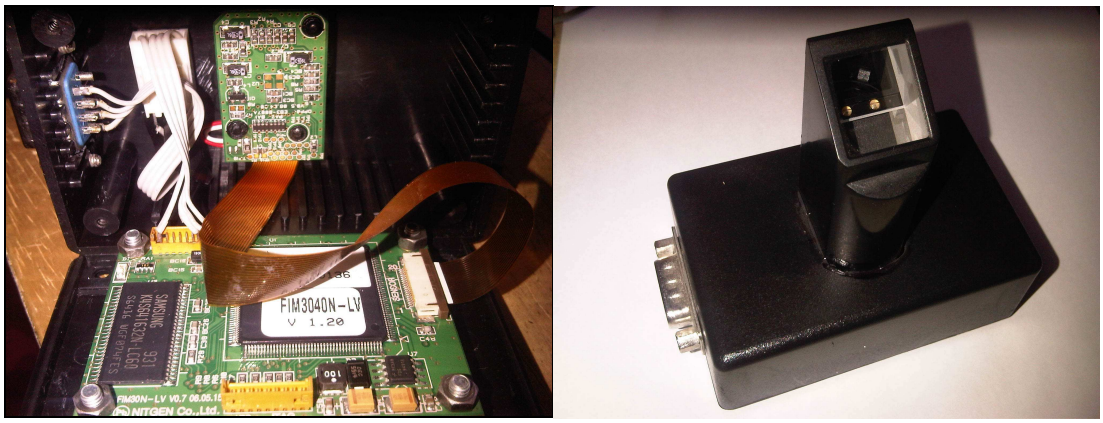


Figura 33: Lector biométrico

Fuente: Autor

- Módulo de control de acceso:

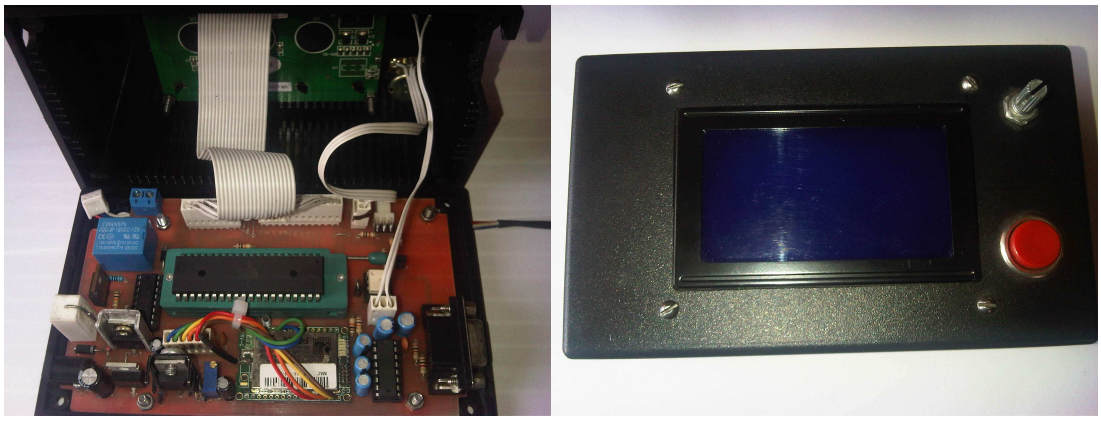


Figura 34: Control de acceso

Fuente: Autor

- Interfaz para conexión del lector biométrico a la PC:

Figura 35: Interfaz para conexión del lector biométrico a la PC

Fuente: Autor

- Sensor de apertura de la puerta:

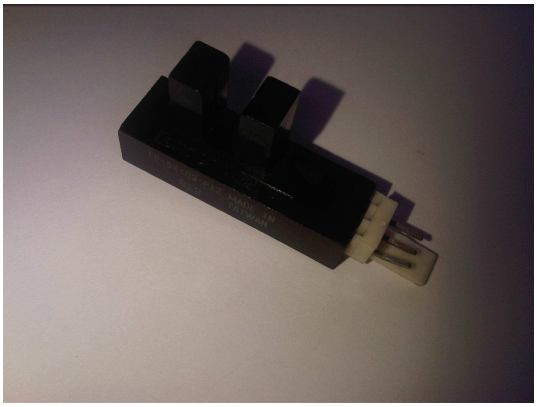


Figura 36: Sensor óptico de apertura de la puerta

Fuente: Autor

- Punto de acceso:

Figura 37: Punto de acceso

Fuente: Autor

4.1.2. IMPLEMENTACIÓN

La implementación del dispositivo se realizó procurando causar el menor impacto posible tanto en la estructura civil como en el cableado de la hostal.

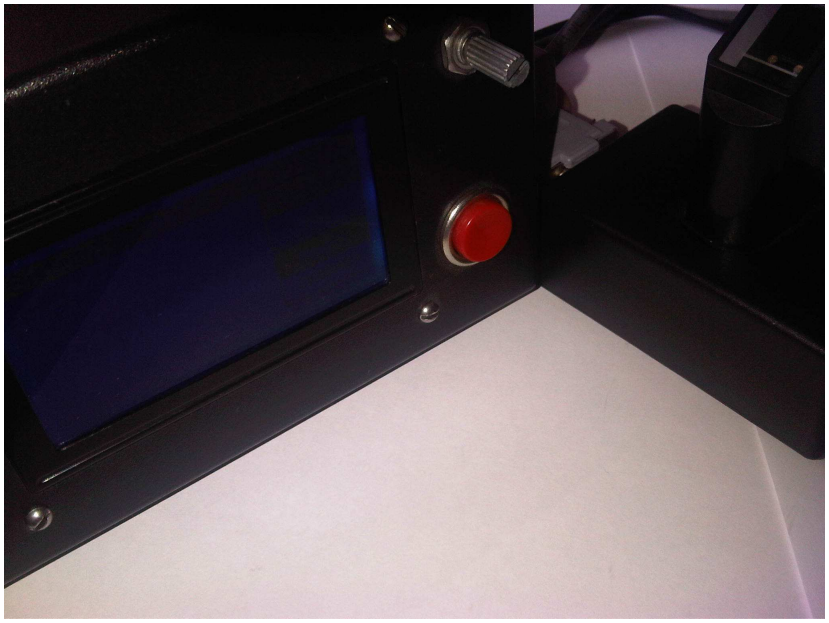


Figura 38: Implementación del sistema de control de acceso

Fuente: Autor

Las conexiones de la alimentación se hicieron de tal manera que no queden descubiertos los cables para evitar que el sistema sea violado por

desconexión. El mismo cuidado se tuvo al conectar el sensor de barrera y la cerradura eléctrica.

Figura 39: Módulo electrónico en funcionamiento

Fuente: Autor

4.1.2.1. Configuración del lector biométrico

Para configurar el lector biométrico se lo debe conectar cable serial y la interfaz a la PC.

Figura 40: Conexión del lector biométrico a la PC

Fuente: Autor

Se utilizan las siguientes imágenes para detallar el uso del software EVTOOLS en el proceso de administración de las huellas dactilares de los usuarios.

- Se abre la aplicación EVTOOLS y se selecciona ARCHIVO / SERIAL COM. Se selecciona 9600 baudios y el número de puerto COM que el sistema operativo le da al cable USB /RS232.

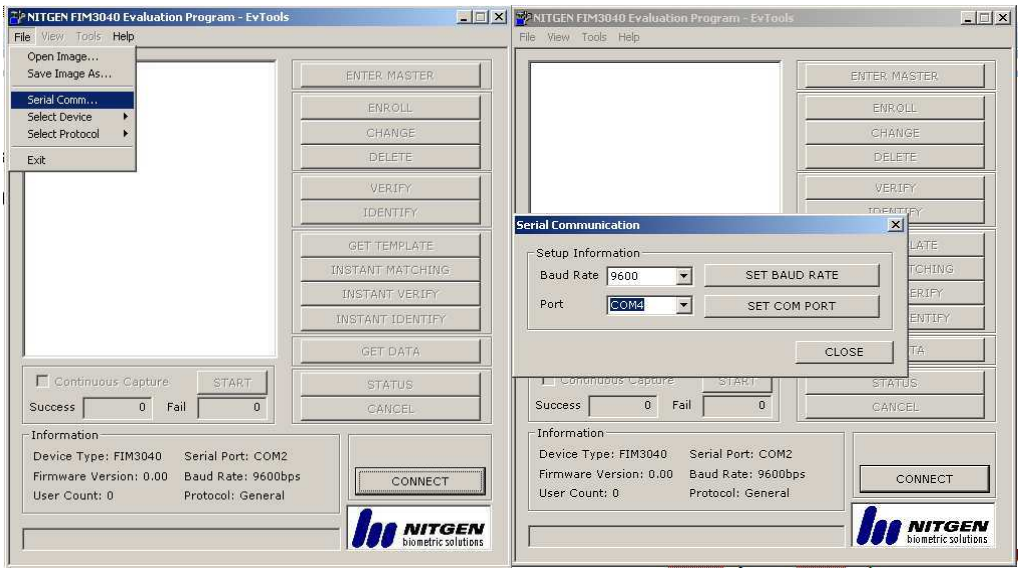


Figura 41: Configuración del puerto serial de conexión

Fuente: Autor

- El sistema indica que se ha configurado correctamente el puerto COM. Posteriormente se presiona en CONNECT y se espera el mensaje de confirmación. Se ingresa en ENTER MASTER, se escoge DEVICE PASSWORD.

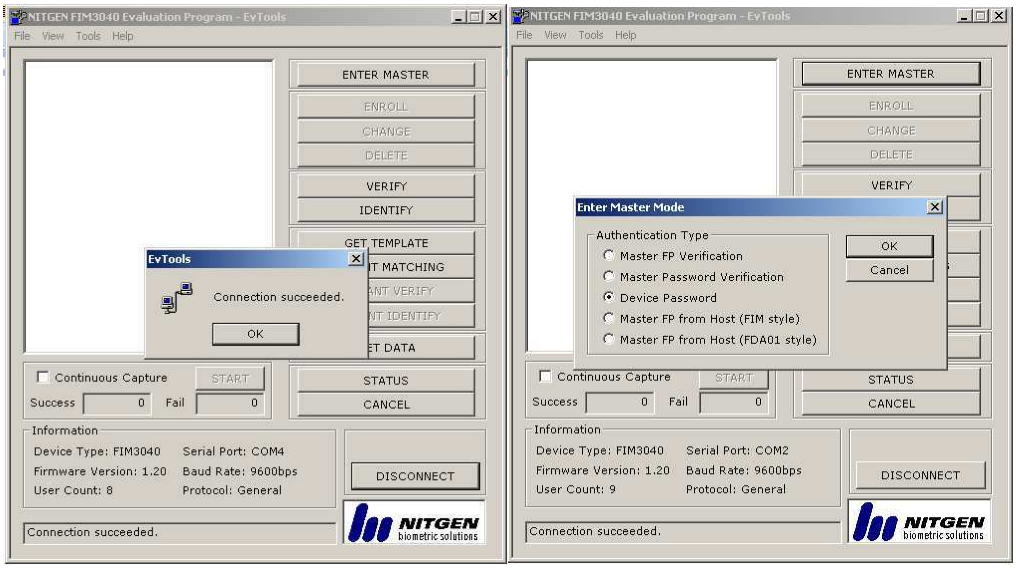


Figura 42: Conexión e ingreso a modo maestro

Fuente: Autor

- Se ingresa la contraseña “0123456” y se hace click en ENROLL. En este punto el dispositivo está listo para ingresar un nuevo usuario. Aquí se debe teclear una identificación de 4 dígitos (ID). Este código posteriormente se va a ingresar en la base de datos de la computadora.

Figura 43: Proceso de ingreso de ID antes de inclusión de un nuevo usuario al lector biométrico

Fuente: Autor

- El nuevo usuario enseguida debe colocar una de sus huellas en el lector por dos ocasiones y esperar el mensaje de confirmación.

Figura 44: Proceso de lectura de la huella dactilar del nuevo usuario

Fuente: Autor

4.1.2.2. Configuración de la interfaz HMI en la PC

Una vez terminado el proceso anterior, se debe asignar una cadena de caracteres a aquel código de 4 dígitos que se ingresó al insertar un nuevo usuario en la base de datos. Para esto se inicia el programa que maneja la base de datos y se hace click en CONECTAR.

