

# 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.

Emerson Gabriel Haro Flores

*Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Ibarra, Imbabura*  
egharo@utn.edu.ec

**Resumen -** El presente trabajo 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 un identificador único y una base de datos.

**Palabras clave** – RFID, PHP, TCP/IP, Arduino, SPI.

## I. INTRODUCCIÓN

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.

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.

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.

## II. SISTEMAS DE IDENTIFICACIÓN POR RADIOFRECUENCIA

La tecnología de identificación por radio frecuencia RFID (Radio Frequency Identification), se caracteriza por contener 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.

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. La Fig. 1 muestra la estructura de un sistema RFID:

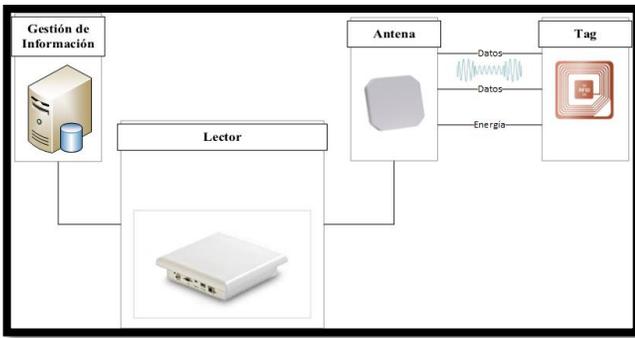


Fig. 1 Estructura de un Sistema RFID.

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.

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.

#### A. 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. La Fig. 2 muestra la estructura de un tag y sus componentes principales:

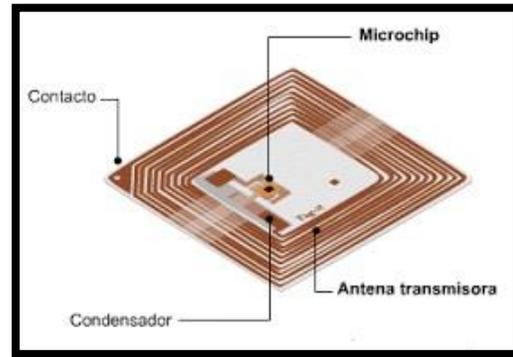


Fig. 2 Componentes de un tag RFID.

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 Fig.3 muestra un diagrama en bloques de la arquitectura de una etiqueta RFID:

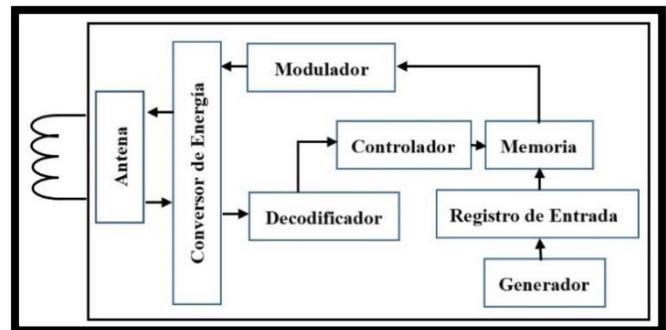


Fig. 3 Estructura de un Tarjeta RFID.

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 convertor 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 [1].

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.

- Etiquetas pasivas.- Este tipo de etiquetas se caracterizan por utilizar la energía obtenida de las ondas generadas por el lector.
- 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.
- 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 [2].

### B. 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. La Fig. 4 muestra la estructura interna de un lector RFID:

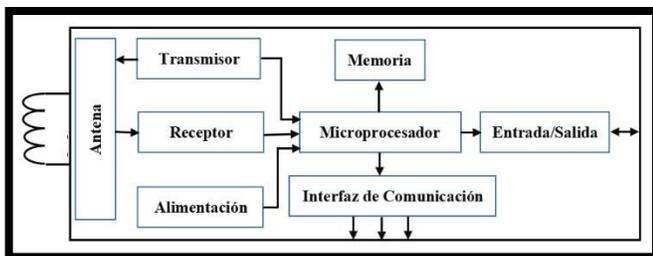


Fig 4. Estructura de un Lector RFID.

### C. 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 [3].

## III. SITUACION 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 Fig. 5 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.

