Access control system and monitoring of students with the use of wireless automatic identification (RFID) technology at Técnica Del Norte University.

Emerson Gabriel Haro Flores
Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Ibarra, Imbabura
egharo@utn.edu.ec

***Abstract* - The present work has with objective the design of a control access system using radio frequency identification (RFID) technology. This project it will primarily benefit students of the Técnica del Norte University to have an appropriate control and monitoring of all people, who are coming in the campus through a record using a unique identifier and database.**

***Keywords* - RFID, PHP, TCP/IP, Arduino, SPI.**

I. INTRODUCTION

Many cases of robberies have arisen within public institutions by outsiders, who enter with complete ease and without being detected. These cases have been seen especially in places of massive concurrence, in which there is not enough personnel that controls that aspect of security.

At present many institutions and companies have opted to implement in their installations systems of control of entrance of personnel, in order to improve the security. In this way you can control the entry of users who have an identifier that authorizes their passage, otherwise deny the same.

An access control system, as its name implies, is characterized by presenting security and control characteristics, ensuring the integrity of the users and the material assets of the institutions, in addition to keeping a proper register of the users' entry, and presenting an added value to the modernization.

The access control system to be implemented at Técnica del Norte University aims to contribute to the existing security system and provide an extra level of security, specifically to students. For this purpose, electronic cards will be used to identify each user and can validate their entry. In addition, there will be an alternative key entry system by keyboard in case the user does not have the electronic card.

II. RADIO FREQUENCY IDENTIFICATION SYSTEM

Radio Frequency Identification (RFID) technology is characterized by containing the information in electronic cards or also called tags. As soon as these tags enter the coverage area generated by the reading system for this technology, it sends a signal to this tag to transmit the information that is stored in its memory and that it is usually an identification code.

One of the important characteristics of RFID systems is precisely the retrieval of radiofrequency information without the need for line of sight or physical contact between the tag and the reader, although in many cases a specific distance is established for the transference to exist of such information

An RFID system is basically constituted by three important elements that it comply specific functions: electronic cards or tags, antennas, reader and in some cases also includes an information management system when it is necessary to handle a great amount of information, which cannot be operated in the reader's own memory. Figure 1 shows the structure of an RFID system: they comply

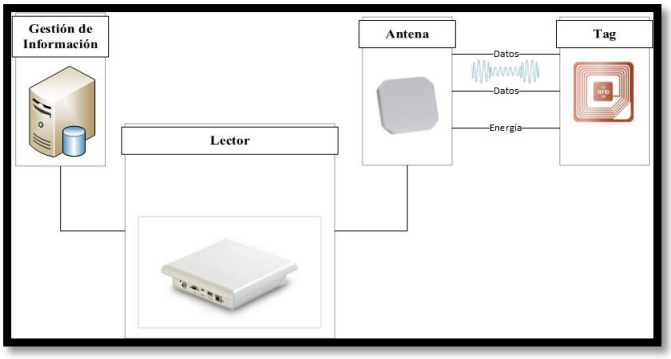

Fig. 1 Structure of an RFID System.

The basic mode of operation of this type of systems is done sequentially since the tag enters the area of emission of the reader, which controls the reading and writing of the information stored in the cards through a field of radiofrequency. Internally the tag is made up of a micro-antenna and a chip, which at the moment it perceives electromagnetic waves from the reader, activates the chip to release the information stored in its memory.

Once the reader has captured the response of the tag it processes the information and proceeds to send it to a database which contains information of the previously registered card for the processing of the action to which it has associated and that the rest of the system must execute, according to the application that is being given.

A. Tag RFID

The RFID tag is one of the key elements in radio frequency identification systems, it is considered as a transponder device, that is to say that thanks to its operation it has the capacity to receive and issue signals, but only as a response to a request of a transceiver or reader device. Fig. 2 shows the structure of a tag and its main components:

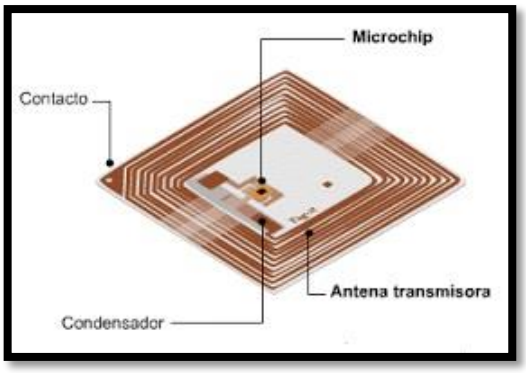

Fig. 2 Components of an RFID tag.

The basic components of an RFID tag are without a doubt the antenna and the chip, where the antenna is responsible for sending the information to the chip, the same inside its structure has a non-volatile memory in this case an EEPROM memory, the capacity depends on the model and are in the range of 96 bytes up to 32Kbits depending on your application.

