Neiva, 15/06/2017

Señores

CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD SURCOLOMBIANA

Neiva, Huila.

El (Los) suscrito(s):

_SEBASTIAN TAMAYO RESTREPO_____, con C.C. No. _1.075.276.634_____,

_LADY VANESSA MORALES ROMERO_____, con C.C. No. _1.081.155.826_____,

_____, con C.C. No. _____,

_____, con C.C. No. _____,

autor(es) de la tesis y/o trabajo de grado o _____

titulado _SISTEMA DE CONTROL DE ACCESO A LOS AUDITORIOS DE LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD SURCOLOMBIANA USANDO TECNOLOGIA RFID_

presentado y aprobado en el año _2017_ como requisito para optar al título de

___INGENIERO ELECTRÓNICO_____;

Autorizo (amos) al CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN de la Universidad Surcolombiana para que con fines académicos, muestre al país y el exterior la producción intelectual de la Universidad Surcolombiana, a través de la visibilidad de su contenido de la siguiente manera:

- Los usuarios puedan consultar el contenido de este trabajo de grado en los sitios web que administra la Universidad, en bases de datos, repositorio digital, catálogos y en otros sitios web, redes y sistemas de información nacionales e internacionales “open access” y en las redes de información con las cuales tenga convenio la Institución.

- Permita la consulta, la reproducción y préstamo a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato Cd-Rom o digital desde internet, intranet, etc., y en general para cualquier formato conocido o por conocer, dentro de los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia.

- Continúo conservando los correspondientes derechos sin modificación o restricción alguna; puesto que de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación del derecho de autor y sus conexos.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, “Los derechos morales sobre el trabajo son propiedad de los autores” , los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.

EL AUTOR/ESTUDIANTE:

Firma: _____

EL AUTOR/ESTUDIANTE:

Firma: _____

EL AUTOR/ESTUDIANTE:

Firma: Vanessa Morales R.

EL AUTOR/ESTUDIANTE:

Firma: _____

TÍTULO COMPLETO DEL TRABAJO: sistema de control de acceso a los auditorios de la facultad de ingeniería de la Universidad Surcolombiana usando tecnología rfid**.**

AUTOR O AUTORES:

Primero y Segundo Apellido	Primero y Segundo Nombre
Tamayo Restrepo	Sebastian
Morales Romero	Lady Vanessa

DIRECTOR Y CODIRECTOR TESIS:

Primero y Segundo Apellido	Primero y Segundo Nombre
Quintero Polanco	Jesus David

ASESOR (ES):

Primero y Segundo Apellido	Primero y Segundo Nombre
Bravo Obando	Martin Diomedes
Molina Mosquera	Johan Julian

PARA OPTAR AL TÍTULO DE: Ingeniero electrónico

FACULTAD: Ingeniería

PROGRAMA O POSGRADO: Ingeniería electrónica

CIUDAD: Neiva **AÑO DE PRESENTACIÓN:** 2017 **NÚMERO DE PÁGINAS:** 61

TIPO DE ILUSTRACIONES (Marcar con una **X**)**:**
Diagramas **X** Fotografías **X** Grabaciones en discos___ Ilustraciones en general **X** Grabados___

Láminas___ Litografías___ Mapas___ Música impresa___ Planos **X** Retratos___ Sin ilustraciones___
Tablas o Cuadros **X**

SOFTWARE requerido y/o especializado para la lectura del documento: lector pdf.

MATERIAL ANEXO:

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o Meritoria)*:

PALABRAS CLAVES EN ESPAÑOL E INGLÉS:

ESPAÑOL	INGLÉS
Rfid	Rfid
Control de acceso	Access control
Radio frecuencia	Radio frequency
Base de datos	Databases

RESUMEN DEL CONTENIDO: (Máximo 250 palabras)

La implementación de nuevas tecnologías ha acelerado a grandes pasos el desarrollo del mundo. Entre esas tenemos las etiquetas RFID, esta tecnología lleva consigo un número único, el cual puede ser transmitido a través de ondas de radio, permitiendo identificar la persona o artículo en cualquier momento y lugar, para realizar una trazabilidad eficaz durante toda la etapa de identificación[1].

Este trabajo plantea el diseño e implementación de tecnologías que permitan garantizar la seguridad de las instalaciones y equipos, usando la tecnología RFID, proponiendo un sistema que permita controlar el acceso a los auditorios, de manera segura y eficaz, asimismo se toma en consideración el desarrollo, análisis y mejoramientos futuros del sistema de acceso.

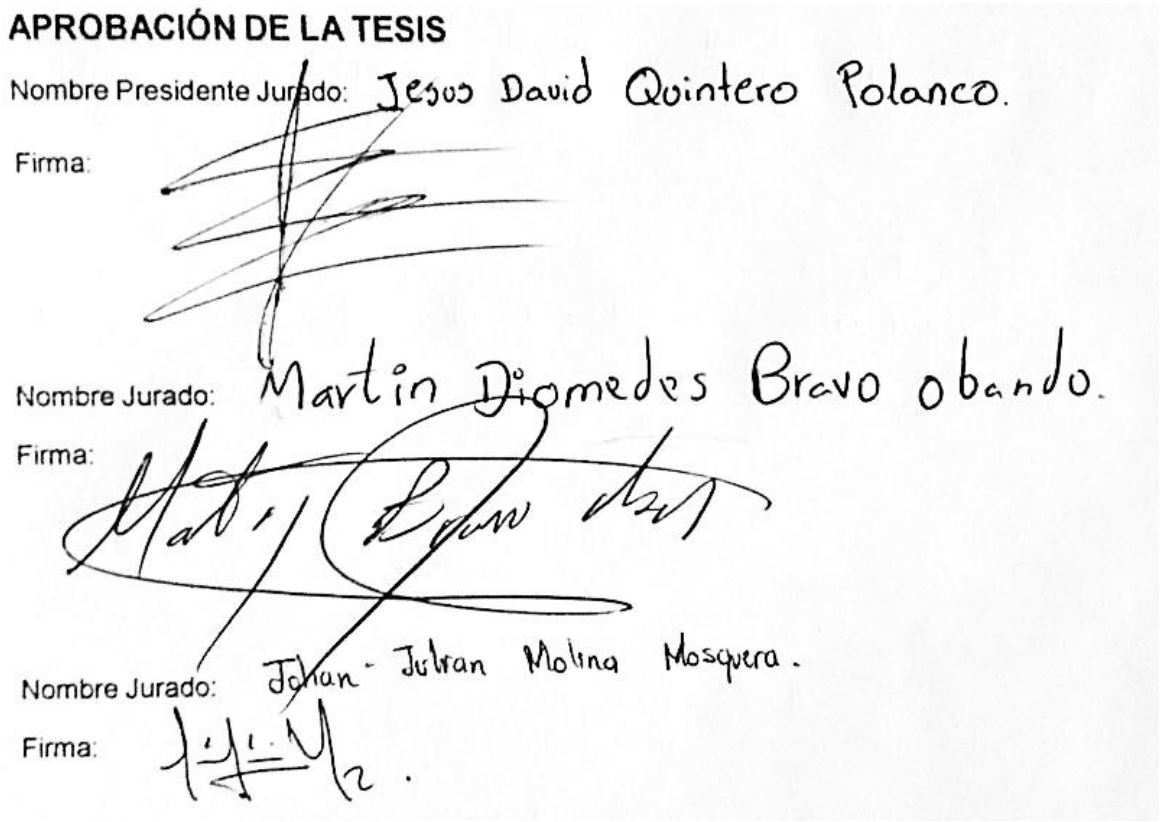
El documento está dividido en cuatro partes claves, en el primero se analiza los requerimientos necesarios para el desarrollo del proyecto, el segundo presenta el diseño del control de acceso y de la aplicación para escritorio, el tercero se basa en el desarrollo del sistema conociendo cada parte fundamental que constituye el control de acceso y por último se muestra la infraestructura del sistema y el funcionamiento del aplicativo web.

ABSTRACT: (Máximo 250 palabras)

The implementation of new technologies has accelerated the development of the world in great strides. Among these we have the RFID tags, this technology carries a unique number, which can be transmitted through radio waves, allowing to identify the person or article at any time and place, to perform an effective traceability throughout the identification stage[1].

This work proposes the design and implementation of technologies to guarantee the safety of installations and equipment, using RFID technology, proposing a system that allows control of access to the auditoriums, in a safe and effective way, also taking into consideration the development , Analysis and future improvements of the access system.

The document is divided into four key parts, the first one analyzes the requirements necessary for the development of the project, the second presents the design of access control and the application for desktop, the third is based on the development of the system knowing each Fundamental part that constitutes the control of access and finally it shows the infrastructure of the system and the operation of the web application.


APROBACIÓN DE LA TESIS

Nombre Presidente Jurado: Jesus David Quintero Polanco.

Firma:

Nombre Jurado: Martin Digmedes Bravo obando.

Firma:

Nombre Jurado: Johan - Julian Molina Mosquera.

Firma:

SISTEMA DE CONTROL DE ACCESO A LOS AUDITORIOS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD SURCOLOMBIANA USANDO TECNOLOGÍA RFID

SEBASTIAN TAMAYO RESTREPO
LADY VANESSA MORALES ROMERO

UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE INGENIERÍA
NEIVA
2017

SISTEMA DE CONTROL DE ACCESO A LOS AUDITORIOS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD SURCOLOMBIANA USANDO TECNOLOGÍA RFID

SEBASTIAN TAMAYO RESTREPO
LADY VANESSA MORALES ROMERO

Trabajo de grado presentado como requisito
Para optar al título de Ingeniero Electrónico.

Director
Jesús David Quintero Polanco
Ingeniero Electrónico

UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE INGENIERÍA
NEIVA
2017

Nota de aceptación:

_____

_____

_____

_____

Firma del jurado

Firma del jurado

Neiva, 09 de Junio **de 2017.**

AGRADECIMIENTOS

Gracias a Dios por brindarnos el temple y la sabiduría para sacar este proyecto adelante, a nuestras familias que siempre estuvieron presentes para llenarnos de ánimo y no desfallecer, de igual manera a nuestros compañeros que nos ayudaron a dar solución a problemas que se iban presentando en el camino.

Un agradecimiento muy especial para la Universidad Surcolombiana, por el apoyo económico que nos brindaron para llevar a cabo este proyecto que moderniza la facultad de ingeniería, al colega Joan Sebastian integrante de CTIC “recursos de redes de la universidad” por su gestión en el enlace de este proyecto a la red de la USCO.

Cabe resaltar el acompañamiento de los jurados y director de tesis, Jesús David Quintero, por su apoyo y orientación para la realización de este proyecto.

Por último y no menos importante agradecemos a nuestros Padres, que con su apoyo, motivación y sabios consejos, nos impulsaron para sacar a luz un buen proyecto para destacar nuestra buena calidad como ingenieros.

Después de Dios porque soy consciente que todas y cada una de mis bendiciones son gracias a su presencia en mi vida, el primer agradecimiento quiero hacerlo llegar a los principales impulsores de mis sueños, pues sin ustedes mis padres, mis hermanas y mi abuelita no hubiese podido conseguir que entre muchos vaivenes de la vida lograra alcanzar la meta, mi carrera profesional, que primero fue su sueño, luego el mío y juntos hoy lo vemos materializado, también debo agradecer a mis amigos que con el paso del tiempo se convirtieron en hermanos y a esa persona que estuvo luchando conmigo, a mi lado durante tanto tiempo, esto jamás sería posible sin ustedes ¡ Esto es por y para ustedes!

Lady Vanessa Morales Romero.

