UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

TEMA:

Sistema automático para el registro del personal de la Empresa SeguMedik

AUTORA:

Ing. Diana Carolina Bohórquez Heras

Trabajo de titulación previo a la obtención del grado de

MAGISTER EN TELECOMUNICACIONES

TUTOR:

Ing. Daniel Iván Garrido Rodríguez, MSc.

Guayaquil, Ecuador

20 de Febrero de 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Bohórquez Heras Diana Carolina**, como requerimiento para la obtención del Título de **Magíster en Telecomunicaciones**.

TUTOR

f. _____
Ing. Daniel Iván Garrido Rodríguez, MSc.

DIRECTOR DEL PROGRAMA

f. _____
Ing. Manuel Romero Paz, MSc.

Guayaquil, a los 20 días del mes de Febrero del año 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Bohórquez Heras Diana Carolina**

DECLARO QUE:

El Trabajo de Titulación, **Sistema automático para el registro del personal de la Empresa SeguMedik** previo a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 20 días del mes de Febrero del año 2017

LA AUTORA

f. _____
Ing. Diana Carolina Bohórquez Heras

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Bohórquez Heras Diana Carolina**

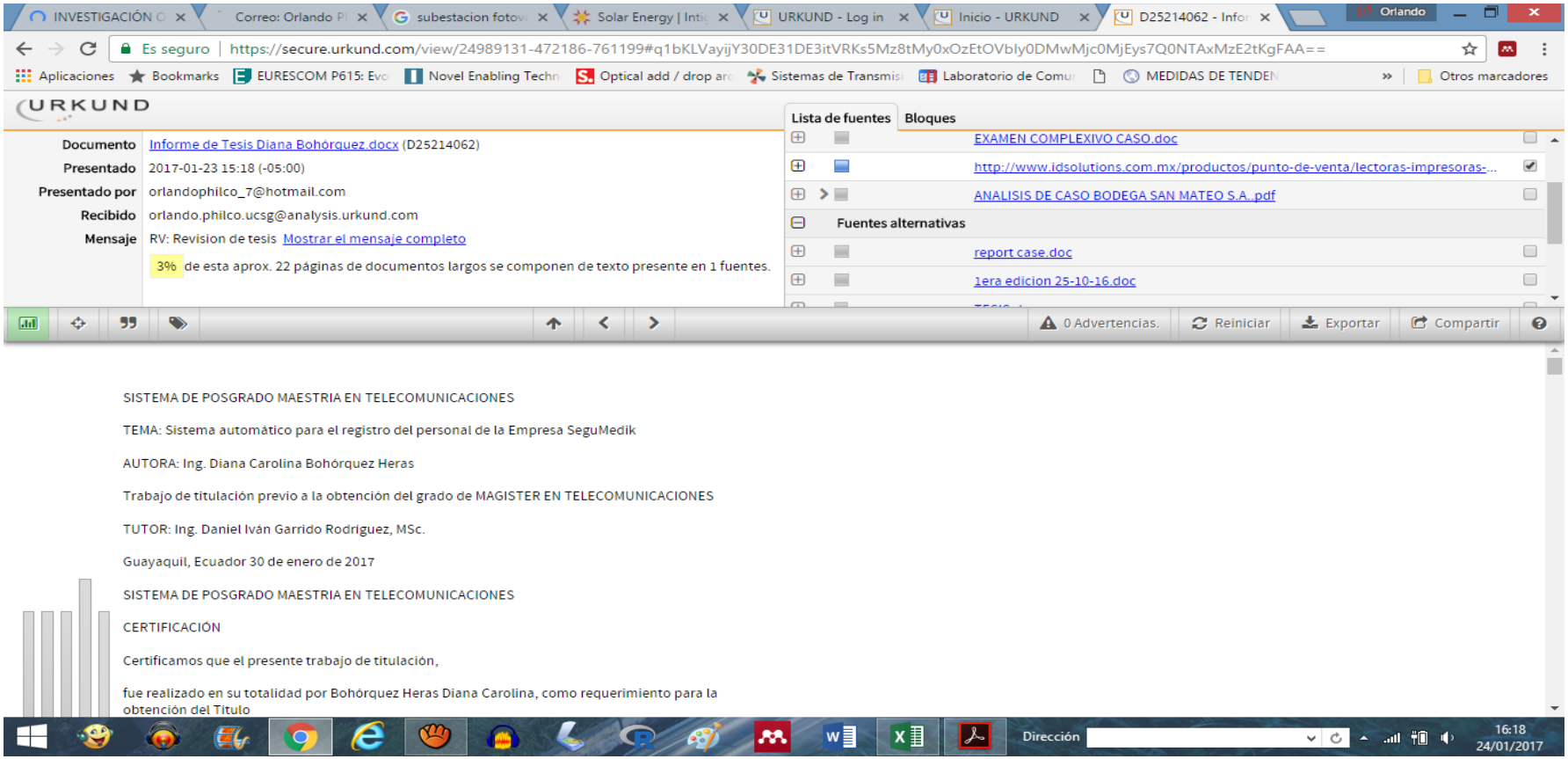
Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Sistema automático para el registro del personal de la Empresa SeguMedik**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 20 días del mes de Febrero del año 2017

LA AUTORA

f. _____
Ing. Diana Carolina Bohórquez Heras

REPORTE URKUND



Reporte Urkund de Tesis "**Sistema automático para el registro del personal de la Empresa SeguMedik**" de la ingeniera **Diana Carolina Bohórquez Heras**, al 3% de coincidencias.
Atentamente.

MSc. Orlando Philco Asqui.

Agradecimientos

Quisiera agradecer primeramente a Dios por darme la oportunidad de vivir estos momentos, y ser mi guía para culminar esta etapa tan importante en mi carrera profesional.

A mi esposo Rafael, que me apoyo en todo momento y supo darme el ánimo necesario para continuar y proyectar mi vida profesional siempre aspirando a ser la mejor.

A mis padres Bayardo y Fanny por su cariño y apoyo sin condiciones por ser mi pilar fundamental. Agradecerle a mi padre por ser siempre mi fortaleza, mi guía y mi gran ejemplo a seguir, a mi madre por ser incondicional, mi mejor amiga, la que siempre ha estado a mi lado pendiente de mis alegrías y tristezas.

A mi director de tesis el Ing. Daniel Iván Garrido Rodríguez, por estar presto a brindarme siempre apoyo con sus ideas y opiniones, que me ayudaron para que me sienta enorgullecida con mi proyecto de tesis. Gracias a cada uno de los maestros, que participaron en mi desarrollo profesional durante la maestría.

Dedicatoria

Dedico la siguiente tesis a Dios que fue mi guía, y me dio la fuerza para seguir adelante y no desmayar en los problemas que se me iban presentando durante este periodo de aprendizaje.

A mi esposo Rafael y mi hijo Santiago que me dieron las fuerzas día a día para culminar esta etapa de mi vida. A mi familia quienes por ellos soy lo que soy. A mis padres por su apoyo, consejos, amor, y ayuda en los momentos difíciles.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ing. Daniel Iván Garrido Rodríguez, MSc.

TUTOR

f. _____

Ing. Orlando Philco Asqui, MSc.

REVISOR

f. _____

Ing. Luis Córdova Rivadeneira, MSc.

REVISOR

f. _____

Ing. Manuel Romero Paz, MSc.

DIRECTOR DEL PROGRAMA

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

En este trabajo se presenta una propuesta de sistema de control de acceso para las empresas a las que SeguMedik ofrece el servicio de seguridad ocupacional. El sistema, se basa en la lectura del código de barra del documento de identificación de la persona que quiere acceder o salir de un determinado local. Utilizando el Arduino Mega con un escudo inalámbrico, envía esa información a un servidor para que la compare con la base de datos confeccionada para este fin. Para permitir la entrada a un determinado local, si la coincidencia es positiva, actúa sobre el mecanismo de apertura de la puerta y registra en la base de datos, fecha y hora de entrada de la persona autorizada. Si no hay coincidencia, el sistema mantiene la puerta cerrada. Para controlar la salida y el tiempo de estancia, de la persona ya autentificada, el personal dentro del local debe presentar y validar su documento de identificación para accionar el mecanismo de apertura de la puerta y que se registre en la base de datos la fecha y hora de salida.

Palabras claves: SeguMedik, Código de barra, Arduino Mega, Escudo inalámbrico

ABSTRACT

This paper presents a proposal for an access control system for the companies to which SeguMedik offers the occupational safety service. The system is based on reading the barcode of the identification document of the person who wants to access or leave a certain location. Using the Arduino Mega with a wireless shield, send that information to a server to compare it with the database prepared for this purpose. In order to allow entry to a certain location, if the match is positive, it acts on the opening mechanism of the door and registers in the database, date and time of entry of the authorized person. If there is no match, the system keeps the door closed. In order to control the departure and residence time of the person already authenticated, the personnel within the premises must present and validate their identification document to activate the door opening mechanism and that the date and departure time.

Keywords: SeguMedik, Barcode, Arduino Mega, Wireless shield

Capítulo 1: Descripción del proyecto de intervención.

1.1. Introducción.

La empresa SeguMedik ubicada en el Norte de la ciudad de Guayaquil nace de la necesidad de una asesoría apropiada, estructurada y comprensible para facilitar a otras empresas la implementación del modelo de Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST), en base a los lineamientos del Sistema de Auditorias de Riegos del Trabajo (SART).

1.2. Justificación del problema a investigar.

SeguMedik, en las empresas a las que le presta servicio, ha detectado violaciones de la seguridad y de permanencia de su personal en sus puestos de trabajo.

1.3. Antecedentes.

Se conoce la existencia de empresas que realizan el control de acceso del personal a través de sistemas de video cámaras para el reconocimiento facial o sistemas de escáneres que leen códigos de identificación de tarjetas desarrolladas para ese fin.

1.4. Definición del problema

En numerosas empresas a las que SeguMedik les brinda servicio, se ha visto afectada la integridad de las instalaciones, y la remuneración justa de los servicios prestados.

1.5. Objetivos

1.5.1. Objetivo General:

Presentar una propuesta de sistema de control de acceso para las empresas a las que SeguMedik ofrece el servicio de seguridad ocupacional.

1.5.2. Objetivos específicos:

- ✓ Proponer un sistema para la lectura del código de barra del documento de identificación de la persona que quiere acceder o salir de un determinado departamento.
- ✓ Confeccionar una base de datos con la información del personal que labora en cada departamento.
- ✓ Proponer un sistema que permita comparar la lectura del código de barra del documento de identificación de la persona que quiere acceder o salir de un determinado departamento con la base de datos confeccionada para este fin.
- ✓ Registrar, en una base de datos, la entrada y salida del personal que labora en la instalación con vistas a cuantificar la estancia en su puesto de trabajo.

1.6. Hipótesis

Si se propone un sistema de control de acceso propietario y eficiente para las empresas a las que SeguMedik les brinda servicio, se podrá garantizar la seguridad e integridad de las mismas y remunerar de forma justa los servicios prestados por el personal que labora en estas.

1.7. Metodología de investigación.

- Método de observación documental y científica: Se emplea con el objetivo de obtener información y lograr la definición del problema del marco teórico y el desarrollo de la tesis.
- Método analítico: Se emplea con objetivo de analizar los elementos de forma separada para ver las relaciones entre ellos.

Capítulo 2: Fundamentación Teórica.

2.1. Introducción.

Debido a las constantes violaciones de la seguridad, detectadas por SeguMedik, en las empresas a las que les brinda el servicio, se hace necesario, denegar el acceso, al personal ajeno a las mismas, identificar, controlar y registrar el acceso de los especialistas de la salud (médicos) y personal no médico (auxiliares) a cada una de las empresas, cuantificando el tiempo de estancia en sus puestos de trabajo con vistas a remunerar su actividad en función del tiempo dedicado a ella dentro de la instalación.

2.2. Sistemas de identificación de personas

La identificación de personas se puede realizar por distintas formas, desde la presentación de un documento o tarjeta hasta el uso de sistemas electrónicos y de procesamiento de imágenes o señales. Sus aplicaciones se centran en todo aquello relacionado con la seguridad. Los sistemas de identificación pueden ser manuales o automatizados.

Los manuales utilizan una persona que lee el documento de identificación u observa directamente a la persona que quiere entrar para comparar contra un documento que autorice o no su acceso. Son susceptibles a la violación de códigos de ética del controlador y amenaza de cualquier infractor.

Los automatizados se basan en:

- El uso de un documento que debe ser procesado por un sistema de control para su validación y su registro en una base de datos.

- La identificación biométrica basada en huellas dactilares, características de los ojos (retina, iris) y características de la voz.
- El reconocimiento de imágenes, específicamente, el reconocimiento de caras a partir de determinadas características especiales. Se puede considerar como parte de la identificación biométrica, pero, como se ha desarrollado, muchas de las bibliografías lo consideran como un método independiente.

2.3. Identificación por códigos de barras.

Se trata de un sistema de identificación automatizado basado en el uso de un documento que debe ser procesado por un sistema de control para su validación y registro en una base de datos. Se dice que la primera patente asociada a esta idea data de 1952, en Estados Unidos y estaba asociada a un sistema automático para la identificación de vagones de ferrocarril. Sin embargo, no es hasta 1980 que se asienta como un éxito comercial, posiblemente gracias al desarrollo de los sistemas de cómputo.

Es un código basado en barras verticales, que puede ser de colores, aunque el más utilizado es en blanco y negro. Se emplea para la identificación de artículos de forma automática, principalmente en supermercados, almacenes y, de forma general, en aquellos lugares que requieren de un inventario rápido y fiable.

Su estructura está basada en módulos, siendo este la unidad mínima de espacio. De esta forma el ancho de una barra o un espacio se mide en módulos. La barra es el elemento que representa al valor lógico 1. El espacio, por tanto, representa al valor lógico 0. Un conjunto de barras y espacios determina a un carácter que tiene asociado un carácter ASCII alfanumérico. En la figura 2.1 se muestra un ejemplo, indicando cada uno de los campos.

Figura 2.1: Estructura de un código de barras
Fuente: Google Images

Existen varios formatos de códigos, uno de los más utilizados es el GINT 13 (Global Item Number Trade de 13 dígitos) que permite identificar de forma única cualquier producto a nivel mundial. Su asignación está reglamentada por el GS1 (Global System 1) que radica en Bruselas. El número 1 indica que es el grupo encargado de asignar los códigos a las barras. Según este sistema los códigos se asignan según el nivel en la cadena de suministro, de esta forma se tienen distintos códigos para productores, suministradores al por mayor y minoristas. Estos últimos emplean uno de tres sistemas:

- EAN/UCC-8: Este emplea siete dígitos para el prefijo de la compañía y el identificador del producto y uno para el chequeo de errores.
- EAN/UCC-12: Este emplea seis dígitos para el prefijo de la compañía, cinco para la referencia del producto y uno para el chequeo de errores. Aunque existen otras combinaciones, esta es la más común y todas mantienen los tres campos incluyendo el dígito para el chequeo de errores.

- EAN/UCC-13: Este emplea doce dígitos para el prefijo de la compañía y el identificador del producto y uno para el chequeo de errores.

Como ventajas del sistema de códigos de barra aplicado a la identificación de personas se tiene:

- Mayor agilidad en etiquetar personas pues no es necesario el empleo de un documento nuevo confeccionado para este fin, basta el uso del código de barras de su documento de identificación disminuyendo los costos de inversión del sistema.
- Rápido control de forma automatizada pues permite, en tiempo real, conocer entradas y salidas para llevar un control de presencia por fecha y hora.
- Posee porcentajes muy bajos de error.
- Los equipos de lectura e impresión de código de barras al ser tan extendidos en sistemas de tiendas comerciales, son baratos, flexibles y fáciles de conectar e instalar.

Una vez que se tiene asignado el código este se escanea o se introduce en formato digital en una computadora para luego imprimirlo. Existen distintos tipos de impresoras, desde aquellas para imprimir documentos con códigos grandes hasta aquellas que permiten la impresión de documentos pequeños. En la figura 2.2 se muestran algunas impresoras de códigos de barras.