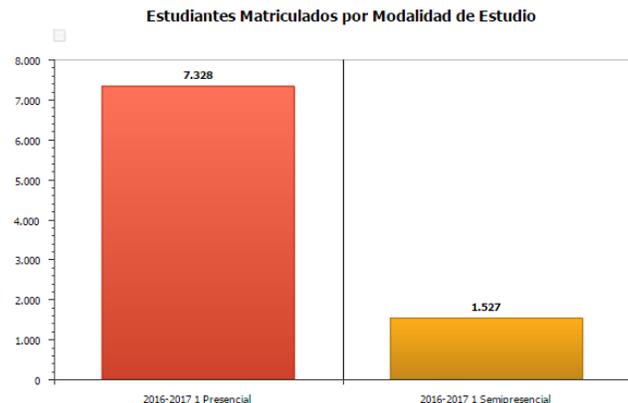


Fig. 5 Estudiantes matriculados por modalidad de estudio.

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 mediante el uso de un identificador único a modo de tarjeta para cada uno de los estudiantes, docentes y demás trabajadores de la Universidad.

## IV. 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

La Fig. 6, muestra el esquema de las principales áreas de diseño de hardware:

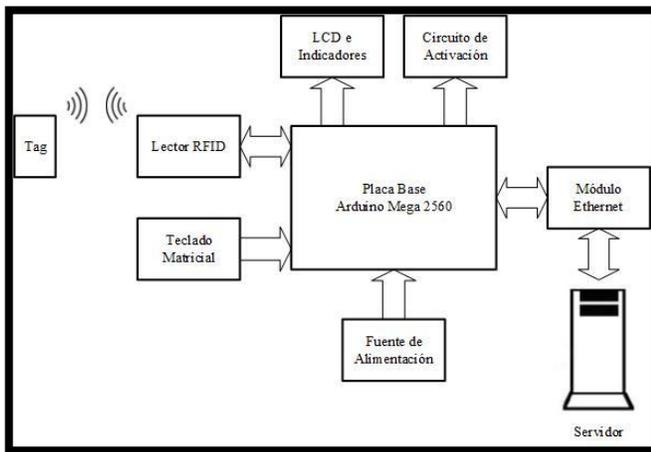


Fig. 6 Diagrama en bloques del hardware del sistema de control de acceso.

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. A continuación se describe cada uno de los módulos principales que componen el diseño de hardware del sistema.

### A. Arduino MEGA 2560

La placa Arduino MEGA 2560 al ser una plataforma de hardware libre y que gracias a las características que presenta, es la más indicada para desarrollar un sistema de control de acceso. Las principales características técnicas que presenta la placa Arduino MEGA 2560 se detallan a continuación en la Tabla 1:

TABLA 1

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

### B. Módulo Arduino Ethernet

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. Arduino Ethernet Shield se comunica

con las demás placas Arduino compatibles a través de comunicación SPI.

Dentro de las características principales del módulo Ethernet se pueden citar las siguientes en la Tabla 2:

TABLA 2

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

### C. Lector 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 3 a continuación muestra algunas características de este dispositivo:

TABLA 3

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	<80 $\mu$ A
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

### D. 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 Tabla 4:

TABLA 1

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	<b>288mA</b>	

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 Fig. 7:

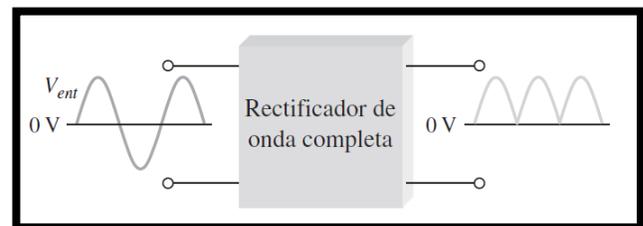


Fig. 7 Tipo de onda generada por rectificador de onda completa.

La fuente utilizará de un capacitor de alto valor, haciendo 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.

### E. Esquema General

A continuación la Fig. 8 muestra el esquema general del sistema de control de acceso con todos los bloques y elementos que lo conforman:

