



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE
COMUNICACIÓN**

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN**

TEMA

**SISTEMA DE CONTROL DE ACCESO Y MONITOREO DE ESTUDIANTES CON
EL USO DE TECNOLOGÍA INALÁMBRICA DE IDENTIFICACIÓN AUTOMÁTICA
(RFID) EN LA UNIVERSIDAD TÉCNICA DEL NORTE.**

AUTOR: EMERSON GABRIEL HARO FLORES.

DIRECTOR: Ing. CARLOS VÁSQUEZ A.

Ibarra-Ecuador

2016



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, determinó 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:	100329282-6		
APELLIDOS Y NOMBRES:	Haro Flores Emerson Gabriel		
DIRECCIÓN:	Quiroga – Vía principal al lago		
E-MAIL:	egharo@utn.edu.ec		
TELÉFONO MÓVIL:	0986566591	TELÉFONO FIJO:	062-565-010
DATOS DE LA OBRA			
TÍTULO:	SISTEMA DE CONTROL DE ACCESO Y MONITOREO DE ESTUDIANTES CON EL USO DE TECNOLOGÍA INALÁMBRICA DE IDENTIFICACIÓN AUTOMÁTICA (RFID) EN LA UNIVERSIDAD TÉCNICA DEL NORTE.		
AUTOR:	Emerson Gabriel Haro Flores		
FECHA:	2016/11/30		
PROGRAMA:	<input checked="" type="checkbox"/> Pregrado <input type="checkbox"/> Postgrado		
TÍTULO:	Ingeniero en Electrónica y Redes de Comunicación		
DIRECTOR:	Ing. Carlos Vásquez		

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Emerson Gabriel Haro Flores, con cédula de identidad Nro. 100329282-6, en calidad de autor 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 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 30 días del mes de noviembre del 2016

EL AUTOR:

Firma: 

Nombre: Emerson Gabriel Haro Flores



UNIVERSIDAD TÉCNICA DEL NORTE

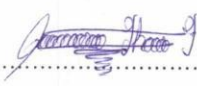
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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

Yo, Emerson Gabriel Haro Flores, con cedula de identidad Nro. 100329282-6, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador artículos 4, 5 y 6, en calidad de autor del trabajo de grado con el tema: SISTEMA DE CONTROL DE ACCESO Y MONITOREO DE ESTUDIANTES CON EL USO DE TECNOLOGÍA INALÁMBRICA DE IDENTIFICACIÓN AUTOMÁTICA (RFID) EN LA UNIVERSIDAD TÉCNICA DEL NORTE. Que ha sido desarrollado con propósito de obtener el título de Ingeniero en Electrónica Redes de Comunicación de la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, a los 30 días del mes de noviembre del 2016

Firma:

Nombre: Emerson Gabriel Haro Flores

Cédula: 100329282-6



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Emerson Gabriel Haro Flores con cédula de identidad Nro. 100329282-6, estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro que el presente trabajo de investigación, es de mi autoría y no ha sido realizado, ni calificado por otro profesional, para efectos académicos y legales será de mi responsabilidad.

Firma: 

Nombre: Emerson Gabriel Haro Flores

Cedula: 100329282-6



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico, que el presente trabajo de Titulación “SISTEMA DE CONTROL DE ACCESO Y MONITOREO DE ESTUDIANTES CON EL USO DE TECNOLOGÍA INALÁMBRICA DE IDENTIFICACIÓN AUTOMÁTICA (RFID) EN LA UNIVERSIDAD TÉCNICA DEL NORTE” ha sido desarrollado por el señor Emerson Gabriel Haro Flores bajo mi supervisión.

A handwritten signature in blue ink, appearing to read 'Carlos Vásquez A.', is positioned above a horizontal dotted line.

Ing. Carlos Vásquez A.
DIRECTOR DE TESIS

DEDICATORIA

Dedico este proyecto de titulación principalmente a mis padres, Carlos y Elva, que han sido y serán siempre el pilar fundamental en mi vida, y que con su ejemplo de responsabilidad y perseverancia han sabido brindarme su apoyo incondicional para el cumplimiento de los objetivos propuestos.

A mi hermana Viviana que siempre ha estado junto a mí, a toda mi familia y amigos que me han brindado su apoyo y confianza, y se han convertido en parte fundamental de mi vida.

Emerson Gabriel Haro Flores

AGRADECIMIENTOS

De manera muy especial agradezco a la Universidad Técnica del Norte por acogerme en sus aulas y brindar todas las herramientas necesarias en el proceso de aprendizaje, promoviendo valores éticos y morales con el fin de generar profesionales de alto conocimiento.

De igual forma agradezco a la Facultad de Ingeniería en Ciencias Aplicadas y a la Carrera de Ingeniería en Electrónica y Redes de Comunicación, a sus autoridades y representantes, que día a día trabajan en mejora de nuestra educación.

Agradezco al Ing. Carlos Vásquez por su tiempo y ayuda prestada para la elaboración de este proyecto, por todos sus consejos y seguimiento constante para la culminación del mismo.

Al Ing. Jaime Michilena y a todos los docentes de la carrera por haber compartido su conocimiento y prestar su ayuda dentro y fuera de las aulas.

A la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, que abrió sus puertas y permitió realizar mi trabajo de titulación en sus instalaciones.

Emerson Gabriel Haro Flores

ÍNDICE DE CONTENIDO

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD	
TÉCNICA DEL NORTE.....	I
DEDICATORIA.....	VI
AGRADECIMIENTOS.....	VII
ÍNDICE DE CONTENIDO	VIII
ÍNDICE DE FIGURAS	XIV
ÍNDICE DE TABLAS.....	XX
ÍNDICE DE ECUACIONES.....	XXII
RESÚMEN.....	XXIII
ABSTRACT	XXIV
PRESENTACIÓN	XXV
CAPÍTULO I.....	1
1. ANTECEDENTES.....	1
1.1. PROBLEMA	1
1.2. JUSTIFICACIÓN.....	2
1.3. OBJETIVOS.....	3
1.3.1. General.....	3
1.3.2. Específicos.....	3

1.4. ALCANCE	4
CAPÍTULO II.....	7
FUNDAMENTACIÓN TEÓRICA	7
2.1 SISTEMAS DE CONTROL DE ACCESO	7
2.1.1 Funcionamiento de un Sistema de Control de Acceso	7
2.1.2. Componentes de un Sistema de Control de Acceso	8
2.1.3. Sistemas de Identificación	9
2.2. IDENTIFICACIÓN POR RADIOFRECUENCIA	14
2.3. SISTEMA RFID	15
2.3.1. Componentes del sistema RFID	17
2.3.2. Frecuencias de operación.....	24
2.3.3. Estandarización de la tecnología RFID	25
2.3.3. Usos y aplicaciones RFID	31
2.4. HARDWARE LIBRE	35
2.4.1. Raspberry Pi	36
2.4.2. Arduino.....	37
2.4.3. Diferencias entre Raspberry y Arduino	47
2.5. ELEMENTOS ELECTRÓNICOS	48
2.5.1. Resistencias	48
2.5.2. Capacitores	50

2.5.3. Diodos.....	52
2.5.4. Diodos LED (Light Emitted Diode)	53
2.5.5. Transistores de unión bipolar	54
2.5.6. Relés	56
2.5.7. Transformadores.....	57
2.5.8. Reguladores de voltaje.....	59
2.5.9. Pantalla gráfica LCD	60
2.5.10. Teclado matricial	61
2.6. INTRODUCCIÓN A REDES	62
2.6.1. Modelo de referencia TCP/IP	63
2.7. BASE DE DATOS	70
2.7.1. Arquitectura de Base de Datos	70
2.7.2. Sistemas Gestores de Bases de Datos.....	71
2.7.3. Bases de Datos Centralizadas	73
CAPÍTULO III	74
3. DISEÑO Y CONTRUCCIÓN DE HARDWARE Y SOFTWARE.....	74
3.1. SITUACIÓN ACTUAL	74
3.2. DISEÑO DE HARDWARE	76
3.2.1. Elección de la placa base	78
3.2.2. Módulo RFID	81

3.2.3. Terminales de conexión de la Placa Arduino MEGA 2560 con demás dispositivos	88
3.2.4. Diagramas de conexión de los elementos.....	89
3.2.5. Fuente de alimentación.....	104
3.2.6. Esquema general.....	113
3.2.7. Elaboración de placas de circuito impreso	115
3.2.8. Interconexión	118
3.3. DISEÑO DE SOFTWARE.....	125
3.3.1. Requerimientos del software	125
3.3.2. Programación del sistema de código abierto	126
3.3.3. Creación de tablas en MySQL.....	136
CAPÍTULO IV	141
4. PRUEBAS DE FUNCIONAMIENTO Y ANÁLISIS ECONÓMICO	141
4.1. PRUEBAS DE HARDWARE.....	141
4.1.1. Pruebas de Lectura del código de la tarjeta electrónica.....	141
4.1.2. Pruebas de funcionamiento del teclado matricial	142
4.1.3. Pruebas de funcionamiento del módulo Ethernet.....	145
4.2. PRUEBAS DE FUNCIONAMIENTO DE SOFTWARE.....	147
4.2.1. Ingreso a la página de administración a través de usuario y contraseña	147
4.2.2. Registro de usuarios en la base de datos	148

4.2.3. Monitoreo de registros.....	154
4.2.4. Registro de visitantes.....	154
4.3. ANÁLISIS ECONÓMICO.....	156
4.3.1. Presupuesto de hardware utilizado	156
4.3.2. Presupuesto para elaboración de placas de circuito impreso.....	157
4.3.3. Presupuesto para el montaje de circuitos.....	157
4.3.4. Presupuesto para servidor y elementos de interconexión para la red	158
4.3.5. Mano de obra directa	158
4.3.6. Presupuesto de software utilizado	159
4.3.7. Análisis económico	159
CAPÍTULO V	163
5. CONCLUSIONES Y RECOMENDACIONES	163
5.1. CONCLUSIONES.....	163
5.2. RECOMENDACIONES	166
BIBLIOGRAFÍA	168
LINKOGRAFÍA.....	170
GLOSARIO DE TÉRMINOS	173
ANEXOS	177
ANEXO A. CÓDIGO DE PROGRAMACIÓN DEL SISTEMA DE CONTROL DE ACCESO.	177

ANEXO B. CÓDIGO PHP Y HTML	183
ANEXO C. INSTALACIÓN DE SERVIDOR XAMPP Y CREACIÓN DE BASE DE DATOS.....	189
ANEXO D. INFORME PARA LA UBICACIÓN DE CONTROLES DE ACCESO EN LAS ENTRADAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE.....	195
ANEXO E. PROFORMAS	202
ANEXO F. HOJA DE DATOS DEL LECTOR RFID RC522	207

ÍNDICE DE FIGURAS

Figura 1: Estructura de un Sistema de Control de Acceso.	8
Figura 2: Lectura de código de barras.	10
Figura 3: Tarjeta con cinta magnética.	11
Figura 4: Tarjeta Inteligente.	12
Figura 5: Tarjeta de Proximidad.	13
Figura 6: Sistema biométrico dactilar.	13
Figura 7: Estructura de un Sistema RFID.	16
Figura 8: Componentes de un tag RFID.	17
Figura 9: Estructura de un Tarjeta RFID.	18
Figura 10: Estructura de un Lector RFID.	20
Figura 11: Formato de código EPC.	28
Figura 12: Sistema de Control de Acceso en estación del metro.	31
Figura 13: Medicamentos con etiquetas RFID.	32
Figura 14: Trazabilidad de Alimentos con RFID.	33
Figura 15: Identificación de equipaje con RFID.	34
Figura 16: Reconocimiento de sustancias químicas con RFID.	34
Figura 17: Control de Inventarios con RFID.	35
Figura 18: Placa Raspberry Pi 2.	36
Figura 19: IDE de Arduino.	40
Figura 20: Arduino Uno.	42
Figura 21: Arduino MEGA.	43
Figura 22: Arduino Nano.	43

Figura 23: Arduino Yun.	44
Figura 24: Arduino Micro.	45
Figura 25: Arduino Ethernet.	45
Figura 26: Símbolo esquemático de la resistencia.	48
Figura 27: Resistencias de distintas potencias.	49
Figura 28: Bandas de colores de resistencia.	49
Figura 29: Símbolo esquemático del capacitor.	50
Figura 30: Tipos de Capacitores.	51
Figura 31: Capacitor cerámico 104.	52
Figura 32: Símbolo del diodo.	52
Figura 33. Estructura de diodo LED.	53
Figura 34. Tipos de transistores Bipolares.	54
Figura 35: Tipos de transistores BJT.	55
Figura 36: Configuraciones de un transistor BJT.	55
Figura 37. Estructura de un Relé.	56
Figura 38: Tipos de relés.	57
Figura 39: Símbolo eléctrico de un transformador.	58
Figura 40: transformador reductor de 12V.	59
Figura 41: Estructura y símbolo de un regulador de voltaje.	59
Figura 42: LCD 16x2.	60
Figura 43: Estructura de un teclado matricial 4x4.	61
Figura 44: Teclado matricial tipo membrana 4x4.	62
Figura 45: Modelo en capas TCP/IP.	64

Figura 46: Cabecera IPv4.	66
Figura 47: Campos que componen a una dirección IP.	67
Figura 48: Formato de direcciones IP.....	68
Figura 49: Sistema gestor como interfaz entre usuarios y base de datos.	72
Figura 50: Logo MySQL.	72
Figura 51: Estudiantes matriculados por modalidad de estudio.	75
Figura 52: Diagrama en bloques del hardware del sistema de control de acceso.	76
Figura 53: Distribución de terminales en Arduino MEGA 2560.	79
Figura 54: Lector RFID RC522.....	84
Figura 55: Etiqueta RFID tipo tarjeta.	86
Figura 56: Conexión SPI con múltiples esclavos.	87
Figura 57: Comunicación SPI entre maestro y esclavo.....	88
Figura 58: Diagrama esquemático de conexión del módulo RFID RC522.....	90
Figura 59: Terminales ICSP.	91
Figura 60: Diagrama esquemático de conexión del módulo Ethernet.....	92
Figura 61: Diagrama esquemático de conexión de la pantalla grafica LCD 16x2.	93
Figura 62: Diagrama esquemático de conexión del teclado matricial.....	94
Figura 63: Conexión de diodos LED.....	99
Figura 64: Diagrama de conexión de relé con transistor.....	100
Figura 65: Diagrama de conexión de pulsador de cambio de estado.	103
Figura 66: Diagrama de conexión de bocina.	104
Figura 67: Medición de la corriente total del sistema.	105
Figura 68: Tipo de onda generada por rectificador de onda completa.	106

Figura 69: Semiciclo positivo en fuente de alimentación de onda completa tipo puente.	106
Figura 70: Fuente de onda completa tipo puente con filtro.....	107
Figura 71: Diagrama esquemático de la fuente de alimentación.....	111
Figura 72: Diagrama en bloques del sistema de control de acceso.	113
Figura 73: Diagrama esquemático del sistema de control de acceso.	114
Figura 74: Diagrama esquemático de la placa para la LCD.	115
Figura 75: Circuito impreso para la conexión de la LCD, leds y pulsadores.	116
Figura 76: Diagrama esquemático del circuito actuador con relé.	116
Figura 77: Circuito impreso para actuador con rele.	117
Figura 78: Diagrama esquemático para fuente de alimentación.....	117
Figura 79: Circuito impreso para fuente de alimentación.	118
Figura 80: Topología lógica de la red de la Universidad Técnica del Norte.....	119
Figura 81: Plano referencial de la Universidad Técnica del Norte.....	121
Figura 82: Comandos para visualizar el tamaño de bases de datos en MySQL.....	122
Figura 83: Tamaño de base de datos en MySQL.....	123
Figura 84: Características eléctricas del UPS.....	124
Figura 85: Diagrama de flujo del funcionamiento del Sistema de Control de Acceso	127
Figura 86: Diagrama de flujo de la subrutina de inicialización del módulo Ethernet.	129
Figura 87: Diagrama de flujo de la subrutina de la obtención del código del tag.....	130
Figura 88: Diagrama de flujo de la subrutina de obtención de la clave por teclado.	132
Figura 89: Diagrama de flujo de la subrutina de mensajes en la LCD.....	133
Figura 90: Esquema de interacción de la base de datos a través de PHP.....	134
Figura 91: Diagrama de flujo de la subrutina de validación de código y clave.	135

Figura 92: Página principal de phpMyAdmin.	136
Figura 93: Estructura de la tabla “login”	137
Figura 94: Estructura de la tabla usuarios.	138
Figura 95: Estructura de la tabla registros.	139
Figura 96: Estructura de la tabla “no registrados”	140
Figura 97: Estructura de la tabla “visitantes”	140
Figura 98: Lectura de Código de tarjeta RFID.	142
Figura 99: Activación de subrutina para ingreso de clave por teclado:.....	143
Figura 100: Ingreso correcto de clave a través del teclado matricial.	143
Figura 101: Visualización de ingreso de clave correcta a través del monitor serial.	144
Figura 102: Ingreso de clave incorrecta mediante teclado matricial.	144
Figura 103: Configuración de tarjeta de red.	145
Figura 104: Ping hacia dirección IP del módulo Ethernet.	146
Figura 105: Captura de paquetes entre el sistema y la base de datos.	146
Figura 106: Características de paquete capturado.	147
Figura 107: Página de ingreso de usuario y contraseña.	148
Figura 108: Ingreso incorrecto de usuario y contraseña.	148
Figura 109: Ingreso de datos en la tabla usuarios a través de phpMyAdmin.	149
Figura 110: Datos ingresados correctamente en la tabla usuarios.	150
Figura 111: Lectura de tarjeta no registrada.	151
Figura 112: Obtención del código RFID de la última lectura a través de la página web	151
Figura 113: Ingreso de datos de usuario a través de página web.	152
Figura 114: Mensaje de registro completo.	152

Figura 115: Datos de usuario almacenados en la base.	153
Figura 116: Lectura de tarjeta registrada:.....	153
Figura 117: Monitoreo de registros.	154
Figura 118: Ingreso de datos de visitante.	155
Figura 119: Monitoreo de registro de visitantes.	155
Figura 120: Control de acceso Stand Alone ASI-8910.	160
Figura 121: Control de acceso ZK X7 ID.....	161

ÍNDICE DE TABLAS

Tabla 1: Tabla comparativa de Sistemas de Identificación.....	14
Tabla 2: Tabla comparativa de placas Raspberry Pi.....	37
Tabla 3: Tabla comparativa de las placas Arduino.....	46
Tabla 4: Diferencias entre Raspberry Pi y Arduino.	47
Tabla 5: Código de colores de resistencias.....	50
Tabla 6: Características eléctricas de distintos tipos de diodos LED.	54
Tabla 7: Funciones de cada terminal de una pantalla LCD.....	60
Tabla 8: Características de teclado matricial 4x4.....	62
Tabla 9: Especificaciones técnicas de la placa Arduino MEGA 2560.....	79
Tabla 10: Especificaciones técnicas de la placa Arduino Ethernet.....	81
Tabla 11: Especificaciones técnicas del módulo RFID RC522.....	83
Tabla 12: Especificaciones técnicas del módulo RFID ID-12LA.....	83
Tabla 13: Terminales de conexión entre Arduino MEGA 2560 y demás dispositivos.....	88
Tabla 14: Corriente de funcionamiento de cada dispositivo.....	105
Tabla 15: Características de servidor para base de datos.....	123
Tabla 16: Características de UPS Computer Power.....	125
Tabla 17: Presupuesto de hardware utilizado.....	156
Tabla 18: Presupuesto para elaboración de placas de circuito impreso.....	157
Tabla 19: Presupuesto para montaje de los circuitos.....	157
Tabla 20: Presupuesto para servidor y elementos de interconexión con la red.....	158
Tabla 21: Costos de mano de obra.....	158
Tabla 22: Presupuesto de software utilizado.....	159

Tabla 23: Costo total del sistema de control de acceso.	159
--	-----

ÍNDICE DE ECUACIONES

Ecuación 1: Cálculo del valor de la resistencia pull-down.....	95
Ecuación 2: Cálculo de la resistencia de un led.....	96
Ecuación 3: Cálculo de la potencia de una resistencia.	97
Ecuación 4: Cálculo de la intensidad de la bobina de carga del relé.....	100
Ecuación 5: Cálculo de la ganancia de un transistor.	101
Ecuación 6: Cálculo de la resistencia de base.	102
Ecuación 7: Cálculo de la relación de vueltas en un transformador.....	108
Ecuación 8: Cálculo de voltaje pico del primario.....	108
Ecuación 9: Cálculo del voltaje pico del secundario.....	108
Ecuación 10: Cálculo de voltaje rectificado de onda completa pico sin filtrar.	109
Ecuación 11: Cálculo de voltaje de rizo pico pico.	109
Ecuación 12: Cálculo de voltaje de salida del filtro.	110
Ecuación 13: Cálculo de factor de rizo.....	110
Ecuación 14: Cálculo de la potencia de la batería.	112
Ecuación 15: Calculo de la potencia del sistema.....	112
Ecuación 16: Cálculo del tiempo de duración de la batería.	112

RESÚMEN

El presente trabajo de titulación tiene como objetivo diseñar un sistema de control de acceso con el uso de tecnología inalámbrica de identificación por radiofrecuencia. Este proyecto beneficiará principalmente a los estudiantes de la Universidad Técnica del Norte, ya que mediante el uso de este sistema se podrá tener un control y monitoreo adecuado de todas las personas que ingresen al campus, a través de un registro mediante una base de datos.

Se analizaron los fundamentos teóricos necesarios para la realización del proyecto, detallando las principales características y aplicaciones de las tecnologías de identificación automática y específicamente la de identificación por radiofrecuencia, así como también se describieron los elementos y dispositivos electrónicos que forman parte del sistema.

El diseño del sistema de control de acceso se dividió en dos segmentos, diseño del hardware y diseño de software. Para el diseño de hardware se realizó las especificaciones de las características técnicas de cada elemento que conforma el sistema y su conexión a través de diagramas esquemáticos. De igual forma para el diseño del software se mostró el proceso de ejecución del código de programación a través de diagramas de flujo, así como también el manejo de tablas en la base de datos.

Finalmente, se realizaron las pruebas de funcionalidad del prototipo y un análisis económico en base al costo de elaboración del proyecto, con referencia a todos los elementos de hardware y software empleados.

ABSTRACT

The present work of titulation has with objective the design of a control access system using RFID technology. It will primarily benefit students of this University to have an appropriate control and monitoring of all people, who are coming in the campus through a record using a database.

It were analyzed the necessary theoretical foundations for the project: the main features and applications of radio frequency identification technology, as well as there are also some important elements of the system.

The design of a control access system it split in two segments, design of hardware and software. For the design of hardware specifications were made the technical characteristics of each element of the system and its connection through schematic diagrams. In the same way, the design of software through flow charts, showing the process running the program code, as well as the management of tables in the database.

Finally, some tests of the prototype functionality were performed and an economic analysis based on the cost of project was development, regarding all elements of hardware and software used.

PRESENTACIÓN

Innumerables casos de robos se han suscitado dentro de instituciones públicas por parte de personas ajenas a las mismas, las cuales ingresan con total facilidad y sin ser detectadas. Estos casos se han visto especialmente en lugares de masiva concurrencia, en los que no existe personal suficiente que controle ese aspecto de seguridad, tal es el caso de la Universidad Central, la cual se ha visto obligada a implementar varios mecanismos de seguridad.

En la actualidad muchas instituciones y empresas han optado por implementar en sus instalaciones sistemas de control de ingreso de personal, con el fin de mejorar la seguridad. De esta forma se puede controlar el ingreso de usuarios que posean un identificador que autorice su paso, caso contrario deniegue el mismo.

Un sistema de control de acceso, como su nombre lo indica se caracteriza por presentar características de seguridad y control, precautelando la integridad de los usuarios y los bienes materiales de las instituciones, a más de llevar un registro adecuado del ingreso de usuarios, y presentar un valor agregado a la modernización de las instituciones.

El sistema de control de acceso a implementar en la Universidad Técnica del Norte pretende contribuir al sistema de seguridad existente y brindar un nivel de seguridad extra, específicamente a los estudiantes. Para ello se utilizará tarjetas electrónicas que identifiquen a cada usuario y puedan validar su ingreso, además se contará con un sistema alternativo de ingreso de clave por teclado en caso de que el usuario no cuente con la tarjeta electrónica.

CAPÍTULO I

En el presente capítulo se describe los antecedentes del proyecto, que indican el planteamiento del problema, así como también los objetivos a cumplirse, el alcance y la justificación para el desarrollo del mismo.

1. ANTECEDENTES

1.1. PROBLEMA

La Universidad Técnica del Norte se ha caracterizado por ser una institución de alta calidad de enseñanza y un referente dentro de la investigación en la zona norte. Diariamente existe una alta afluencia de personas en toda la institución, y esto ha dificultado a los encargados de seguridad tener un mayor control de las mismas, por lo que muchas veces se tiene personas infiltradas que no pertenecen a la Universidad y que ingresan con malas intenciones.

Actualmente la Universidad alberga en sus instalaciones alrededor de 9000 estudiantes. Este significativo número de personas que transitan diariamente por las instalaciones han hecho que se tomen medidas especiales en cuanto a seguridad se trata, pero no se puede llevar un control adecuado de toda esta cantidad, por lo que se han tenido algunos casos de robo dentro del campus, haciendo necesaria la implementación de un sistema de control de acceso en las entradas de la Universidad.

La solución más adecuada para poder controlar el acceso de las personas y específicamente de los estudiantes que ingresan a la Universidad es mediante la implementación de un sistema de control, el cual permita el acceso a aquellas personas que tengan un código o dispositivo de acceso

especifico que les permita ingresar a las instalaciones universitarias, además de que a través de este mismo dispositivo se llevará un registro o una bitácora en una base de datos.

Con el uso de nuevas tecnologías inalámbricas que se vienen desarrollando y en especial con el constante aumento del acceso hacia las TIC's en el país, es necesario crear sistemas que permitan solucionar problemas que se generan a diario, y en especial aquellos que tengan que ver con la seguridad y el control de personal en ciertas entidades educativas del país.

1.2. JUSTIFICACIÓN

A causa de la falta de control en el ingreso de distintas personas a las instalaciones de la Universidad, se ha tenido algunos casos de robo dentro de las facultades y hacia los estudiantes por lo que se hace necesario tomar medidas de seguridad que aporten al control de acceso únicamente de personal autorizado. Para ello se desea implementar un sistema de control de acceso mediante el uso de dispositivos de identificación automática, los mismos que permitirán a los estudiantes, docentes, administrativo y demás personas pertenecientes al establecimiento tener un identificador único dentro de la Universidad.

Aunque no se tenga un alto porcentaje de robos dentro del establecimiento es necesario cuidar los bienes materiales con los que cuenta la Universidad, pero sobre todo cuidar la integridad de cada uno de los estudiantes, garantizando un nivel adecuado de seguridad.

Este proyecto no se basa únicamente en diseñar un sistema electrónico de control de acceso, sino que también se quiere contribuir al desarrollo de un sistema de seguridad y vigilancia completo que aporte a la excelencia académica, ya que se estará utilizando mecanismos tecnológicos para brindar seguridad en la Universidad.

Además la ventaja de tener un sistema electrónico basado en Open Source es que no se tendrá un diseño fijo, es decir que el sistema será flexible y adaptable a nuevas aplicaciones y cambios que se quieran dar y que aporten con nuevas soluciones acordes a las necesidades que se vayan generando.

1.3. OBJETIVOS

1.3.1. General

Diseñar un sistema de control de acceso mediante el uso de tecnología inalámbrica de identificación automática que permita la regulación en el ingreso a la Universidad Técnica del Norte, y registro de personas mediante el uso de una base de datos.

1.3.2. Específicos

- Considerar aspectos importantes que involucra el control de acceso de personas a la Universidad y una posible solución.
- Investigar en base a la solución que brindará el sistema, acerca de tecnologías inalámbricas que sirvan para el desarrollo del control de acceso, mediante un análisis de sus principales características y enfocadas principalmente a la tecnología de identificación por radio frecuencia (RFID).
- Elegir una base de datos adecuada entorno al sistema de gestión MySQL, la misma que se ajuste al sistema de control de acceso.
- Establecer el diseño electrónico del prototipo a realizar de acuerdo a la funcionalidad de un control de acceso.

- Especificar el tipo de conexión que tendrá el sistema con la red de la Universidad mediante un análisis de tráfico de información.
- Demostrar mediante las pruebas pertinentes el correcto funcionamiento del sistema de control de acceso.
- Realizar un análisis de viabilidad económica entorno a la inversión del proyecto.

1.4. ALCANCE

El objetivo que se persigue mediante la elaboración del proyecto es la de diseñar un sistema de control de acceso mediante el uso de tecnología inalámbrica de identificación automática, específicamente la de identificación por radiofrecuencia (RFID) y una base de datos, la cual permita tener un registro de cada una de las personas que ingresan diariamente a la universidad, esto a través del uso de un dispositivo o tarjeta que contenga un código único, el cual permita a los estudiantes y demás personas pertenecientes a la universidad ingresar sin ningún inconveniente.

Para iniciar se realizará un estudio de ciertos aspectos que hay que considerar en el control de acceso, específicamente en el caso de personas que no pertenezcan a la universidad y que tengan la necesidad de ingresar a la misma, dando una solución adecuada que se adapte a las soluciones que brinda el sistema.

Se procederá a realizar un análisis y comparación de las principales tecnologías inalámbricas, fundamentando principalmente la tecnología de identificación por radiofrecuencia (RFID) a utilizar en el sistema electrónico, para de esta forma justificar la elección de la mejor tecnología en base a sus características y ventajas; además de su adaptabilidad con el sistema en general.

Además se procederá a realizar la elección de una adecuada base de datos que soporte la información a registrar y se adapte a la funcionalidad del sistema electrónico, esto mediante el uso del sistema de gestión de base de datos MySQL y pruebas que permitan establecer la adecuada elección en base al funcionamiento requerido en todo el sistema.

Para el diseño del sistema electrónico en general se considerara el número de accesos que se vayan a implementar en cada una de las entradas y de acuerdo a este punto se tendrá un concentrador o un Switch con el que se podrá conectar a la red de la Universidad y posteriormente acceder a la base de datos en donde se registrará la actividad captada por el sistema, esto mediante una conexión vía Ethernet, la cual garantice también la conexión hacia la red interna de la universidad; a más de esto también se considerara el uso de una plataforma electrónica de código abierto (Open Source) que facilite la operatividad con otras tarjetas o módulos a utilizar y que garantice la conexión hacia el servidor que contenga la base de registros de control de acceso. Para la elección del sistema de código abierto se procederá a realizar las pruebas pertinentes que garanticen el correcto funcionamiento del sistema y que además se pueda integrar otras funcionalidades a futuro, garantizando el diseño de un sistema flexible, el cual permita un acceso controlado o total, así como también una denegación en todo el sistema según la necesidad generada.

Mediante algunas pruebas se elegirá la conexión del sistema electrónico hacia la base de datos, observando principalmente la integridad de la información y el funcionamiento estable de la conexión del sistema electrónico con la base de información.

Finalmente se procederá a realizar pruebas de diagnóstico del funcionamiento general del sistema electrónico y la base de datos, mediante la implementación de un prototipo, el cual podrá

ser aplicado en alguna dependencia o laboratorio de la Universidad, comprobando el desempeño del sistema en cualquier ambiente donde se lo quiera aplicar; además de realizar un presupuesto referencial de todos los componentes y materiales que se requerirán para implementar el proyecto.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

En este capítulo se describe brevemente el funcionamiento de un sistema de control de acceso, tipos de tecnología de identificación automática y principalmente características de la tecnología RFID, sus componentes y aplicaciones, así como también el fundamento teórico de los principales elementos y dispositivos que conforman y complementan un sistema de control de acceso.

2.1 SISTEMAS DE CONTROL DE ACCESO

Un sistema de control de acceso es un conjunto de dispositivos electrónicos y mecanismos que interactúan entre sí con el fin de permitir o denegar el acceso hacia algún tipo de servicio, mediante un proceso de validación y autenticación de códigos (Villegas, 2015).

Anteriormente se realizaban controles con la ayuda de personal de seguridad que se encargaba manualmente de registrar el acceso, lo que dificultaba de cierto modo la productividad y fácil movilidad del personal que requiere acceder a un lugar o recurso específico.

Actualmente los avances tecnológicos han permitido que se llegue a tener sistemas complejos de control de acceso que no solo permitan o denieguen el paso hacia algún sitio, sino que también puedan generar otros datos útiles de registro, así como también brindar facilidad de uso y seguridad a los usuarios mediante el empleo de diversos mecanismos y sistemas de autenticación.

2.1.1 Funcionamiento de un Sistema de Control de Acceso

Un sistema de control de acceso ejerce su función en cuanto el código de acceso del usuario sea identificado por el lector del sistema, es decir se tendrá una base de códigos, los mismos que

serán procesados para validar la información y registrar al usuario en la base de datos, para finalmente mostrar en el panel de control si la validación fue correcta o caso contrario mostrar un mensaje el cual especifique que el código de ingreso es incorrecto y por tanto el sistema no se accionará para el ingreso.

2.1.2. Componentes de un Sistema de Control de Acceso

Básicamente un sistema de control de acceso está conformado por distintos segmentos, según sea su diseño y cumpliendo cada uno con una función en específico.

En la Figura 1 a continuación se muestra un esquema de los componentes de un sistema de control de acceso:

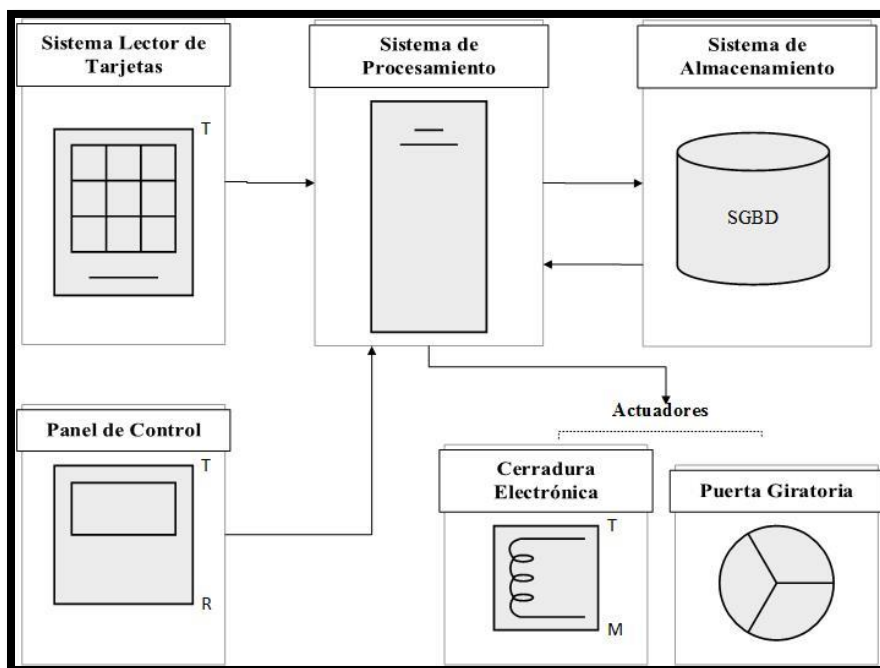


Figura 1: Estructura de un Sistema de Control de Acceso.

Fuente: AETIC, 2009.

A continuación se detalla brevemente la función que cumple cada segmento que conforma un sistema de control de acceso:

- Sistema Lector.- Este sistema se encarga de leer el código del dispositivo de identificación que posea el usuario, para posteriormente enviarlo al sistema de procesamiento.
- Sistema de Procesamiento.- Se encarga de procesar la información que recibe del usuario a través del sistema de lectura para realizar los procesos de control del sistema en general.
- Panel de control.- Provee una interfaz física entre el sistema y el usuario permitiendo visualizar el proceso que realiza el sistema, además de permitir el ingreso de un código alternativo en caso de no tener el dispositivo de identificación.
- Sistema de almacenamiento y registro.- se encarga de registrar los eventos que se generen en el sistema, además de proveer una base de información de los usuarios que van a tener privilegios de acceso.
- Sistema de Actuadores.- este sistema entrará en funcionamiento una vez que los datos hayan sido procesados y comprobados, para finalmente accionar distintos tipos de actuadores, entre los cuales están: cerradura eléctrica, cerradura magnética, puerta giratoria, etc.

2.1.3. Sistemas de Identificación

Actualmente se pueden encontrar varias tecnologías utilizadas en sistemas de identificación automática aplicadas en distintas áreas, sin embargo las que mayor acogida han tenido en este tipo de sistemas han sido:

- Código de barras
- Cinta magnética

- Tarjetas inteligentes
- Tarjetas de proximidad
- Biométricos

2.1.3.1. Código de barras

Sin duda alguna los sistemas basados en código de barras siguen siendo uno de los más utilizados en muchas aplicaciones gracias a su velocidad, fiabilidad y precisión. Se trata de un código binario, que utiliza dos símbolos basados en una sucesión de colores (blanco y negro) configurados paralelamente que llevan en si un código, el cual va a ser captado por el lector óptico, como muestra la Figura 2, mismo que envía una señal eléctrica binaria a un microprocesador para decodificarla y finalmente poder generar los caracteres mediante un software especial (Godínez, 2008).



Figura 2: Lectura de código de barras.

Fuente: Recuperado de <http://www.mypesoft.galeon.com/>

2.1.3.2. Tecnología de cinta magnética

Esta tecnología basa su funcionamiento en la lectura de una banda magnética formada por óxidos metálicos ferromagnéticos, los cuales están ubicados en una posición espacial de puntos

que serán codificados por el sistema lector a través de inducción electromagnética. Una de las aplicaciones más importantes se ve en las tarjetas de crédito, las cuales aprovechan las características que presenta esta tecnología en cuanto a costos agilidad de autenticación e identificación única para cada usuario. La Figura 3 indica la banda ferromagnética que posee una tarjeta:



Figura 3: Tarjeta con cinta magnética.

Fuente: AKROCARD, 2016. Recuperado de <http://akrocard.com/producto/tarjeta-pvc-banda-magnetica/>

2.1.3.3. Tarjetas Inteligentes

Una tarjeta inteligente o Smart Card es un sistema de almacenamiento electrónico con capacidad de procesamiento. Este tipo de sistemas aprovechan la información codificada que se encuentra almacenada en una memoria ROM, además posee un microprocesador capaz de realizar ciertos cálculos en los procedimientos de funcionamiento, todo esto integrado en un pequeño chip sobre una tarjeta plástica, como se observa en la Figura 4:



Figura 4: Tarjeta Inteligente.

Fuente: AKROCARD, 2016. Recuperado de <http://akrocard.com/producto/tarjeta-chip-contacto-microprocesador-cpu/>

Su aplicación más común está dada para servicios pagados, debido a que la información está protegida mediante mecanismos avanzados de seguridad, sin embargo por su alto costo de fabricación no se ha ampliado su uso en otras aplicaciones (Godínez, 2008).

2.1.3.4. Tarjetas de Proximidad

Estas tarjetas basan su funcionamiento en la tecnología de identificación por radio frecuencia, la transacción electrónica se realiza mediante ondas de radiofrecuencia cuando la tarjeta se encuentra dentro del campo magnético que genera el lector. Gracias a sus características y a la rapidez de sus operaciones ha tenido gran acogida en distintas aplicaciones, además de no necesitar visión directa entre emisor y receptor brindando una mayor velocidad de lectura. La Figura 5 a continuación indica una tarjeta de proximidad RFID:

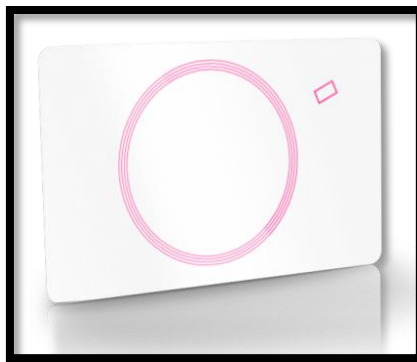


Figura 5: Tarjeta de Proximidad.

Fuente: AKROCARD, 2016. Recuperado de <http://akrocard.com/producto/tarjeta-proximidad-rfid-a-125khz/>

2.1.3.5. Sistemas biométricos

Este tipo de sistemas son utilizados en la verificación de individuos a partir de ciertas características físicas como: huellas dactilares, el iris del ojo, reconocimiento facial, entre otros. Es un mecanismo de identificación automática que presenta gran ventaja frente a otros sistemas en lo que a seguridad refiere ya que la información será única e intransferible para cada usuario. Sin embargo por su compleja funcionalidad estos sistemas presentan un alto costo frente a otro tipo de sistemas de identificación (Godínez, 2008).

La Figura 6 muestra un sistema biométrico mediante el uso de huellas dactilares:



Figura 6: Sistema biométrico dactilar.

Fuente: ML Consultores, 2016. Recuperado de <https://www.mlconsultores.com/sistemas-biometricos/>

2.1.3.6. Tabla comparativa de los principales sistemas de identificación

A continuación la Tabla 1 representa una comparativa de las principales tecnologías de identificación automática y sus características más relevantes:

Tabla 1: Tabla comparativa de Sistemas de Identificación.

Parámetros del Sistema	Código de Barras	Cinta magnética	Tarjetas Inteligentes	Tarjetas de Proximidad (RFID)	Sistemas Biométricos
Capacidad de Almacenamiento (Número de caracteres)	1 – 100	-----	16 – 64	16 – 256	No aplica
Densidad de Datos	Baja	Alta	Muy Alta	Muy Alta	Alta
Costo	Bajo	Bajo	Medio	Bajo	Alto
Interferencia por obstrucción	Fallo total	-----	-----	No afecta	Posible
Accesos no autorizados	Poca protección	Imposible	Imposible	Imposible	Imposible
Velocidad de lectura	Baja 4s	Bajo 4s	Bajo 4s	Muy rápido menos de 1s	Muy baja, menos de 5 a 10s
Distancia máxima	0 a 50cm	Requiere contacto	Requiere contacto	0 a 5m	Requiere contacto

Fuente: Ortiz , Ibarra , Andrade , & Almanza, 2012.

2.2. IDENTIFICACIÓN POR RADIOFRECUENCIA

La tecnología de identificación por radio frecuencia RFID, conocida así por sus siglas en inglés (Radio Frequency Identification) ha tenido su aparición desde hace algunos años atrás pero recientemente se ha visto un mayor número de aplicaciones y una gran acogida en el mercado, esto gracias a los avances tecnológicos de hoy en día y específicamente a la miniaturización de materiales electrónicos, lo que ha permitido desarrollar sistemas complejos de comunicación de corto alcance dentro de pequeños chips.

Este tipo de tecnología de identificación automática contiene la información en etiquetas electrónicas o también llamadas tags. Al momento que estas etiquetas ingresan en el área de cobertura que genera el sistema de lectura para esta tecnología, este envía una señal a dicha etiqueta para que transmita la información que se encuentra almacenada en su memoria y que generalmente se trata de un código de identificación.

Una de las características importantes de los sistemas RFID es justamente la recuperación de información vía radiofrecuencia sin que exista la necesidad de línea de vista o contacto físico entre el tag y el lector, aunque en muchos casos se establece cierta distancia específica para que exista la transferencia de dicha información.

Se ha visto últimamente que los sistemas RFID han venido técnicamente perfeccionándose con el fin de tener mayor aplicación y aceptación en las empresas, es por ello que se ha estandarizado la tecnología con el fin de especificar las bandas de operación, garantizando así un correcto uso del recurso y la compatibilidad de la tecnología a nivel mundial (AETIC, 2009).

2.3. SISTEMA RFID

Un sistema RFID está constituido básicamente por tres elementos importantes que cumplen funciones específicas: tarjetas electrónicas o tags, antenas, lector y en algunos casos se incluye también un sistema de gestión de información cuando se requiere manejar gran cantidad de información, la cual no pueda ser operada en la propia memoria del lector (Gidekel, 2008). La Figura 7 muestra la estructura de un sistema RFID:

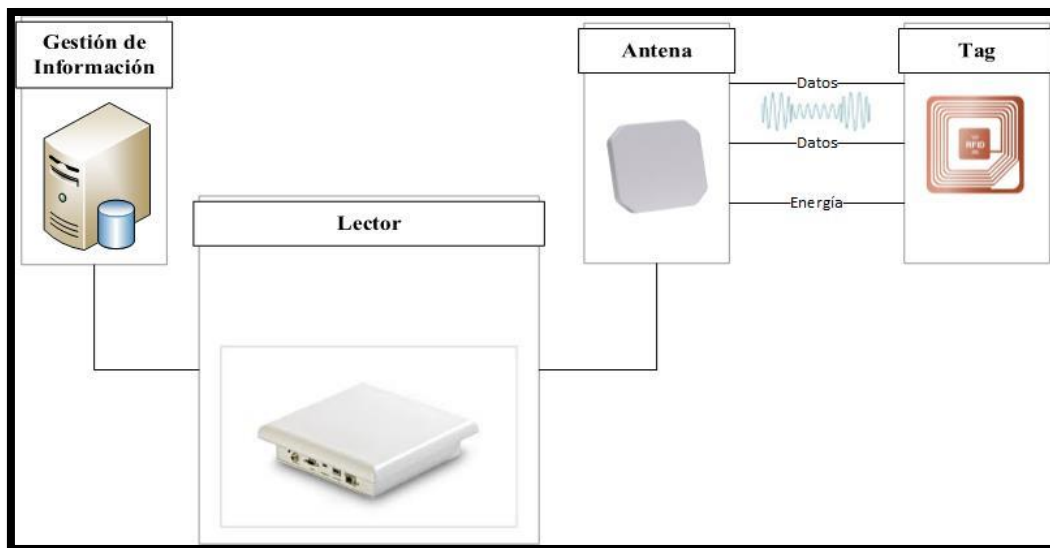


Figura 7: Estructura de un Sistema RFID.

Fuente: Portillo, Bermejo, Bernardos, & Martínez, 2008.

El modo de funcionamiento básico de este tipo de sistemas se realiza de forma secuencial desde que el tag entra en el área de emisión del lector, el cual controla la lectura y escritura de la información almacenada en las tarjetas a través de un campo de radiofrecuencia. Internamente el tag está conformado por una microantena y un chip, que al momento que percibe ondas electromagnéticas desde el lector, activa al chip para liberar la información alojada en su memoria (AETIC, 2009).

Una vez que el lector haya captado la respuesta del tag procesa la información y procede a enviar la misma a una base de datos la cual contiene información de la tarjeta previamente registrada para el procesamiento de la acción a la que se haya asociado y que el resto del sistema deberá ejecutar, según la aplicación que se le esté dando (Godínez, 2008).

2.3.1. Componentes del sistema RFID

Como se ha mencionado anteriormente un sistema RFID está compuesto por: etiquetas RFID, antenas y lector.