2.4. Los lectores de código de barra.

Los lectores de código de barra son escáneres ópticos que, por medio de un láser, escanean la imagen del código y la traducen a un código alfanumérico para que sea procesado por una computadora.

Figura 2.2: Distintos tipos de impresoras de códigos de barras. A la izquierda una para pequeño formato, la del cetro y la derecha industriales de alto rendimiento.
Fuente: El autor a partir de imágenes de catálogo: Soluciones AIDC de BlueStar

Los primeros lectores se conectaban por medio de los puertos serie o PS2, en la actualidad suelen usar los puertos USB o las tecnologías inalámbricas Wi-Fi o Bluetooth. Estos dos últimos son muy útiles en aquellos lugares donde el servidor de control está muy distante de cada lector e indiscutiblemente contribuyen a mantener la estética arquitectónica fundamentalmente en edificios antiguos donde se quiere conservar su imagen de época. En la figura 2.3 se muestran algunos de estos lectores.

Figura 2.3: Distintos tipos de lectores
Fuente: El autor a partir de imágenes de http://ezoco.es/lorena/perifericos-de-entrada-3/lector-de-codigo-de-barras/ Compuson, 2011

2.5. Algunos fabricantes de lectores de código de barras.

Lector Symbol

Symbol es ahora de Motorola. Se Reconoce como el líder de los productos para movilidad y soluciones que hacen el trabajo más efectivo, manteniendo interconectadas las aplicaciones de negocio y los procesos fuera del lugar de trabajo. Symbol permite la aplicación de lectores de código de barras y colección de datos para distintas aplicaciones como industrias, gobierno, y más.

Lector PSC

Es el fabricante mundial de productos para recolección y lectura de código de barras avanzado. Sus líneas de productos incluyen escáneres inalámbricos y fijos, así como terminales de colección de datos, que son utilizados en el sector industrial, minorista, distribución, de transporte y logística. Los productos PSC permiten la automatización de los centros de trabajo haciendo más fácil y eficiente las actividades de productividad. PSC también es conocida como Percon.

Lector Intermec

Intermec desarrolla, fabrica e integra computadoras móviles, terminales alámbricas e inalámbricas para la captura de datos, tiene más de 100 patentes en tecnología RFID (identificación por radio frecuencia) y sistemas de computación móvil para las compañías del mundo entero. Y es pionero en el desarrollo e investigación de impresoras código de barras y lectores o escáneres.

Lector Metrologic

Metrologic

La empresa fundada en 1968 ha sido pionera en la captura de datos industriales. Ha sido reconocida como experta global en desarrollo e innovación de soluciones para la captura de datos y recolección. Como líder en mercados verticales integrados fabrica lectores de código de barras, es la compañía que más invierte en hardware para decodificación de simbologías de barras, software de procesamiento de imágenes y proporciona un servicio al cliente de excelencia.

Lector HHP

Hand Held

HHP también conocido como Hand Held Products es distinguido líder mundial en la recolección de datos basado en imágenes, con su tecnología exclusiva Adaptus™ Imaging Technology. Las soluciones bajo Adaptus Imaging ofrecen al usuario final versatilidad, confiabilidad en el funcionamiento y lectura de código de barras. Con la tecnología Adaptus, los clientes pueden leer virtualmente cualquier código de barras o tag, capturar imágenes digitales, firmas, código de barras dañados, y mucho más.

Lector Datalogic

DATALOGIC

Datalogic produce una gran variedad de lectores de código de barra de mano utilizando tecnología láser y CCD. Datalogic ofrece un gran rango de terminales móviles para la recolección de datos. Así como tecnología RFID para aplicaciones industriales, electrónicas y de manejo de inventarios.

2.6. Propuesta de solución.

Atendiendo al objetivo general y a los específicos declarados en este trabajo, con vistas a dar solución a este proyecto, se decide no adquirir un sistema desarrollado por otra empresa y desarrollar uno propio basado en la lectura de un documento de identificación que contenga un código de barras.

El sistema debe tener dos componentes: una de hardware y otra de software. La componente de hardware será la encargada de identificar y permitir el acceso del personal a un determinado departamento mientras que, la componente de software será la encarga de almacenar los datos para la identificación del personal, el registro de entradas y salidas y el tiempo de estancia además, permite al administrador del sistema la configuración del hardware.

Capítulo 3: Hardware propuesto.

3.1. Introducción.

En la figura 3.1 se ilustra el diagrama funcional.

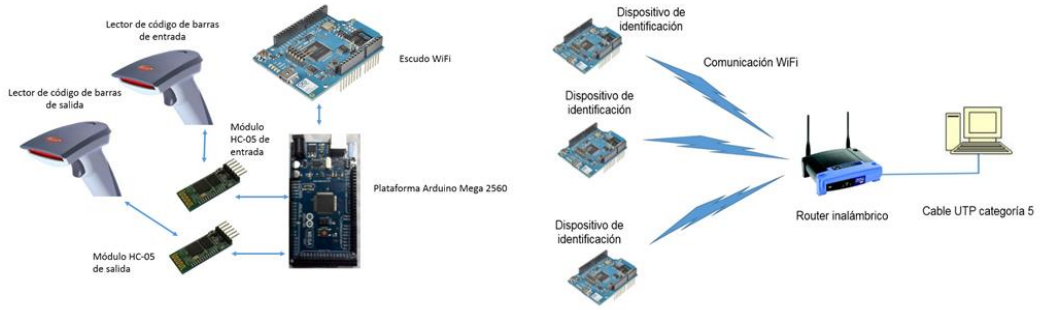


Figura 3.1: Diagrama funcional del sistema.

Fuente: La autora.

Los lectores de códigos de barra se comunican con un Arduino Mega 2560 utilizando módulos Bluetooth HC-05. El Arduino por medio del escudo Wi-Fi se conecta a la red inalámbrica. El router inalámbrico se conecta a la PC servidor por el cable UTP categoría 5E.

En cada puerta se requiere de dos lectores. Uno para validar y registrar la entrada al local y el otro para registra la salida.

Se propone el uso de la tecnología Wi-Fi porque tiene las siguientes ventajas:

- No se necesitan grandes inversiones de cableado.
- Brinda flexibilidad a la hora de agregar o eliminar locales.

Se propone el uso de un Router inalámbrico para garantizar una red de datos totalmente independiente y dedicada a este sistema. De esta forma una estación de trabajo que no pertenezca a esta red no tiene

acceso a los datos que circulan por ella. Además, implementando el filtrado por medio de direcciones de Control de Acceso al Medio o MAC se impide la conexión a cualquier dispositivo ajeno a la red.

Se recomienda el uso de un router como el WRT54G2 de Cisco, el TL-WR720 de TP-Link o similar siempre que permita:

- Filtrado MAC.
- Soportar el protocolo de encriptación Wireless Protected Access 2 (WPA2).
- Soportar Dynamic Host Configuration Protocol (DHCP).

En la figura 3.2 se ilustra el Router Wi-Fi TL-WR720 de TP-Link.

Figura 3.2: Router Wi-Fi TL-WR720 de TP-Link.
Fuente: Manual de usuario.

3.2. Dispositivo de identificación.

El diagrama funcional del dispositivo de identificación se muestra en la figura 3.1.Está constituido por dos lectores de código de barras que se comunican con un Arduino Mega 2560 utilizando 2 módulos (uno para cada lector pues soportan solo comunicación punto a punto) Bluetooth

HC-05. El Arduino a su vez se conecta a la red inalámbrica y actualiza los datos al servidor por medio del escudo (shield) Wi-Fi.

Uno de los lectores de código de barra se utiliza para la autenticación al realizar el acceso al local y el otro para la salida. El Arduino también se encarga de abrir la puerta cerrada por medio de un electroimán en caso de que la persona sea admitida.

En la figura 3.3 se ilustra el Dispositivo de identificación.

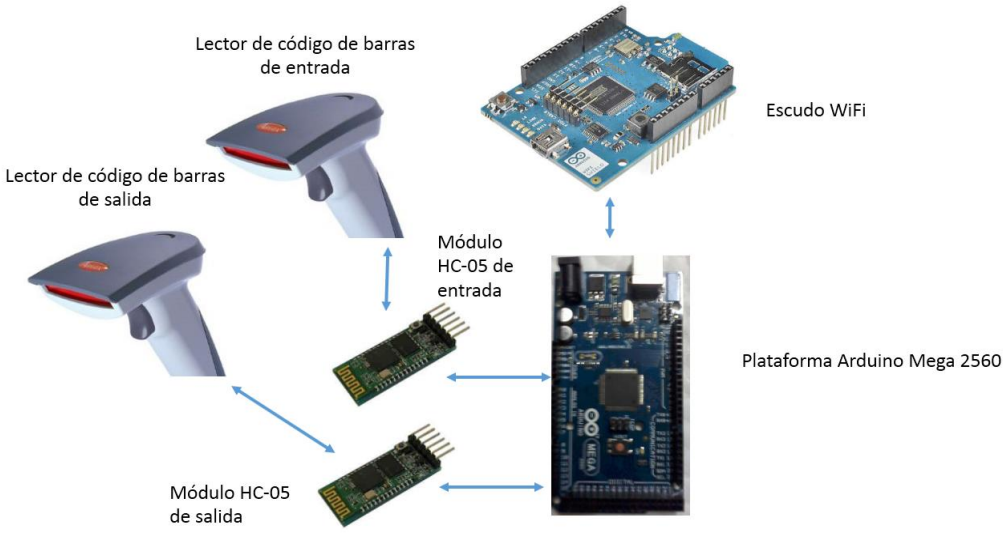


Figura 3.3: Dispositivo de identificación.
Fuente: La autora.

3.3. Plataforma Arduino Mega 2560.

El Arduino Mega 2560 utiliza al microcontrolador ATmega2560 (Arduino, 2015). Posee 54 entradas/salidas digitales (14 se pueden utilizar como moduladores de ancho de pulso) y 16 entradas analógicas. Cuenta con 4 puertos serie, uno de ellos para la comunicación con una computadora por medio del puerto USB. Además garantiza comunicación Serial Peripheral Interface o SPI, tiene 4 fuentes de interrupción externa, botón de reset y tensión de alimentación variable entre 7V y 12V.

Además, de algunos de sus terminales se puede obtener una tensión de alimentación de 5V para energizar otros circuitos.

Los niveles de tensión de las entradas/salidas digitales son compatibles con la lógica TTL y son capaces de entregar hasta 40 mA por terminal. Esto es válido ya sea que funcione como entrada o como salida, si se tiene en cuenta que la corriente que se demande a un puerto no sea de más de 100 mA. Posee memoria Flash de 256 kB, SRAM de 8 kB, EEPROM de 4 kB y trabaja con un reloj de 16 MHz. El kit se muestra en la figura 3.4.

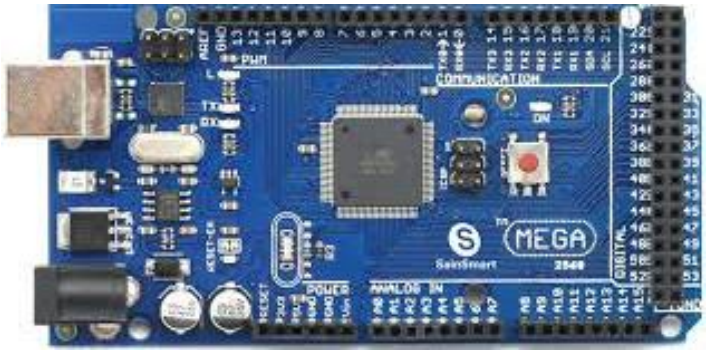


Figura 3.4: Arduino Mega 2560.

Fuente: La autora.

3.4. Módulo Bluetooth HC-05.

El HC-05 es una tarjeta electrónica, que permite la comunicación por medio del protocolo Bluetooth tanto en modo Master como Esclavo(Guangzhou HC Information Technology Co., Ltd),(ITeadStudio, 2010),(NoMADA, 2015). Posee 6 terminales, su tensión de alimentación se encuentra entre 3,3V y 5V (cuenta con un regulador de tensión de 5V a 3,3V) y los niveles de tensión de las salidas son compatibles con la lógica TTL. La comunicación con el controlador se realiza por un puerto serie que soporta varias velocidades de transmisión. Se puede configurar por medios de comandos AT,con una sintaxis similar al conjunto de comandos Hayes (fabricante de módems) y recogidos en la Unión Internacional de

Telecomunicaciones (UIT) para la comunicación módems utilizados antes de la aparición de Windows 95.

Sus características eléctricas son las siguientes:

- Sensibilidad de -80dBm
- Potencia de transmisión de +4dBm que le confiere un alcance de hasta 10 m.
- Velocidad de transmisión del puerto serie programable (9600 baudios por defecto, aunque en algunos documentos refieren 38400) con 8 bits de datos, 1 bit de parada y sin bit de paridad.
- Antena integrada

En la figura 3.5 se muestra este dispositivo y en la tabla 3.1 se describen los terminales.

Figura 3.5: Módulo Bluetooth HC-05.
Fuente: Hoja de datos del fabricante

Tabla 3.1: Listado de los terminales del módulo HC-05.

Nombre	Uso
State	Indica el estado en el que se encuentra el módulo.
Rx	Terminal de recepción serie, se conecta al de transmisión del controlador
TX	Terminal de transmisión serie, se conecta al de recepción del microcontrolador.
GND	Tierra del dispositivo.
VCC	Terminal de alimentación
KEY	Permite acceder al modo AT para la configuración del módulo

Fuente: Hojas de datos.

Al comenzar a trabajar con este dispositivo, es importante comprobar la velocidad de transmisión que tiene predefinida. Aunque se especifica que es de 9600 baudios, según documentación encontrada, esto no siempre se cumple. Una vez que se logra establecer comunicación con el dispositivo se puede lograr la configuración deseada por medio de los comandos AT. Entre los más útiles se encuentran:

- AT+VERSION Indica la versión del firmware. Se puede utilizar variando la velocidad de transmisión del controlador hasta lograr caracteres legibles. De esta forma se conoce cuál es la velocidad a la que está programado por defecto.
- AT+NAME: da el nombre del dispositivo. Si a continuación se escribe un nombre se le asigna este al dispositivo. Puede hacerse de dos formas: AT+NAMEMIO o AT+NAME=MIO.
- AT+BAUD: devuelve la velocidad de transmisión a la que está configurado. Si a continuación se escribe un número del 1 al 8 se cambia según el siguiente orden.

1. 1200bps
2. 2400bps

3. 4800bps
4. 9600bps
5. 19200bps
6. 38400bps
7. 57600bps
8. 115200bps

- AT+PIN o AT+PSWD: permite conocer el PIN. Si se escribe un número a continuación se cambia el valor de este. El comando varía según fuentes bibliográficas consultadas.
- AT+ROLE: permite conocer si está configurado como Master (1) o Esclavo (0). Permite configurarlo en alguno de estos modos.
- AT+CMOD: si se le pasa cero indica que se puede conectar solo a una dirección específica.
- AT+BIND: fija la dirección del dispositivo al que se puede conectar.
- AT+RESET: resetea al dispositivo.
- AT+ORLG: restablece la configuración de fábrica.
- AT+RNAME: indica el nombre de todos los dispositivos Bluetooth a su alcance.

Para trabajar en el modo de comandos AT o para salir de este modo y entrar al de comunicación, se recomienda desenergizar al dispositivo, cambiar el nivel del terminal KEY y luego energizarlo. No se aconseja el cambio de nivel del terminal con el dispositivo alimentado. Al trabajar con los comandos AT hay que garantizar que se transmitan los caracteres de retorno de carro y salto de línea (\r\n) ya que no se ejecuta el comando hasta recibir estos caracteres.

Posee un LED que mientras no esté conectado o en modo de comandos AT se mantiene parpadeando. El PIN por defecto es 1234.