The integrated circuit that is inside the chip has some functionalities among which are: power conversion, logic control, data storage and retrieval and modulation required to return the data to the reader. Figure 3 shows a block diagram of the architecture of an RFID tag:

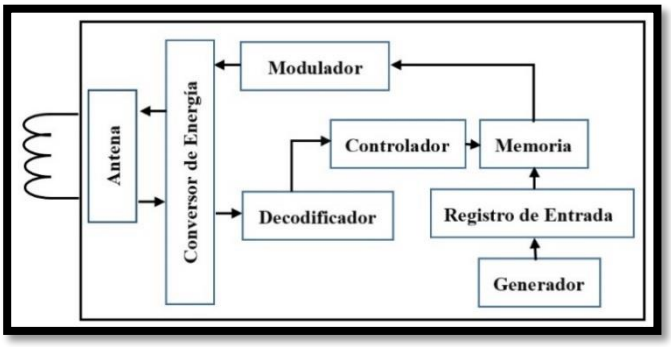

Fig. 3 Structure of an RFID tag.

Radio waves generated by the reader and captured by the antenna are processed and become not only in requests but also in energy for the remaining units that make up the chip through an ADC converter, which provides power to the rest of devices. The chip also contains a decoder and encoder to convert the analog signal into digital and vice versa. Subsequently this signal goes to the logical control block in which a low level processing is performed to read the unique code that is recorded in the memory and that was encoded by the manufacturer. Finally this code becomes modulated to send the information to the reader [1].

The classification of the RFID tags is varied, however the most common one given to them, is specified by the feeding mode they have, thus having tags: passive, semi active and active.

- Passive tags.- These types of tags are characterized by using the energy obtained from the waves generated by the reader.

- Semiactive tags.- Semiactive tags have their own power supply, however this serves only to feed the chip of the tag, but not to carry out the transmission of information, for it will continue to use the energy provided by the reader system.

- Active tags.- The active tags are characterized by being independent of the signal transmitted by the reader, have their own battery which improves their reach reaching a maximum of 100 meters, in addition to possessing a greater capacity of storage and better immunity to noise [2].

B. *Reader RFID*

The RFID reader is a device that incorporates subsystems for transmitting and receiving encoded signals or electromagnetic waves through an antenna system. One of its main objectives is to generate the radio frequency signal to activate and feed the tag, as well as interacting with the information management system for its processing. Fig. 4 shows the internal structure of an RFID reader:

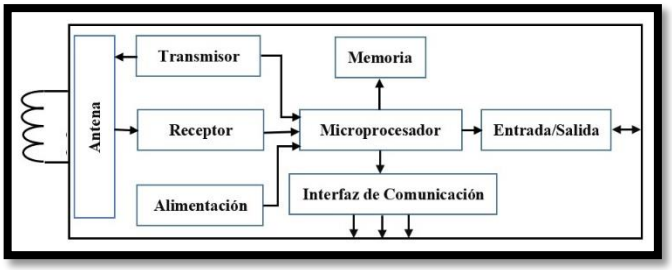

Fig 4. Structure of a RFID reader.

C. *Antennas*

Antennas are the most sensitive elements within an RFID system, since they are in charge of sending and receiving the signals that contain the information to be processed. Their size and shape varies, depending on the frequency of operation and the coverage area they generate, as well as on the application they are going to have [3].

III. ACTUAL SITUATION

Actually the Técnica del Norte University, does not have an access control system in its entrances, for that reason, there have been many cases of robbery within the institution. This has caused the authorities to order the closure of the north and south entrances, in order to have a single access and exit route through the main entrance, and thus be able to carry a better control. However, these measures have not been sufficient to improve this situation.

Figure 5 shows the number of students enrolled for the 2016-2017 period, in which a total of 8855 are observed, of which 7328 are in the presently modality, however this figure is distributed in the different dependencies with which The University has a daily number of about 5000 people on campus, including students, teachers, administrative staff and other employees.

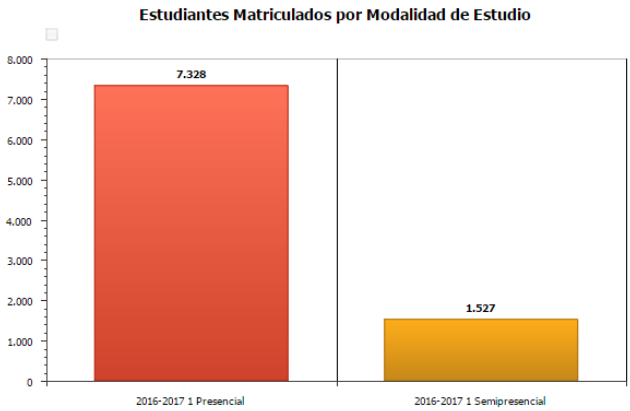

Fig. 5 Students enrolled by study modality.