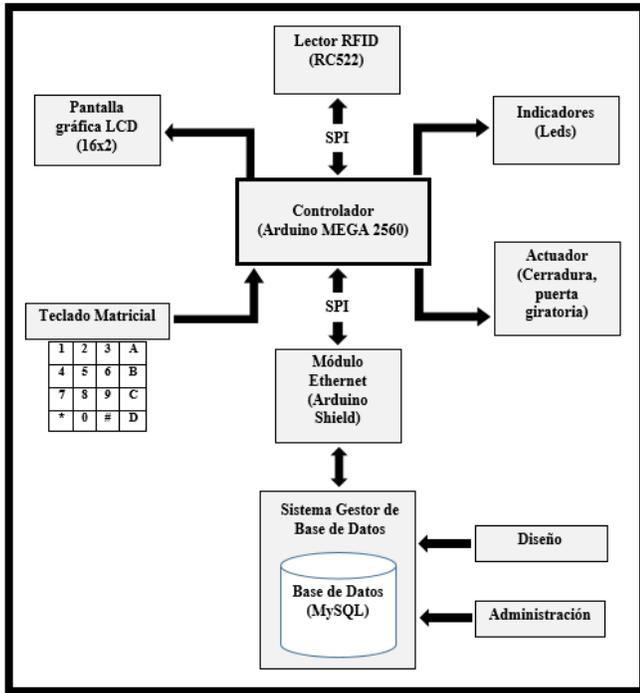


Fig. 8 Diagrama esquemático de la fuente de alimentación.

## V. DISEÑO DE SOFTWARE

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

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.

Como se puede observar en la Fig. 9, luego de la declaración de variables e inicialización de módulos, 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.

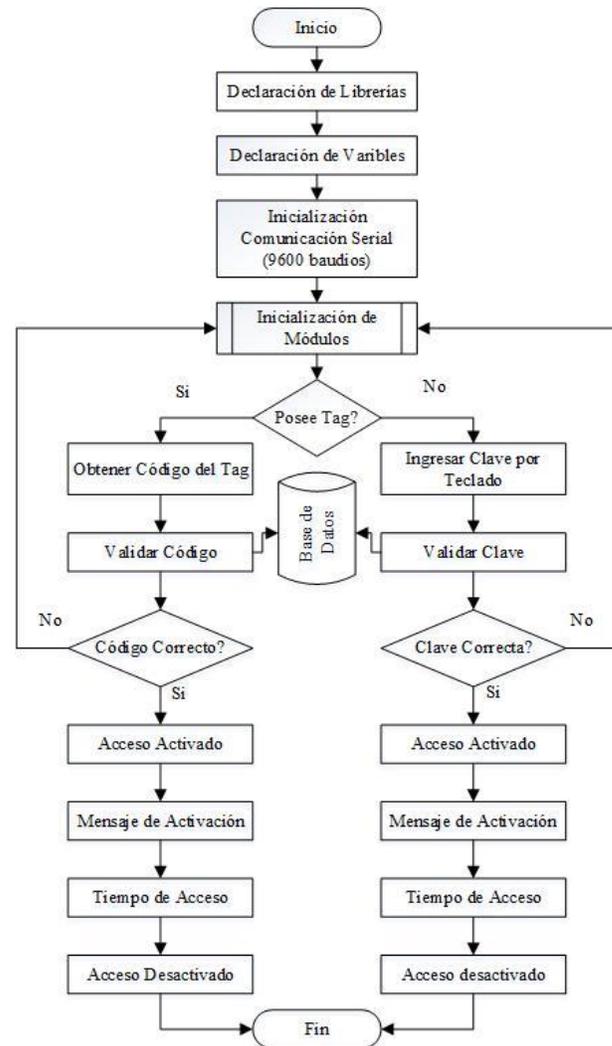


Fig. 9 Diagrama de flujo del funcionamiento del Sistema de Control de Acceso

### A. Envío y recepción de datos

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 Fig.10 a continuación muestra el proceso de interacción de la base de datos con el sistema a través de PHP:

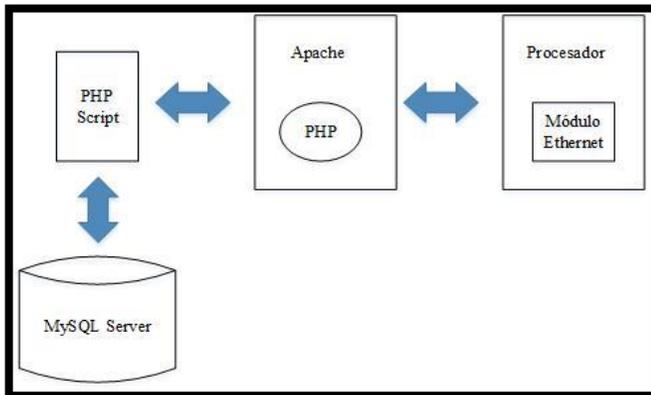


Fig. 10 Esquema de interacción de la base de datos a través de PHP.

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 [4].

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 [5].