Agradecido con mi Dios todo poderoso, familia y las personas que hicieron esto posible.

Sebastian Tamayo Restrepo.

CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

HTML: *HyperText Markup Language* (lenguaje de marcas de hipertexto), hace referencia al lenguaje de marcado para la elaboración de páginas web.

ADMINISTRADOR: persona encargada de efectuar las reserva en el sistema y del monitoreo del sistema de acceso a los auditorios.

RFID: (Radio Frequency Identification, en español Identificación por radiofrecuencia) es un método de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas o tags RFID. Una etiqueta rfid es un dispositivo pequeño, como una pegatina, que puede ser adherida o incorporada a un producto, animal o persona. Las etiquetas RFID contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID.

APLICATIVO WEB: es la página que nos sirve para el gestionamiento de las reservas de los auditorios mediante la consulta a la base de datos de la universidad, es accesible por un navegador mediante una URL.

XAMPP: es un servidor independiente de plataforma, software libre, que consiste principalmente en el sistema de gestión de bases de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl.

LECTOR: es el modulo que nos permite realizar la lectura de los carnets para así poder procesar la orden de acceso.

NOOBS: es el paquete instalador del sistema operativo que contiene Raspbian

RASPBIAN: es una distribución del sistema operativo GNU/Linux y por lo tanto libre basado en Debian Wheezy para la placa Raspberry Pi, orientado a la enseñanza de informática.

ANGULARJs: es un framework MVC de JavaScript para el Desarrollo Web Front End que permite crear aplicaciones **SPA** *Single-Page Applications*.

FRAMEWORK: es un esquema (un esqueleto, un patrón) para el desarrollo y/o la implementación de una aplicación.

MVC: (Model-View-Controller) significa que “separa en tu aplicación la gestión de los datos, las operaciones, y la presentación”.

GPIO: (Entrada/Salida de Propósito General) es un pin genérico en un chip, cuyo comportamiento (incluyendo si es un pin de entrada o salida) se puede controlar (programar) por el usuario en tiempo de ejecución.

TAG: es una combinación de un transmisor y un receptor, que está diseñado para recibir una señal específica de radio y transmitir automáticamente una respuesta.

RASPBERRY PI: es un ordenador de placa reducida con múltiples funciones.

MySQL: es un sistema de gestión de bases de datos relacional desarrollado bajo licencia dual GPL/Licencia comercial por Oracle Corporation y está considerada como la base datos open source más popular del mundo, enfocada sobre todo para entornos de desarrollo web.

JAVA: lenguaje de programación utilizado para conectar a la base de datos y hacer consultas.

SWEET ALERT: es un sustituto de “alerta” de java script, que nos permite darle mejor presentación a nuestros mensajes de alerta para nuestro aplicativo web.

CSS: (*Cascading Stylesheets*) es un lenguaje de hojas de estilo para definir y crear la presentación de un documento estructurado escrito en un lenguaje de marcado. Es muy usado para establecer el diseño visual de las páginas web, e interfaces de usuario escritas en HTML.

ISO1443A: es un estándar internacional relacionado con las tarjetas de identificación electrónicas, en especial las tarjetas de proximidad, se describen dos tipos de tarjetas: tipo A y tipo B. Las principales diferencias entre estos tipos se encuentran en los métodos de modulación.

RESUMEN

La implementación de nuevas tecnologías ha acelerado a grandes pasos el desarrollo del mundo. Entre esas tenemos las etiquetas RFID, esta tecnología lleva consigo un número único, el cual puede ser transmitido a través de ondas de radio, permitiendo identificar la persona o artículo en cualquier momento y lugar, para realizar una trazabilidad eficaz durante toda la etapa de identificación[1].

Este trabajo plantea el diseño e implementación de tecnologías que permitan garantizar la seguridad de las instalaciones y equipos, usando la tecnología RFID, proponiendo un sistema que permita controlar el acceso a los auditorios, de manera segura y eficaz, asimismo se toma en consideración el desarrollo, análisis y mejoramientos futuros del sistema de acceso.

El documento está dividido en cuatro partes claves, en el primero se analiza los requerimientos necesarios para el desarrollo del proyecto, el segundo presenta el diseño del control de acceso y de la aplicación para escritorio, el tercero se basa en el desarrollo del sistema conociendo cada parte fundamental que constituye el control de acceso y por último se muestra la infraestructura del sistema y el funcionamiento del aplicativo web.

Palabras claves: RFID, control de acceso, radio frecuencia, base de datos.

---

[1] InformaticaHoy. Implementación de tecnología RFID [En Línea]. En: Informática hoy. 2007-2016 Disponible en internet: http://www.informatica-hoy.com.ar/rfid/Implementacion-de-Tecnologia-RFID.php.

ABSTRACT

The implementation of new technologies has accelerated the development of the world in great strides. Among these we have the RFID tags, this technology carries a unique number, which can be transmitted through radio waves, allowing to identify the person or article at any time and place, to perform an effective traceability throughout the identification stage[1].

This work proposes the design and implementation of technologies to guarantee the safety of installations and equipment, using RFID technology, proposing a system that allows control of access to the auditoriums, in a safe and effective way, also taking into consideration the development , Analysis and future improvements of the access system.

The document is divided into four key parts, the first one analyzes the requirements necessary for the development of the project, the second presents the design of access control and the application for desktop, the third is based on the development of the system knowing each Fundamental part that constitutes the control of access and finally it shows the infrastructure of the system and the operation of the web application.

Key words: RFID, access control, radio frequency, database.

---

[1] InformaticaHoy. Implementación de tecnología RFID [En Línea]. En: Informática hoy. 2007-2016 Disponible en internet: http://www.informatica-hoy.com.ar/rfid/Implementacion-de-Tecnologia-RFID.php.

INTRODUCCIÓN

En fábricas, laboratorios, bibliotecas, entradas de empresas y hasta en edificios públicos, los derechos de acceso deben controlarse. Esto se consigue por medio de la tecnología RFID.

Los sistemas RFID representan una opción fiable y exenta de mantenimiento para controlar los derechos de acceso. El personal autorizado obtiene acceso a un área con solo pasar una etiqueta RFID por un lector. Se pueden conceder y modificar derechos de acceso a ubicaciones específicas según sean necesario, y es posible bloquear aquellas etiquetas que se hayan perdido, permitiendo que no haya suplantación[2].

Actualmente las organizaciones se han preocupado por implementar tecnologías que les permitan garantizar la seguridad de sus instalaciones, equipos e información, desarrollando sistemas que se encarguen de limitar los accesos a ciertas áreas, monitorear las actividades del personal y prevenir perdidas.

El uso de soluciones basadas en tecnología RFID (Radio Frequency Identification) o Identificación por radio frecuencia, se ha convertido en una buena elección, puesto que ofrece una amplia gama de soluciones, las cuales son fáciles de adaptar a cualquier organización. Este tipo de tecnología permite el monitoreo, seguridad y también procesar los datos, almacenándolos en bases de datos con diversa información, como lo son las horas de entrada/salida, tipo de actividad, y autentificación de usuarios.

Por otro lado, se desarrolló e implemento una aplicación, la cual se encarga de manejar el hardware del lector y coordinar el proceso de autenticación de los usuarios registrados en la base de datos de la universidad. Dicha aplicación se desarrolló en JavaScript.

Este proyecto, está dirigido primordialmente a determinar los requerimientos estratégicos, cambios en los procesos, innovación, beneficios y los riesgos de implementación en un ambiente real; así, como su posible aplicación en conjunto con el sistema de control de acceso al campus universitario desarrollado en 2011.

---

[2] PeePrel+Fuchs. La tecnología RFID gestiona el control de acceso [En Línea]. En: Peeprel más Fuchs. Disponible en internet: http://www.pepperl-fuchs.es/spain/es/23763.htm

1. ANÁLISIS DE REQUERIMIENTOS

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad el acceso a los auditorios de la facultad de Ingeniería de la Universidad Surcolombiana, no cuenta con un control eficaz y confiable, ya que este se realiza con la intervención de una persona encargada de abrirlos a las horas establecidas, pero no se verifica si el auditorio ha sido separado con anterioridad, permitiendo el ingreso libre al mismo. Las repercusiones más notorias de esta situación son el deterioro de las instalaciones, la ocupación de estos cuando no se han asignado por parte de docentes y estudiantes entre otras.

Para solucionar estas falencias, la universidad se ve obligada a destinar anualmente fondos en sostenimiento de la estructura (pintura, mantenimiento aires y redes eléctricas), y la compra de implementos para la misma, sumando a esto el pago mensual de cuentas elevadas por consumo de energía eléctrica. Por esta razón viendo la necesidad de controlar el ingreso a los auditorios y aprovechando la ventaja en seguridad que brinda la tecnología RFID en este campo, se planteó una solución potencial basada en el diseño, desarrollo e implementación de un sistema que permita controlar el acceso a cada auditorio y llevar un registro de actividades que allí se realizan.

1.2 PLANTEAMIENTO DEL CASO

Se requiere crear un sistema de acceso que pueda leer tarjetas de identificación, extraer su UID (Código de identificación de usuario) y compararla con la que se encuentra alojada en la base de datos de la universidad junto a lo ordenado en el aplicativo web. Esto se hace una vez el administrador encargado del software efectué la reserva al docente o administrador con los datos del carnet que lo identifica como miembro del plantel universitario.

Al momento de ingresar la C.C (cedula de ciudadanía) que se encuentra en el carnet, el sistema debe ser capaz de identificar si el usuario está activo o inactivo, por medio de la consulta a la base de datos en tiempo real de la universidad surcolombiana, haciendo más confiable y seguro el uso de los auditorios.

La aplicación web debe suplir las necesidades de un sistema de gestión de acceso a los auditorios proporcionando información del usuario coincidente con la presentada por el mismo, además de cumplir con funciones especiales para la asignación de fecha, hora y actividad que se va a realizar en los auditorios y llevar un historial para un mejor control y seguimiento.

La aplicación no tiene la potestad de crear o eliminar usuarios pero si de editar o eliminar reservas, para una mejor comodidad para el usuario en caso de presentársele algún inconveniente y no pierda del todo su cupo de reserva.

Una vez efectuada la reserva por el administrador, el lector de carnets que se encuentra alojado en los auditorios debe procesar la información por medio de comunicación directa vía ethernet a la base de datos y paralelamente al aplicativo web para poder enviar una señal de control que de acceso al auditorio desactivando el electroimán.

1.3 ACTORES

Los actores son los roles empleados por usuarios del sistema, estos representan la actividad que cada usuario puede realizar. En la figura 1 se presentan los actores del sistema de control de acceso a los auditorios.

Figura 1. Actores control de acceso a los auditorios.
Fuente. Elaboración propia.

ADMINISTRADOR: Personal encargado de la administración del sistema, otorga las reservaciones a los usuarios.

USUARIOS: Profesores o administrativos activos en la base de datos de la universidad Surcolombiana, quienes por medio del aplicativo de escritorio podrán solicitar el uso de los auditorios de la facultad de Ingeniería.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar e implementar un sistema que permita controlar el acceso a los auditorios de la facultad de ingeniería de la universidad Surcolombiana mediante la implementación de un sistema de cerraduras electrónicas basadas en tecnología RFID.

2.2 OBJETIVOS ESPECÍFICOS

- Permitir o restringir la apertura de las cerraduras electrónicas que se instalarán en los auditorios Miguel Felipe Ospina y José Milciades Vargas Epia (auditorio de Ambiental).

- Diseñar una aplicativo bajo licencia de software libre que permita a las personas previamente autorizadas por el administrador reservar uno de los auditorios de la facultad, luego al momento de efectuar su uso, pase su carnet en el lector RFID y pueda desactivar la cerradura para tener su acceso.