3.5. Escudo Wi-Fi.

El shield Wi-Fi de Arduino, es el equivalente a una tarjeta de red para el protocolo 802.11 de la IEEE (Arduino, 2016). Permite a una plataforma de Arduino conectarse a una red de este tipo. Para ello se utilizan una serie de instrucciones recogidas en la librería Wi-Fi disponible en el sitio web de la plataforma. Entre sus características se encuentra:

- Tensión de alimentación de 5V que debe ser suministrada por la placa de Arduino.
- Compatible con los protocolos 802.11b/g
- Soporta encriptación WEP y WPA2.
- La comunicación con el Arduino se realiza por medio del puerto SPI, al igual que con un lector de tarjetas micro SD incorporada en el escudo.

Se utiliza un microcontrolador ATmega 32UC3 encargado de la comunicación y control soportando los protocolos TCP y UDP. El lector de tarjeta micro SD se puede utilizar para almacenar archivos que sean necesarios transmitir por la red e incluso los datos de una página web. Es importante resaltar que cuando se accede a la tarjeta SD no se tiene acceso al bloque Wi-Fi.

La comunicación SPI se realiza por medio de los terminales 11,12 y 13 para el Arduino 1 y el 50,51 y 52 en el Arduino Mega. En ambos casos el terminal 10 se utiliza para seleccionar el bloque de red y el 4 para seleccionar la tarjeta SD. El terminal 7 es utilizado en el handshake entre el shield y la placa de Arduino. En el caso de utilizar una placa Mega el terminal 5, aunque no se utiliza en la selección de los bloques del escudo, se debe definir como salida para evitar errores. Si no se utiliza uno de los bloques presentes en el escudo, hay que deshabilitarlo de forma explícita

en el programa. En la figura 3.6 se muestra la distribución de terminales del shield.

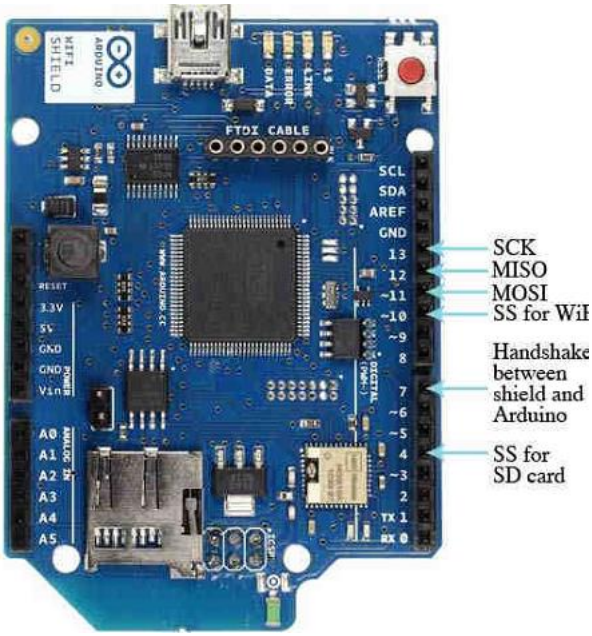


Figura 3.6: Arduino Mega 2560.

Fuente: Arduino, 2016

La librería para el trabajo con el escudo(Arduino, 2015) permite su conexión como cliente o como servidor, soporta las encriptaciones WEP y WAP2. Requiere que la red tenga activo el modo de radiodifusión para poder conectarse.

3.6. Lector de código de barras.

Se recomienda utilizar el lector Gryphon BT100 o BT200. Se trata de unos lectores inalámbricos, con comunicación Bluetooth fabricados por Datalogic que permiten la conexión con cualquier medio de cómputo que soporte este protocolo en un radio de 10m. Puede realizar 270 lecturas por segundo, el alcance de lectura máximo es de 30cm. Se suministra con una base que permite recargar las baterías y se configura por medio de un programa de ambiente Windows con comunicación serie, o por medio de lecturas de códigos de barras pre establecidos presentes en el manual

de usuario(Datalogic, 2004). En la figura 3.7 se muestra el lector en su base.

Figura 3.7: Lector de códigos de barras Gryphon BT100 en su base cargando las baterías.
Fuente: Manual de usuario.

Puede configurarse lo mismo como un dispositivo Master que como Esclavo. En caso de ser configurado como Esclavo, una vez que se enciende, espera a que el Master remoto lo localice (Nombre Gryphon BT100) y le envíe una solicitud de conexión. No requiere de PIN (en caso de necesitarlo el valor por defecto es 1234) ni contraseña para la conexión. En la figura 3.8 se ilustra el funcionamiento.

Figura 3.8: Gryphon BT100 operando en modo Esclavo.
Fuente: Manual de usuario.

Si se configura en modo Master, debe pasársele la dirección del dispositivo Esclavo con el que se desea comunicar. Por defecto, al encenderse, intenta localizar y conectarse con el Esclavo. En caso de conexión exitosa comienza a enviar las lecturas de los códigos de barras al dispositivo. En la figura 3.9 se ilustra el esquema de funcionamiento.

Figura 3.9: Gryphon BT100 operando en modo máster.
Fuente: Manual de usuario.

Teniendo en cuenta que el módulo HC-05 puede trabajar lo mismo en modo master que esclavo, que se le puede configurar para que se conecte a una dirección fija y que se requiere un dispositivo para cada lector; se decide que los lectores trabajen en modo master y los módulos HC-05 en modo esclavo.

3.7. Dispositivo de identificación. Simulación en Proteus.

El dispositivo de identificación debe garantizar la recepción de un código por parte del identificador de códigos de barras por medio de la comunicación Bluetooth y la transmisión de esta información por Wi-Fi al servidor utilizando el escudo. Aunque se van a utilizar módulos ya fabricados, se hace necesario conectar estos a la placa de Arduino y se incorporan otros elementos para la interacción con el administrador del sistema. En la figura 3.10 se muestra el esquema electrónico de simulación utilizando el Proteus, el visor SPI representa la conexión del shield Wi-Fi.

El circuito cuenta con dos botones conectados a las interrupciones externas 0 (terminal 3) y 1 (terminal 2), ambas activas a nivel bajo que permiten configurar al dispositivo para la comunicación Wi-Fi o Bluetooth respectivamente. Para esto además de presionar el botón correspondiente, el Arduino debe estar conectado a la PC por medio del puerto USB.

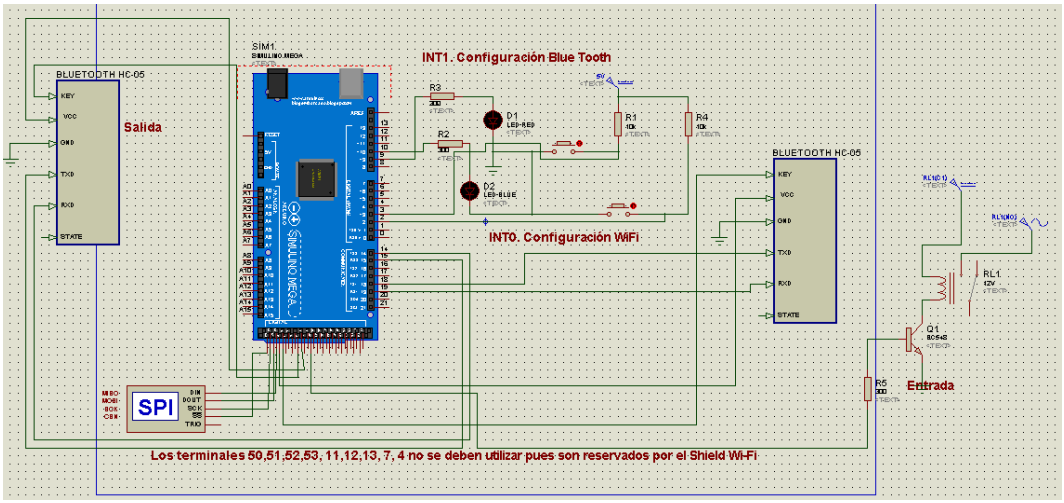


Figura 3.10: Esquema del dispositivo de identificación en Proteus.

Fuente: La autora.

Los diodos LED se utilizan para indicar que el dispositivo ha entrado o salido de algún modo de configuración. El LED D1 (rojo) indica que se ha entrado al modo de configuración Bluetooth y D2 (azul) modo de configuración Wi-Fi. También se utilizan para indicar que no se puede conectar a una red (los LED se encienden y apagan tres veces) o que hay problemas en la comunicación con el escudo Wi-Fi (se encienden ambos LED). Fuera del modo de configuración indican que el acceso ha sido denegado (LED rojo) o autorizado (LED azul).

El módulo Bluetooth de la derecha se encarga de comunicarse con el lector de entrada. Se energiza desde el terminal 49 del Arduino Mega 2560 pues su consumo de corriente es mucho menor del que es capaz de entregar este terminal, utiliza el puerto Serie1 y el terminal Key va conectado al terminal 48 del Arduino. En el caso del módulo de la

izquierda se comunica con el lector de salida. Se energiza por el terminal 42 y KEY se conecta al terminal 43, para la comunicación se emplea Serie3.

El terminal 39, mediante un transistor y un relay, es utilizado para controlar un electroimán que abre o cierra la cerradura de la puerta de los locales. Para mayor comprensión, en la tabla 3.2 se detallan los terminales del Arduino Mega 2560 y su aplicación respectiva.

Tabla 3.2: Terminales del Arduino Mega 2560 y su aplicación.

Terminal	Conectado a:	Uso
2	Interrupción externa INT0	Permite acceder al modo de configuración de la conexión Wi-Fi
3	Interrupción Externa INT1	Permite acceder al modo de configuración de la conexión Bluetooth
4	Terminal 4 del escudo Wi-Fi	SD_Select, permite seleccionar o no la tarjeta SD en dependencia si se desea trabajar con ella o no.
7	Terminal 7 del escudo Wi-Fi	Handshake entre ambos dispositivos.
9	LED2	Brinda información al operador
10	LED1	Brinda información al operador
14	Terminal TX de comunicación serie del módulo Bluetooth de salida	Recibe información del módulo
15	Terminal RX de comunicación serie del módulo Bluetooth de salida	Envía información al módulo
18	Terminal RX de comunicación serie del módulo Bluetooth de entrada	Envía información al módulo
19	Terminal TX de comunicación serie del	Recibe información del módulo

	módulo Bluetooth de entrada	
39	Transistor para el control del electroimán	Permite abrir o cerrar la puerta del local
42	Alimentación del módulo Bluetooth de salida.	Permite energizar al módulo Bluetooth de salida
43	Terminal KEY del módulo Bluetooth de salida	Permite activar o salir del modo de trabajo con comandos AT de salida
48	Terminal KEY del módulo Bluetooth	Permite activar o salir del modo de trabajo con comandos AT
49	Alimentación del módulo Bluetooth de entrada	Para energizar al módulo Bluetooth de entrada
50	Terminal 12 (MISO) del escudo Wi-Fi	Permite enviar información al escudo. Es controlado de forma transparente al programador al utilizar las funciones de la librería WiFi.h, requiere declarar la librería SPI.h.
51	Terminal 11 (MOSI) del escudo Wi-Fi	Permite recibir información desde el escudo. Es controlado de forma transparente al programador al utilizar las funciones de la librería WiFi.h, requiere declarar la librería SPI.h.
52	Terminal 13 (SCK) del escudo Wi-Fi	Señal de reloj. Es controlada de forma transparente al programador al utilizar las funciones de la librería WiFi.h, requiere declarar la librería SPI.h.
53	Terminal 10 (SS) del escudo Wi-Fi	Permite seleccionar o no al módulo Wi-Fi del escudo. Es controlado de forma transparente al programador al utilizar las funciones de la librería WiFi.h

Fuente: La autora.

La conexión a los terminales del bus SPI se realiza por medio del conector ICSP de la placa Arduino y el escudo. En la figura 3.11 se señalan dichos conectores.

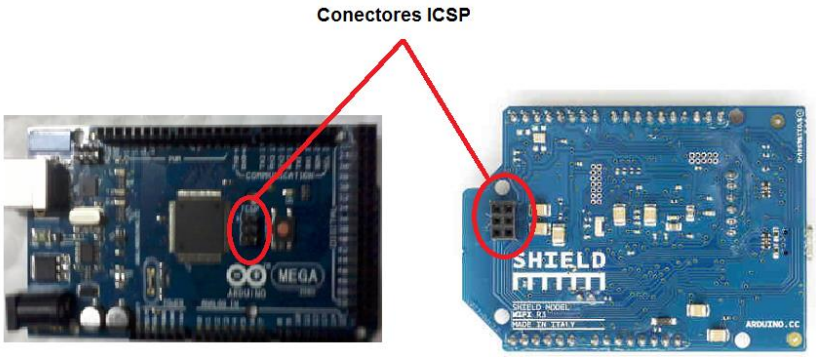


Figura 3.11: Conectores ICSP del Arduino Mega 2560 (izquierda) y del escudo Wi-Fi (derecha).

Fuente: La autora.

En la figura 3.12 se muestra el esquema utilizado en la simulación. En este caso, los HC-05 se sustituyen por terminales virtuales de comunicación serie para simular la interacción entre los módulos y el Arduino. El otro terminal virtual se utiliza para realizar la comunicación entre el Arduino y la PC por medio del puerto Serie 0 que es el correspondiente al puerto USB.

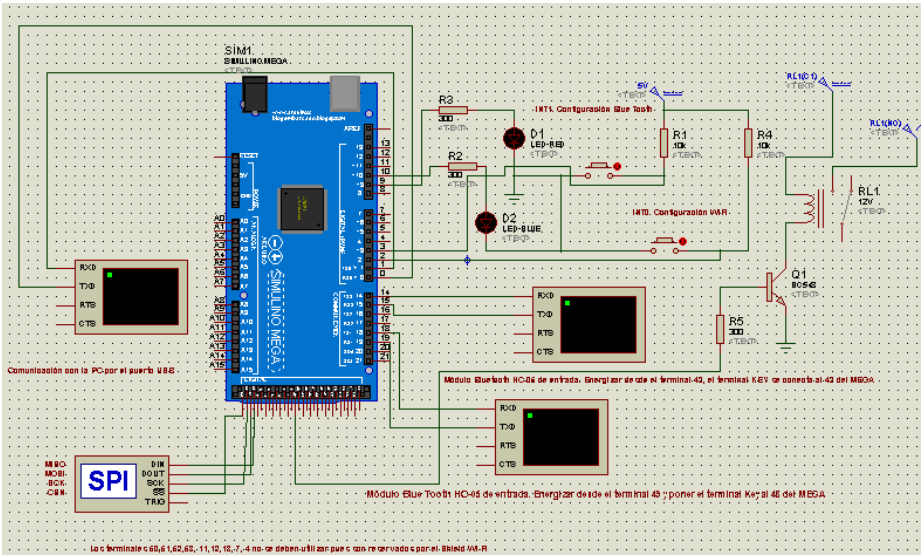


Figura 3.12: Esquema de simulación realizado en Proteus.

Fuente: La autora.

3.8. Firmware del dispositivo de identificación.

El firmware que se ejecuta en el dispositivo de identificación puede dividirse en cuatro subrutinas. Una subrutina de configuración, otra de trabajo, una para la configuración delos módulos Bluetooth y una última para la configuración de los datos de la red Wi-Fi. Ambas subrutinas de configuración se ejecutan en caso de que ocurra una interrupción externa. Para la programación es necesario utilizar las librerías EEPROM.h, WiFi.h y SPI.h creadas por los desarrolladores de la plataforma Arduino.

- **Subrutina de configuración:**

Se encarga de definir cuáles terminales se utilizan y si se utilizan como entradas y salidas. Activa y configura las interrupciones externas, carga los datos necesarios para la comunicación con la red Wi-Fi desde la memoria EEPROM y se encarga de establecer la conexión con la aplicación servidor. En caso de fallo lo indica por medio delos diodos LED.

En la figura 3.13 se muestra este algoritmo.