This high number of people makes the work of security personnel complex, since they cannot provide adequate control, nor provide the necessary security guarantees to each person,

In view of these facts, Técnica del Norte University has been obliged to establish new security and control projects, in which there is an access control system through the use of a unique identifier as a card for each one of students, teachers and other workers of the University.

IV. HARDWARE DESING

For the hardware design of the access control system should focus on the type of connection of modules and other devices that comprise it, in addition to other important aspects to consider as requirements in the design, such as:

- High availability RFID Reader
- Alternative matrix keyboard access
- Ethernet connection to the database server
- End-user interface (indicators, LCD graphic display, sound generator)
- Circuit with relay for activation of actuators

Fig. 6 shows the outline of the main areas of hardware design:

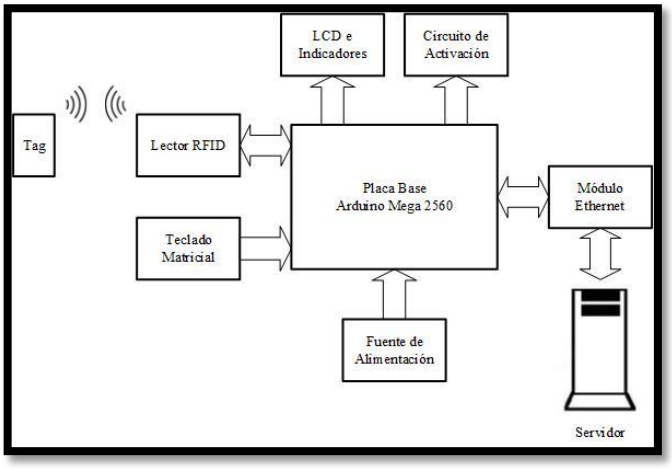

Fig. 6 Block diagram of the access control system hardware.

The operation of the system starts when the user enters its unique identifier contained in a tag, the area of coverage of the reader. The reader is responsible for extracting the tag code in an EPC format hexadecimal and sending it to the processing base plate, this information will be sent through the Ethernet module to the server that contains the database, which compares and validates the Information received with the stored information of each user, this request is sent back from the database to the motherboard, which according to the response obtained from it will execute the necessary actions through an activation circuit, which Activate or deactivate the system according to the response. This action is verified by the user through indicators, which are: LCD graphic screen, leds and sound generator.

Alternatively to the tag, the user also has an identification key, which can be used in case of not having the electronic identifier. In the same way, the system processes the code entered by the user through the keyboard through the motherboard, in order to verify and validate the key with the existing one in the database and to be able to generate the actions through the actuator circuit.

All system is powered by a power supply, which provides the appropriate levels of energy relative to voltage and current, according to the consumption of each element, and that serves for the correct functionality of the system, also has a battery of backup, which provides power in the event of a power cut for a certain time, in which the system can be adapted to have full access without identification, blocking or normal operation, depending on the cut-off time.

The following describes each of the main modules that make up the system's hardware design.

A. Arduino MEGA 2560

The Arduino MEGA 2560 board is a free hardware platform and thanks to the features it presents, is the most suitable for developing an access control system. The main technical characteristics of the Arduino MEGA 2560 board are detailed below in Table 1:

TABLE 1

Technical specifications of the Arduino MEGA 2560.

Characteristics	**Settings**
Microcontroller	ATmega2560
Feeding tension	5V
Recommended Input Voltage	7-12V
Input Limit	6-20V
Digital pins	54 (14 con PWM)
Analog inputs	16
Maximum current per pin	20 mA
Maximum current for pin 3.3V	50 mA
Flash memory	256 KB
SRAM	8 KB
EEPROM	4 KB
Clock Speed	16 MHz

B. Arduino Ethernet Module

The module or also called Arduino Ethernet Shield is a device fully compatible with Arduino Mega 2560 that uses the Ethernet library for ease of use.

The Ethernet library allows you to make a connection to the internet or any local network to an Arduino board, in this way you can have a server that accepts incoming and outgoing requests from a client. Arduino Ethernet Shield communicates with all other compatible Arduino boards through SPI communication. Among the main features of the Ethernet module are the following in Table 2:

TABLE 2

Technical specifications of the Arduino Ethernet board.

Characteristics	**Settings**
Microcontroller	ATmega328
Feeding tension	5V
Recommended Input Voltage	7-12V
Input Limit	6-20V
Digital pins	14 (4 con PWM)
Analog inputs	6
Maximum current per pin	40 mA
Communication	TWI y SPI
Flash memory	32 KB
SRAM	2 KB
EEPROM	1 KB
Clock Speed	16 MHz

C. *Reader RC522*

This type of RFID reader is based on the MFRC522 integrated circuit used for wireless communication at a frequency of 13.56Mhz. This device is operated under the international standard ISO 14443A and operates with a 3.3v supply voltage. Table 3 below shows some features of this device:

TABLE 3
RFID RC522 Module Technical Specifications.