- Implementar un botón como alternativa que permita abrir directamente la cerradura en caso de emergencias desde adentro del auditorio.

- Generar reportes con filtros del mes a consultar, de que usuario, para que y en que horarios ha usado cada uno de los auditorios.

- Facilitar la supervisión del uso adecuado de los auditorios de la facultad de ingeniería de la Universidad Surcolombiana.

3. SISTEMAS DE CONTROL DE ACCESO A AUDITORIOS

Un sistema de control de acceso a los auditorios, es en un conjunto de equipos que operan de forma óptima para la identificación de personas que pretenden acceder, también obtener información de quien efectúa la reserva, y conocer instantáneamente la incidencia con la cual lo reserva y el número de horas.

Es importante efectuar un buen estudio y diseño previo a cualquier instalación y puesta en marcha de un proyecto de seguridad y control de acceso como este. La adecuada integración de los dispositivos electrónicos en este caso la raspberry con los dispositivos electromecánicos como el electroimán permiten reducir drásticamente los costos de personal y el valor final del proyecto.

3.1. ELEMENTOS BÁSICOS DE UN SISTEMA DE CONTROL DE ACCESO A LOS AUDITORIOS.

Un sistema de control de acceso a los auditorios de la facultad, como se muestra en la figura 2, consta básicamente de cuatro elementos: carnet, reserva, lector, procesamiento de la información y componente de seguridad.

Figura 2. Sistema control de acceso a los auditorios.
Fuente. Elaboración propia.

El carné, permite identificar y diferenciar a cada usuario dentro del sistema si es administrativo o docente y si se encuentra activo o no en la base de datos de la universidad. Es esencial en esta parte del documento especificar que la base de datos que a la que fue enlazado el proyecto solo almacena administrativos y docentes, por ello alguien que se encuentre por fuera de este grupo, así tenga un carnet que lo identifique como miembro de la universidad como sería el caso un estudiante no podrá realizar reservación.

La reserva se efectúa cuando el administrador, pide el carné y verifica en el sistema si él se encuentra activo en la base de datos de la universidad o ya no por razones de vencimiento de contrato u otros, esta reserva se lleva a cabo en el aplicativo web.

El lector es el modulo encargado de capturar la información contenida en el carné y enviarla a la unidad de procesamiento de información la cual la relaciona con la base de datos y la reserva efectuada en el aplicativo web, para comparar si está dentro del horario establecido para hacer uso del auditorio.

El componente de seguridad (el electroimán), es el encargado de brindar la protección al auditorio en caso de que no se haya seguido el protocolo anteriormente mencionado, y si todo se ha hecho con normalidad permite el ingreso al recinto.

3.2 APLICATIVO WEB.

Este aplicativo web permite hacer el control de los accesos a los auditorios, cumpliendo con las siguientes expectativas:

✓ Ayuda a controlar y gestionar adecuadamente los carnets que se encuentren dentro de la base de datos de la universidad, efectuando la consulta con la posibilidad de permitir o restringir el acceso al recinto.

✓ Software único diseñado de manera que sea sencillo de operar y entendible permitiendo así la gestión y control de accesos, visitas, rango de horarios y frecuencia de uso mediante un reporte.

✓ Se diseñó con la posibilidad de expandirse para la implementación de toda la universidad acoplándose a las aulas y laboratorios.

4. DISEÑO DEL SISTEMA DE CONTROL ACCESO

A continuación se explicara el proceso de diseño de un sistema para el control de acceso de los auditorios de la facultad de ingeniería de la Universidad Surcolombiana.

Para el diseño del sistema, se optó por el uso de la tecnología RFID, teniendo en cuenta que la identificación del personal perteneciente a la comunidad universitaria se hace a través de carnés basados en esta tecnología, establecida por el estándar internacional ISO14443.

En la Figura 3, se observa un diagrama que describe el sistema, el usuario presenta el carné universitario al administrador, el cual extrae el número de identificación personal (cedula), inmediatamente lo ingresa en el aplicativo web para saber si se encuentra activo o no en la base de datos, una vez constatada la información se procede con la reserva en el horario que el usuario desee y la hora que esté a disposición, hecho lo anterior y llegada la fecha y hora en la que se realizó la reservación y el usuario se encuentre en el auditorio especificado inicia el trabajo del lector RFID, cuya labor consiste en leer el código UID presente en el carné que se está desplazando sobre él y en tiempo real mediante el dispositivo de control raspberry compara la UID (identificación único de usuario) que tiene cada carné con la cedula que fue asignada para la reserva en el aplicativo web, esta comparación que se lleva acabo está asociada a la información de la base de datos de la universidad, como estos dos parámetros están en conjunto es fácil hacer la comparación entre UID y cedula de un mismo usuario si esa comparación es correcta y además coincide con la hora y fecha en la cual está pasando el carné, entonces se da vía libre activando el electroimán para el acceso al auditorio.

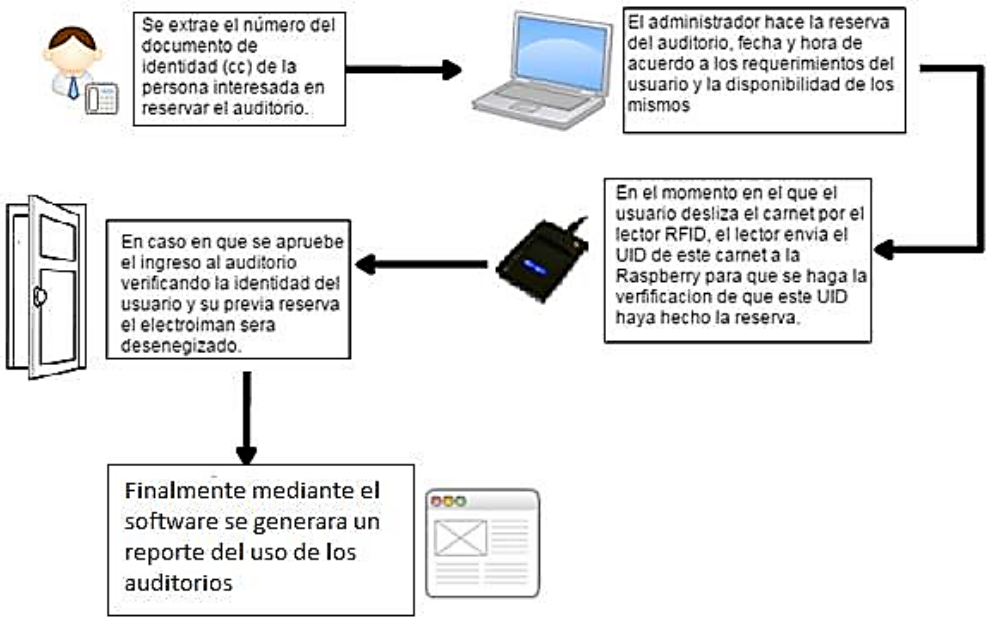


Figura 3. Diagrama de bloques del sistema de control de acceso.
Fuente. Elaboración propia.

4.1 REQUERIMIENTOS DEL SISTEMA

4.1.1 Requerimientos funcionales. El sistema debe estar en la capacidad de:

- ✓ Detectar los carnés cercanos al lector RFID y obtener su UID.
- ✓ Permitir el ingreso de los usuarios autorizados.
- ✓ Establecer conexión con el servidor que aloja la base de datos de permisos de acceso.
- ✓ Permitir agregar y eliminar permisos de acceso en tiempo real y generar registros de entrada de los auditorios.
- ✓ Brindar seguridad en caso de apagones de energía eléctrica.

4.1.2 Requerimientos no funcionales. Para que el sistema trabaje de forma adecuada se debe garantizar que:

- ✓ El lector RFID junto con la raspberry no se ubiquen sobre superficies metálicas o húmedas.
- ✓ La distancia entre la tarjeta y el lector RFID debe ser de 7 mm a 10 mm;
- ✓ El administrador encargado de los permisos deben tener conocimientos básicos en el manejo de aplicaciones web.

4.2 CASOS DE USO

En esta sección se presentan los diagramas de casos de uso. Un caso de uso es una descripción de las acciones de un sistema desde el punto de vista del usuario. Esta es una herramienta importarte que permite analizar los requerimientos del sistema desde el punto de vista de cada usuario.

4.2.1 Administración de permisos de acceso. En la Figura 4, se muestra el diagrama de casos de uso que describe las funciones y operaciones que realiza el sistema en el proceso de administración de permisos de acceso a los auditorios.

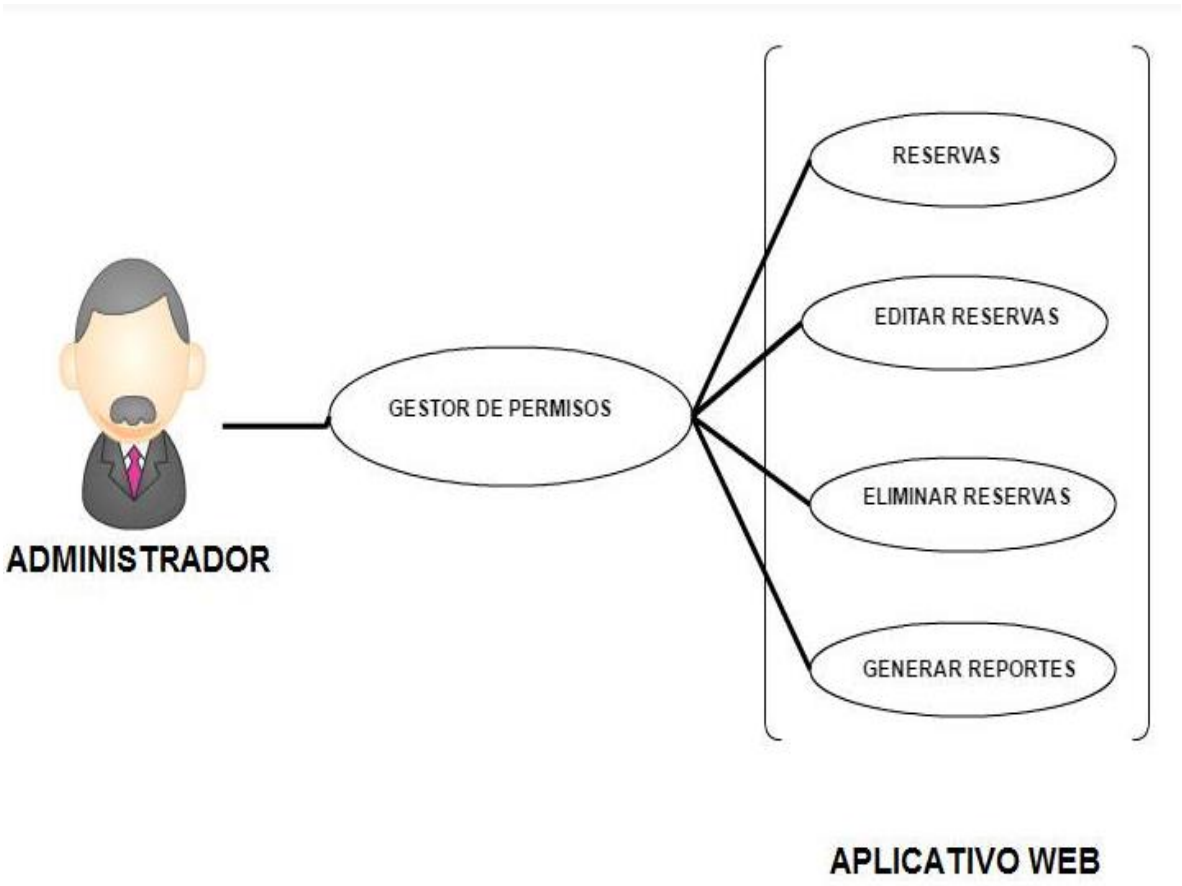


Figura 4. Diagrama de casos de uso administración de permisos de acceso.
Fuente. Elaboración propia.