Primero se definen los terminales 4, 9, 10, 39, 42, 43, 48 y 49 como salidas digitales. Se mantienen la puerta cerrada poniendo un nivel bajo en el terminal 39, que corta al transistor por lo que el relay no permite el paso de la corriente por el electroimán que activa la cerradura. Luego se deshabilita el acceso al bloque de la tarjeta micro SD del escudo para evitar conflictos en la comunicación con el bloque Wi-Fi, esto se realiza poniendo un nivel alto en el terminal 4. A continuación se garantiza que ambos LED se encuentren apagados poniendo un nivel bajo en los terminales correspondientes.

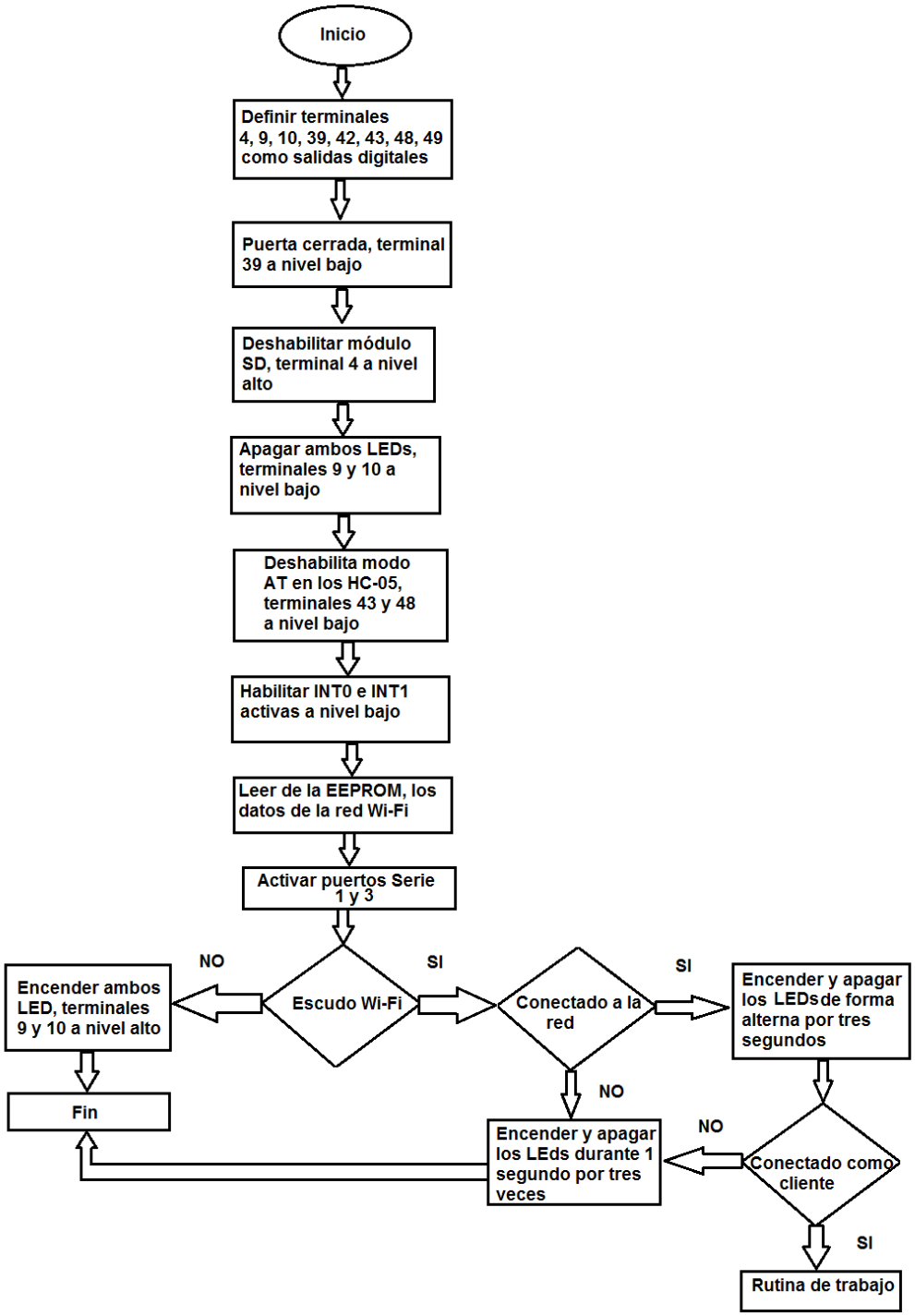


Figura 3.13: Algoritmo de configuración para establecer las condiciones iniciales. Fuente: La autora.

Para garantizar la comunicación Bluetooth de ambos módulos HC-05, se deshabilita el modo de trabajo con comandos AT. Se activan y configuran las interrupciones externas INT0 (configuración de los datos

Wi-Fi) e INT1 (configuración delos módulos HC-05 por medio de comandos AT). Las interrupciones se configuran de modo tal que sean activadas por un cambio de nivel de alto a bajo.

Se cargan los datos de la red Wi-Fi que se han almacenado en la memoria EEPROM del microcontrolador ATmega, se activa el puerto Serie1 para comunicarse con el módulo HC-05 de entrada y el Serie 3 para comunicarse con el de salida. Posteriormente se pasa a configurar el escudo Wi-Fi.

En caso de no detectar al escudo se indica encendiendo ambos LEDs. Si se detecta el escudo se pasa a conectarse a la red cuyo nombre está almacenado en la memoria EEPROM y autenticarse por medio de la contraseña almacenada en el mismo lugar. En caso de no poder conectarse se indica encendiendo y apagando los LEDs de forma alternada. Si la conexión fue exitosa, luego de indicarlo haciendo parpadear ambos LEDs, se configura como cliente e intenta conectarse a la aplicación servidor. En caso de que ocurra un problema se indica encendiendo y apagando los LEDs de forma alternada.

- **Subrutina de trabajo:**

Si la subrutina de configuración se ejecuta de forma exitosa, se pasa a ejecutar la subrutina de trabajo. Esta se encarga de esperar un dato de alguno de los lectores de códigos de barras por medio de los módulos HC-05.En la figura 3.14 se muestra este algoritmo.

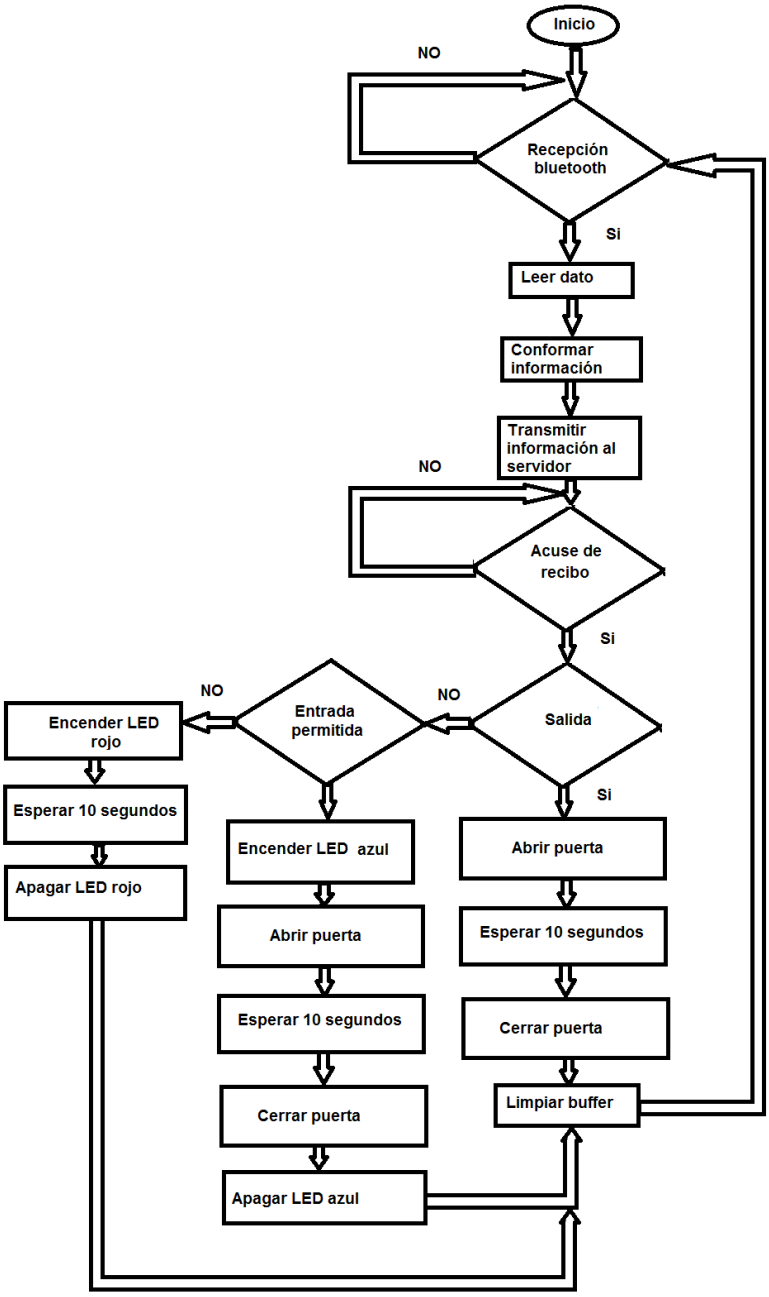


Figura 3.14: Algoritmo de trabajo.

Fuente: La autora.

Cuando se tiene una recepción de datos por alguno de los puertos serie, se pasa a conformar el dato a transmitir. Este consiste en el número de identificación asignado al dispositivo, un campo para indicar que se trata de una salida o una entrada y el código correspondiente al código de barras del documento de identificación. De esta forma la aplicación

servidor puede validar si dicha persona tiene acceso al local y a qué hora realizo la entrada y salida del local.

Una vez conformada la información se transmite al servidor y se espera por confirmación de recepción, en caso de que sea una persona que desee entrar a un local se recibe si está autorizado o no. En caso de que esté autorizado se activa la cerradura y se enciende el LED azul; en caso contrario no se activa y se enciende el LED rojo.

De esta subrutina se sale por medio de una interrupción, un reset o que se des-energice el dispositivo.

- **Subrutina de la interrupción INT1:**

Se encarga de realizar la configuración delos módulos HC-05. Para ello, el dispositivo debe estar conectado a la PC donde se ejecuta la aplicación servidor por medio del puerto USB. Además el administrador debe presionar el botón correspondiente a esta función e indicar cuál módulo va a configurar. Una vez terminada la configuración, el administrador debe presionar nuevamente el botón para regresar al modo de trabajo. El algoritmo se muestra en la figura 3.15.

Al ejecutarse la subrutina se pregunta si es la primera vez que se presiona al botón de configuración. En caso de que sea cierto, una bandera cambia de valor y se continúa con la configuración. En el caso de que no sea cierto se limpia la bandera y se actualizan las condiciones iniciales, necesarias para salir al modo de trabajo, a partir de la nueva configuración.

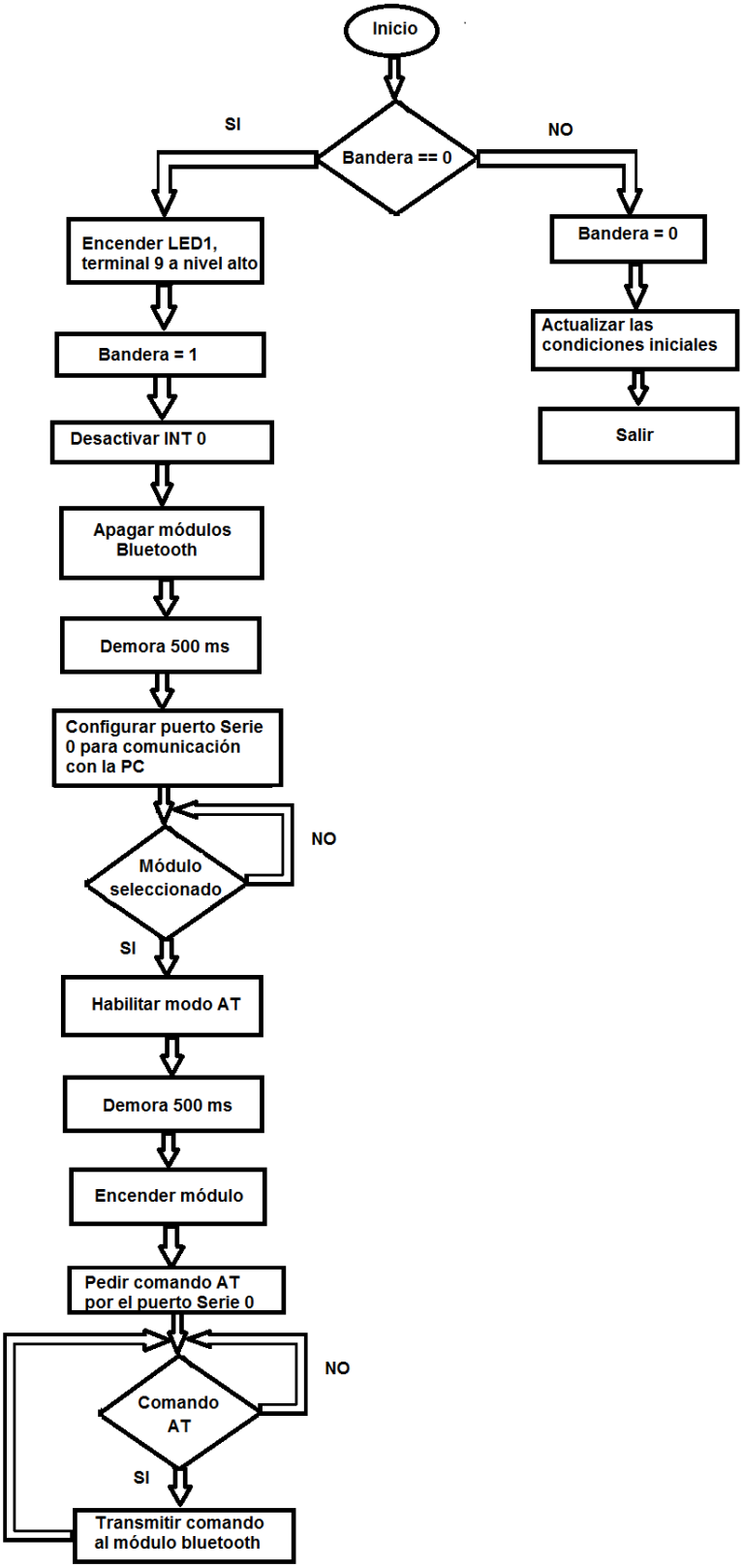


Figura 3.15: Algoritmo INT1 para la configuración del módulo Bluetooth.

Fuente: La autora.

Al presionarse el botón por primera vez, se enciende el LED1 poniendo al terminal 9 a nivel alto. De esta forma se indica que se está trabajando en el modo de configuración delos módulos HC-05. Posteriormente se desactiva la interrupción INT0 para evitar conflictos en caso de que se oprima el botón de configuración Wi-Fi por error.

Para entrar la modo de comandos AT, primero se des-energizan los módulos, se espera por 500 ms y configura el puerto Serie 0 para pasar a ejecutar un ciclo en espera de un número valido que indique cuál módulo se desea configurar. Una vez recibida esta información, pone un nivel alto en el terminal KEY del módulo correspondiente, se espera por 500ms y se energiza el módulo correspondiente.

Luego se pasa a ejecutar un ciclo en espera de recibir un comando, el cual es retransmitido al módulo HC-05 y posteriormente la respuesta de este se transmite a la PC. De este ciclo se sale al presionarse nuevamente el botón de configuración.

En la figura 3.16 se muestra el resultado de la simulación.