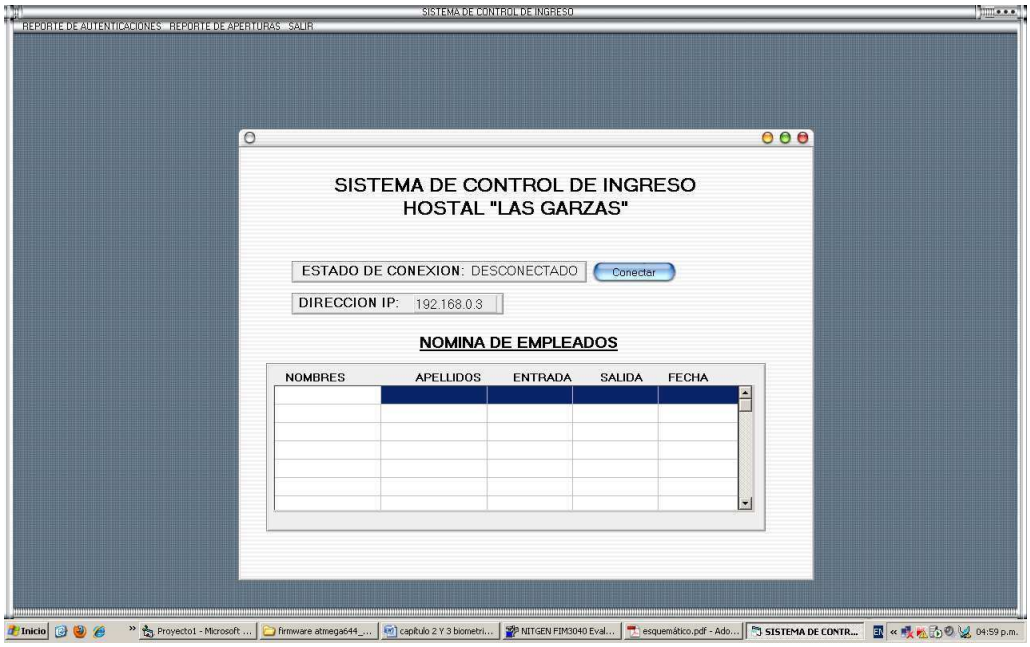


Figura 45: Proceso de inserción de un nuevo usuario en la base de datos

Fuente: Autor

Luego de iniciada la conexión, se llenan los campos de la base tales como nombres, apellidos, hora de entrada, hora de salida y fecha a partir de la cual empieza a laborar el empleado. Además, se ingresa el código ID con el que a ese usuario se ingresó en el lector biométrico.

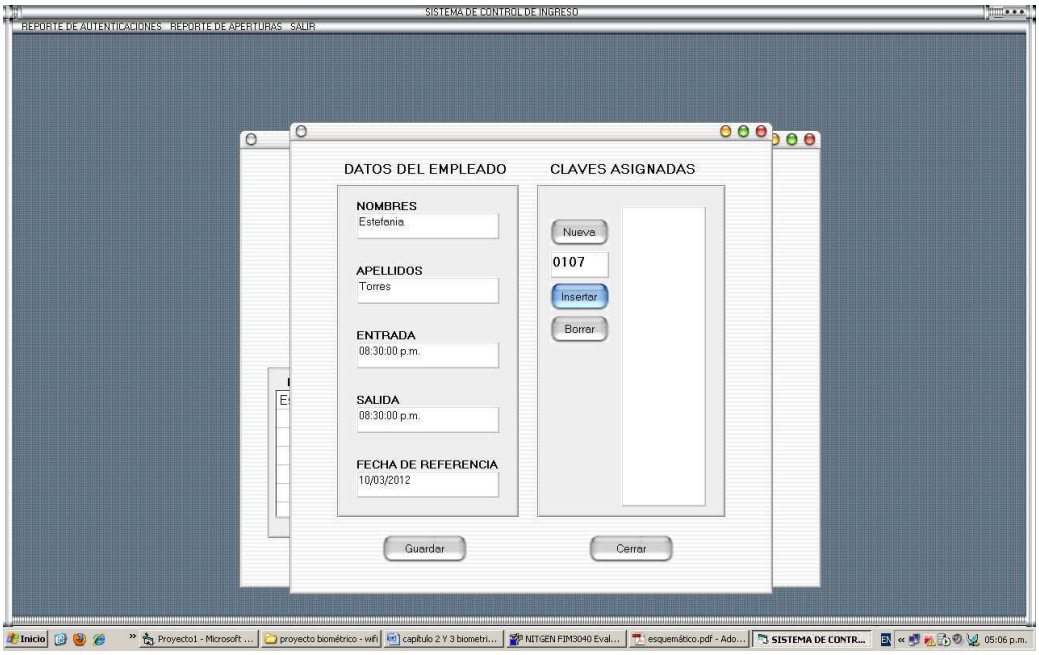


Figura 46: Asignación de un nombre al código de 4 dígitos (ID) de un usuario.

Fuente: Autor

Si el proceso se realizó satisfactoriamente, se tendrá un nuevo empleado ingresado y el sistema empezará a aplicar el control de acceso con él.

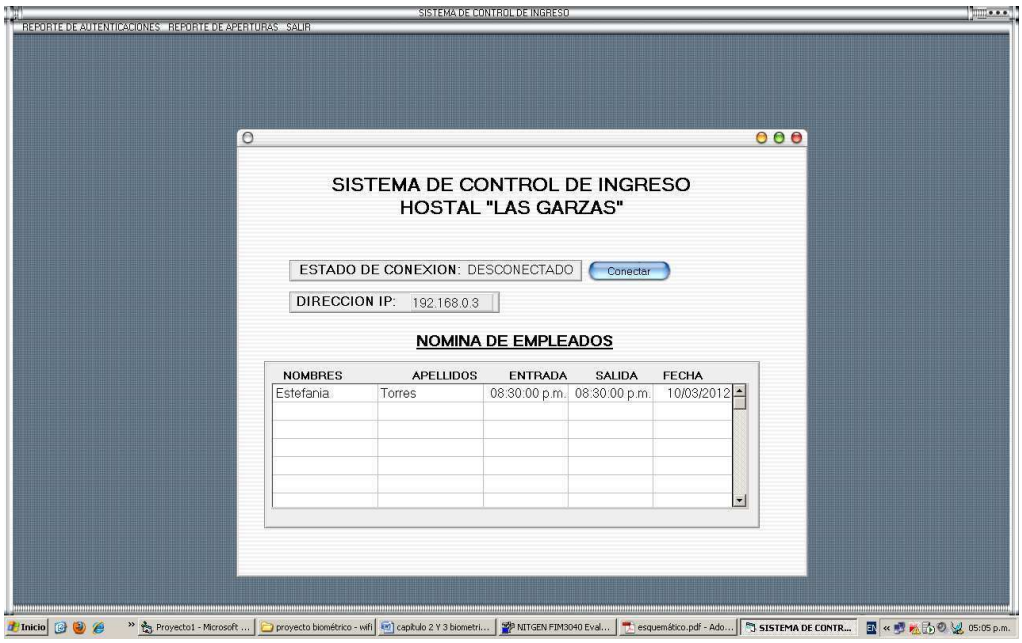


Figura 47: Usuario asignado en la base de datos

Fuente: Autor

4.2. PRUEBAS

A lo largo del desarrollo del proyecto, se realizaron múltiples pruebas tanto a nivel de firmware como de hardware; pruebas individuales y con todo el sistema funcionando. Las pruebas individuales más importantes consistieron básicamente en verificar lo siguiente:

- Funcionamiento correcto de las interfaces utilizadas; así mismo la interacción de éstas con el microcontrolador.
- Comunicación entre el microcontrolador y el módulo WIFLY.
- Comunicación entre el microcontrolador y el lector biométrico.
- Actualización de datos en la GLCD.
- Pruebas con las diferentes tramas manejadas en la transmisión inalámbrica de datos.
- Manipulación de datos por parte del software en la PC, observando la correcta codificación de las tramas enviadas e interpretación de las tramas recibidas.

Después de superadas todas las pruebas individuales, se procedió con la verificación del funcionamiento de todo el sistema en conjunto.

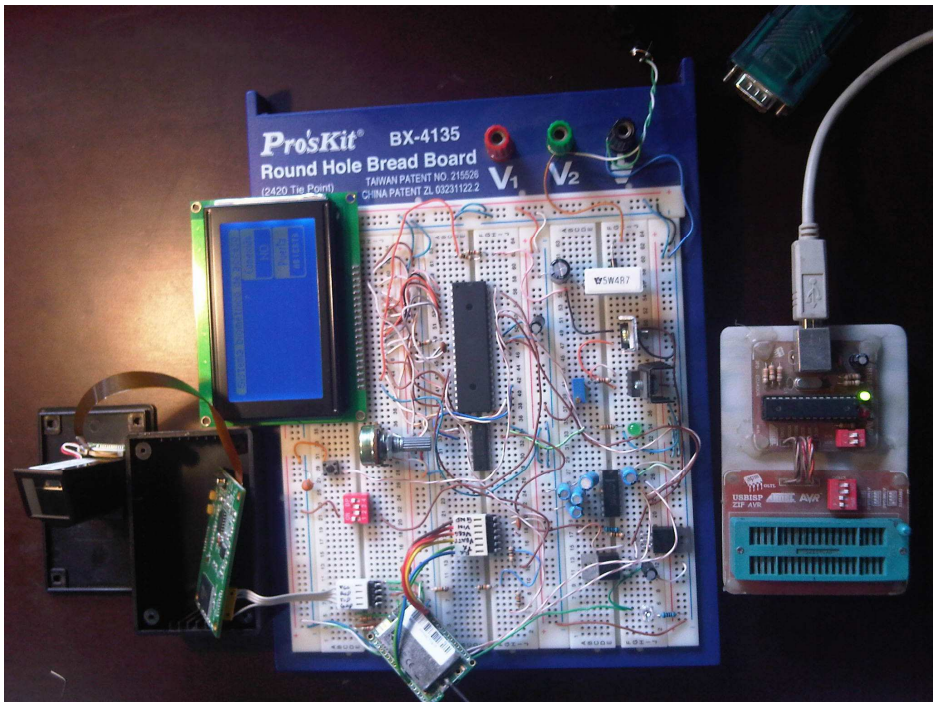


Figura 48: Pruebas previas del sistema en tablero de ensayo electrónico
Fuente: Autor

4.2.1. PRUEBA DE ALCANCE

En cuanto a la distancia hay un patrón que predomina en la calidad del enlace inalámbrico. Al aire libre y sin obstáculos, la distancia máxima a la que funciona la comunicación entre el AP y el módulo WIFLY es de 110m. Pero a medida que se incluyen obstáculos en medio de la comunicación la calidad del enlace se va deteriorando.

Se realizaron pruebas en diferentes escenarios, utilizando los materiales más comunes encontrados en la realidad. Se pudieron constatar los valores indicados en la siguiente tabla:

Tabla 14: Pruebas de alcance en diferentes escenarios

OBSTÁCULO	ALCANCE
Paredes de concreto	50m
Puertas de metal	10m
Puertas de madera	70m
Vehículos y árboles	80m

Fuente: Autor

4.2.2. PRUEBA DE INTERFERENCIA EN EL MEDIO DE TRANSMISIÓN

La prueba se realizó en espacios reducidos donde existe presencia masiva de dispositivos que trabajan en la frecuencia del sistema (2.4Ghz).

Se consideraron lugares como centros comerciales, parques y centros educativos, en donde la presencia del Acces Point para brindar internet es concurrida.

El sistema disminuyó el alcance y aumentó su velocidad de respuesta cuando se lo puso a trabajar cerca a una red que funcionaba en el mismo canal de comunicación que la del enlace. Hay que tener en cuenta que no se trabajó con salto dinámico de canal.

Tabla 15: Pruebas de respuesta en diferentes escenarios

CANTIDAD DE INTERFERENCIA	RESPUESTA [seg]
Ninguna	1
Media	1.3
Alta	1.8

Fuente: Autor

4.3. DESEMPEÑO GENERAL DEL SISTEMA

De las anteriores pruebas se puede indicar que todas las mediciones arrojaron valores muy satisfactorios.