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.

## VI. 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 el desarrollo de la base de datos que contendrá la información de los usuarios del sistema de control de acceso se utilizaran las siguientes tablas:

### A. 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. 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 Fig. 11 a continuación indica la estructura de la tabla login:

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
1	id	int(11)			No	Ninguna	AUTO_INCREMENT
2	usuario	varchar(20)			No	Ninguna	
3	password	varchar(20)			No	Ninguna	

Fig. 11 Estructura de la tabla "login".

### B. 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 irrepitible 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 Fig. 12:

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

Fig. 12 Estructura de la tabla usuarios.

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.

### C. 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 realizo su registro de acceso.

El tipo y valor asignado para cada uno de estos campos se muestra a continuación en la Fig. 13:

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
1	id	int(11)			No	Ninguna	AUTO_INCREMENT
2	tag	varchar(30)			No	Ninguna	
3	hora	time			No	Ninguna	
4	fecha	date			No	Ninguna	

Fig. 13 Estructura de la tabla registros.

### D. 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 Fig. 14 a continuación:

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
1	id	int(11)			No	Ninguna	AUTO_INCREMENT
2	tag	varchar(30)			No	Ninguna	

Fig. 14 Estructura de la tabla “no registrados”.

### E. 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 Fig. 15 a continuación muestra la estructura de la tabla “visitantes”:

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
1	id	int(11)			No	Ninguna	AUTO_INCREMENT
2	nombre	varchar(30)			No	Ninguna	
3	cedula	varchar(10)			No	Ninguna	
4	hora	time			No	Ninguna	
5	fecha	date			No	Ninguna	

Fig. 15 Estructura de la tabla “visitantes”.

## VII. PRUEBAS DE FUNCIONAMIENTO

### A. 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 Fig. 16 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.

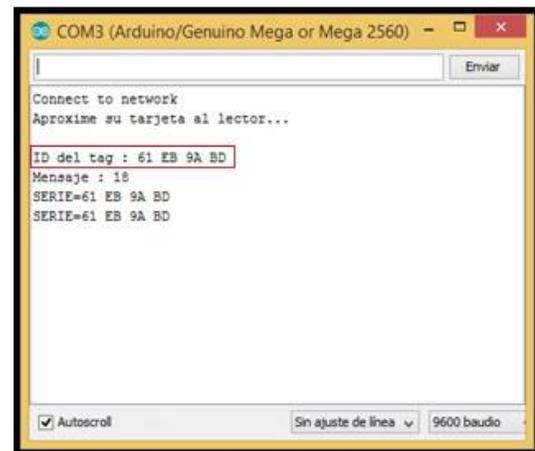


Fig. 16 Lectura de Código de tarjeta RFID.

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.

### B. Pruebas de funcionamiento del teclado matricial

Al igual que el lector RFID, la funcionalidad del teclado matricial fue comprobada 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 Fig. 17:

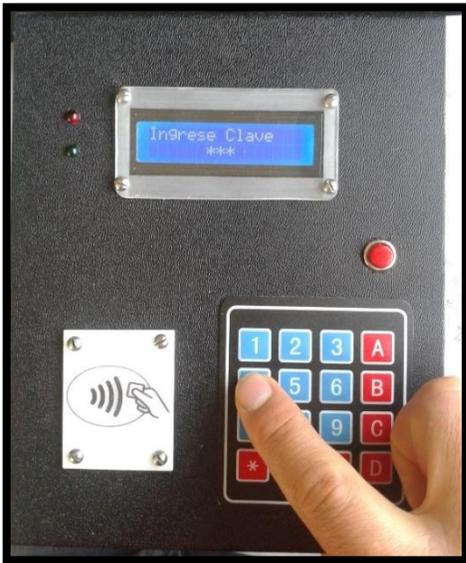


Fig. 17 Activación de subrutina para ingreso de clave por teclado.

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 Fig. 18:



Fig. 18: Ingreso correcto de clave a través del teclado matricial.

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 Fig. 19:



Fig. 19: Ingreso de clave incorrecta mediante teclado matricial.

### C. Ingreso a la página de administración a través de usuario y contraseña

Fue necesaria la creación de una página web como indica la Fig 20, 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.