Characteristics	Settings
Feeding tension	3.3V
Operating Current	13-26mA
Standby Current	10-13mA
Sleep-mode current	<80µA
Maximum current	30mA
Operating Frequency	13.56Mhz
Reading distance	0 a 60mm
Communication protocol	SPI
Max data rate	10Mbit/s
Operating temperature	-20 a 80ºC

D. *Power Supply*

The power supply in any electronic circuit is undoubtedly one of the most important devices that must be considered, since its main function is to provide the energy necessary to put into operation all the modules and elements that are part of a system.

The most important parameters that are taken into account in a power supply are undoubtedly the output voltage and especially the current that will deliver the same. In order to do this, it is necessary to consider the operating current of each of the elements that form part of the access control system, as indicated in Table 4:

TABLE 1
Operating current of each device.

Elements	Operating Current	Quantity
Arduino MEGA 2560	93mA	1
Arduino Ethernet	80mA	1
LCD graphic display	20mA	1
Matrix keyboard	5mA	1
RFID Module	15mA	1
LED Diodes	15mA	3
5v Relay	15mA	1
NPN 3904 Transistor	10mA	1
Horn	5mA	1
Total	**288mA**	

From the current value obtained, the design of the source, which is based on a full-wave bridge rectifier, is performed, this type of power supply has a great advantage over others, since it allows to take advantage of both the positive half-cycle and the negative, thus having a constant pulsating current output as shown in Fig. 7:

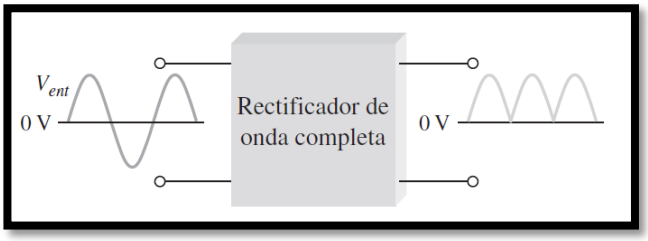

Fig. 7 Wave type generated by full-wave rectifier

The source will use a high-value capacitor, making it have a low curl percentage, however this can be further reduced by combining the capacitor with a voltage regulator. For this case, two voltage regulators, 5V and 8V, are used to cover the power requirements of the motherboard, which is supplied with a recommended voltage of between 7V and 12V through its external connection. In the meantime the 5V will be used for power supply through its internal connection terminal, in addition to other devices and modules that operate under this voltage range. In addition to the two regulators a current regulator circuit is also used for the connection and charging of a backup battery.

E. *General Scheme*

Next, Fig. 8 shows the general scheme of the access control system with all the blocks and elements that make it up:

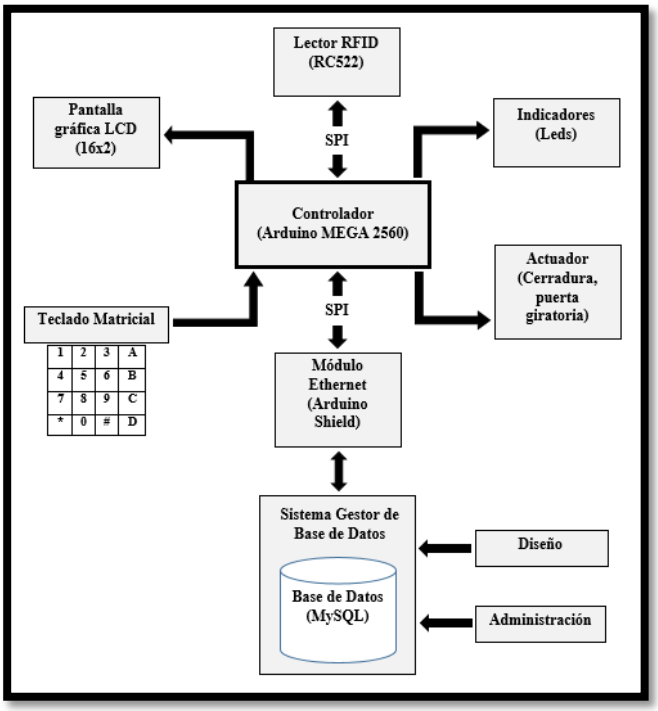

Fig. 8 General Scheme of the system.