En lo referente al tiempo de respuesta de la base de datos, se tienen mínimas variaciones debido a que el computador está trabajando libre (no existen aplicaciones de usuario abiertas).

En cuanto a los valores tomados en las pruebas de alcance existe una limitación debido a la sensibilidad y la clase de radio de los equipos.
Por otro lado, las pruebas de funcionamiento del sistema completo, indican que el dispositivo es seguro. Su implementación es recomendable.

4.4. PRESUPUESTO REFERENCIAL

El presupuesto que describe los costos de los elementos del módulo es el siguiente:

Tabla 16: Costos de componentes del módulo control de acceso

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Microcontrolador ATMEGA644	1	10.00	10.00
Regulador de voltaje variable LM317T	1	0.60	0.60
Regulador de voltaje a 9V LM7809	1	0.60	0.60
Regulador de voltaje a 3.3V LM1117T	1	1.00	1.00
Conector MOLEX	8	0.40	3.20
Conector DB9	5	0.70	3.50
Módulo WIFLY	1	80.00	80.00
Lector biométrico	1	120.00	120.00
Zócalo ZIF 40 pines	1	3.00	3.00
Módulo GLCD 128x64 con BACKLIGHT	1	35.00	35.00
Sensor infrarrojo de barrera	1	4.00	4.00
Elementos de soldadura	1	5.00	5.00
Placa de fibra de vidrio, incluida manufactura de la PCB	1	10.00	10.00
Elementos varios (resistencias, capacitores y diodos)	1	10.00	10.00
Cerradura eléctrica	1	15.00	15.00
Caja de plástico para alojamiento del dispositivo electrónico	1	10.00	10.00
Base para fijación de la caja	1	10.00	10.00
Cable blindado de 9 conductores con terminales DB9	1	5.00	5.00
Cable plano de 20 conductores (0.5m)	1	1.00	1.00
ACCESS POINT	1	70.00	70.00
Cable USB - RS232	1	10.00	10.00
Brazo hidráulico para cierre automático de la puerta	1	15.00	15.00
TOTAL (USD)			421.90

Fuente: Autor

A continuación se presenta el detalle de todos los gastos realizados en el diseño y construcción del módulo:

Tabla 17: Costo total del diseño y construcción del sistema

INGENIERÍA E INFORMACIÓN		**200**
Colaboración científica	100	
Investigación	100	
COSTOS DIRECTOS		**531.90**
Elementos eléctricos y electrónicos	421.90	
Programador para AVRs USBASP	30	
Edición de trabajo escrito	80	
IMPREVISTOS		**100**
Transporte y desplazamiento	50	
Otros	50	
COSTO TOTAL		**831.90**

Fuente: Autor

4.5. ANÁLISIS COSTO – BENEFICIO

Un proyecto de las mismas características que el presente, tiene un costo de implementación que fluctúa entre 300 y 400 dólares.

El dispositivo está en plena capacidad de ser competitivo con sistemas profesionales, debido a la cantidad de servicios que presta con hardware reducido. Además, su naturaleza programable lo hace versátil ante distintas aplicaciones.

Se concluye que el sistema tiene bajo costo en relación de su gran desempeño.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se cumplieron los objetivos planteados en el plan del proyecto de titulación, es decir, se construyó un prototipo de red para el control de ingreso utilizando las tecnologías para reconocimiento biométrico y de huella dactilar.

- Se analizaron las características que ofrecen las tecnologías de identificación las cuales pudieron ser aplicadas a las comunicaciones inalámbricas en los sistemas microcontrolados.

- El software elaborado en Visual Basic realiza la consulta en la base de datos para autorizar o denegar el ingreso de los empleados a la bodega; permite además imprimir reportes.

- El sistema de control de acceso que se implementó en la Hostal las Garzas es confiable, debido a que se trata de un sistema rápido que incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado.

- Los elementos electrónicos que fueron utilizados en la implementación fueron los correctos ya que estos permitieron el buen funcionamiento del prototipo con ayuda de diagramas de bloques y de flujo. Se aplicaron los conocimientos adquiridos, especialmente los de seguridad de la información, redes inalámbricas, base de datos y programación.

- El costo final que involucra el poner en marcha este sistema de control de acceso es una inversión que se justifica, puesto que permite un ingreso en menor tiempo y de manera ordenada.

5.2. RECOMENDACIONES

- Debido a que la información almacenada en la base de datos es muy valiosa se recomienda mantener respaldos de la misma, de esta manera se da confiabilidad al sistema.

- Es imprescindible mantener restringido el acceso a la base de datos al personal no autorizado, puesto que en ésta se almacenan los códigos de las huellas dactilares.

- Es necesario que el lector reciba protección adicional debido a que deben estar protegidos contra el vandalismo que siempre está presente.

- Es necesario disponer de un sistema de respaldo de energía eléctrica en caso de existir fallas en la misma durante el ingreso de las personas, de esta manera se garantiza la disponibilidad del sistema.

6. REFERENCIAS BIBLIOGRÁFICAS

6.1. TEXTOS

- **REID** Neil, *802.11 (Wi-Fi): Manual de Redes Inalámbricas*, McGraw – Hill Interamericana, México, 2007.
- **TANENBAUM** Andrew, *Redes de Computadoras*, Prentice Hall Hispanoamericana, México, 2007.
- **STALLINGS**, W., *Comunicaciones y Redes de Computadores*, Prentice Hall, 2008.
- **FISH** Peter, *Electronic Noise and Low Noise Design*, McGraw – Hill, 2007.
- **MOMPIM**, José, *Electrónica y automática industriales*, Marcombo Boixareu, Barcelona – España, 2008.
- **PARDUE** Joe, *C Programming for Microcontrollers*, Smiley Micros, Knoxville TN 37909, USA, 2007.
- **GADRE** Dhananjay, *Programming and Customizing the AVR Microcontroller*, McGraw – Hill, USA, 2008.
- **VALENCIA** Ramiro, *Aplicaciones Electrónicas con Microcontroladores*, Microtel, Ibarra – Ecuador, 2008.
- **ATMEL** CORPORATION, *8 – Bit AVR Microcontroller with 16 / 32 / 64Kbytes In – System Programmable Flash*, Atmel Corporation, San Jose CA 95131 – USA, 2007.
- **JOHNSON** David, *Análisis Básico de Circuitos Eléctricos*, Quinta Edición, Prentice, 2008.
- **MUHAMMAD** Rashid, *Electrónica de Potencia: Circuitos, Dispositivos y Aplicaciones*, Tercera Edición, Pearson Educación, México, 2007.
- **RAMOS** Guillermo, Electrónica *Digital y Circuitos Integrados*, CEKIT Compañía Editorial Tecnológica, Pereira – Colombia, 2008.

6.2. TESIS

- **HIDALGO** A., *"Implementación de un sistema de autenticación biométrica basado en huellas digitales"*, Proyecto de titulación, Escuela Superior Politécnica de Chimborazo, Riobamba – Ecuador, 2009.
- **BRIONES** O., "*Análisis y Diseño de un sistema que permita controlar el acceso y asistencia del personal para la empresa Tren"*, Proyecto de titulación, Escuela Politécnica Nacional, Quito – Ecuador, 2010.
- **BURGA** A., **PASTRANO** R., *"Diseño e Implementación de un sistema de verificación mediante huella dactilar",* Proyecto de titulación, Escuela Politécnica Nacional, Quito – Ecuador, 2007.