2.3.1.1 Etiqueta RFID

La etiqueta RFID o tag es uno de los elementos clave en los sistemas de identificación por radiofrecuencia, es considerado como un dispositivo transponedor, es decir que gracias a su funcionamiento tienen la capacidad de recibir y emitir señales, pero únicamente a modo de respuesta ante una petición de un dispositivo transceptor o lector (AETIC, 2009).

La Figura 8 muestra la estructura de un tag y sus componentes principales:

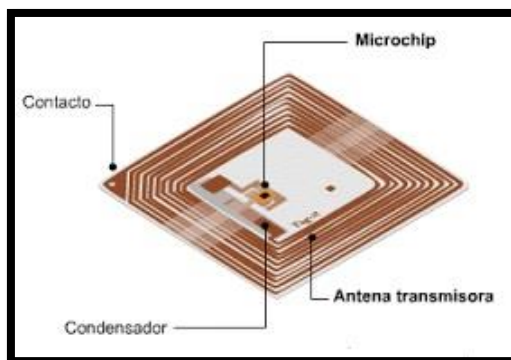


Figura 8: Componentes de un tag RFID.

Fuente: Gerometta, 2007. Recuperado de <http://librosnetworking.blogspot.com/2007/06/unas-notas-sobre-rfid.html>

Su fabricación viene dada en algunos formatos, esto según la aplicación que se vaya a dar al sistema, sin embargo el proceso básico de montaje consta en primer lugar de una base de material de sustrato (papel, PVC, PET, etc.), sobre esta base se colocará una micro antena la cual es fabricada de materiales conductores, como el aluminio y el cobre. La antena estará conectada al chip del tag para finalmente poder revestir con un material protector a estos elementos.

2.3.1.1.1 Arquitectura de una etiqueta RFID

Los componentes básicos de una etiqueta RFID son sin duda la antena y el chip, en donde la antena es la encargada de enviar la información al chip, el mismo que dentro de su estructura posee una memoria no volátil en este caso una memoria EEPROM, en la que su capacidad depende del modelo y se encuentran en un rango de los 96 bytes hasta los 32Kbits dependiendo de su aplicación.

El circuito integrado que se encuentra dentro del chip tiene algunas funcionalidades entre las cuales están: la conversión de energía, el control lógico, el almacenamiento y recuperación de datos y la modulación requerida para devolver los datos al lector. La Figura 9 muestra un diagrama en bloques de la arquitectura de una etiqueta RFID:

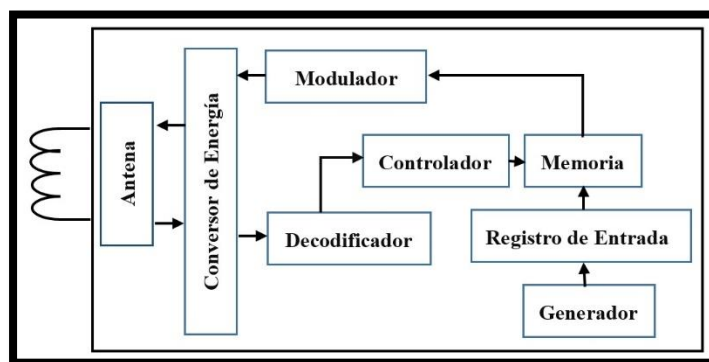


Figura 9: Estructura de un Tarjeta RFID.

Fuente: Basado en Godínez (2008).

Las ondas de radio generadas por el lector y captadas por la antena son procesadas y pasan a convertirse no solo en peticiones sino también en energía para el resto de unidades que conforman del chip a través de un conversor ADC, el cual provee de energía al resto de dispositivos. El chip contiene además un decodificador y codificador para convertir la señal analógica en digital y viceversa. Posteriormente esta señal va al bloque de control lógico en el cual se realiza un procesamiento de bajo nivel para leer el código único que se encuentra grabado en la memoria y

que fue codificado por el fabricante. Finalmente este código pasa a ser modulado para enviar la información al lector (Godínez, 2008).

2.3.1.2 Tipos de etiquetas RFID

La clasificación de las etiquetas RFID es variada, sin embargo la más común que se les da, está especificada por el modo de alimentación que poseen, teniendo así etiquetas: pasivas, semiactivas y activas.

2.3.1.2.1. Etiquetas pasivas

Este tipo de etiquetas se caracterizan por utilizar la energía obtenida de las ondas generadas por el lector, es decir que no poseen una fuente de energía propia incorporada. Tienen un rango de lectura limitado con un máximo de alcance de 5 metros, no obstante su vida útil es ilimitada y su costo es bajo (AETIC, 2009).

2.3.1.2.2. Etiquetas semiactivas

Las etiquetas semiactivas poseen una fuente de alimentación propia, sin embargo esta sirve únicamente para alimentar el chip del tag, más no para realizar la transmisión de información, para ello se seguirá utilizando la energía que provee el sistema lector.

La fuente de alimentación en este tipo de tarjetas permite tener energizado a todo su sistema, mejorando así su rango de lectura, que puede llegar hasta los 10 metros. Tiene un tiempo de vida útil limitado dependiendo de la duración de su batería, que puede variar de acuerdo a las características que la tecnología presente, llegando hasta 10 años de vida útil (AETIC, 2009).

2.3.1.2.3 Etiquetas activas

Las etiquetas activas se caracterizan por ser independientes de la señal transmitida por el lector, cuentan con su propia batería lo que mejora su alcance llegando a un máximo de 100 metros, además de poseer una mayor capacidad de almacenamiento y mejor inmunidad al ruido. Su velocidad de transmisión de la información es alta en comparación a las etiquetas pasivas, y no se requiere de una orientación específica entre la tarjeta y el lector lo que aumenta su eficiencia y confiabilidad. Sin embargo su inconveniente se encuentra en su elevado costo de fabricación y su vida útil que depende de la batería del dispositivo, misma que puede llegar a durar hasta 10 años de acuerdo a sus características (AETIC, 2009).

2.3.1.3. Lector RFID

El lector RFID es un dispositivo que incorpora subsistemas de emisión y recepción de señales codificadas u ondas electromagnéticas a través de un sistema de antenas. Uno de sus principales objetivos es generar la señal de radio frecuencia para activar y alimentar al tag, así como también se encarga de interactuar con el sistema de gestión de información para el procesamiento de la misma (AETIC, 2009). La Figura 10 muestra la estructura interna de un lector RFID:

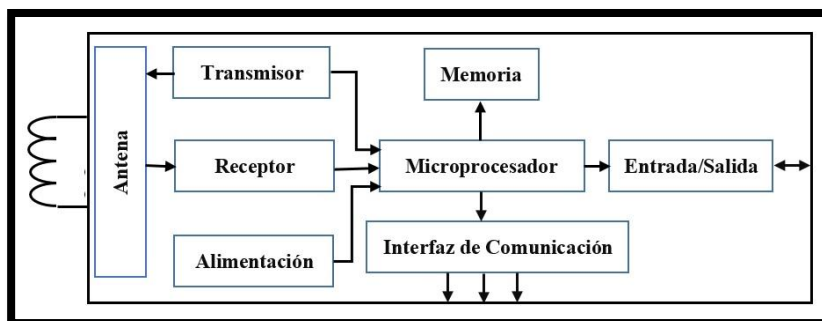


Figura 10: Estructura de un Lector RFID.

Fuente: Godínez, 2008.

Al sistema lector lo conforman varios subsistemas que se mencionan a continuación:

- Transmisor
- Receptor
- Microprocesador
- Memoria
- Entradas y salidas
- Controlador
- Interfaz de comunicación
- Fuente de alimentación
- Antenas

2.3.1.3.1 Transmisor

El transmisor es el encargado de la emisión de ondas electromagnéticas que contengan información codificada, además de la energía necesaria para poner en funcionamiento a las etiquetas, esto a través de antenas.

2.3.1.3.2. Receptor

El receptor a través de las antenas se encarga de recibir las señales análogas provenientes de las etiquetas para su posterior procesamiento en el microprocesador.

2.3.1.3.3. Microprocesador

Dentro del microprocesador se realiza un procesamiento de bajo nivel para la información que se haya recibido por parte del tag, además de la decodificación de los datos así como también de la verificación de errores en la señal captada.

2.3.1.3.4. Memoria

A través de la memoria se podrá almacenar datos importantes tales como: parámetros de configuración del sistema lector o códigos de distintas tarjetas que hayan sido leídas por el sistema.

2.3.1.3.5. Entradas y salidas / actuadores

Mediante este tipo de sistemas se puede hacer que el lector RFID interactúe con dispositivos externos como: sensores y actuadores, los mismos que permitan implementar mecanismos de encendido y apagado, evitando que el sistema se encienda únicamente cuando exista una lectura del tag.

2.3.1.3.6. Controlador

Permite al usuario poder comunicarse con el sistema lector mediante la ayuda de un computador o un programa, en caso de que exista más de un lector en el sistema a través de una interfaz de comunicación.

2.3.1.3.7. Interfaz de comunicación

Es el medio por el cual se va a realizar la comunicación entre el usuario y el controlador del sistema lector. En el sistema lector se pueden tener distintos tipos de interfaces de comunicación, de las cuales se puede mencionar: RS-232, RS-485, adaptador de red, etc.

2.3.1.3.8. Fuente de alimentación

Se encarga de proveer la energía eléctrica necesaria para poner en funcionamiento al sistema en general. Dependiendo del tipo de lector (fijo o móvil) se puede tener una fuente de alimentación conectada a un tomacorriente o una batería recargable.

2.3.1.4. Antenas

Las antenas son los elementos más sensibles dentro de un sistema RFID, ya que son las encargadas de enviar y recibir las señales que contienen la información que se desea procesar. Su tamaño y forma varía, dependiendo de la frecuencia de operación y el área de cobertura que generen, así como también de la aplicación que vayan a tener (Portillo, Bermejo, Bernardos, & Martínez, 2008).

2.3.1.4.1. Antenas Móviles

Este tipo de antenas se encuentran dentro de dispositivos móviles que son utilizados para la identificación de una gran cantidad de objetos que no puedan ser movilizadas hacia el lector.

2.3.1.4.2. Antenas Fijas

Las antenas fijas se caracterizan por estar conectadas mediante cables a un sistema lector estático ubicado en un lugar estratégico, desde donde se realizará la lectura de tags que se encuentren dentro del área de cobertura.

2.3.2. Frecuencias de operación

Otra forma de clasificar a las etiquetas electrónicas, es también mediante la frecuencia en la que estén operando, y de esto también dependen las aplicaciones que puedan tener los sistemas RFID, debido a que, a mayor frecuencia se tendrá una mayor velocidad de transmisión, lo que implica a su vez un mayor costo del sistema.

2.3.2.1. Baja frecuencia (9-135 kHz)

Los sistemas RFID que operan en el rango de baja frecuencia por lo general suelen utilizar tags pasivos, brindando una baja tasa de transferencia (entre 200 bps y 1 Kbps) y corto alcance en su cobertura (aproximadamente 0.5 metros), por lo que son utilizados para aplicaciones de poca distancia (Portillo, Bermejo, Bernardos, & Martínez, 2008).

2.3.2.2. Alta frecuencia (13,56 MHz)

En su mayoría los sistemas que trabajan dentro del rango de alta frecuencia utilizan tags pasivos con una baja tasa de transferencia (25 Kbps) y alcance, sin embargo no se ven afectados por materiales y líquidos no conductores; además tiene muchas aplicaciones debido a que se maneja dentro de estándares internacionales que denominaron a esta banda de frecuencia como ISM,

orientada específicamente a un uso no comercial en las áreas de la industria, ciencia y medicina (Portillo, Bermejo, Bernardos, & Martínez, 2008).

2.3.2.3. Frecuencia ultra alta (433 MHz y 860-960 MHz)

La principal ventaja de los sistemas RFID que operen dentro del rango UHF es un elevado rango de cobertura (mayor a 3 metros) que se encontrará regulado por normas que sistematizan y establecen la potencia en cada país. Sin embargo, presentan interferencias frente a concentraciones de líquidos y otros materiales (Godínez, 2008).

2.3.2.4. Frecuencia de microondas (2,45 GHz y 5.8 GHz)

Los sistemas RFID dentro del rango de microondas se caracterizan principalmente por trabajar con altas tasas de transferencia (debajo de 100 Kbps), además de presentar un mayor alcance de lectura que va de 1 a 2 metros para tags pasivos y hasta 15 metros para activos. La banda de frecuencia de 2.45 GHz también se encuentra dentro del rango de bandas ISM (Godínez, 2008).

2.3.3. Estandarización de la tecnología RFID

Existen muchos organismos regulatorios que influyen en la estandarización de la tecnología de identificación por radiofrecuencia que permite tener una arquitectura abierta de la misma, con el fin de que los productos elaborados por distintos fabricantes puedan interactuar entre sí, abordando áreas fundamentales como: protocolos de comunicación, tipo de modulación, contenido de la información, velocidades de transmisión, aplicaciones, etc.

2.3.3.1. Estándar AIAG

El estándar AIAG o también denominado Grupo de Acción de Industria Automotriz, es una entidad sin fines de lucro que tiene como objetivo principal la implementación de nuevos sistemas y reducción de costos, en torno a la industria automotriz. Uno de los estándares más conocidos es el AIAG B-11, el cual especifica la identificación de neumáticos y ruedas mediante tecnología RFID (AIAG, 2016).

2.3.3.2. Estándar ANSI

ANSI es una organización que administra y coordina el desarrollo de estándares para distintos productos y servicios sin ningún fin de lucro. Esta organización facilita el desarrollo de los estándares americanos para generar una acreditación en distintos procesos de elaboración de productos. Su objetivo inicial es mejorar la competitividad, facilitando el desarrollo de normas y sistemas de evaluación para la tecnología y el mejoramiento de la misma (American National Standards Institute, 2015).

Existen numerosos estándares promovidos por ANSI, pero aquellos relacionados con la tecnología RFID son los siguientes:

- ANSI INCITS 256-2001.- Estándar para la promoción de los dispositivos RFID interoperables, operando en bandas internacionales que están disponibles libremente y niveles de energía con licencia gratuita.
- ANSI INCITS 371.- Estándar para especificaciones de Tecnología de la información- sistemas de localización en tiempo real (RTLS).
- ANSI MH10.8.4.- Estándar de RFID para contenedores de plástico reutilizables.

2.3.3.3. Estándar EAN*UCC

EAN es un organismo de sistemas de numeración encargado de manejar estándares internacionales que permitan la identificación de productos y servicios con el fin de promover un lenguaje común en el comercio. El UCC de igual forma es una asociación encargada de promover estándares de identificación para el comercio electrónico en USA y Canadá.

La integración de estos dos organismos EAN*UCC facilita el acceso a la comercialización de productos y servicios, con códigos de identificación únicos, estándares de comunicación y un comercio electrónico a nivel mundial.

2.3.3.4. Especificación EPCGlobal

EPCGlobal es una asociación entre EAN y UCC con el apoyo de otras entidades más, con el único fin de impulsar a nivel mundial la adopción de la red EPC y poder vincular tecnologías de las cuales RFID es una de ellas, con el fin de crear sistemas de suministros más eficientes (Godínez, 2008).

La red global EPC promueve la identificación en tiempo real, lo que amplía su campo de aplicación a sistemas no solo de suministros sino también a rastreo y localización.

El EPC es un código universal de un producto que está dividido en números y dentro de este se puede identificar al fabricante, producto, versión y número de serie, donde además se pueden incorporar campos especiales (Godínez, 2008). La Figura 11 a continuación muestra un ejemplo de cómo está distribuido el código EPC:

ELECTRONIC PRODUCT CODE			
01	. 0000A89	. 00016F	. 000169DC0
Encabezado	Administrador	Clase de Objeto	Número Serial

Figura 11: Formato de código EPC.

Fuente: Godínez, 2008.

- Encabezado (8 bits).- Identifica la longitud, tipo, estructura, versión y generación de EPC.
- Administrador del número (28 bits).- Identifica a la empresa que adopta el número.
- Clase de Objeto (24 bits).- Identifica la clase de objeto etiquetado.
- Numero serial (36 bits).- Especifica el número del objeto etiquetado.

2.3.3.5. ISO

Los estándares ISO garantizan la fiabilidad y la buena calidad de los productos. La mayoría de los estándares mundiales están dirigidos por ISO con sede en la ciudad de Ginebra (Godínez, 2008).

Dentro de la gran cantidad de estándares que ha emitido la organización, muchos de estos están relacionados con la tecnología RFID. ISO (2015) detalla una gran cantidad de estándares, de entre los cuales se pueden mencionar:

- ISO 6346.- Contenedores de transporte, codificación, identificación y marca.
- ISO 7810.- Tarjetas de identificación, características físicas. Provee criterios de rendimiento, requerimientos para intercambios internacionales, y criterios mínimos con características hombre-máquina.
- ISO 7816.- Tarjetas de identificación con circuito integrado y contactos.
- ISO 9798.- Información tecnológica, técnica de seguridad y autenticación de la entidad.

- ISO 9897.- Normas para contenedores. Equipamiento, intercambio de información, códigos de comunicación.
- ISO 10373.- Tarjetas de identificación. Métodos de test.
- ISO 10374.- Normas para contenedores. Identificación automática.
- ISO 10536.- Tarjetas de identificación. Circuitos integrados para tarjetas sin contactos.
- ISO 11784.- RFID para identificación de animales. Estructura del código.
- ISO 11785.- RFID para identificación de animales. Conceptos técnicos. Especifica el proceso de transmisión entre etiqueta y lector.
- ISO 14223.- RFID para identificación de animales. Lectores avanzados. Contiene el protocolo de interfaz aire.
- ISO 14443.- Tarjetas de identificación. Circuitos integrados para tarjetas sin contactos. Tarjetas de proximidad.
- ISO 14816.- Normas para teletráfico. Equipamiento y automatización de vehículos. Numeración y estructuración de datos.
- ISO 15434.- Información tecnológica. Sintaxis para transferencia de información ADC.
- ISO 15459.- Información tecnológica. Identificación de unidades de transporte.
- ISO 15961.- Información tecnológica. RFID para gestión de objetos. Protocolo de datos e interfaz de aplicación.
- ISO 15962.- Información tecnológica. RFID para gestión de artículos y protocolos de datos. Reglas de codificación de datos y funciones de memoria.
- ISO 15963.- Información tecnológica. RFID para gestión de objetos. Identificación única para etiquetas RF.
- ISO 17358.- Aplicación para cadenas de suministro. Requerimientos de aplicación.

- ISO 17363.- Aplicación para cadenas de suministro. Contenedores de carga.
- ISO 17364.- Aplicación para cadenas de suministro. Unidades de transporte.
- ISO 17365.- Aplicación para cadenas de suministro. Objetos reutilizables.
- ISO 17366.- Aplicación para cadenas de suministro. Empaquetamiento.
- ISO 17367.- Aplicaciones de la cadena de suministro. Producto etiquetado (ISO, 2015).

2.3.3.6. ETSI

El Instituto Europeo de Estándares de Telecomunicaciones-ETSI es una organización sin fines de lucro que se encarga de generar estándares mundialmente aplicables para el desarrollo de las TIC, incluyendo tecnologías móviles, de difusión e internet (ETSI, 2015).

Algunos estándares ETSI relacionados con la tecnología RFID son:

- ETSI TR 102 449.- Telecomunicaciones y Servicios de Internet convergido y Protocolos para Redes Avanzadas; RFID en la industria de las telecomunicaciones.
- ETSI TR 101 445.- Dispositivos de corto alcance destinados para operar en la banda de 862 MHz a 870 MHz; Documento de referencia del sistema para equipos RFID.
- ETSI TR 102 436.- Dispositivos de corto alcance destinados a la operación en la banda de 865 MHz a 868 MHz; Pautas para la instalación y puesta en funcionamiento de equipos de identificación por radiofrecuencia en la banda UHF.
- ETSI TR 102 644.- Pruebas para investigar la interoperabilidad de las etiquetas fabricadas por distintos proveedores.
- ETSI EN 302 291.- Dispositivos de corto alcance; Equipos de comunicación de corto alcance inductivo que operan a 13,56 MHz.

2.3.3. Usos y aplicaciones RFID

La tecnología RFID gracias a sus características y constantes avances abarca una gran cantidad de aplicaciones en distintos sectores industriales, de las cuales se puede mencionar:

2.3.3.1. Sistemas de control de acceso

La tecnología RFID aplicada a un sistema de control de acceso brinda información de localización y seguimiento en tiempo real, con una continua monitorización tanto de personas como de recursos o activos dentro de un entorno (Godínez, 2008).

El principal objetivo de la tecnología aplicada a un sistema de control de acceso es el controlar el acceso a zonas restringidas y reforzar la seguridad, en muchos países este tipo de sistemas es muy utilizado en estaciones de tren y de otros servicios, como se observa en la Figura 12:

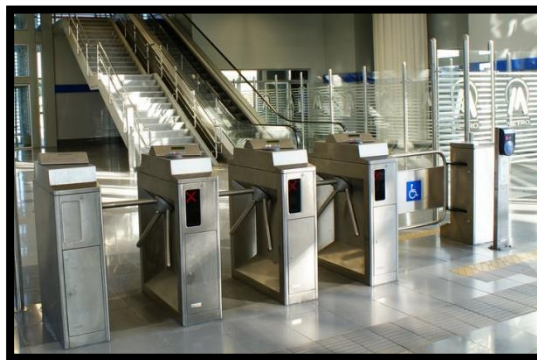


Figura 12: Sistema de Control de Acceso en estación del metro.

Fuente: FLICKR, 2016. Recuperado de: <https://www.flickr.com/photos/opaulus/sets/72157619132188869/>

Se tienen varias ventajas para este tipo de soluciones, entre las cuales se pueden mencionar:

- Localización en tiempo real
- Control de personal para el acceso a zonas restringidas
- Alarmas de control de acceso

- Control de visitantes
- Control de acceso vehicular
- Servicio mejorado de seguridad
- Exactitud en el control
- Acceso a servicios
- Menor tiempo de espera

2.3.3.2. Industrias Farmacéuticas

Una de las áreas de mayor aplicación de la tecnología RFID es justamente la industria farmacéutica, donde en innumerables ocasiones se han producido robos, falsificaciones y el desvío de prescripciones de medicamentos costosos. Una forma de frenar este tipo de ilícitos es aplicando etiquetas RFID como se observa en la Figura 13, mismas que eviten estos problemas y que faciliten a las farmacias y hospitales verificar la validez de los productos y prescripciones (Gidekel, 2008).



Figura 13: Medicamentos con etiquetas RFID.

Fuente: eConfianza, 2011. Recuperado de <https://econfianza.files.wordpress.com/2011/02/medicamento-con-etiqueta-rfid.jpg>

2.3.3.3. Trazabilidad de Alimentos

La aplicación de etiquetas RFID sobre productos alimenticios ayuda a relacionar dichos productos con un identificador único que permita hacer un seguimiento y control adecuado, a través de un lector, como se observa en la Figura 14. Además se puede llevar un control más detallado de los productos facilitando la auditoría de los mismos (Gidekel, 2008).



Figura 14: Trazabilidad de Alimentos con RFID.

Fuente: PATALE BUSINESS ADVISOR CORP, 2016. Recuperado de <http://patale.biz/12-rfid-cadena-de-frio/6-rfid-cadena-de-frio>

2.3.3.4. Identificación y seguimiento de equipajes

Este tipo de aplicación es muy utilizada en aeropuertos y terminales terrestres, donde se inserta una etiqueta en el equipaje, como se indica en la Figura 15, brindando una solución efectiva de seguimiento del mismo. Las etiquetas RFID a diferencia del código de barras presentan una respuesta mucho más veloz y exacta en su lectura (Gidekel, 2008).



Figura 15: Identificación de equipaje con RFID.

Fuente: ELMUNDO.ES, 2006. Recuperado de <http://www.elmundo.es/navegante/2006/07/10/empresas/1152526384.html>

2.3.3.5. Seguimiento de materiales peligrosos

Las industrias químicas manejan un gran número de sustancias peligrosas las cuales deben estar debidamente etiquetadas, y evitar incidentes al momento de transportarlas o manipularlas, es así que una solución a este tipo de problemas es la colocación de etiquetas RFID en cada uno de estos productos con el fin de poder identificar rápidamente el tipo de sustancia, además del grado de peligrosidad que posean dichos químicos (Gidekel, 2008). La Figura 16 muestra la lectura de etiquetas RFID aplicadas en sustancias químicas:



Figura 16: Reconocimiento de sustancias químicas con RFID.

Fuente: RFID JOURNAL, 2016. Recuperado de <http://www.rfidjournal.com/articles/view?10850>

2.3.3.6. Monitoreo y control de inventarios

Esta aplicación es una de las más comunes y se orienta al sector industrial, específicamente para dar seguimiento a partes o piezas en líneas aéreas o de fabricación automotriz. Anteriormente el control de inventario se lo realizaba manualmente, sin embargo se tenía un alto porcentaje de error en el mismo por lo que hoy en día se utilizan sistemas basados en etiquetas y lectores de la tecnología RFID, como se muestra en la Figura 17. Las etiquetas RFID que operan en el rango de frecuencia 13.56 MHz son recomendadas para esta aplicación (Gidekel, 2008).



Figura 17: Control de Inventarios con RFID.

Fuente: SISMODE, 2015. Recuperado de <http://www.sismode.com/tec-rfid.html>

2.4. HARDWARE LIBRE

Se denomina hardware libre u open hardware a todos los dispositivos electrónicos que compartan su información y arquitectura de diseño al usuario, para permitir el desarrollo científico, académico e industrial de proyectos (Aranda, 2014).

El concepto de Open Hardware o Hardware libre nace por los años 70 en los clubes de electrónica de los E.E.U.U y desde ese momento se han venido desarrollando muchos dispositivos y placas destinadas al ámbito estudiantil y de investigación, así se pueden mencionar a Raspberry Pi y Arduino (Aranda, 2014).

2.4.1. Raspberry Pi

Raspberry Pi es una placa de pequeño tamaño que integra la funcionalidad de una computadora, fue desarrollada en Reino Unido por la Fundación Raspberry Pi. Su objetivo es estimular la enseñanza de ciencias de la computación en las escuelas (Raspberry-Pi-Shop, 2016).

Raspberry Pi actualmente cuenta con dos modelos en el mercado, A y B, siendo la principal diferencia las prestaciones que brinda cada una, de donde el modelo B es el más potente (Aranda, 2014). La Figura 18 muestra la placa Raspberry Pi 2:

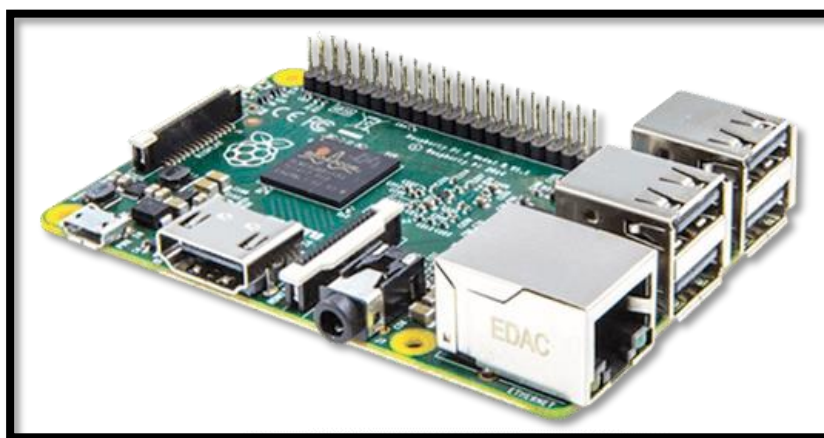


Figura 18: Placa Raspberry Pi 2.

Fuente: Raspberry Pi Shop, 2016. Recuperado de: <http://www.raspberrypi-shop.es/>

Raspberry Pi se desempeña mediante la utilización de software diseñado bajo los sistemas GNU/Linux (Aranda, 2014).

Las placas Raspberry Pi actualmente presentan características muy interesantes, con un chip integrado Broadcom BCM2835, que contiene un procesador ARM con diversas frecuencias de funcionamiento y memoria RAM de hasta 1GB, todo esto equivale a tener un computador con capacidad de reproducir videos en alta definición. Además se cuenta con una salida de audio y video a través de un conector HDMI, para la conexión de las placas a televisores o monitores con

la misma interfaz. Posee también una conexión Ethernet 10/100 y puertos USB que facilitan la conexión de otro tipo de adaptadores (Raspberry-Pi-Shop, 2016).

El modelo B integra un SoC (System on Chip) que contiene varios módulos, los cuales optimizan los recursos de la placa para la obtención de buen rendimiento en espacio reducido (Aranda, 2014).

A continuación en la Tabla 2 se detallan las principales características de las distintas placas Raspberry Pi:

Tabla 2: Tabla comparativa de placas Raspberry Pi.

Características	RPI Modelo A	RPI Modelo B	RPI Modelo B+	RPI2 Modelo B
Procesador	ARM11 ARMV6	ARM11 ARMV6	ARM11 ARMV6	ARM11 ARMV7 ARM CORTEX-A7
Velocidad CPU	700 MHZ	700 MHZ	700 MHZ	4 NÚCLEOS 900 MHZ
SoC	BROADCOM BCM2835	BROADCOM BCM2835	BROADCOM BCM2835	BROADCOM BCM2835
Memoria RAM	256MB	512MB	512MB	1GB
Puertos USB	1	2	4	4
GPIO	40	26	40	40
Video	HDMI 1.4 1920X1200	HDMI 1.4 1920X1200	HDMI 1.4 1920X1200	HDMI 1.4 1920X1200
Almacenamiento	Micro SD	Full SD	Micro SD	Micro SD
Ethernet 10/100	No	Si	Si	Si

Fuente: Raspberry-Pi-Shop, 2016. Recuperado de: <http://www.raspberrypi-shop.es/hardware-raspberrypi.php>

2.4.2. Arduino

Arduino se ha convertido en poco tiempo en una plataforma de gran acogida y en los últimos años ha mostrado gran desarrollo en el campo investigativo de la electrónica, siendo una plataforma abierta de hardware y software flexible de fácil uso, pudiendo utilizarse libremente para el desarrollo de proyectos tecnológicos multidisciplinarios (Arduino, 2015).

Arduino nace en el año 2005 en el Instituto de Diseño Interactivo Ivrea de Italia como un proyecto destinado a estudiantes, con el fin de crear una plataforma útil y sencilla que base su funcionamiento con el uso de un microcontrolador y un entorno de desarrollo (Aranda, 2014).

2.4.2.1. Lenguaje de desarrollo y entorno de programación

La placa Arduino y específicamente el microcontrolador que la conforma se programan en base al lenguaje Arduino que se basa en Wiring y el entorno de desarrollo Arduino basado en Processing (Arduino, 2015).

2.4.2.1.1. Wiring

Wiring se trata de una plataforma abierta para la elaboración de dispositivos o prototipos electrónicos compuestos de un entorno de programación, en la que participan profesionales expertos, estudiantes y demás participantes que aportan y comparten sus ideas, conocimientos e investigaciones para distintos proyectos (Letrán, 2011).

2.4.2.1.2. Processing

Processing es software que permite enseñar los fundamentos de programación en un contenido visual basándose en un lenguaje de programación de código abierto, orientado para usuarios que deseen crear imágenes, animaciones e interacciones, así como también generar trabajos en un contexto profesional (Letrán, 2011).

2.4.2.2. Ventajas y características

Arduino establece su funcionamiento en microcontroladores AVR, específicamente: Atmega8, Atmega168, Atmega328 y Atmega1280 por su simplicidad y bajo costo. Los programas de

Arduino se basan en el lenguaje de programación Processing/Wiring (básicamente C/C++) permitiendo desarrollar múltiples diseños (Martínez, 2014).

Actualmente Arduino es una plataforma de gran uso en proyectos electrónicos de distinta índole gracias a las características que posee, brindando muchas ventajas a los usuarios frente a otro tipo de plataformas de hardware libre. Entre las principales ventajas se pueden citar:

- Su costo es relativamente bajo en comparación a otras placas.
- Posee un software multiplataforma que se ejecuta en distintos sistemas operativos: Windows, Linux y Macintosh.
- Su IDE es sencillo de usar para los principiantes y lo suficientemente flexible para los usuarios avanzados.
- Las placas se basan en la licencia Creative Commons que permiten optimizar o ampliar las funcionalidades de las mismas.

2.4.2.3. IDE de Arduino

El IDE de Arduino se trata de una interfaz bastante simple y amigable con las personas que no tengan experiencia en el desarrollo de software. “El IDE fue desarrollado en Java y tiene características simples, destacando el realce de palabras clave y una base con diversos códigos listos para servir como un ejemplo” (Garrido, 2015, p.35).

Para Arduino (2015):

El entorno de desarrollo integrado de Arduino posee algunas partes: editor de texto para escribir el código de programación, área de mensajes, consola de texto, barra de herramientas

con botones para funciones comunes y una serie de menús. Se conecta al hardware de Arduino para cargar programas y poder comunicarse (párr.1).

La Figura 19 muestra el entorno gráfico que maneja el IDE de Arduino, en el mismo que se identifican 5 secciones importantes:

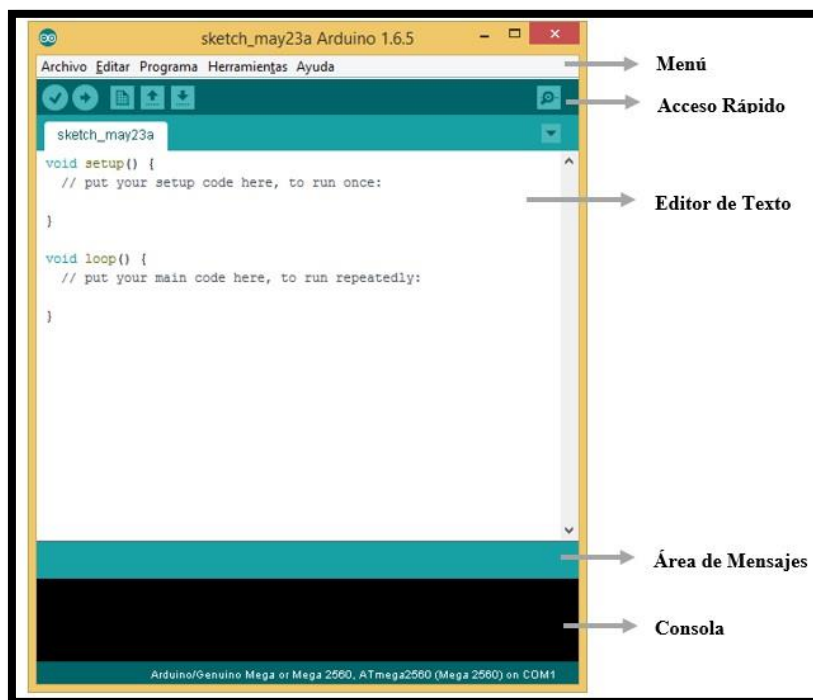


Figura 19: IDE de Arduino.

Fuente: Software de Arduino.

Dentro de cada sección se encuentran distintas opciones que tienen funcionalidades específicas para el desarrollo del programa:

- Archivo.- despliega las opciones de nuevo, abrir, cerrar, salvar, guardar como, imprimir, configurar página, preferencias y salir.
- Editar.- despliega las opciones referentes a la edición del código de programa en el campo de edición de texto.

- Programa.- muestra opciones para compilar, subir, exportar, añadir fichero e inclusión librerías para el uso de distintos dispositivos y sensores.
- Herramientas.- contiene una variedad de funciones de entre las cuales se puede destacar la opción para elegir la placa a utilizar, así como también el puerto de comunicación USB.
- Ayuda.- se despliegan distintas opciones de ayuda para la solución de problemas típicos con el IDE, además de mostrar enlaces directos con la página de Arduino.
- Acceso rápido.- esta barra posee las opciones más útiles al momento de desarrollar programas: verificar, subir, nuevo, abrir y salvar.
- Editor de texto.- es el área donde se desarrollaran los distintos códigos de programación.
- Área de mensajes.- muestra distintos mensajes con respecto a la compilación del código, sean estos mensajes de éxito o error en el código.
- Consola.- en esta área se puede visualizar mensajes con respecto al estado de la memoria, verificación de programas, actualizaciones de estado, etc. (Boxall, 2013).

2.4.2.4. Módulos Arduino

Debido a la aceptación de Arduino en el mercado, se vio la necesidad de desarrollar placas que posean funcionalidades específicas que se adapten a distintas aplicaciones que el usuario desarrollará.

A continuación se detalla algunas de las placas que hasta el momento se han desarrollado y pueden ser utilizadas en la elaboración de un sistema de control de acceso:

- Arduino Uno.
- Arduino Mega 2560.
- Arduino Nano.

- Arduino Micro.
- Arduino Yún.
- Arduino Ethernet.

2.4.2.4.1. Arduino Uno

La placa de Arduino Uno trabaja en torno al microcontrolador Atmega328P y su nombre fue elegido en base a la versión 1.0 del IDE. Posee 14 pines digitales de entrada/salida, 6 de las cuales se pueden utilizar como salidas PWM, además posee 6 pines de entrada analógica, un cristal de cuarzo de 16MHZ, conector USB, conector de alimentación externa y botón de reset (Arduino, 2015). En la Figura 20 se observa la placa Arduino Uno:



Figura 20: Arduino Uno.

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/en/Guide/Windows>

2.4.2.4.2. Arduino MEGA 2560

Según Arduino (2015):

La placa de Arduino MEGA 2560 está basada en el microcontrolador Atmega2560. Cuenta con 54 pines digitales de entrada / salida, de los cuales 15 se pueden utilizar como salidas PWM, 16

entradas analógicas, 4 puertos seriales UART, un oscilador de cristal de 16MHz, conexión USB, conector y un botón de reinicio. La Figura 21 indica la placa Arduino MEGA 2560:

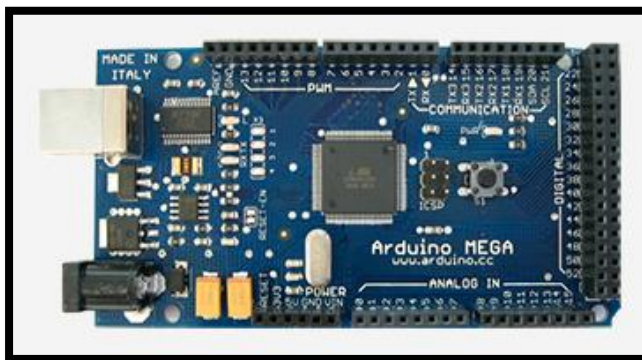


Figura 21: Arduino MEGA.

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/en/Main/ArduinoBoardMega>

2.4.2.4.3. Arduino Nano

El Arduino Nano es una placa de tamaño pequeño que puede ser conectada a un protoboard para facilitar las conexiones. Está basado en el microcontrolador Atmega328, además posee una conexión USB mini-B (Arduino, 2015). En la Figura 22 se observa la placa Arduino Nano:

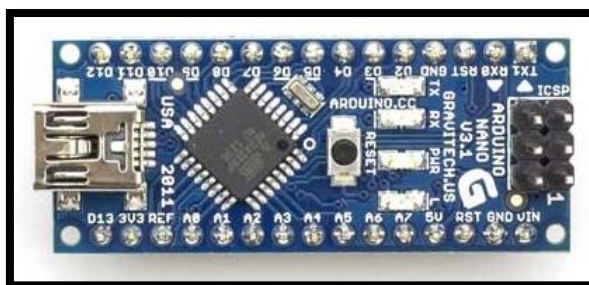


Figura 22: Arduino Nano.

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/en/Main/ArduinoBoardNano>

2.4.2.4.4. *Arduino Yun*

Para Arduino (2015):

La placa electrónica Arduino Yun está basada en el ATmega32u4 y Atheros AR9331, siendo este último compatible con una distribución Linux basada en OpenWrt llamado OpenWrt-Yun. Se tiene una conexión Ethernet y soporte a WiFi, puerto USB-A, ranura para tarjeta micro-SD, 20 pines de entradas/salida digitales, de los cuales 7 se pueden utilizar como salidas PWM y 12 como entradas analógicas, un cristal oscilador de 16 MHz, una conexión micro USB y un 3 botones de reinicio (párr.1). En la Figura 23 se observa la placa Arduino Yún:

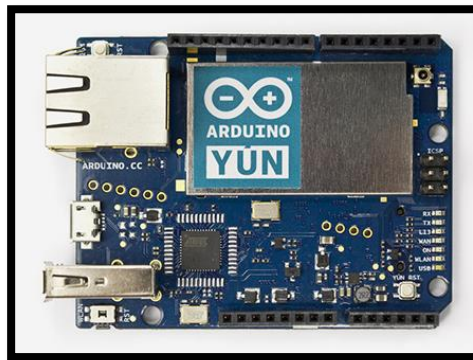


Figura 23: Arduino Yun.

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/en/Main/ArduinoBoardYun>

2.4.2.4.6. *Arduino Micro*

Esta placa pequeña con dimensiones de 40x18 mm, es similar a Arduino Leonardo en lo referente a la incorporación de comunicación USB en el microcontrolador Atmega32u4 (Arduino, 2015), como indica la Figura 24:

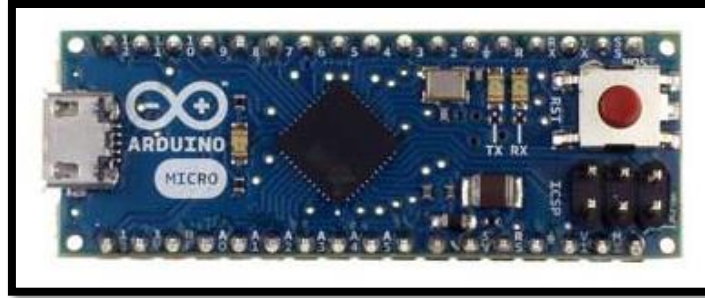


Figura 24: Arduino Micro.

Fuente: ARDUINO, 2015. Recuperado de <https://blog.arduino.cc/2012/11/08/new-arduino-micro-available/>

2.4.2.4.7. Arduino Ethernet

Este tipo de placa está basada en el chip Ethernet Wiznet W5100 que permite conectar a Internet a otra placa Arduino que sea compatible con Arduino Ethernet a una velocidad de 10/100Mbps, esto a través del conector RJ-45 que posee. Tiene un lector de tarjetas micro-SD para almacenar datos a través de la red (Arduino, 2015), como se observa en la Figura 25:



Figura 25: Arduino Ethernet.

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/en/Main/ArduinoEthernetShield>

2.4.2.5. Tabla comparativa de las principales placas Arduino

A continuación la Tabla 3 muestra las características principales que poseen las placas Arduino:

Tabla 3: Tabla comparativa de las placas Arduino.

Características	Arduino Uno	Arduino Mega 2560	Arduino Nano	Arduino Micro	Arduino Yún	Arduino Ethernet
Microcontrolador	Atmega328P	Atmega2560	Atmega168/ Atmega328	Atmega32U4	Atmega32U4	Atmega328
Voltaje de Operación	5V	5V	5V	5V	5V	5V
Voltaje Recomendado	7-12V	7-12V	7-12V	7-12V	5V	7-12V
Voltaje Límite	6-20V	6-20V	6-20V	6-20V	5V	6-20V
Entradas/Salidas Digitales	14(6 PWM)	54(15 PWM)	14(6 PWM)	20(7PWM)	20(7 PWM)	14(4 PWM)
Entradas Analógicas	6	16	8	12	12	6
Corriente DC por Entradas/Salidas	20Ma	20mA	40mA	20mA	40mA	40mA

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/>

2.4.3. Diferencias entre Raspberry y Arduino

En base a la descripción presentada anteriormente, tanto de la plataforma Arduino como Raspberry Pi se puede concluir que, a pesar de ser plataformas que se enfocan en un mismo objetivo, Raspberry y Arduino presentan algunas diferencias. En las dos placas se pueden controlar entradas y salidas, así como también se puede integrar distintos dispositivos; sin embargo, Arduino enfoca su funcionalidad en circuitos de automatización, control y robótica, mientras que, Raspberry se presenta como un computador de pequeño tamaño, que permite integrar funciones multimedia con el control de elementos (Aranda, 2014).

En la Tabla 4 se presentan las principales características que diferencian a Raspberry Pi y Arduino:

Tabla 4: Diferencias entre Raspberry Pi y Arduino.

Características	Raspberry Pi	Arduino
Memoria RAM	Hasta 1GB	256MB
Velocidad de Reloj	700MHZ	16MHZ
Salida Ethernet	10/100	No integrada (excepto Arduino Yun)
Sistema operativo	Distribuciones Linux	Ninguno
Entorno de desarrollo	Scratch, IDLE, cualquiera con soporte Linux	Arduino
Voltaje de entrada	5V	7-12V
Terminales entrada/salida	Hasta 40	Hasta 54
Desarrollo de aplicaciones	Orientado a Software	Orientado a Hardware

Fuente: Hacedores Maker Community, 2016. Recuperado de : <http://hacedores.com/arduino-o-raspberry-pi-cual-es-la-mejor-herramienta-para-ti/>

2.5. ELEMENTOS ELECTRÓNICOS

Todo circuito electrónico posee distintos elementos que cumplen con funciones específicas y generalmente están encapsulados en un material cerámico, metálico o plástico, y tienen dos o más terminales metálicas para su conexión.

Según el tipo de funcionalidad que presenten se puede encontrar elementos del tipo activos, capaces de excitar un circuito y generar ganancias o control. También se encuentran los elementos pasivos, encargados de conectar elementos activos, además de otras funciones específicas que aseguren la transmisión de señales eléctricas (Aristizabal Gómez, 2010).

2.5.1. Resistencias

Las resistencias son componentes eléctricos pasivos que presentan una oposición al paso de la corriente eléctrica, permitiendo controlar el flujo de corriente y tensión dentro de un circuito. Su símbolo esquemático se muestra en la Figura 26 a continuación:

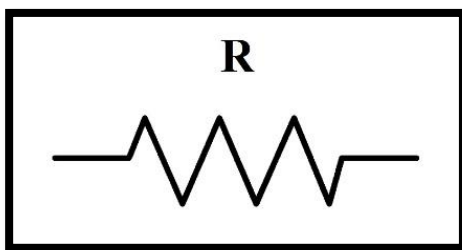


Figura 26: Símbolo esquemático de la resistencia.