V. SOFTWARE DESING

The system and all its components must be configured properly for its correct functionality, in addition to the connection and interoperability with the database and the information contained therein. Specifically, the following requirements must be met:

- Availability and user-friendly interface
- Logging interface for administration
- Display information

For programming the motherboard (Arduino MEGA 2560) you should consider some libraries that facilitate the use of different devices and modules that are integrated into the system. In this case the following will be used:

- Library SPI (#include <SPI.h>)
- Library Ethernet (#include <Ethernet.h>)
- Library RFID (#include <MFRC522.h>)
- Library Matrix keyboard (#include <Keypad.h>)
- Library LCD (#include <LiquidCrystal.h>)
- Library RestClient (#include ”RestClient.h”)

The use of these libraries causes the system to interact properly with other devices, based on the functionality and programming that is performed.

As can be seen in Fig. 9, after the declaration of variables and initialization of modules, there are two processes, one for validation of the tag code and the other for the key by keyboard. For both processes, the validation will be almost the same since both code and key are stored in the database.

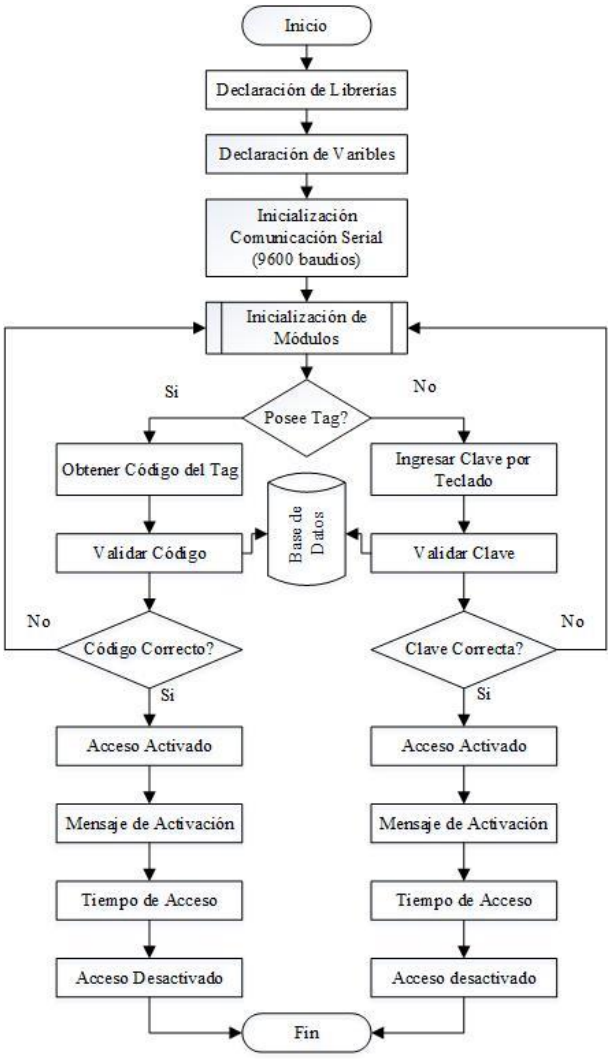

Fig. 9 Flow diagram of the operation of the Access Control System

A. Sending and receiving data

The system operates under the exchange of information delivered by the user and validated in the database. The user at the time of making a record causes the system to store that record in a variable, which will be sent as a request to a PHP module, which will execute the request through a TCP / IP communication, where the information will be stored In an IP datagram with source information and destination of the packet, which will be communicated through specific ports, in this case will be ports 80 and 443 for Apache and port 3306 for MySQL. The request submitted by PHP is processed by MySQL and sends the information back to the PHP module. Finally PHP is responsible for communicating to the system processor the results of the request, which generate the action in the system. Fig. 10 below shows the process of interacting the database with the system through PHP:

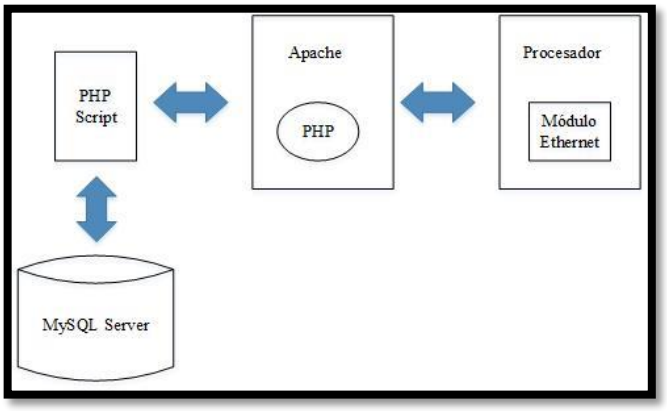

Fig. 10 Schema of interaction of the database through PHP.

The process of sending information from the system is done using the POST method to PHP. This method is characterized by sending the data in a hidden way, that is, the data sent from the form are not visible in the URL, but they are recoverable using the appropriate instructions [4].

The data sent through the POST method are available in variables called superglobales, because they are always usable throughout a PHP script [5].

Within the access control system the codes and keys of the reader and keyboard respectively will be stored in vector to later transform them into a string and associate them with a prefix that facilitates the search of information through PHP.