7. ANEXOS

7.1. FIRMWARE DEL MICROCONTROLADOR

```
//////////archivo programa.c/////////
#include "programa_complemento.h"

void main()
{
  char resultado;
  char i,j,k;

  inicia_puertos();//inicialización de puertos e/s
  Delay_ms(500);
  rele=0;//apaga relé
  backlight=1;//enciende retroiluminación
  biometrico=0;//apaga lector biométrico
  Glcd_Init();//inicialización de glcd
  Glcd_Set_Font(FontSystem5x7_v2,5,7,32);//escoge tipo de fuente
  Glcd_Fill(0x00);//limpia pantalla
  mascara();//pantalla principal
  inicia_uart_hw();//inicialización de hardware uart
  inicia_uart_sw();//inicialización de uart por software
  SREG_I_bit=1;//activa permiso global de interrupciones
  muestra_estado();//indica estado de conexión y de apertura de puerta

  while(1)
  {
    if(!boton)
    {
      Delay_ms(50);//delay antirrebotes
```

```
        if(!boton)
        {
          while(!boton);//espera a que se suelte botón
          if(puerta)//si puerta cerrada
          {
            if(lee_biometrico()==1)//entra si se ha leído a un usuario autenticado
            {
              if((usuario_recibido[0]=='0')&&(usuario_recibido[1]=='0')
                &&(usuario_recibido[2]=='0')&&(usuario_recibido[3]=='0'))//verifica si
es usuario master
              {
                borra_texto();
                Glcd_Write_Text("Usuario",0,2,1);
                Glcd_Write_Text("maestro,",0,3,1);
                Glcd_Write_Text("puerta abierta",0,4,1);
                rele=1;//enciende solenoide
                Delay_ms(duracion_apertura);
                rele=0;//apaga solenoide
                borra_texto();
              }
              else//entra aquí si es un usuario normal
              {
                if(conexion==1)//si todavía existe conexión con servidor
                {
                  Delay_ms(2000);//delay para mostrar mensaje anterior
                  UART1_Write('$');//envía trama de datos
                  UART1_Write(usuario_recibido[0]);
                  UART1_Write(usuario_recibido[1]);
                  UART1_Write(usuario_recibido[2]);
                  UART1_Write(usuario_recibido[3]);
```

```
                UART1_Write('&');

                for(i=0;i<espera_rx;i++)//espera dinámica de recepción de datos desde
el servidor
                {
                  Delay_ms(10);
                  if(trama_completa==1)//si se ha recibido respuesta desde el servidor
                  {

                  /////////
                    //while(trama_completa==0);//espera a que llegue una trama
completa, esto es provisional, quitar después
                  /////////

if((dato_bufer[0]=='$')&&(dato_bufer[14]=='$')&&(dato_bufer[28]=='$')&&(dato_b
ufer[30]=='$'))
                    {
                      borra_texto();
                      Glcd_Write_Text("Bienvenid@",0,2,1);

                      k=0;
                      for(j=1;j<=13;j++)//escribe nombre
                      {
                        Glcd_Write_Char(dato_bufer[j],k,3,1);
                        k+=6;
                      }

                      k=0;
                      for(j=15;j<=27;j++)//escribe apellido
                      {
```

```
    Glcd_Write_Char(dato_bufer[j],k,4,1);
    k+=6;
  }

  if(dato_bufer[29]=='A')//acceso permitido
  {
    Glcd_Write_Text("Puerta abierta",0,5,1);
    rele=1;//enciende solenoide
    Delay_ms(duracion_apertura);
    rele=0;//apaga solenoide
    borra_texto();
  }
  else if(dato_bufer[29]=='B')//acceso no permitido
  {
    Glcd_Write_Text("Horario no",0,5,1);
    Glcd_Write_Text("permitido",0,6,1);
    Delay_ms(2000);
    borra_texto();
  }
}
else
{
  borra_texto();
  Glcd_Write_Text("Error,",0,2,1);
  Glcd_Write_Text("mensaje no",0,3,1);
  Glcd_Write_Text("comprendido",0,4,1);
  Delay_ms(2000);
  borra_texto();
}
trama_completa=0;//encera bandera
```

```
                for(j=0;j<=30;j++)
                {
                  dato_bufer[j]=' ';//encera búfer de procesamiento
                }
                goto fin_proceso;
              }
            }
            //aquí, se terminó el tiempo de espera y no se recibió respuesta desde
el servidor
            borra_texto();
            Glcd_Write_Text("Error,",0,2,1);
            Glcd_Write_Text("no existe",0,3,1);
            Glcd_Write_Text("respuesta",0,4,1);
            Glcd_Write_Text("desde servidor",0,5,1);
            for(j=0;j<=30;j++)
            {
              dato_bufer[j]=' ';//encera búfer de procesamiento
            }
            trama_completa=0;//encera bandera
            Delay_ms(2000);
            borra_texto();
          }
          else//si no existe conexión inalámbrica con servidor
          {
            Delay_ms(2000);//delay para mostrar mensaje anterior
            borra_texto();
            Glcd_Write_Text("Error,",0,2,1);
            Glcd_Write_Text("verifique",0,3,1);
            Glcd_Write_Text("conexion con",0,4,1);
```

```
                Glcd_Write_Text("servidor",0,5,1);
                Delay_ms(2000);
                borra_texto();
              }
            }
          }
          else//aquí, lectura errónea o usuario no autenticado
          {
            Delay_ms(2000);//delay para indicar texto indicado en la subrutina de
lectura del biomético
            borra_texto();
          }
        }
        else//si puerta abierta
        {
          Glcd_Write_Text("Puerta abierta",0,2,1);
          Glcd_Write_Text("previamente",0,3,1);
          Delay_ms(2000);
          borra_texto();
        }

        fin_proceso:
          asm{nop;}
      }
    }
    muestra_estado();//indica estado de conexión y de apertura de puerta
  }
}
```

```
//////////archivo programa_complemento.h/////////

//definiciones para uart
#define RXB8 1
#define TXB8 0
#define UPE 2
#define OVR 3
#define FE 4
#define UDRE 5
#define RXC 7

#define FRAMING_ERROR (1<<FE)
#define PARITY_ERROR (1<<UPE)
#define DATA_OVERRUN (1<<OVR)
#define DATA_REGISTER_EMPTY (1<<UDRE)
#define RX_COMPLETE (1<<RXC)

const code char pantalla_bmp[1024];

const unsigned long duracion_apertura=2000;//2 segundos de duración de apertura de puerta
const char espera_rx=200;//200*10ms=2seg. de espera a recibir datos desde el servidor

//conexiones del módulo glcd
char GLCD_DataPort at PORTB;
char GLCD_DataPort_Direction at DDRB;
```

```
char error;
char usuario_recibido[4];
char conexion=0;
char contador_conexion=0;
char contador_dato=0;
char trama_completa=0;
char conexion_anterior=0;
char puerta_anterior=0;
char primera_lectura=1;//indica que es la primera vez que se lee estado de
conexión y estado de puerta

char dato_bufer[50];//bufer de datos para procesamiento de trama recibida
char dato_recibe[50];//bufer de datos para recepción de trama por interrupción

char
trama_inicializacion[25]={0x7E,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x0
0,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01};
char
trama_identificacion[25]={0x7E,0x00,0x00,0x00,0x12,0x00,0x00,0x00,0x00,0x00,0x
00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x12};
char trama_recibida[40];
sbit GLCD_RS  at PORTD2_bit;
sbit GLCD_RW  at PORTD3_bit;
sbit GLCD_EN  at PORTD4_bit;
sbit GLCD_CS2 at PORTD5_bit;
sbit GLCD_CS1 at PORTD6_bit;
sbit GLCD_RST at PORTD7_bit;

sbit GLCD_RS_Direction  at DDD2_bit;
sbit GLCD_RW_Direction  at DDD3_bit;
```

```
sbit GLCD_EN_Direction  at DDD4_bit;
sbit GLCD_CS2_Direction at DDD5_bit;
sbit GLCD_CS1_Direction at DDD6_bit;
sbit GLCD_RST_Direction at DDD7_bit;

sbit backlight at PORTC0_bit;
sbit rele at PORTC1_bit;
sbit biometrico at PORTC2_bit;
sbit boton at PINA0_bit;
sbit puerta at PINA1_bit;

void recibe_dato()
{
  char dato_recibido,estado,j;
  SREG_I_bit=0;//deshabilita interrupciones

  estado=UCSR0A;
  dato_recibido=UDR0;

  if((estado&(FRAMING_ERROR|PARITY_ERROR|DATA_OVERRUN))==0)
  {
    if(conexion==0)//si está desconectado el puerto ip, espera el mensaje "%*#"
    {

if((dato_recibido=='%')||(dato_recibido=='*')||(dato_recibido=='#')||(dato_recibid
o=='/'))
      {
        switch(contador_conexion)
        {
          case 0:
```

```
  if(dato_recibido=='%')
  {
    contador_conexion++;
  }
  else
  {
    contador_conexion=0;
  }
  break;
case 1:
  if(dato_recibido=='*')
  {
    contador_conexion++;
  }
  else
  {
    contador_conexion=0;
  }
  break;
case 2:
  if(dato_recibido=='#')
  {
    contador_conexion++;
  }
  else
  {
    contador_conexion=0;
  }
  break;
default:
```

```
            contador_conexion=0;
            break;
          }
          if(contador_conexion==3)
          {
            conexion=1;
            contador_conexion=0;
          }
        }
        else
        {
          contador_conexion=0;
        }
      }
      else if(conexion==1)//si está conectado el puerto ip, espera el mensaje "%/#"
      {

if((dato_recibido=='%')||(dato_recibido=='/')||(dato_recibido=='#')||(dato_recibid
o=='*'))
        {
          switch(contador_conexion)
          {
            case 0:
              if(dato_recibido=='%')
              {
                contador_conexion++;
              }
              else
              {
                contador_conexion=0;
```

```
    }
    break;
  case 1:
    if(dato_recibido=='/')
    {
      contador_conexion++;
    }
    else
    {
      contador_conexion=0;
    }
    break;
  case 2:
    if(dato_recibido=='#')
    {
      contador_conexion++;
    }
    else
    {
      contador_conexion=0;
    }
    break;
  default:
    contador_conexion=0;
    break;
}
if(contador_conexion==3)
{
  conexion=0;
  contador_conexion=0;
```

```
        }
      }
      else
      {
        contador_conexion=0;
        if(dato_recibido=='&')//fin de trama recibido
        {
          for(j=0;j<=contador_dato;j++)
          {
            dato_bufer[j]=dato_recibe[j];
            dato_recibe[j]=' ';//encera búfer de recepción
          }
          trama_completa=1;
          contador_dato=0;
        }
        else
        {
          dato_recibe[contador_dato]=dato_recibido;//lee el buffer y almacena en
dato
          contador_dato++;
          if(contador_dato>49)
          {
            contador_dato=0;
          }
        }
      }
    }
  }
  SREG_I_bit=1;//habilita interrupciones
}
```

```
void inter_recep_uart()//rutina especial de interrupción ante recepción uart
org IVT_ADDR_USART0__RX
{
  recibe_dato();
}

void inter_timer1_ovf()
org IVT_ADDR_TIMER1_OVF
{
  backlight=0;//apaga backlight
  TOIE1_bit=0;//deshabilita interrupción por desbordamiento de timer1
}

void inicia_puertos()
{
  DDC0_bit=1;//salida para backlight
  DDC1_bit=1;//salida para control de relé
  DDC2_bit=1;//salida para encendido de biométrico

  DDA0_bit=0;//entrada para lectura de botón
  PORTA0_bit=1;//pullup activada
  DDA1_bit=0;//entrada para lectura de estado de puerta
  PORTA1_bit=1;//pullup activada
}

void muestra_estado()
{
  if(primera_lectura)
  {
```

```
  if(conexion)
  {
    Glcd_Write_Text("OK",103,3,1);
  }
  else
  {
    Glcd_Write_Text("NO",103,3,1);
  }
  conexion_anterior=conexion;

  Glcd_Set_Font(System3x5,3,5,32);//cambia tipo de letra
  if(puerta)
  {
    Glcd_Write_Text("CERRADA",95,6,1);
    UART1_Write_Text("$CCCC&");
  }
  else
  {
    Glcd_Write_Text("ABIERTA",95,6,1);
    UART1_Write_Text("$AAAA&");
  }
  Glcd_Set_Font(FontSystem5x7_v2,5,7,32);//regresa tipo de fuente anterior
  puerta_anterior=puerta;
  primera_lectura=0;//desactiva bandera de primera lectura
}
else
{
  if(conexion!=conexion_anterior)
  {
    if(conexion)
```

```
      {
        Glcd_Write_Text("OK",103,3,1);
      }
      else
      {
        Glcd_Write_Text("NO",103,3,1);
      }
      conexion_anterior=conexion;
    }

    if(puerta!=puerta_anterior)
    {
      Glcd_Set_Font(System3x5,3,5,32);//cambia tipo de letra
      if(puerta)
      {
        Glcd_Write_Text("CERRADA",95,6,1);
        UART1_Write_Text("$CCCC&");
      }
      else
      {
        Glcd_Write_Text("ABIERTA",95,6,1);
        UART1_Write_Text("$AAAA&");
      }
      Glcd_Set_Font(FontSystem5x7_v2,5,7,32);//regresa tipo de fuente anterior
      puerta_anterior=puerta;
    }
  }
}

void mascara()
```

```
{
  Glcd_Image(pantalla_bmp);
}

void borra_texto()
{
  Glcd_Write_Text("          ",0,2,1);//borra todos los mensajes
  Glcd_Write_Text("          ",0,3,1);
  Glcd_Write_Text("          ",0,4,1);
  Glcd_Write_Text("          ",0,5,1);
  Glcd_Write_Text("          ",0,6,1);
  Glcd_Write_Text("          ",0,7,1);
}

void inicia_uart_hw()
{
  UART1_Init(9600);//inicializa módulo uart a 9600bps
  Delay_ms(100);//delay para estabilización del módulo uart
  RXCIE0_bit=1;//activa interrupción ante recepción de datos
}

void inicia_uart_sw()
{
  Soft_UART_Init(&PORTC,7,6,9600,0);//9600bps,rx-->rc7
}                                   //tx-->rc6

void activa_timer1()
{
  //inicialización de timer1 como temporizador
  TCCR1A=0x00;
```

```
  TCCR1B=0x05;//preescaler 1024
  TCNT1H=0x00;
  TCNT1L=0x00;
  ICR1H=0x00;
  ICR1L=0x00;
  OCR1AH=0x00;
  OCR1AL=0x00;
  OCR1BH=0x00;
  OCR1BL=0x00;

  TOIE1_bit=1;//habilita interrupción por desbordamiento de timer1
  //desbordamiento=Tosc*(65536-TCNT0)*preescala
  //desbordamiento=(1/8Mhz)*65536*1024=8.388seg
}

void desactiva_timer1()
{
  TOIE1_bit=0;//deshabilita interrupción por desbordamiento de timer1
  TCCR1A=0x00;
  TCCR1B=0x00;
  TCNT1H=0x00;
  TCNT1L=0x00;
}

char lee_biometrico()
{
  char i;
  char usuario_ok=0;

  biometrico=1;//enciende biométrico
```

```
SREG_I_bit=0;//apaga interrupciones

Glcd_Write_Text("Iniciando",0,2,1);
Glcd_Write_Text("lector",0,3,1);

Delay_ms(500);//estabilización del lector

for(i=0;i<25;i++)//envía trama de inicialización
{
  Soft_UART_Write(trama_inicializacion[i]);
}

for(i=0;i<25;i++)//recibe trama de respuesta
{
  trama_recibida[i]=Soft_UART_Read(&error);//si no hay respuesta, el programa
}                                  //se quedará estancado aquí

if(trama_recibida[8]==0x01)
{
  Glcd_Write_Text("Ok",48,3,1);
}
else
{
  Glcd_Write_Text("Error,",48,3,1);
  Glcd_Write_Text("verifique",0,5,1);
  Glcd_Write_Text("conexion del",0,6,1);
  Glcd_Write_Text("lector",0,7,1);
  usuario_ok=0;
  goto salir;
}
```

```
Glcd_Write_Text("Empezando",0,5,1);
Glcd_Write_Text("autenticacion",0,6,1);
Glcd_Write_Text("en  seg.",0,7,1);

for(i=3;i>0;i--)//escribe cuenta regresiva en glcd
{
  Glcd_Write_Char(i+0x30,16,7,1);
  Delay_ms(1000);
}

borra_texto();

for(i=0;i<25;i++)//envía trama de identificación
{
  Soft_UART_Write(trama_identificacion[i]);
}

for(i=0;i<25;i++)//recibe los primeros 25 caracteres de la trama de respuesta
{
  trama_recibida[i]=Soft_UART_Read(&error);//si no hay respuesta, el programa
}                                  //se quedará estancado aquí

if(trama_recibida[16]!=0)//entra aquí si se ha leído a un usuario autenticado
{                    //aquí la trama tendrá 39 caracteres
  for(i=25;i<39;i++)//recibe el resto de la trama
  {
    trama_recibida[i]=Soft_UART_Read(&error);//si no hay respuesta, el programa
  }                                  //se quedará estancado aquí
}
```

```
  if(trama_recibida[8]==0x01)//usuario registrado
  {
    usuario_recibido[0]=trama_recibida[25];//guarda identificación del usuario
recibido
    usuario_recibido[1]=trama_recibida[26];//en registros de trabajo
    usuario_recibido[2]=trama_recibida[27];//guarda identificación del usuario
recibido
    usuario_recibido[3]=trama_recibida[28];//en registros de trabajo

    Glcd_Write_Text("Usuario",0,2,1);
    Glcd_Write_Text("registrado,",0,3,1);
    Glcd_Write_Text("verificando en",0,4,1);
    Glcd_Write_Text("base de datos",0,5,1);
    usuario_ok=1;
  }
  else if(trama_recibida[8]==0x02)//usuario no registrado
  {
    Glcd_Write_Text("Usuario no",0,2,1);
    Glcd_Write_Text("registrado",0,3,1);
    usuario_ok=0;
  }
  else if(trama_recibida[8]==0x07)//error en la lectura
  {
    Glcd_Write_Text("Error de",0,2,1);
    Glcd_Write_Text("lectura,",0,3,1);
    Glcd_Write_Text("intente",0,4,1);
    Glcd_Write_Text("nuevamente",0,5,1);
    usuario_ok=0;
  }
```

```
  else
  {
    Glcd_Write_Text("Error",0,2,1);
    Glcd_Write_Text("desconocido",0,3,1);
    usuario_ok=0;
  }
salir:
  biometrico=0;//apaga biométrico
  SREG_I_bit=1;//enciende interrupciones
  return usuario_ok;
}
```

```
//////////archivo bitmap.c/////////

// -----------------------------------------------------
// GLCD Picture name: pantalla.bmp
// GLCD Model: KS0108 128x64
// -----------------------------------------------------

unsigned char const pantalla_bmp[1024] = {
 126,255,255,255,255,211,181,181,173,203,255,133,255,183,171,219,
 255,251,129,187,255,199,171,167,255,131,251,131,251,135,255,155,
 171,171,199,255,255,255,255,129,187,187,199,255,133,255,199,187,
 187,199,255,131,251,131,251,135,255,199,170,166,255,251,129,187,
 255,131,251,255,133,255,199,187,187,215,255,199,187,187,199,255,
 255,255,255,199,187,187,129,255,199,171,167,255,255,255,255,155,
 171,171,199,255,199,187,187,215,255,199,187,187,215,255,199,171,
 167,255,183,171,219,255,199,187,187,199,255,255,255,255,255,126,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,252,254,254,254,254, 14,246,246,
 254, 62,222, 30,254, 30,222, 62,254, 62, 94, 30,254,158,126,158,
 254, 22,254, 62,214, 22,254, 30,222, 62,254,254,254,254,254,252,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
   0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,
```