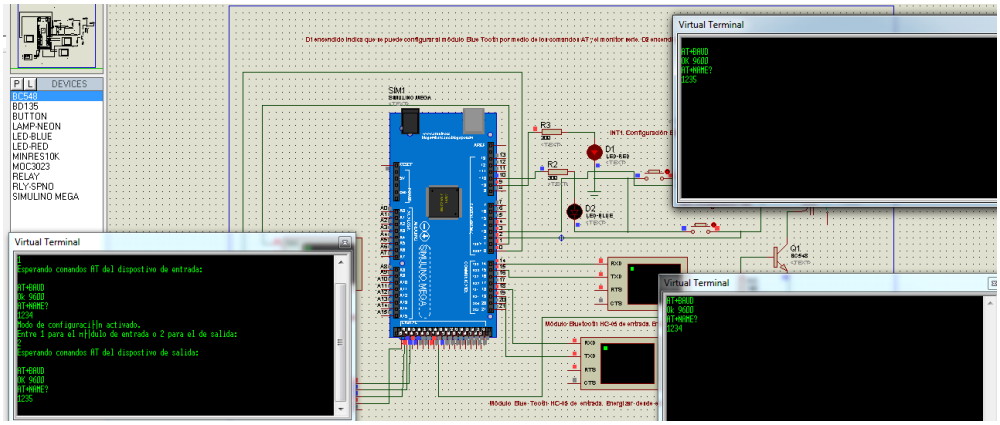


Figura 3.16: Simulación de la configuración por comandos AT.

Fuente: La autora.

- **Subrutina de la interrupción INT0:**

Se encarga de realizar la configuración delos datos de la red Wi-Fi. Estos datos son: nombre y contraseña de la red y nombre del dispositivo (número de cuatro dígitos). Por su parte informa de la dirección IP que debe tener la PC donde se ejecuta la aplicación servidor y el número del puerto a utilizar por la aplicación, además devuelve la dirección MAC de la tarjeta, necesaria para el filtrado por direcciones MAC a implementar en el router inalámbrico para lograr seguridad en la red.

La causa por la cual la dirección IP del servidor es predefinida radica en que el tipo de dato utilizado por el compilador de Arduino es único para este asistente y no es compatible con los tipos de datos que soporta la comunicación serie. Esto hace muy difícil la configuración desde la PC. Una solución es cambiar la dirección IP desde el asistente en el código del firmware para que el dispositivo quede programado con este dato.

Al igual que en el caso de la interrupción antes descrita, el dispositivo debe estar conectado a la PC donde se ejecuta la aplicación servidor por medio del puerto USB. Además el administrador debe presionar el botón correspondiente a esta función. En este caso no es necesario oprimir nuevamente el botón para salir del modo de configuración. El algoritmo se muestra en la figura 3.17. Como se puede observar es parecido al anterior, con la diferencia de que los datos se almacenan en la EEPROM por lo que no se explica en detalle. En la figura 3.18 se muestra el resultado de la simulación.

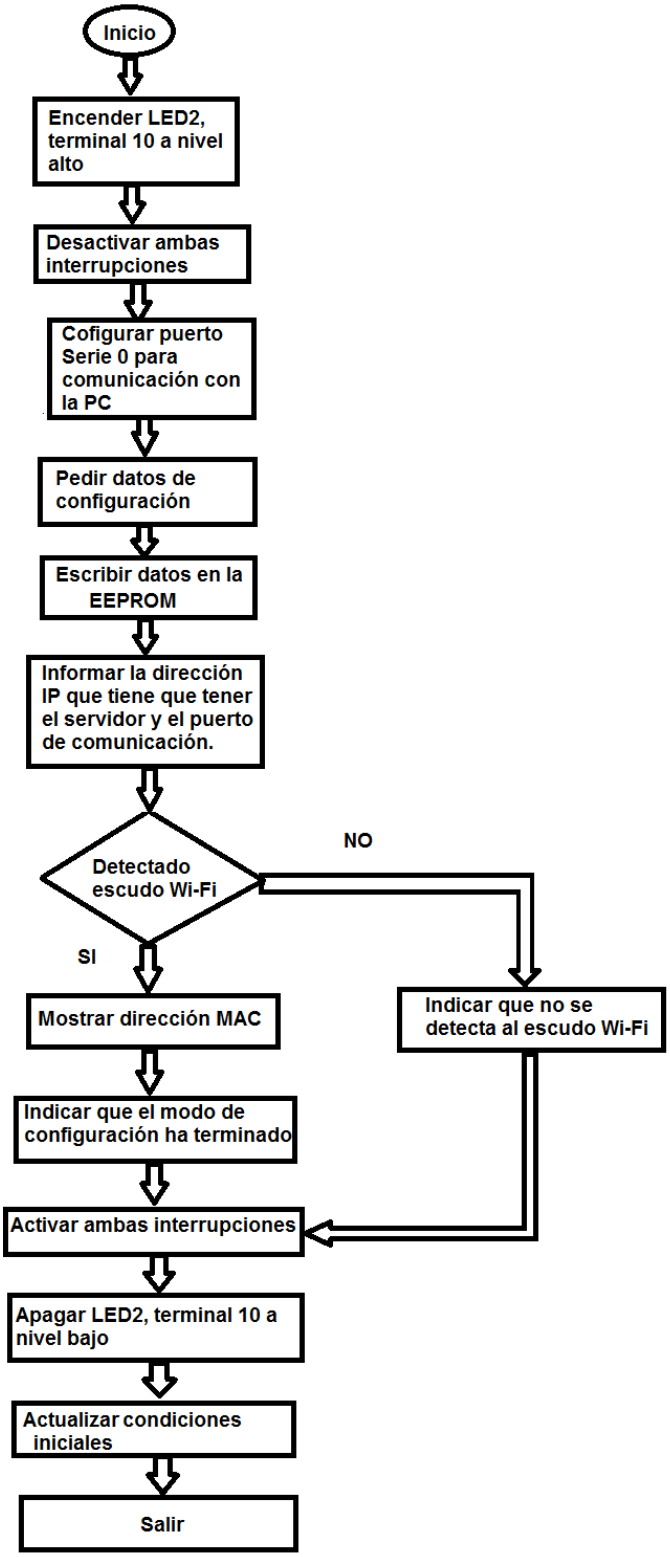


Figura 3.17: Algoritmo de la interrupción INT 0 para la configuración de la comunicación Wi-Fi.

Fuente: La autora.

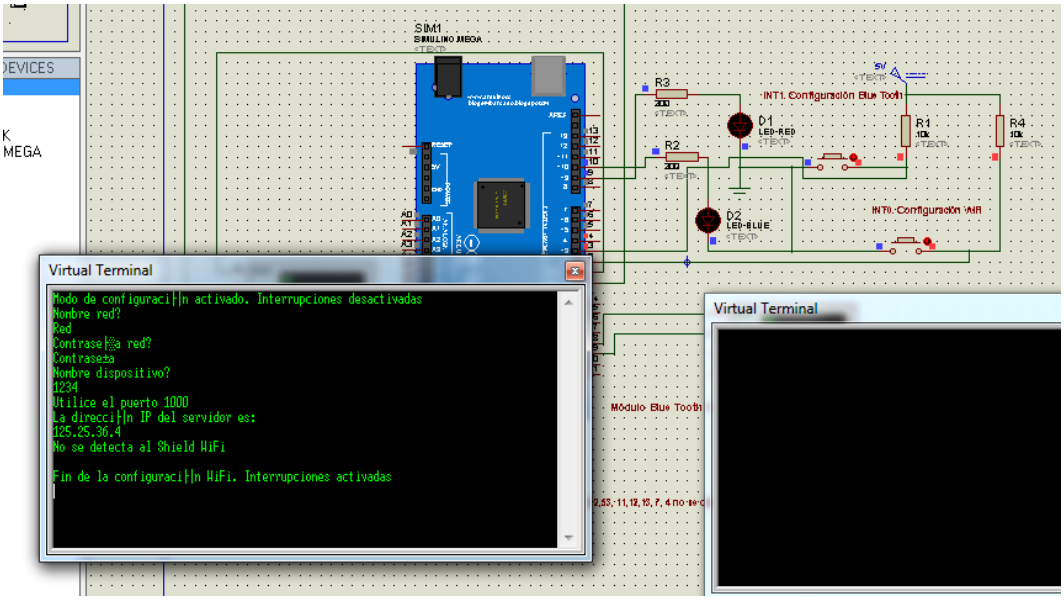


Figura 3.18: Simulación de la configuración de la comunicación Wi-Fi.

Fuente: La autora.

Capítulo 4: Software propuesto.

4.1. Introducción.

El software propuesto fue desarrollado en LabWindows/CVI que es un asistente para el desarrollo de aplicaciones de instrumentación virtual de National Instruments (National Instruments, 1999). Permite desarrollar aplicaciones con una interfaz gráfica para el usuario del programa por medio de objetos predefinidos, utiliza el lenguaje de programación C aunque hace referencia al uso de objetos propio del C++ de forma transparente al usuario. Posee una gran cantidad de librerías, bien documentadas y con ejemplos que se pueden encontrar en la ayuda o en los foros soportados en el sitio web de National Instruments (www.ni.com) lo cual lo hace muy potente.

4.2. El LabWindows/CVI.

Soporta comunicación por los puertos serie RS-232 y USB, por medio del protocolo TCP/IP y con bases de datos entre otras que no son utilizadas en este trabajo. También permite realizar la programación por medio de hilos o threads y todas las librerías de la norma ANSI C. Su filosofía de trabajo se basa en la ocurrencia de eventos. Un evento es un indicador de que ha ocurrido “algo” que saca al programa de un supuesto estado de reposo. Su equivalente más cercano en la electrónica son las interrupciones que existen en los microcontroladores.

Un evento es generalmente causado por una interacción del usuario de la aplicación con la interfaz gráfica de esta, aunque no está limitado a este caso. También pueden generarlos las comunicaciones por medio de puertos, el protocolo TCP o por el uso de temporizadores por poner tres ejemplos.

En la figura 4.1 se ilustra este principio. Cuando el usuario presiona el botón PLOTEAR ocurre un evento. De esta forma el compilador lo remite a una sección de código asociada a este botón y se ejecuta esta sección del programa, en este caso mostrar una forma de onda.

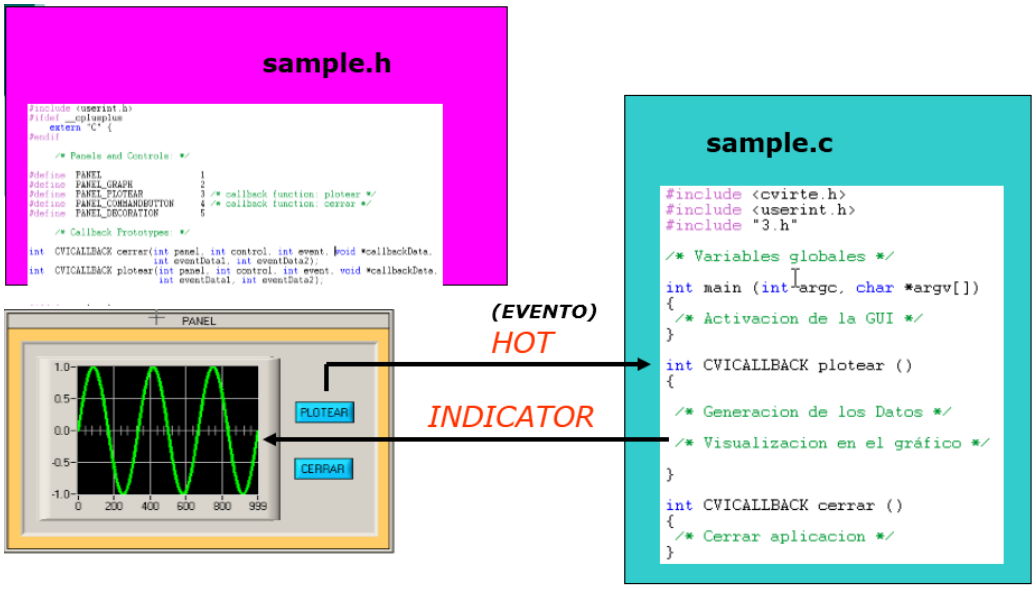


Figura 4.2: Filosofía de trabajo del LabWindows/CVI

Fuente: La autora.

4.3. Trabajo con bases de datos.

El trabajo con bases de datos se realiza por medio del SQL Toolkit (National Instruments, 1995). No es más que una librería que permite trabajar con bases de datos, sean estáticas o servidores, utilizando el lenguaje SQL (Structured Query Language). Este toolkit, no se instala por defecto al instalar el LabWindows, sino que hay que adquirirlo de forma independiente e instalarlo como un complemento.

La filosofía de trabajo con bases de datos se ilustra en la figura 4.2 por medio de las principales funciones de la herramienta.

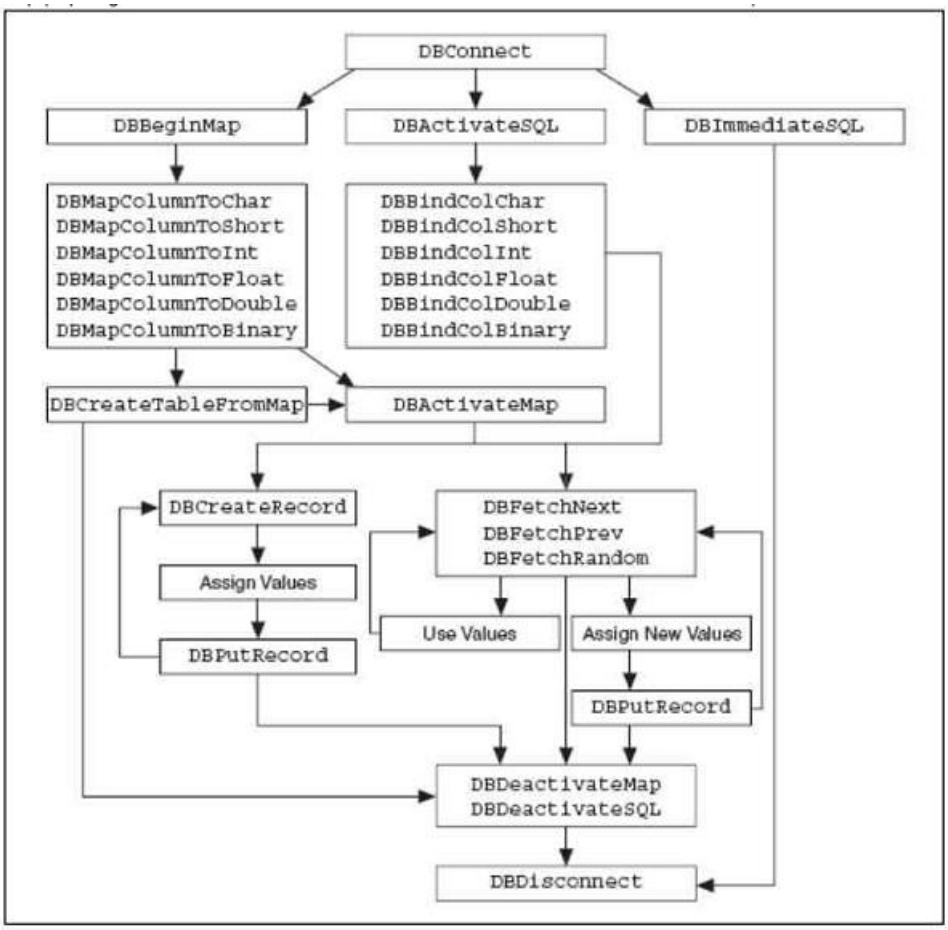


Figura 4.2: Filosofía de trabajo con bases de datos utilizando el SQL Toolkit
Fuente: https://decibel.ni.com/content/docs/DOC-39390.