VI. CREATING TABLES IN MYSQL

The creation of tables in MySQL is done through the manager phpMyAdmin, this manager is a program that operates under free license providing a graphical web tool for the creation and management of databases

For the development of the database that will contain the information of the users of the access control system, the following tables will be used:

A. Table "login"

This table contains user data and password, with which the administrator can enter the main page, in order to prevent anyone from entering the page. It contains three fields: id, user and password, from where the information stored in the user and password fields will be the ones that validate the entry to the main page. Fig.11 below indicates the structure of the login table:

#	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 Structure of the table "login".

B. Table "usuarios"

The users table will contain all the data and personal information of each of the users of the access control system. This table contains the following fields:

- Id. - this field will be unique and unrepeatable and will identify each user.
- Nombre. - This field will contain the name and surname of each user.
- Correo. - The email field will have the pertinent information to each user's email address.
- Tag. - In this field, the unique code of the electronic card must be stored.
- Clave. - Just like the previous field, this field contains a unique key.
- Cedula. - Here the user ID number will be stored here.
- Rol. - This field describes the role played by each person who will make use of the access control system.

Each of these fields must be created with a specific variable type and value as shown in 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 Structure of the users table.

The administrator will have to enter the data through the phpMyAdmin manager, or in turn, through an HTML template that helps to register a much faster users

C. Table "registros"

Within the records table will store certain information of the user who has made use of the system. The specific information within this table will be stored in the following fields:

- Id.- field used for the identification of each user.

- Tag.- this field will contain the names of the users that have accessed through the access control system.
- Hora.- Here the time is stored in which the user has made his registration of entrance.
- Fecha.- The date in which the user registers access is stored.

The type and value assigned for each of these fields is shown below in 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 Structure of the records table

D. *Table "no registrados"*

The information that contains the unregistered table is the code of the electronic card that is not registered in the users table and is to be registered for a new user. To do this, it will show this code in the HTML template a field where you can view the last reading of a tag that has not yet been registered, this is done in order that the administrator can easily add a new user to the system. The structure of the "no registrados" table is shown in Fig. 14 below:

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

Fig. 14 Structure of the table "no registrados".

E. *Table "visitantes"*

The "visitantes" table contains information relevant to the people who need to enter the campus and do not have an identifier or a password, so a registration is made and access is granted. In this way the system keeps the register not only of the users, but also allows to carry a control of those people who do not have information stored in the database. Fig. 15 below shows the structure of the "visitantes" table:

#	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 Structure of the table "visitantes".

VII. FUNCIONALITY TEST

A. *Electronic Card Code Reading Testing*

The first prototype was designed solely to read the code of the electronic cards, in order to obtain the serial number and then store it in the database. Fig.16 shows the reading of a tag in which a code, which belongs to the section of the serial number, is visualized according to the specification of the EPC standard.

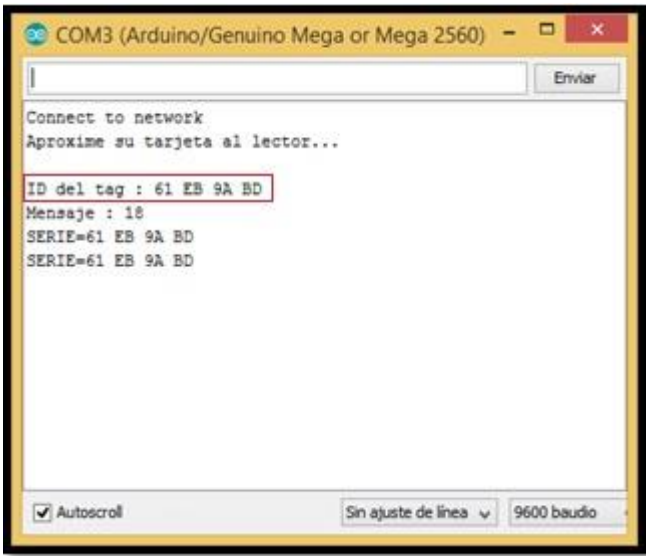

Fig. 16 Reading RFID Card Code.

The EPC standard indicates that the section of the serial number has a length of 36 bits, which are expressed in hexadecimal form, according to this, the information in the database must be stored in the same format, so that there is no inconsistency at the time of its validation.

B. *Matrix keyboard operation tests*

Like the RFID reader, the functionality of the matrix keyboard was checked separately, trying to make a correct code that can later be adapted to the rest of the system.

The anti-rebound method that is used facilitates the operation of the keyboard and its library, ensuring that there are no problems with the rest of the devices in the system, by first pressing the button that activates the subroutine only until entering the key, after This terminates the subroutine and executes the rest of the program normally, as shown in Fig. 17:

Fig. 17 Activation of subroutine for keyboard input.