Fuente: HADA, 2016. Recuperado de: <http://www.hadaelectronics.com/Tutoriales/?tutorial=4>

El valor de una resistencia viene dado en ohmios y pueden ser fabricadas para soportar disipaciones de 1/8, 1/4, 1/2, 1 y 2 watts de potencia. A medida que aumenta su capacidad de disipación, también aumenta su tamaño, como se observa en la Figura 27:

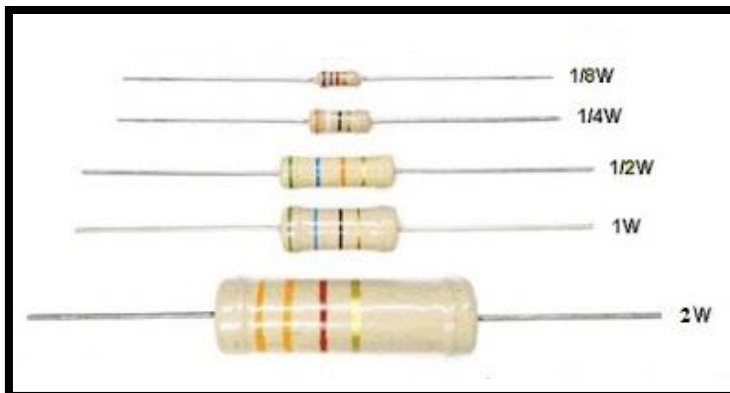


Figura 27: Resistencias de distintas potencias.

Fuente: Robo-Help, 2005. Recuperado de: http://robohelpnews.blogspot.com/2015_07_01_archive.html

Para identificar el valor óhmico de una resistencia se hace uso de un código de colores, que se distribuye en la misma en forma de bandas, como se indica la Figura 28:

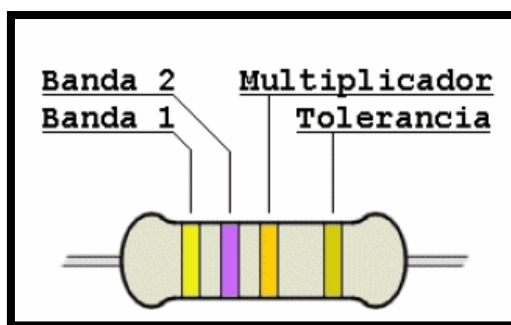


Figura 28: Bandas de colores de resistencia.

Fuente: Bricopage.com, 2003. Recuperado de <http://www.bricopage.com/electricidad/resistencias.htm>

La primera y segunda banda indica valores específicos de cada color, la tercera banda indica el valor por el que se debe multiplicar los dos primeros valores y la cuarta banda muestra el valor porcentual de tolerancia que maneja cada resistencia.

La Tabla 5 muestra el código de colores que manejan las resistencias y sus respectivos valores en cada una de sus bandas:

Tabla 5: Código de colores de resistencias.

Color	1ra banda	2da banda	Multiplicadora	Tolerancia
Negro	---	0	x1	
Marrón	1	1	x10	1%
Rojo	2	2	x100	2%
Naranja	3	3	x1000	
Amarillo	4	4	x10000	
Verde	5	5	x100000	0.50%
Azul	6	6	x1000000	
Violeta	7	7	---	
Gris	8	8	---	
Blanco	9	9	---	
Dorado			x0.1	5%
Plata			x0.01	10%
Sin color				20%

Fuente: D'Addario, 2015.

2.5.2. Capacitores

Un capacitor es un componente pasivo capaz de almacenar energía durante un tiempo determinado, la misma que después de dicho periodo se descarga. Su valor se representa en faradios y su símbolo esquemático se muestra en la Figura 29, en donde se puede observar dos tipos de representación, uno para un capacitor normal y otro para un capacitor electrolítico o polarizado:

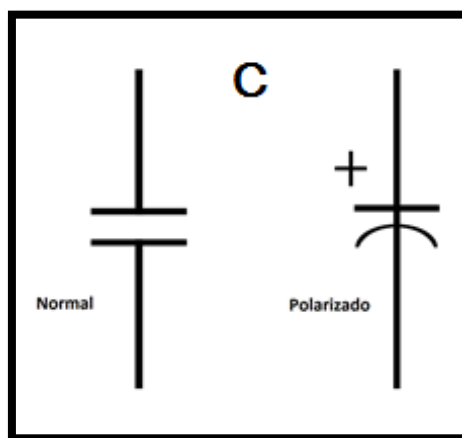


Figura 29: Símbolo esquemático del capacitor.

Fuente: PROMETEC, 2016. Recuperado de: <http://www.prometec.net/fuentes-de-alimentacion/>

Su comportamiento varía de acuerdo al tipo de corriente suministrada, es así que para corriente continua opera como un circuito abierto (D'Addario, 2015). A continuación la Figura 30 muestra algunos tipos de capacitores, de los cuales se puede observar un capacitor electrolítico, mismo que lleva en si su valor de capacitancia expresado en micro faradios y su voltaje. Además este tipo de capacitor al poseer polaridad, su terminal negativo puede ser identificado a través de una banda que especifica el mismo.

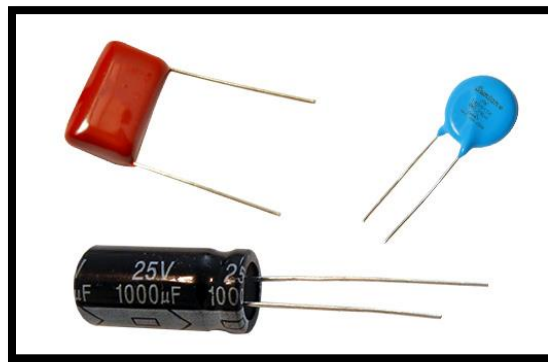


Figura 30: Tipos de Capacitores.

Fuente: CODICE, 2016. Recuperado de <http://www.codice-sa.com.mx/capacitores/capacitores.html>

Por otro lado un capacitor normal o de tipo cerámico lleva impreso un número, del cual, el último dígito indica el número de ceros que se debe poner al mismo, de esta forma el valor que queda se encuentra expresado en pico faradios. A continuación la Figura 31 muestra un ejemplo de un capacitor cerámico 104, del cual su valor en pico faradios es 100000pF de acuerdo a la explicación anterior. Sin embargo también se puede expresar el valor de capacitor utilizando otros prefijos, es así que, el mismo capacitor 104 se lo puede expresar como un capacitor de 100nF o 0.1µF.



Figura 31: Capacitor cerámico 104.

Fuente: Central Clubs, 2016. Recuperado de: <http://www.centralclubs.com/capacitor-t117231.html>

2.5.3. Diodos

Un diodo es un elemento semiconductor de dos terminales, compuesto por un material de tipo N y otro de tipo P. Su función principal radica en la rectificación de una señal de corriente alterna, permitiendo convertir esta señal en corriente continua pulsante (Ramos Alvarez, 2012). Su símbolo se muestra en la Figura 32, en la que también se observa que el elemento lleva en si un código el cual especifica sus características eléctricas y de funcionamiento. Además se puede identificar su polaridad a través de una banda, la cual indica terminal negativo del diodo o el cátodo.

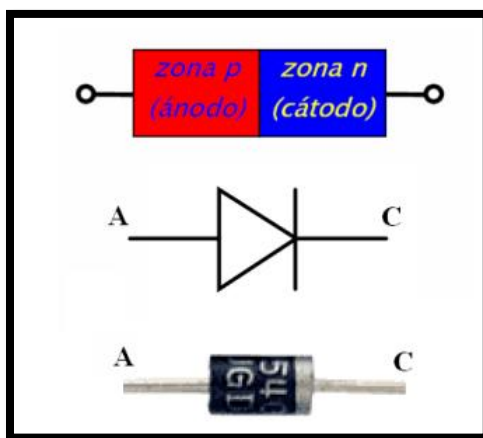


Figura 32: Símbolo del diodo.

Fuente: Gerzo Alejandro, 2015. Recuperado de: <https://gerzoalejandro.wordpress.com/2015/02/06/practica-diodos/>

Un diodo se polariza en forma directa, al aplicar una tensión positiva al ánodo, de esta forma se empezara a conducir la señal a través de él, por otro lado si se polariza de forma inversa el diodo actuará como un interruptor abierto y no conducirá.

2.5.4. Diodos LED (Light Emited Diode)

Los diodos emisores de luz son componentes semiconductores pasivos que poseen dos terminales como se observa en la Figura 33: ánodo y cátodo, los cuales polarizados correctamente generan una luz de espectro reducido. Su aplicación más común es como indicadores en distintos circuitos electrónicos (Melgoza, 2013).

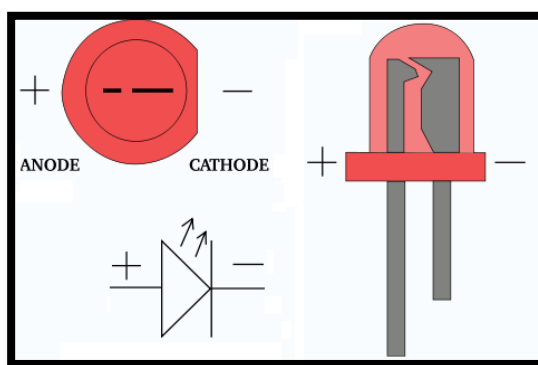


Figura 33. Estructura de diodo LED.

Fuente: Society of Robots, 2014. Recuperado de http://www.societyofrobots.com/electronics_led_tutorial.shtml

El voltaje y corriente de operación de un diodo LED varía de acuerdo al material de elaboración de cada uno, es así que se tienen algunos tipos de diodos con distintos colores y distinta intensidad luminosa.

La Tabla 6 a continuación muestra los distintos tipos de diodos LED, con sus características eléctricas de funcionamiento y su material de construcción:

Tabla 6: Características eléctricas de distintos tipos de diodos LED.

Color	Material de construcción	Voltaje	Corriente
Rojo	GaAsP	1,8V	20mA
Verde	GaP	2,2V	20mA
Amarillo	AlInGaP	2.1V	20mA
Naranja	GaAsP	2V	20mA
Blanco	GaN	4,1V	30mA
Azúl	GaN	5V	30mA

Fuente: Boylestad & Nashelsky, 2009.

2.5.5. Transistores de unión bipolar

Los transistores son componentes semiconductores que cumplen con funciones específicas de amplificación, oscilación, conmutación y rectificación. En función a la configuración de los bloques que conforman el transistor se tienen transistores de tipo NPN y PNP (Melgoza, 2013). Poseen tres terminales: base, emisor y colector, como se observa en la Figura 34:

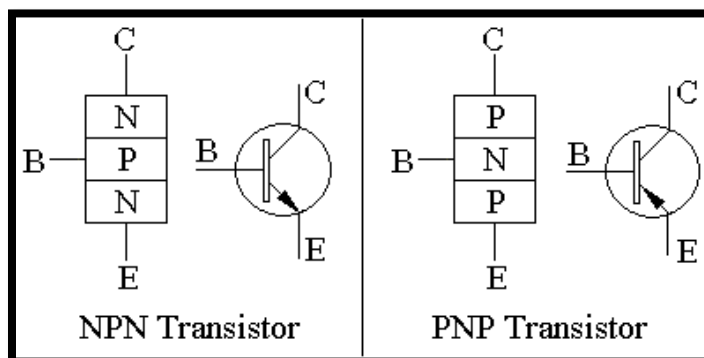


Figura 34. Tipos de transistores Bipolares.

Fuente: Quora, 2015. Recuperado de <https://www.quora.com/topic/Transistors>

Normalmente un transistor lleva en si un código de identificación, de acuerdo al tipo y a las características que maneje el mismo, la Figura 35 indica un transistor de base epitaxial y un transistor de silicio de tipo NPN, los cuales difieren en su tamaño y forma de acuerdo a la función y aplicación que cumplen, además se puede apreciar el código de cada uno de estos impreso sobre su base:

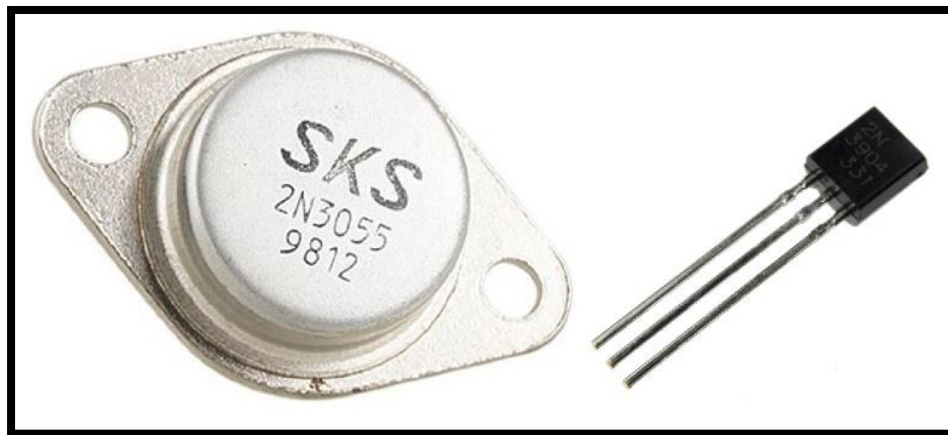


Figura 35: Tipos de transistores BJT.

Fuente: Twuenga, 2016. Recuperado de: <http://www.twenga.es/transistor.html>

De acuerdo a la aplicación que se le vaya a dar a un transistor se pueden tener algunos tipos de configuraciones, como se observa en la Figura 36 a continuación:

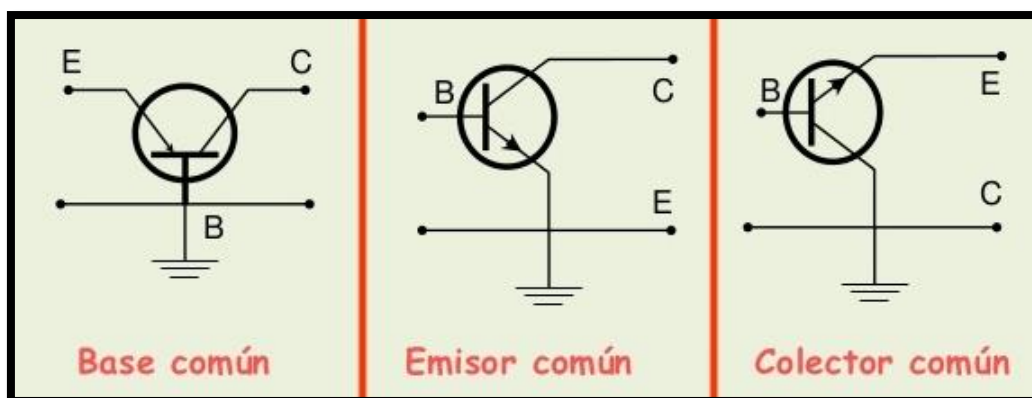


Figura 36: Configuraciones de un transistor BJT.

Fuente: Ortiga, 2014. Recuperado de: <http://es.slideshare.net/ooortigaaa/transistor-bjt-y-fet-uni>

Cada una de estas configuraciones posee características específicas, que se detallan a continuación.

- Base común.- se caracteriza por tener una baja impedancia de entrada y es apta para adaptar fuentes de señal de baja impedancia de salida (Hernandez Ovando, 2012).

- Emisor común.- esta configuración es la más utilizada, ya que se puede amplificar voltaje como corriente y es utilizada en circuitos de baja frecuencia, debido a su alta impedancia de entrada (Hernandez Ovando, 2012).
- Colector común.- este tipo de configuración es utilizada para circuitos igualadores de impedancia, ya que tiene una alta impedancia de entrada y una baja impedancia de salida (Boylestad & Nashelsky, 2009).

2.5.6. Relés

Un relé es un dispositivo electromecánico que opera como un interruptor controlado por un electroimán, que retorna a su posición inicial cuando la fuerza que lo acciona deja de actuar. Su funcionamiento se basa en la excitación de una bobina que magnetiza un núcleo ferromagnético que atrae la parte móvil donde se encuentran los contactos (Castillo, 2012). La Figura 37 muestra la estructura de un relé:

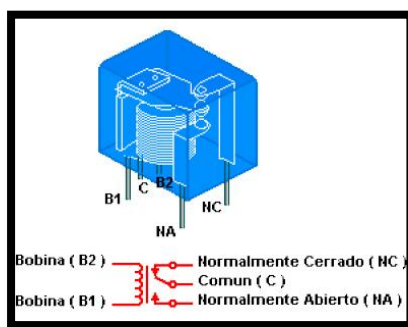


Figura 37. Estructura de un Relé.

Fuente: Foros de Electrónica, 2016. Recuperado de <http://www.forosdeelectronica.com/f27/existe-contrario-rele-96220/>

Un relé tiene como propósito principal controlar circuitos de mayor potencia a través de su activación con una corriente reducida. Existen algunos tipos de relés que varían de acuerdo a la corriente y voltaje de funcionamiento, como se indica en la Figura 38, en la que se observan

distintos tipos de relés, los cuales están identificados mediante un código que llevan impreso sobre ellos.

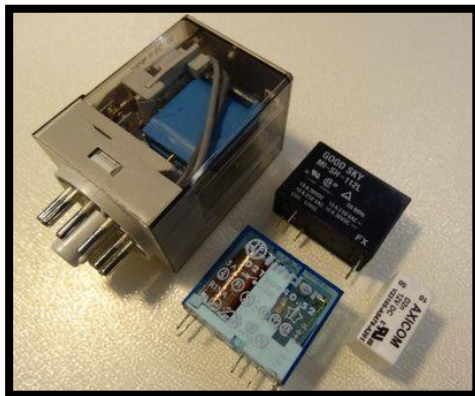


Figura 38: Tipos de relés.

Fuente: INVENTABLE, 2015. Recuperado de: <http://www.inventable.eu/introduccion-a-los-reles/>

2.5.7. Transformadores

Un transformador es un dispositivo eléctrico formado por dos bobinas, las cuales están separadas por algún tipo de núcleo, sea este de ferrita, hierro, aire, entre otros. Cada una de las bobinas adopta un nombre específico, y es así que se las conoce como bobina primaria y bobina secundaria, de donde, la bobina primaria es la que recibe el suministro de corriente alterna a la entrada, mientras que la secundaria entrega una corriente a la salida con un nivel de voltaje distinto al que ingreso.

La Figura 39 a continuación muestra el símbolo eléctrico de un transformador con núcleo de hierro:

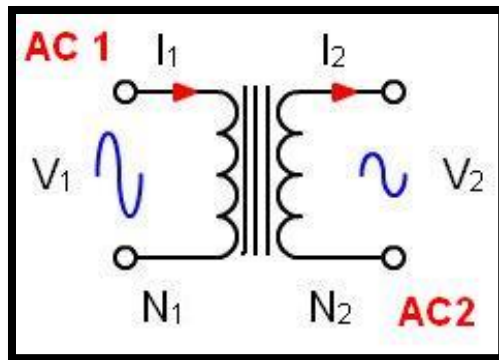


Figura 39: Símbolo eléctrico de un transformador.

Fuente: Kits-Electrónica, 2016. Recuperado de: <http://www.kitelectronica.com/2016/02/electronica-basica-el-transformador.html>

Su funcionamiento se basa en la inducción electromagnética, donde el campo magnético generado por la bobina primaria es inducido o pasado hacia la bobina secundaria, la misma que generará una fuerza electromagnética en proporción al número de vueltas que tenga la misma (Kits-Electrónica, 2016).

Existen varios tipos de transformadores que difieren de acuerdo al tipo de aplicación que vayan a tener y específicamente al número de espiras que tenga cada bobina. Entre los más comunes están los transformadores elevadores, los mismos que a su salida tendrán un voltaje mayor que el de entrada. También están los transformadores reductores los cuales tendrán un voltaje a su salida inferior al de la entrada, estos últimos son los más utilizados para la construcción de fuentes de alimentación. La Figura 40 muestra un transformador reductor de 230VAC a 12VAC:

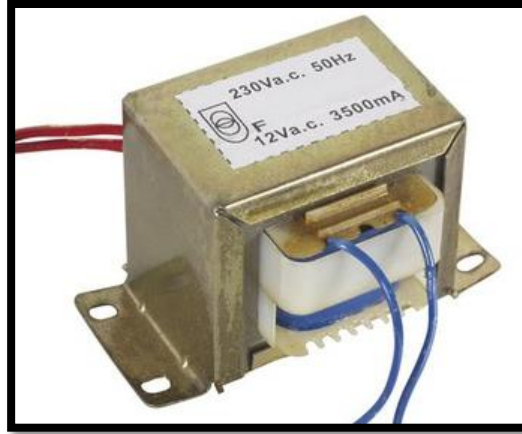


Figura 40: transformador reductor de 12V.

Fuente: Eclats-Antivolts, 2016. Recuperado de: http://www.eclats-antivolts.fr/transformador-chasis-abierto-42va-1-x_T12F3500_itm_spanish.html

2.5.8. Reguladores de voltaje

Un regulador de voltaje es un circuito integrado, el cual se encarga de proporcionar un voltaje DC de salida constante, independiente del voltaje de entrada (Floyd, 2008). Estos dispositivos son muy utilizados en fuentes de alimentación, y se los coloca luego de la salida filtrada de un rectificador. Existen muchos tipos de reguladores de acuerdo al voltaje de salida que suministren, los más comunes son los reguladores de voltaje fijo y de voltaje ajustable. Cuentan con tres terminales de conexión, los mismos que se indican en la Figura 41:

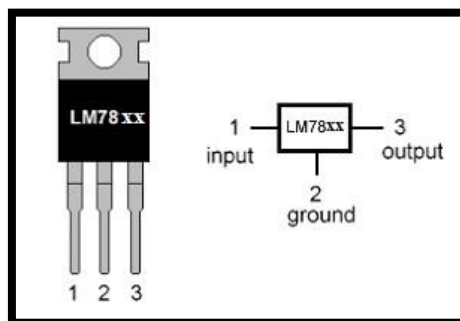


Figura 41: Estructura y símbolo de un regulador de voltaje.

Fuente: ETOOLS, 2016. Recuperado de: <http://www.electrontools.com/Home/WP/2016/03/09/regulador-de-voltaje-7805/>

2.5.9. Pantalla gráfica LCD

Una pantalla gráfica LCD es un dispositivo electrónico que permite visualizar distintos caracteres y símbolos. Existe una gran variedad de estos dispositivos y cada uno varía del otro de acuerdo al número de caracteres que se puedan visualizar en ellos. Una de las pantallas graficas más comunes es la pantalla LCD 16x2, misma que está formada por dos filas en las que se pueden visualizar 16 caracteres al mismo tiempo, posee 16 terminales como se observa en la Figura 42:

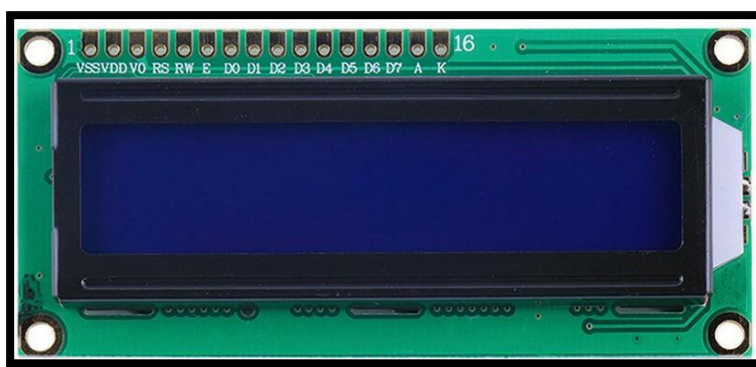


Figura 42: LCD 16x2.

Fuente: *Electrónica Store*, 2015. Recuperado de: <http://electronicastore.net/producto/lcd-16x2-hd4478-display-con-luz-de-fondo-azul/>

Cada uno de los terminales que posee la LCD 16x2 cumple con una función específica, la cual se detalla en la Tabla 7 a continuación:

Tabla 7: Funciones de cada terminal de una pantalla LCD.

Número de Pin	Símbolo	Función
1	VSS	GND
2	VDD	+3V/+5V
3	VO	Ajuste de Contraste
4	RS	Selección de registro ("1" datos, "0" instrucciones)
5	RW	Lectura/Escritura ("1" lectura, "0" escritura)
6	E	Habilitación
7	D0	Bit de datos
8	D1	Bit de datos
9	D2	Bit de datos
10	D3	Bit de datos

11	D4	Bit de datos
12	D5	Bit de datos
13	D6	Bit de datos
14	D7	Bit de datos
15	A	Ánodo del Led
16	K	Cátodo del Led

Fuente: Vishay, 2015. Recuperado de <http://www.engineersgarage.com/sites/default/files/LCD%2016x2.pdf>

2.5.10. Teclado matricial

Un teclado matricial es un dispositivo que está formado por pulsadores digitales conectados en filas y columnas en forma de matriz como se muestra en la Figura 43, a los cuales se les asigna un símbolo o carácter específico.

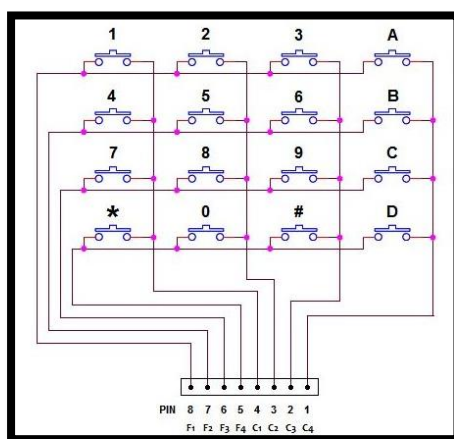


Figura 43: Estructura de un teclado matricial 4x4.

Fuente: Hudor, 2014. Recuperado de <http://huborarduino.com/programacion/curso-programacion/34-leccion15.html>

Actualmente existen dos tipos de teclados matriciales, los cuales se diferencian por el número de teclas o botones que poseen, siendo estos los teclados 4x3 y 4x4. Además del número de botones, existe otra característica que los diferencian y es la forma física del dispositivo, teniendo así teclados flexibles y adheribles, denominados tipo membrana. La Figura 44 muestra un teclado 4x4 tipo membrana:

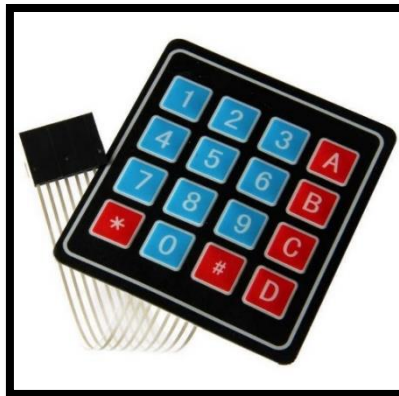


Figura 44: Teclado matricial tipo membrana 4x4.

Fuente: Electrónica Store, 2015. Recuperado de: <http://electronicastore.net/producto/teclado-matricial-4x4-compatible-con-arduino-y-microcontroladores/>

La utilización de este tipo de dispositivos se ha vuelto muy práctica de realizar ya que hoy en día se han creado librerías que permiten su uso de forma fácil y rápida al momento de conectarlo a cualquier dispositivo de hardware libre, para este caso será Arduino.

La Tabla 8 muestra algunas de las principales características que posee un teclado matricial:

Tabla 8: Características de teclado matricial 4x4.

Características	Parámetros
Tensión máxima de alimentación	24V
Corriente de Operación	30mA
Resistencia de aislamiento	100MΩ
Tiempo de rebote (Bounce time)	≤5 ms
Temperatura de Operación	0-50°C
Dimensiones	6.9 x 7.6 cm

Fuente: PARALLAX Inc., 2011. Recuperado de http://www.electronicoscaldas.com/datasheet/27899_Parallax.pdf

2.6. INTRODUCCIÓN A REDES

Un sistema de comunicación tiene como fin intercambiar información entre las entidades que lo conforman, para ello se ha establecido modelos de referencia por capas que contribuyan al análisis del envío y recepción de la información en dichos sistemas.

Las comunicaciones a nivel mundial inician su cambio y avance en la década de los años 70 y 80, y es específicamente en el año de 1969 en que el Departamento de defensa de los Estados Unidos financia un proyecto de investigación y crea la Agencia de proyectos de investigación avanzada.

ARPANET se estableció como una red de conmutación de paquetes de computadoras conectadas mediante líneas punto a punto alquiladas, sin embargo las investigaciones continuaron y se hizo necesario tener una interconexión de redes de arquitectura abierta, de ahí nace Internet, que se basó en la idea de que habría múltiples redes independientes para conectar (Cerf, y otros, 2016).

Con esa base se empezaron a desarrollar varias convenciones por ARPA con el fin de especificar la forma en la que las computadoras individuales puedan comunicarse entre sí, a través de la red, esto posteriormente se convirtió en TCP/IP.

2.6.1. Modelo de referencia TCP/IP

El modelo de referencia TCP/IP ha venido desarrollándose durante muchos años atrás, con el fin de conseguir la interconexión de distintos sistemas de comunicación o redes totalmente incompatibles entre sí, mediante un conjunto de protocolos de comunicaciones que permitan interoperar o llegar a constituir un lenguaje común entre dichos sistemas que estén conectados a la red (Gómez Vieites & Otero Barros, 2011).

La fortaleza principal del modelo TCP/IP son sus protocolos, los cuales han venido desarrollándose hasta establecerse como una arquitectura dominante que rige Internet, esto gracias a sus dos protocolos primarios (Tanenbaum & Wetherall, 2012).

TCP/IP hace referencia a un modelo por capas, que a diferencia del modelo OSI que contiene siete capas, TCP/IP únicamente opera bajo el uso de cuatro. Sin embargo también se puede trabajar con un modelo híbrido de cinco capas, como se indica en la Figura 45:

OSI	TCP/IP	Modelo Híbrido
Aplicación	Aplicación	Aplicación
Presentación		
Sesión		
Transporte	Transporte	Transporte
Red	Red	Red
Enlace de Datos	Enlace de Datos	Enlace de Datos
Física		Física

Figura 45: Modelo en capas TCP/IP.

Fuente: Tanenbaum & Wetherall, 2012.

2.6.1.1. Capa enlace de datos

La capa más baja de este modelo es la capa enlace de datos, en esta se define el tipo de enlaces la interfaz física y el medio de transmisión a través del cual se realizará la trasmisión de información. “Esta capa se encarga de especificar todas las características correspondientes al medio de transmisión, naturaleza de las señales, velocidad de datos, entre otras cuestiones afines” (Stallings, 2004, p.17).

Esta capa al estar relacionada con el acceso a la red y el encaminamiento de datos, maneja algunas tecnologías de acceso de red tanto para LAN como para WAN, de las cuales se pueden mencionar los siguientes: Ethernet, ATM, Frame Relay, 802.11, etc.

En esta capa se emplean dos protocolos de bajo nivel que se manejan tanto en capa acceso, así como también en la capa internet. Estos protocolos son:

- ARP.- Este protocolo se encarga de realizar la conversión entre direcciones IP a direcciones físicas en redes que soporten difusión.
- RARP.- Desempeña la función inversa del protocolo ARP.

2.6.1.2. Capa de red

La capa de red o internet es la encargada del enrutamiento de los datos desde un origen hacia un destino a través de la red, es decir que permite a los host el envío de paquetes en cualquier red y que viajen de forma independiente hacia cualquier destino (Tanenbaum & Wetherall, 2012).

Dentro de esta capa se define uno de los protocolos con más importancia que maneja el modelo TCP/IP, y es el protocolo IP, además de un protocolo complementario denominado ICMP.

- Protocolo IP.- Se trata de un protocolo no orientado a conexión, no confiable, que ofrece el servicio de menor esfuerzo, sin embargo, este protocolo es el de mayor importancia en esta capa y su objetivo es el enrutamiento o encaminamiento de los paquetes de datos por la red, seleccionando la ruta que deben seguir para llegar a su destino (Gómez Vieites & Otero Barros, 2011).
- Protocolo ICMP.- Este protocolo permite a IP intercambiar mensajes de control y error, utilizando un esquema de prueba/respuesta de eco, con el fin de comprobar si un destino es alcanzable o no.

2.6.1.2.1. El protocolo Ipv4

IPv4 es la versión 4 del Protocolo IP que se caracteriza por estar constituida por direcciones de 32 bits. Dentro de la capa Internet del modelo TCP/IP los paquetes se denominan datagramas. Un datagrama consta de dos partes: la cabecera y la carga útil (Tanenbaum & Wetherall, 2012).

A continuación en la Figura 46 se muestran los campos que componen la cabecera IPv4:



Figura 46: Cabecera IPv4.

Fuente: Tanenbaum & Wetherall, 2012.

- Versión (4bits).- indica el número de versión del protocolo.
- HLEN (bits).- longitud de la cabecera.
- Tipo de servicios (8 bits).- especifica los parámetros de seguridad, prioridad, retardo y rendimiento.
- Longitud total (16 bits).- Especifica la longitud total del datagrama.
- Identificador (16 bits).- Número de secuencia utilizado para identificar de forma única al datagrama.
- Indicadores (3 bits).- Solo 2 de los 3 bits de este campo están definidos. Los dos bits utilizados sirven para el control de la fragmentación, donde se especifica si el paquete puede o no fragmentarse, puede ser el primero o el último fragmento.
- Desplazamiento del fragmento (13 bits).- Muestra el desplazamiento de los datos dentro del datagrama original.
- Tiempo de vida (8 bits).- Especifica el número de saltos del datagrama antes de ser descartado.

- Protocolo (8 bits).- Especifica el protocolo de nivel superior que se encuentra encapsulado en el datagrama.
- Suma de comprobación de la cabecera (16 bits).- Provee de un código de detección de errores que ayude a comprobar la integridad de la cabecera.
- Dirección origen (32 bits).- Contienen la dirección IPv4 que identifica el origen del datagrama.
- Dirección destino (32 bits).- Este campo contiene la dirección IPv4 del destino del datagrama.
- Opciones (variable).- Contiene funcionalidades solicitadas por el usuario para el envío del datagrama.
- Relleno (variable).- Este campo se utiliza para asegurar que la cabecera tenga una longitud múltiplo de 32 bits.
- Datos (variable).- Este campo debe tener una longitud múltiplo de 8 bits.

2.6.1.2.2. Direccionamiento Ipv4

Una característica importante que define a las direcciones IPv4 es su longitud de 32 bits, en la que se pueden definir 3 campos: la clase, identificador de la red y el identificador de estaciones o host (Tanenbaum & Wetherall, 2012). La Figura 47 muestra los tres campos que componen a una dirección IP:

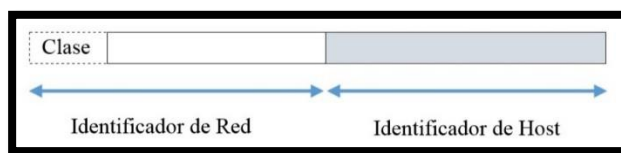


Figura 47: Campos que componen a una dirección IP.

Fuente: Tanenbaum & Wetherall, 2012.

Actualmente existen 5 patrones que permiten diferenciar distintas clases de direcciones, como se observa en la Figura 48, cada una está orientada a cubrir necesidades específicas en las aplicaciones de las redes de comunicación.

- Clase A.- Esta clase de redes utilizan un prefijo de 1byte para identificar la clase y la porción de red, dedicando tres bytes para los host dentro de la subred, esto significa que se tendrá pocas redes con muchos host (Gómez Vieites & Otero Barros, 2011).
- Clase B.- En este tipo de direcciones se emplea un prefijo de dos bytes para identificar la clase y red, mientras que los dos restantes serán para los host (Gómez Vieites & Otero Barros, 2011).
- Clase C.- En esta clase de direcciones se emplean tres bytes para el identificador de clase y red, y tan solo un byte para host, es decir que se tendrá varias redes con pocas computadoras (Gómez Vieites & Otero Barros, 2011).
- Clase D.- Este tipo de direcciones están reservadas para casos especiales, específicamente para multienvio o multidifusión de datos (Gómez Vieites & Otero Barros, 2011).
- Clase E.- Utilizadas en investigaciones y para usos futuros.

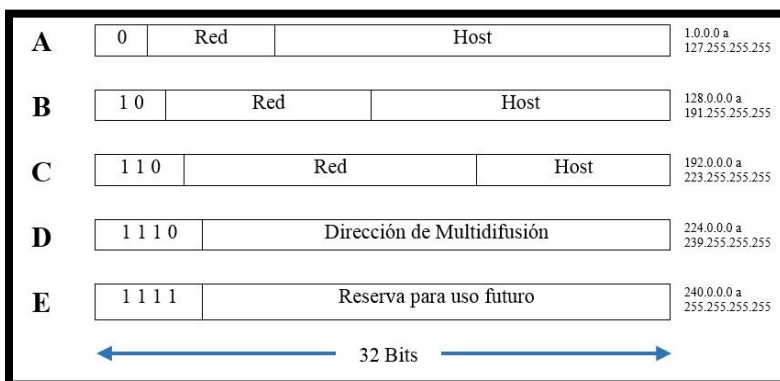


Figura 48: Formato de direcciones IP.

Fuente: Tanenbaum & Wetherall, 2012.

2.6.1.3. Capa transporte

Esta capa es la encargada de proporcionar una comunicación extremo a extremo, incluyendo mecanismos de seguridad. En este nivel de capa transporte se encuentran dos protocolos: TCP y UDP.

- TCP.- Es un protocolo confiable orientado a conexión que asegura la integridad de los datos de origen a destino, con un manejo de mecanismos de detección de errores y control de flujo, proporcionando servicios completos de transporte a las aplicaciones (Tanenbaum & Wetherall, 2012).
- UDP.- Este es un protocolo no confiable, no orientado a conexión en el que la recepción de la información no es garantizada, no provee mecanismos de control de errores y flujo (Tanenbaum & Wetherall, 2012).

2.6.1.4 Capa aplicación

La capa aplicación contiene todos los protocolos de alto nivel, y es la encargada de proporcionar la comunicación de procesos o aplicaciones entre dos host distintos (Tanenbaum & Wetherall, 2012). La capa Aplicación interactúa con la capa transporte enviando y recibiendo información necesaria para las aplicaciones.

Dentro de esta capa se manejan varios protocolos de aplicación, entre los principales se pueden mencionar:

- DNS.- Sistema de nombres de dominio.
- TELNET.- Protocolo de conexión remota.
- FTP.- Protocolo de transferencia de ficheros.

- SMTP.- Protocolo sencillo de transferencia de correo electrónico.
- SNMP.- Protocolo sencillo de gestión de redes.
- HTTP.- Protocolo para la transferencia de hipertextos.

2.7. BASE DE DATOS

Inicialmente, los distintos organismos y empresas que comenzaron a utilizar sistemas informáticos para almacenar datos, manejaban programas que hacían uso de distintos tipos de archivos de almacenamiento o ficheros. De cierto modo este tipo de almacenamiento con el tiempo fue generando serias dificultades, considerando que cada equipo debía encargarse de su propia gestión, mantenimiento, y debido al incremento de información y de usuarios que debían acceder a la misma, surgieron problemas de duplicidad de información, ficheros incompatibles, deficiencia en la seguridad y falta de organización en la información. Estas dificultades llevaron a crear un sistema centralizado y organizado de información en forma de base de datos (Hueso Ibañez, 2012).

Actualmente las bases de datos tienen un amplio uso que va desde pequeños negocios y hogares, hasta grandes empresas y agencias gubernamentales y de cierto modo día a día están en constante contacto, sea directa o indirectamente (Ricardo, 2009).

En su definición más sencilla se puede decir que una base de datos es un conjunto de información almacenada y relacionada lógicamente, a la que pueden acceder varios usuarios al mismo tiempo (Hueso Ibañez, 2012).

2.7.1. Arquitectura de Base de Datos

ANSI-SPARC estableció un estándar para la creación de bases de datos basadas en una arquitectura de tres niveles con el objetivo de tener una independencia de la información, que

permita modificar el esquema en un nivel sin tener que modificar un esquema de nivel superior (Hueso Ibañez, 2012).

Los tres niveles en una arquitectura de Base de Datos son los siguientes:

- Nivel Interno.- describe los detalles para almacenar información, así como también métodos de acceso a la misma (ficheros, discos, directorios, etc.).
- Nivel Global.- describe toda la estructura de la base de datos mediante un esquema conceptual (entidades, atributos, relaciones y restricciones).
- Nivel Externo.- describe la parte de la base de datos que interesa a un grupo de usuarios, ocultando el resto de la misma.

Dado que una base de datos tiende a crecer a medida que incrementa el número de usuarios y de información, se deben manejar herramientas que permitan describir de mejor forma los datos, su relación y restricción, para ello se hará uso de un modelo de datos que ayude a representar una sección de interés de la información (Hueso Ibañez, 2012).

2.7.2. Sistemas Gestores de Bases de Datos

Dado que los modelos nos ayudan a representar de forma sencilla la información, se requiere de una aplicación que permita a los usuarios crear y mantener la base de datos, así como también mantener un acceso controlado a la misma. Esta aplicación o software se denomina Sistema de Gestión de Base de Datos (SGBD) y sirve de interfaz entre el usuario y la base de datos, como indica la Figura 49 (Hueso Ibañez, 2012). Actualmente existen muchos sistemas gestores de bases de datos, de entre los cuales se pueden mencionar: Oracle, MySQL, SQL Server, PostgreSQL, etc.

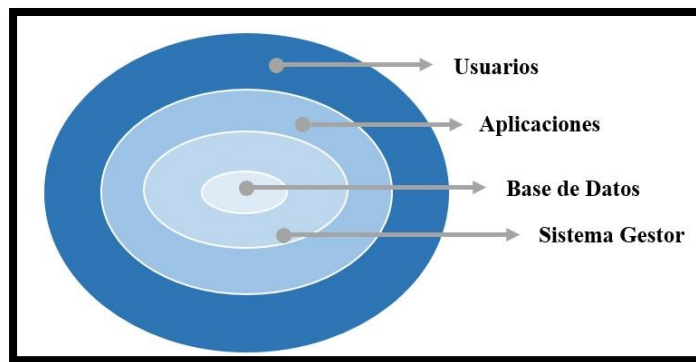


Figura 49: Sistema gestor como interfaz entre usuarios y base de datos.

Fuente: Hueso Ibañez, 2012.

2.7.2.1. MySQL

MySQL es el sistema de gestión de base de datos de código abierto más popular y de mayor aceptación mundial, que permite la oferta económica de aplicaciones de bases de datos fiables, de alto rendimiento y fácilmente ampliables (ORACLE, 2016). La Figura 50 muestra el logo oficial de MySQL:



Figura 50: Logo MySQL.

Fuente: ORACLE, 2016. Recuperado de <https://www.mysql.com/about/legal/logos.html>

Oracle impulsa la innovación de MySQL, la entrega de nuevas capacidades a la web de próxima generación de potencia, nube, aplicaciones móviles e integradas, esto hace que se convierta en una opción atractiva para la realización de distintas aplicaciones de tipo comercial, gracias a su facilidad de uso y rápida puesta en marcha. Una ventaja importante de este tipo de base de datos

es su libre distribución en Internet bajo licencia GPL (General Public License) con un alto grado de estabilidad y un rápido desarrollo (Casillas Santillán, Ginestà, & Pérez Mora, s.f).

2.7.3. Bases de Datos Centralizadas

Un sistema que contenga una base de datos centralizada tiene todos sus componentes en un mismo lugar, sean estos: software, datos y soportes fijos (Hueso Ibañez, 2012).

Entre las características más relevantes de las bases de datos centralizadas se pueden mencionar las siguientes:

- La información se almacena en su totalidad en un solo servidor central, evitando redundancia.
- No posee distintos elementos para su procesamiento ni mecanismos para la intercomunicación, esto a diferencia de las bases de datos distribuidas.
- Los componentes de las bases de datos centralizadas son: los datos, el software de gestión de bases de datos y los dispositivos de almacenamiento.
- Los problemas de seguridad son relativamente fáciles en estos sistemas de bases de datos.
- El procesamiento de los datos ofrece un mejor rendimiento y resulta más confiable que los sistemas distribuidos.
- Menor complejidad en su diseño.

CAPÍTULO III

3. DISEÑO Y CONTRUCCIÓN DE HARDWARE Y SOFTWARE

En este capítulo se detallará el diseño del sistema de control de acceso considerando los requerimientos establecidos, construcción de hardware y software necesario, especificaciones técnicas de cada elemento, así como también el desarrollo y manejo de la base de datos.

3.1. SITUACIÓN ACTUAL

Actualmente la Universidad Técnica del Norte, no cuenta con un sistema de control de acceso en sus entradas, por tal motivo, se han dado muchos casos de robo dentro de la institución. Esto ha ocasionado que las autoridades ordenen el cierre de las entradas norte y sur, con fin de tener una única ruta de acceso y salida por la entrada principal, y así poder llevar un mejor control. Sin embargo, estas medidas no han sido suficientes para mejorar esta situación.

La Figura 51 a continuación muestra el número de estudiantes matriculados para el periodo 2016-2017, en la cual se observa un total de 8855, de los cuales 7328 están en la modalidad presencial, sin embargo esta cifra se distribuye en las distintas dependencias con las que cuenta la Universidad, teniendo a diario un número aproximado de 5000 personas que transitan en el campus, incluidos estudiantes, docentes, personal administrativo y demás empleados.

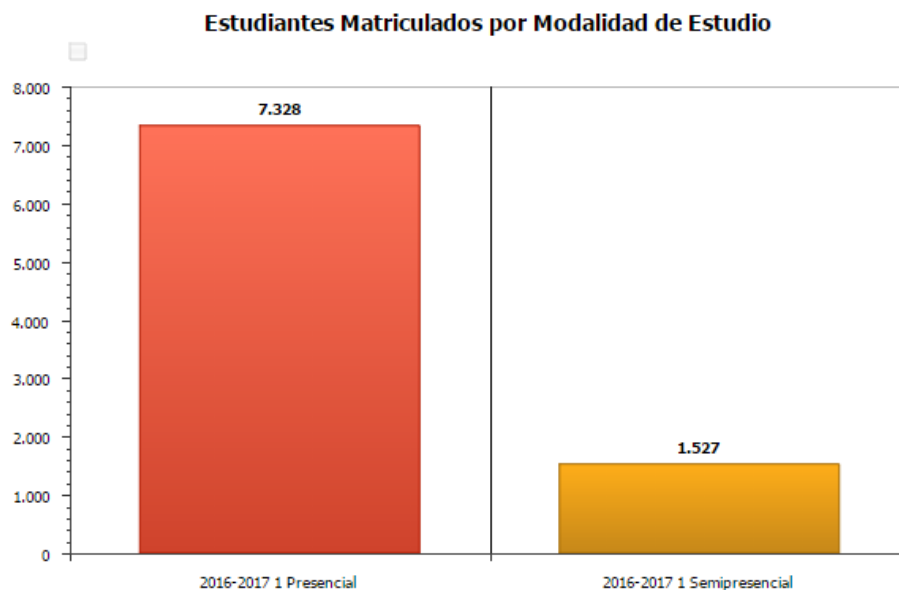


Figura 51: Estudiantes matriculados por modalidad de estudio.

Fuente: Universidad técnica del Norte. Recuperado de: <http://svrapp3.utn.edu.ec:7001/apex/f?p=224:3:0::NO::>

Esta alta cantidad de personas hace compleja la labor del personal de seguridad, ya que no pueden brindar un control adecuado, ni ofrecer las garantías necesarias de seguridad a cada persona.