A continuación se realiza una descripción concreta de cada uno de los casos de uso que envuelve al sistema en el proceso de administración de permisos de acceso.

Cuadro 1. Gestor de permisos.

Caso de uso: gestor de permiso.
Actor: administrador.
Función: administrar el sistema dando vía libre a las reservas
Descripción: la persona encargada de la administración del sitio puede efectuar la reserva al auditorio, exigiendo la identificación correspondiente que sería el carnet universitario en donde extraerá la identificación personal para posteriormente ingresarlo al aplicativo web donde constatara si está activo o no y proceder con la reserva en el horario indicado por el usuario, también posee la facultad de editar, eliminar y ver los reportes de las reservas hechas.

Cuadro 2. Manejo reservas.

Caso de uso: manejo permisos
Actor: administrador.
Función: controlar y supervisar el acceso a los auditorios
Descripción: el administrador puede registrar nuevos permisos de acceso a los auditorios. El sistema debe verificar que el horario esté disponible. También puede, revisar reportes de ingresos y eliminar reservas que ya no sean necesarios.

4.2.2 Acceso a las aulas. En la Figura 5, se muestra el diagrama de casos de uso que describe las funciones que realiza el sistema para permitir el acceso a los auditorios, así como su interacción con los usuarios involucrados en este proceso.

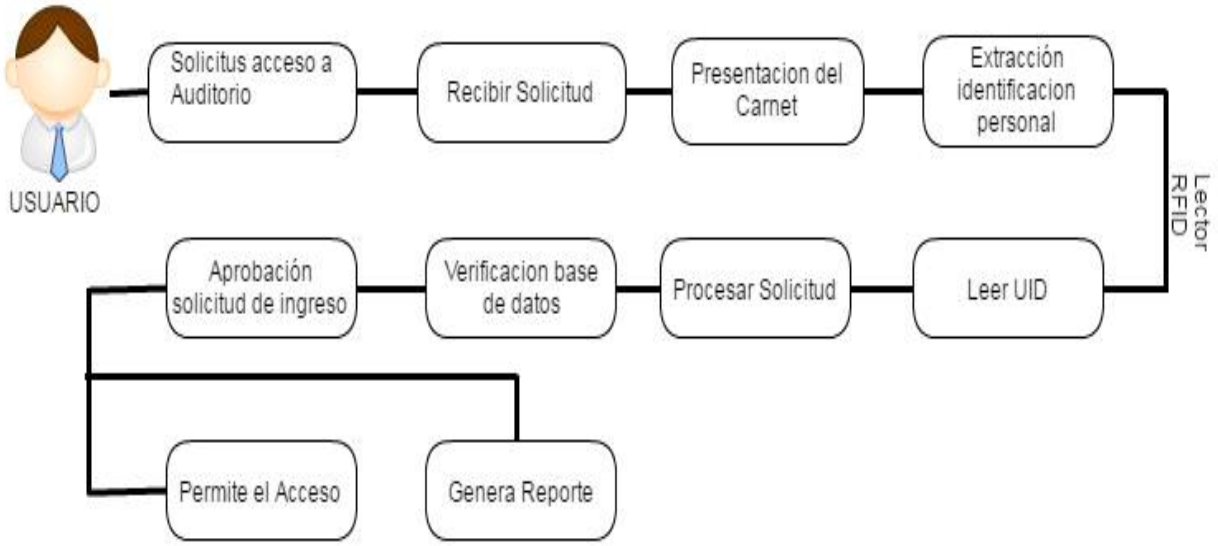


Figura 5. Diagrama de casos de uso acceso a los auditorios.

Fuente. Elaboración propia.

A continuación se realiza la descripción detallada de cada caso de uso que envuelve al sistema en el proceso de acceso a los auditorios.

Cuadro 3. Solicitud de acceso.

Caso de uso: solicitud de acceso
Actor: usuario.
Función: solicitar al sistema acceso a un auditorio.
Descripción: el usuario por medio de la identificación personal de su carné universitario, solicita al sistema acceder un auditorio.

Cuadro 4. Recibir solicitud.

Caso de uso: recibir solicitud
Actor: administrador
Función: recibir esa solicitud para procesarla en el aplicativo web
Descripción: el sistema recibe la solicitud del usuario mediante la identificación personal (C.C).

Cuadro 5. Procesar solicitud.

Caso de uso: procesar solicitud
Actor: - - - -
Función: el sistema determina si el usuario puede reservar el auditorio.
Descripción: el sistema se encarga de procesar la solicitud de permisos recibida, verificando si el usuario está activo dentro de la universidad para el ingreso al auditorio y si la fecha y hora de reserva está en un rango de disponibilidad. Para determinar si el usuario puede acceder al auditorio el sistema compara la UID del lector RFID del carnet del usuario con la identificación personal dada en el aplicativo web, si están asociadas ambos parámetros con el usuario en la base de datos de la universidad se procede al acceso.

Cuadro 6. Aprobar solicitud de acceso.

Caso de uso: aprobar solicitud de acceso
Actor: ------
Función: permitir acceso al auditorio.
Descripción: una vez el sistema verifica que el usuario tiene permiso de acceso, el sistema aprueba la solicitud y le permite acceder al auditorio con la deshabilitación del electroimán. Adicionalmente se genera un reporte con la fecha, hora y nombre del usuario.

4.3 DIAGRAMA DE CLASES

En el sistema de control de acceso están vinculados dos tipos de personas: el administrador y los usuarios a los que se le permitirá el acceso a los auditorios. Cada persona tiene un nombre una identificación y un UID obtenido de su carné que lo identifica como miembro de la comunidad universitaria. El administrador tiene asociado un nombre de usuario y una contraseña para el ingreso al aplicativo web y cada usuario del sistema tiene la facultad de poder hacer una solicitud de reserva.

El administrador del sistema puede encargarse del control de permisos de acceso. Los usuarios mediante el administrador interactúan con el sistema realizando solicitudes para acceder a un auditorio y llevar cabo su reserva.

La generación de permisos de acceso siempre dependerá de la existencia de auditorios desocupados a las horas establecidas por los usuarios. Así mismo solo podrán reportarse eventos de ingreso siempre y cuando exista un permiso de acceso.

En la Figura 6, se muestra el diagrama de clases que modela al sistema descrito anteriormente, sus componentes, funcionalidad y la relación existente entre cada uno de ellos.

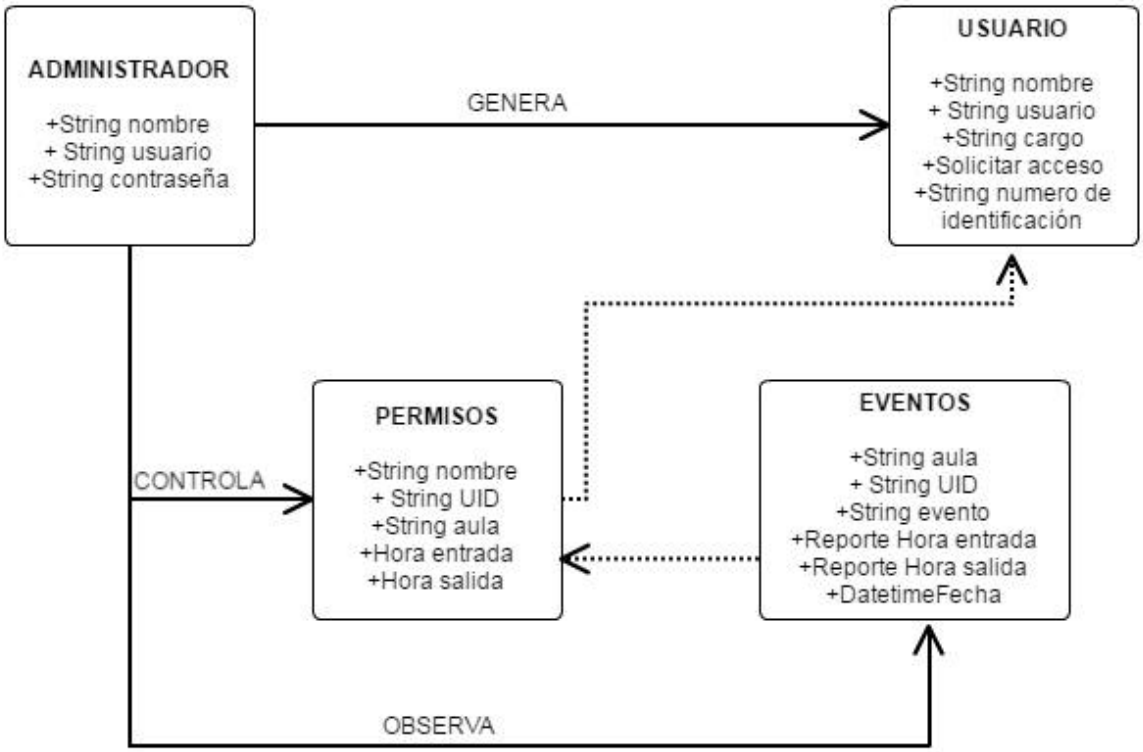


Figura 6. Diagrama de clases del sistema
Fuente. Elaboración propia.

5. DESARROLLO DEL SISTEMA

El sistema para el control de acceso a los auditorios de la facultad de ingeniera de la Universidad Surcolombiana que se muestra en la Figura 7, consta básicamente de cuatro etapas: solicitud del usuario, administración, lectura y control de reserva.

La etapa de solicitud del usuario, es cuando el usuario se acerca a la oficina del administrador del sistema para hacer la solicitud de reserva de un auditorio.

En la etapa de administración el sistema cuenta con un aplicativo web para la gestión de reservas enlazado a la base de datos de la universidad.

En la etapa de lectura el sistema cuenta con un lector RFID (sl030) que se encarga de detectar y leer el número de identificación único de usuario (UID) de los carnés, para luego trasmitir esa información por comunicación i2c a la raspberry pi.

Finalmente en la etapa de Control de reserva el sistema cuenta con la raspberry pi que se encarga de recibir la información que obtiene el lector RFID a través de la comunicación i2c del cual dispone; una vez la raspberry recibe la información del lector RFID este se comunica por el puerto Ethernet, enviando el dato de la UID del usuario para que sea procesado por el servidor de la universidad, el cual valida los datos que en él se encuentran almacenados en conjunto con el aplicativo web respondiendo con un comando para indicar si tiene permiso o no para acceder al auditorio; si existe el permiso, un script en Python programado en la raspberry activa el sistema de acondicionamiento, que se encarga de adaptar la señal a los niveles necesarios para la activación del electroimán. Por otra parte la alimentación de la raspberry pi es por corriente eléctrica, no está asociada al protocolo PoE (Power over Ethernet) el cual nos permite la alimentación por el cable de datos UTP.