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,255, 15, 15, 15, 15, 14, 13, 13,
15, 12, 13, 14, 15, 12, 15, 12, 15, 14, 13, 13, 15, 12, 15, 12,
15, 12, 15, 12, 13, 14, 15, 12, 15, 12, 15, 15, 15, 15, 15,255,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,255, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,255,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,241,251,250,250,250,250,250,250,
250,250, 58,186,122,250,250,250,250,250,250,250,250,250,250,250,
186, 26,186,250,250,250,250,250,250,250,250,250,250,251,241,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,255,127,127,127,127,127,127,127,
127,127, 96,123,124,127,112,111, 96,127,113,106,104,127, 96,126,
127, 96,127,102,106, 96,127,127,127,127,127,127,127,127,127,255,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

```
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0,255, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,255,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 7, 12, 8, 8, 8, 8, 8, 8,
  8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8,
  8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 12, 7
};
```

7.2. MODULO WIFLY

ROVING NETWORKS
WIRELESS FOR LESS

RN-111B

www.rovingnetworks.com

DS-RN111B_V1 4/20/2009

"WiFly" 802.11B Module

Features

- Ultra-low power module with 40mA average RX, 120ma TX burst current usage.
- Embedded stacks with TCP/UDP/IP, sockets, no host or processor stacks required.
- ICMP, Telnet, TFTP, DHCP, FTP, UDP Time server clients.
- Flash memory for user code, API for user applications.
- FTP client "over the air" firmware upgrade.
- Simple ACSII command interface, over local UART and remote from TCP/IP client.
- Sustained data rates (each direction) of >200 kbps.
- Security: WEP128, WPA-PSK, and WPA2-PSK (TKIP and AES) supported.
- Real-time clock for datalogging/timestamping.
- Up to 500Kbytes of Flash memory storage for data logs.
- World wide approvals/certifications (FCC, IC, CE).
- RoHS compliant

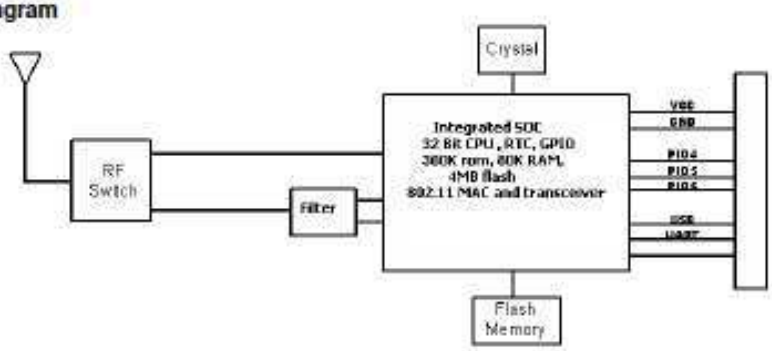
Applications

- Wireless thermostats
- RS232/RS485 cable replacement
- Remote equipment monitoring
- Scanners, GPS and measurement systems
- Industrial sensor and control

Description

The WiFly module is a stand alone, embedded 802.11b device. Because of its small form factor and extremely low power consumption, the RN-111B is perfect for mobile wireless applications such as asset monitoring, GPS tracking and portable devices. The Wifly modules include an on board TCP/IP stack and networking application programs such as telnet and ftp. The hardware requires only four connections (PWR, TX, RX, GND) to create a simple wireless data connection. The WiFly module is programmed via a straight forward ASCI command. Once is setup it can automatically associated and authenticate with a network, connect to remote hosts, and reliably transmit data, making your application accessible worldwide.

Block Diagram



ROVING networks
WIRELESS FOR LESS

RN-111B

www.rovingnetworks.com DS-RN111B_V1 4/20/2009

Overview

- Accepts Wide range DC power input , (3.0V - to 16Vdc). Can power from single battery cell.
- 801.11b compliant radio. CHIP ANT, U.FL, SMA options.
- UART Serial Port TTL level, speeds: 1200bps up to 921Kbps, even,odd parity.
- SPI port available.
- Low power consumption (<120mA transmitting., 40mA idle mode)
- Ultra low power (~12ua) sleep mode with "instant on" (30ms) wakeup and attach.
- Wake on programmable timer, wake on UART receive character settings.
- Small-form factor 32 Pin DIP radio modem package (2mm pitch X 0.90" socket width)
- 6 General Purpose Input/Output Pins (4ma source/sink) controlled via remote commands.
- 8 sensor inputs (0 – 1.2VDC)

Environmental Conditions

Parameter	Value
Temperature Range (Operating)	-40 °C - +85 °C
Temperature Range (Storage)	-40 °C - +85 °C
Relative Humidity (Operating)	≤90%
Relative Humidity (Storage)	≤90%

Electrical Characteristics

Parameter	Min	Typ.	Max.	Unit
Supply Voltage VIN	4.0	5.0	12	VDC
Supply Voltage VDD	3.0	3.3	3.6	VDC
Supply Voltage (VBATT option)	2.0	3.0	3.3	VDC
Average power consumption				
Standby/Idle (default settings)	-	35	-	mA
Sleep	10	12	15	uA (micro)
Connected(idle, RX)		40		mA
Connected(TX)		110	180	mA

The power management unit turns off unused functions and switches between sleep and active modes. In sleep mode the real-time clock and sensor interface remain active, enabling the WiFly to wake up at any interval or when a specific condition is detected. This "instant-on" capability allows mobile devices to remain in low-power sleep mode until it is ready to transfer data. **The WiFly module can wake up, join a network, transmit data and go back to sleep in under 100 msec**.

This unique combination of low latency and low power makes it possible to run for over two years transmitting data every 5 minutes using just two standard AAA Alkaline batteries!

Radio Characteristics

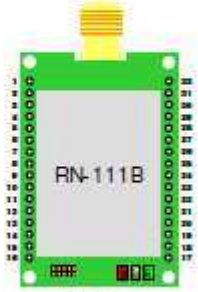
Parameter	Specifications
Frequency	2402 ~ 2480MHz
Modulation	DSSS(CCK-11, CCK-5.5, DQPSK-2, DBPSK-1)
Channel intervals	5MHz
Channels	1 - 14
Transmission rate (over the air)	11/5.5/2/1Mbit
Receive sensitivity	-82 to -93dBm
Output level (Class1)	12dBm max.

Antenna configurations

Part Number	Description	Picture
RN-111B-R	Ultra low power WiFly GX module with RP-SMA connector	
RN-111B-S	Ultra low power WiFly GX module with on board ceramic antenna	
RN-111B-E	Ultra low power WiFly GX module with SMA connector	
RN-111B-W	Ultra low power WiFly GX module with simple wire antenna	

Pin Description

Note: Any unused pins should be left floating (No Connect)



Top view

Pin	Name	Description	Default
1	PIO7	General Purpose IO	No Connect
2	VDD_SW	Switched sensor output power	No Connect
3	SENSE-5	Analog sensor input (1.2V)	
4	SENSE-6	Analog sensor input (1.2V)	
5	SENSE-7	Analog Sensor Input (1.2V)	
6	SENSE-8	Analog Sensor Input (1.2V)	
7	PIO6	Controls red LED	Input
8	PIO9	General purpose IO	Sets factory defaults
9	DEBUG_TX	2nd serial port	No Connect
10	DEBUG_RX	2nd serial port	No Connect
11	RESET	Active low with 10k built in pullup	
12	SHUTDOWN		No Connect
13	VIN	3.6-16VDC	
14	VREG	3.3V LDO output	
15	VBATT	Tie to VREG if USING VIN	Battery option
16	GND		
17	VDD	3.3V out-in	Power input
18	SP_MO	Spi port	No Connect
19	SP_CK	Spi port	No Connect
20	SP_CS	Spi port	No Connect
21	SP_MI	Spi port	No Connect
22	PIO5	Controls yellow LED	Connect/disconnect input
23	PIO4	Controls GREEN LED	Connection status output
24	RTS-PIO3	HW flow control output	TTL output
25	CTS-PIO2	Also can be used as PIO3	TTL input
26	RX	TTL Data IN	Input
27	TX	TTL Data Out	output
28	SENSE-4	Analog Sensor Input (1.2V)	Wake up GPIO
29	SENSE-3	Analog Sensor Input (1.2V)	Wake up GPIO
30	SENSE-2	Analog Sensor Input (1.2V)	Wake up GPIO
31	SENSE-1	Analog sensor input (3.3V tolerant)	Wake UP GPIO
32	GND		

7.3. DATASHEET DE FIM30N

1. General Descriptions

FIM30N is a low-price stand-alone Fingerprint Identification Device with many excellent features. It provides benefits such as high identification performance, low power consumption and RS-232 serial interface with the various commands for easy integration into a wide range of applications. It is a durable and compact device with fingerprint identification module containing NITGEN's optics-based fingerprint sensor inside.