En vista de estos hechos la Universidad Técnica del Norte se ha visto en la obligación de establecer nuevos proyectos de seguridad y control, en las que se encuentra un sistema de control de acceso, que de acuerdo a las especificaciones técnicas realizadas por la Dirección de Desarrollo Tecnológico e Informático – DDTI, así como también por el informe de diseño e instalación de infraestructura realizado por la Universidad y especificado en el ANEXO D, se tiene como prioridad la implantación de un sistema de control, mediante el uso de un identificador único a modo de tarjeta para cada uno de los estudiantes, docentes y demás trabajadores de la Universidad.

3.2. DISEÑO DE HARDWARE

Para el diseño de hardware del sistema de control de acceso se debe enfocar en el tipo de conexión de módulos y demás dispositivos que lo conforman, además de otros aspectos importantes a considerar como requerimientos en el diseño, tales como:

- Lector RFID de alta disponibilidad
- Acceso alternativo por teclado matricial
- Conexión Ethernet con el servidor de base de datos
- Interfaz para usuario final (indicadores, pantalla grafica LCD, generador de sonido)
- Circuito con relé para activación de actuadores

A continuación la Figura 52, muestra el esquema de las principales áreas de diseño de hardware:

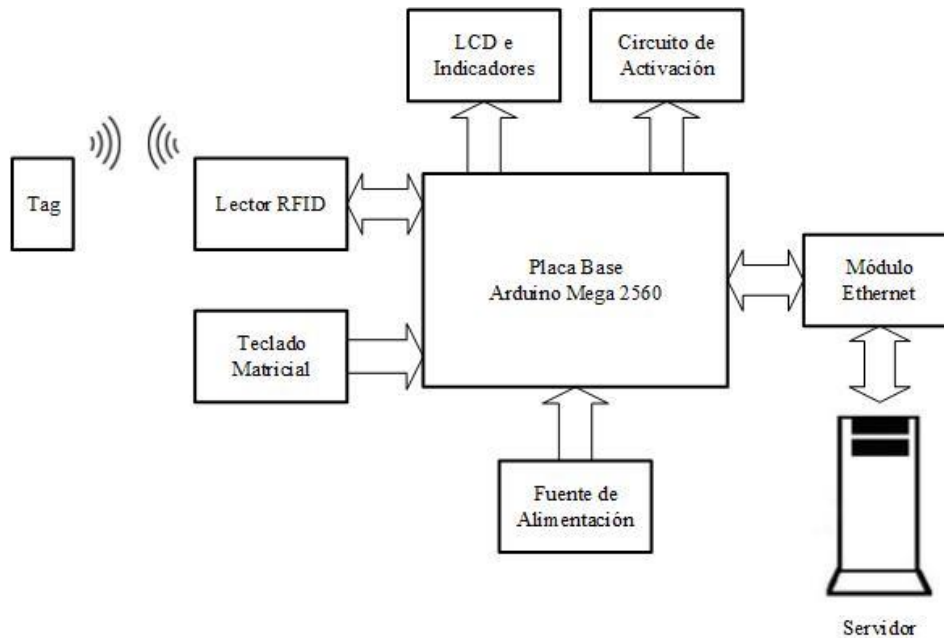


Figura 52: Diagrama en bloques del hardware del sistema de control de acceso.

Fuente: Desarrollo del proyecto.

El funcionamiento del sistema inicia cuando el usuario ingresa su identificador único contenido en un tag, al área de cobertura del lector. El lector se encarga de extraer el código del tag en un formato EPC de forma hexadecimal y enviarlo a la placa base de procesamiento, esta información se enviará a través del módulo Ethernet al servidor que contiene la base de datos, la cual compara y valida la información recibida con la información que tiene almacenada de cada usuario, esta solicitud se envía nuevamente desde la base de datos hacia la placa base, que de acuerdo a la respuesta obtenida desde la misma ejecutará las acciones necesarias a través de un circuito de activación, que activará o desactivará el sistema de acuerdo a la respuesta conseguida. Esta acción el usuario la verifica a través de indicadores, que son: pantalla grafica LCD, leds y generador de sonido.

Alternativamente al tag, el usuario también cuenta con una clave de identificación, la cual puede ser utilizada en caso de no poseer el identificador electrónico. De la misma forma, el sistema procesa el código ingresado por el usuario mediante el teclado a través de la placa base, con el fin de verificar y validar la clave con la existente en la base de datos y así poder generar las acciones a través del circuito actuador.

Todo el sistema es energizado mediante una fuente de alimentación, la cual provee los niveles adecuados de energía referente a voltaje y corriente, de acuerdo al consumo de cada elemento, y que sirva para la correcta funcionalidad del sistema, además se cuenta con una batería de respaldo, la cual provee de energía en caso de un corte eléctrico por un determinado tiempo, en el cual se podrá adecuar el sistema para tener un acceso total sin identificación, bloqueo ó un funcionamiento normal, según el tiempo de corte.

En base al diagrama en bloques que indica la Figura 52, a continuación se detalla la elección de cada uno de los elementos constitutivos del sistema de control de acceso, iniciando con la placa base, módulo Ethernet, lector RFID y tipo de tag.

3.2.1. Elección de la placa base

En base a la descripción realizada en la Tabla 3 de algunos tipos de placas Arduino, y de los requerimientos generales del sistema, la elección de o las placas se fundamenta principalmente en: el número de terminales entrada/salida que esta posea, así como también la compatibilidad con el lector RFID y el controlador Ethernet.

La placa Arduino Yun es una de las más indicadas para el desarrollo del proyecto, ya que posee conexión Ethernet integrada e interfaz SPI para la comunicación con el lector, sin embargo el número de terminales de entrada/salida que posee es limitado. Es así que, otro factor a considerar es justamente el número de terminales entrada/salida, mismos que serán utilizados para la conexión de otros dispositivos complementarios.

Considerando el número de terminales de entrada/salida, la placa Arduino MEGA 2560 posee la mayor cantidad de estos, además de contar con los demás requerimientos establecidos, sin embargo, no cuenta con un controlador Ethernet integrado, por lo que es necesario utilizar el módulo Arduino Ethernet, el cual es totalmente compatible con Arduino MEGA 2560, para de esta forma complementar todos los requerimientos necesarios de la placa base y convertirse en las más idóneas para el desarrollo del sistema.

3.2.1.1. Arduino MEGA 2560

La placa Arduino MEGA 2560 al ser una plataforma de hardware libre y que gracias a las características que presenta, referente a la compatibilidad con el Modulo Ethernet de Arduino y el número de entradas/salidas que posee para la integración de más dispositivos sobre la misma, es la más indicada para desarrollar un sistema de control de acceso. Basa su funcionamiento en el microcontrolador Atmega 2560, el cual posee la siguiente distribución de terminales, como se observa en la Figura 53:

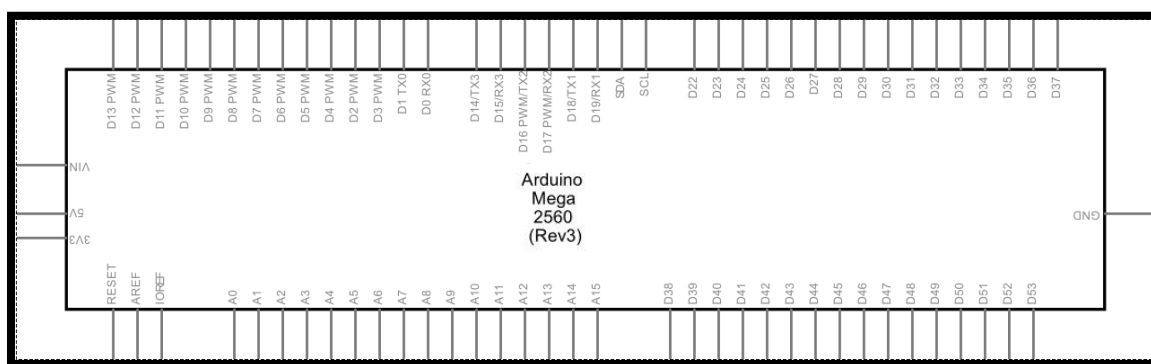


Figura 53: Distribución de terminales en Arduino MEGA 2560.

Fuente: Simulador Fritzing.

3.2.1.1.1. Especificaciones

Las principales características técnicas que presenta la placa Arduino MEGA 2560 se detallan a continuación en la Tabla 9:

Tabla 9: Especificaciones técnicas de la placa Arduino MEGA 2560.

Características	Parámetros
Microcontrolador	ATmega2560
Tensión de alimentación	5V
Tensión de entrada recomendada	7-12V
Límite de entrada	6-20V
Pines digitales	54 (14 con PWM)

Entradas analógicas	16
Corriente máxima por pin	20 mA
Corriente máxima para el pin 3.3V	50 mA
Memoria flash	256 KB
SRAM	8 KB
EEPROM	4 KB
Velocidad de reloj	16 MHz

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/en/Main/ArduinoBoardMega2560>

3.2.1.2. Módulo Arduino Ethernet

Una de las ventajas más importantes que posee Arduino como plataforma de hardware libre es justamente la compatibilidad con distintos dispositivos y módulos. El módulo o también denominado Shield Ethernet de Arduino es un dispositivo totalmente compatible con Arduino Mega 2560 que utiliza la librería Ethernet para facilitar su uso.

La librería Ethernet permite realizar una conexión a internet o a cualquier red local a una placa Arduino, de esta forma se puede tener un servidor que acepte solicitudes entrantes y salientes de un cliente.

3.2.1.2.1. Especificaciones

Arduino Ethernet Shield se comunica con las demás placas Arduino compatibles a través de comunicación SPI. En este tipo de comunicación la placa Arduino trabaja en modo maestro ante otros dispositivos conectados a ella y que soporten este tipo de comunicación.

Dentro de las características principales del módulo Ethernet se pueden citar las siguientes en la Tabla 10:

Tabla 10: Especificaciones técnicas de la placa Arduino Ethernet.

Características	Parámetros
Microcontrolador	ATmega328
Tensión de alimentación	5V
Tensión de entrada recomendada	7-12V
Límite de entrada	6-20V
Pines digitales	14 (4 con PWM)
Entradas analógicas	6
Corriente máxima por pin	40 mA
Comunicación	TWI y SPI
Memoria flash	32 KB
SRAM	2 KB
EEPROM	1 KB
Velocidad de reloj	16 MHz

Fuente: ARDUINO, 2015. Recuperado de <https://www.arduino.cc/en/Main/ArduinoBoardEthernet>.

3.2.2. Módulo RFID

El sistema de control de acceso que se desea diseñar tiene como objetivo principal proveer de un identificador único a cada uno de los estudiantes, docentes y demás personal perteneciente a la Universidad Técnica del Norte, con el fin de tener acceso al campus universitario en general o a distintas dependencias, laboratorios y departamentos que posee la misma y que requieran de un control de ingreso. Para ello se utilizará la tecnología de identificación por radiofrecuencia que actualmente tiene mucha aplicabilidad en sistemas de control de acceso.

La tecnología RFID ha sido desarrollada para cumplir con varias funcionalidades en distintas áreas de aplicación, es así que para el diseño de un control de acceso es sin duda la tecnología más viable gracias a sus características de entre las cuales se pueden mencionar: facilidad de uso para el usuario y su costo de implementación, que en comparación a otras tecnologías es sin duda mucho más accesible.

El tipo de módulo RFID que se utilizará debe cumplir con ciertas características importantes que garanticen una correcta funcionalidad del sistema, entre las cuales se pueden mencionar:

distancia corta de lectura (3cm aproximadamente), protocolo especial anticolidión, disponibilidad en el mercado y bajo costo de adquisición.

Con respecto a la distancia de lectura se debe tener un adecuado acercamiento entre la tarjeta y el lector, sin que exista la necesidad de formar un campo amplio de cobertura, esto con el fin de evitar la generación de un consumo de potencia innecesaria y obtener así una rápida lectura.

Al tratarse de un sistema de control de acceso la aplicación de mecanismos anticolidión está por demás ya que se tendrá una lectura ordenada, sin que exista la posibilidad de tener dos lecturas simultáneas en un mismo lector, garantizando así un orden en las mismas. Sin embargo la mayoría de lectores RFID cuentan con un mecanismo anticolidión ALOHA, mismo que se encarga de que los tags escuchen el medio antes de transmitir y si existen colisiones, se intenta reenviar la información luego de un determinado tiempo.

3.2.2.1. Lector RFID

Hoy en día existe una gran variedad de lectores RFID que difieren uno de otro según la aplicación que se vaya a dar a cada uno de estos elementos. A continuación se detallarán algunos tipos de lectores RFID que se encuentran disponibles en el mercado y se realizará una comparación para elegir la mejor opción.

3.2.2.1.1. Lector RFID RC522

Este tipo de lector RFID está basado en el circuito integrado MFRC522 utilizado para comunicación inalámbrica a una frecuencia de 13.56Mhz. Este dispositivo se maneja bajo el estándar internacional ISO 14443A y opera con un voltaje de alimentación de 3.3v. La Tabla 11 a continuación muestra algunas características de este dispositivo:

Tabla 11: Especificaciones técnicas del módulo RFID RC522.

Características	Parámetros
Tensión de alimentación	3.3V
Corriente de Operación	13-26mA
Corriente de standby	10-13mA
Corriente de sleep-mode	<80µA
Corriente máxima	30mA
Frecuencia de operación	13.56Mhz
Distancia de lectura	0 a 60mm
Protocolo de comunicación	SPI
Velocidad de datos máxima	10Mbit/s
Temperatura de operación	-20 a 80°C

Fuente: NXP Semiconductors, 2016. Recuperado de http://www.nxp.com/documents/data_sheet/MFRC522.pdf

3.2.2.1.2. Lector RFID ID-12LA

El lector RFID ID-12LA es un módulo inalámbrico de radiofrecuencia que tiene incorporada la antena y es utilizado para identificar tarjetas electrónicas que trabajen en el rango de 125Khz. Su fácil uso ha hecho que tenga distintas aplicaciones.

La Tabla 12 a continuación muestra algunas de las características más importantes que posee el lector RFID ID-12LA:

Tabla 12: Especificaciones técnicas del módulo RFID ID-12LA.

Características	Parámetros
Tensión de alimentación	2.8-5V
Corriente de Operación	35mA
Frecuencia de operación	125Khz
Distancia de lectura	0 a 120mm
Formato de la Tarjeta	EM 4001 o compatibles
Salidas	9600bps TTL y RS232

Fuente: ID Innovations, 2013. Recuperado de <http://cdn.sparkfun.com/datasheets/Sensors/ID/ID-2LA,%20ID-12LA,%20ID-20LA2013-4-10.pdf>

3.2.4.1.3. Elección del lector RFID

En base a las características presentadas anteriormente, se puede concluir que la mejor elección en cuanto al lector RFID es el lector RC522, ya que presenta las funcionalidades óptimas que satisfacen los requerimientos que necesita el sistema para su correcto funcionamiento, esto en base a una distancia corta (3cm aproximadamente) y adecuada de lectura, que no demande de un alto consumo de energía y que además se encuentre disponible en el mercado y a un costo adecuado. La Figura 54 a continuación indica los terminales que posee el Lector RFID RC522:



Figura 54: Lector RFID RC522.

Fuente: *aerial.net*, 2016. Recuperado de: https://www.aerial.net/shop/product/161_206/1674/rc522-mifare-rfid-readerwriter.html

3.2.2.2. Etiquetas RFID

La elección de las etiquetas RFID depende en gran medida del tipo de lector que se vaya a utilizar, además de ciertas características importantes que garantizan el correcto funcionamiento del sistema, de las cuales se puede mencionar: la frecuencia de operación, el tipo de aplicación que se vaya a tener y el costo.

Entre los principales tipos de etiquetas que se pueden encontrar en el mercado destacan las etiquetas: tipo botón, tipo llavero y tipo tarjeta.

3.2.2.2.1. Etiqueta RFID tipo botón

Este tipo de etiqueta RFID posee un tamaño reducido, por lo que puede ser utilizado en aplicaciones en las que pueda fácilmente ser adherido a la ropa de los usuarios o insertado a cualquier objeto que se desee etiquetar. Su frecuencia de operación depende del tipo de lector que se utilice y su reducido tamaño hace que este tipo de etiquetas sean únicamente pasivas y de solo lectura.

3.2.2.2.2. Etiqueta RFID tipo llavero

Las etiquetas tipo llavero tienen un práctico diseño que facilita en gran medida su uso, sus aplicaciones son diversas y pueden ser utilizadas en empresas, instituciones, bancos, etc. Su frecuencia de operación depende del tipo de lector que se utilice y al igual que las etiquetas tipo botón se trata de un dispositivo pasivo de solo lectura.

3.2.2.2.3. Etiqueta RFID tipo tarjeta

Este tipo de etiquetas son sin duda las que más se utiliza en cualquier aplicación, esto gracias a su diseño y fabricación que las hace prácticas al momento de utilizarlas. Su frecuencia de trabajo depende del tipo de lector que se utilice, pero comúnmente se las puede encontrar para frecuencias de 125Khz y 13.56Mhz. Al igual que las anteriores, estas etiquetas son de solo lectura y del tipo pasivo.

3.2.2.2.4. Elección de la mejor alternativa en etiqueta RFID

Una vez que se ha detallado cada uno de los tipos de etiquetas existentes en el mercado se ha llegado a concluir que la mejor opción para utilizar dentro del sistema de control de acceso para la

Universidad Técnica del Norte es sin duda la etiqueta tipo tarjeta que se observa en la Figura 55, ya que su diseño la hace practica para su uso y además de tener una tarjeta electrónica de identificación única, se puede también colocar información del usuario sea este alumno, docente o empleado de la institución a forma de carnet.



Figura 55: Etiqueta RFID tipo tarjeta.

Fuente: Nomada Store, 2016. Recuperado de: <https://nomada-e.com/store/home/23-tags-nfc-tarjeta.html>

3.2.2.2.5. Comunicación SPI

SPI es un protocolo sincrónico de comunicación serie full dúplex, utilizado en la transferencia de información entre microcontroladores para la comunicación con uno o más dispositivos que operen bajo este mismo protocolo (Arduino, 2015). La Figura 56 a continuación muestra una conexión SPI entre un dispositivo maestro y varios esclavos:

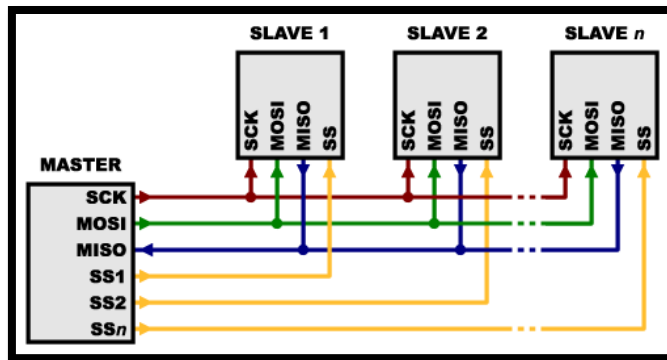


Figura 56: Conexión SPI con múltiples esclavos.

Fuente: PROMETEC, 2016. Recuperado de <http://www.prometec.net/bus-spi/>

En una conexión SPI por lo general siempre habrá un dispositivo que trabaje como maestro y genere una señal de reloj a un nivel menor o igual a la frecuencia máxima que soporte el esclavo, en este caso la placa base Arduino MEGA 2560, para de esta forma controlar los dispositivos periféricos que en este caso son el módulo Ethernet y RFID RC522.

Generalmente la conexión se realiza a través de tres líneas principales, siendo estas:

- MISO (Master Input Slave Output). - Línea de esclavo para el envío de datos, y entrada al Maestro.
- MOSI (Master Output Slave Input) - Línea principal para el envío de datos del Maestro y entrada de datos al Esclavo.
- SCK (Serial Clock).- Impulsos de reloj que sincronizan la transmisión de datos generado por el maestro.

Además se cuenta con una cuarta línea denominada SS (Slave Select), encargada de seleccionar un esclavo y puede activar o desactivar dispositivos específicos. La Figura 57 indica el proceso de comunicación entre un maestro y un esclavo:

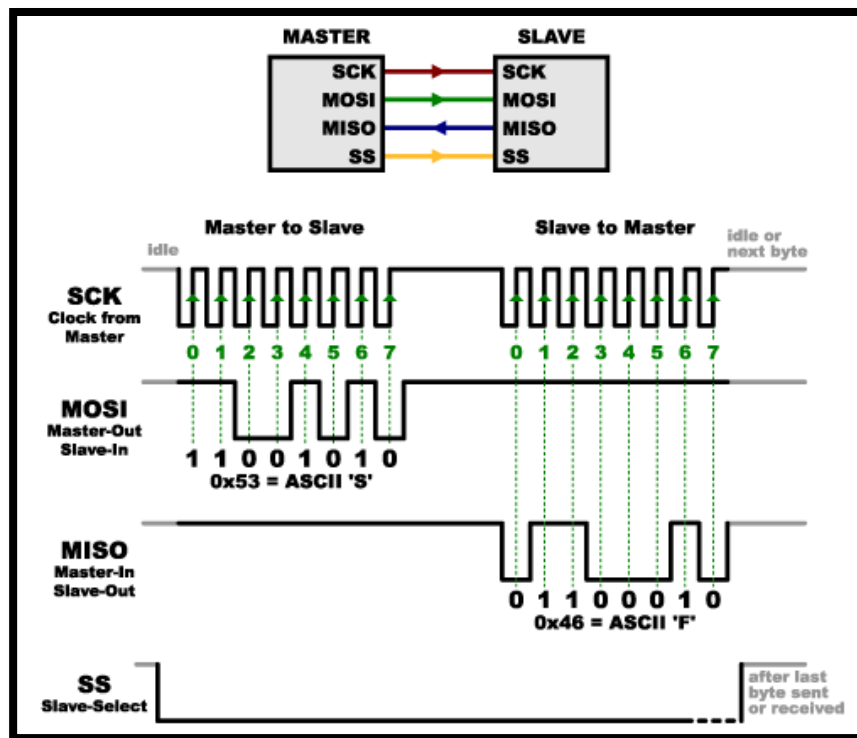


Figura 57: Comunicación SPI entre maestro y esclavo.

Fuente: PROMETEC, 2016. Recuperado de <http://www.prometec.net/bus-spi/>

3.2.3. Terminales de conexión de la Placa Arduino MEGA 2560 con demás dispositivos

La Tabla 13 a continuación muestra los terminales de conexión de la placa hacia los distintos dispositivos que conforman el proyecto:

Tabla 13: Terminales de conexión entre Arduino MEGA 2560 y demás dispositivos.

Arduino MEGA 2560	Dispositivos
Pin 5	Lector RFID – Pin RST
Pin 22	Teclado matricial – Pin F2
Pin 23	Teclado matricial – Pin F1
Pin 24	Teclado matricial – Pin F4
Pin 25	Teclado matricial – Pin F3
Pin 26	Teclado matricial – Pin C2
Pin 27	Teclado matricial – Pin C1
Pin 28	Teclado matricial – Pin C4
Pin 29	Teclado matricial – Pin C3
Pin 31	LCD 16x2 – Pin
Pin 32	LCD 16x2 – Pin

Pin 33	LCD 16x2 – Pin
Pin 34	LCD 16x2 – Pin
Pin 35	LCD 16x2 – Pin
Pin 36	LCD 16x2 – Pin
Pin 37	Configuración pull-down (Pulsador Teclado)
Pin 38	Configuración pull-down (Pulsador Cambio de estado)
Pin 39	Bocina
Pin 40	Led indicador
Pin 41	Led indicador
Pin 42	Led indicador
Pin 45	Entrada del circuito actuador
Pin 50	Lector RFID – Pin MISO
Pin 51	Lector RFID – Pin MOSI
Pin 52	Lector RFID – Pin SCK
Pin 53	Lector RFID – Pin SS

Fuente: Desarrollo del proyecto.

3.2.4. Diagramas de conexión de los elementos

A continuación se detallan los diagramas esquemáticos de conexión de cada uno de los elementos que conforman el sistema de control de acceso.

3.2.4.1. Diagrama de conexión del lector RFID

El módulo RFID opera bajo el protocolo de comunicación SPI, por tanto su conexión se realiza de forma paralela a la placa base y considerando los terminales de conexión MISO, MOSI, SCK y SS, referentes al envío y recepción de datos, y la generación de señal de reloj; su conexión es hacia los terminales 50, 51, 52 y 53 respectivamente, mientras que RESET se conecta al terminal 5. La Figura 58 muestra la conexión de los terminales del lector RFID con la placa base:

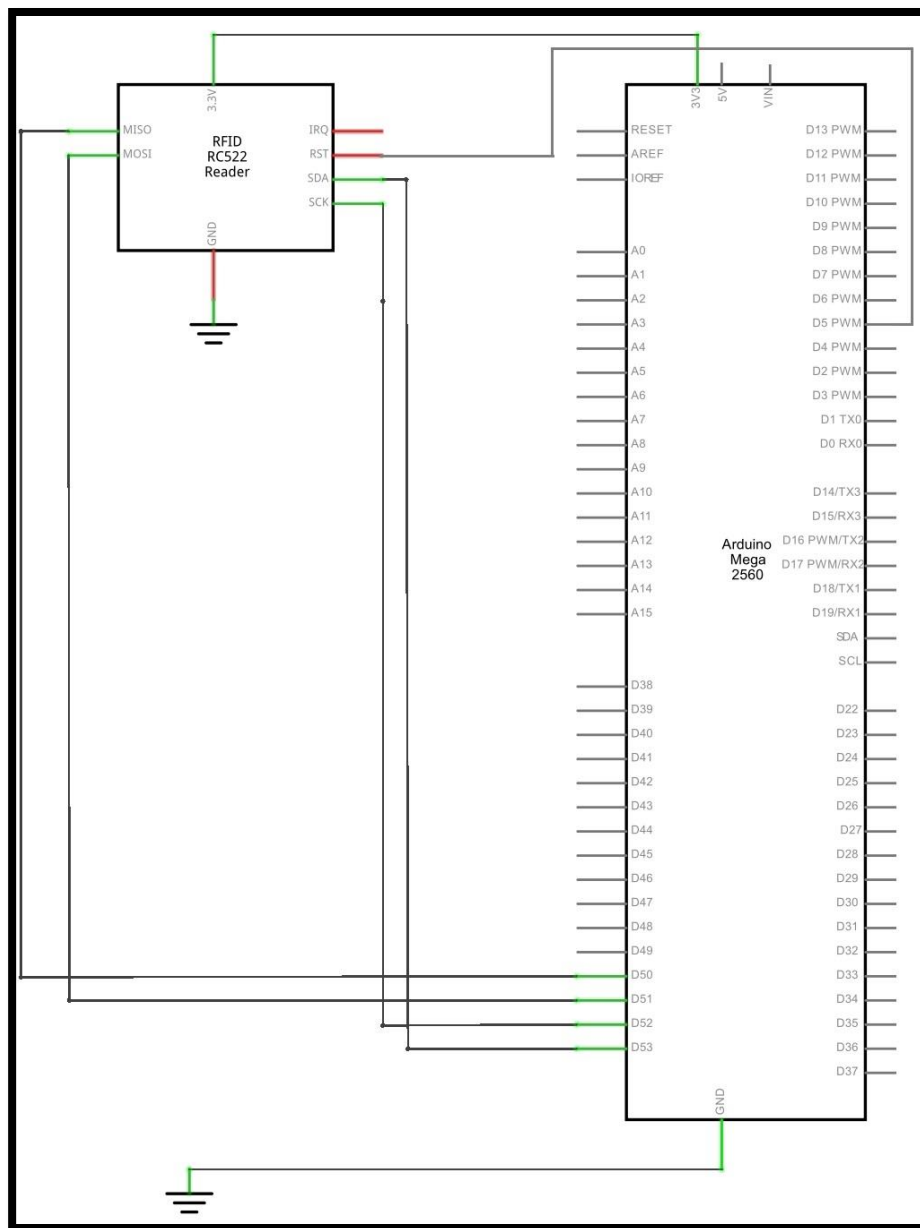


Figura 58: Diagrama esquemático de conexión del módulo RFID RC522.

Fuente: Simulador Fritzing.

3.2.4.2 Diagrama de conexión del módulo Ethernet

La conexión del módulo Ethernet sobre la placa base es simple, ya que se trata de un Shield de Arduino y únicamente se debe sobreponerla, teniendo cuidado en que los terminales ingresen

correctamente sobre el conector ICSP que se indica la Figura 59, estos terminales corresponden a la comunicación SPI del módulo con la placa base.

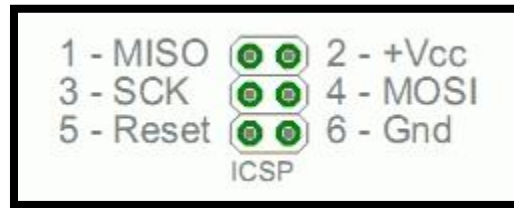


Figura 59: Terminales ICSP.

Fuente: Arduino, 2015. Recuperado de <https://www.arduino.cc/en/Reference/SPI>

La siguiente Figura 60 muestra la conexión de los terminales correspondientes a la comunicación SPI del módulo Ethernet con la placa Arduino:

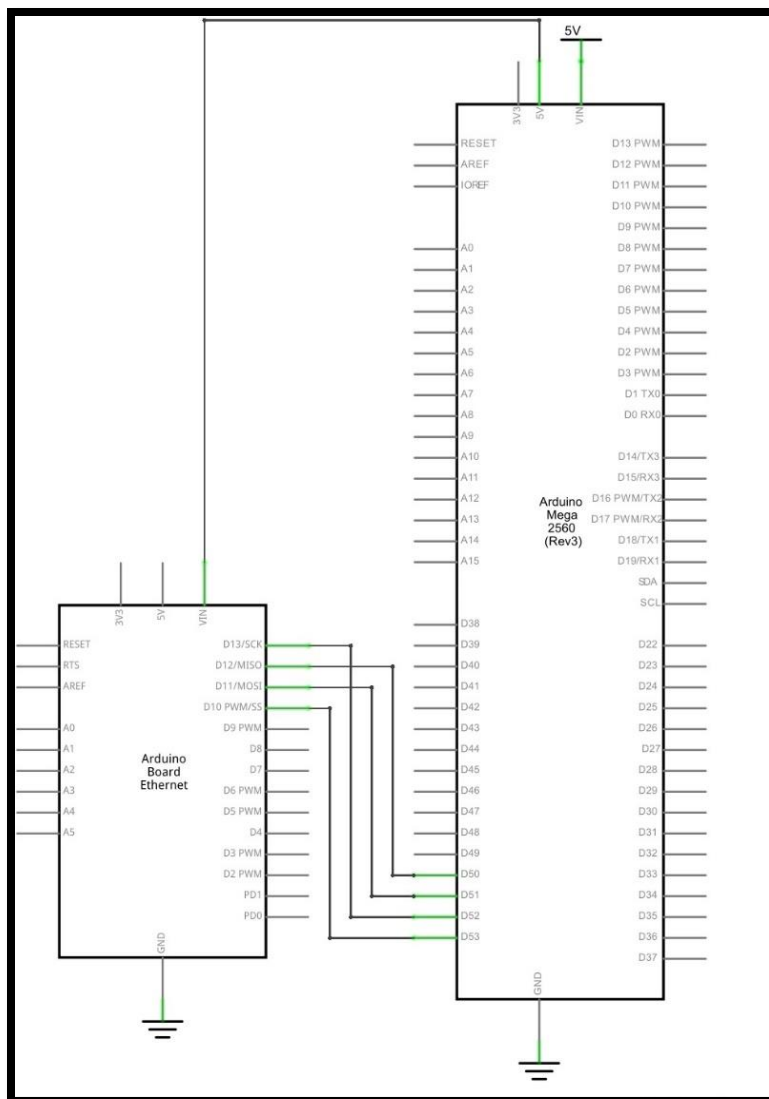


Figura 60: Diagrama esquemático de conexión del módulo Ethernet.

Fuente: Simulador Fritzing.

3.2.4.3. Diagrama de conexión de la LCD

Para la conexión de la pantalla gráfica LCD se utiliza los terminales 31, 32, 33, 34, 35, 36 de la placa base conectados a D7, D6, D5, D4, E, RS en la LCD respectivamente.

Los terminales correspondientes a VSS, R/W y K se conectan a tierra, mientras que los terminales VDD y A se conectan a 5V. Finalmente se conecta el terminal VO a un potenciómetro

configuración pull-down que permite activar la subrutina del teclado como se observa en la Figura 62:

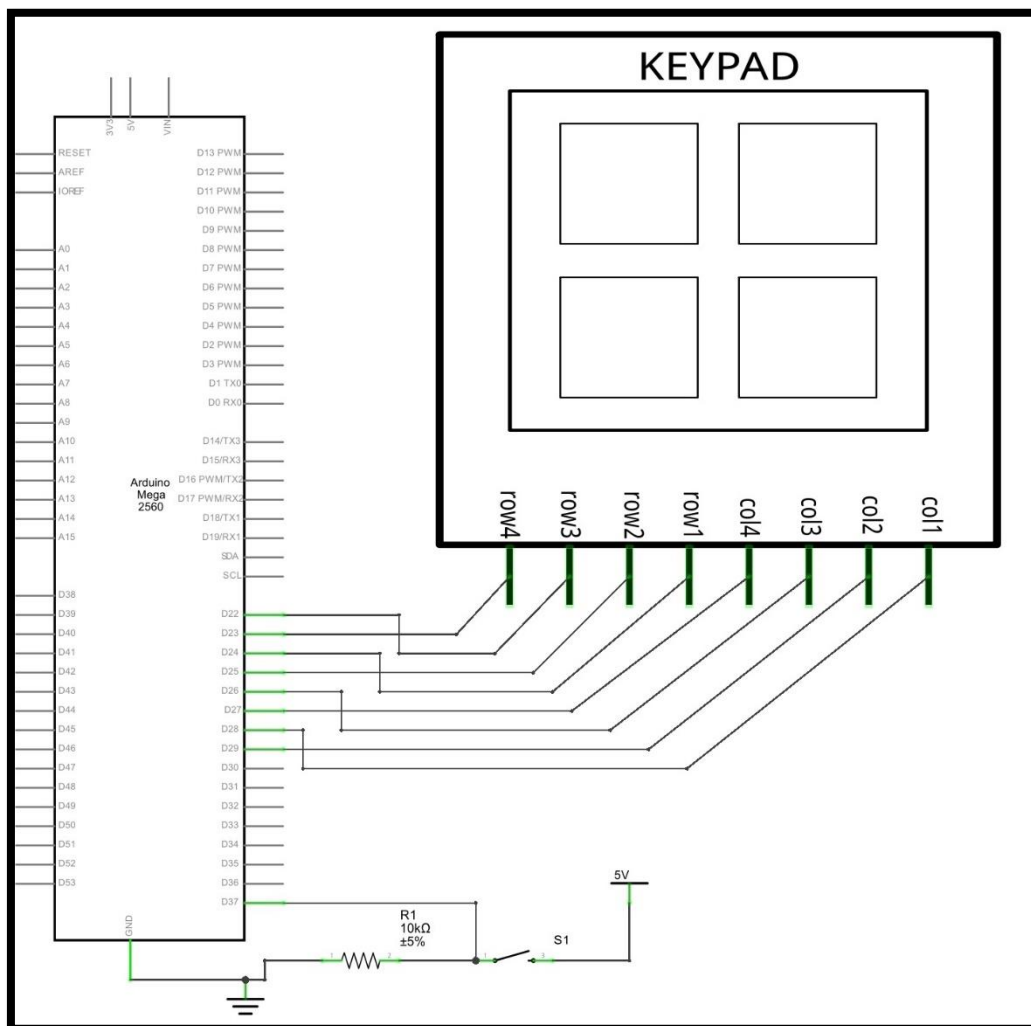


Figura 62: Diagrama esquemático de conexión del teclado matricial.

Fuente: Simulador Fritzing.

El valor de la resistencia en la configuración pull-down debe ser un valor relativamente alto para no influir en el circuito. Comúnmente este valor es $10\text{k}\Omega$, y es considerado un valor estándar para esta configuración, ayudando a establecer un estado lógico al circuito. La Ecuación 1 a continuación muestra el cálculo de la resistencia pull-down a partir de la ley de ohm:

$$R_{\text{pull-down}} = \frac{V_{cc}}{I_{R1}}$$

Ecuación 1: Cálculo del valor de la resistencia pull-down.

Fuente: SparkFun Electronics, 2016. Recuperado de: <https://learn.sparkfun.com/tutorials/pull-up-resistors>

Donde:

- V_{cc} = valor del voltaje al que se conecta la configuración
- I_{R1} = valor de la corriente que atraviesa la resistencia

El valor de corriente para la resistencia, debe ser una corriente baja y para este caso se considerará el valor de 0,05mA.

$$R_{\text{pull-down}} = \frac{5V}{0,05mA}$$

$$R_{\text{pull-down}} = 10000\Omega = 10K\Omega$$

3.2.4.5. Diagrama de conexión de leds indicadores

Estos leds cumplen la función de indicar las etapas de funcionamiento del sistema (registro correcto, registro incorrecto), para lo cual deben estar conectados a una resistencia que limite la corriente proveniente de la placa base. El cálculo de la resistencia se lo realiza tomando como referencia los valores de la corriente y voltaje de funcionamiento de un diodo led, especificados en la Tabla 6, de acuerdo al material de fabricación y color de los mismos.

A continuación se muestra la Ecuación 2, con la cual se calcula el valor de la resistencia de un led:

$$R = \frac{V - V_f}{I_f}$$

Ecuación 2: Cálculo de la resistencia de un led.

Fuente: Charly Labs, 2016. Recuperado de: <https://www.charlylabs.cl/charly-labs/como-calcular-la-resistencia-para-leds/>

Donde:

- V = voltaje de alimentación
- Vf = voltaje de funcionamiento de un led
- If = intensidad de funcionamiento del led

Para el diseño del sistema de control de acceso se utilizan tres diodos led de diferente color, rojo, verde y blanco, que están conectados a los terminales 40, 41 y 42 respectivamente de la placa base, para lo cual se realiza un cálculo para la resistencia de cada uno de estos; es así que para el diodo led de color rojo se tendrán los siguientes valores:

$$R(\text{led rojo}) = \frac{5V - 1,8V}{20\text{mA}}$$

$$R(\text{led rojo}) = \frac{3,2V}{20\text{mA}}$$

$$R(\text{led rojo}) = 160\Omega$$

Además del valor óhmico, también se debe calcular la potencia que disipará cada una de las resistencias, para ello se utiliza la fórmula de la potencia derivada de la ley de ohm y que se indica en la Ecuación 3:

$$P = V_R \times I_R$$

Ecuación 3: Cálculo de la potencia de una resistencia.

Fuente: Ramos Álvarez, 2012.

Donde:

- V_R = voltaje de la resistencia
- I_R = intensidad de la resistencia, para este caso se considera el valor de corriente que entrega el terminal de Arduino MEGA 2560 que es de 20mA

$$P = 3,2 \times 20\text{mA}$$

$$P = 0,064\text{W}$$

Para el cálculo de la resistencia del led de color verde se utilizaran los siguientes valores:

$$R(\text{led verde}) = \frac{5\text{V} - 2,2\text{V}}{20\text{mA}}$$

$$R(\text{led verde}) = \frac{2,8\text{V}}{20\text{mA}}$$

$$R(\text{led verde}) = 120\Omega$$

De donde su potencia es igual a:

$$P = 2,8 \times 20\text{mA}$$

$$P = 0,056\text{W}$$

Finalmente se calcula el valor de la resistencia para el led blanco con los siguientes valores:

$$R(\text{led blanco}) = \frac{5\text{V} - 4,1\text{V}}{300\text{mA}}$$

$$R(\text{led blanco}) = \frac{0,9V}{30\text{mA}}$$

$$R(\text{led blanco}) = 30\Omega$$

De donde su potencia es igual a:

$$P = 0,9V \times 30\text{mA}$$

$$P = 0,027W$$

De los cálculos de potencia obtenidos de cada una de las resistencias, se puede observar que la potencia de disipación de cada una es muy baja por lo que se puede utilizar resistencias de 1/8W o 1/4W según la disponibilidad de estas en el mercado. La Figura 63 muestra la conexión de las resistencias y los leds a la placa base:

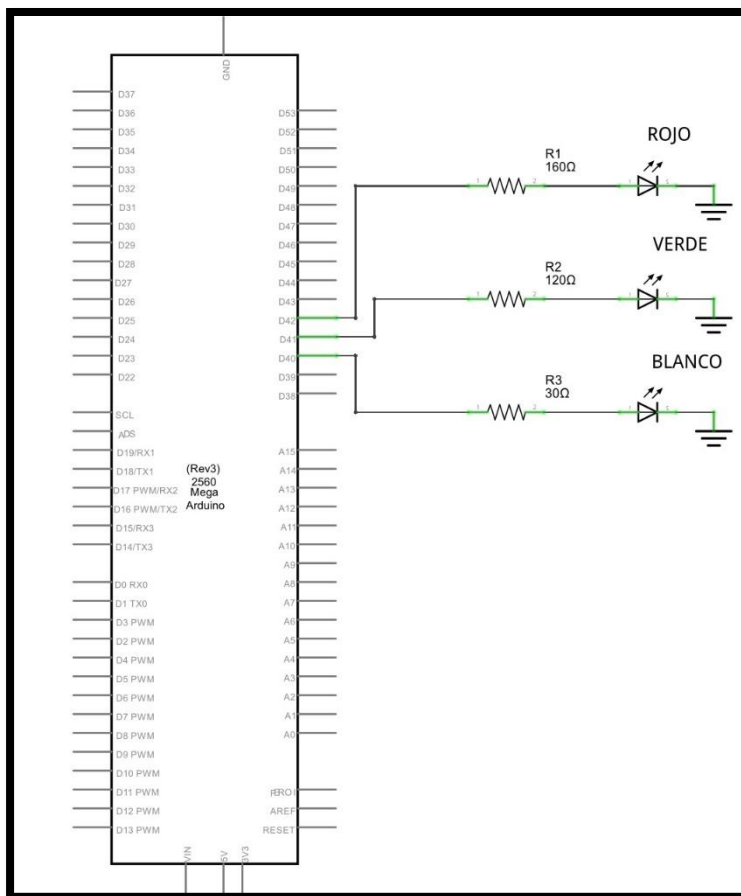


Figura 63: Conexión de diodos LED.

Fuente: Simulador Fritzing.

3.2.4.6. Diagrama de conexión del circuito de activación por relé

Para el funcionamiento de los actuadores (cerradura eléctrica, cerradura magnética, puerta tipo torniquete, etc) se requiere de un circuito de activación de relé mediante un transistor que provea de corriente necesaria para alimentar una carga externa que no puede ser activada con la corriente que generan los terminales del Arduino MEGA 2560, para ello se utiliza una conexión determinada como se observa en la Figura 64, de la cual se debe calcular la resistencia que se conecta a la base del transistor:

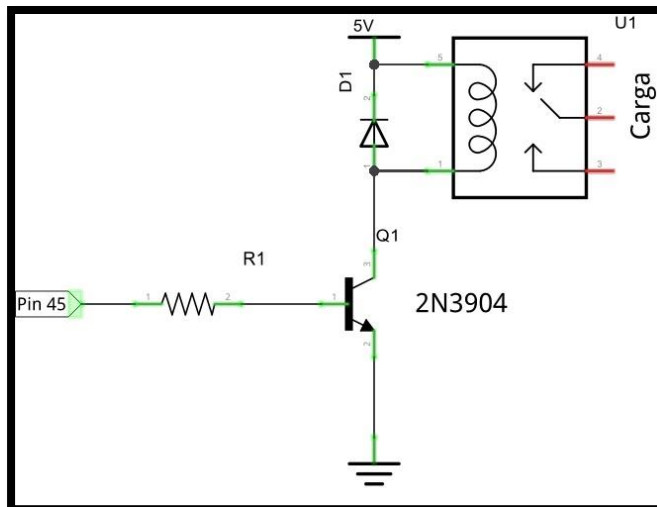


Figura 64: Diagrama de conexión de relé con transistor.

Fuente: Simulador Fritzing.

Para encontrar el valor de la resistencia se debe primeramente calcular la intensidad de la bobina de carga del relé, a través del uso de la Ecuación 4, para lo cual se considera su resistencia que en este caso es de 70.2Ω , de acuerdo a la medición realizada con un óhmetro y el voltaje de funcionamiento de 5V.

$$I = \frac{V}{R}$$

Ecuación 4: Cálculo de la intensidad de la bobina de carga del relé.

Fuente: Geek Factory, 2012. Recuperado de: <http://www.geekfactory.mx/tutoriales/conectar-un-relevador-con-un-microcontrolador-o-arduino/>

$$I = \frac{5V}{70.2\Omega}$$

$$I = 0.0712A$$

Una vez calculado el valor de la corriente de la bobina del relé y que en este caso será también el valor de corriente del colector, es necesario calcular la corriente que circulara en la base, para

ello se maneja el valor de ganancia del transistor a utilizar a través de la Ecuación 5 que se muestra a continuación:

$$\beta = \frac{I_c}{I_b}$$

Ecuación 5: Cálculo de la ganancia de un transistor.

Fuente: Geek Factory, 2012. Recuperado de: <http://www.geekfactory.mx/tutoriales/conectar-un-relevador-con-un-microcontrolador-o-arduino/>

Donde:

- β = Ganancia de transistor
- I_c = Intensidad de colector
- I_b = Intensidad de base

El valor típico de ganancia del transistor 2N3904 el cual se lo va a utilizar en este circuito es de 100, por lo que se tiene que la intensidad de base despejada de la Ecuación 5 es:

$$I_b = \frac{I_c}{\beta}$$

$$I_b = \frac{0.0712A}{100}$$

$$I_b = 0.000712A$$

Con el valor de la corriente que circula en la base del transistor, se procede al cálculo de la resistencia. El valor del voltaje de la resistencia va a ser el voltaje que suministre la placa base menos el voltaje que existe entre la base y el emisor del transistor. Aplicando la ley de Ohm y mediante la Ecuación 6 se obtiene:

$$R = \frac{V - V_{be}}{I_b}$$

Ecuación 6: Cálculo de la resistencia de base.

Fuente: Geek Factory, 2012. Recuperado de: <http://www.geekfactory.mx/tutoriales/conectar-un-relevador-con-un-microcontrolador-o-arduino/>

$$R = \frac{5V - 0.7V}{0.000712A}$$

$$R = \frac{4.3V}{0.000712A}$$

$$R = \frac{4.3V}{0.000712A}$$

$$R = 6039.325\Omega$$

El valor de la resistencia a utilizar para poder llevar al transistor a operar en modo saturación es de $6K\Omega$ aproximadamente.

Se debe también conectar un diodo rectificador 1N4001 de 1A inversamente polarizado y paralelo a la carga del relé, esto con el fin de evitar sobretensiones que afecten al transistor. Además, se puede colocar paralelamente un diodo led y una resistencia en serie al diodo protector, con fin de tener un indicador de estado.