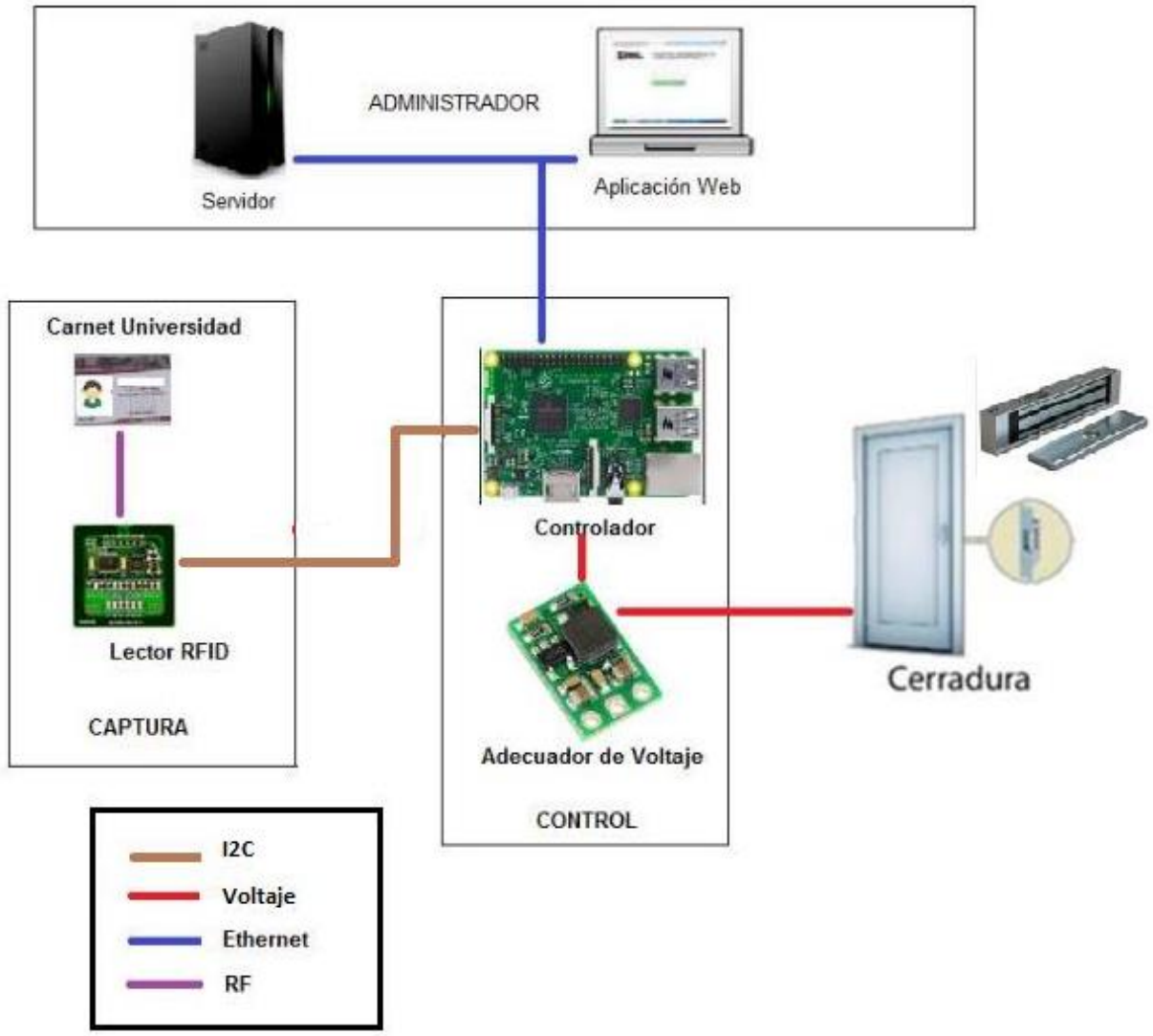


Figura 7. Arquitectura del sistema de control de acceso.
Fuente. Elaboración propia.

5.1 COMPONENTES FÍSICOS DEL SISTEMA

5.1.1 Carnés con tecnología RFID. Para la identificación de cada uno de los usuarios de la universidad dentro del sistema, se tomó en cuenta las tarjetas que ya se venían utilizando que son las MIFARE 4K, 4 byte UID, con los que se identifica a cada uno de los miembros pertenecientes a la comunidad universitaria.

Estas tarjetas cumplen con las tres primeras componentes de la ISO 14443A de 13.56 MHz con protocolo de alto nivel. Cuenta con una memoria EEPROM de 4Kbytes, organizada en 32 sectores de 4 bloques y 8 sectores de 16 bloques. El último bloque de cada sector contiene dos claves y condiciones de acceso programables para cada bloque en ese sector.

Figura 8. Carné RFID de la universidad Surcolombiana.

Fuente. Elaboración propia.

5.1.2 Modulo RFID. Para la selección del dispositivo encargado de la lectura de las UID de los carnets, se consideró que el sistema debería contar con un dispositivo lector de tarjetas compatibles con los tags de los carnets ya estipulados en la universidad para permitir el acceso a los auditorios.

Para la lectura de tarjetas de los usuarios (administrativos/docentes) que solicitan el acceso, se escogió el modulo lector/escritor MIFARE SL030 HF el cual se muestra en la Figura 9. Este módulo soporta el estándar ISO 14443 Tipo A de 13.56MHz e integra una antena y los elementos necesarios para la lectura/escritura de tarjetas.

Frecuencia	13.56MHz
Protocolo	ISO14443A
Etiqueta apoyo	MIFARE Ultralight®, NTAG203, MIFARE Mini, MIFARE Classic® 1K, MIFARE Classic® 4K, FM11RF08
Interfaz	I2C
Voltaje	2.5 - 3.6 VDC
Dimensión	38 × 38 mm

Figura 9. Lector/Escritor RFID SL030 HF STRONGLINK.

Fuente. http://www.stronglink-rfid.com/es/rfid-modules/sl030.html

Una de las características destacables del lector es que cuenta con una interfaz de comunicación i2c, la cual da la posibilidad de controlarlo por medio de la placa raspberry PI, opción que permite realizar operaciones tales como

- La detección automática de tarjetas cercanas.
- Extraer de manera automática el UID del carnet.
- Procesar la información obtenida de las tarjetas, enviando los datos por interfaz i2c a la placa raspberry pi.

Ahora se dará a conocer de forma detallada la composición del módulo con el cual se desarrolló el proyecto, lo referente a lo pines y la descripción de los mismos.

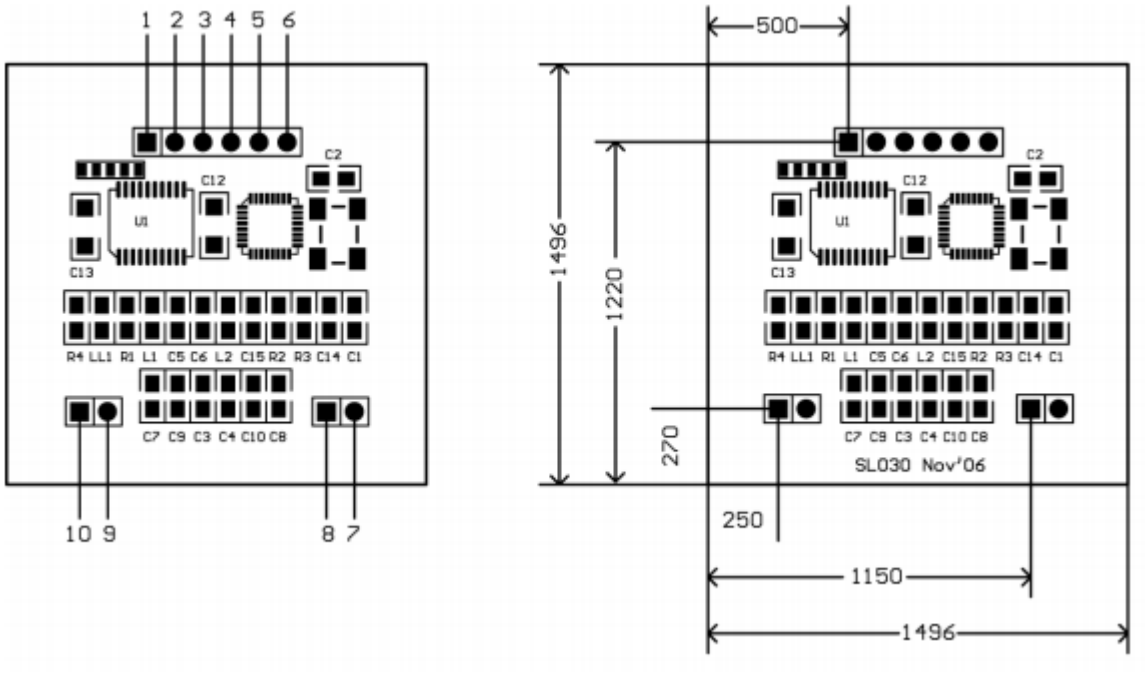


Figura 10. Información de los Pines.
Fuente. http://www.stronglink-rfid.com/download/SL030-User-Manual.pdf

Cuadro 7. Descripción pines módulo RFID.

PIN	SIMBOLO	TIPO	DESCRIPCIÓN
1	VDD	PWR	Fuente de alimentación, 2.5V a 3.6VDC
2	IN	ENTRADA	Flanco de activación SL030 del modo de apagado.
3	SDA	IN/OUT	Línea serial de datos.
4	SLC	ENTRADA	Línea serial de tiempo (Clock)
5	SALIDA	SALIDA	Tag detectar la señal bajo nivel que indica la etiqueta de alto nivel que indica la etiqueta cabo
6	GND	PWR	Tierra.
7	NC		
8	NC		
9	NC		
10	NC		

Fuente. Elaboración propia**.**

Ahora bien la realización de todas estas acciones se logran a través del envió de comandos desde el microcontrolador hacia el lector RFID.
A continuación se presentará la descripción de la acción que realiza el lector RFID.

Cuadro 8. Comando anfitrión de escritura del SL030.

Address	Len	Command	Data

Address: 1 byte, 0xA0
Len: 1 byte indicating the number of bytes from Command to the end of Data
Command: 1 byte Command code, see Table 3
Data: Variable length depends on the command type

Cuadro 9. Lectura del resultado del Host.

Address	Len	Command	Status	Data

Address: 1 byte, 0xA1
Len: 1 byte indicating the number of bytes from Command to the end of Data
Command: 1 byte Command code, see Table 3
Status: 1 byte Command status, see Table 4
Data: Variable length depends on the command type.

Cuadro 10. Comandos compacto.

No.	Comando	Descripción
1	0x01	Buscar tarjetas cercanas automáticamente
2	0x02	Lee automáticamente la UID de una tarjeta cercana
3	0x03	Almacena automáticamente la UID de la tarjeta en la EEPROM
4	0x04	Determina automáticamente si una tarjeta está almacenada en la EEPROM
5	0x05	Encuentra y elimina automáticamente la UID de la tarjeta de la EEPROM

Fuente. Elaboración propia**.**

Un comando básico consiste en tres o más bytes y se usa para que el lector realice acciones solo cuando se le solicite. Consta de un encabezado, el cual tiene un tamaño de un byte y valor estático hexadecimal de 0xAB; un campo longitud, que tiene un tamaño de un byte, y su valor abarca el número de bytes del campo longitud hasta el último byte del campo de datos; un campo de instrucción, cuyo valor varía dependiendo de la función que debe hacer el lector y tiene tamaño de un byte; un campo de datos cuyo tamaño depende de la función realizada por el lector; y un checksum que permite verificar que no haya error en los valores obtenidos.

El Cuadro 11 se observa la lista de instrucciones de los comandos básicos y la descripción de la acción que realiza el lector RFID.

Cuadro 11. Comandos básicos del lector RFID.