2. Target Application

Door-lock system
Safe Box
Simple Access Controller
Vehicle Control
ATM , POS
And more

3. Basic Feature

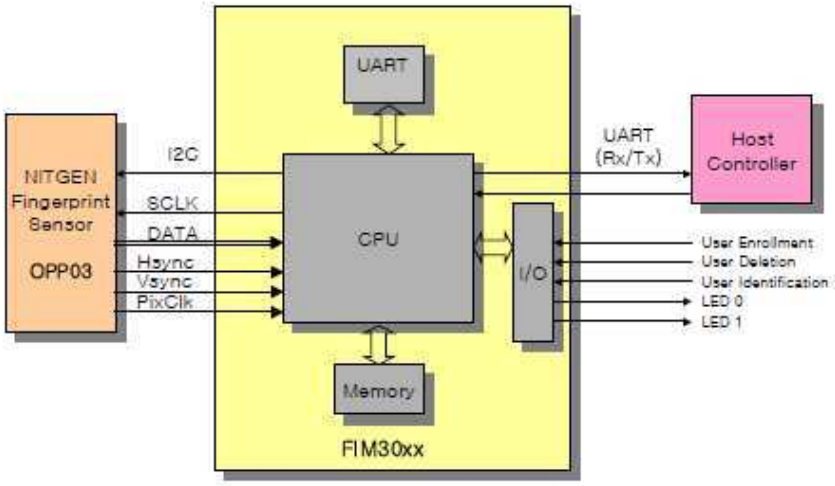
Hardware Specification

ITEM		FIM3030-LV	FIM3030-HV
Board Spec.	CPU	ADSP-BF531	
	DRAM	8Mbyte SDRAM	
	Flash ROM	1Mbytes	
Dimension		43 x 60 [mm^2]	
Sensor		NITGEN OPP03	
Supply Voltage		3.3 ± 0.3 [V]	5.0± 0.5 [V]
Current Consumption		(Idle) 55 ~ (Op.) 210 [mA]	(Idle) 55 ~ (Op.) 210 [mA]
Operating Temperature		-20 ~ 60 [℃]	
Humidity		90 [% RH]	
ESD Tolerance		±8 [KV] (indirect)	
Communication Channel		RS-232 Speed: 9600 ~ 115200 [bps]	
External I/O		3 Key Input 2 Result Output	

Operation Specification

ITEM	FIM3030-LV/HV
Capture Speed	0.2(normal) / 0.7(secure) sec
Verification Speed (Normal Mode)	1.0 [sec] (Capture + Extract + Match)
Boot Up Time	Max. 0.5 [sec]
Data Encryption Method	AES for saving data

4. Block Diagram



RS-232C communication data consist of 8-bit data, no parity, 1-bit start-bit and 1-bit stop-bit.

5. Operation

Communication

FIM30N has RS-232 serial communication port through that FIM30N communicates at the same time. These ports support 6 baudrate modes such as 9600, 14400, 19200, 38400, 57600, and 115200 bps.

FIM30N follows NITGEN Serial Communication protocol. For more detail information refer to the document "NITGEN_ComProtocl.pdf".

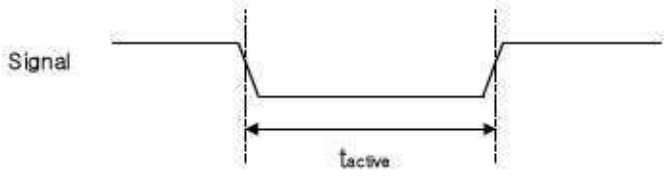
User Data Area

FIM30N provides 64 Kbytes flash memory. Using this memory, host can save private data for specific usage. The caution is needed because the responsibility for reading, writing and erasing user data area is given to the host.

Key Function

FIM30N supports 3 function key inputs such as Enroll_Key, Delete_Key, and Identify_Key. Using these keys without serial communication, enrollment, deletion, all deletion and identification operating can be executed.

The following timing diagram and table show the operation condition of keys.



7.4. DATASHEET DE ATMEGA 644P

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
- Nonvolatile Program and Data Memories
  - 16/32/64K Bytes of In-System Self-Programmable Flash
    Endurance: 10,000 Write/Erase Cycles
  - Optional Boot Code Section with Independent Lock Bits
    In-System Programming by On-chip Boot Program
    True Read-While-Write Operation
  - 512B/1K/2K Bytes EEPROM
    Endurance: 100,000 Write/Erase Cycles
  - 1/2/4K Bytes Internal SRAM
  - 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: 338/398/TBD µA
  - Power-down Mode:0.035 /0.027/TBD µA
  - Power-save Mode:0.5 /0.5/TBD µA (Including 32 kHz RTC)

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

ATmega164P/V
ATmega324P/V
ATmega644P/V

Advance Information

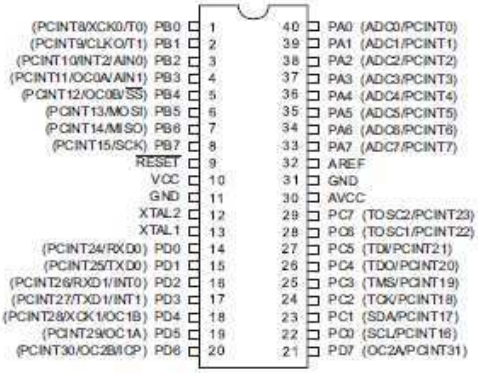
Summary

8011DS–AVR–02/07

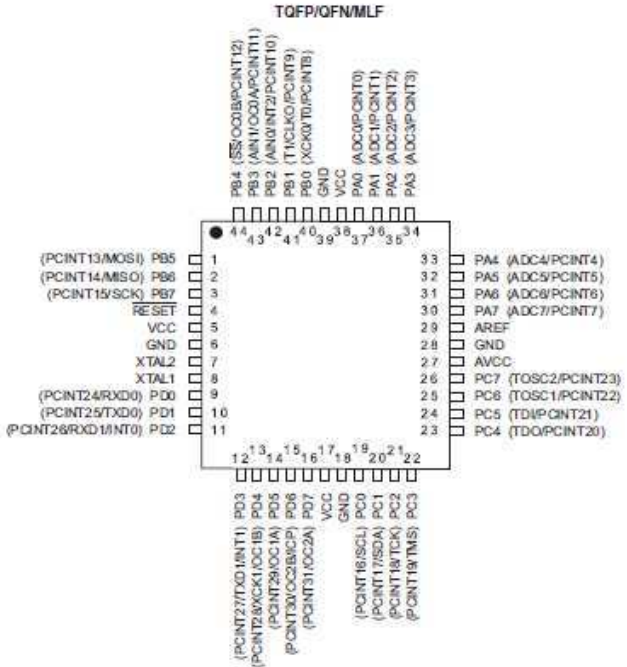
1. Pin Configurations

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

PDIP



TQFP/QFN/MLF



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

1.1 Disclaimer

Typical values contained in this datasheet are based on simulations and characterization of other AVR microcontrollers manufactured on the same process technology. Min and Max values will be available after the device is characterized.

7.5. DATASHEET DE GLCD

1. Features

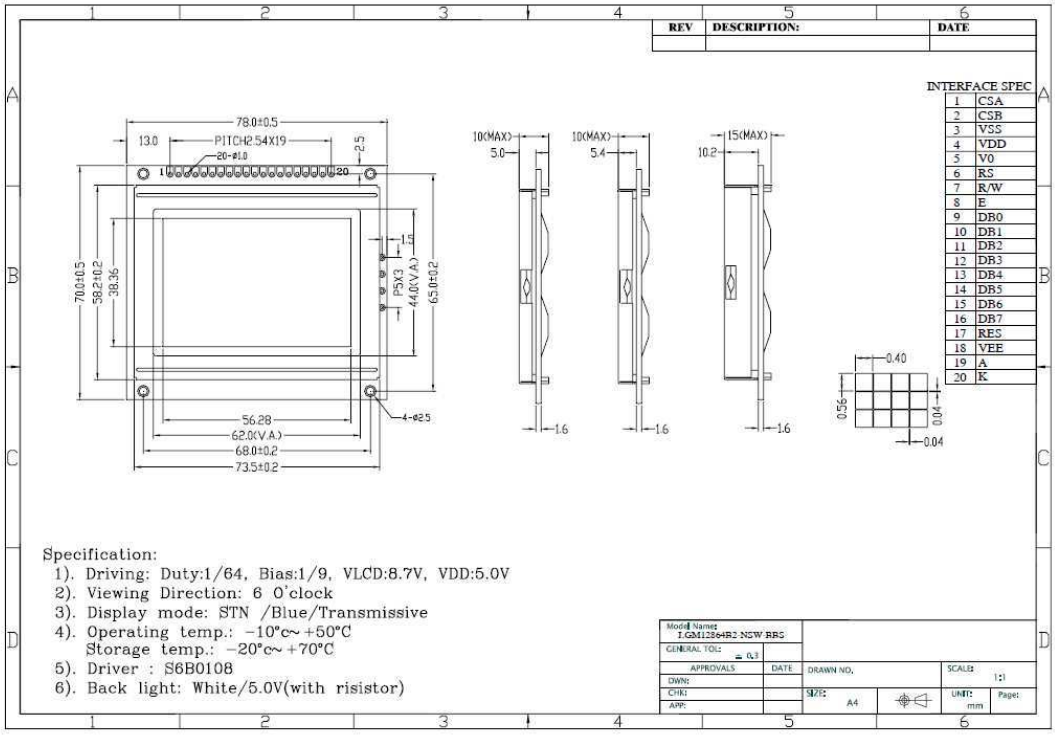
1. 128X64 dots
2. Built-in controller (S6B0108)
3. +5.0V power supply
4. 1/64 duty cycle;1/9bias
5. BKL to be driven by pin19, pin20.

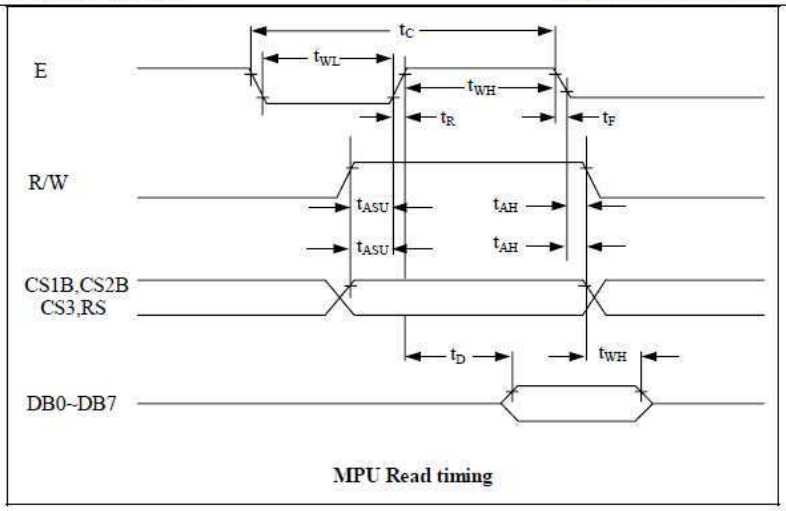
LCD type	☐FSTN positive		☐FSTN Negative	
	☐STN Yellow Green	☐STN Gray		☑STN-Blue
View direction	☑6 O'clock	☐12 O'clock		
Rear Polarizer	☐Reflective	☐Transflective		☑Transmissive
Backlight Type	VLED	☐EL	☐Internal Power	☐4.2V input
		☐CCFL	☑External Power	☐3.3 input
Backlight Color	☑White	☐Amber	☐Blue-Green	☐Yellow-Green
Temperature Range	☐Normal	☑Wide		☐Super Wide
DC to DC circuit	☑Build-in		☐Not Build-in	
EI Driver IC	☐Build-in		☑Not Build-in	
Touch screen	☐With		☑Without	
Font type	☐English-Japanese	☐English-Europen	☐English-Russian	☐other

1. MECHANICAL SPECIFICATIONS

Module size	78.0mm(L)*70.0mm(W)* Max14(H)mm
Viewing area	62.0mm(L)*44.0mm(W)
Dots size	0.40mm(L)*0.56mm(W)
Dots pitch	0.44mm(L)*0.60mm(W)
Weight	Approx. 80g

2. Outline dimension





MPU Read timing

7. OPERATING PRINCIPLES & METHODS

1. **I/O Buffer**
   Input buffer controls the status between the enable and disable of chip. Unless the CS1B to CS3 is in active mode, Input or output of data and instruction does not execute. Therefore internal state is not change. But RSTB and ADC can operate regardless CSIB-CS3.

2. **Input register**
   Input register is provided to interface with MPU which is different operating frequency. Input register stores the data temporarily before writing it into display RAM.
   When CS1B to CS3 are in the active mode, R/W and RS select the input register. The data from MPU is written into input register. Then writing it into display RAM. Data latched for falling of the E signal and write automatically into the display data RAM by internal operation.