3.2.4.7. Diagrama de conexión del pulsador de cambio de estado

El pulsador de cambio de estado se conecta a través de una configuración en pull-down con el terminal 38 de la placa Arduino MEGA 2560, como indica la Figura 65. Este pulsador se encarga de variar los estados del sistema, sea el caso de, tener un acceso abierto a cualquier usuario sin

necesidad del tag ni clave de teclado, bloquear el acceso a cualquier usuario, ó regresar al sistema a un funcionamiento normalizado, esto con el fin de tener un mayor control del mismo.

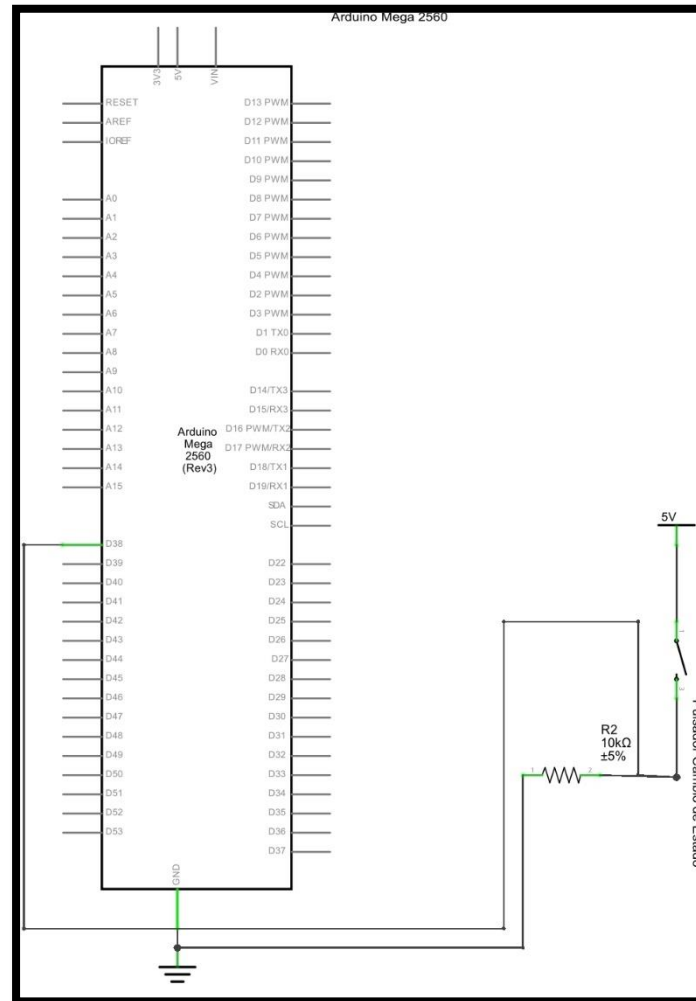


Figura 65: Diagrama de conexión de pulsador de cambio de estado.

Fuente: Simulador Fritzing.

3.2.4.8. Diagrama de conexión de bocina

La bocina está conectada al terminal 39 de la placa base, como muestra la Figura 66, este dispositivo emitirá una alarma sonora en caso de que se active el acceso para algún usuario.

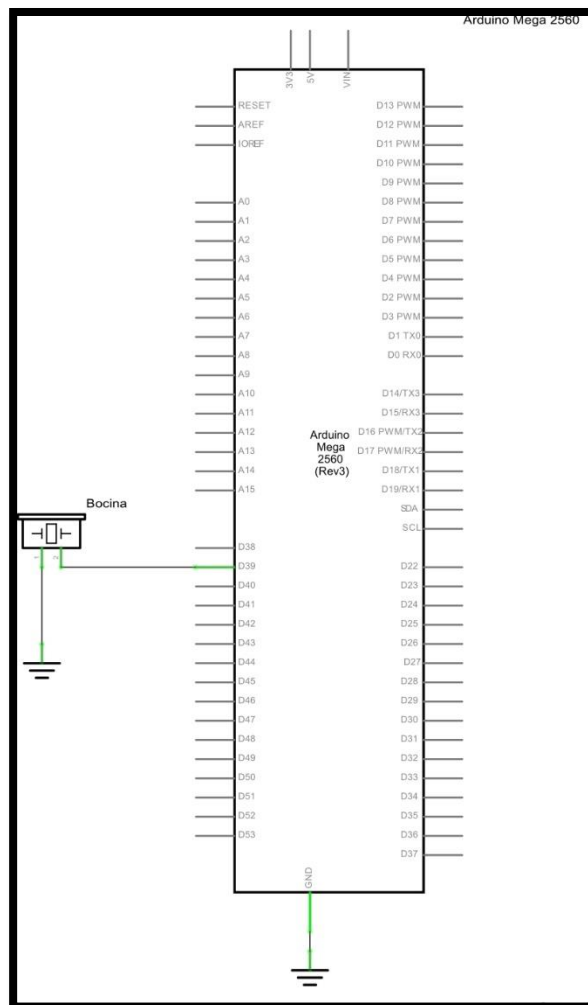


Figura 66: Diagrama de conexión de bocina.

Fuente: Simulador Fritzing.

3.2.5. Fuente de alimentación

La fuente de alimentación en cualquier circuito electrónico es sin duda, uno de los dispositivos más importantes que se deben considerar, ya que su función principal es proveer la energía necesaria para poner en funcionamiento todos los módulos y elementos que formen parte de un sistema.

Los parámetros más importantes que se toman cuenta en una fuente de alimentación son sin duda el voltaje de salida y especialmente la corriente que entregará la misma. Es así que, para ello

se debe considerar la corriente de funcionamiento de cada uno de los elementos que formen parte del sistema de control de acceso, como se indica en la siguiente Tabla 14:

Tabla 14: Corriente de funcionamiento de cada dispositivo.

Elementos	Corriente de Funcionamiento	Cantidad
Arduino MEGA 2560	93mA	1
Arduino Ethernet	80mA	1
Pantalla grafica LCD	20mA	1
Teclado matricial	5mA	1
Módulo RFID	15mA	1
Diodos LED	15mA	3
Relé de 5v	15mA	1
Transistor NPN 3904	10mA	1
Bocina	5mA	1
Total	288mA	

Fuente: Mediciones y especificaciones técnicas.

En base a los valores de la corriente de funcionamiento de cada dispositivo, obtenidos a través de mediciones con un amperímetro como se indica en la Figura 67, se establece que la fuente de alimentación debe proveer una corriente de 288mA aproximadamente.



Figura 67: Medición de la corriente total del sistema.

Fuente: Mediciones a través de amperímetro.

A partir del valor de corriente obtenido, se realiza el diseño de la fuente, la cual se basa en un rectificador tipo puente de onda completa, este tipo de fuente de alimentación presenta gran ventaja ante otras, ya que permite aprovechar tanto el semiciclo positivo como el negativo, teniendo así una salida constante de corriente pulsante como se observa en la Figura 68:

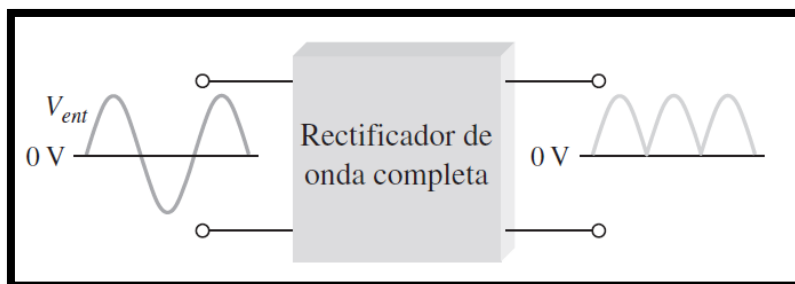


Figura 68: Tipo de onda generada por rectificador de onda completa.

Fuente: Floyd, 2008.

Este tipo de fuente está conformada por 4 diodos, de los cuales, durante el semiciclo positivo D_1 y D_2 están polarizados directamente y por tanto conducen la corriente, mientras que los diodos D_3 y D_4 están polarizados inversamente y no conducen, la Figura 69 muestra el proceso antes descrito:

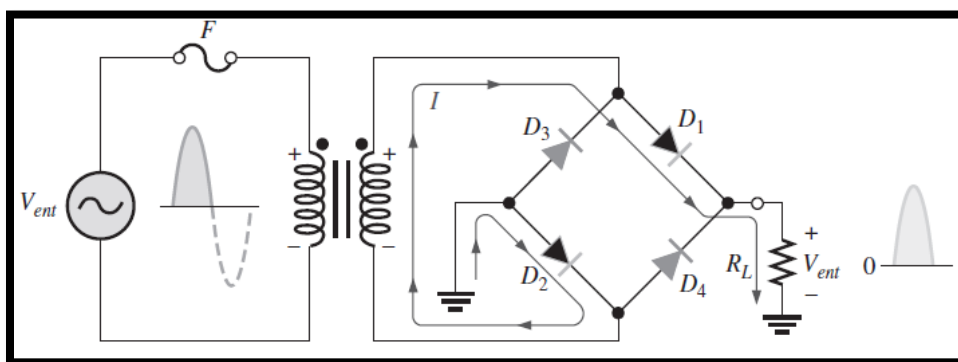


Figura 69: Semiciclo positivo en fuente de alimentación de onda completa tipo puente.

Fuente: Floyd, 2008.

En el semiciclo negativo ocurre lo contrario al positivo, ya que, D_1 y D_2 están polarizados inversamente mientras que D_3 y D_4 lo están directamente.

El valor de la corriente que entrega una fuente de alimentación depende del tipo de transformador que se vaya a utilizar y la corriente que entregue el mismo, es por eso que para cubrir el requerimiento de corriente que necesita el sistema se utiliza un transformador reductor de 120V a 12V con una corriente de 1A.

Para el rectificador tipo puente se utiliza los diodos 1N4001, los cuales operan bajo una corriente de un amperio, misma que entregará el transformador.

A la salida de los rectificadores se tendrá una señal de tipo pulsante la cual debe ser filtrada a través de un capacitor electrolítico de un alto valor, en este caso se utiliza un capacitor de $2200\mu\text{F}$ a 25V como se indica en la Figura 70. Este capacitor se encarga de eliminar el factor de rizo, que no es más que la variación de voltaje de carga y descarga que se produce en el mismo.

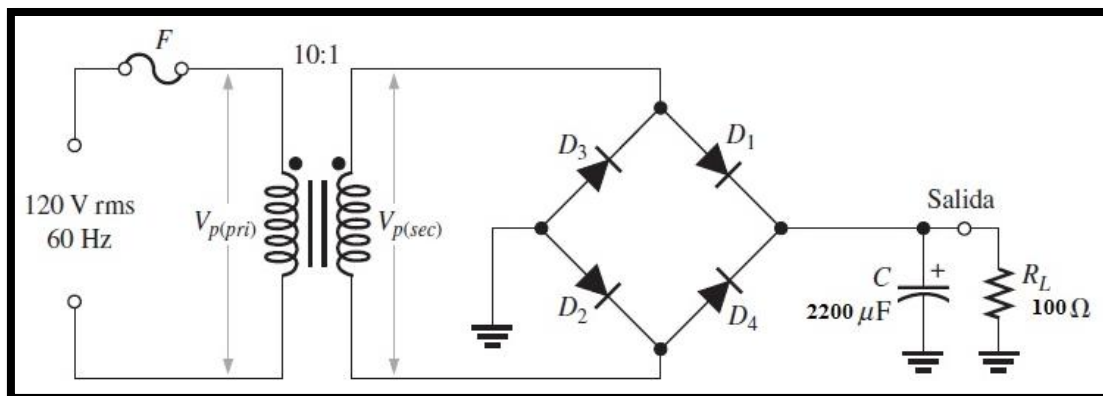


Figura 70: Fuente de onda completa tipo puente con filtro.

Fuente: Floyd, 2008.

Para el cálculo del factor de rizo se deben considerar algunos aspectos importantes, por lo que se debe iniciar calculando la relación de vueltas del transformador, a través de la Ecuación 7, en la que V_p es el voltaje del primario y V_s es el voltaje del secundario.

$$n = \frac{V_{\text{secundario}}}{V_{\text{primario}}}$$

Ecuación 7: Cálculo de la relación de vueltas en un transformador.

Fuente: Floyd, 2008.

$$n = \frac{12}{120}$$

$$n = 0,1$$

Se calcula el voltaje pico del primario mediante la Ecuación 8:

$$V_p(\text{primario}) = 1,414V_{\text{rms}}$$

Ecuación 8: Cálculo de voltaje pico del primario.

Fuente: Floyd, 2008.

Donde:

- V_{rms} = Voltaje eficaz

$$V_p(\text{primario}) = 1,414(120V)$$

$$V_p(\text{primario}) = 169,68V$$

Ahora se calcula el voltaje pico en el secundario, a través de la Ecuación 9:

$$V_p(\text{secundario}) = nV_p(\text{primario})$$

Ecuación 9: Cálculo del voltaje pico del secundario.

Fuente: Floyd, 2008.

$$V_p(\text{secundario}) = 0,1(169,68V)$$

$$V_p(\text{secundario}) = 16,968V$$

Una vez calculado el voltaje pico del secundario, la Ecuación 10 muestra la fórmula para el cálculo del voltaje rectificado de onda completa pico sin filtrar:

$$V_p(\text{rectificado}) = V_p(\text{secundario}) - 1,4 \text{ V}$$

Ecuación 10: Cálculo de voltaje rectificado de onda completa pico sin filtrar.

Fuente: Floyd, 2008.

$$V_p(\text{rectificado}) = 16,968\text{V} - 1,4 \text{ V}$$

$$V_p(\text{rectificado}) = 15,568\text{V}$$

La frecuencia de un voltaje rectificado es el doble de la frecuencia de entrada, por tanto el voltaje de rizo a la salida se calcula a través de la Ecuación 11:

$$V_r(pp) \approx \left(\frac{1}{f_x R L x C} \right) V_p(\text{rectificado})$$

Ecuación 11: Cálculo de voltaje de rizo pico pico.

Fuente: Floyd, 2008.

Considerando un valor de resistencia de carga de 100Ω se tiene:

$$V_r(pp) \approx \left(\frac{1}{(120)(100\Omega)(2200\mu\text{F})} \right) 15,568\text{V}$$

$$V_r(pp) \approx 0,589\text{V}$$

Es importante mencionar que mientras mayor valor se tenga en el capacitor o en la resistencia de carga el voltaje de rizo va a ser menor. La Ecuación 12 muestra la fórmula para el cálculo del voltaje aproximado de salida del filtro:

$$V_{cd} \approx \left(1 - \frac{1}{2f \times RL \times C}\right) V_{p(\text{rectificado})}$$

Ecuación 12: Cálculo de voltaje de salida del filtro.

Fuente: Floyd, 2008.

$$V_{cd} \approx \left(1 - \frac{1}{(240\text{Hz})(100\Omega)(2200\mu\text{F})}\right) 15,568\text{V}$$

$$V_{cd} \approx (1 - 0,0189)15,568\text{V}$$

$$V_{cd} \approx 15,27\text{V}$$

Finalmente el factor de rizo se determina a través de la Ecuación 13:

$$r = \frac{V_{r(pp)}}{V_{cd}} \times 100\%$$

Ecuación 13: Cálculo de factor de rizo.

Fuente: Floyd, 2008.

$$r = \frac{0,589\text{V}}{15,27\text{V}} \times 100\%$$

$$r = 0,038 \times 100\%$$

$$r = 3,85\%$$

La utilización de un capacitor de alto valor, hace que se tenga un porcentaje de rizo bajo, sin embargo este puede reducirse aún más mediante la combinación del capacitor con un regulador de voltaje. Para este caso se utilizan dos reguladores de voltaje, 5V y 8V, para de esta forma poder cubrir los requerimientos de alimentación de la placa base, la cual se alimenta con un voltaje recomendado de entre 7V y 12V mediante su conexión externa. Mientras tanto los 5V servirán para la alimentación a través de su terminal de conexión interna, además se alimentará a otros

dispositivos y módulos que operen bajo este rango de voltaje. A más de los dos reguladores también se utiliza un circuito regulador de corriente para la conexión y carga de una batería de respaldo, como se indica en la Figura 71:

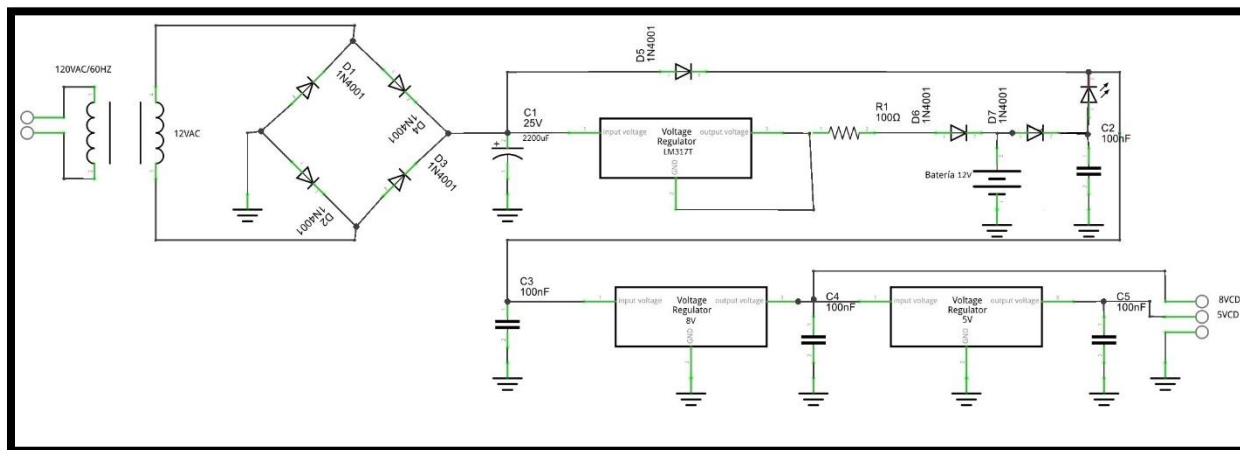


Figura 71: Diagrama esquemático de la fuente de alimentación.

Fuente: Simulador Fritzing.

La función del regulador de corriente es la de mantener un nivel continuo a la salida, mismo que servirá para cargar la batería de respaldo que posee el sistema, de esta forma se garantiza el funcionamiento del mismo por determinado tiempo, en caso de que exista un corte de energía. También se utilizan diodos rectificadores, en este caso del tipo 1N4001, con el fin de permitir el paso de corriente en un solo sentido, evitando retroalimentación de la batería al resto de la fuente de alimentación.

3.2.3.5. Cálculo de batería

Al tratarse de un sistema el cual necesita tener una fuente constante de alimentación y en caso de que ocurra algún corte de energía, se debe considerar el uso de un sistema de respaldo a través de baterías. En este caso por las características anteriormente descritas del sistema en cuanto a su consumo de energía y voltaje de funcionamiento, se utilizará una batería de 12V a 4.5A por hora.

De acuerdo a los valores de consumo del sistema y de la batería, el cálculo de su tiempo de vida útil parte de la Ecuación 14, donde:

$$\text{Potencia de la batería} = \text{Voltaje de la batería} * \text{Corriente de la batería}$$

Ecuación 14: Cálculo de la potencia de la batería.

Fuente: TODOPIC, 2015. Recuperado de: <http://www.todopic.com.ar/foros/index.php?topic=14382.0>

$$P = 12V * 4.5A$$

$$P = 54W$$

Considerando el voltaje de la batería y la corriente total de consumo, se obtiene el valor de la potencia que consumirá el sistema a partir de la Ecuación 15:

$$P = \text{Voltaje de la batería} * \text{Intensidad total del sistema}$$

Ecuación 15: Calculo de la potencia del sistema.

Fuente: TODOPIC, 2015. Recuperado de: <http://www.todopic.com.ar/foros/index.php?topic=14382.0>

$$P = 12V * 288mA$$

$$\text{Consumo del sistema} = 3,456W$$

De donde la duración de la batería es la relación entre la potencia de la batería generada en una hora y la potencia total del sistema:

$$t = \frac{54W * 1hora}{3,456W} * 0,7$$

Ecuación 16: Cálculo del tiempo de duración de la batería.

Fuente: TODOPIC, 2015. Recuperado de: <http://www.todopic.com.ar/foros/index.php?topic=14382.0>

$$t = 10,937 \text{ horas}$$

Del resultado obtenido se ve que el tiempo de vida útil de la batería en relación al consumo total de corriente del sistema es de aproximadamente 11 horas.

3.2.6. Esquema general

A continuación la Figura 72 muestra el esquema general del sistema de control de acceso con todos los elementos que lo conforman:

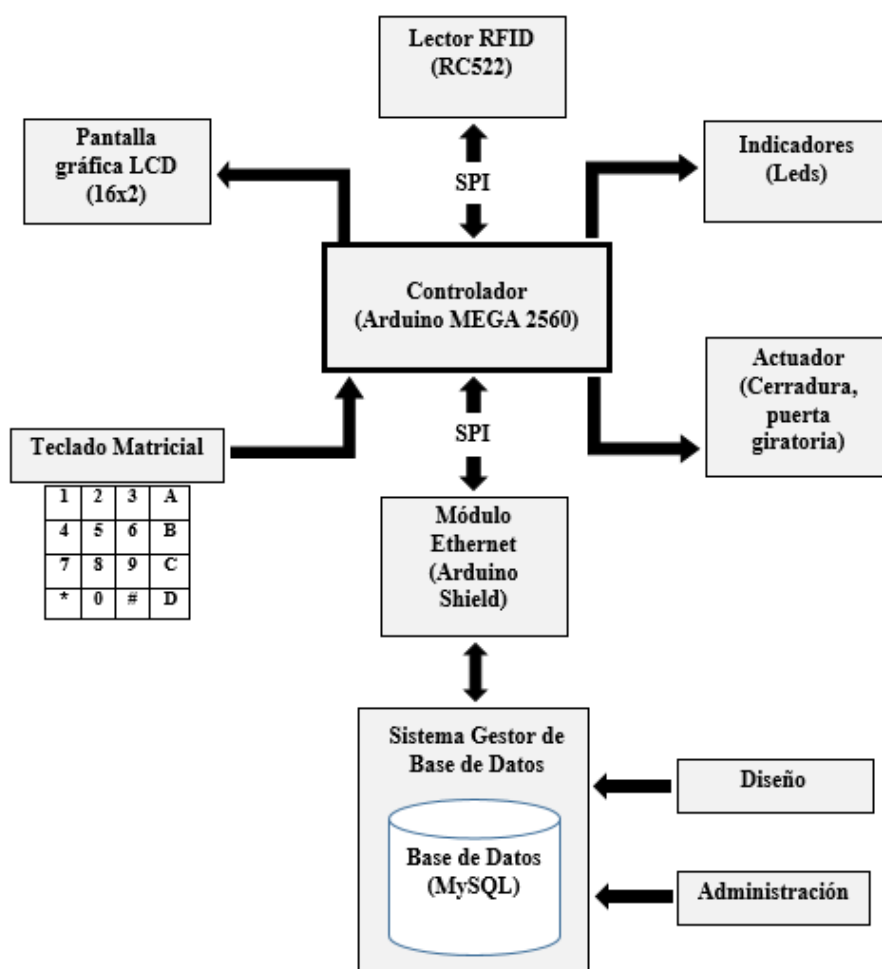


Figura 72: Diagrama en bloques del sistema de control de acceso.

Fuente: Desarrollo del proyecto.

La Figura 73 muestra el diagrama esquemático de la conexión de cada uno de los elementos electrónicos y de hardware que forman parte del sistema de control de acceso:

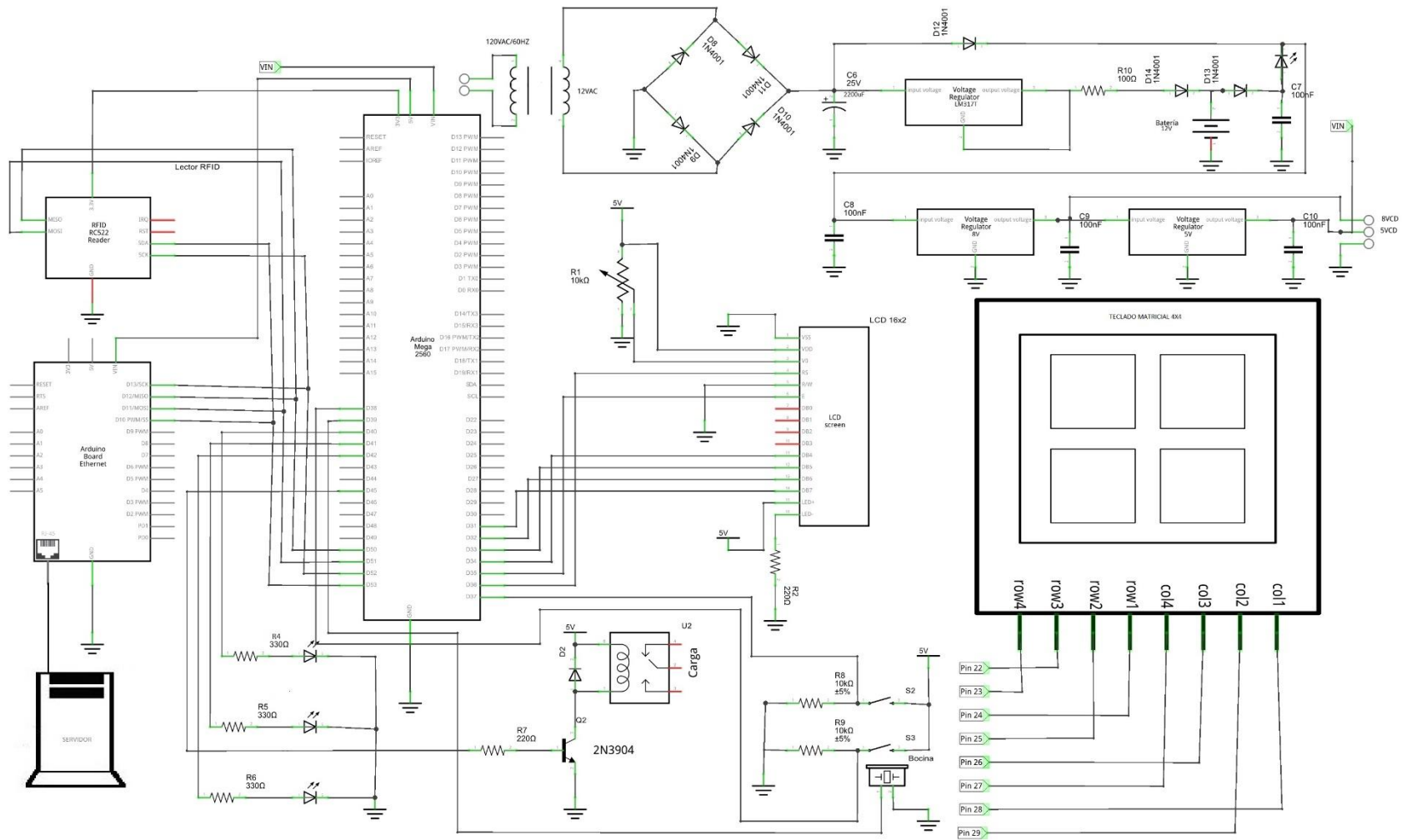


Figura 73: Diagrama esquemático del sistema de control de acceso.

Fuente: Simulador Fritzing.

3.2.7. Elaboración de placas de circuito impreso

Para el circuito de conexión de la LCD es necesario la realización de una placa de circuito impreso, misma que contenga las resistencias correspondientes para su conexión hacia la fuente de alimentación y regulación de intensidad de brillo. De igual forma en la misma placa deben estar las resistencias de conexión de los diodos led, además de los circuitos de conexión pull-down para el pulsador de ingreso de clave y de cambio de estado del sistema, como se indica en la Figura 74:

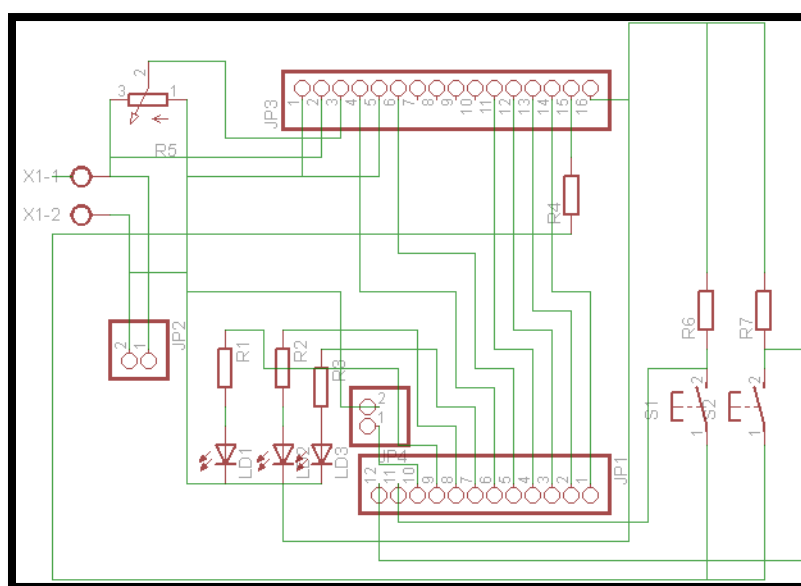


Figura 74: Diagrama esquemático de la placa para la LCD.

Fuente: Programa Eagle.

A través del diagrama esquemático anterior, se genera el circuito impreso, tal como se indica en la Figura 75:

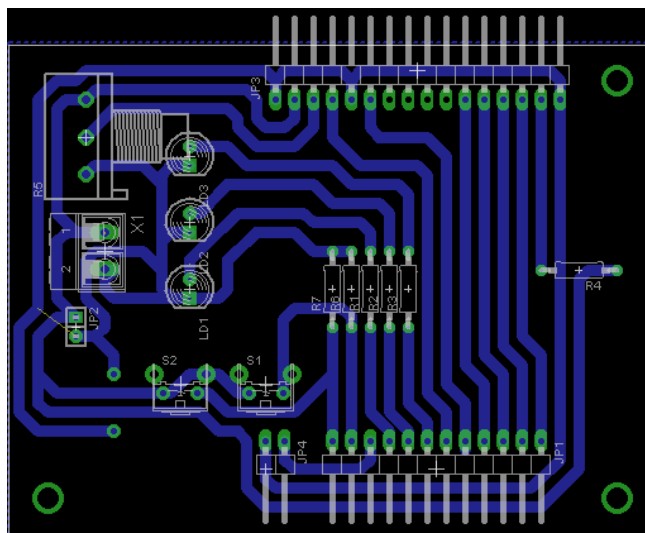


Figura 75: Circuito impreso para la conexión de la LCD, leds y pulsadores.

Fuente: Programa Eagle.

Otra placa necesaria es la que contiene la conexión del circuito actuador con el relé, el transistor de activación y su configuración, así como también el diodo de protección y el circuito indicador de activación tal como indica la Figura 76:

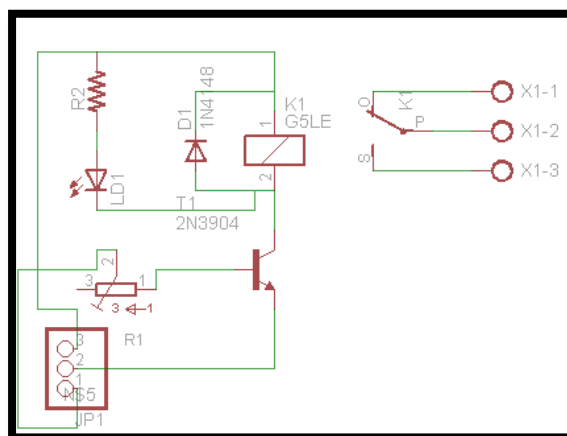


Figura 76: Diagrama esquemático del circuito actuador con relé.

Fuente: Programa Eagle.

A partir del circuito anterior se generó la placa de circuito impreso correspondiente al circuito de activación por relé que se indica en la Figura 77:

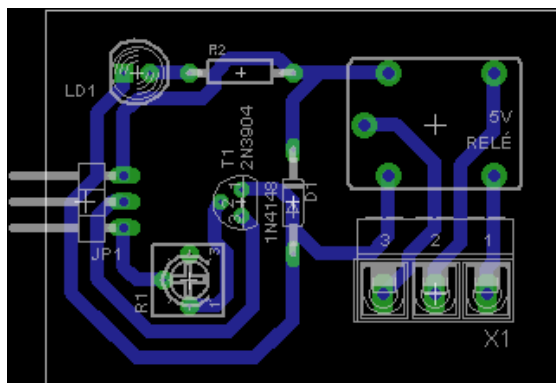


Figura 77: Circuito impreso para actuador con rele.

Fuente: Programa Eagle.

Finalmente se realizó el diagrama esquemático de la fuente de alimentación de onda completa tipo puente, la misma que cuenta con dos salidas, una de 8V y otra de 5V, esta última en caso de que se requiera conectar la alimentación a través de los terminales de entrada de la placa Arduino MEGA 2560. La Figura 78 muestra el diagrama esquemático del circuito de la fuente de alimentación:

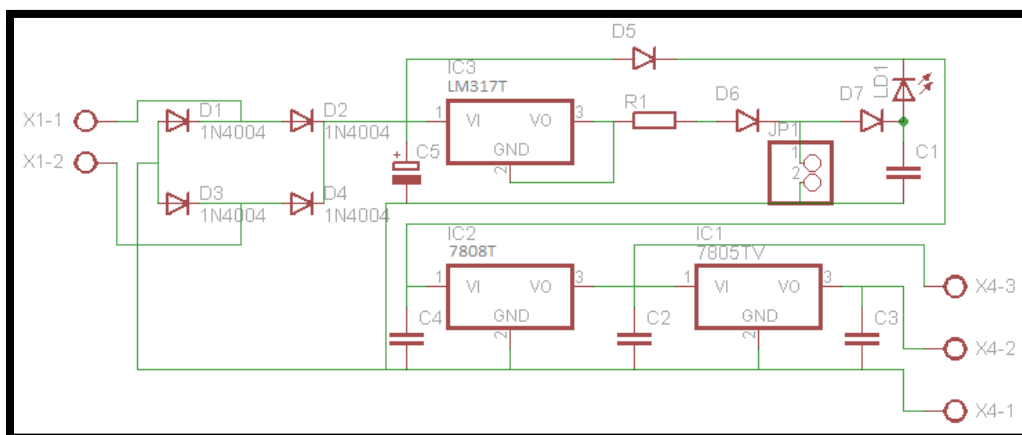


Figura 78: Diagrama esquemático para fuente de alimentación

Fuente: Programa Eagle.

A partir del diagrama esquemático de la fuente de alimentación, se pudo obtener la placa de circuito impreso que se muestra a continuación en la Figura 79:

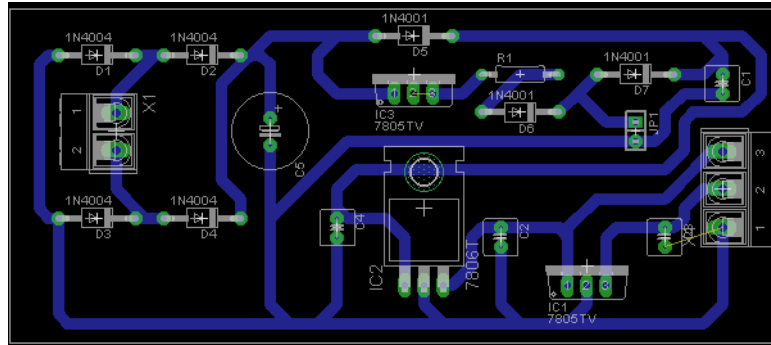


Figura 79: Circuito impreso para fuente de alimentación.

Fuente: Programa Eagle.

3.2.8. Interconexión

Una vez que se ha diseñado el sistema electrónico, se debe especificar la interconexión que tendrá el mismo con la red de datos de la Universidad Técnica del Norte, para lo cual se detalla a continuación la topología lógica que maneja la institución en la Figura 80:

3.2.8.1. Topología lógica

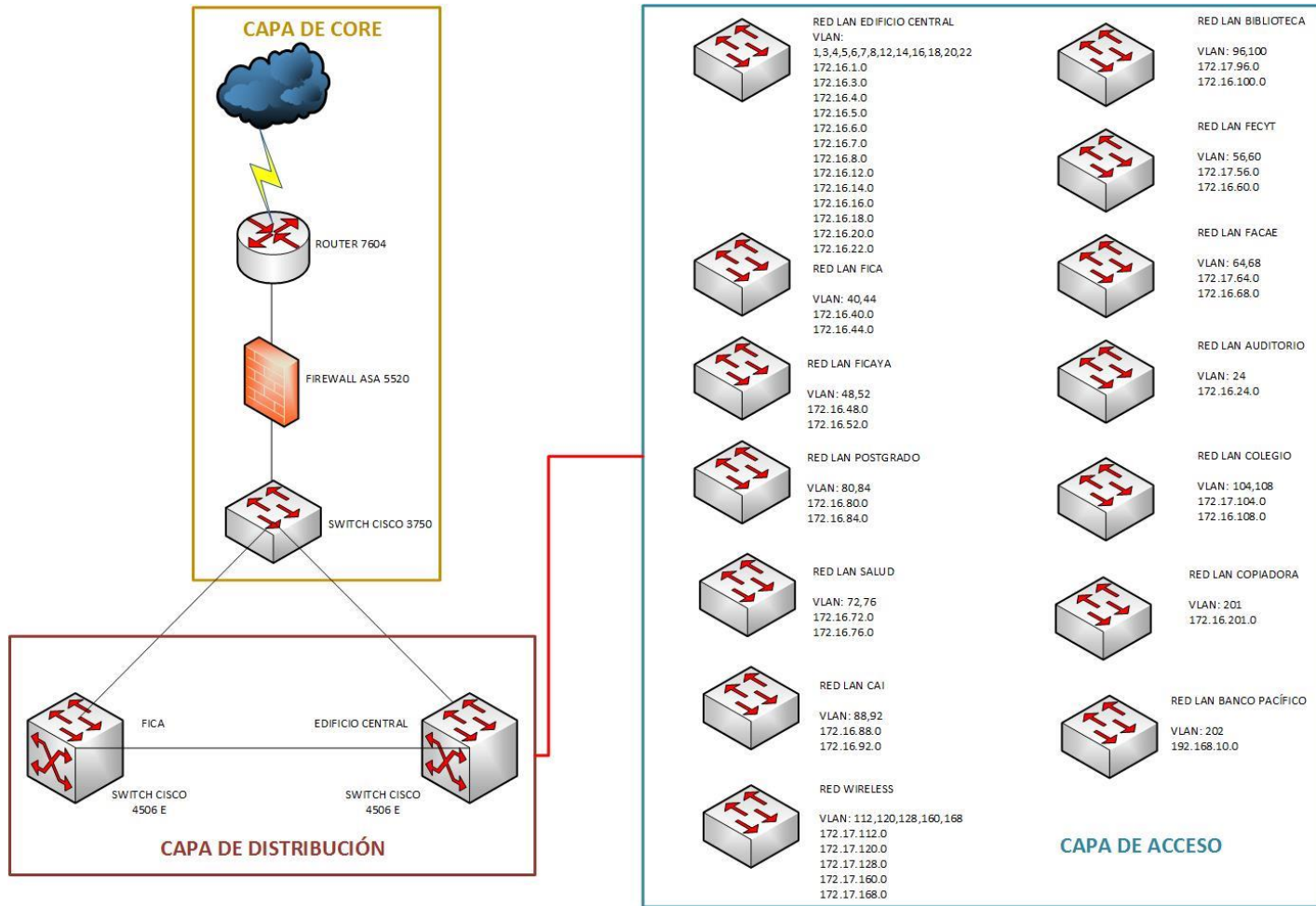


Figura 80: Topología lógica de la red de la Universidad Técnica del Norte.

Fuente: Dirección de Desarrollo Tecnológico e Informático – UTN.

3.2.8.2. Segmentación de la red

La creación de VLAN en cualquier red permite que las topologías lógicas cubran la infraestructura conmutada física, es así que, se puede dividir lógicamente la red en distintos segmentos de dominios de broadcast que brinden mejores características (Cisco Systems, 2013).

La Universidad Técnica del Norte cuenta con una red debidamente segmentada que facilita su administración y además brinda muchas ventajas, como por ejemplo:

- Mejoramiento de la escalabilidad en la red
- Mejor tráfico de datos
- Control de broadcast
- Comunicación entre VLAN

3.2.8.3. VLAN de conexión del sistema

El sistema de control de acceso estará conectado a la VLAN 1 perteneciente a todos los Equipos Activos con los que cuenta la universidad. Dentro de esta también están conectados los sistemas de control de acceso vehicular, por lo que se hace pertinente realizar la conexión en esta misma VLAN y si poder tener una adecuada administración de los sistemas de control de acceso en general.

El rango de direcciones a utilizar para esta VLAN es 172.16.1.0/24, en la que se tiene 254 direcciones utilizables.

no sería conveniente utilizar un medio cableado, y en este caso lo ideal sería al igual que en las entradas anteriores utilizar un medio inalámbrico de radioenlace.

3.2.8.5. Características del servidor para alojamiento de la base de datos

La base de datos debe estar alojada en un servidor con ciertas especificaciones que garanticen su correcta funcionalidad a corto y largo plazo según la cantidad de información que esta vaya almacenando. Entre las principales características a considerar al momento de realizar la elección de un servidor están:

- Suficiente espacio de almacenamiento actual y futuro
- Índices de memoria RAM adecuados
- Procesadores rápidos
- Uso de la tecnología RAID para brindar confiabilidad y mejorar el rendimiento

En base a estas características es importante conocer el tamaño de la base de datos, con el fin de poder tener un número estimado en cuanto al valor de almacenamiento se refiere. Dentro de MySQL existe una línea de comandos que permite la obtención del tamaño de las bases de datos, mismo que se indica en la Figura 82:

```
> SELECT table_schema "tesis", sum(data_length+index_length) / 1024 / 1024 "Espacio en MB"  
FROM information_schema.TABLES  
GROUP BY table_schema;
```

Figura 82: Comandos para visualizar el tamaño de bases de datos en MySQL.

Fuente: phpMyAdmin.

Este comando realiza la consulta de la información de esquema con la suma de la cantidad de datos como de índices generados, para poder obtener el tamaño de la base en Mega Bytes, como se observa en la Figura 83:

tesis	Espacio en MB
information_schema	0.17187500
mysql	0.83296204
performance_schema	0.00000000
phpmyadmin	0.39062500
tesis	0.06250000

Figura 83: Tamaño de base de datos en MySQL.

Fuente: phpMyAdmin.

Considerando el tamaño de la base de datos y el número de usuarios que están ingresados actualmente se establece un valor estimado de 32KB para cada uno, de esta forma se establece que para un número aproximado de 10000 usuarios se necesitaría aproximadamente 320MB para la base de datos. De esta forma se debe buscar un servidor que cubra este valor y además provea de características futuras suficientes para mantener la base de datos funcional. De acuerdo a especificaciones técnicas en cuanto a requerimientos de hardware de un servidor para base de datos, la Tabla 15 a continuación indica algunas características técnicas que debe poseer:

Tabla 15: Características de servidor para base de datos.

Características	Parámetros
Procesador	Procesador Quad-Core Intel / Core i(X) Series (basado en una arquitectura de 64 bits)
Velocidad de procesamiento	2.5 GHz
Controlador estándar	RAID
Memoria RAM	4 GB
Disco Duro	100 GB
NIC	100Mb/s

Fuente: SIGADE, 2013. Recuperado de:

http://unctad.org/divs/gds/dmfas/who/Documents/DMFAS_6_HardwareSoftware_4_SP.pdf

3.2.8.6. Conexión UPS para servidor

El servidor que contiene la base de datos requiere de una conexión a UPS, esto con el fin de garantizar el funcionamiento del mismo durante un determinado intervalo de tiempo en caso de que exista un corte inesperado de energía eléctrica.

La Universidad Técnica del Norte cuenta con un sistema UPS de la marca Computer Power de 20 KVA, mismo que se encarga del suministro de energía por un tiempo de respaldo de alrededor de 20 minutos a todos los servidores que se encuentran en el Datacenter de la institución. La Figura 84 muestra características eléctricas referentes al equipo UPS de la Universidad:

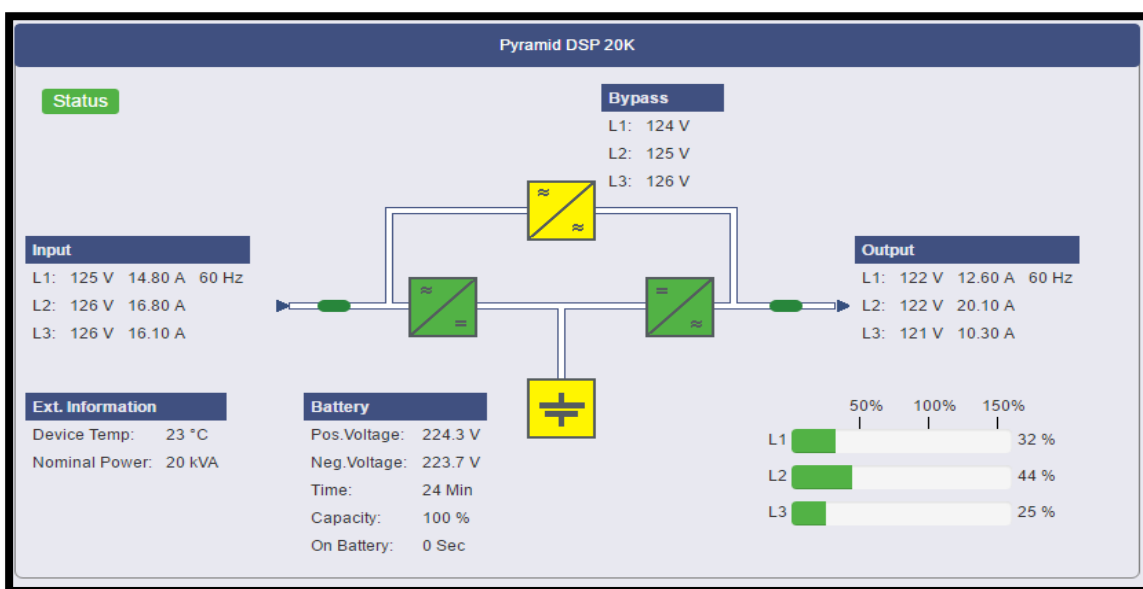


Figura 84: Características eléctricas del UPS.

Fuente: Dirección de Desarrollo Tecnológico e Informático – UTN.

En la Tabla 16 se menciona las principales características que posee el equipo UPS con que cuenta la Universidad:

Tabla 16: Características de UPS Computer Power.