No.	Instrucción	Descripción
1	0x01	Lee el tipo de tarjeta
2	0x02	Busca la tarjeta y lee la UID
3	0x03	Lee los datos de la tarjeta
4	0x04	Escribir datos en la tarjeta
5	0x09	Leer datos de la EEPROM
6	0x0a	Escribir en la EEPROM
7	0x0b	Borrar datos de la EEPROM
8	0x0c	Verifica si se está escribiendo en la EEPROM
9	0x0d	Hablita/deshabilita la suma de verificación
10	0x0e	Configura la velocidad en baudios
11	0x0f	Volver la configuración por defecto
12	0x10	Volver al estado de espera

Fuente. Elaboración propia**.**

5.1.3 Configuración de la raspberry Pi 3 Model B. Como bien se ha venido mencionando, el centro de control se lleva acabo con la placa raspberry pi 3 model B, allí se centra la programación del módulo SL030 y la adecuación a las consultas a la base de datos de la universidad.

Para que se lleve a cabo todo este proceso, es necesario preparar y adecuar bien nuestro dispositivo madre para tener un óptimo rendimiento.

Como observamos en la Figura 11. La Raspberry Pi es un ordenador de placa reducida, con dimensiones de 85 x 54 milímetros, común mente se le ha denominado Mini PC ya que son una buena opción para disfrutar de toda la potencia de un ordenador pero recurriendo a un tamaño compacto, este modelo presenta unas características indudablemente mejoradas respecto a su antecesora (Pi 2) entre ellas, cuenta con conexión wireless LAN y bluetooth.

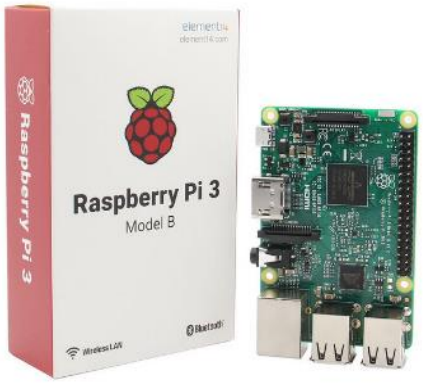


Figura 11. Raspberry Pi 3 Model B.
Fuente. http://img.dxcdn.com/productimages/sku_426431_5.jpg

Para el primer arranque de la placa raspberry pi, se debe tener un dispositivo de almacenamiento que hará la función de disco duro, en este caso se usaron tarjetas de memoria micro SD de 16 GB para cada una de las placas cumpliendo con el requisito mínimo de 4GB.

Una vez cumplido lo anterior se procede a descargar el paquete de instalación del S.O en la página oficial de raspberry (www.raspberrypi.org**)** y se da clic en la opción de descarga NOOBS.

NOOBS es un paquete que se encuentra incluido raspbian el Sistema operativo más optimizado para la tarjeta Pi, si se quisiera instalar otros S.O actualmente se encuentra NOOBS LITE es liviano y se podría usar como mediador para llevar acabo la instalación de cualquier otro sistema operativo.

Una vez descargado se descomprime y se utiliza el programa SDformatter, que prepara la MICRO SD eliminando impurezas o software que puedan afectar la instalación del S.O raspbian, luego se procede a descomprimir el archivo de descarga NOOBS sobre la tarjeta micro SD.

Ejecutado todo lo anterior se procede a insertar la tarjeta SD en la raspberry pi 3 para así comenzar la instalación como se aprecia en la Figura 12, con los parámetros que se quieran determinar.

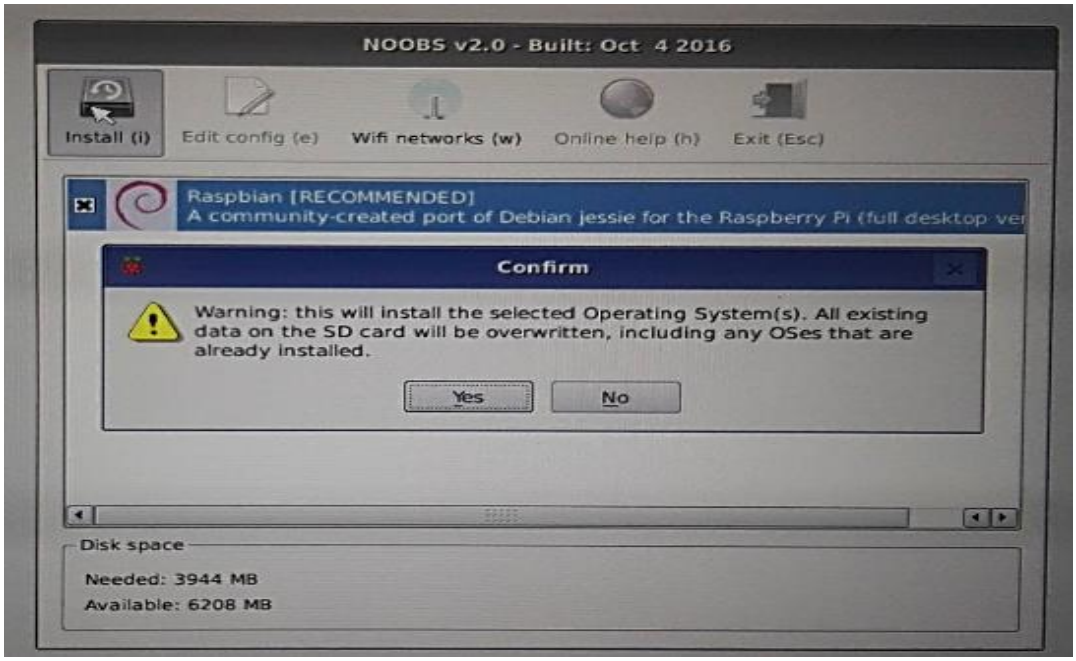


Figura 12. Visualización al encender por primera vez la raspberry.
Fuente. Elaboración propia**.**

Este es el pantallazo en el cual se debe seleccionar si realmente es ese el sistema operativo que se desea instalar y se procede a aceptar e iniciar la instalación.

Figura 13. Barra de estado instalación.
Fuente. Elaboración propia**.**

Después se muestra una barra de carga como vemos en la Figura 13, donde el tiempo aproximado de espera en el proceso de instalación del S.O es de 15 minutos. Mientras este proceso se está desarrollando la raspberry no debe ser desenergizada y en ningún momento se debe extraer la micro SD.

Una vez culminado el proceso anterior, el programa de instalación descomprime los paquetes como se observa en la Figura 14, para finalizar el proceso de instalación.

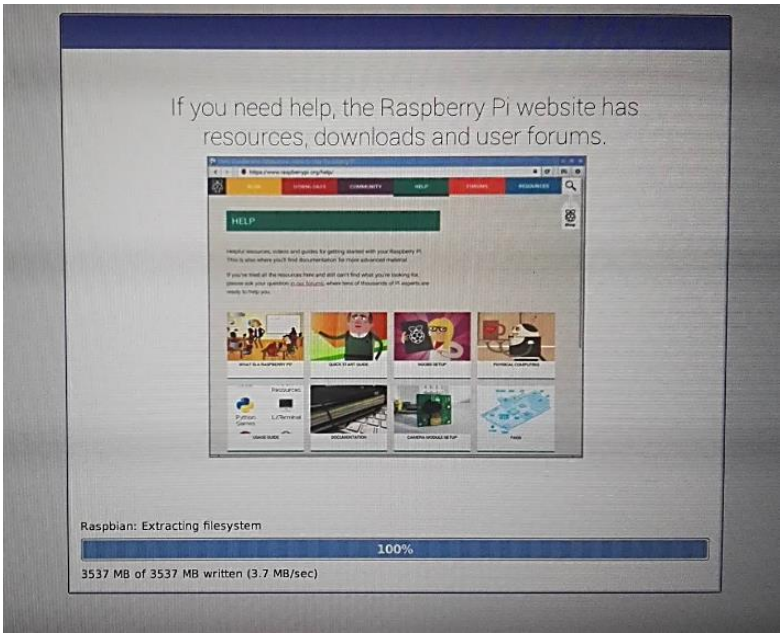


Figura 14. Proceso de extracción del sistema de archivos.
Fuente. Elaboración propia**.**

Por ultimo arroja un pantallazo visualizado en la Figura 15, con el cual comunica que la instalación se ha realizado con éxito, se selecciona OK y se puede empezar a programar.

Figura 15. Aviso del proceso de instalación terminado.
Fuente. Elaboración propia**.**

Una vez realizado todo este proceso se puede iniciar el trabajo para avanzar a la siguiente fase del proyecto, en la figura 16. Se puede apreciar el entorno del S.O Raspbian.

Figura 16. Escritorio del sistema operativo instalado.
Fuente. Elaboración propia**.**

5.1.4 Acondicionador de voltaje. En la Figura 17, se muestra el circuito diseñado para acondicionar las salidas GPIO de la raspberry pi para poder operar la activación/desactivación del electroimán cuando sea pertinente.

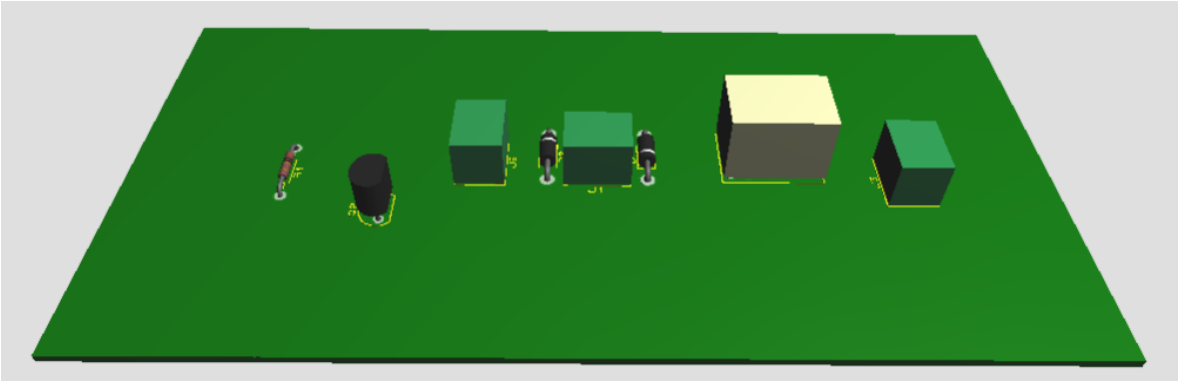


Figura 17. Circuito de acondicionamiento.
Fuente. Elaboración propia**.**

El circuito diseñado cuenta con la configuración del transistor en corte – saturación, ya que esta es una forma de poder controlar un Relé, (activar/desactivar), que es lo que se necesita para operar el electroimán mediante una señal de control del GPIO asignado en la raspberry pi.

La configuración que se presenta depende de la cantidad de corriente que pase por su base, cuando no pasa corriente por la base, no puede pasar tampoco por sus otros terminales; se dice entonces que el transistor está en corte, es como si se tratara de un interruptor abierto. El transistor está en saturación cuando la corriente en la base es muy alta; en ese caso se permite la circulación de corriente entre el colector y el emisor y el transistor se comporta como si fuera un interruptor cerrado.

La representación más básica se muestra en la figura 18, donde de forma explícita muestra la forma de operación.

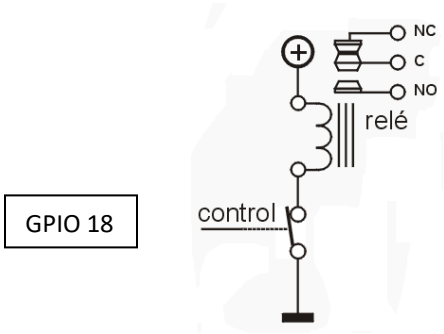


Figura 18. Diagrama Eléctrico etapa control.
Fuente. Elaboración propia**.**

Para controlar un relé nos sirve saber solamente que la base del transistor debe superar los 0,7V para que este entre en conducción y que la corriente que el transistor dejará pasar entre emisor y colector puede depender de la corriente que entra por la base multiplicado por la ganancia en continua característica del transistor (hFE).