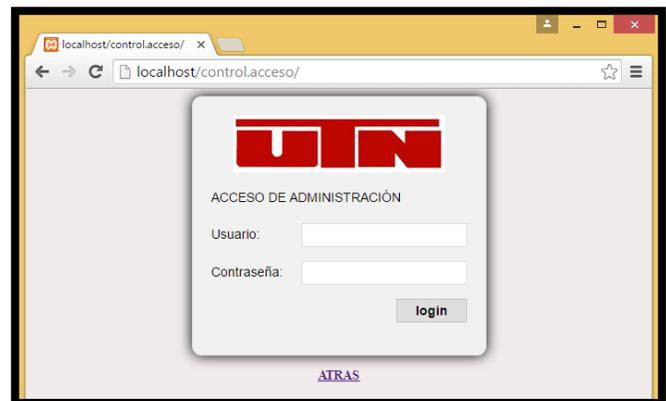


Fig. 20 Página de ingreso de usuario y contraseña.

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 Fig. 21:

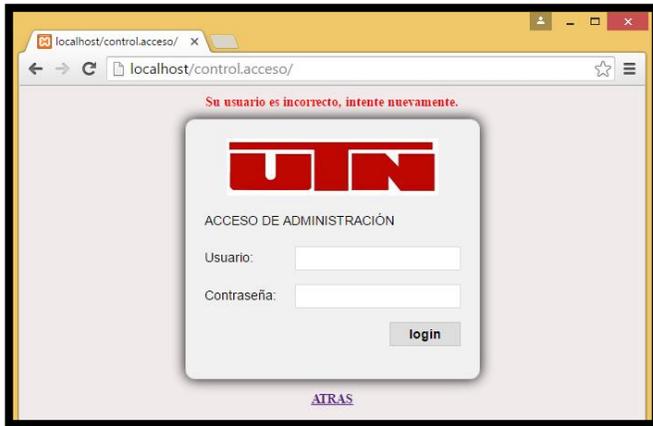


Fig. 21 Ingreso incorrecto de usuario y contraseña.

#### D. 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 interfaz web del sistema, para ello se debe acceder a cualquiera de los dos sitios. 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 Fig. 22:

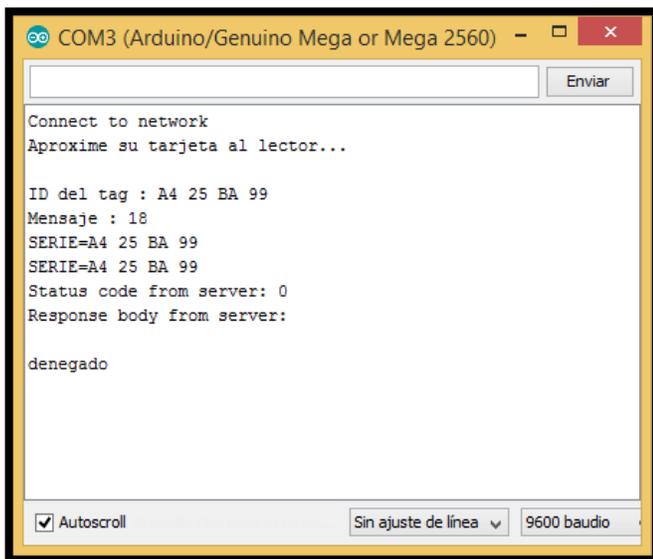


Fig. 22 Lectura de tarjeta no registrada.

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. Una vez que se haya seleccionado el código, se procede a ingresar los datos del usuario como indica la Fig. 23:

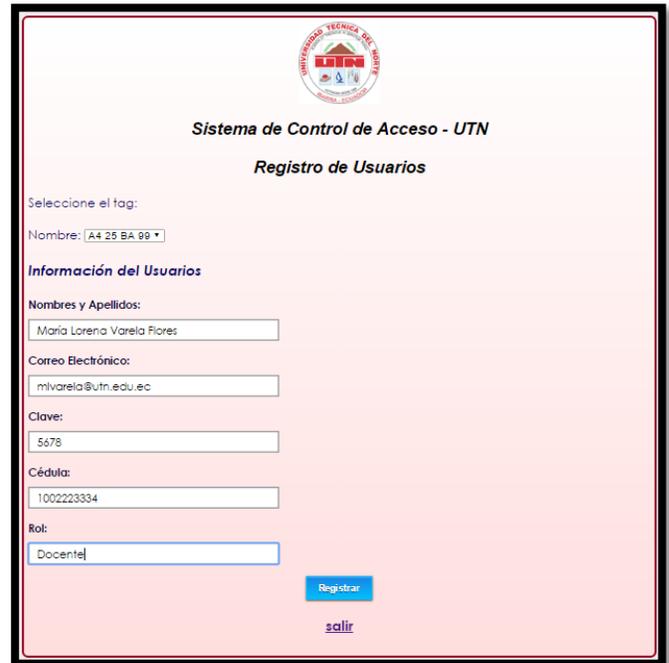


Fig. 23 Ingreso de datos de usuario a través de página web.