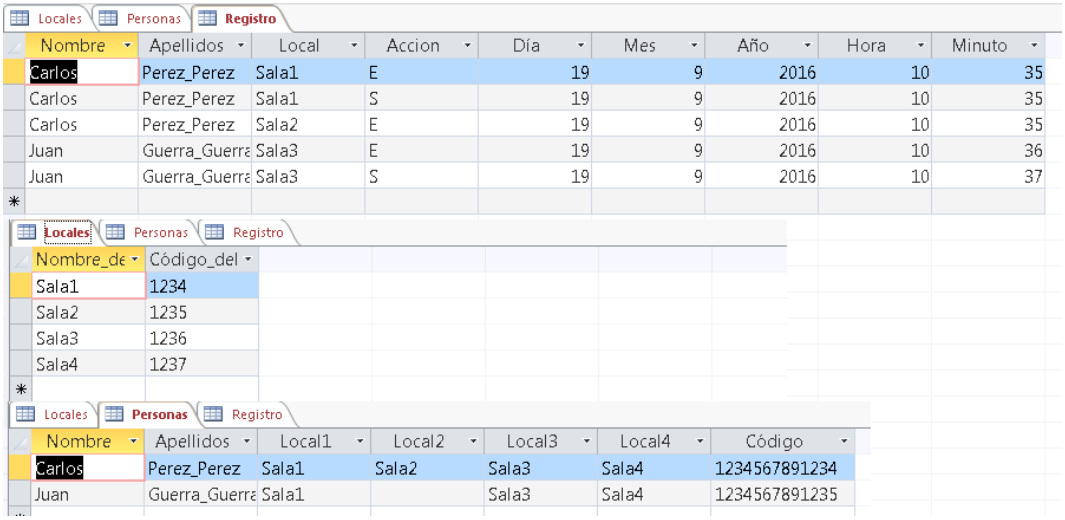
Una vez que se realiza la conexión a la base de datos, se debe confeccionar un mapa de la o las tablas que se desean utilizar o crearla si no existen. Posteriormente se debe activar la tabla y es en ese momento que se puede ingresar un nuevo registro, buscar un dato específico, modificar o eliminar los datos. El último paso debe ser desactivar las tablas y desconectarse de la base de datos.

La base de datos para este trabajo se desarrolló en Microsoft Access 2013 para sistemas operativos Windows de 32 bits. Consta de tres tablas:

- Personas: guarda nombre, apellidos, locales con acceso autorizado y código personal de las personas.

- Locales: guarda un código de 4 dígitos (no puede comenzar con el dígito cero) y el nombre del local.
- Registro: guarda nombre completo, fecha y hora en que una persona entra y sale de un local.

En la figura 4.3 se muestran las tablas creadas.



Locales | Personas | **Registro**

Nombre	Apellidos	Local	Accion	Día	Mes	Año	Hora	Minuto
Carlos	Perez_Perez	Sala1	E	19	9	2016	10	35
Carlos	Perez_Perez	Sala1	S	19	9	2016	10	35
Carlos	Perez_Perez	Sala2	E	19	9	2016	10	35
Juan	Guerra_Guerra	Sala3	E	19	9	2016	10	36
Juan	Guerra_Guerra	Sala3	S	19	9	2016	10	37

Locales | Personas | Registro

Nombre_de	Código_del
Sala1	1234
Sala2	1235
Sala3	1236
Sala4	1237

Locales | **Personas** | Registro

Nombre	Apellidos	Local1	Local2	Local3	Local4	Código
Carlos	Perez_Perez	Sala1	Sala2	Sala3	Sala4	1234567891234
Juan	Guerra_Guerra	Sala1		Sala3	Sala4	1234567891235

Figura 4.3: Tablas de la base de datos. De arriba hacia abajo: Registro, Locales y Personas.

Fuente: La autora.

4.4. Programación multi-hilos (multithreading) en LabWindows.

La capacidad aparente de los Sistemas Operativos de ejecutar varios programas o procesos, se ha visto incrementada con la aparición del concepto de hilos de ejecución. De eta forma, aplica un equivalente a la capacidad multitarea (impresión de que ejecuta varios programas de forma simultánea) a las aplicaciones. Bajo esta idea, en una misma aplicación se pueden ejecutar varias tareas de forma simultánea, en especial si se ejecutan en microprocesadores de varios núcleos ya que se ejecutan al mismo tiempo pero en núcleos diferentes.

El LabWindows/CVI brinda esta posibilidad mediante el uso de la librería Utility.h(National Instruments, 2002). Entre las principales ventajas que ofrecen las aplicaciones que emplean múltiples hilos se encuentran:

- Reducir el tiempo de interacción entre la interfaz gráfica y el usuario: mientras el programa está ejecutando un código, el usuario no puede acceder a los elementos de la interfaz visual dando la impresión de que el programa se ha bloqueado. Independientemente de que existen secciones de código de gran importancia, que tienen prioridad de ejecución, en muchos casos no es así por lo que se puede utilizar la capacidad multihilos.
- Mejora la eficiencia en la utilización del microcontrolador.

En aplicaciones como la atención a múltiples dispositivos, sean de adquisición, o de comunicación (por ejemplo la comunicación entre un servidor y múltiples clientes) se hace indispensable su uso para poder atender a todos los dispositivos evitando pérdida de información por estar dedicado a otra tarea. En la figura 4.4 se muestra un ejemplo del uso de hilos en una aplicación Android.

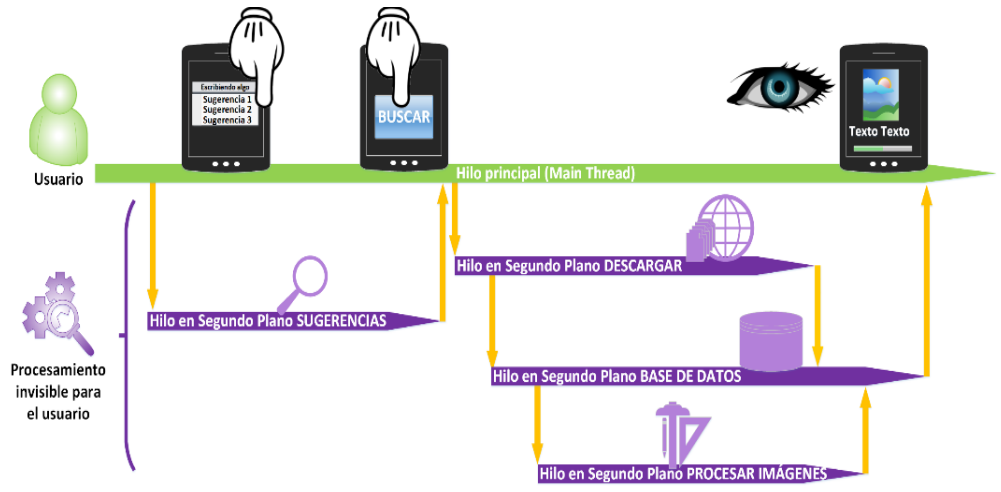


Figura 4.4: Ejemplo del uso de hilos en una aplicación Android

Fuente: Ramón Invarato, 2013

En esta figura se observa que el hilo principal se encarga de procesar los eventos relacionados con la interfaz de usuario, mientras que existen varios hilos secundarios para el control de las aplicaciones de segundo plano como acceso a base de datos, descarga de datos desde internet o para procesar imágenes.

4.5. Software servidor.

Este software se ejecuta en una PC y tiene que garantizar:

- Seguridad, no se puede cambiar la configuración de los dispositivos, ni acceder a la base de datos sin autenticarse.
- Conexión a la base de datos y a los dispositivos remotos (clientes TCP) aunque no se registre un administrador.
- Agregar y/o eliminar usuarios o locales en la base de datos.
- Visualizar los registros de la base de datos.

Para esto se ejecutan una serie de subrutinas en dependencia de las acciones que se ejecutan. A continuación se explican los más representativos.

4.6. Estableciendo las condiciones iniciales.

El algoritmo es el mostrado en la figura 4.5. Lo primero es definir al sistema operativo que se trata de una aplicación que se desempeña como servidor. A continuación se chequea si existe la base de datos, en caso de que no exista se crean las tablas. Una vez que se garantiza que la base de datos exista, se procede a conectarse a ella y se lanza la interfaz de usuario. Dicha interfaz se muestra en la figura 4.6. Se puede ver que cuenta con una serie de opciones en un menú pero no se encuentran activas ya que no se ha procedido a conectarse como administrador.

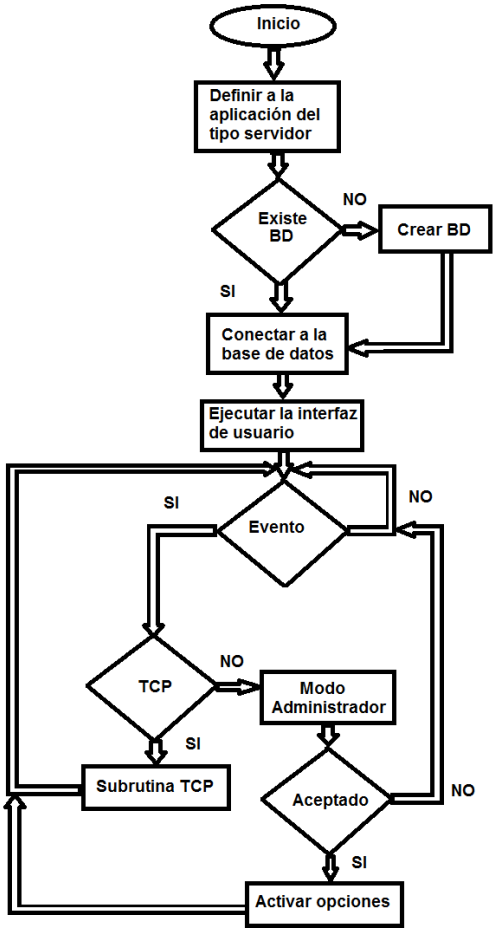


Figura 4.5: Algoritmo para establecer las condiciones iniciales.

Fuente: La autora.

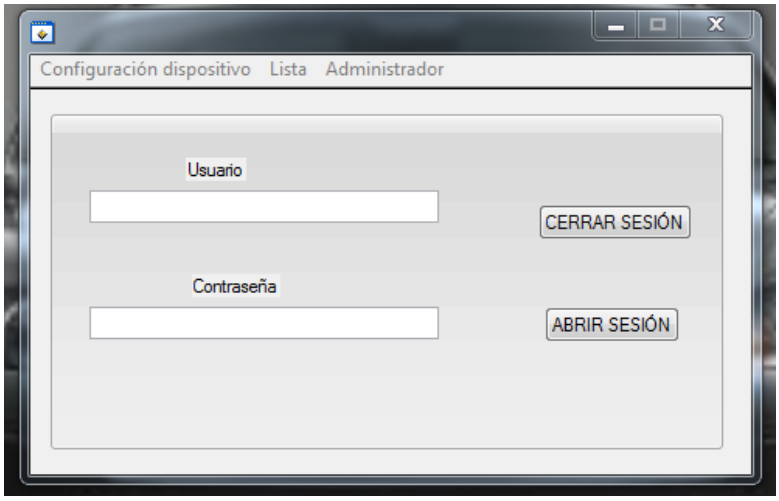


Figura 4.6: Ventana principal de la interfaz de usuario.

Fuente: La autora.

Una vez que se ejecuta la interfaz de usuario, las condiciones iniciales están establecidas. Queda esperar por que ocurra un evento. Los eventos pueden ser de tipo TCP (relacionados con la conexión Wi-Fi con los dispositivos clientes) o que el administrador se registre en el programa. En caso de que el usuario y contraseña sean válidas se procede a activar las opciones del menú.

Se pueden cambiar tanto el nombre del usuario y la contraseña, pero si se cambia esta última también es preciso hacerlo en la base de datos pues de lo contrario el programa no se podrá conectar a esta.

4.7. Subrutina TCP.

El algoritmo de la subrutina TCP se muestra en la figura 4.7.El LabWindows define 4 tipos de eventos TCP: conexión, recepción de datos, transmisión de datos y desconexión. En el caso de conexión y desconexión son interpretadas de forma distinta en dependencia de si se trata de una aplicación cliente o servidor. En el caso del servidor (que es la aplicación que se implementa) se interpreta como que el cliente solicita conectarse o que se ha cerrado la aplicación cliente respectivamente.

Al ejecutar la subrutina lo primero es identificar el evento ocurrido. Si se trata de un evento de conexión al cliente se toma nombre y dirección IP, posteriormente se crea un hilo para controlar de forma unívoca la conexión con el cliente y se agregan sus datos a una lista de clientes. En caso de que se trate de una desconexión, se libera el hilo de ejecución y se elimina al cliente de la lista.

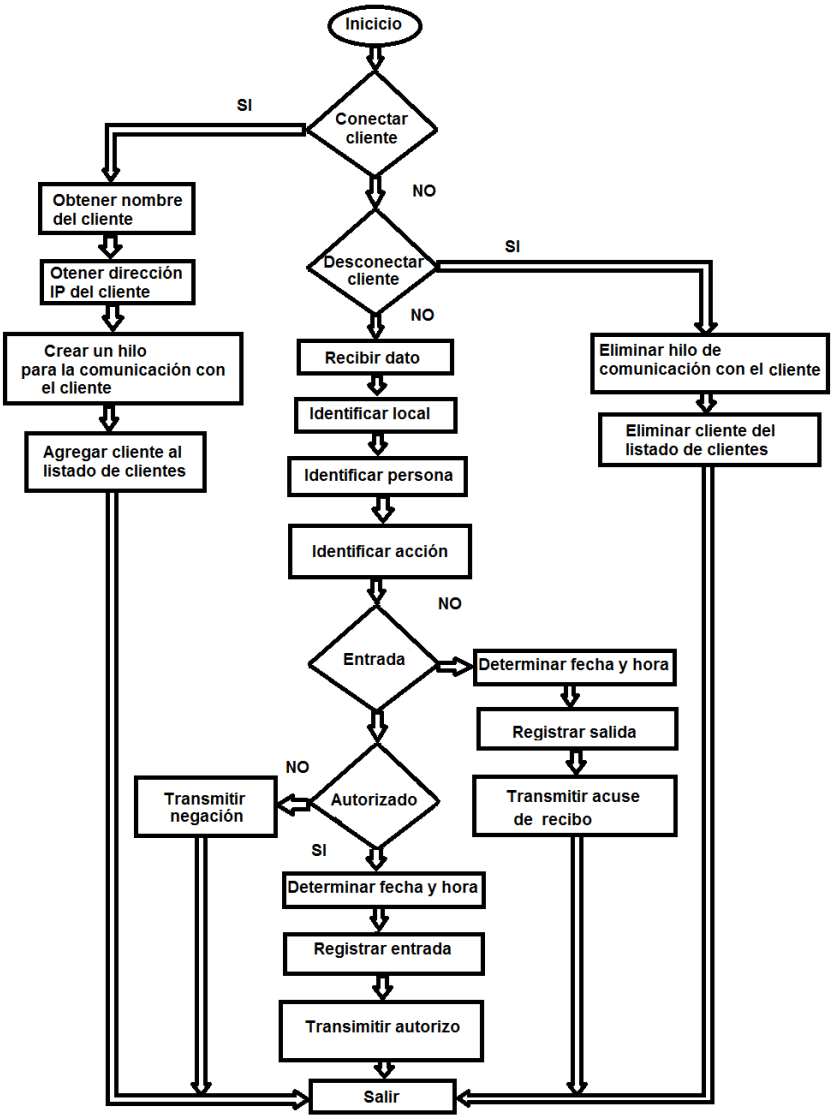


Figura 4.7: Subrutina TCP.

Fuente: La autora.

El otro evento posible es que se reciba un dato. En este caso se identifica el local en que se encuentra el dispositivo a partir del código asignado a este y que se encuentra en la base de datos; y el nombre de la persona a partir del código personal de cada una. Luego se pasa a identificar la acción: si se trata de una entrada o una salida del local. En caso de que se trate de una salida, se determina fecha y hora, se actualiza la tabla Registros y se envía un acuse de recibo. En caso de que se trate de una entrada, se valida si la persona tiene acceso al local, en caso de no tener permiso se transmite una negación de autorizo. Si se

encuentra autorizada se determina fecha y hora, se actualiza la base de datos y se transmite un autorizo.