- $V_{Rele} = 5V - V_{CE}(0.2v)$

  Para Relés de 5v pequeños como el que utilizamos, la I_{bobina}=50mA
  Donde la $I_{bobina}=I_{saturacion}$

$$Isat = \frac{5v - 0.2v}{R}$$

$$R = \frac{4.8v}{50mA} = 100\Omega$$

Para asegurar I_{sat}-I_b=1mA

Por tanto,

$$1mA = \frac{3.3v - 0.7v}{Rb}$$

$$Rb = \frac{3.3v - 0.7v}{1mA} = 2{,}6K\Omega$$

Tenemos que la resistencia de base es de 2,6Kohm.

Existe también un cuadro en el cual dependiendo del tipo de relé o tensiones de control, presenta el valor de Rb.

TIPO DE RELÉ	TENSION DE CONTROL (FAMILIA LÓGICA)			
	1,8V (LVCMOS)	3,3V (LVCMOS, LVTTL)	5V (CMOS, TTL)	12V (CMOS)
relé 5V pequeño (I = 50mA)	1,2K	2,7K	4,7K	12K
relé 5V medio (I = 100mA)	680	1,2K	2,2K	5,6K
relé 12V pequeño (I = 25mA)	2,2K	4,7K	8,2K	22K
relé 12V medio (I = 50mA)	1,2K	2,7K	4,7K	12K
relé 12V grande (I = 100mA)	680	1,2K	2,2K	5,6K

Cuadro 12. Resistencias de base para distintos tipos de relés y distintas tensiones de control.
Fuente. https://www.inventable.eu/controlar-rele-con-transistor/

5.1.5. Equipos de seguridad. El proceso de acceso a los auditorios está relacionado por un conjunto de equipos de seguridad, que se encargan de restringir ese acceso no autorizado por el sistema. A continuación se presentara cada equipo asociado con este proyecto.

5.1.5.1 Electroimán.

Figura 19. Cerradura magnética MLR-600.
Fuente. https://www.google.com.co/search?q=mlr+600+electroiman

Las cerraduras magnéticas son elementos diseñados para asegurar cualquier tipo de puerta, las cuales con una instalación apropiada cubrirán todas las expectativas de operación y confiabilidad.

Las cerraduras de este tipo se encuentran conformadas por un electroimán que se instala en el marco de la puerta, y una placa montada en la hoja de la misma. Cuando se encuentra energizada, la fuerza magnética del electroimán asegura la puerta. Estos elementos están diseñados para ser utilizados en diferentes tipos de puertas, según el volumen de tráfico peatonal y el nivel de seguridad que se requiera.

En este proyecto se usó el electroimán MLR-600, ver Figura 21.

Cuadro 13. Dimensiones electroimán MLR-600

Dimensiones Electroimán	**Dimensiones Tapa**
Ancho: 38mm	Ancho: 40mm
Largo: 160mm	Largo: 142mm
Alto: 25mm	Alto: 12mm
Peso: 953gr	Peso: 507gr

Características Técnicas:

- Fuerza de retención: 600 libras
- Voltaje alimentación: 12V-14V

- Corriente: 480mA Accesorios
- Adaptador de 13.7V (COD: 350-420-054)

- Módulo Antirremanente Con Buzzer (COD:300-010-003)

- Botón pulsador

El electroimán cuenta con un módulo anti remanente único, el cual funciona como interfaz entre la cerradura electromagnética, el usuario y otros sistemas de control de acceso, contra incendio y de seguridad. Su circuito electrónico con microprocesador permite realizar un sinnúmero de funciones inteligentes, además de operar de forma eficiente y segura la cerradura electromagnética.

Las características técnicas generales de los módulos anti remanentes son:

- Voltaje de alimentación: 12VDC – 14VDC.
- Corriente nominal de funcionamiento: 36mA.
- Operación del buzzer con frecuencia de 2400Hz.
- Máximo hasta diez pulsadores en paralelo.
- Máxima distancia hacia el electroimán: 20 metros.
- Máxima distancia hacia el pulsador: 30 metros.
- Máxima distancia hacia el buzzer: 20 metros.

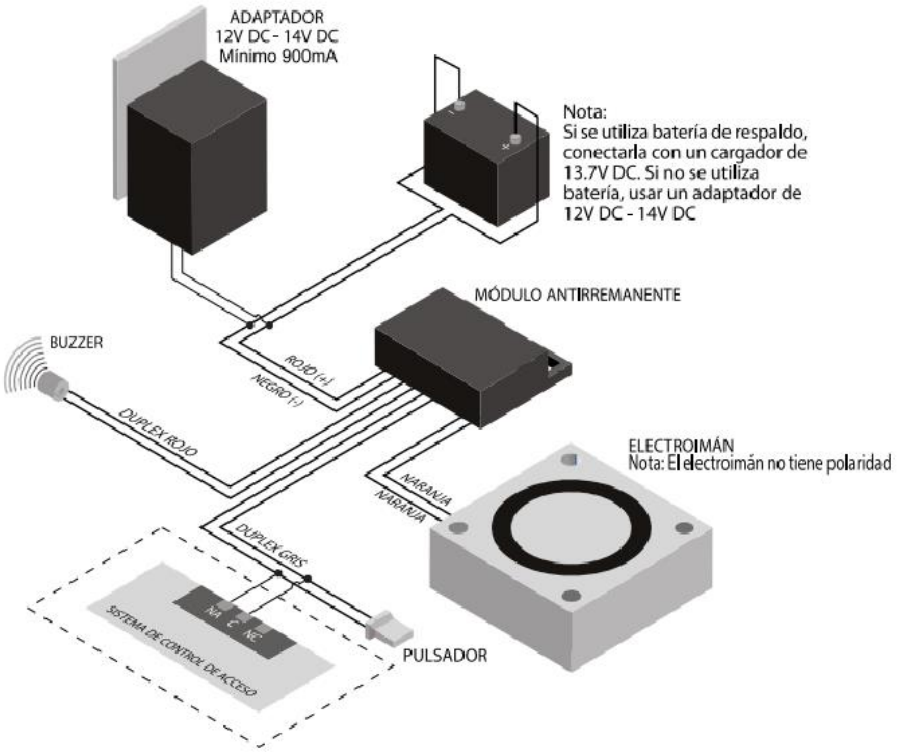


Figura 20. Instalación eléctrica de una cerradura electromagnética con módulo antirremanente.

Fuente.http://www.micromotores.com/site/components/com_jshopping/files/demo_products/PRESENTACION_MAGNETIC_LOCK4.pdf

Para la correcta instalación del electroiman primero se debe conocer la forma adecuada de prepararlo para la posterior instalacion en una puerta, asi como se puede observar en la Figura. 21, luego se debe tener en cuenta el tipo de puerta en el cual se vaya a ensamblar, para el caso de los auditorios de la facultad se usara la configuracion de puerta hacia “adentro”, como se aprecia en la Figura. 22 siendo este el caso más común de instalación y se utiliza un soporte tipo “Z” para acoplar la cerradura a la tapa de cierre.

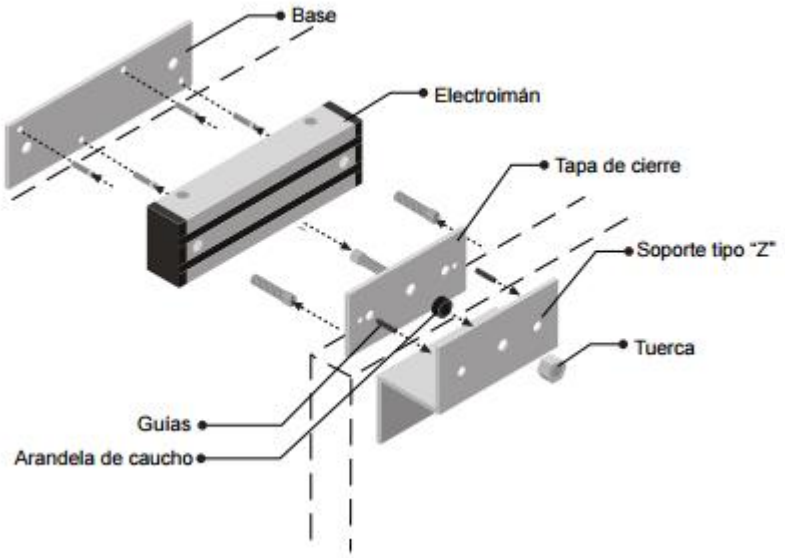


Figura 21. Conexiones del electroimán.
Fuente.http://www.micromotores.com/site/components/com_jshopping/files/demo_products/PRESENTACION_MAGNETIC_LOCK4.pdf

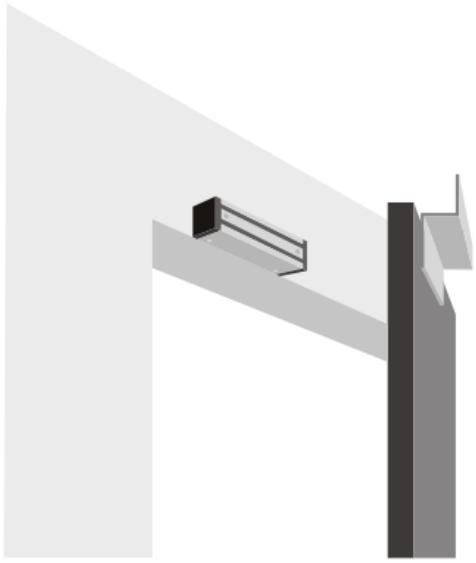


Figura 22. Montaje del electroimán con soporte tipo Z.
Fuente.http://www.micromotores.com/site/components/com_jshopping/files/demo_products/PRESENTACION_MAGNETIC_LOCK4.pdf

5.1.5.2 Cantonera eléctrica. El fallo de energía en la facultad de ingeniería es uno de los problemas principales que se establecieron al iniciar este proyecto, puesto que esto es constante y la Universidad no cuenta con un sistema de respaldo para ello. Por esto y debido a que sin energía eléctrica el sistema de control de acceso quedaría completamente deshabilitado, se decidió implementar en conjunto la cantonera eléctrica (Figura. 23) la cual en el momento en el que haya ausencia de energía se active ocasionando que la puerta quede completamente cerrada y solo sea posible entrar a los auditorios por medio de una llave que será manejada por el administrador.

Figura 23. Cantonera eléctrica.
Fuente.https://www.google.com.co/search?q=cantonera+electrica+110v.

5.1.6 Comunicación entre Raspberry pi y Servidor web. Por razones de seguridad se optó que la comunicación sea de tipo Ethernet, entre la placa y el servidor, con IP fijas donde solo se pueda hacer la consulta a la base de datos de la universidad en los puntos destinados para tal fin, que se encuentra conectados a las RACK (bastidor metálico destinado a alojar equipos) respectivos del tercer piso de la facultad de ingeniería.

Entre las características más importantes de estar conectado a la red interna de la Universidad es que en caso de presentarse una falla en el internet (Datos) el sistema de seguridad sigue operando normalmente debido a que es independiente de ese factor, llevando acabo la consulta de forma casi instantánea, evitando retrasos y demoras en el acceso.