If the code entered by the keyboard is correct, a response will be obtained by the server through the system, allowing access, as indicated in Fig. 18:

Fig. 18 Enter key correctly through the matrix keyboard.

On the other hand, if a wrong key is entered there will be no response from the server, and therefore access will be denied, as shown in Fig. 19:

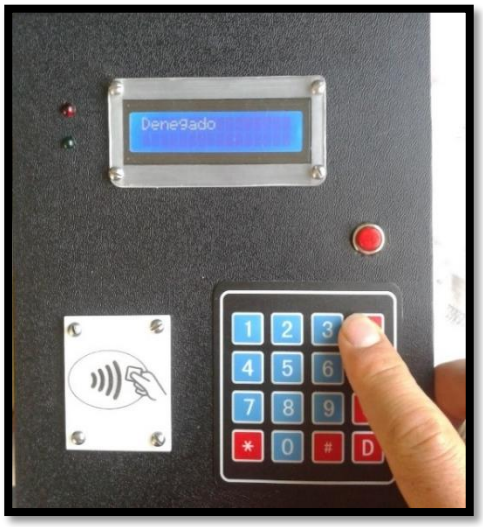

Fig. 19: Incorrect key entry using matrix keyboard.

C. Login to the admin page by user and password

It was necessary to create a web page as indicated in Fig 20, which serves to register users to the system, however, if the page does not have a user validation process and password, it is likely that any unauthorized person can enter to it and make unauthorized records.

Fig. 20 User login page and password.

In case erroneous data is entered, a message will be displayed indicating that the entered data was incorrect and must be entered again, as shown in Fig. 21:

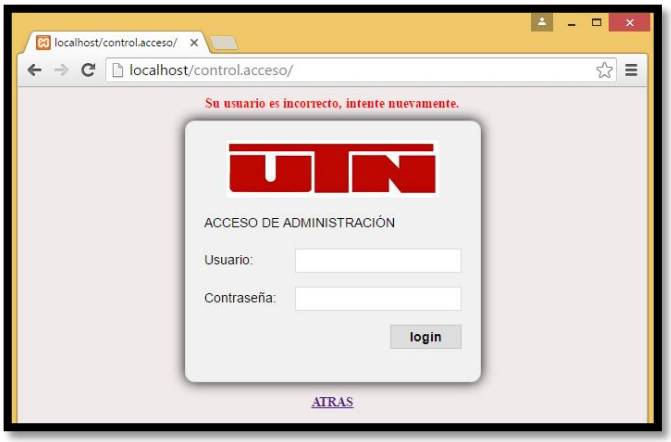

Fig. 21 Incorrect user login and password.

D. Registration of users in the database

Users can be registered through the phpMyAdmin manager, as well as through the web interface of the system, for this you must access either of the two sites. If you want to enter users through the web page, the database must be connected to the rest of the electronic system, since the code of the unregistered tag will be obtained through the RFID reader.

If it is done the read to an unregistered card, the server will not send any response and access will be denied, as shown in Fig. 22:

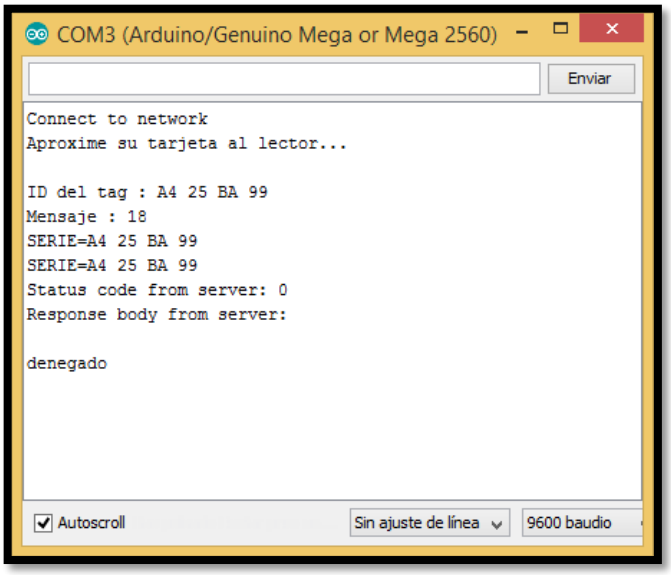

Fig. 22 Unregistered card reading.

In this case if you want to register the user with that card, you must access the web page and enter the relevant data and in the tag selection option you can display the last reading made, this case will be that of the unregistered user. Once the code has been selected, user data is entered as shown in Fig. 23:

Fig. 23 Login of user data through web page.

If the log was properly performed, a full log message will be displayed, as shown in Fig. 24:

Fig. 24 Full log message.