Si el registro se realizó adecuadamente, se mostrará un mensaje de registro completo, como se observa en la Fig. 24:



Fig. 24 Mensaje de registro completo.

Finalmente se puede constatar que el usuario ha sido agregado a la base de datos y de esta forma se permitirá el acceso. La Fig. 25 muestra el mensaje de lectura del tag, luego de haber sido registrado:

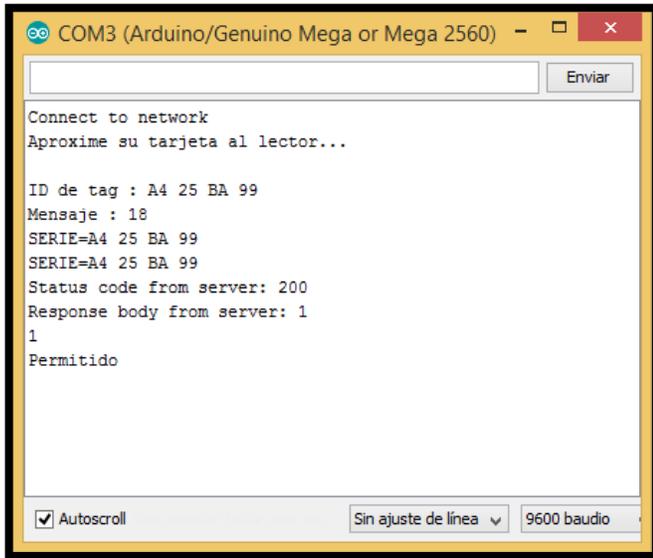


Fig. 25 Lectura de tarjeta registrada.

## VIII. 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 5. Estos costos deben justificar el beneficio que conlleva la elaboración del proyecto hacia los usuarios.

TABLA 5

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
<b>TOTAL</b>			<b>\$14991,50</b>

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.

## IX. 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.

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.

## X. REFERENCIAS

- [1] Godínez, L. M. (2008). RFID Oportunidades y riesgos, su aplicación práctica. Barcelona: Alfaomega.
- [2] AETIC. (2009). La tecnología RFID: Usos y Oportunidades. Madrid: red.es.
- [3] Portillo, J., Bermejo, A., Bernardos, A., & Martínez, I. (2008). Tecnología de identificación por radio frecuencia (RFID): aplicaciones en el ámbito de la salud. Madrid.
- [4] Aprenderaprogramar. (2016). Aprenderaprogramar.com. Obtenido de Aprenderaprogramar.com: <http://aprenderaprogramar.com/>
- [5] Berni Millet , P., & Gil de la Iglesia, D. (2010). Laboratorio de PHP y MySQL. Catalunya: Eureka Media, SL.

- [6] Gidekel, A. (2008). Introducción a la Identificación por Radio Frecuencia. Electrónica Codificación S.A.
- [7] Boxall, J. (2013). Arduino Workshop A Hands-On Introduction.
- [8] Ortiz, E., Ibarra, M., Andrade, J., & Almanza, D. (2012). Control de acceso usando FPGA y RFID. 8.
- [9] Arduino. (30 de Noviembre de 2015). arduino.cc. Obtenido de <https://www.arduino.cc>
- [10] Letrán, J. (2011). cortoc.com. Obtenido de <http://www.cortoc.com/2011/12/introduccion-arduino.html>
- [11] Pillo, D. (9 de Enero de 2013). Repositorio Digital - Universidad Técnica del Norte. Obtenido de <http://repositorio.utn.edu.ec/handle/123456789/999>



### **Emerson Gabriel Haro Flores.**

Nació en Atuntaqui – Ecuador el 9 de marzo de 1990. Sus estudios primarios los realizó en la escuela “Andrés Bello de la Torre”, sus estudios secundarios en la “Instituto Tecnológico Otavalo”. Estudiante de la Universidad

Técnica del Norte en la Facultad de Ingeniería en Ciencias Aplicadas, Carrera de Electrónica y Redes de Comunicación.