3. **Output register**
   Output register stores the data temporarily from display data RAM when CS1B, CS2B and CS3 are in active mode and R/W and RS=H, stored data in display data RAM is latched in output register. When CS1B to CS3 is in active mode and R/W=H , RS=L, status data (busy check) can read out.
   To read the contents of display data RAM, twice access of read instruction is needed. In first access, data in display data RAM is latched into output register. In second access, MPU can read data which is latched. That is to read the data in display data RAM, it needs dummy read. But status read is not needed dummy read.

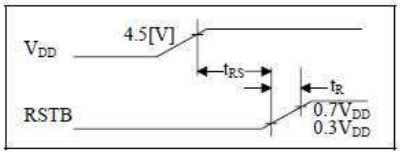
RS	R/W	Function
L	L	Instruction
	H	Status read (busy check)
H	L	Data write (from input register to display data RAM)
	H	Data read (from display data RAM to output register)

4. **Reset**
   The system can be initialized by setting RSTB terminal at low level when turning power on, receiving

instruction from MPU. When RSTB becomes low, following procedure is occurred.
1. Display off
2. Display start line register become set by 0.(Z-address 0)
While RSTB is low, No instruction except status read can by accepted. Therefore, execute other instructions after making sure that DB4= (clear RSTB) and DB7=0 (ready) by status read instruction.
The conditions of power supply at initial power up are shown in table 1.

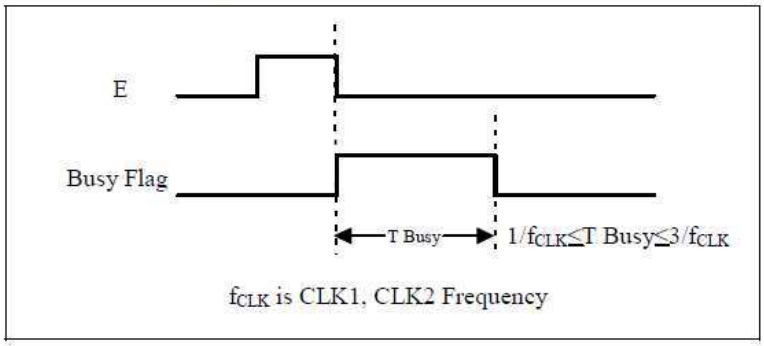
Table 1. Power Supply Initial Conditions

Item	Symbol	Min	Typ	Max	Unit
Reset Time	t_{RS}	1.0	-	-	us
Rise Time	t_R	-	-	200	ns



5. **Busy flag**

Busy flag indicates that S6B0108 is operating or no operating. When busy flag is high, S6B0108 is in internal operating .
When busy flag is low, S6B0108 can accept the data or instruction.
DB7indicates busy flag of the S6B0108.



6. **Display On/Off Flip-Flop**

The display on/off flip-flop makes on/off the liquid crystal display. When flip-flop is reset (logical low), selective voltage or non selective voltage appears on segment output terminals. When flip-flop is set (logic high), non selective voltage appears on segment output terminals regardless of display RAM data. The display on/off flip-flop can changes status by instruction. The display data at all segment disappear while RSTB is low.
The status of the flip-flop is output to DB5 by status read instruction.
The display on/off flip-flop synchronized by CL signal.

7. **X Page Register**

X page register designates pages of the internal display data RAM.
Count function is not available. An address is set by instruction.

8. **Y address counter**

UNIVERSIDAD TÉCNICA DEL NORTE

7.6. MANUAL DE USUARIO

SISTEMA ELÉCTRONICO PARA CONTROL DE ACCESO DE PERSONAS POR RECONOCIMIENTO DE HUELLA DACTILAR, CON AUTENTICACIÓN REMOTA EN BASE DE DATOS A TRAVÉS DE UNA WLA.

Desarrollada por: Estefanía Torres A.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

El presente manual de usuario brinda información básica necesaria para gestionar el Sistema Electrónico para control de acceso de personas por reconocimiento de huella dactilar, con autenticación remota en base de datos a través de una WLAN implementada en el entorno de la Hostal las Garzas.

A través de esta guía, se exponen las características y funciones de las interfaces y base de datos configuradas. Además, se detalla el proceso para la correcta administración del sistema.

2. VISIÓN GENERAL

2.1. ACCESS POINT

Para ingresar a la interfaz gráfica utilizada para la configuración del punto de acceso se introduce la dirección https://192.168.0.50 en la barra de navegación de un explorador Web.

El punto de acceso AP, de este dispositivo tiene un módulo de configuración gráfico (WIZARD) que permite ponerlo a funcionar fácilmente y en pocos instantes.

La siguiente imagen indica la interfaz gráfica utilizada para la configuración del AP, así como los datos ingresados en ella.

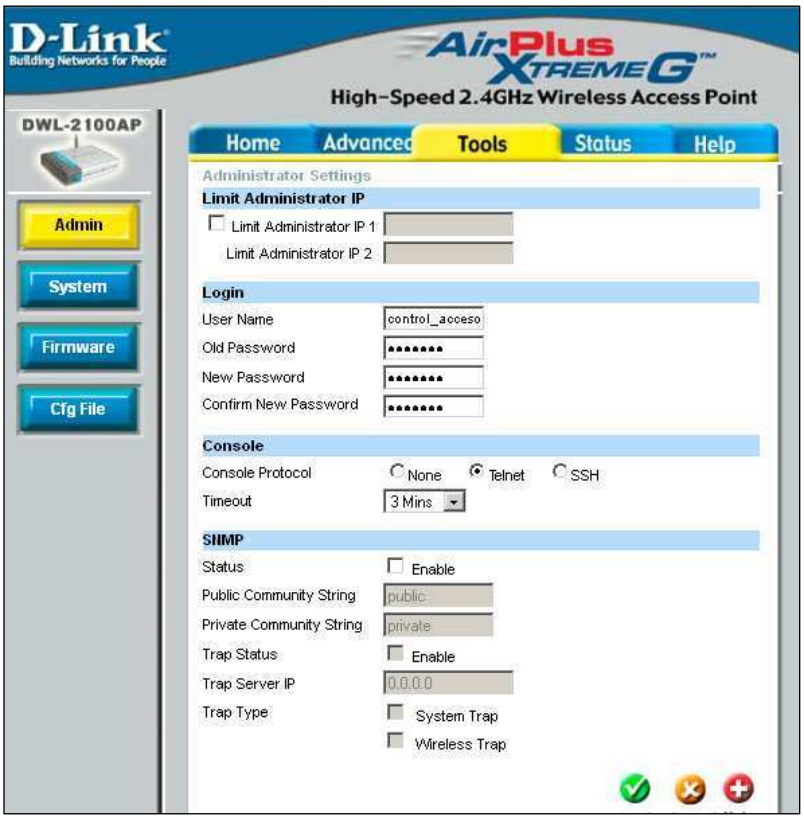


Figura 1: Interfaz gráfica de configuración del AP

En la tabla 1 se indica los parámetros básicos configurados en él.

Tabla 1: Resumen de configuración del AP

ELEMENTO	CONFIGURACIÓN
ACCESS POINT	MODO DE TRABAJO: AP DIRECCIÓN IP: 192.168.0.50 SEGURIDAD: ABIERTO SSID: control_acceso CANAL: 6 (2.437GHZ) DHCP: NO (IP ESTÁTICA) MÁSCARA DE SUBRED: 255.255.255.0

3. SOFTWARE DE CONFIGURACIÓN DEL LECTOR BIOMÉTRICO

3.1. Para configurar el hardware del lector biométrico de ingreso de nuevos usuarios se utiliza el software EVTOOLS de NITGEN. Inicialmente, se encuentra en el escritorio, para dar acceso al software, hacer clic en el icono, donde se visualiza la siguiente pantalla que se observa en la Figura 1, este programa mantiene una comunicación serial con el lector biométrico y permite identificar, agregar y borrar las huellas dactilares.

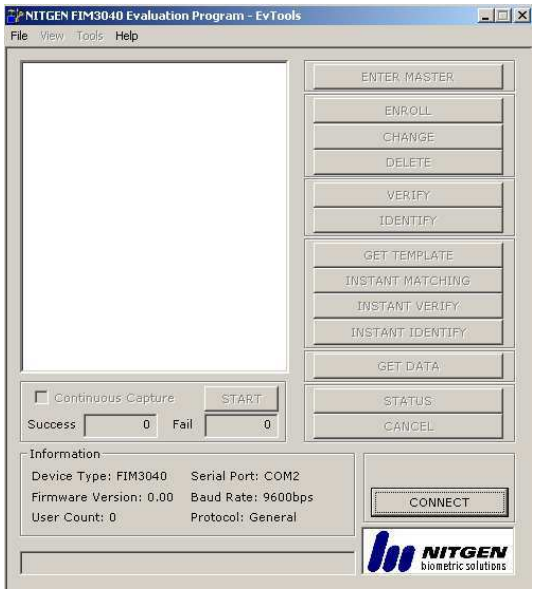


Figura 2: Software EVTOOLS de NITGEN

Para configurar el lector biométrico se lo debe conectar cable serial y la interfaz a la PC como se indica en la figura 3.

Figura 3: Conexión del lector biométrico a la PC

En las siguientes imágenes se detalla el uso del software EVTOOLS en el proceso de administración de las huellas dactilares de los usuarios.

- Se abre la aplicación EVTOOLS y haciendo clic en la pestaña FILE, ARCHIVO / SERIAL COM. Se selecciona 9600 baudios y el número de puerto COM que el sistema operativo le da al cable USB /RS232.

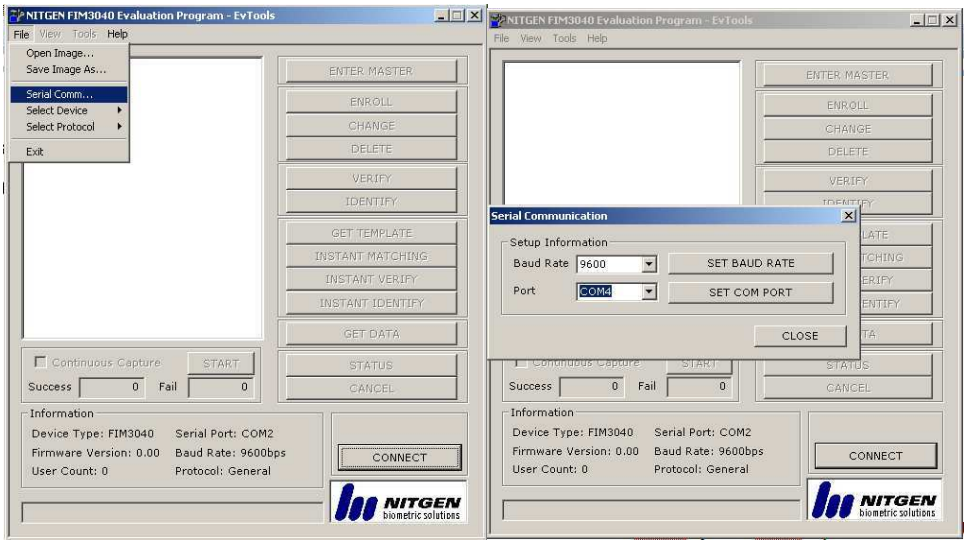


Figura 4: Configuración del puerto serial de conexión

Autenticación De Usuario

El ingreso a EVTOOLS requiere de la autenticación de usuario y contraseña (véase Figura 5). Al introducir los datos solicitados, se despliega la ventana principal de la interfaz (véase Figura 5), si la información proporcionada es

correcta, de lo contrario, se presenta un mensaje de error y se retorna al paso anterior.

- El sistema indica que se ha configurado correctamente el puerto COM. Posteriormente se presiona en CONNECT y se espera el mensaje de confirmación. Se ingresa en ENTER MASTER, se escoge la opción DEVICE PASSWORD.