Características	Parámetros
Capacidad	20000VA
Potencia	14000W
Voltaje de entrada	208V, 220V, 230V, 240V
Voltaje de salida	100V, 110V, 115V, 120V/ 208V, 220V, 230V, 240V
Frecuencia	50/60 Hz
Protección	Contra corto circuitos, rayos y sobretensiones
Tiempo de respaldo	Alrededor de 6 minutos con carga completa/15 minutos con media carga
Comunicación	RS-232, USB y tarjeta SNMP (opcional)

Fuente: Computer Power, 2012. Recuperado de <http://www.computerpower.com>

3.3. DISEÑO DE SOFTWARE

A continuación se realiza el diseño de software en el que se especifica el proceso que cumple el código de programación y cada una de las subrutinas generadas, así como también se detalla la creación de tablas en la base de datos.

3.3.1. Requerimientos del software

Dentro de los requerimientos para el diseño de Software se debe considerar la flexibilidad del sistema al momento de registrar información de usuarios y de igual forma eliminar o modificar esta.

El sistema y todos sus componentes deben estar configurados adecuadamente para su correcta funcionalidad, además de la conexión e interoperabilidad con la base de datos y la información que esta contenga. Específicamente se debe cumplir con los siguientes requisitos:

- Disponibilidad e interfaz adecuada para usuarios
- Interfaz de registro para administración
- Visualización de información

3.3.2. Programación del sistema de código abierto

Para la programación de la placa base (Arduino MEGA 2560) se deben considerar algunas librerías que facilitan el uso de distintos dispositivos y módulos que se integran en el sistema. En este caso se hará uso de las siguientes:

- Librería SPI (`#include <SPI.h>`)
- Librería Ethernet (`#include <Ethernet.h>`)
- Librería RFID (`#include <MFRC522.h>`)
- Librería Teclado matricial (`#include <Keypad.h>`)
- Librería LCD (`#include <LiquidCrystal.h>`)
- Librería RestClient (`#include "RestClient.h"`)

El uso de estas librerías hace que el sistema interactúe de forma adecuada con los demás dispositivos, en base a la funcionalidad y programación que se realice.

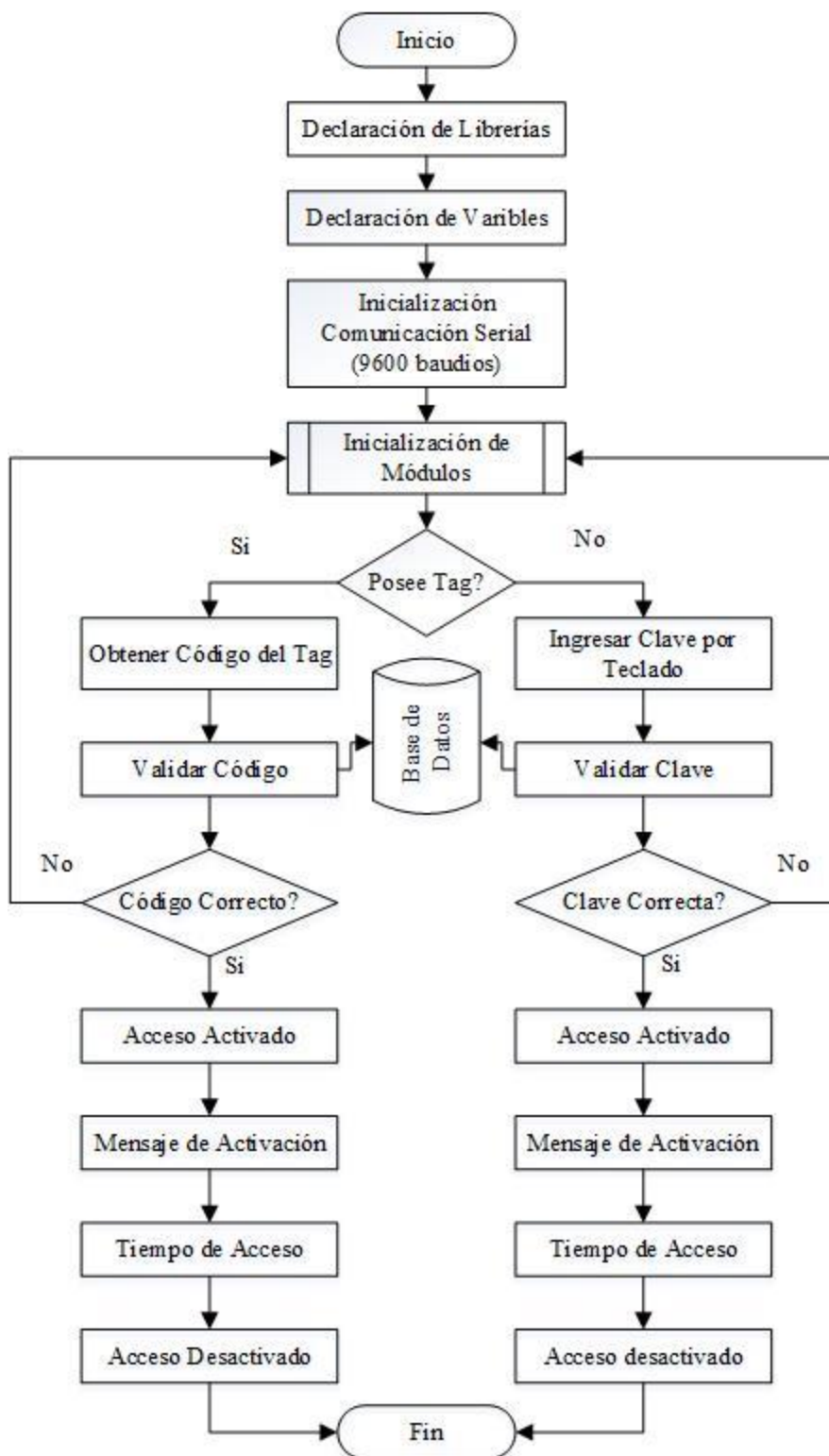


Figura 85: Diagrama de flujo del funcionamiento del Sistema de Control de Acceso

Fuente: Desarrollo del proyecto.

Como se puede observar en la Figura 85, luego de la declaración de variables e inicialización de módulos, de acuerdo al código de programación del ANEXO A, Sección 1 y 2, se tiene dos procesos, uno para la validación del código del tag y el otro para la clave por teclado. Para ambos procesos la validación será casi la misma ya que tanto código como clave están almacenadas en la base de datos.

3.3.2.2. Configuración de módulo Ethernet

El funcionamiento de este módulo se basa en la utilización de la librería Ethernet, la cual permite realizar una conexión TCP/IP entrante o saliente a través de una interfaz RJ-45. Además de la librería Ethernet se utiliza la librería RestClient, misma que facilita la realización de peticiones HTTP POST a un servidor en el cual se almacenan los reportes para la base de datos a través de un script PHP. Su comunicación con la placa base es a través de SPI mediante los terminales 50, 51, y 52 correspondientes a MISO, MOSI y SCK respectivamente (Arduino, 2015).

El trabajo de la librería sobre el módulo Ethernet se detalla en la Figura 86, que especifica la subrutina de inicialización del módulo Ethernet en el esquema general de funcionamiento del sistema, referente al código de programación del ANEXO A en la Sección 4:

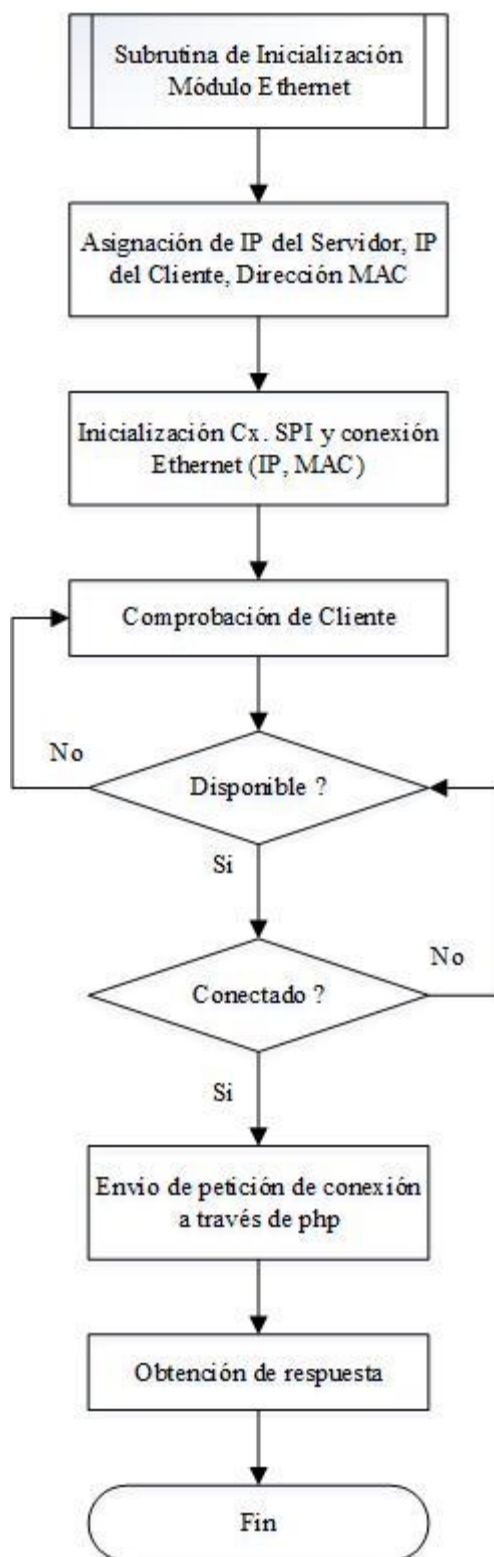


Figura 86: Diagrama de flujo de la subrutina de inicialización del módulo Ethernet.

Fuente: Desarrollo del proyecto.

3.3.2.3. Configuración módulo RFID RC522

El módulo RFID RC522 utiliza la librería MFRC522 para su funcionamiento, misma que provee mecanismos necesarios para la comunicación con la placa base a través de SPI. Su proceso de configuración y funcionamiento se muestra en la Figura 87, la cual hace referencia al código de programación del ANEXO A, Sección 2 y 7:

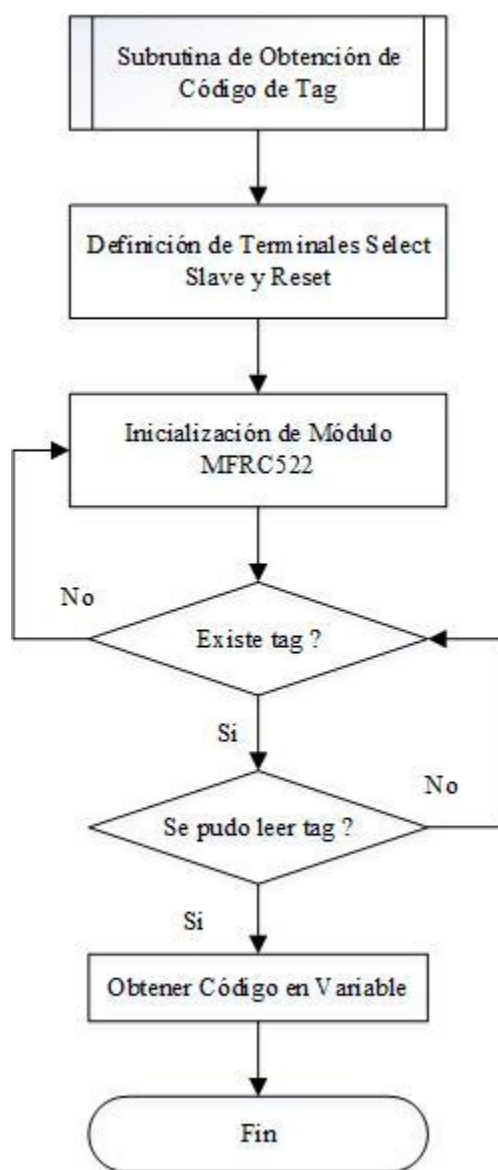


Figura 87: Diagrama de flujo de la subrutina de la obtención del código del tag.

Fuente: Desarrollo del proyecto.

Una de la funciones de más importancia que brinda la librería MFRC522 es “mfr522.uid.uidByte[i]”, la cual permite obtener la serie de las tarjetas electrónicas y almacenarlas en un vector, vector que posteriormente se transforma en un dato de tipo String, el cual será validado con información almacenada en la base de datos.

3.3.2.4. Programación teclado matricial

El teclado matricial 4x4 permite digitar un código único y almacenarlo temporalmente hasta ser validado con la información de la base de datos, para permitir o denegar el acceso a los usuarios. Este proceso se realiza mediante la utilización de un método anti rebote “waitForKey ()”, haciendo que el sistema ingrese en una subrutina que permita digitar la clave y evitando así el ingreso a bucles infinitos que ocasionen problemas en el sistema. La Figura 88 a continuación muestra el proceso de configuración y funcionamiento del teclado matricial, de acuerdo al programa del ANEXO A, Sección 6:

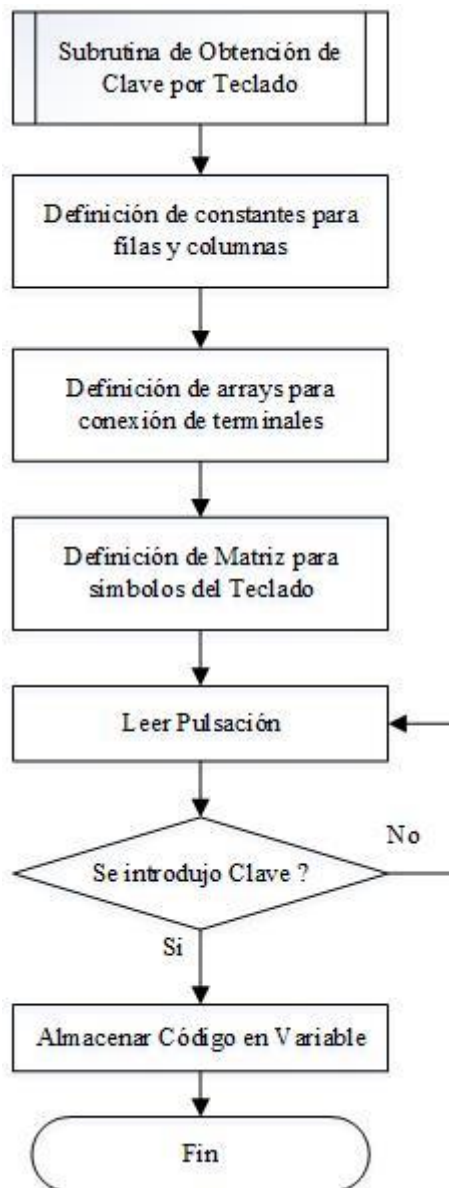


Figura 88: Diagrama de flujo de la subrutina de obtención de la clave por teclado.

Fuente: Desarrollo del proyecto.

3.3.2.5. Programación pantalla grafica LCD

La pantalla grafica LCD 16x2 permitirá al usuario visualizar un mensaje de validación o denegación de código o clave insertada a través del tag o del teclado. La Figura 89 muestra el proceso de configuración y funcionamiento de la LCD:

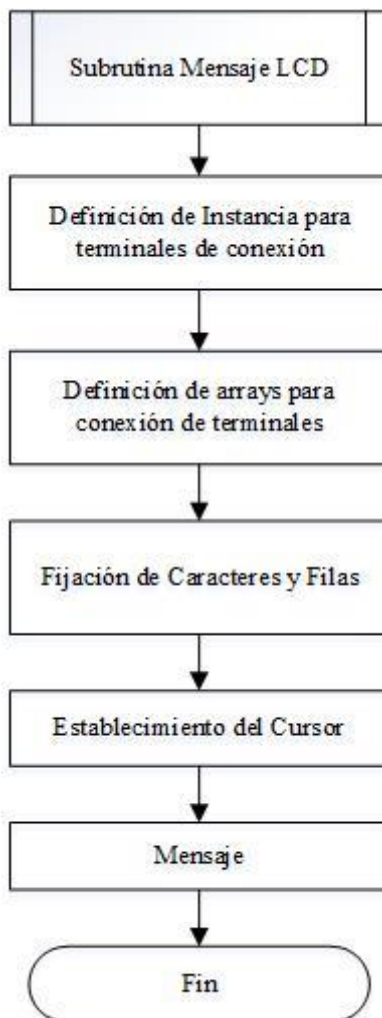


Figura 89: Diagrama de flujo de la subrutina de mensajes en la LCD.

Fuente: Desarrollo del proyecto.

3.3.2.6. Subrutina de envío y recepción de paquetes

El sistema opera bajo el intercambio de información entregada por el usuario y validada en la base de datos. El usuario al momento de realizar un registro hace que el sistema almacene dicho registro en una variable, misma que será enviada como una solicitud a un módulo PHP, el cual ejecutará la petición a través de una comunicación TCP/IP, donde la información se almacenará en un datagrama IP con información de origen y destino del paquete, que se comunicará a través de puertos específicos, en este caso serán los puertos 80 y 443 para Apache y el puerto 3306 para

MySQL. La petición entregada por PHP es procesada por MySQL y envía la información de vuelta hacia el modulo PHP. Finalmente PHP se encarga de comunicar al procesador del sistema los resultados de la petición, que generen la acción en el sistema. La Figura 90 a continuación muestra el proceso de interacción de la base de datos con el sistema a través de PHP:

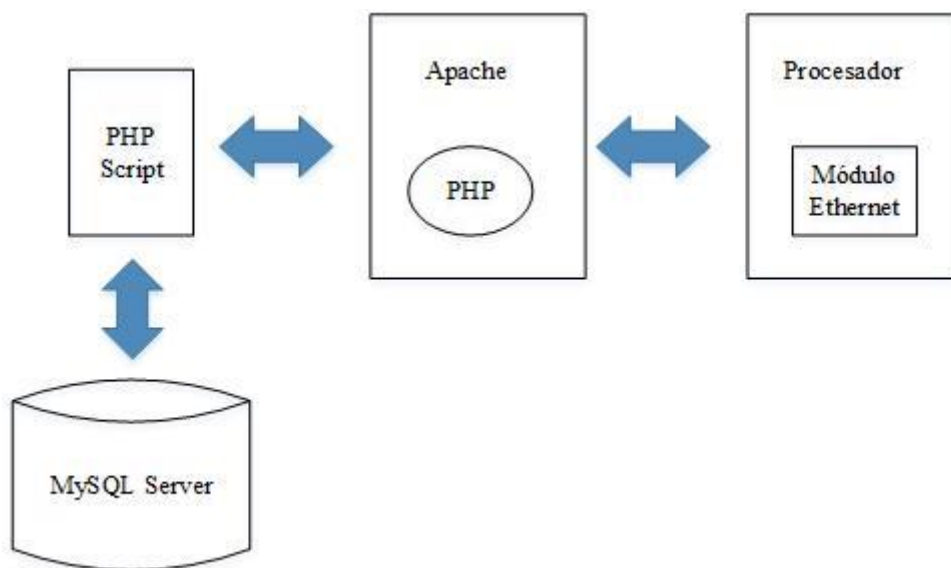


Figura 90: Esquema de interacción de la base de datos a través de PHP.

Fuente: Berni Millet & Gil de la Iglesia, 2010.

El proceso de envío de información desde el sistema se realiza mediante el método POST hacia PHP. Este método se caracteriza por enviar los datos de forma oculta, es decir que, los datos enviados desde el formulario no son visibles en la URL, pero sí son recuperables usando las instrucciones adecuadas (Aprenderaprogramar, 2016).

Los datos enviados a través del método POST están disponibles en variables denominadas superglobales, debido a que siempre se encuentran utilizables a lo largo de un script PHP (Berni Millet & Gil de la Iglesia, 2010).

Dentro del sistema de control de acceso los códigos y claves del lector y teclado respectivamente serán almacenados en vector para posteriormente transformarlos en una cadena y

asociarlos a un prefijo que facilite la búsqueda de información a través de PHP. La Figura 91 a continuación muestra el proceso de la subrutina de validación de código y clave de acuerdo al código de programa del ANEXO A, Sección 4, 6 y 7:

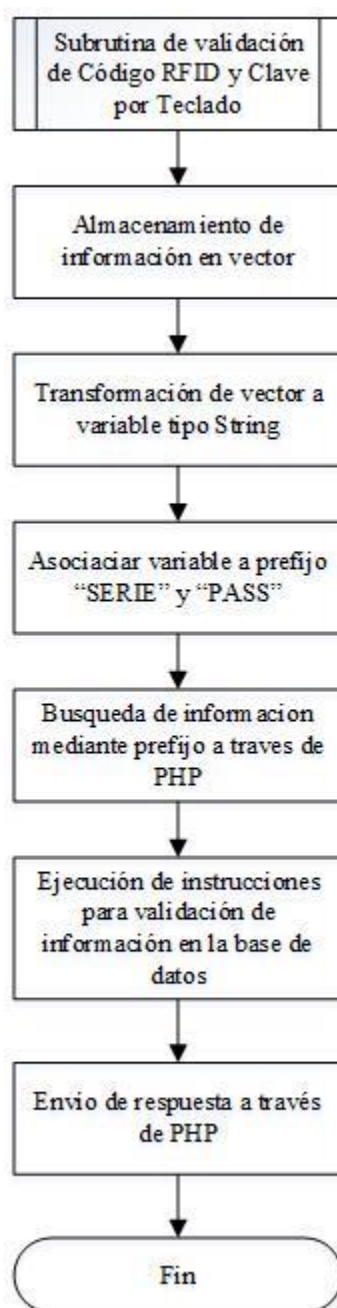


Figura 91: Diagrama de flujo de la subrutina de validación de código y clave.

Fuente: Desarrollo del proyecto.

3.3.3. Creación de tablas en MySQL

La creación de tablas en MySQL se las realiza a través del gestor phpMyAdmin, este gestor es un programa que opera bajo libre licencia proporcionando una herramienta gráfica web para la creación y administración de bases de datos.

Para acceder al programa se ingresa en la barra de direcciones “localhost/phpmyadmin/” de cualquier buscador de internet. Una vez que se ingresa se puede visualizar la página principal del programa y todas las herramientas que posee para la creación y administración de bases de datos y tablas, como indica la Figura 92:

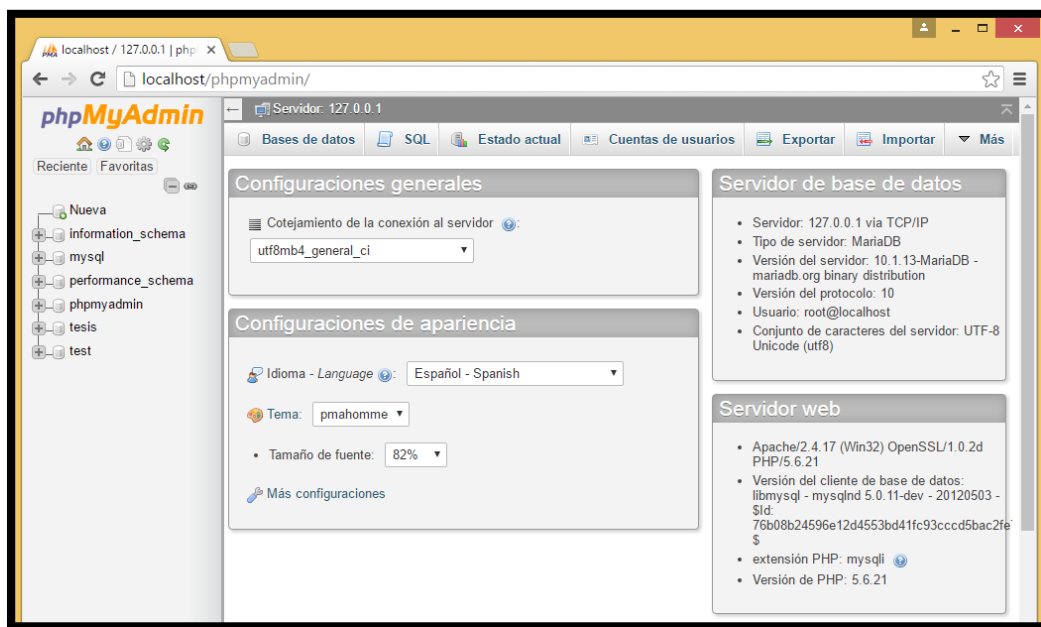


Figura 92: Página principal de phpMyAdmin.

Fuente: phpMyAdmin.

Para el desarrollo de la base de datos que contendrá la información de los usuarios del sistema de control de acceso se utilizarán las siguientes tablas:

- Tabla “login”

- Tabla “usuarios”
- Tabla “registros”
- Tabla “no registrados”
- Tabla “visitantes”

3.3.4.1. Tabla “login”

Esta tabla contiene datos de usuario y contraseña, con los que el administrador podrá ingresar a la página principal, esto con el fin de evitar que cualquier persona pueda ingresar a la página.

Esta tabla contiene tres campos: id, usuario y password, de donde la información almacenada en los campos usuario y password serán los que validen el ingreso a la página principal. La Figura 93 a continuación indica la estructura de la tabla login:


#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
<input type="checkbox"/>	1 id 	int(11)			No	Ninguna	AUTO_INCREMENT
<input type="checkbox"/>	2 usuario	varchar(20)			No	Ninguna	
<input type="checkbox"/>	3 password	varchar(20)			No	Ninguna	

Figura 93: Estructura de la tabla “login”.

Fuente: phpMyAdmin.

3.3.4.2. Tabla “usuarios”

La tabla usuarios contendrá todos los datos e información personal de cada uno de los usuarios del sistema de control de acceso. Esta tabla contiene los siguientes campos:

- Id.- este campo será único e irrepetible e identificara a cada usuario.
- Nombre.- este campo contendrá el nombre y apellidos de cada usuario.

- Correo.- el campo correo tendrá la información pertinente al correo electrónico de cada usuario.
- Tag.- en este campo se debe almacenar el código único de la tarjeta electrónica.
- Clave.- al igual que el campo anterior, este campo contiene una clave única.
- Cédula.- aquí se tendrá almacenado el número de cedula de los usuarios.
- Rol.- este campo describe el rol que desempeña cada persona que hará uso del sistema de control de acceso.

Cada uno de estos campos debe ser creado con un tipo y valor específico de variable como se indica en la Figura 94:

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
<input type="checkbox"/>	1	id		int(11)	No	Ninguna	AUTO_INCREMENT
<input type="checkbox"/>	2	nombre		varchar(30)	No	Ninguna	
<input type="checkbox"/>	3	correo		varchar(40)	No	Ninguna	
<input type="checkbox"/>	4	tag		varchar(15)	No	Ninguna	
<input type="checkbox"/>	5	clave		varchar(10)	No	Ninguna	
<input type="checkbox"/>	6	cedula		varchar(10)	No	Ninguna	
<input type="checkbox"/>	7	rol		varchar(40)	No	Ninguna	

Figura 94: Estructura de la tabla usuarios.

Fuente: phpMyAdmin.

El administrador tendrá que ingresar los datos a través del gestor phpMyAdmin, o a su vez, a través de una plantilla HTML que ayude a realizar un registro mucho más rápido de los usuarios.

3.3.4.3. Tabla “registros”

Dentro de la tabla registros se almacenará cierta información del usuario que haya hecho uso del sistema. La información específica dentro de esta tabla estará almacenada en los siguientes campos:

- Id.- campo utilizado para la identificación de cada usuario.
- Tag.- este campo contendrá el nombre de los usuarios que haya accedido mediante el sistema de control de acceso.
- Hora.- aquí se almacena la hora en la que el usuario haya realizado su registro de ingreso.
- Fecha.- se almacena la fecha en la que el usuario realizó su registro de acceso.

El tipo y valor asignado para cada uno de estos campos se muestra a continuación en la Figura

95:


#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
<input type="checkbox"/> 1	id 	int(11)			No	Ninguna	AUTO_INCREMENT
<input type="checkbox"/> 2	tag	varchar(30)			No	Ninguna	
<input type="checkbox"/> 3	hora	time			No	Ninguna	
<input type="checkbox"/> 4	fecha	date			No	Ninguna	

Figura 95: Estructura de la tabla registros.

Fuente: phpMyAdmin.

3.3.4.4. Tabla “no registrados”

La información que contiene la tabla no registrados es el código de la tarjeta electrónica que no esté registrada en la tabla usuarios y que vaya a ser registrada para un nuevo usuario. Para ello se mostrara este código en la plantilla HTML un campo en el que pueda visualizar la última lectura realizada de un tag que aún no este registrado, esto se realiza con el fin de que el administrador pueda agregar fácilmente un nuevo usuario al sistema. La estructura de la tabla “no registrados” se muestra en la Figura 96 a continuación:


#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
<input type="checkbox"/>	1	id 	int(11)		No	Ninguna	AUTO_INCREMENT
<input type="checkbox"/>	2	tag	varchar(30)		No	Ninguna	

Figura 96: Estructura de la tabla “no registrados”.

Fuente: phpMyAdmin.

3.3.4.5. Tabla “visitantes”

La tabla “visitantes” contiene la información pertinente a las personas que requieren ingresar al campus y no poseen un identificador ni una clave de acceso, por tal motivo, se realiza un registro y posteriormente se concede el acceso. De esta forma el sistema lleva el registro no solo de los usuarios, sino que también permite llevar un control de aquellas personas que no tienen información almacenada en la base de datos. La Figura 97 a continuación muestra la estructura de la tabla “visitantes”:


#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
<input type="checkbox"/>	1	id 	int(11)		No	Ninguna	AUTO_INCREMENT
<input type="checkbox"/>	2	nombre	varchar(30)		No	Ninguna	
<input type="checkbox"/>	3	cedula	varchar(10)		No	Ninguna	
<input type="checkbox"/>	4	hora	time		No	Ninguna	
<input type="checkbox"/>	5	fecha	date		No	Ninguna	

Figura 97: Estructura de la tabla “visitantes”.

Fuente: phpMyAdmin.

CAPÍTULO IV

4. PRUEBAS DE FUNCIONAMIENTO Y ANÁLISIS

ECONÓMICO

En este capítulo se realiza las pruebas de funcionamiento del sistema de control de acceso, comprobando la funcionalidad de cada elemento que lo conforma y finalmente su interacción con la base de datos, así como también se realiza el análisis económico de los materiales y elementos electrónicos utilizados en el diseño.

4.1. PRUEBAS DE HARDWARE

A continuación se realiza las pruebas de hardware de cada uno de los módulos y secciones más importantes que componen el sistema, iniciando por el lector RFID y posteriormente el teclado y modulo Ethernet.

4.1.1. Pruebas de Lectura del código de la tarjeta electrónica

El primer prototipo realizado tuvo como finalidad únicamente la lectura del código de las tarjetas electrónicas, para de esta forma poder obtener el número de serie y posteriormente almacenarlo en la base de datos. La Figura 98 muestra la lectura de un tag en el que se visualiza un código, el mismo que pertenece a la sección del número de serie, de acuerdo a la especificación del estándar EPC.

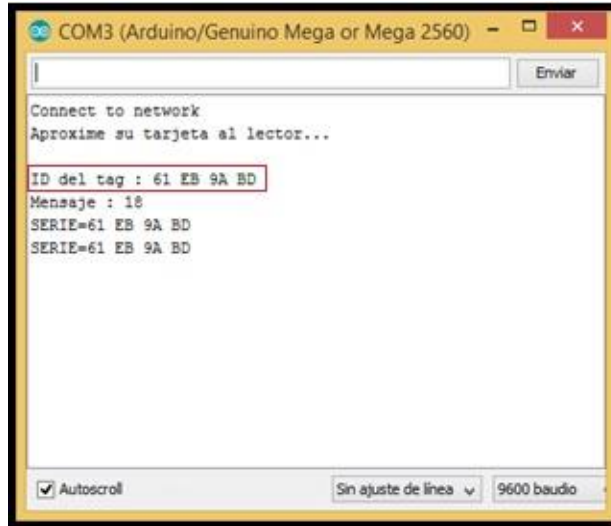


Figura 98: Lectura de Código de tarjeta RFID.

Fuente: IDE Arduino.

El estándar EPC indica que la sección del número de serie posee una longitud de 36 bits, los cuales se encuentran expresados de forma hexadecimal, de acuerdo a esto, se debe almacenar la información en la base de datos en ese mismo formato, para que no exista ningún tipo de inconsistencia al momento de su validación.

4.1.2. Pruebas de funcionamiento del teclado matricial

Al igual que el lector RFID, la funcionalidad del teclado matricial fue comprobada primeramente por separado, tratando de realizar un código correcto que pueda adaptarse posteriormente al resto del sistema.

El método anti rebotes que se utiliza facilita el funcionamiento del teclado y su librería, garantizando que no se produzcan inconvenientes con el resto de dispositivos del sistema, para ello se debe primeramente presionar el pulsador que activa la subrutina únicamente hasta ingresar la clave, luego de esto termina la subrutina y se ejecuta el resto del programa normalmente, como se indica en la Figura 99:

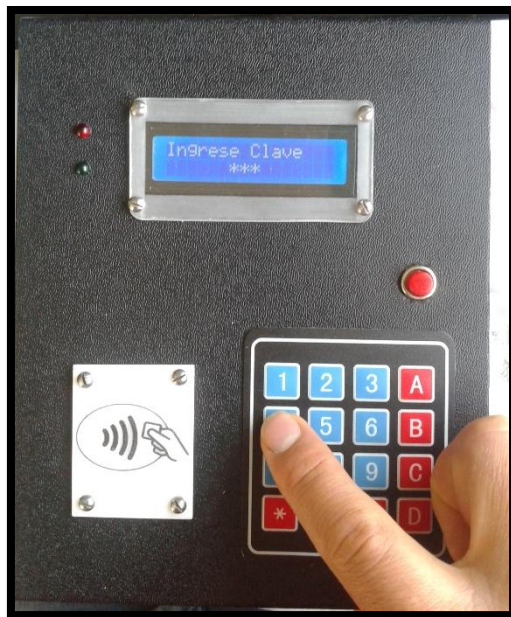


Figura 99: Activación de subrutina para ingreso de clave por teclado:

Fuente: Desarrollo del proyecto.

Si el código ingresado mediante el teclado es el correcto, se obtendrá una respuesta por parte del servidor a través del sistema, permitiendo el acceso, como se indica en la Figura 100:

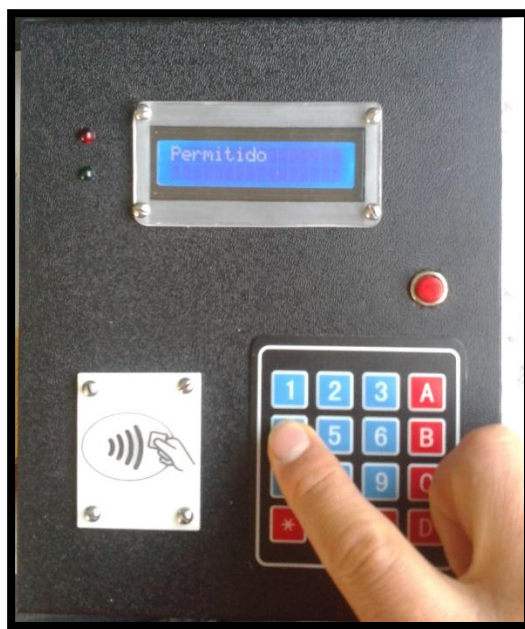


Figura 100: Ingreso correcto de clave a través del teclado matricial.

Fuente: Desarrollo del proyecto.

Además de la interfaz del sistema a través de la LCD, también se puede verificar las respuestas del mismo, mediante el uso del monitor serial de Arduino, tal como indica la Figura 101:

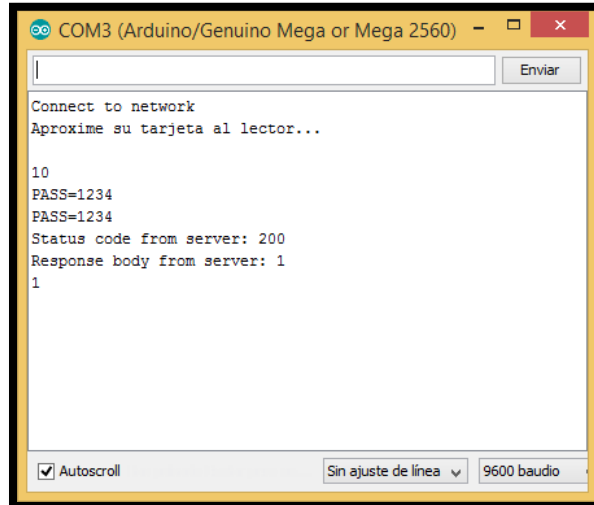


Figura 101: Visualización de ingreso de clave correcta a través del monitor serial.

Fuente: IDE Arduino.

Por otro lado, si se ingresa una clave errada no se obtendrá ningún tipo de respuesta por parte del servidor, y por tanto se denegará el acceso, como se puede observar en la Figura 102:



Figura 102: Ingreso de clave incorrecta mediante teclado matricial.

Fuente: IDE Arduino.

4.1.3. Pruebas de funcionamiento del módulo Ethernet

Para comprobar la funcionalidad del módulo Ethernet al momento de conectarlo, se debe primeramente configurar la tarjeta de red del computador y poner una dirección IP que se encuentre dentro del mismo rango que el modulo, como se observa en la Figura 103. En este caso la dirección establecida para el computador es la 172.16.1.210/24.

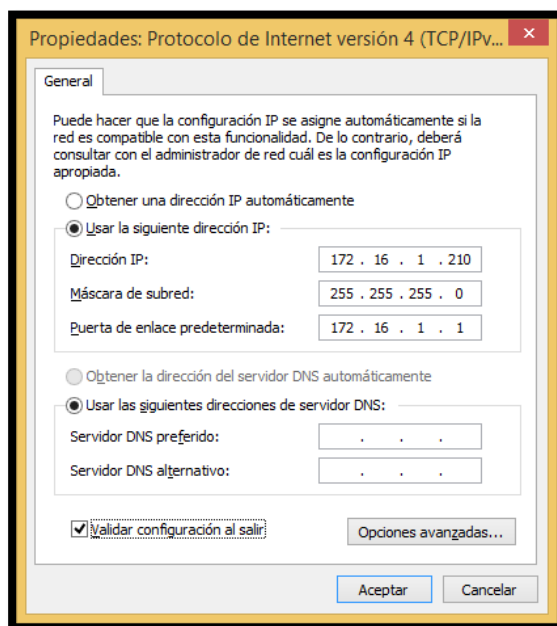


Figura 103: Configuración de tarjeta de red.

Fuente: Tarjeta de red.

Una vez configurada la tarjeta de red del computador, se puede fácilmente comprobar su funcionalidad a través de un ping hacia la dirección del módulo Ethernet, como se observa en la Figura 104, el cual indicara si su dirección IP está debidamente configurada y si el modulo está conectado adecuadamente y listo para funcionar.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Emerson>ping 172.16.1.211

Haciendo ping a 172.16.1.211 con 32 bytes de datos:
Respuesta desde 172.16.1.211: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.1.211: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.1.211: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.16.1.211: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 172.16.1.211:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Emerson>_

```

Figura 104: Ping hacia dirección IP del módulo Ethernet.

Fuente: Símbolo del sistema.

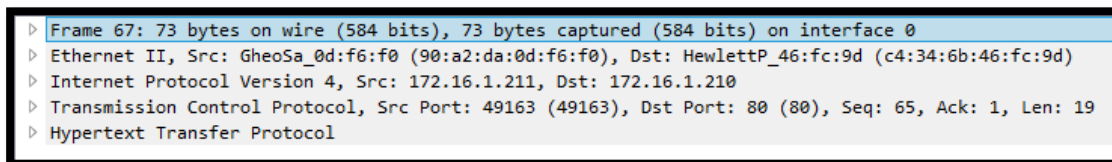
Una vez que el módulo tenga configurada su dirección IP se debe verificar el flujo de información a través del mismo, para ello se procede a realizar una captura de paquetes con la finalidad de comprobar la funcionalidad del sistema y específicamente del controlador Ethernet en la red. La Figura 105 a continuación muestra el envío de información a través de la red desde el sistema hasta la base de datos y viceversa:

No.	Time	Source	Destination	Protocol	Length	Info
98	74.021601	172.16.1.211	172.16.1.210	TCP	60	49165 → 80 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
99	74.021700	172.16.1.210	172.16.1.211	TCP	58	80 → 49165 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
100	74.021952	172.16.1.211	172.16.1.210	TCP	60	49165 → 80 [ACK] Seq=1 Ack=1 Win=2048 Len=0
101	74.023127	172.16.1.211	172.16.1.210	TCP	60	[TCP segment of a reassembled PDU]
102	74.024066	172.16.1.211	172.16.1.210	TCP	60	[TCP segment of a reassembled PDU]
103	74.024104	172.16.1.211	172.16.1.210	TCP	82	[TCP segment of a reassembled PDU]
104	74.024146	172.16.1.210	172.16.1.211	TCP	54	80 → 49165 [ACK] Seq=1 Ack=6 Win=64240 Len=0
105	74.025255	172.16.1.211	172.16.1.210	TCP	65	[TCP segment of a reassembled PDU]
106	74.025326	172.16.1.210	172.16.1.211	TCP	54	80 → 49165 [ACK] Seq=1 Ack=45 Win=64201 Len=0
107	74.025417	172.16.1.211	172.16.1.210	TCP	60	[TCP segment of a reassembled PDU]
108	74.025536	172.16.1.211	172.16.1.210	TCP	66	[TCP segment of a reassembled PDU]
109	74.025564	172.16.1.210	172.16.1.211	TCP	54	80 → 49165 [ACK] Seq=1 Ack=63 Win=64183 Len=0
110	74.025643	172.16.1.211	172.16.1.210	TCP	60	[TCP segment of a reassembled PDU]
111	74.026671	172.16.1.211	172.16.1.210	TCP	73	[TCP segment of a reassembled PDU]
112	74.026732	172.16.1.210	172.16.1.211	TCP	54	80 → 49165 [ACK] Seq=1 Ack=84 Win=64162 Len=0
113	74.026835	172.16.1.211	172.16.1.210	TCP	73	[TCP segment of a reassembled PDU]
114	74.027870	172.16.1.211	172.16.1.210	TCP	103	[TCP segment of a reassembled PDU]

Figura 105: Captura de paquetes entre el sistema y la base de datos.

Fuente: Wireshark.

A través del programa Wireshark se puede observar una serie de paquetes, de los cuales se obtiene información detallada de cada uno, como por ejemplo el tipo de mensaje IPv4, TCP, entre otras características como indica la Figura 106:



```
▷ Frame 67: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▷ Ethernet II, Src: GheoS_a_0d:f6:f0 (90:a2:da:0d:f6:f0), Dst: HewlettP_46:fc:9d (c4:34:6b:46:fc:9d)
▷ Internet Protocol Version 4, Src: 172.16.1.211, Dst: 172.16.1.210
▷ Transmission Control Protocol, Src Port: 49163 (49163), Dst Port: 80 (80), Seq: 65, Ack: 1, Len: 19
▷ Hypertext Transfer Protocol
```

Figura 106: Características de paquete capturado.

Fuente: Wireshark.

4.2. PRUEBAS DE FUNCIONAMIENTO DE SOFTWARE

Las pruebas de funcionamiento de software se enfocan principalmente en la interacción de la página para la gestión de información de los usuarios y su almacenamiento en la base de datos.

4.2.1. Ingreso a la página de administración a través de usuario y contraseña

Fue necesaria la creación de una página web como indica la Figura 107, que sirva para el registro de usuarios al sistema, sin embargo, si la página no tiene un proceso de validación de usuario y contraseña, es probable que cualquier persona no autorizada pueda ingresar a la misma y realizar registros no autorizados. Es por eso que se creó una tabla con el nombre “login” en la base de datos que contenga información de usuario y contraseña para el ingreso del administrador a la página principal.

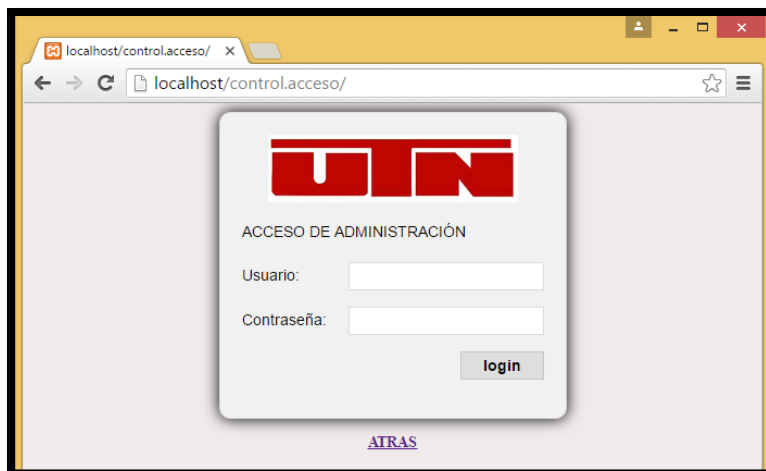


Figura 107: Página de ingreso de usuario y contraseña.

Fuente: Página Web del sistema.

En caso de que se ingresen datos errados se mostrará un mensaje que indique que los datos ingresados fueron incorrectos y se deben ingresar nuevamente, como se observa en la Figura 108:

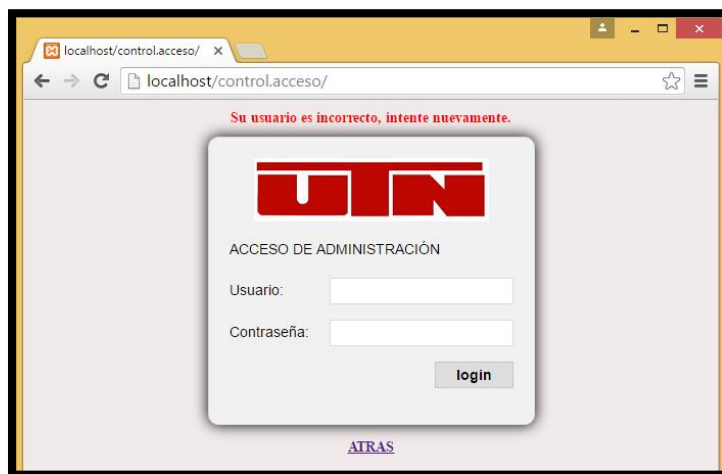


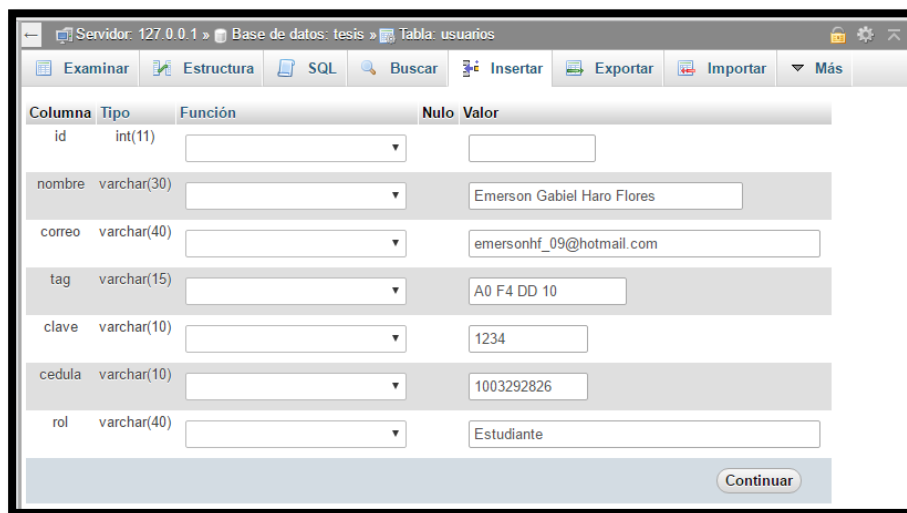
Figura 108: Ingreso incorrecto de usuario y contraseña.

Fuente: Página Web del sistema.

4.2.2. Registro de usuarios en la base de datos

Los usuarios pueden ser registrados a través de gestor phpMyAdmin, así como también a través de la página web, para ello se debe acceder a cualquiera de los dos sitios.

En el caso de que se utilice phpMyAdmin, se debe seleccionar la tabla usuarios e ingresar a la opción insertar y proceder a editar los datos solicitados para cada usuario, como se observa en la Figura 109:



Columna	Tipo	Función	Nulo	Valor
id	int(11)	<input type="text"/>		<input type="text"/>
nombre	varchar(30)	<input type="text"/>		Emerson Gabriel Haro Flores
correo	varchar(40)	<input type="text"/>		emersonhf_09@hotmail.com
tag	varchar(15)	<input type="text"/>		A0 F4 DD 10
clave	varchar(10)	<input type="text"/>		1234
cedula	varchar(10)	<input type="text"/>		1003292826
rol	varchar(40)	<input type="text"/>		Estudiante

Figura 109: Ingreso de datos en la tabla usuarios a través de phpMyAdmin.

Fuente: phpMyAdmin.

Al momento de terminar de ingresar los datos del usuario se procede a guardar los cambios realizados, y se puede observar que los datos se ingresaron correctamente, como indica la Figura 110:

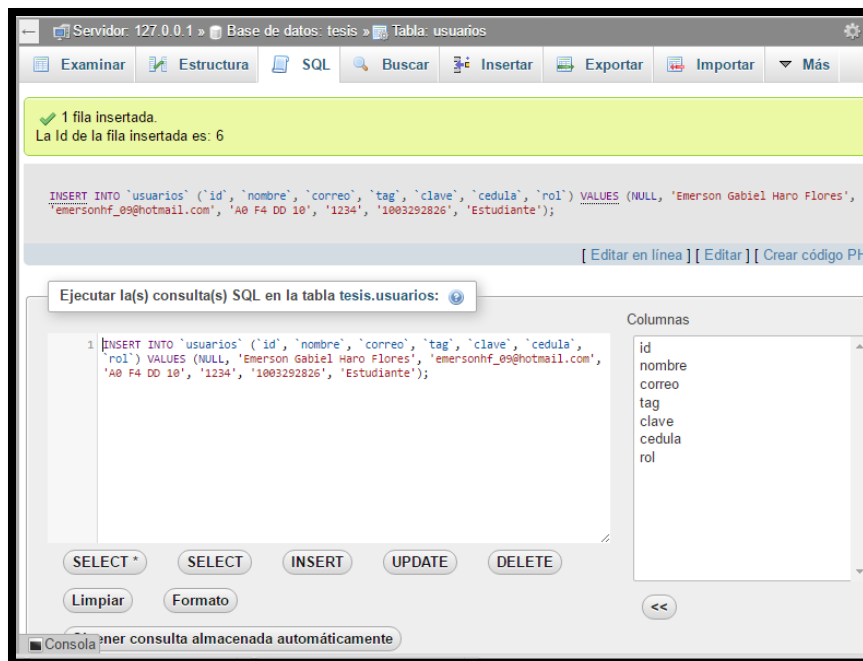


Figura 110: Datos ingresados correctamente en la tabla usuarios.

Fuente: phpMyAdmin.

Por otro lado, si se desea ingresar usuarios mediante la página web, la base de datos debe estar conectada al resto del sistema electrónico, ya que, el código del tag no registrado se obtendrá mediante el lector RFID.

Si se realiza la lectura a una tarjeta que no esté registrada el servidor no enviará ningún tipo de respuesta y el acceso se denegará, como se observa en la Figura 111:

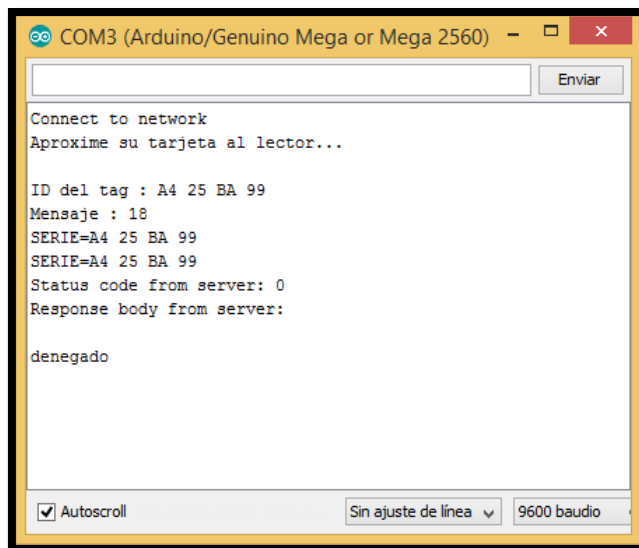


Figura 111: Lectura de tarjeta no registrada.

Fuente: IDE Arduino.

En este caso si se desea registrar al usuario con esa tarjeta, se debe acceder a la página web e ingresar los datos pertinentes y en la opción de selección de tag se puede visualizar la última lectura realizada, que este caso será la del usuario no registrado. La Figura 112 a continuación muestra el código de la tarjeta electrónica no registrada en la página web:



Figura 112: Obtención del código RFID de la última lectura a través de la página web

Fuente: Página Web del sistema.

Una vez que se haya seleccionado el código, se procede a ingresar los datos del usuario como indica la Figura 113:

The screenshot shows a web form for user registration. At the top center is the logo of the Universidad Técnica del Norte (UTN). Below the logo, the text reads "Sistema de Control de Acceso - UTN" and "Registro de Usuarios". The form includes a "Seleccione el tag:" label and a dropdown menu with the value "A4 25 BA 99". Under the heading "Información del Usuarios", there are several input fields: "Nombres y Apellidos" (filled with "María Lorena Varela Flores"), "Correo Electrónico" (filled with "mlvarela@utn.edu.ec"), "Clave" (filled with "5678"), "Cédula" (filled with "1002223334"), and "Rol" (filled with "Docente"). At the bottom of the form, there is a blue "Registrar" button and a purple "salir" link.

Figura 113: Ingreso de datos de usuario a través de página web.

Fuente: Página Web del sistema.

Si el registro se realizó adecuadamente, se mostrará un mensaje de registro completo, como se observa en la Figura 114:



Figura 114: Mensaje de registro completo.

Fuente: Página Web del sistema.

Se puede verificar ingresando a phpMyAdmin que los datos fueron almacenados correctamente en la base, como se observa en la Figura 115:

Mostrando filas 0 - 1 (total de 2. La consulta tardó 0.0009 segundos.)

`SELECT * FROM 'usuarios'`

[Editar en línea] [Editar] [Explicar SQL] [Crear código PHP] [Actualizar]

Mostrar todo | Número de filas: 25 | Filtrar filas: Buscar en esta tabla

Ordenar según la clave: Ninguna

+ Opciones

	id	nombre	correo	tag	clave	cedula	rol
<input type="checkbox"/>	6	Emerson Gabriel Haro Flores	emersonhf_09@hotmail.com	A0 F4 DD 10	1234	1003292826	Estudiante
<input type="checkbox"/>	9	Maria Lorena Varela Flores	mlvarela@utn.edu.ec	A4 25 BA 99	5678	1002223334	Docente

Seleccionar todo | Para los elementos que están marcados: Editar Copiar Borrar Exportar

Figura 115: Datos de usuario almacenados en la base.

Fuente: phpMyAdmin.

Finalmente se puede constatar que el usuario ha sido agregado a la base de datos y de esta forma se permitirá el acceso. La Figura 116 muestra el mensaje de lectura del tag, luego de haber sido registrado:

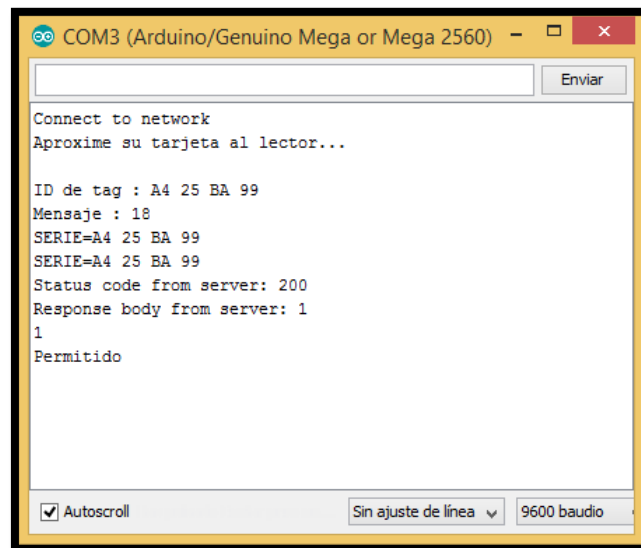


Figura 116: Lectura de tarjeta registrada:

Fuente: IDE Arduino.

4.2.3. Monitoreo de registros

Una opción importante que posee el sistema es la de monitorizar los registros que se vayan generando, con el fin de conocer los usuarios que acceden al servicio, además de registrar su hora y fecha de ingreso. La Figura 117 a continuación muestra la tabla de monitoreo de registros:



ID	Usuario	Hora	Fecha
21	Emerson Gabiel Haro Flores	01:27:52	2016-07-13
24	Emerson Gabiel Haro Flores	01:32:30	2016-07-13
25	María Lorena Varela Flores	01:46:43	2016-07-13
26	Emerson Gabiel Haro Flores	01:47:59	2016-07-13
27	María Lorena Varela Flores	01:48:38	2016-07-13

Figura 117: Monitoreo de registros.

Fuente: Página Web del sistema.

4.2.4. Registro de visitantes

En caso de que personas que no estén registradas como usuarios en el sistema deseen ingresar a la Universidad, el sistema cuenta con una opción de registro de visitantes, en la cual se ingresarán datos específicos de cada persona, y una vez terminado el registro se le asignará a cada una, un identificador que les permita el acceso de forma controlada. La Figura 118 muestra la interfaz gráfica para el registro de visitantes:




Sistema de Control de Acceso - UTN
Registro de Visitantes

Información de Visitantes

Nombres y Apellidos:

Cédula:

[Registrar](#)

[Monitorear Registro de Visitantes](#)

[Atrás](#)

[Salir](#)

Figura 118: Ingreso de datos de visitante.

Fuente: Página Web del sistema.

De esta forma el sistema permite llevar un control de todos los usuarios y personas que no estén registradas como tal, especificando la hora y fecha exacta de cada registro, como se observa en la Figura 119:




Monitoreo de Registro de Visitantes

2	Juan Carlos Castro Flores	1002345678	19:41:51	2016-11-13
---	---------------------------	------------	----------	------------

Figura 119: Monitoreo de registro de visitantes.

Fuente: Página Web del sistema.

4.3. ANÁLISIS ECONÓMICO

En referencia a los materiales utilizados para la elaboración del proyecto se analizará el costo de cada uno de ellos, con respecto al hardware, software y demás elementos utilizados.

4.3.1. Presupuesto de hardware utilizado

En referencia al presupuesto utilizado para la adquisición de materiales, dispositivos electrónicos y elaboración del prototipo de acuerdo al diseño establecido, se presentan los costos generales en la siguiente Tabla 17:

Tabla 17: Presupuesto de hardware utilizado.

Material	Costo Unitario	Cantidad	Total
Arduino Mega 2560	\$ 60,71	1	\$ 60,71
Arduino Ethernet Shield	\$ 25,00	1	\$ 25,00
Lector RFID RC522	\$ 42,86	1	\$ 42,86
LCD 16x2	\$ 5,09	1	\$ 5,09
Teclado Matricial 4x4 tipo membrana	\$ 5,80	1	\$ 5,80
Diodos Led	\$ 0,20	3	\$ 0,60
Relé de 5V	\$ 0,75	1	\$ 0,75
Transistor 2N3904	\$ 0,15	1	\$ 0,15
Buzzer miniatura	\$ 1,00	1	\$ 1,00
Resistencias	\$ 0,05	8	\$ 0,40
Potenciómetro	\$ 0,50	1	\$ 0,50
Capacitor 2200 μ F/25V	\$ 0,75	1	\$ 0,75
Capacitor 0.1 μ F	\$ 0,15	2	\$ 0,30
Reguladores de voltaje	\$ 1,00	2	\$ 2,00
Pulsadores	\$ 0,75	2	\$ 1,50
Diodos rectificadores 1N4001	\$ 0,15	8	\$ 1,20
Transformador de 12V	\$ 6,50	1	\$ 6,50
Bornera 3 terminales	\$ 0,30	2	\$ 0,60
Bornera 2 terminales	\$ 0,25	3	\$ 0,75
Batería 12V/4.5Ah	\$ 24,00	1	\$ 24,00
Cables para protoboard tipo bus de datos	\$ 4,50	1	\$ 4,50
Espadines macho	\$ 0,50	1	\$ 0,50
Espadines hembra	\$ 0,50	1	\$ 0,50
TOTAL			\$ 185,96

Fuente: ANEXO E. Proformas.

4.3.2. Presupuesto para elaboración de placas de circuito impreso

Los costos para la fabricación de las placas de circuito impreso se detallan a continuación en la

Tabla 18:

Tabla 18: Presupuesto para elaboración de placas de circuito impreso.

Material	Costo Unitario	Cantidad	Total
Baquelita de fibra (10x20)	\$ 2,20	1	\$ 2,20
Cloruro Férrico	\$ 0,80	1	\$ 0,80
Broca para baquelita	\$ 0,40	1	\$ 0,40
Cautín tipo lápiz	\$ 1,50	1	\$ 1,50
Pasta para soldar	\$ 1,25	1	\$ 1,25
Laminas termotransferibles	\$ 0,25	2	\$ 0,50
Impresión laser	\$ 0,25	2	\$ 0,50
TOTAL			\$ 7,15

Fuente: ANEXO E. Proformas.

4.3.3. Presupuesto para el montaje de circuitos

El montaje de los circuitos que conforman el sistema se realiza sobre una caja de material acrílico, misma que tiene un costo de adquisición y adecuación que se detalla en la Tabla 19:

Tabla 19: Presupuesto para montaje de los circuitos.

Descripción	Cantidad	Valor
Caja de montaje para proyectos	1	\$ 12,00
Placa de acrílico de 4x5cm	1	\$ 1,00
Placa de acrílico de 4x8cm	1	\$ 1,00
Cortes y perforaciones de la caja	1	\$ 1,00
Impresión de etiquetas y logo	1	\$ 1,00
Tornillos	10	\$ 0,20
TOTAL		\$ 16,20

Fuente: ANEXO E. Proformas.

4.3.4. Presupuesto para servidor y elementos de interconexión para la red

De acuerdo a las especificaciones antes realizadas de cada uno de los elementos de interconexión, en los que se incluía: el servidor, UPS y radios para enlace inalámbrico, se establecen costos referenciales a los mismos en la Tabla 20:

Tabla 20: Presupuesto para servidor y elementos de interconexión con la red.

Descripción	Cantidad	Valor	Total
Servidor para base de Datos	1	\$ 1189,99	\$ 1189,99
UPS 1KVA	1	\$ 219,99	\$ 219,99
Radios para enlace	3	\$ 244,99	\$ 734,97
TOTAL			\$ 2144,95

Fuente: ANEXO E. Proformas.

4.3.5. Mano de obra directa

La mano de obra directa es generada específicamente para la instalación de cada uno de los elementos del sistema de control de acceso, mismo que se especifican en la Tabla 21 a continuación:

Tabla 21: Costos de mano de obra.

Descripción	Cantidad	Valor	Total
Instalación del sistema electrónico y base de datos	5	\$ 500,00	\$2500,00
Instalación de enlaces inalámbricos	3	\$ 100,00	\$300,00
TOTAL			\$2800,00

Fuente: Anexo E. Proformas.

El valor total obtenido hace referencia al costo de mano de obra para la instalación de 5 controles de acceso.

4.3.6. Presupuesto de software utilizado

Los programas utilizados para la creación del código en el IDE de Arduino, así como también para la elaboración de la base de datos en MySQL, se encuentran bajo la arquitectura de Open Source y GNU/GPL respectivamente, es decir que operan bajo licencia libre que garantizan su uso.

En la Tabla 22 a continuación se detallan los costos generados por el software empleado:

Tabla 22: Presupuesto de software utilizado.

Descripción	Cantidad	Valor
IDE de Arduino	1	\$ 0
Apache v2.4.17	1	\$ 0
MySQL v5.0.11	1	\$ 0
PHP v5.6.21	1	\$ 0
TOTAL		\$ 0

Fuente: Costos del sistema.

4.3.7. Análisis económico

Para el análisis económico del sistema se deben considerar todos los costos empleados en la elaboración del mismo, como se detalla en la Tabla 23. Estos costos deben justificar el beneficio que conlleva la elaboración del proyecto hacia los usuarios.

Tabla 23: Costo total del sistema de control de acceso.

Descripción	Cantidad	Valor	Total
Hardware	5	\$ 185,96	\$929,80
Tags RFID	9000	\$ 1,00	\$ 9000,00
Software	1	\$ 0,00	\$0,00
Elaboración de placas	5	\$ 7,15	\$35,75
Montaje de circuitos	5	\$ 16,20	\$81,00
Servidor y elementos de interconexión	1	\$ 2144,95	\$ 2144,95
Mano de obra	1	\$2800,00	\$2800,00
TOTAL			\$14991,50

Fuente: ANEXO E. Proformas y costos del sistema.

De acuerdo al número de usuarios que tendrá el sistema se debe adquirir los tags adecuados para cada uno, para este caso se ha considerado 9000 usuarios.

Los beneficios que se obtienen al realizar el diseño de un sistema de control de acceso, es el permitir la regulación del ingreso de personas autorizadas al campus universitarios, esto con el fin de disminuir los robos que se producen dentro de la universidad por causa de personas ajenas a la misma que pueden ingresar fácilmente al campus. Entre otros aspectos también se puede considerar el hecho de tener un sistema flexible, el cual puede ser adaptado con el fin de mejorar sus prestaciones y funcionalidad, a un costo accesible.

Al realizar una comparación del sistema con otras marcas existentes en el mercado, se puede notar que su costo es más elevado, debido a que, muchos de los sistemas comerciales no poseen las características con las que cuenta el sistema de control de acceso, y que requiere la Universidad Técnica del Norte. Por ejemplo se puede citar al sistema Stand Alone que indica la Figura 120, el mismo que posee las siguientes características:



Figura 120: Control de acceso Stand Alone ASI-8910.

Fuente: PFC. Accesos automáticos del Ecuador. Recuperado de: <http://www.pfc.com.ec/lectoras-stand-alone.html>

- Acceso mediante tarjetas RFID y teclado
- Voltaje de operación de 9-15 VDC +/- 10%, 0.1A.

- Salida para chapa eléctrica o electromagnética 5A.
- Capacidad para 800 usuarios con tarjeta y 1 password
- Distancia de activación 5-15 cm
- Precio \$ 55.00

Otro sistema existente en el mercado es el ZK X7 ID que se observa en la Figura 121, el cual cuenta con las siguientes características:



Figura 121: Control de acceso ZK X7 ID.

Fuente: ZKSoftware. Recuperado de: http://www.zksoftware.com.ar/control_accesos_zk_x7_id.php

- Acceso mediante huella digital, lectura de tarjetas RFID y teclado
- Conexión de cerradura eléctrica, botón de salida, sensor de puerta, alarma y timbre
- Capacidad contraseña hasta 8 grupos
- Huellas 200
- Tarjetas 2000
- Precio \$ 129.00

Como se mencionó anteriormente los sistemas de control de acceso existentes en el mercado, no cumplen con las necesidades que demanda la Universidad, y una de ellas es el almacenamiento

de información de una gran cantidad de usuarios en una base de datos, característica que en los sistemas comerciales es limitada.

Es importante mencionar que, mediante el diseño del sistema de control de acceso se genera un sistema de seguridad y control mucho más robusto en la institución, de esta forma se desea garantizar el bienestar y la integridad de cada uno de los usuarios y personas en general que ingresan a diario a la Universidad Técnica del Norte.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

Una vez concluido la etapa de diseño y pruebas de funcionamiento, se procede a realizar las conclusiones y recomendaciones generadas a partir del desarrollo del proyecto.

5.1. CONCLUSIONES

- Se diseñó el sistema de control de acceso para la Universidad Técnica del Norte en base a la tecnología de identificación por radiofrecuencia, con el fin de tener un control adecuado en el ingreso, mediante el registro de usuarios, y la validación de un código único dentro de una tarjeta electrónica o una clave personal a través de comunicación TCP/IP con la información almacenada en una base de datos.
- El sistema de control de acceso permite llevar un control adecuado de las personas que ingresan a diario a la Universidad, generando una alternativa practica a los problemas relacionados con robos dentro de la institución, ya que no podrán ingresar personas ajenas a la misma, sin antes realizar un respectivo registro de entrada.
- Dentro de los principales aspectos a considerar en el diseño de un sistema de control de acceso se encuentran, el tipo de tecnología a utilizar y el número de usuarios que manejaran el mismo, es así que la Universidad Técnica del Norte al ser una institución que crece día a día y posee un alto índice de personas que transitan en el campus, requiere una gran cantidad de identificadores, y justamente una solución práctica a esto es el uso de tecnología de identificación por radiofrecuencia, que de acuerdo a estándares y

especificaciones internacionales se pueden llegar a obtener alrededor de 68 billones de códigos, haciendo de esta tecnología una de las más utilizadas y confiables.

- La tecnología que mejor se adapta para el desarrollo de un sistema de control de acceso para la Universidad Técnica del Norte, sin duda es la de un sistema basado en la tecnología RFID, siendo esta una de las más flexibles en cuanto a su funcionalidad a través del uso de librerías totalmente compatibles con placas de hardware libre, además de su costo y disponibilidad en el mercado. Permitiendo a los usuarios llevar el tag como un carnet de identificación para otro tipo de gestión dentro de la Universidad.
- El uso del gestor de base de datos MySQL facilita la administración de la información a través de una interfaz amigable para el usuario, además de generar respuestas rápidas ante peticiones de los usuarios con respecto a la lectura de los tags, con tiempo aproximado de procesamiento de 2 segundos.
- La instalación y uso de MySQL facilita la administración de una base de datos, pudiéndose constatar su funcionalidad en el manejo y respuesta de lectura de la información, además de su flexibilidad para adaptarse y operar junto con un sistema electrónico, y brindar facilidad de gestión y soporte multiplataforma.
- Arduino como herramienta de hardware libre se ha convertido en una plataforma muy amplia y flexible, que permite a los usuarios desarrollar proyectos de control y automatización electrónica a través del uso de distintos dispositivos y módulos, los cuales se adaptan a la aplicación que se quiera dar, tal es el caso del sistema de control de acceso, en el cual se vio que no existió ningún tipo de problema referente a incompatibilidad o mal funcionamiento del mismo, con el módulo RFID y el modulo Ethernet.

- El sistema de control de acceso al utilizar un módulo Ethernet requiere de conexión a la red a través de un medio de comunicación idóneo que permita la conexión con la base de datos, se estableció que el medio adecuado para esto es un medio inalámbrico de radioenlace, ya que por las características que presentan los sitios donde se requiere la instalación del mismo, hace difícil la conexión a través de un medio cableado, ya que sobrepasa los 90 metros que establecen las normas para tener una comunicación fiables sin pérdida de información.
- Las pruebas de funcionamiento del sistema se basaron principalmente en la interoperabilidad del sistema electrónico con la base de datos, por lo que fue necesario realizar pruebas en distintas fases, las cuales fueron enfocadas en la funcionalidad del módulo Ethernet que permite la conexión con la base de datos a través de comunicación TCP/IP, y la del lector RFID mediante la lectura del código del tag y su validación con la base de datos, al igual que en el ingreso de la clave mediante el teclado.
- Los costos generados para la elaboración del proyecto respaldan su operatividad, ya que se tiene un sistema adaptado a la necesidad y requerimientos de la Universidad Técnica del Norte, teniendo como fin el brindar garantías de seguridad a los usuarios, a través del control y registro de los mismos.

5.2. RECOMENDACIONES

- El sistema de control de acceso diseñado cuenta con módulos y dispositivos que operan bajo un rango de voltaje específico, por tal motivo es recomendable utilizar dispositivos reguladores de voltaje que permitan estabilizar la alimentación a los circuitos y así poder evitar posibles fallas futuras.
- La elección de la tecnología de identificación por radiofrecuencia debe estar enmarcada de acuerdo al tipo de aplicación que se vaya a dar y al área donde se va a desarrollar la misma, con el fin de tener un sistema que cumpla adecuadamente con sus funciones.
- Es recomendable revisar las hojas de datos de cada dispositivo o módulo a utilizar, esto con el fin de conocer características técnicas importantes que se deben considerar al momento de realizar su diseño y conexión con los demás elementos.
- Al elegir un tipo específico de placa Arduino, se debe tener clara la funcionalidad del proyecto para cubrir todos los requerimientos que demande el mismo, así como también posibles modificaciones futuras, en las que se requiera agregar algún otro dispositivo, y así evitar conflictos de funcionamiento.
- Es recomendable comprobar el funcionamiento por separado de cada elemento y dispositivo que forme parte de un sistema, de esta forma se garantiza su funcionalidad al momento de conectarse con los demás dispositivos.
- Se recomienda generar distintas tablas para almacenar información de los usuarios, de esta forma se tiene una base ordenada que permita realizar una gestión y manejo de datos adecuada para cualquier administrador.

- Al momento de realizar las pruebas de funcionamiento del sistema es recomendable verificar los niveles de voltaje que entrega la fuente de poder a todos los dispositivos, además de visualizar si su conexión se encuentra de acuerdo al diseño establecido.
- Los sistemas de control de acceso tanto de la entrada norte como sur, pueden ser conectados al mismo medio de comunicación inalámbrica a la que están conectados los controles de acceso vehicular, con el fin de aprovechar estos recursos, ya que el flujo de información que maneja el sistema de control de acceso es de un tamaño bajo, no colapsará el medio de comunicación en caso de conectarse a él.
- El tiempo de duración de un tag pasivo es ilimitado, por lo que un usuario puede tener el dispositivo durante todo el tiempo de estadía del mismo en la Universidad, o hasta culminar la carrera en caso de los estudiantes, esto con el fin de aprovechar al máximo este recurso y no modificar tan a menudo la información en la base de datos. sin embargo se pueden dar casos especiales en los que el tag se pierda o se vea deteriorado, en estos casos las autoridades deberían proveer un nuevo identificador y por ende un nuevo registro de información.
- Para el registro de las personas que ingresen como visitantes y no posean el identificador, el sistema debe estar respaldado con el personal de seguridad, el cual se encargará de realizar los registros como visitantes y de proveer el acceso provisional a las personas que lo requieran.

BIBLIOGRAFÍA

Forouzan, B. (2002). *Transmisión de Datos y redes de comunicación*. Madrid: McGraw-Hill.

Gidekel, A. (2008). *Introducción a la Identificación por Radio Frecuencia*. Electrónica Codificación S.A.

AETIC. (2009). *La tecnología RFID: Usos y Oportunidades*. Madrid: red.es.

Aranda, D. (2014). *Electrónica – Plataformas Arduino y Raspberry PI*. Buenos Aires: Fox Andina.

Aristizabal Gómez, A. (11 de Noviembre de 2010). *Electrónica Actual*.

Berni Millet , P., & Gil de la Iglesia, D. (2010). *Laboratorio de PHP y MySQL*. Catalunya: Eureka Media, SL.

Boxall, J. (2013). *Arduino Workshop A Hands-On Introduction*.

Boylestad, R. L., & Nashelsky, L. (2009). *Electrónica: Teoría de Circuitos y dispositivos Electrónicos*. México: PEARSON.

Cisco Systems, I. (2013). *Cisco*.

D'Addario, M. (2015). *Manual de Electrónica*. Autor-Editor.

Floyd, T. (2008). *Dispositivos Electrónicos*. México: PEARSON EDUCACIÓN.

Godínez, L. M. (2008). *RFID Oportunidades y riesgos, su aplicación práctica*. Barcelona: Alfaomega.

- Gómez Vieites, Á., & Otero Barros, C. (2011). *Redes de Ordenadores e Internet*. Madrid: Ra-Ma.
- Hueso Ibañez, L. (2012). *Bases de Datos*. Madrid: Ra-Ma.
- Ortiz , E., Ibarra , M., Andrade , J., & Almanza , D. (2012). Control de acceso usando FPGA y RFID. 8.
- Portillo, J., Bermejo, A., Bernardos, A., & Martínez, I. (2008). *Tecnología de identificación por radio frecuencia (RFID): aplicaciones en el ámbito de la salud*. Madrid: Fundación madrid para el Conocimiento Velázquez, 76. E-28001 Madrid.
- Ramos Álvarez, M. (2012). *Principios de Electrónica*. México: Red Tercer Milenio.
- Ricardo, K. M. (2009). *Base de Datos*. México: McGraw-Hill.
- Stallings, W. (2004). *Comunicaciones y Redes de Computadoras*. Pearson .
- Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras*. México: Pearson.

LINKOGRAFÍA

AIAG. (2016). *Automotive Industry Action Group*. Obtenido de Automotive Industry Action

Group: <http://www.aiag.org/>

AKROCARD. (2016). *AKROCARD*. Obtenido de <http://akrocard.com/>

American National Standards Institute. (2015). *ANSI*. Obtenido de <http://www.ansi.org>

Aprenderaprogramar. (2016). *Aprenderaprogramar.com*. Obtenido de [Aprenderaprogramar.com](http://aprenderaprogramar.com):

<http://aprenderaprogramar.com/>

Arduino. (30 de Noviembre de 2015). *arduino.cc*. Obtenido de <https://www.arduino.cc>

Casillas Santillán, L., Ginestà, M., & Pérez Mora, Ó. (s.f). *Base de Datos en MySQL*. Obtenido

de uoc.edu: http://ocw.uoc.edu/computer-science-technology-and-multimedia/bases-de-datos/bases-de-datos/P06_M2109_02151.pdf

Castillo, J. (5 de Julio de 2012). *SlideShare*. Obtenido de Relés y Contactores:

<http://es.slideshare.net/Jomicast/rels-y-contactores>

Cerf, V., Clark , D., Kahn , R., Kleinrock, L., Lynch, D., Postel , J., . . . Wolff, S. (2016).

Internet Society. Obtenido de <http://www.internetsociety.org/>

ETSI. (2015). *European Telecommunications Standards Institute-ETSI*. Obtenido de

<http://www.etsi.org/about>

Gerometta, O. (20 de junio de 2007). *Mis Libros de Networking*. Obtenido de

<http://librosnetworking.blogspot.com/>

Hacedores Maker Community. (2016). Obtenido de <http://hacedores.com/>

HADA. (2016). *Hada Electronics* . Obtenido de

<http://www.hadaelectronics.com/Tutoriales/?tutorial=4>

Hernandez Ovando, O. (Septiembre de 2012). *Configuración en base común*. Obtenido de

SlideShare: <http://www.slideshare.net/OthonielHernandezOvando/33-configuracin-en-base-comn>

ISO. (2015). *International Standard Organization-ISO*. Obtenido de

<http://www.iso.org/iso/home/search.htm?qt=rfid&sort=rel&type=simple&published=on>

Kits-Electrónica. (2016). *Kits de Electrónica y Circuitos*. Obtenido de

<http://www.kitelectronica.com>

Letrán, J. (2011). *cortoc.com*. Obtenido de <http://www.cortoc.com/2011/12/introduccion-arduino.html>

Martínez, S. (23 de Marzo de 2014). *es.slideshare.net*. Obtenido de

<http://es.slideshare.net/witwicky/tipos-de-arduino-y-sus-caracteristicas>

Melgoza, J. (2013). *Jonathanmelgoza*. Obtenido de <http://jonathanmelgoza.com/>

ML Consultores. (2016). *ML Consultores Soluciones Informáticas Integrales*. Obtenido de

<https://www.mlconsultores.com/>

ORACLE. (2016). *ORACLE*. Obtenido de <https://www.oracle.com>

Ortiga, A. (25 de Octubre de 2014). *SlideShare*. Obtenido de Transistor BJT y FET:

<http://es.slideshare.net/ooortigaaa/transistor-bjt-y-fet-uni>

Pillo, D. (9 de Enero de 2013). *Repositorio Digital - Universidad Técnica del Norte*. Obtenido de <http://repositorio.utn.edu.ec/handle/123456789/999>

PROMETEC. (2016). *PROMETEC*. Obtenido de <http://www.prometec.net>

Raspberry-Pi-Shop. (2016). *Raspberry Pi en Español*. Obtenido de <http://www.raspberrypi-shop.es/>

Robo-Help. (2005). *Automatización y Electrónica*. Obtenido de

http://robohelpnews.blogspot.com/2015_07_01_archive.html

Villegas, J. (2015). *Tecnoseguro.com*. Obtenido de [Tecnoseguro.com](http://www.tecnoseguro.com):

<http://www.tecnoseguro.com/faqs/control-de-acceso/%C2%BF-que-es-un-control-de-acceso.html>

GLOSARIO DE TÉRMINOS

RFID: Siglas de Radio Frequency Identification. Es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags.

Tag: Un Tag es una tarjeta electrónica compuesta por un chip y una antena que almacena información de identificación.

ADC: Siglas de Analog Digital Converter. Conversor de señales analógicas a digitales.

ROM: Read Only Memory, Tipo de memoria de solo lectura.

PVC: Policloruro de vinilo, Plástico que surge a partir de la polimerización del cloroetileno.

PET: Polietileno Tereftalato, Plástico utilizado en la fabricación de envases y textiles.

EEPROM: Electrically Erasable Programmable Read-Only Memory, Memoria de solo lectura programable y borrrable eléctricamente.

ISM: Industrial, Scientific and Medical, Bandas no comerciales de frecuencia reservadas para desarrollo industrial, científico y médico.

AIAG: Automotive Industry Action Group. Organización a escala mundial que sirve de foro abierto para que empresas de todo el mundo desarrollen y compartan información que contribuya con la industria automotriz.

ANSI: American National Standards Institute. Instituto Nacional de Estándares Americanos.

RTLS: Sistemas de Localización en Tiempo Real.

EAN: European Article Numbering Association. Organismo internacional para el manejo de estándares internacionales para la identificación de productos.

UCC: Uniform Code Council. Código uniforme de comercio.

EPC: Electronic Product Code, Código de Producto Electrónico.

ISO: International Standard Organization. La Organización Internacional de Normalización es una organización para la creación de estándares internacionales de calidad.

ETSI: European Telecommunications Standards Institute. Instituto de Telecomunicaciones de estándares Europeos.

TIC: Término para referirse a las Tecnologías de Información y Comunicación.

IDE: Integrated Development Environment, Ambiente de Desarrollo Integrado.

JAVA: Lenguaje de Programación de propósito general.

USB: Universal Serial Bus. Puerto que permite conectar periféricos a una computadora.

PWM: Pulse Width Modulation, Modulación por Ancho de Pulsos, es una técnica en la que se modifica el ciclo de trabajo de una señal periódica.

UART: Universal Asynchronous Receiver-Transmitter, Transmisor-Receptor Asíncrono Universal.

ARPANET: Advanced Research Projects Agency Network, Red de la Agencia de Proyectos de Investigación Avanzada.

LAN: Local Area Network, Red de Área Local.

WAN: Wide Area Network, Red de Área Amplia.

ATM: Asynchronous Transfer Mode, Modo de Transferencia Asíncrona, es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

ARP: Address Resolution Protocol, Protocolo de Resolución de Direcciones.

RARP: Reverse Address Resolution Protocol, Protocolo de Resolución de Direcciones Inversa.

IP: Internet Protocol, Protocolo de Internet, se trata de un estándar que se emplea para el envío y recepción de información.

ICMP: Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet.

TELNET: Telecommunication Network, Protocolo de conexión remota.

FTP: File Transfer Protocol, Protocolo de Transferencia de archivos.

SMTP: Simple Mail Transfer Protocol, Protocolo sencillo de transferencia de correo electrónico.

SNMP: Simple Network Management Protocol, Protocolo sencillo de gestión de redes.

HTTP: Hypertext Transfer Protocol, Protocolo para la transferencia de hipertextos.

ANSI-SPARC: American National Standard Institute – Standards Planning and Requirements Committee. Es un estándar de diseño abstracto para un sistema de gestión de bases de datos.

GPL: General Public License, Licencia General Pública utilizada en el mundo del software y garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software.

SPI: Serial Peripheral Interface. Estándar de comunicación para controlar dispositivos electrónicos digitales que acepten un flujo de bits serie, a través de comunicación sincrónica.

ALOHA: Es un protocolo del nivel de enlace de datos para el control de acceso al medio.

LCD: Siglas de Liquid Crystal Display. Pantalla de cristal líquido que permite visualizar caracteres alfanuméricos.

TCP/IP: Siglas de Transmission Control Protocol/Internet Protocol o Protocolo de Control de Transmisión/Protocolo de Internet. Es un conjunto de protocolos de red en los que se basa Internet y que permite la transmisión de información entre computadoras.

MySQL: Es un sistema o aplicación que permite gestionar archivos llamados bases de datos, basado en un lenguaje de consulta estructurado.

PHP: Hypertext Preprocessor. Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

VLAN: Red de área local virtual. Es un método para crear redes lógicas independientes dentro de una misma red física.

ANEXOS

ANEXO A. CÓDIGO DE PROGRAMACIÓN DEL SISTEMA DE CONTROL DE ACCESO.

Sección 1. Declaración de Librerías

```
#include <Ethernet.h> // Librería Ethernet
#include "RestClient.h" // Librería Ethernet RestClient
#include <stdlib.h> // Librería
#include <SPI.h> // Librería Cx.SPI
#include <MFRC522.h> // Librería Módulo RFID RC522
#include <LiquidCrystal.h> // Librería LCD 16x2
#include <Keypad.h> // Librería teclado matricial 4x4
```

Sección 2. Declaración de variables, definición de terminales de conexión e inicialización de módulos

```
#define SS_PIN 53 // Definición de pin 53 - SS para módulo RFID
#define RST_PIN 5 // Definición de pin 5 - Reset para módulo RFID
MFRC522 mfrc522(SS_PIN, RST_PIN); // Definición de terminales para módulo RFID
LiquidCrystal lcd(36, 35, 34, 33, 32, 31); // Declaración de terminales de conexión para LCD
byte mac[] = { 0x90, 0xA2, 0xDA, 0x0D, 0xF6, 0xF0 }; // Asignación de MAC para módulo Ethernet
byte ip[] = { 172, 16, 1, 211 }; // Asignación de IP para módulo Ethernet
RestClient client = RestClient("172.16.1.210"); // Asignación de IP para cliente
String temp; // Variable tipo String para almacenamiento temporal
String SERIE = "Arduino1"; // Variable tipo String para reconocer el número de placa
int i=0,j=0,f=0,w=0,k=0; // Variables tipo entero para botón
char pss2[10]; // Variable tipo Char para almacenamiento de la clave por teclado
const byte filas=4; // Definición de constantes para filas
const byte columnas=4; // Definición de constantes para columnas
byte pinsFilas[filas]= { 22, 23, 24, 25 }; // Terminales de conexión para filas
byte pinsColumnas[columnas]={ 26, 27, 28, 29 }; // Terminales de conexión para columnas
String response; // Variable tipo String para respuesta
char teclas[filas][columnas]={ // Declaración de matriz para teclado
  {'5', '4', 'B', '6'},
  {'2', '1', 'A', '3'},
  {'0', '6', 'D', '#'},
  {'8', '7', 'C', '9'}
};
Keypad teclado= Keypad(makeKeymap(teclas),pinsFilas,pinsColumnas,filas,columnas); // Creación de instancia para teclado

char tecla; // Variable tipo Char
int led_acceso = 40; // Led indicador de acceso
int led_negado = 41; // Led indicador de negación
```

```

int rele = 45; // Salida para activar relé
int bocina = 39; // Salida para activar bocina
int frecuencia = 440; // Asignación de valor de frecuencia
int estadoBotonAnterior; // Variable de almacenamiento de estado anterior dl botón
para el teclado
int estadoBoton; // Variable de almacenamiento del estado del botón para
el teclado
const int Boton =37; // Botón de teclado conectado al terminal
int boton; // Variable botón
const int botonCtrl=38; // Botón de control conectado al pin 38
const int tiempoAntireboteCtrl=2; // Declaración de constante de tiempo anti rebote para
botón de control
int cuenta =0; //Guarda el número de veces que el botón de control ha
sido presionado
int estadoBotonCtrl; // Variable para el estado del botón de control
int estadoBotonAnteriorCtrl; // Variable para el estado anterior del botón de control
char st[20];

```

Sección 3. Función antirebote para cambio de estado

```

boolean antireboteCtrl (int pin ) { // Función anti rebote
int contadorCtrl =0; // Contador inicializado en 0
boolean estadoCtrl; // Guarda el estado del botón
boolean estadoAnteriorCtrl; // Guarda el último estado del botón

do {
estadoCtrl = digitalRead (pin);
if (estadoCtrl != estadoAnteriorCtrl ){ // Comparación del estado actual
contadorCtrl = 0; // Reinicio del contador
estadoAnteriorCtrl = estadoCtrl; // Se almacena el estado del botón
}
else{
contadorCtrl = contadorCtrl +1; // Aumento del contador en 1
}
delay (1); // Retardo de 1 milisegundo
}
while (contadorCtrl < tiempoAntireboteCtrl); //Bucle de comparación para el contador
return estadoCtrl;
}

void setup (){
pinMode(led_acceso, OUTPUT); // Declaración de pin led_acceso como salida
pinMode(led_negado, OUTPUT); // Declaración de led_negado como salida
pinMode(rele, OUTPUT); // Declaración pin relé como salida
Serial.begin(9600); // Inicio de Cx. Serial
pinMode(botonCtrl,INPUT); // Declaración de botón de control como entrada
lcd.begin(16,2); // Inicio de LCD 16x2
SPI.begin(); // Inicio de Cx. SPI
Ethernet.begin(mac,ip); // Inicio de Cx. Ethernet
Serial.begin(9600);
Serial.println("Connect to network"); // Mensaje serial de conexión a la red
mfr522.PCD_Init(); // Inicio de módulo RFID RC522

```

```

Serial.println("Aproxime su tarjeta al lector..."); // Mensaje serial de inicio de lectura
Serial.println(); // Mensaje en blanco para espacio
lcd.setCursor(0,0); // Inicio del cursor para LCD
lcd.print(" Bienvenido "); // Mensaje de bienvenida en la LCD
}

```

Sección 4. Función reporte para conexión con script PHP a través del módulo Ethernet

```

void reporte (){
char otro [temp.length()]; // Variable tipo char para almacenar la longitud de una
cadena
Serial.println (temp.length()); // Imprimir la longitud de la cadena
temp.toCharArray(otro, temp.length()); // Copia caracteres de la cadena en la variable de
almacenamiento
Serial.println (otro); // Imprimir la variable de almacenamiento
const char* body= otro; // Definición de variable no modificable (solo lectura)
Serial.println (body); // Imprimir variable
response = "";
int statusCode = client.post("/control.acceso/reportes.php", body, &response); // Variable para conexión
con script php
Serial.print("Status code from server: "); // Mensaje serial para estado del código del servidor
Serial.println(statusCode); // Imprimir estado de código
Serial.print("Response body from server: "); // Mensaje serial para respuesta desde el servidor
Serial.println(response); // Imprimir respuesta desde el servidor
delay(1000); // Retardo de un segundo
return; // Retorno
}

```

Sección 5. Cambio de estado del sistema

```

void loop () {
estadoBotonCtrl =digitalRead (botonCtrl); // Lectura del estado del botón de control
if (estadoBotonCtrl != estadoBotonAnteriorCtrl) { // Verificación de cambio con respeto al estado
if (antireboteCtrl (botonCtrl)){ // Se verifica si el pulsador está presionado y si lo esta
cuenta++; //La cuenta se incrementa en uno
Serial.println (cuenta); // Imprimir mensaje serial con el valor de la variable
cuenta
}
if (cuenta == 1) // Si el valor de cuenta es 1
{
digitalWrite(rele,HIGH); // Se activa el terminal designado para el relé
lcd.clear(); // Limpieza de la LCD
lcd.setCursor(0,0); // Posicionamiento del cursor en la LCD
lcd.print("Acceso Abierto"); // Imprimir mensaje en la LCD
}
if (cuenta == 2) // Si el valor de cuenta es 2
{
digitalWrite(rele,LOW); // Se desactiva el terminal designado para el relé
lcd.clear(); // Limpieza de la LCD
lcd.setCursor(0,0); // Posicionamiento del cursor en la LCD
lcd.print("Acceso Bloqueado"); // Imprimir mensaje en la LCD
}
}
}

```

```

}
if (cuenta == 3){ // Si el valor de cuenta es 3
  cuenta==0; // Variable cuenta vuelve a 0
  lcd.clear(); // Limpieza de la LCD
  lcd.setCursor(0,0); // Posicionamiento del cursor en la LCD
  lcd.print(" Bienvenido "); // Imprimir mensaje en la LCD
}
estadoBotonAnteriorCtrl = estadoBotonCtrl; // Se guarda el estado del botón

```

Sección 6. Ingreso de clave por teclado.