4.8. Editar personas y locales.

Se trata del mismo algoritmo aplicado a dos entidades distintas por lo que se explica uno solo a partir de la edición de personas. Se muestra en la figura 4.8.

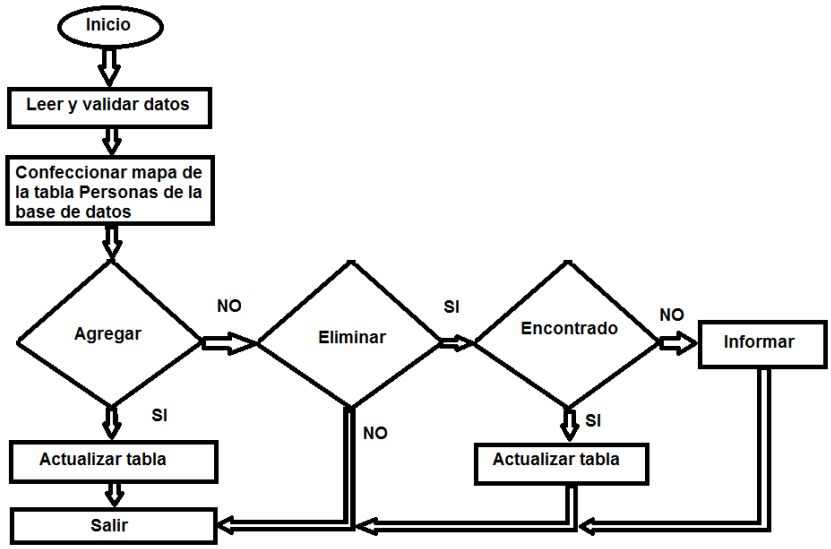


Figura 4.8: Subrutina para editar la tabla Personas.

Fuente: La autora.

Lo primero es leer y validar los datos. En este caso hay que garantizar que el código asignado a la persona tenga 13 caracteres (cuatro para los locales). Una vez realizado esto se determina si se desea agregar a la persona, eliminarla o cancelar la operación. Si es agregar se actualiza la tabla. En el caso de eliminar, se busca a la persona comprobando que todos los datos sean coincidentes con la base de datos, en caso de que así sea se elimina, en caso contrario se muestra un mensaje de error.

En la figura 4.9, de izquierda a derecha se muestra el menú con las opciones de edición, la ventana correspondiente a la edición de personas y la ventana para la edición de locales.

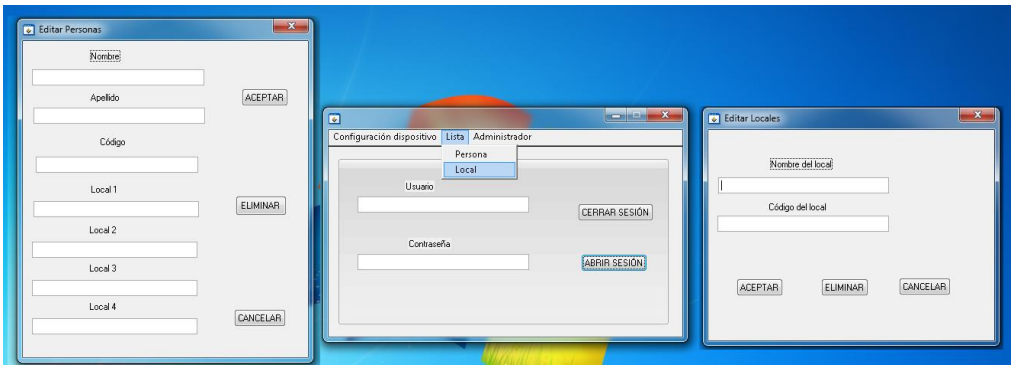


Figura 4.9: Ventanas para la edición de personas y locales.

Fuente: La autora.

4.9. Mostrar datos.

En la figura 4.10 se muestra el algoritmo que ilustra el proceso para presentar la información almacenada en la base de datos.

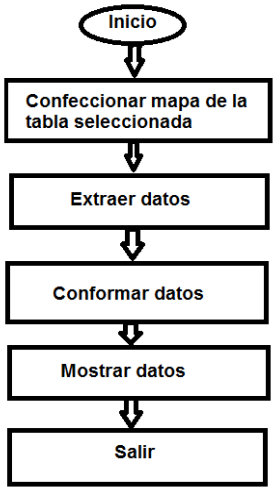


Figura 4.10: Algoritmo para la presentación de la información almacenada.

Fuente: La autora.

Primero se identifica se confecciona el mapa de la base de datos, específicamente de la tabla Registro, se ajusta la información al tipo de dato que soporta la interfaz de visualización y finalmente se muestra.

4.10. Comprobación del funcionamiento de la propuesta.

Este trabajo es una propuesta de diseño, por lo que el funcionamiento se comprueba por bloques. En la figura 4.11 se observa el funcionamiento de la visualización de la información de la base de datos, específicamente la tabla Registro.

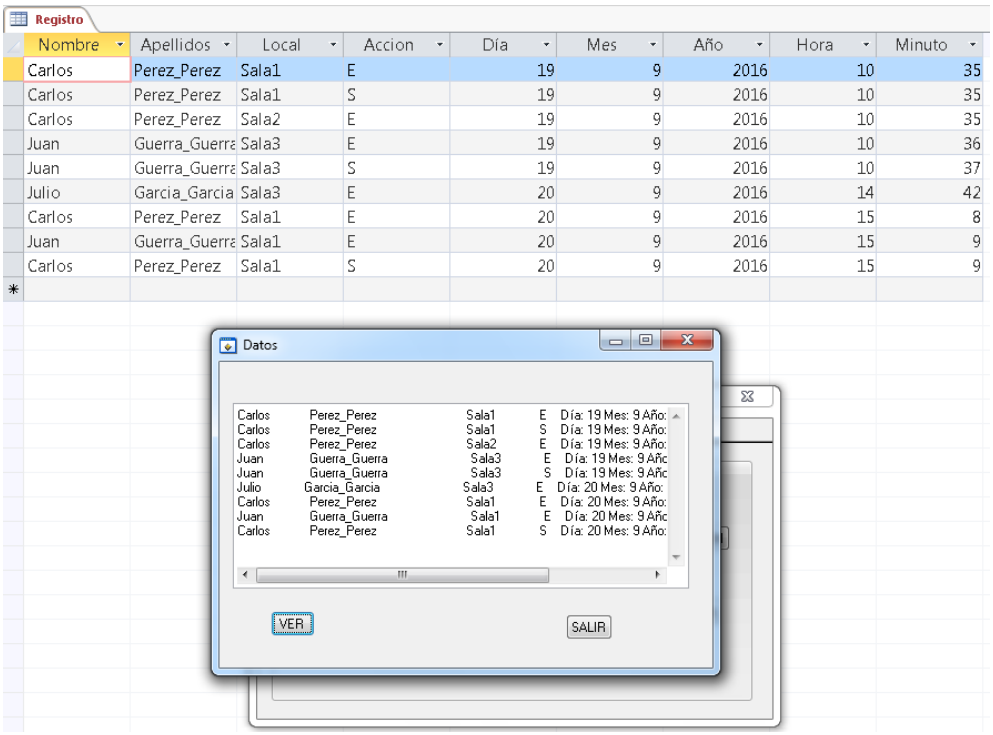


Figura 4.11: Comprobación de la visualización de la información.

Fuente: La autora.

En la figura 4.12 se puede observar los datos de dos personas de la tabla Personas, y los datos de una tercera que se va a introducir. En la figura 4.13, se observa que estos datos ya se han introducido actualizando la tabla.

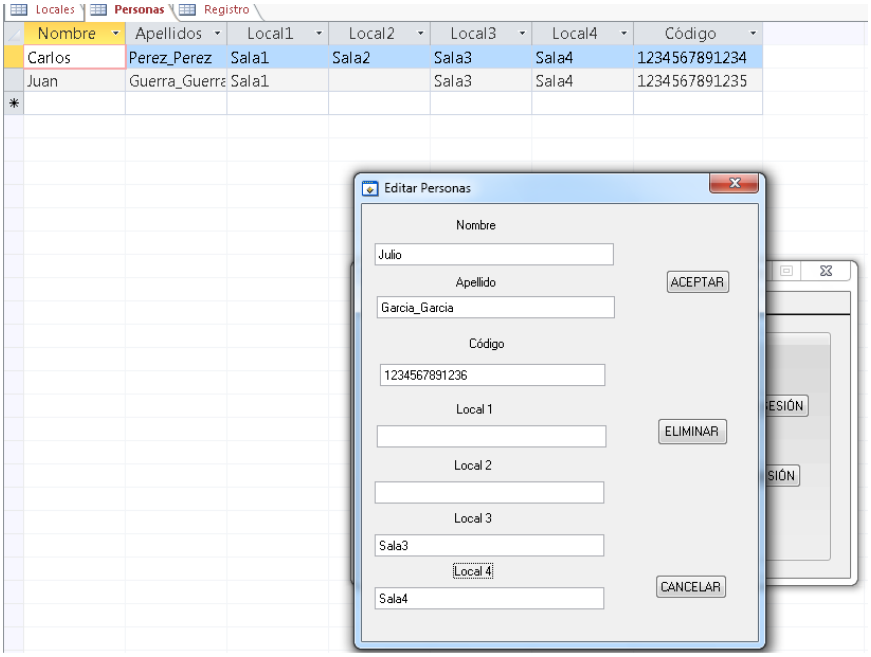


Figura 4.12: Entrada de datos de una persona. En la tabla solo se tienen dos entradas

Fuente: La autora.

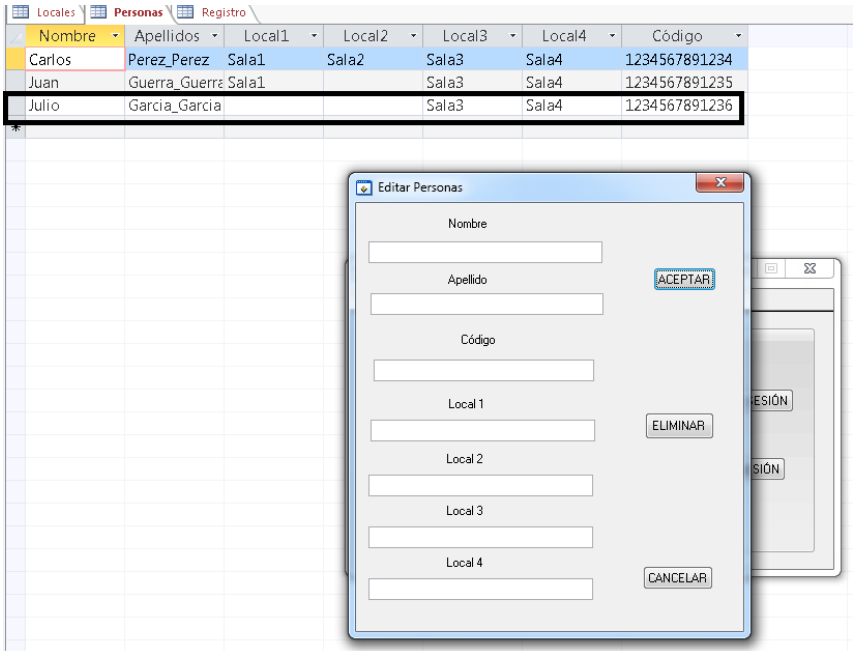


Figura 4.13: Se observa que los datos de la persona se introdujeron en la tabla.

Fuente: La autora.

En las figura 4.12 y 4.13, se comprueba el acceso a la tabla Registros para introducir datos recibidos por comunicación TCP. Para ello se desarrolla una aplicación cliente en el LabWindows (la interfaz aparece

en la figura en la parte inferior). En la figura 4.14 se intenta acceder a un local pero no se concede el permiso (se transmite la letra B) por lo que no se incluye en la base de datos. En la figura 4.15 sí se autoriza la entrada (se transmite la letra A) lo que aparece como una entrada en la tabla Registros.

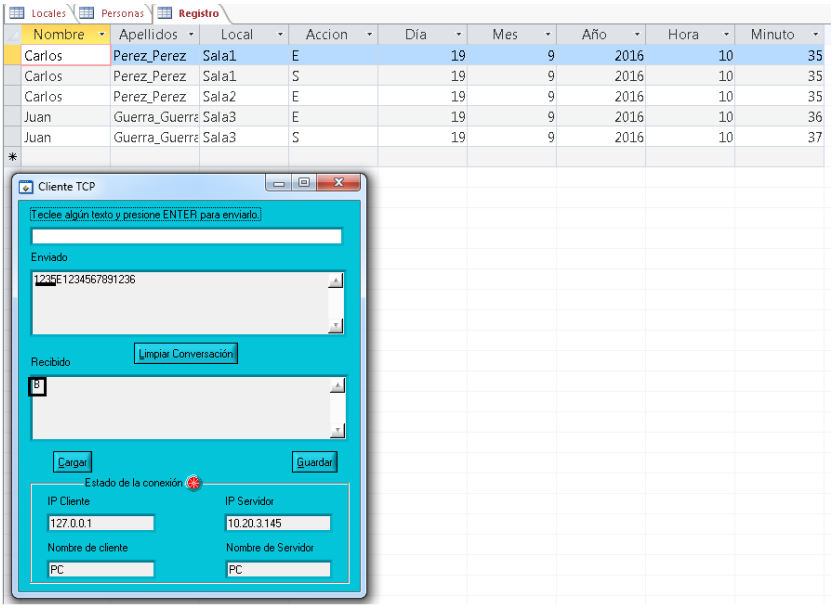


Figura 4.14: Registro de datos recibidos por el protocolo TCP. La persona con el código 1234567891236 no está autorizada a entrar en el local 1235 por lo que se recibe el comando B y no se introduce en la base de datos.

Fuente: La autora.

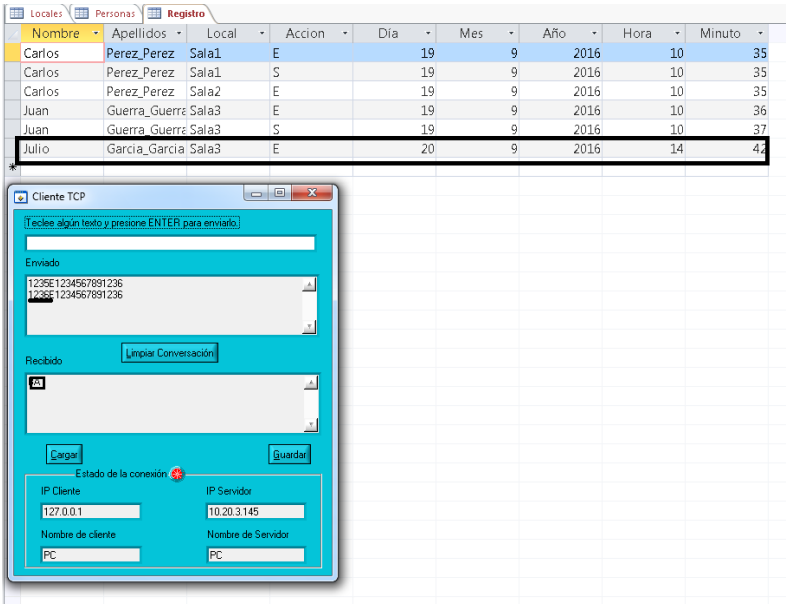


Figura 4.15: Registro de datos recibidos por el protocolo TCP. La persona con el código 1234567891236 está autorizada a entrar en el local 1236 por lo que se recibe el comando A y se introduce en la base de datos.

Fuente: La autora.

En la figura 4.16se observa el funcionamiento de la comunicación serie, con un Arduino Mega 2560, simulando la configuración de los datos de la red Wi-Fi.