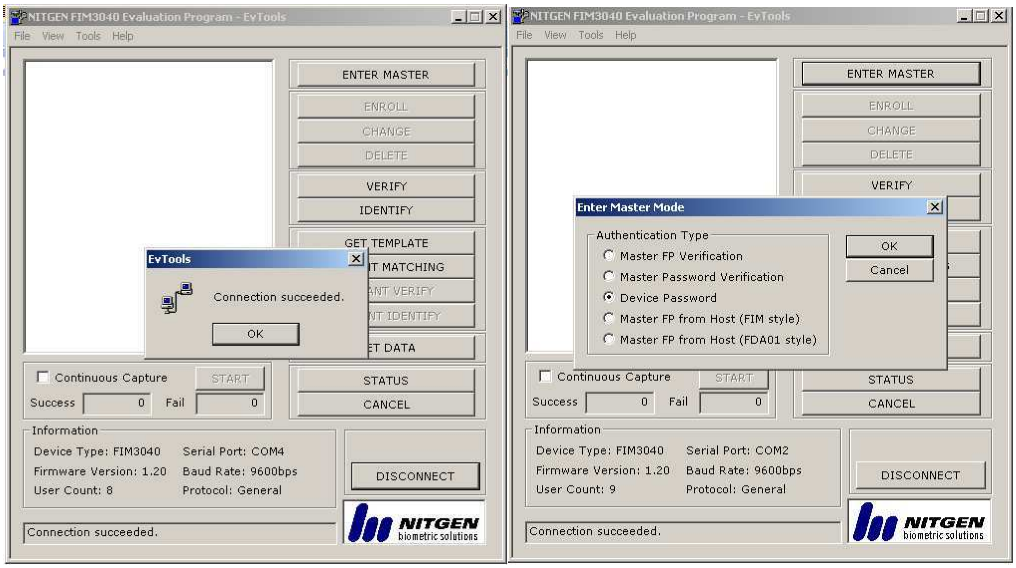


Figura 5: Conexión e ingreso a modo maestro

- Se ingresa la contraseña “0123456” y se hace clic en ENROLL. En este punto el dispositivo está listo para ingresar un nuevo usuario. Aquí se debe teclear una identificación de 4 dígitos (ID). Este código posteriormente se va a ingresar en la base de datos de la computadora.

Figura 6: Proceso de ingreso de ID antes de inclusión de un nuevo usuario al lector biométrico

- El nuevo usuario enseguida debe colocar una de sus huellas en el lector por dos ocasiones y esperar el mensaje de confirmación si esta correctamente la huella se queda guardada con su respectivo ID.

Figura 7: Proceso de lectura de la huella dactilar del nuevo usuario

Haciendo clic en la pestaña **"TOOLS"** (Herramientas) se obtiene una página que resume la cantidad de huellas que se han ingresado con su respectiva identificación durante las últimas 24 horas. Éstas se agrupan, de acuerdo a su dirección de flujo (entrada, salida o bidireccional).

4. SOFTWARE EN PC

4.1. El software de la computadora personal está realizado en Visual Basic 6.0. Se lo escogió debido a su simplicidad de uso y gran robustez. Es un lenguaje orientado a eventos, sus controles e indicadores se pueden personalizar gráficamente.

Los campos de la base de datos que manejan la información del usuario son: nombres, apellidos, hora de entrada, hora de salida, fecha de inicialización del turno.

Los reportes que puede imprimir el administrador del sistema son: autenticaciones (usuario, hora, fecha, acceso), apertura de la puerta (fecha, hora de apertura, hora de cierre).

4.2. La primera interfaz gráfica ofrece información detallada del estado de la conexión de la base de datos con el lector biométrico, la IP del módulo remoto, existe un botón para entablar y terminar la comunicación y una tabla que contiene información de la nómina de empleados

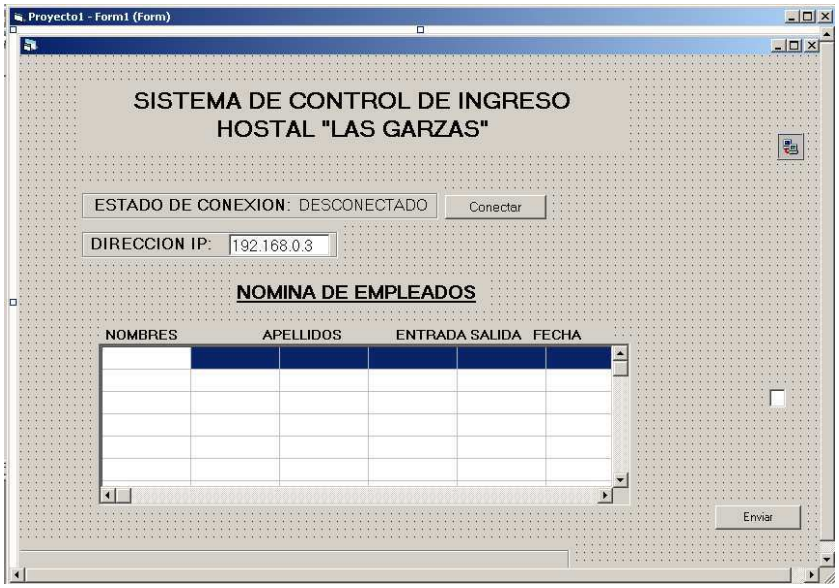


Figura 8: Pantalla principal del programa

4.3. Dando clic en la primera pantalla se ingresa a la segunda interfaz gráfica la cual permite ingresar los empleados, previamente autenticados en el lector biométrico, es importante resaltar la necesidad de coincidencia entre la clave asignada en la base de datos y el número de usuario grabado en la memoria interna del lector biométrico.

Figura 9: Pantalla de ingreso de datos del empleado

4.4. Una vez terminado el ingreso de nombres, apellidos horas de entrada y salida de los usuarios se guarda y se procede a, ingresar una clave de 4 dígitos que se ingresó previamente al insertar un nuevo usuario en el lector biométrico. Para esto se inicia el programa que maneja la base de datos y se hace clic en CONECTAR.

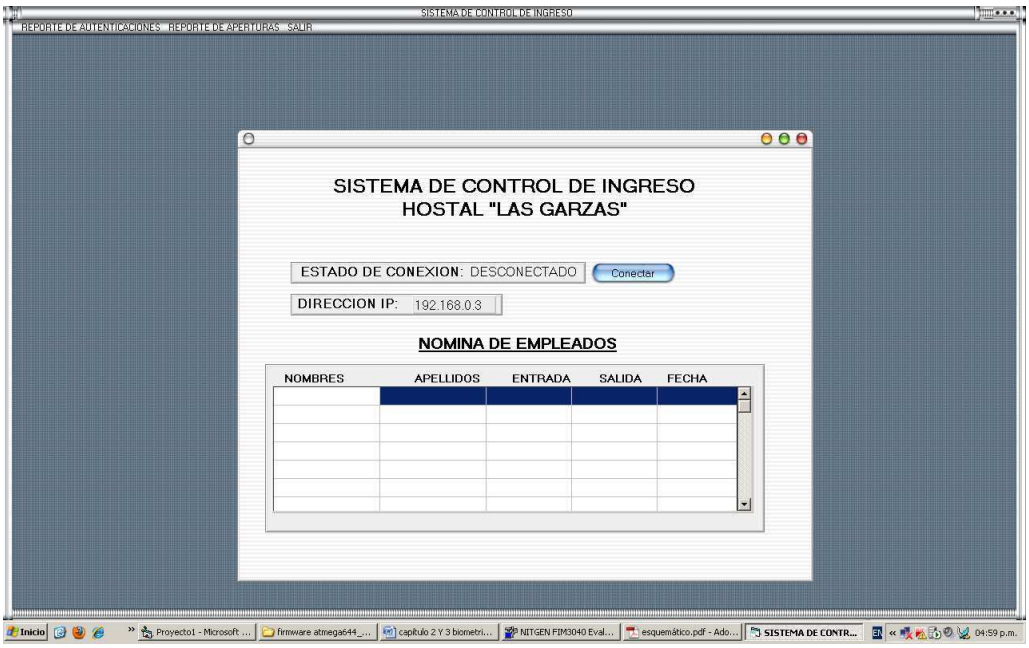


Figura 10: Proceso de inserción de un nuevo usuario en la base de datos

4.5. Luego de iniciada la conexión, se llenan los campos de la base tales como nombres, apellidos, hora de entrada, hora de salida y fecha a partir de la cual empieza a laborar el empleado. Además, se ingresa el código ID con el que a ese usuario se ingresó en el lector biométrico.

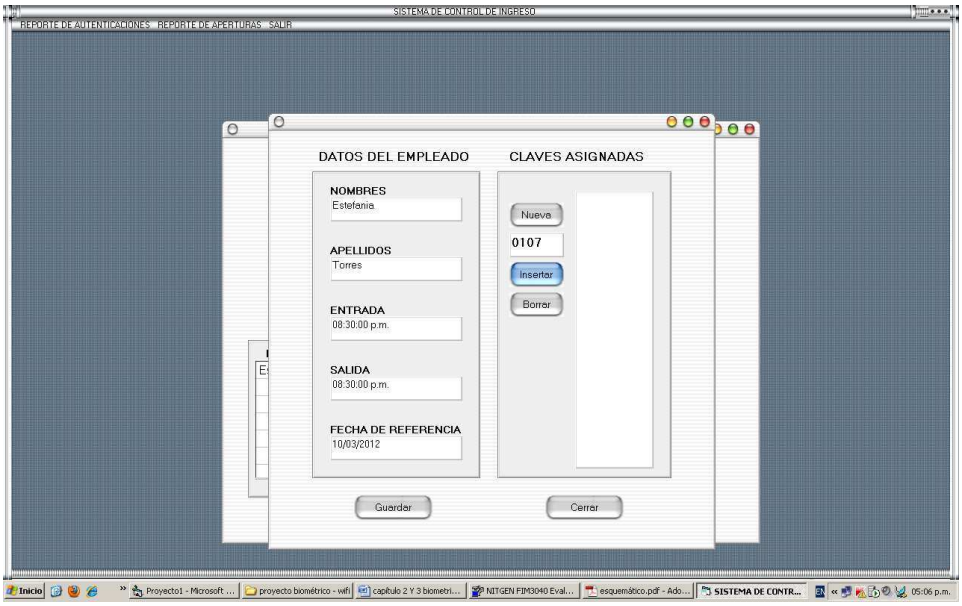


Figura 11: Asignación de un nombre al código de 4 dígitos (ID) de un usuario.

4.6. Si el proceso se realizó satisfactoriamente, se tendrá un nuevo empleado ingresado y el sistema empezará a aplicar el control de acceso con él.

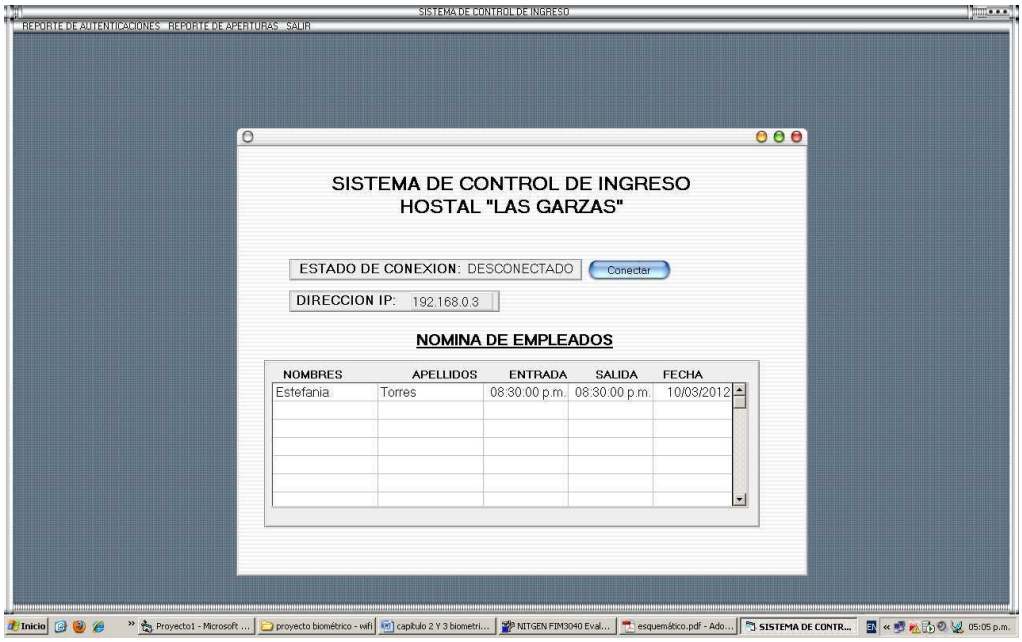


Figura 12: Usuario asignado en la base de datos