Finally it can be verified that the user has been added to the database and this way access will be allowed. Fig.25 shows the reading message of the tag, after having been registered:

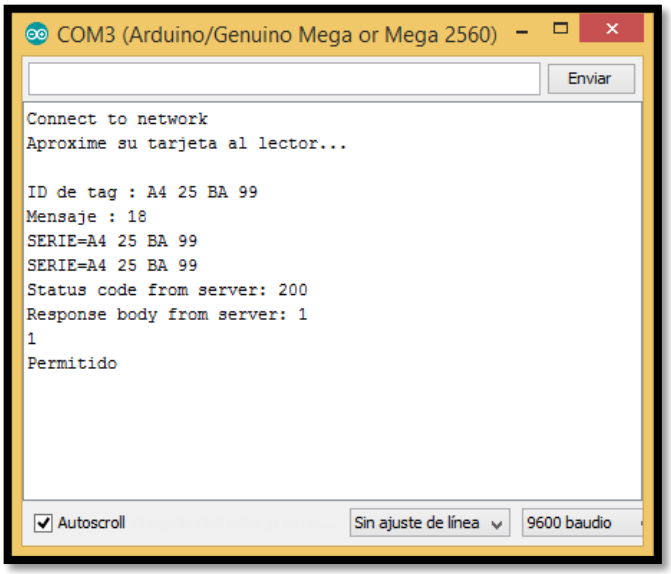

Fig. 25 Registered card reading.

VIII. ECONOMIC ANALYSIS

For the economic analysis of the system, all the costs involved in the elaboration of the system must be considered, as detailed in Table 5. These costs must justify the benefit of the project development towards the users.

TABLE 5
Total cost of access control system.

Description	Quantity	Value	Total
Hardware	5	$ 185,96	$929,80
RFID tags	9000	$ 1,00	$ 9000,00
Software	1	$ 0,00	$0,00
Plating	5	$ 7,15	$35,75
Assembly of circuits	5	$ 16.20	$81,00
Server and interconnection elements	1	$ 2144,95	$ 2144,95
Workforce	1	$2800,00	$2800,00
TOTAL			**$14991,50**

The benefits that are obtained when designing an access control system is to allow the regulation of the admission of authorized persons to the university campus, in order to reduce the thefts that occur within the university because of people Outside the same that can easily enter the campus. Among other aspects can also be considered the fact of having a flexible system, which can be adapted in order to improve its performance and functionality, at an affordable cost.

IX. CONCLUSIONS

The access control system for the Técnica del Norte University was designed based on radio frequency identification technology, in order to have an adequate control in the entrance, through the registry of users, and the validation of a unique code within of an electronic card or a personal key through TCP / IP communication with the information stored in a database.

The access control system allows to take an adequate control of the people who enter daily to the University, generating a practical alternative to the problems related to robberies inside the institution, since they will not be able to enter people outside the same, without before perform a respective entry record.

Among the main aspects to be considered in the design of an access control system are the type of technology to be used and the number of users that will handle the same, It is so the Universidad Técnica del Norte to be an institution that grows day and day and has a high rate of people who travel on campus, requires a large number of identifiers, and just a practical solution to this is the use of radio frequency identification technology, which according to international standards and specifications can get to get about 68 billion of codes, making this technology one of the most used and reliable

The technology that best adapts to the development of an access control system for the Técnica del Norte University, is undoubtedly a system based on RFID technology, which is one of the most flexible in terms of its functionality through The use of fully compatible libraries with free hardware boards, in addition to their cost and availability in the market. Allowing users to carry the tag as an identification card for another type of management within the University.

The installation and use of MySQL facilitates the administration of a database, being able to verify its functionality in the handling and response of reading of the information, besides its flexibility to adapt and operate together with an electronic system, and to provide ease of management and multiplatform support.

Arduino as a free hardware tool has become a very broad and flexible platform, which allows users to develop electronic control and automation projects through the use of different devices and modules, which adapt to the application you want to give, such is the case of the access control system, in which there was no problem of incompatibility or malfunction of the same, with the RFID module and the Ethernet module.

The system performance tests were based mainly on the interoperability of the electronic system with the database, so it was necessary to perform tests in different phases, which were focused on the functionality of the Ethernet module that allows the connection with the base Data through TCP / IP communication, and the RFID reader by reading the tag code and validating it with the database, as well as entering the key using the keyboard.

The costs generated for the development of the project support its operation, since it has a system adapted to the needs and requirements of the Technical University of North, with the purpose of providing security guarantees to users, through the control and registration of the same.

X. REFERENCES

[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: Eureca Media, SL.

[6] Gidekel, A. (2008). Introducción a la Identificación por Radio Frecuencia. Telectrónica 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. Was born in Atuntaqui – Ecuador on 9 March 1990. His primary studies realized them in the school "Andres Avelino de la Torre", his secondary studies in the “Technological Institute Otavalo". Student of the Technical University of North in the Faculty of Engineering in Applied Sciences, Career of Electronics and Communication Networks