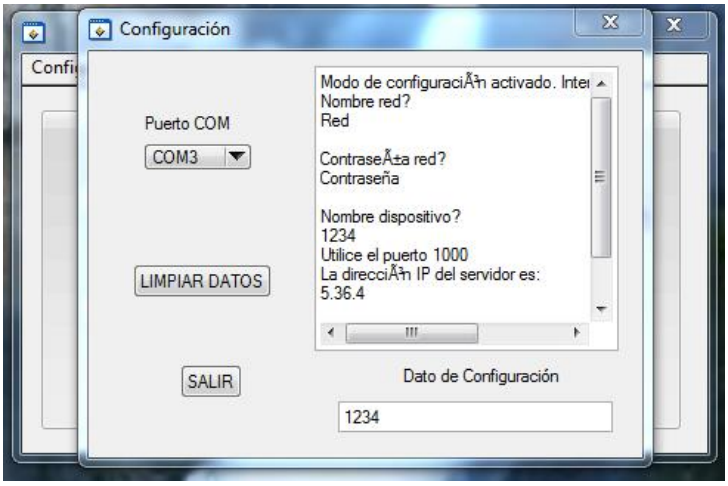


Figura 4.16: Comunicación serie para configurar los datos de la red Wi-Fi.

Fuente: La autora.

Conclusiones.

- Se presentó una propuesta de sistema de control de acceso para las empresas a las que SeguMedik ofrece el servicio de seguridad ocupacional.
- Se propone un sistema para la lectura del código de barra del documento de identificación de la persona que quiere acceder o salir de un determinado departamento.
- Se confeccionó una base de datos con la información del personal que labora en cada departamento.
- Se propone un sistema que permita comparar la lectura del código de barra del documento de identificación de la persona que quiere acceder o salir de un determinado departamento con la base de datos confeccionada para este fin.
- Se propone un sistema para activar o no el mecanismo de apertura de la puerta en función de la validez de la identificación.
- Se propone un sistema que almacena, en una base de datos, la entrada y salida del personal que labora en la instalación con vistas a cuantificar la estancia en su puesto de trabajo.

Recomendaciones.

Para la implementación del proyecto presentado se recomienda:

- Realizar un análisis económico.
- Presentar al cliente la propuesta y su costo.
- Poner el proyecto en etapa de pruebas.
- Realizar las correcciones y cambios pertinentes de acuerdo con el cliente.
- Terminar la fase de implementación del proyecto.

Referencias Bibliográficas

- Arduino. (2015). Arduino Mega 2560. Consultado en abril 2016, disponible en: http://arduino.cc/en/Main/arduinoBoardMega2560
- Arduino. (2015). WiFi library. Consultado en: mayo 2016, disponible en: https://www.arduino.cc/en/Reference/WiFi
- Arduino. (2016). Arduino WiFi Shied. Consultado en: mayo 2016, disponible en: https://www.arduino.cc/en/Main/ArduinoWiFiShield
- Blue Star. Your Solutions Distribuitor. (2014). Soluciones AIDC. Madrid, España. Consultado en: mayo 2016
- Datalogic. (2004). Gryphon BT Reference Manual. (Datalogic, Ed.) Bolonia, Italia. Consultado en: julio 2016
- Guangzhou HC Information Technology Co., Ltd. (n.d.). HC Serial Bluetooth Products. User Instructional Manual. Consultado en: junio 2016, disponible en: www.wavesen.com
- ITeadStudio. (2010). HC-05 Bluetooth to Serial Port Module. Consultado en: junio 2016, disponible en: www.iteadstudio.com
- National Instruments. (1995). LabWindows/CVI SQL Toolkit Reference Manual. Austin, Texas, USA.
- National Instruments. (1999). The Meassurement Revolution. (N. I. Corporation, Ed.) Austin, Texas, United States of America: National Instruments Corporation.
- National Instruments. (2002). Building Multithreading Applications with LabWindos/CVI. Consultado en: julio 2016, disponible en: http://200.126.14.82/web/NationalInstruments/Instrupedia/nstrupedia
- National Instruments. (2008). Building Networked Applications with the LabWindows™/CVI™ TCP Support Library.Consultado en: Julio 2013, disponible en: www.ni.com
- National Instruments. (2008). Multithreading in LabWindows™/CVI™.Consultado en: Julio 2013, disponible en: www.ni.com

- National Instruments. (2016). Connecting to a Database. Consultado en: julio 2016, disponible en: http://zone.ni.com/reference/en-XX/help/370502D-01/cvisqlref/
- NoMADA. (2015). Bluetooth Comercial HC-05. Consultado en: junio 2016, disponible en: http://nomada-e.com
- TP-Link Technologies. (2012). TP-Link TL-WR720N 150Mps Wireless Router User Guide. doi: www.tp-link.com
- Wójick, J. (2011). The conception and the implementation of control systems for servomotor with application of wireless networks. Master´s Thesis. (A. U. Technology, Ed.) Krákow, Poland. Consultado en: abril 2016

Glosario

ANSI C: American National Standards Institute, Instituto Nacional Estadounidense de Estándares

DHCP: Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host

EEPROM: Electrically Erasable Programmable Read-Only Memory, ROM Programable y Borrable Eléctricamente.

ICSP: In-Circuit Serial Programming, Programación serial en circuito.

MAC: Media Access Control, Control de Acceso al Medio.

SD: Secure Digital, Seguro Digital.

SPI: Serial Peripheral Interface, Interfaz Periférica Serial

SQL: Structured Query Language. Lenguaje de Consulta Estructurada.

SRAM: Static Random Access Memory, Memoria Estática de Acceso Aleatorio.

TCP/IP: Transmission Control Protocol/Internet Protocol Protocolo de Control de Transmisión/Protocolo de Internet.

TTL: Transistor-Transistor Logic, Lógica Transistor-Transistor

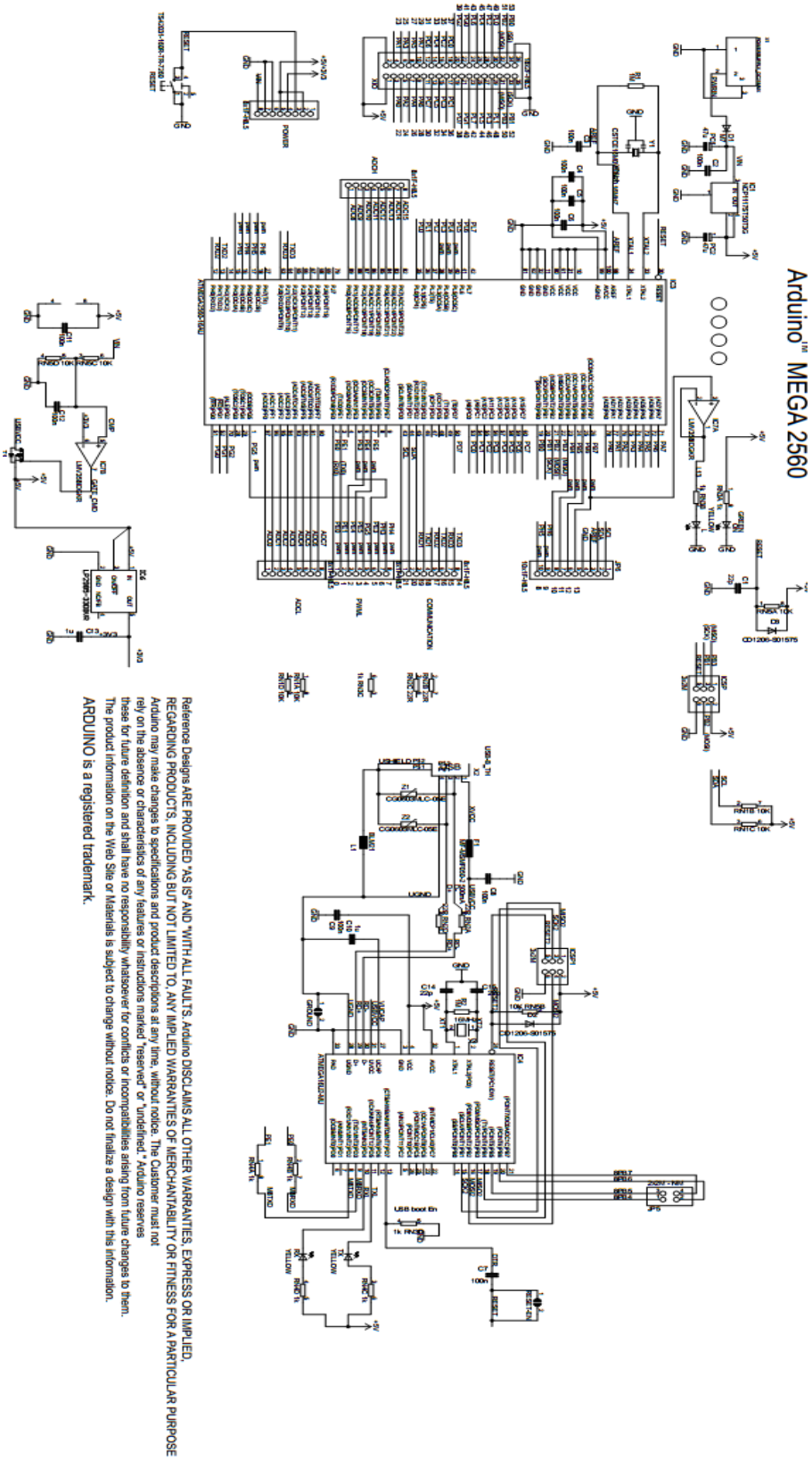
USB: Universal Serial Bus, Bus Universal en Serie.

WEP: Wired Equivalent Privacy, Privacidad Equivalente a Cableado.

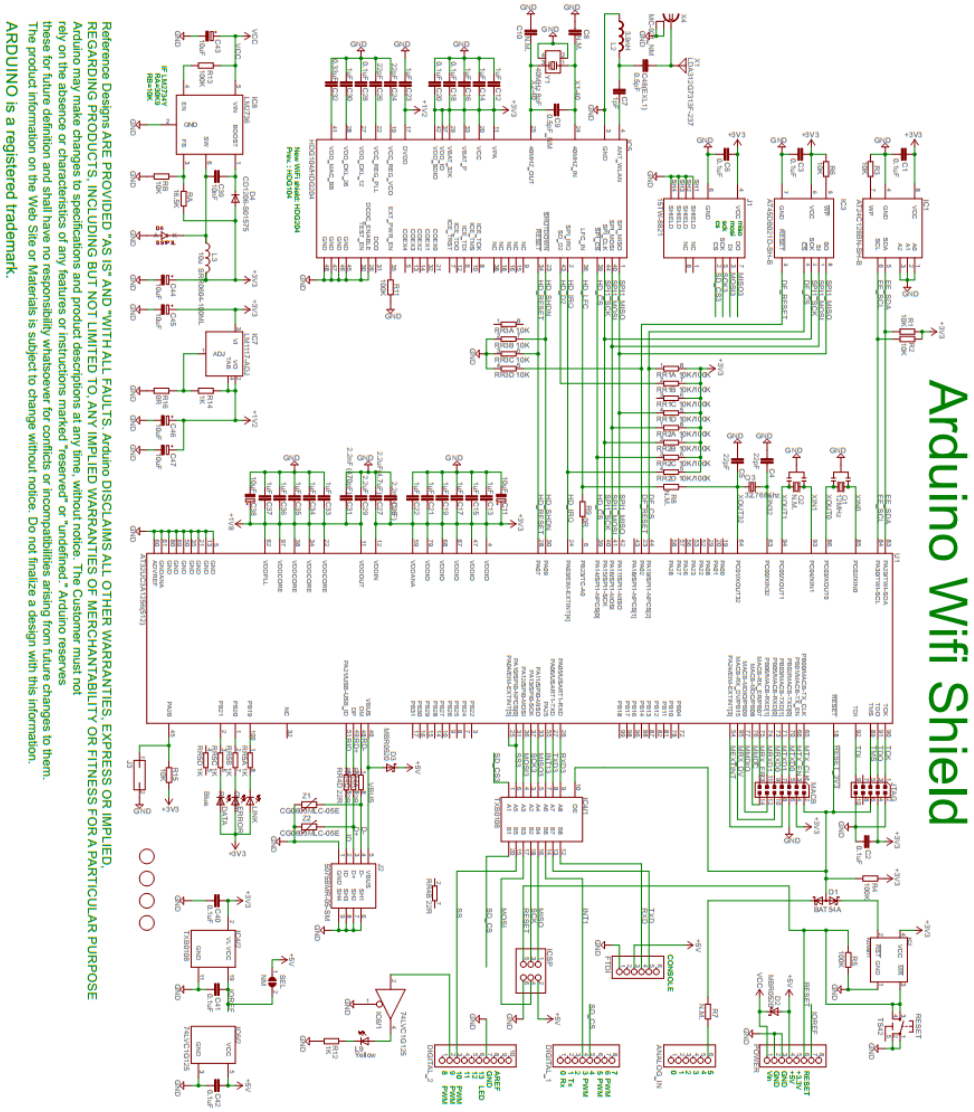
Wi-Fi: Wireless Fidelity, Fidelidad Inalámbrica.

WPA2: Wi-Fi Protected Access 2, Acceso Protegido Wi-Fi 2.

Anexo 1 Esquemático del Arduino Mega 2560



Anexo 2 Esquemático del Arduino WiFi Shield



Anexo 3 Códigos de barras para configurar el lector

Restore GRYPHON™ BT Default

Set Gryphon™ BT as Slave

Restore Gryphon™ BT default

Set Gryphon™ BT as Master

Enter configuration

Set Remote Bluetooth® Device Address (slave)

+

12 characters for the remote Bluetooth® device address specified in each Bluetooth® device.

Exit and Save configuration

Request Radio Connection with Slave

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Bohórquez Heras, Diana Carolina**, con C.C: # **0921686507** autor/a del trabajo de titulación: **Sistema automático para el registro del personal de la Empresa SeguMedik** previo a la obtención del título de **Magíster en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, a los 20 días del mes de Febrero del año 2017

f. _____

Nombre: **Bohórquez Heras Diana Carolina**

C.C: # 0921686507

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Sistema automático para el registro del personal de la Empresa SeguMedik		
AUTOR(ES)	Bohórquez Heras Diana Carolina		
REVISOR(ES)/TUTOR(ES)	MSc. Luis Córdova Rivadeneira, MSc. Orlando Philco Asqui, MSc. Daniel Garrido Rodríguez		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
CARRERA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magíster en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	20 de Febrero de 2017	**No. DE PÁGINAS:**	58
ÁREAS TEMÁTICAS:	Sistemas de identificación de personas, códigos de barras, lectores de código de barra, Plataforma Arduino Mega 2560, Módulo Bluetooth HC-05, LabWindows/CVI.		
PALABRAS CLAVES/ KEYWORDS:	SeguMedik, Código de barra, Arduino Mega, Escudo inalámbrico		
RESUMEN/ABSTRACT (150-250 palabras): En este trabajo se presenta una propuesta de sistema de control de acceso para las empresas a las que SeguMedik ofrece el servicio de seguridad ocupacional. El sistema, se basa en la lectura del código de barra del documento de identificación de la persona que quiere acceder o salir de un determinado local. Utilizando el Arduino Mega con un escudo inalámbrico, envía esa información a un servidor para que la compare con la base de datos confeccionada para este fin. Para permitir la entrada a un determinado local, si la coincidencia es positiva, actúa sobre el mecanismo de apertura de la puerta y registra en la base de datos, fecha y hora de entrada de la persona autorizada. Si no hay coincidencia, el sistema mantiene la puerta cerrada. Para controlar la salida y el tiempo de estancia, de la persona ya autentificada, el personal dentro del local debe presentar y validar su documento de identificación para accionar el mecanismo de apertura de la puerta y que se registre en la base de datos la fecha y hora de salida.			
ADJUNTO PDF:	☒ SI	☐ NO	
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-993247157	E-mail: diana_y2k15@hotmail.com	
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE):	**Nombre:** Manuel de Jesús Romero Paz		
	Teléfono: +593-4-2202935 / 0994606932		
	E-mail: manuel.romero@cu.ucsg.edu.ec / mromeropaz@yahoo.com		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			