```

while(true){
  if (cuenta==0){ // Si el valor de cuenta es 0
    estadoBoton=digitalRead(Boton); //Lectura del estado del botón
    if(estadoBoton != estadoBotonAnterior){ // Verificación de cambio con respecto al estado
      if(antirrebote(Boton)){
        delay(50); // Retardo de 50 milisegundos
        lcd.clear(); // Limpieza de la LCD
        lcd.setCursor(0,0); // Posicionamiento del cursor de la LCD
        lcd.print("Ingrese Clave"); // Mensaje de ingreso de clave en la LCD
        lcd.setCursor(6,1); // Posicionamiento del cursor de la LCD
        for(j=0;(j<=3);j++){ // Bucle para ingreso de contraseña
          pss2[j]=teclado.waitForKey(); // Asignación de la función de espera para ingreso de
          clave
          lcd.print("*"); // Imprimir el símbolo "*" en la LCD
          pss2[j]='\0'; // Vector para almacenar clave
          delay(50); // Retardo 50 milisegundos
          // Verificación de los caracteres correctos
          w=0; // Variable inicializada en 0
          String s=pss2; // Variable tipo string para la clave
          lcd.clear(); // Limpieza de la LCD
          temp = "PASS=" + s + "&"; // Variable para almacenar la clave ingresada
          reporte(); // Llamado a método reporte
          Serial.println(response); // Imprimir respuesta desde el servidor
          if((response=="1") && ((cuenta==0)||(cuenta==3))){ // Verificación de respuesta y estados
            lcd.clear(); // Limpieza de la LCD
            lcd.setCursor(0,0); // Posicionamiento del cursor de LCD
            lcd.print("Permitido"); // Imprimir mensaje en la LCD
            digitalWrite(rele,HIGH); // Se activa el terminal designado para el relé
            tone(bocina,frecuencia); // Inicio de alerta
            delay(2000); // Retardo de 2 segundos
            noTone(bocina); // Se detiene la alerta
            delay(1000);} // Retardo de 1 segundo

          else{
            lcd.clear(); // Limpieza de la LCD
            lcd.setCursor(0,0); // Posicionamiento del cursor de la LCD
            lcd.print("Denegado"); // Imprimir mensaje en la LCD
            digitalWrite(rele,LOW); // Se desactiva el terminal designado para el relé
            delay(2000);} // Retardo 2 segundos

```

```

}
}
}
estadoBotonAnterior = estadoBoton;           // Se guarda el estado del botón

```

Sección 7. Lectura de tags y obtención de ID.

```

if ( ! mfr522.PICC_IsNewCardPresent()){ // Detecta si hay una tarjeta, y si no lo hace vuelve a
intentar
return;}
if ( ! mfr522.PICC_ReadCardSerial()){ // Lee la tarjeta, y si no lo hace vuelve a intentar
return;}
Serial.print("ID de tag :"); // Mensaje serial para el ID del tag
String contenido= ""; // Variable tipo string para contenido
byte letra;
for (byte i = 0; i < mfr522.uid.size; i++) // Bucle para verificar tamaño del código de la tarjeta
{
Serial.print(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " "); // Mensaje serial de código de la tarjeta
Serial.print(mfr522.uid.uidByte[i], HEX); // Mensaje serial hexadecimal de código de la tarjeta
contenido.concat(String(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " ")); // Concatenación de parámetros
contenido.concat(String(mfr522.uid.uidByte[i], HEX)); // Concatenación de parámetros hexadecimal
}
Serial.println(); // Imprimir mensaje en blanco
Serial.print("Mensaje : "); // Imprimir mensaje serial
contenido.toUpperCase(); // Obtención de cadena en mayúsculas
if (contenido.substring(1) != "0"){ // Comparación de subcadena
temp = "SERIE=" + contenido.substring(1) + "&"; // Variable de almacenamiento de código
reporte(); // Método reporte
Serial.println(response); // Imprimir respuesta desde el servidor
if((response=="1")&& ((cuenta==0)||cuenta==3)){ // Verificación de respuesta y estados
Serial.println("Permitido"); // Imprimir mensaje serial
digitalWrite(rele,HIGH); // Se activa el terminal designado para el relé
lcd.clear(); // Limpieza de la LCD
lcd.setCursor(0,0); // Posicionamiento del cursor de la LCD
lcd.print("Permitido"); // Imprimir mensaje en la LCD
tone(bocina,frecuencia); // Inicio de alerta
delay(2000); // Retardo de 2 segundos
noTone(bocina); // Se detiene la alerta
delay(1000); // Retardo de 1 segundo
}
else{
Serial.println("Denegado"); // Imprimir mensaje serial
digitalWrite(rele,LOW); // Se desactiva el terminal designado para el relé
lcd.clear(); // Limpieza de la LCD
lcd.setCursor(0,0); // Posicionamiento del cursor de la LCD
lcd.print("Denegado"); // Imprimir mensaje en la LCD
delay(2000);} // Retardo 2 segundos
}
}
}
}

```

```
const int tiempoAntirebote=10; // Asignación de tiempo antirebote
boolean antirrebote(int pin) // Método antirebote
{
  int contador=0; // Inicio de contador
  boolean estado; // Variable de almacenamiento de estado del botón
  boolean estadoAnterior; // Variable de almacenamiento del último estado del
  botón
  do{
    estado=digitalRead(pin); // Lectura del estado del pin
    if(estado!=estadoAnterior){ // Verificación de cambio con respecto al estado
      contador=0; // Asignación de valor a contador
      estadoAnterior=estado; // Se guarda el estado del botón
    }
    else {
      contador++; // Incremento del contador
    }
    delay(1); // Retardo 1 milisegundo
  } while(contador<tiempoAntirebote); // Bucle comparativo entre contador y tiempo antirebote
  return estado; // Retorno de estado
}
```


ANEXO B. CÓDIGO PHP Y HTML

SCRIPT INDEX

```

<?php
session_start();
include_once "conexion1.php";
function verificar_login($user,$password,&$result) {
$sql = "SELECT * FROM login WHERE usuario = '$user' and password = '$password'";
$rec = mysql_query($sql);
$count = 0;
while($row = mysql_fetch_object($rec)) {
$count++;
$result = $row; }
if($count == 1) {
return 1; }
else {
return 0; }
}
if(!isset($_SESSION['userid'])) {
if(isset($_POST['login'])) {
if(verificar_login($_POST['user'],$_POST['password'],$result) == 1) {
$_SESSION['userid'] = $result->idusuario;
header("location:/control.acceso/index1.php"); }
else {
echo '<div class="error">Su usuario es incorrecto, intente nuevamente.</div>'; } }
?>
<style type="text/css">
*{
font-size: 14px; }
body{
background:#F0EAEA; }
form.login {
background: none repeat scroll 0 0 #F1F1F1;
border: 1px solid #DDDDDD;
font-family: sans-serif;
margin: 0 auto;
padding: 20px;
width: 278px;
box-shadow:0px 0px 20px black;
border-radius:10px; }
form.login div {
margin-bottom: 15px;
overflow: hidden; }
form.login div label {
display: block;
float: left;
line-height: 25px; }
form.login div input[type="text"], form.login div input[type="password"] {
border: 1px solid #DCDCDC;

```

```

float: right;
padding: 4px; }
form.login div input[type="submit"] {
background: none repeat scroll 0 0 #DEDEDE;
border: 1px solid #C6C6C6;
float: right;
font-weight: bold;
padding: 4px 20px; }
.error{
color: red;
font-weight: bold;
margin: 10px;
text-align: center; }
</style>
<form action="" method="post" class="login">
<div><center><IMG align=center SRC="logo.png"></center></div>
<div><label><center>ACCESO DE ADMINISTRACIÓN</center></label></div>
<div><label>Usuario:</label><input name="user" type="text" ></div>
<div><label>Contraseña:</label><input name="password" type="password"></div>
<div><input name="login" type="submit" value="login"></div>
</form>
<h3 ALIGN=center><a href="http://localhost/control.acceso">ATRÁS</a></h3>
<?php
} else {
echo 'Su usuario ingreso correctamente.';
echo '<a href="logout.php">Logout</a>'; }
?>

```

SCRIPT INDEX 1

```

<?php
$mysqli = new mysqli('localhost', 'root', 'root', 'tesis');
?>
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<link href = "file:///C:/xampp\htdocs\rfid.ico" type="image/x-icon" rel = "shorcut icon"/>
<title>Control de Acceso - UTN</title>
<link href="estilos.css" rel="stylesheet" type="text/css">
</head>
<body>
<div class="group">
<form action="registro.php" method="POST">
<center>
<IMG align=center SRC="utn.png">
</center>
<h2><em>Sistema de Control de Acceso - UTN</em></h2>
<h2><em>Registro de Usuarios</em></h2>
<p>Seleccione el tag:</p>
<p>Nombre:

```

```

<select type="text" name="actividad3">
<option value="0">Selección:</option>
<?php

$query = $mysqli -> query ("SELECT tag FROM noregistrados ORDER BY id DESC limit 1");
while ($valores = mysqli_fetch_array($query)) {
echo '<option value="'. $valores[tag]."'>'. $valores[tag]. '</option>'; }
?>
</select>
</p>
</p>
<div align="left">
<h3><em>Información del Usuarios</em></h3>
<label for="actividad1">Nombres y Apellidos: <span></span></label>
<input type="nombre" name="actividad1" class="form-input" required/>
<label for="actividad2">Correo Electrónico: <span></span></label>
<input type="email" name="actividad2" class="form-input" />
<label for="actividad4">Clave: <span></span></label>
<input type="text" name="actividad4" class="form-input" />
<label for="actividad5">Cédula: <span></span></label>
<input type="text" name="actividad5" class="form-input" />
<label for="actividad6">Rol: <span></span></label>
<input type="text" name="actividad6" class="form-input" />
<center> <input class="form-btn" name="submit" type="submit" value="Registrar" /></center>
</p>
</form>
</div>
<h3 ALIGN=center><a href="http://localhost/control.acceso">salir</a></h3>
</body>
</html>

```

SCRIPT INDEX 2

```

<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>Registros</title>
<link href="estilos.css" rel="stylesheet" type="text/css">
</head>
<body>
<div class="group">
<form action="" method="POST">
<center>
<IMG align=center SRC="utn.png">
</center>
<h2><em> Monitoreo de Registros</em></h2>
</form>
</div>
<center>
<?php

```

```

include("conexion.php");
$con = mysql_connect($host,$user,$pw);
mysql_select_db($db,$con);
$consulta=mysql_query("Select * from registros") or die (mysql_error());
$registro=mysql_fetch_array($consulta);
echo "<table border>";
do {
    $id=$registro['id'];
    $nombre=$registro['tag'];
    $hora=$registro['hora'];
    $fecha=$registro['fecha'];
    echo
    "<tr><td>".$registro["id"]."</td><td>".$registro["tag"]."</td><td>".$registro["hora"]."</td><td>".$re
    gistro["fecha"]."</td></tr> \n";
} while($registro=mysql_fetch_array($consulta));
echo "</table>";
?>
</center>
<h3 ALIGN=center><a href="http://localhost/control.acceso/index1.php">Ir a Inicio</a></h3>
<h3 ALIGN=center><a href="http://localhost/control.acceso">Salir</a></h3>
</body>
</html>

```

SCRIPT INDEX

```

<?php
$mysqli = new mysqli('localhost', 'root', 'root', 'tesis');
?>
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<link href = "file:\\C:\xampp\htdocs\rfid.ico" type="image/x-icon" rel = "shorcut icon"/>
<title>Control de Acceso - UTN</title>
<link href="estilos.css" rel="stylesheet" type="text/css">
</head>
<body>
<div class="group">
<form action="registro1.php" method="POST">
<center>
<IMG align=center SRC="utn.png">
</center>
<h2><em>Sistema de Control de Acceso - UTN</em></h2>
<h2><em>Registro de Visitantes</em></h2>
<div align="left">
<h3><em>Información de Visitantes</em></h3>
<label for="actividad1">Nombres y Apellidos: <span></span></label>
<input type="nombre" name="actividad1" class="form-input" required/>
<label for="actividad2">Cédula: <span></span></label>
<input type="text" name="actividad2" class="form-input" />
<center> <input class="form-btn" name="submit" type="submit" value="Registrar" /></center>

```

```

</p>
</form>
</div>
<h3 ALIGN=center><a href="http://localhost/control.acceso/index4.php">Monitorear Registro de
Visitantes</a></h3>
<h4 ALIGN=center><a href="http://localhost/control.acceso/index1.php">Atrás</a></h4>
<h4 ALIGN=center><a href="http://localhost/control.acceso">Salir</a></h4>
</body>
</html>

```

SCRIPT REGISTRO

```

<?php
$db_host="localhost";
$db_user="root";
$db_password="root";
$db_name="tesis";
$db_table_name="usuarios";
$db_connection = mysql_connect($db_host, $db_user, $db_password);
if (!$db_connection) {
die('No se ha podido conectar a la base de datos'); }
$subs_act1 = ($_POST['actividad1']);
$subs_act2 = ($_POST['actividad2']);
$subs_act3 = ($_POST['actividad3']);
$subs_act4 = ($_POST['actividad4']);
$subs_act5 = ($_POST['actividad5']);
$subs_act6 = ($_POST['actividad6']);
$resultado=mysql_query("SELECT * FROM ".$db_table_name." WHERE nombres =
'".$subs_act1."'",$db_connection);
if (mysql_num_rows($resultado)>0){
header('Location: Fail.html'); }
else {
$insert_value = 'INSERT INTO `'.$db_name.`.`'.$db_table_name.` (`nombre`, `correo`, `tag`,
`clave`, `cedula`, `rol`) VALUES ('.$subs_act1.', '$subs_act2.', '$subs_act3.', '$subs_act4.', '$subs_act5.', '$subs_act6.')';
mysql_select_db($db_name, $db_connection);
$retry_value = mysql_query($insert_value, $db_connection);
if (!$retry_value) {
die('Error: ' . mysql_error()); }
header('Location: SuccessActividades.html');
}
mysql_close($db_connection);
?>

```

SCRIPT REPORTE

```

<?php
include ("conexion.php");
if (isset($_POST['SERIE']) && !empty($_POST['SERIE'])){
$serie = $_POST["SERIE"];
$con = mysql_connect ($host, $user, $pw)

```

```

or die ("Pro_server");
mysql_select_db ($db,$con)
or die ("pro_select_db");
$query = mysql_query("Select * from usuarios Where tag='$serie'") or die ("error_en busqueda");
$stab = mysql_fetch_row($query);
$codigo= "".$stab[3]."";
$nombre= "".$stab[1]."";
if ($serie == $codigo){
echo "1";
mysql_query("INSERT INTO registros (tag,hora,fecha) VALUES
('$nombre',CURTIME(),CURDATE())") or die ("ID en uso");}
else {echo "0";
mysql_query("INSERT INTO noregistrados (tag) VALUES ('$serie')") or die ("ID en uso");}
}
else {
if (isset($_POST['PASS']) && !empty($_POST['PASS'])){
$pass = $_POST["PASS"];
$con = mysql_connect ($host, $user, $pw)
or die ("Pro_server");
mysql_select_db ($db,$con)
or die ("pro_select_db");
$query = mysql_query("Select * from usuarios Where clave='$pass'") or die ("error_en busqueda");
$stab = mysql_fetch_row($query);
$codigo= "".$stab[4]."";
$nombre= "".$stab[1]."";
if ($pass == $codigo){
echo "1";
mysql_query("INSERT INTO registros (tag,hora,fecha) VALUES
('$nombre',CURTIME(),CURDATE())") or die ("ID en uso");}
else {echo "0";}
}
else {echo "datosIncorrectos";}
}
?>

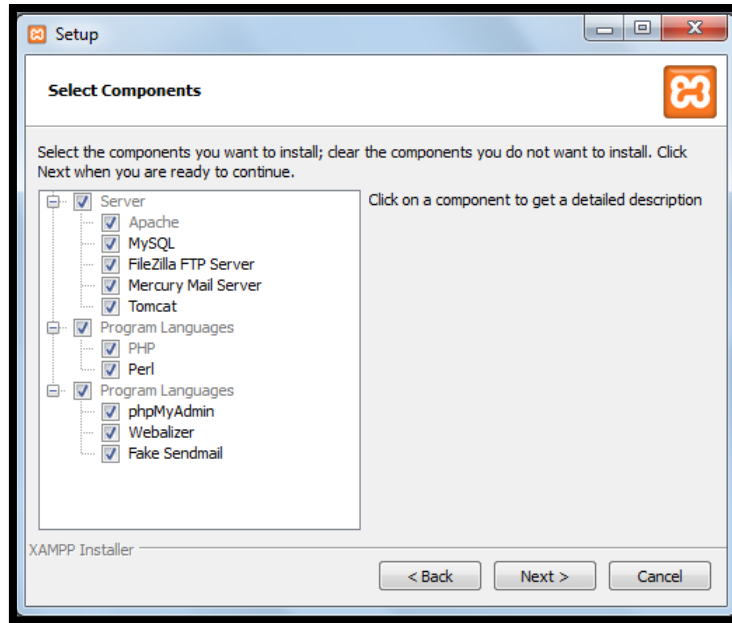
```

ANEXO C. INSTALACIÓN DE SERVIDOR XAMPP Y CREACIÓN DE BASE DE DATOS

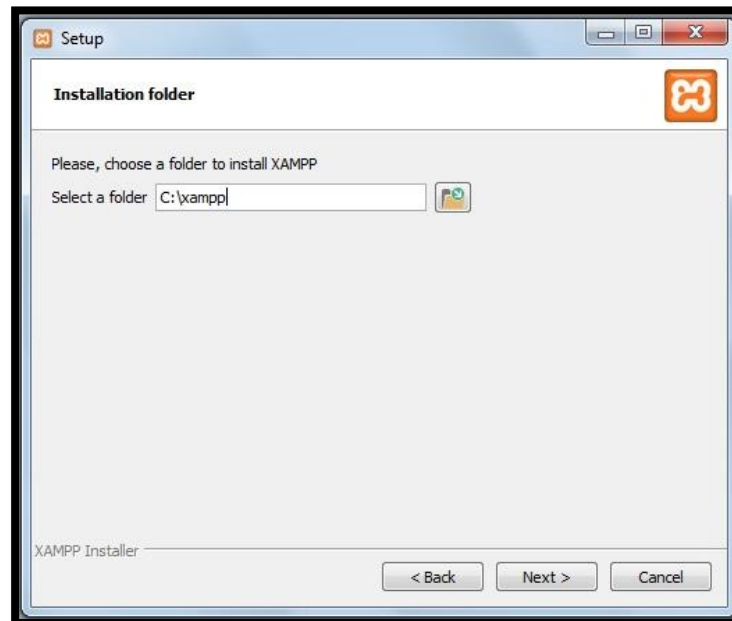
Después de ejecutar como administrador el archivo xampp-win32-5.6.21-0-VC11-installer se visualiza la pantalla de bienvenida al inicio de instalación, como se observa en la figura:



Se debe simplemente presionar el botón Next para continuar con la instalación. A continuación se muestra todos los componentes que trae consigo xampp y que se pueden o no instalar, según la necesidad del usuario.



Se presiona Next y se solicita la carpeta donde instalar la aplicación. Por defecto, la instalación se realiza en la carpeta C:\xampp.



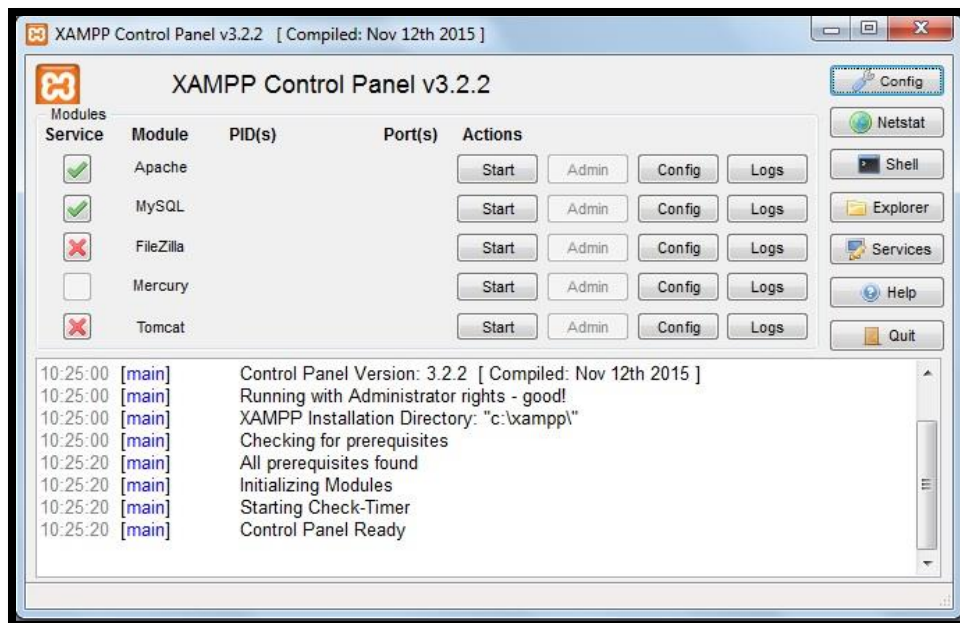
Luego de seleccionar la carpeta de instalación y presionar Next, los paquetes empezaran a instalarse.



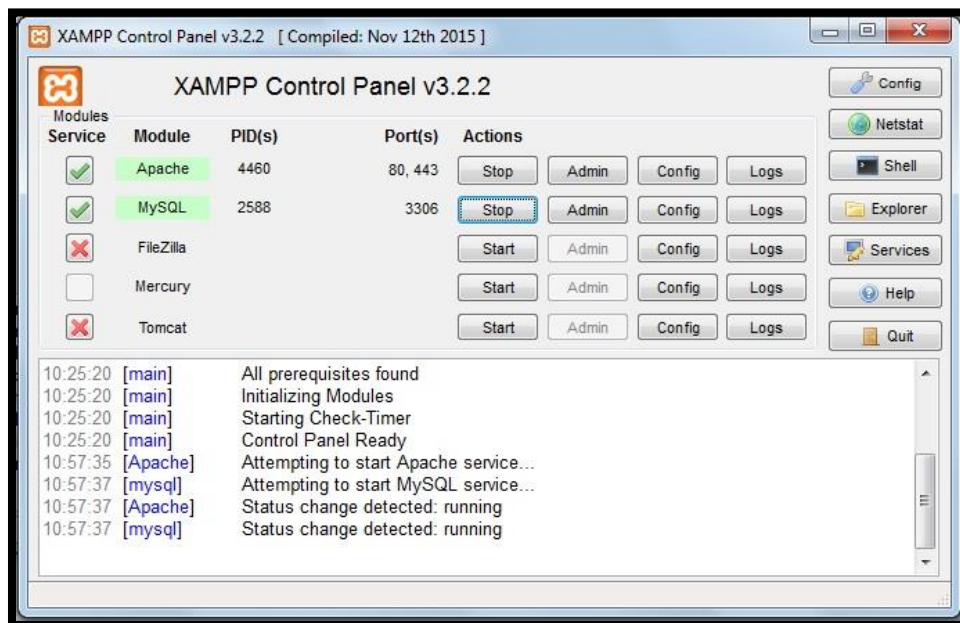
Una vez terminado el proceso de instalación de todos los paquetes que contiene xampp, la pantalla de instalación indica si se desea iniciar o no el panel de control.



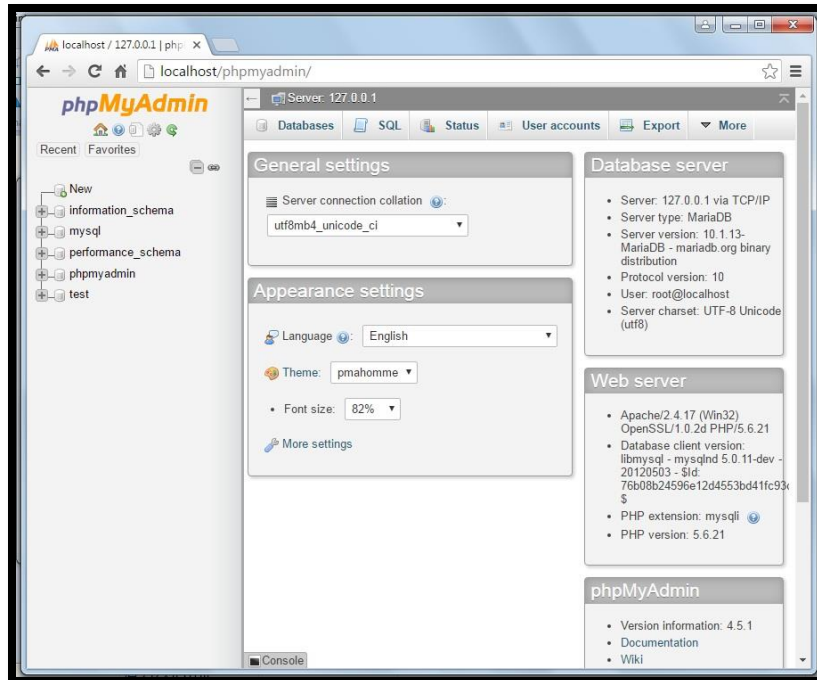
Para finalizar se presiona el botón Finish y se espera que arranque el programa y muestre el panel de control.



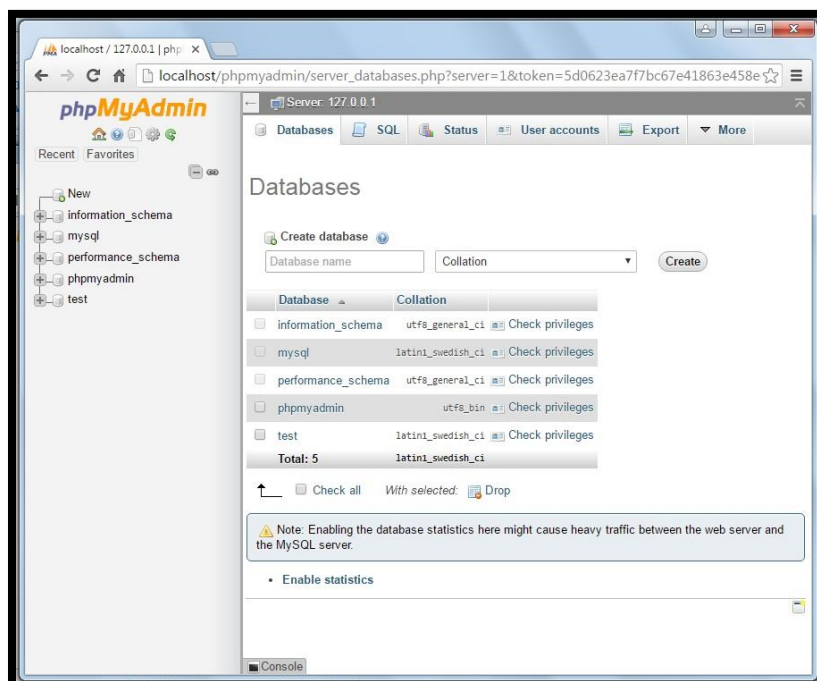
Para comprobar la funcionalidad de xampp se procede a crear una base de datos, para lo cual se debe iniciar los módulos Apache y MySQL.



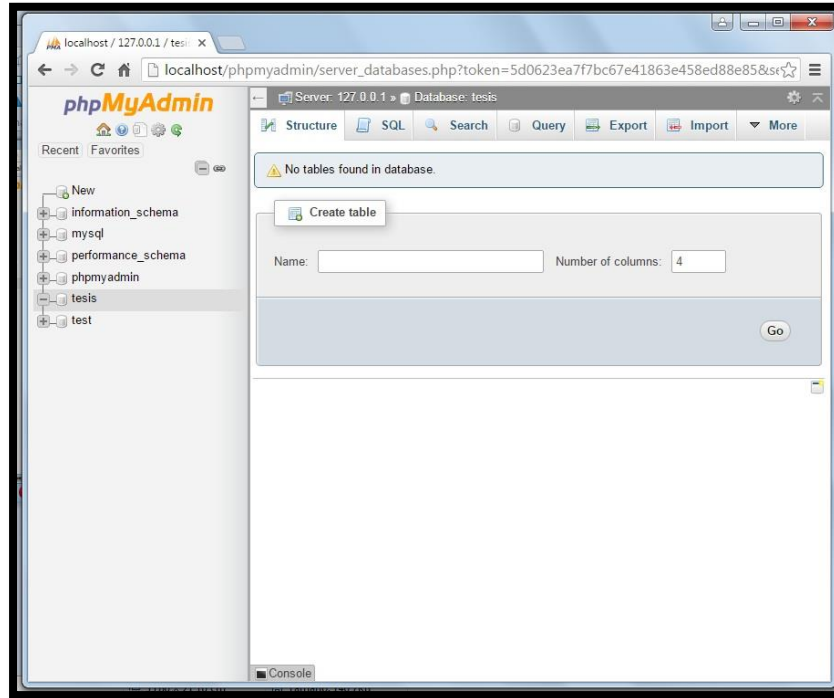
Una vez que los servicios estén corriendo, se digita localhost en la barra de direcciones de cualquier buscador y se visualiza la página principal de phpMyAdmin.



En la parte superior izquierda de la pantalla se visualiza las bases de datos existentes y la opción New que permitirá crear una nueva base de datos. Al presionar New se muestra una página donde se crea una nueva base de datos únicamente asignando un nombre.



Se coloca el nombre deseado y se presiona Create. Ahora la nueva base ya aparece en la barra de bases de datos existentes.



ANEXO D. INFORME PARA LA UBICACIÓN DE CONTROLES DE ACCESO EN LAS ENTRADAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE

INFORME DEL DIMENSIONAMIENTO DE LA

UNIVERSIDAD TÉCNICA DEL NORTE

DISEÑO E INSTALACIÓN DE INFRAESTRUCTURA

1. ASPECTOS GENERALES

Uno de los principales elementos de un sistema de seguridad son las cámaras y los controles de acceso, mismos que permiten controlar las zonas críticas y evitar cualquier acceso de personal no autorizado.

2. OBJETIVOS

2.1. Objetivo General:

- Que las instalaciones de la Universidad Técnica del Norte ofrezcan seguridad y bienestar tanto a su personal como a estudiantes.

2.2. Objetivos Específicos:

- Implementar controles de acceso a las tres entradas de las instalaciones y poder integrar a los controles de acceso antiguos.
- Instalación de controles de acceso.

3. INTRODUCCIÓN

3.1. Control de acceso

Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad. Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos (ej: acceso a una habitación donde hay servidores), recursos lógicos (ej: una cuenta de bancos, de donde solo determinadas personas puedan extraer dinero) o recursos digitales (ej: un archivo informático que sólo puede ser leído, pero no modificado).

4. DIMENSIONAMIENTO DE LA OBRA

4.1. Dimensionamiento Control de Acceso

Entrada Norte:

- En esta entrada es necesario colocar una base sólida de cemento, de la cual se detalla a continuación las dimensiones y los materiales, también es necesario una cubierta para que el control de acceso quede protegido de la lluvia.
- Dimensiones de la Base: 150cm x 120cm x 10cm.
- Nivelar el suelo para mejor desarrollo del producto.
- Especificación del suelo (concertó FCK15 M.P.A o equivalente).
- Cubierta: se necesita proteger el control de acceso de las condiciones climáticas con una cubierta de 180cm x 150cm.



Tipo de control de acceso a instalar:

El tipo de control de acceso a instalar es el CATRAX MASTER, ya que por el espacio que se tiene no se puede colocar otro tipo de control de acceso. Este control de acceso necesita de una cubierta para protegerlo del clima.

Entrada Sur:

- En esta entrada se va a instalar un control de acceso torniquete Light. Aquí solo se necesita colocar una base sólida y nivelar el suelo, a continuación los detalles:
- Dimensiones de la base: 151.5cm x 135cm x 10cm
- Nivelar el suelo para o mejor desarrollo del producto.
- Especificación del suelo (concreto FCK15 M.P.A. o equivalente).





Como se mencionó anteriormente el control de acceso a utilizar es el Torniquete Light, en este caso solo se tendría que nivelar el piso y colocar la base, a continuación se muestra una imagen del controlador:



Entrada Principal:

- En la entrada principal se utilizara un CATRAX MASTER, ya que por el espacio y estética son los más indicados, además para la parte de las personas incapacitadas se utilizará una puerta clip.

- En este sector no se requiere de ninguna adecuación, ya que la entrada principal está en las condiciones óptimas para poder colocar los controles de acceso.



ANEXO E. PROFORMAS

MÓDULOS Y PLACAS



ALL POWER MICROCONTROLLER APM

AV. COLON OE3-31 Y VERSALLES LOCAL N°1

1714061932001

022502124

PROFORMA NO.000005153

CLIENTE:

DIRECCION:

RUC/CI:

FECHA: 15/11/2016 01:39:53 PM

CODIGO	DESCRIPCION	CANT	P.UNIT.	TOTAL
2350	KEYPAD 4X4 NE	1.00	5.8036	5.80
1326	LCD 16X2 AZ	1.00	5.0893	5.09
4710	MODULO ETHERNET SHIELD GENERICO	1.00	25.0000	25.00
1206	ARDUINO MEGA 2560	1.00	60.7143	60.71
5203	TAG CARD NFC	1.00	2.1429	2.14
2162	LECTOR RFID RC522	1.00	42.8571	42.86

SON: CIENTO SESENTA Y UN ,43/100

SUBTOTAL: 141.60

DESCUENTO: 0.00

VALIDEZ DE ESTA PROFORMA: 15 DIAS

IVA: 19.82

PAGOS A LA CTA. CTE. PICHINCHA 3497432604 - FABIAN ORTIZ

FLETE: 0.00

TOTAL: 161.43

DISPOSITIVOS ELECTRÓNICOS

Velco

VIDEO ELECTRÓNICA Y COMUNICACIONES

Dir: Av. Jaime Rivadeneira 665 y Av. Mariano Acosta
Telf: 2950 942 / Ibarra - Ecuador

Persona Natural Obligado a llevar Contabilidad

Escobar León
Gladys Eufemia

PROFORMA

Nº 0001350

RUC: 1001531100001

Señor (es): Emerson Haro.

Dirección: Cotacachi.

Telf: _____

Ruc. _____

Fecha: 18 noviembre 2016.

Cant.	DETALLE	V. UNITARIO	V. TOTAL
02	Diodo Led.	0,10	0,20
03	Resistoria 1/2 w.	0,05	0,15
01	Potenciometro 10K.	0,50	0,50
01	Cerámico 104.	0,15	0,15
01	Filtro electrolítico 2200 MF 2V.	0,75	0,75
01	2N3904	0,15	0,15
01	Diodo 4001	0,15	0,15
01	Relay 5V.	0,75	0,75
01	Bornera 3 P.	0,30	0,30
01	Bornera 2 P.	0,25	0,25
02	Barra espaciadora	0,50	1,00
01	Kit cables proto	4,50	4,50
01	Transformador 12V +.	6,50	6,50
02	Regulador Voltage 8V-5V.	1,00	2,00
01	Baqueta fibra 10x20	2,20	2,20
01	Anillo Ferrico	0,80	0,80

Recibí Conforme



Entregué Conforme

Sub Total \$

IVA. 0%

IVA. 12%

TOTAL \$

1.201 - 1.400

Velco

VIDEO ELECTRÓNICA Y COMUNICACIONES

Dir: Av. Jaime Rivadeneira 665 y Av. Mariano Acosta
Telf: 2950 942 / Ibarra - Ecuador

Persona Natural Obligado a llevar Contabilidad

Escobar León
Gladys Eufemia

PROFORMA

Nº 0001351

RUC: 1001531100001

Señor (es): Emerson Haro

Dirección: Cotacachi

Telf: _____

Ruc. _____

Fecha: 18 Nov. 2016.

Cant.	DETALLE	V. UNITARIO	V. TOTAL
01	Broca Baquelita	0,40	0,40
01	cañón Tipo Lariz	1,50	1,50
01	Rollo estanco sog.	3,00	3,00
01	Pasta para soldar.	1,25	1,25
01	pulsador N/A	0,75	0,75
01	caja para proyectos.	12,00	12,00
01	Bateria 12V - 4.5A	24,00	24,00

Recibí Conforme

Entregué Conforme

Sub Total \$	
IVA. 0%	
IVA. 12%	
TOTAL \$	

SERVIDOR, UPS Y RADIOS

Server Hp Proliant MI30 G9 Intel Xeon Quad Core 4gb 1tb Dvd


Nuevo 10 vendidos



**Hewlett Packard
Enterprise**

U\$S 1.189⁹⁹

 Pago a acordar con el vendedor
Acepta depósito bancario, efectivo.
[Más información](#)

 Entrega a acordar con el vendedor
Quito, Pichincha (Quito)
[Ver costos de envío](#)

Cantidad:

- 1 +


Comprar


Ups Apc Br-1000g 1000va 1kva 600w 8 Tomas Lcd Regulador 110v 

Nuevo 14 vendidos



U\$S 219⁹⁹

 Pago a acordar con el vendedor
Acepta depósito bancario, efectivo.
[Más información](#)

 Entrega a acordar con el vendedor
Quito, Pichincha (Quito)
[Más información](#)

Cantidad:

- 1 +

Comprar



ANEXO F. HOJA DE DATOS DEL LECTOR RFID RC522

MFRC522

GENERAL DESCRIPTION

The MFRC522 is a highly integrated reader/writer IC for contactless communication at 13.56 MHz. The MFRC522 reader supports ISO/IEC 14443 A/MIFARE and NTAG. The MFRC522's internal transmitter is able to drive a reader/writer antenna designed to communicate with ISO/IEC 14443 A/MIFARE cards and transponders without additional active circuitry. The receiver module provides a robust and efficient implementation for demodulating and decoding signals from ISO/IEC 14443 A/MIFARE compatible cards and transponders. The digital module manages the complete ISO/IEC 14443 A framing and error detection (parity and CRC) functionality. The MFRC522 supports MF1xxS20, MF1xxS70 and MF1xxS50 products. The MFRC522 supports contactless communication and uses MIFARE higher transfer speeds up to 848 kBd in both directions.

The following host interfaces are provided:

- Serial Peripheral Interface (SPI)
- Serial UART (similar to RS232 with voltage levels dependant on pin voltage supply)
- I 2C-bus interface

FEATURES AND BENEFITS

- Highly integrated analog circuitry to demodulate and decode responses
- Buffered output drivers for connecting an antenna with the minimum number of external components
- Supports ISO/IEC 14443 A/MIFARE and NTAG
- Typical operating distance in Read/Write mode up to 50 mm depending on the antenna size and tuning
- Supports MF1xxS20, MF1xxS70 and MF1xxS50 encryption in Read/Write mode
- Supports ISO/IEC 14443 A higher transfer speed communication up to 848 kBd

- Supports MFIN/MFOUT
- Additional internal power supply to the smart card IC connected via MFIN/MFOUT
- Supported host interfaces
 - SPI up to 10 Mbit/s
 - I 2C-bus interface up to 400 kBd in Fast mode, up to 3400 kBd in High-speed mode
 - RS232 Serial UART up to 1228.8 kBd, with voltage levels dependant on pin voltage supply
- FIFO buffer handles 64 byte send and receive
- Flexible interrupt modes v Hard reset with low power function
- Power-down by software mode v Programmable timer
- Internal oscillator for connection to 27.12 MHz quartz crystal
- 2.5 V to 3.3 V power supply
- CRC coprocessor
- Programmable I/O pins
- Internal self-test

QUICK REFERENCE DATA

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
AV_{DD}	Supply Voltage	$AV_{SS} = DV_{SS} = PV_{SS} = TV_{SS} = 0\text{ V}$, $PV_{DD} \leq AV_{DD} = DV_{DD} = TV_{DD}$	2.5	-	3.6	V
DV_{DD}						
TV_{DD}						
PV_{DD}	Pad power supply	$AV_{SS} = DV_{SS} = PV_{SS} = TV_{SS} = 0\text{ V}$, $PV_{DD} \leq AV_{DD} = DV_{DD} = TV_{DD}$	1.6	-	3.6	V
SV_{DD}	MFIN/MFOUT Pad Power Supply	$AV_{SS} = DV_{SS} = PV_{SS} = TV_{SS} = 0\text{ V}$,	1.6	-	3.6	V
I_{HPD}	Hard Power-down Current	$AV_{DD} = DV_{DD} = TV_{DD} = PV_{DD} = 3\text{ V}$, $N_{RESET} = \text{LOW}$	-	-	5	μA
I_{SPD}	Soft Power-down Current	$AV_{DD} = DV_{DD} = TV_{DD} = PV_{DD} = 3\text{ V}$, RF level detector on	-	-	10	μA
I_{DVDD}	Digital Supply Current	$DV_{DD} = 3\text{ V}$	-	6.5	9	mA
I_{AVDD}	Analog Supply Current	$AV_{DD} = 3\text{ V}$, bit RCVOFF = 0	-	7	10	mA
$I_{AVDD,RCVOFF}$	Analog Supply Current, receiver switched off	$AV_{DD} = 3\text{ V}$, bit RCVOFF = 1	-	3	5	mA
I_{PVDD}	Pad Supply Current		-	-	40	mA
I_{TVDD}	Transmitter Supply Current	Continuous Wave	-	60	100	mA
T_{amb}	operating ambient temperature		-25		+85	$^{\circ}\text{C}$

[1] Supply voltages below 3 V reduce the performance in, for example, the achievable operating distance.

[2] VDDA, VDDD and VDD (TVDD) must always be the same voltage.

[3] VDD (PVDD) must always be the same or lower voltage than VDDD.

[4] I_{pd} is the total current for all supplies.

[5] I_{DD} (PVDD) depends on the overall load at the digital pins.

[6] I_{DD} (TVDD) depends on VDD (TVDD) and the external circuit connected to pins TX1 and TX2.

[7] During typical circuit operation, the overall current is below 100 mA.

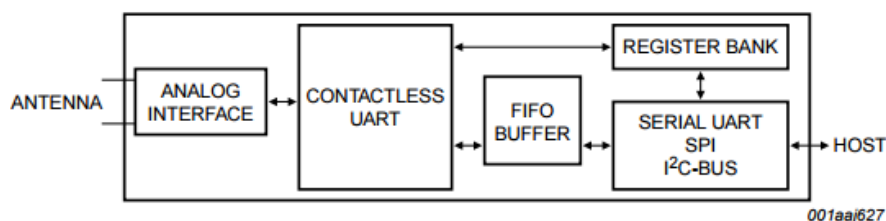
[8] Typical value using a complementary driver configuration and an antenna matched to 40Ω between pins TX1 and TX2 at 13.56 MHz.

BLOCK DIAGRAM

The analog interface handles the modulation and demodulation of the analog signals.

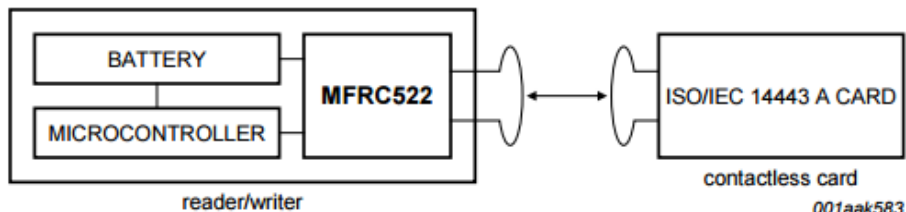
The contactless UART manages the protocol requirements for the communication protocols in cooperation with the host. The FIFO buffer ensures fast and convenient data transfer to and from the host and the contactless UART and vice versa.

Various host interfaces are implemented to meet different customer requirements.

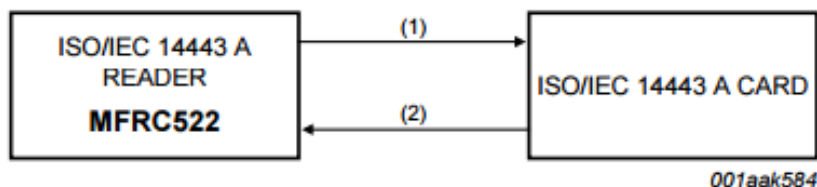


FUNCTIONAL DESCRIPTION

The MFRC522 transmission module supports the Read/Write mode for ISO/IEC 14443 A/MIFARE using various transfer speeds and modulation protocols.



The physical level communication is shown in Figure:



(1) Reader to card 100 % ASK, Miller encoded, transfer speed 106 kBd to 848 kBd.

(2) Card to reader subcarrier load modulation, Manchester encoded or BPSK, transfer speed 106 kBd to 848 kBd.

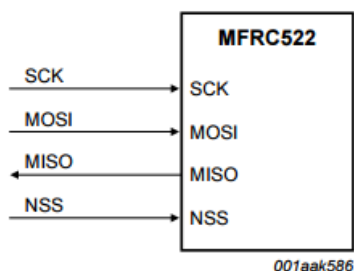
COMMUNICATION OVERVIEW FOR ISO/IEC 14443 A/MIFARE READER/WRITER

Communication direction	Signal type	Transfer speed			
		106 kBd	212 kBd	424 kBd	848 kBd
Reader to card (send data from the MFRC522 to a card)	reader side modulation	100 % ASK	100 % ASK	100 % ASK	100 % ASK
	bit encoding	modified Miller encoding	modified Miller encoding	modified Miller encoding	modified Miller encoding
	bit length	128 (13.56 μs)	64 (13.56 μs)	32 (13.56 μs)	16 (13.56 μs)
Card to reader (MFRC522 receives data from a card)	card side modulation	subcarrier load modulation	subcarrier load modulation	subcarrier load modulation	subcarrier load modulation
	subcarrier frequency	13.56 MHz / 16	13.56 MHz / 16	13.56 MHz / 16	13.56 MHz / 16
	bit encoding	Manchester encoding	BPSK	BPSK	BPSK

SERIAL PERIPHERAL INTERFACE

A serial peripheral interface (SPI compatible) is supported to enable high-speed communication to the host. The interface can handle data speeds up to 10 Mbit/s. When communicating with a host, the MFRC522 acts as a slave, receiving data from the external host for register settings, sending and receiving data relevant for RF interface communication.

An interface compatible with SPI enables high-speed serial communication between the MFRC522 and a microcontroller. The implemented interface is in accordance with the SPI standard.



The MFRC522 acts as a slave during SPI communication. The SPI clock signal SCK must be generated by the master. Data communication from the master to the slave uses the MOSI line. The MISO line is used to send data from the MFRC522 to the master.

Data bytes on both MOSI and MISO lines are sent with the MSB first. Data on both MOSI and MISO lines must be stable on the rising edge of the clock and can be changed on the falling edge. Data is provided by the MFRC522 on the falling clock edge and is stable during the rising clock edge.

SPI READ DATA

Reading data using SPI requires the byte order shown in Table to be used. It is possible to read out up to n-data bytes.

The first byte sent defines both the mode and the address.

Line	Byte 0	Byte 1	Byte 2	To	Byte n	Byte n + 1
MOSI	address 0	address 1	address 2	...	address n	00
MISO	X ^[1]	data 0	data 1	...	data n - 1	data n

[1] X = Do not care.

SPI WRITE DATA

To write data to the MFRC522 using SPI requires the byte order shown in Table. It is possible to write up to n data bytes by only sending one address byte.

The first send byte defines both the mode and the address byte.

Line	Byte 0	Byte 1	Byte 2	To	Byte n	Byte n + 1
MOSI	address 0	data 0	data 1	...	data n - 1	data n
MISO	X ^[1]	X ^[1]	X ^[1]	...	X ^[1]	X ^[1]

[1] X = Do not care.

SPI ADDRESS BYTE

The address byte must meet the following format.

The MSB of the first byte defines the mode used. To read data from the MFRC522 the MSB is set to logic 1. To write data to the MFRC522 the MSB must be set to logic 0. Bits 6 to 1 define the address and the LSB is set to logic 0.

7 (MSB)	6	5	4	3	2	1	0 (LSB)
1 = read 0 = write	address						0