5.2 COMPONENTES DE SOFTWARE

5.2.1 Aplicativo web. Es el eje central y primordial de nuestro control de acceso ya que es una herramienta que permite la comunicación activa entre los elementos de seguridad y el administrador que efectúa los permisos y controla el acceso a ellos junto con el servidor que aloja la base de datos del sistema. Esto da la posibilidad de llevar los registros de usuarios que usan los auditorios y solo el aplicativo web es accesible en el computador del administrador ubicado al lado del

auditorio Miguel Felipe Ospina aumentando la seguridad y descartando la manipulación de terceros.

Para acceder a la aplicación el administrador cuenta con un nombre de usuario y una contraseña.

Por medio de la aplicación se pueden realizar las operaciones listadas en el siguiente cuadro.

Cuadro 14. Operaciones del aplicativo web.

Operación	Encargado
Modificar contraseña	Centro de Redes
Hacer reserva	administrador
Eliminar reserva	administrador
Editar reserva	administrador
Ver registro de reservas	administrador

Fuente. Elaboración propia**.**

La aplicación web para la administración del sistema se desarrolló utilizando los framework de angularJS y Java para la comunicación con el servidor.

5.2.2 Programación módulo SL030 y Raspberry Pi. Una vez preparada la raspberry y configurada para operar, se procede hacer un archivo **.py** donde se programa el lector RFID y se relacionan las librerías **i2c**, que es la utilizada para la comunicación entre la tarjeta y el modulo, **RPi.GPIO**, le da la facultad de poder usar los puertos GPIO, **time**, es la que controla el tiempo en que esta en alto o bajo un pin GPIO, **requests**, es la que permite hacer consulta a una determinada dirección web, **json**, es un formato de texto ligero para el intercambio de datos.

La programación se realizó teniendo en cuenta el diagrama de flujo, que es una representación básica de cómo opera un control de acceso con tecnología RFID que se muestra en la Figura 24.

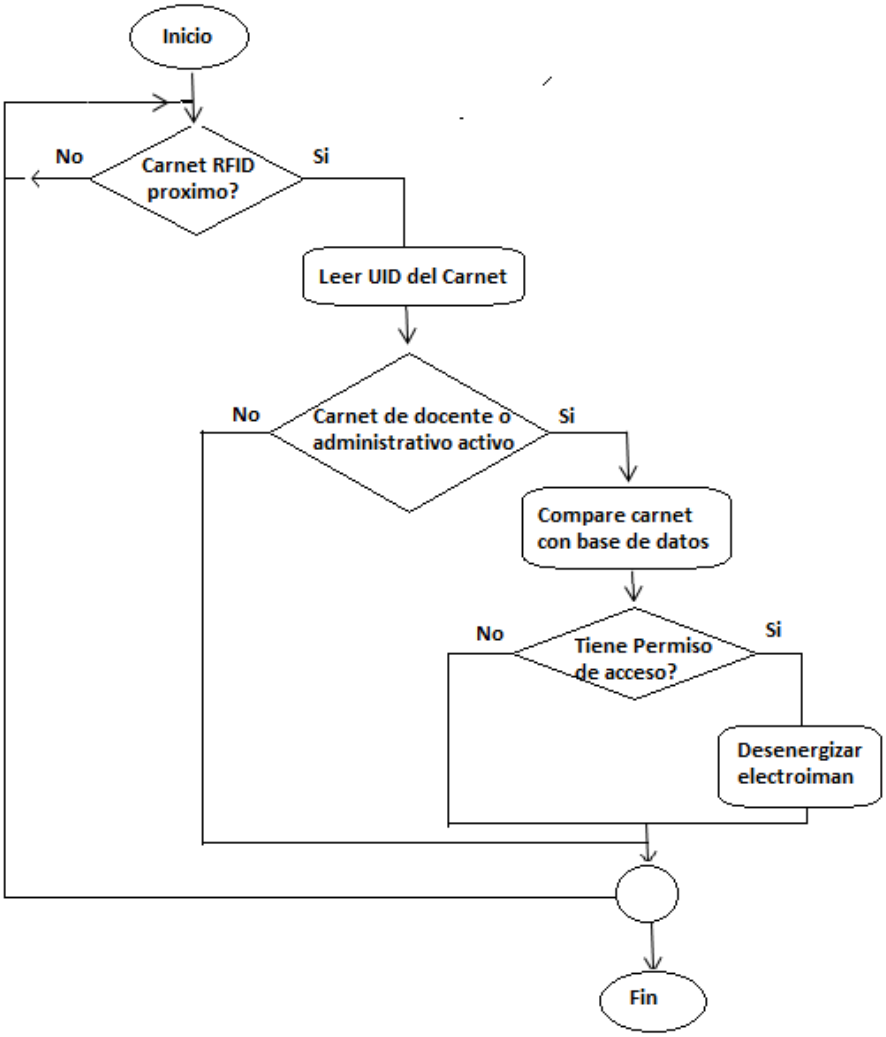


Figura 24. Diagrama de flujo de la lógica del sistema.
Fuente. Elaboración propia**.**

5.2.3 Servidor y base de datos. El sistema de control de acceso hace provecho de la base de datos que ya existe en la Universidad Surcolombiana, en la cual se relacionan los docentes y administrativos que estén activos en el plantel para hacer las consultas. De igual forma hace uso de su servidor, ya que el aplicativo web que fue desarrollado se encuentra alojado en la web de la USCO, denotada con la siguiente dirección:

https://isnos.usco.edu.co/uscop/Auditorio

Se debe tener en cuenta que esta dirección solo se puede acceder desde el punto de Ethernet configurado para tal fin y el conocimiento de la base de datos es restringido.

6. ANÁLISIS DE RESULTADOS

En este capítulo se presentaran los resultados obtenidos en cuanto a la infraestructura, fiabilidad, robustez y desempeño del sistema de control de acceso a los auditorios del tercer piso de la facultad de ingeniera de la Universidad Surcolombiana.

Para las pruebas del sistema, se emplearon dos carnés (docente/administrativo) y enlazado con la base de datos de la universidad, donde se realizó la posterior reserva en la oficina del administrador para cada auditorio en distintas horas. Por otra parte se tuvo en cuenta, que para que el carné sea detectado y no presente inconvenientes a la hora de la lectura, debe estar a una distancia máxima de 2cm frente al módulo RFID.

6.1 INFRAESTRUCTURA DEL SISTEMA

Para poner a prueba el sistema de manera eficaz y evaluar el desempeño, fiabilidad y robustez del sistema, se hizo la instalación de los elementos correspondientes en los dos auditorios, tal como se muestra en la Figura 25.

Cada auditorio se encuentra equipado con una puerta a la cual se le instalo una cantonera eléctrica y un electroimán, adicional a eso se realizó lo pertinente para poder tener un toma al cual se conecta única y exclusivamente la cantonera eléctrica, el electroimán y la Raspberry siendo esta última junto al lector RFID y el circuito acondicionador parte también del sistema de control de acceso de cada uno de los auditorios.

El control de acceso se realiza gracias a una persona que es llamada administrador el cual por medio del aplicativo web que fue desarrollado puede ingresar inicialmente a la base de datos de la universidad y verificar si la persona que desea reservar los auditorios tiene el permiso para hacerlo, este permiso es dado únicamente a administrativos y a profesores de la universidad, una vez este permiso es verificado el administrador procede a efectuar la respectiva reserva informando fecha, hora y auditorio disponible, cabe resaltar que el aplicativo web permite que el administrador de ser necesario pueda eliminar o modificar cualquier reservación que se haya hecho con anterioridad. La asignación de auditorio es en tiempo real y el acceso a la base de datos para verificar permisos también lo es.

Como si fuera poco, se realizaron pruebas en las cuales se efectuaba el acceso a los 2 auditorios en el mismo momento y los resultados fueron satisfactorios pues no se presentó congestión alguna.

Figura 25. Instalación de los elementos control acceso.
Fuente. Elaboración propia**.**

6.2 APLICACIÓN WEB

Para la eficiencia en las reservas de los auditorios se desarrolló un aplicativo web basado en angularJs como framework, para desarrollar un entorno mucho más rápido, expresivo y legible, luego Java para la consulta a la base de datos de la universidad haciendo uso del webservice, que es un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones sin ningún problema, como en el caso raspberry/servidor.

El aplicativo será manejado única y exclusivamente por el administrador. Para poder ingresar al sistema debe contar con un usuario y una contraseña como se muestra en la figura 26.

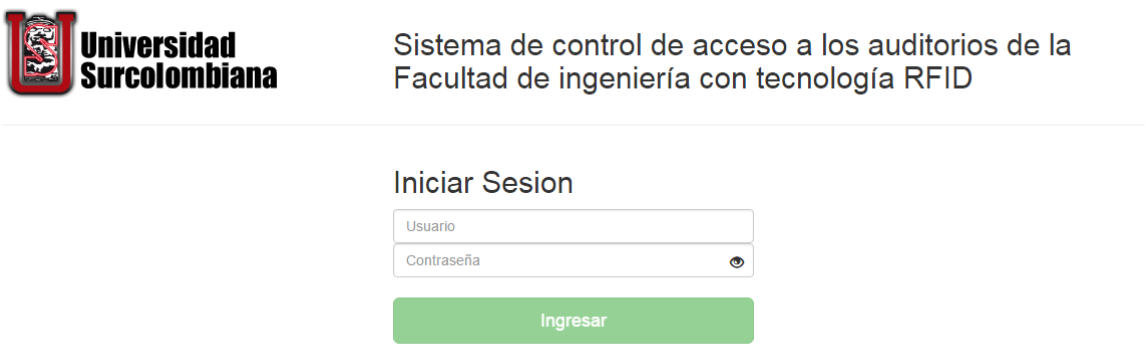


Figura 26. Página de inicio de sesión.
Fuente. Elaboración propia**.**

Se implementaron las *SweetAlert* como se puede observar en la figura 27, para que el administrador pueda observar las advertencias de la página de forma más estética en caso de ejecutar algo indebidamente como escribir mal la contraseña o usuario o también para decir que las operaciones hechas fueron con éxito.

Figura 27. Mensajes de alerta.
Fuente. Elaboración propia**.**

Una vez se hayan ingresado los datos solicitados correctamente, el sistema cargara una nueva pantalla como la que se muestra en la figura 28, en la cual se puede realizar la labor de reservar además de anular y/o editar reservaciones anteriores pero como principal función poder observar la relación de fechas, horas y usuarios a los cuales ya han ejecutado la reserva.

FECHA	HORA INICIAL	HORA FINAL	AUDITORIO	PRESTADO A	ACCIONES
2016-10-28	08:00	10:00	MIGUEL FELIPE OSPINA	SEBASTIAN TAMAYO R	
2016-10-31	09:00	12:00	AMBIENTAL	VANESSA MORALES	
2016-11-01	15:00	17:00	AMBIENTAL	SEBASTIAN TAMAYO R	
2016-11-04	08:00	10:00	MIGUEL FELIPE OSPINA	VANESSA MORALES	
FECHA	HORA INICIAL	HORA FINAL	AUDITORIO	PRESTADO A	ACCIONES

Figura 28. Panel de permisos de acceso.
Fuente. Elaboración propia**.**

En el momento en el que se desee realizar una reservación, se debe cliquear en el botón agregar auditorio y en el espacio que se despliega ingresar el número de documento de identificación del usuario tal como se muestra en la figura 29.

Figura 29. Agregar reserva al auditorio.
Fuente. Elaboración propia**.**

Una vez se ingrese el número de identificación del usuario se despliega un menú como se muestra en la figura 30, el cual solicita los datos necesarios para llevar a cabo la reservación, como la fecha, hora inicial, hora final y el auditorio que desea usar. Una vez establecido todos los datos se selecciona la opción Reservar y de esta manera queda generada la reservación.

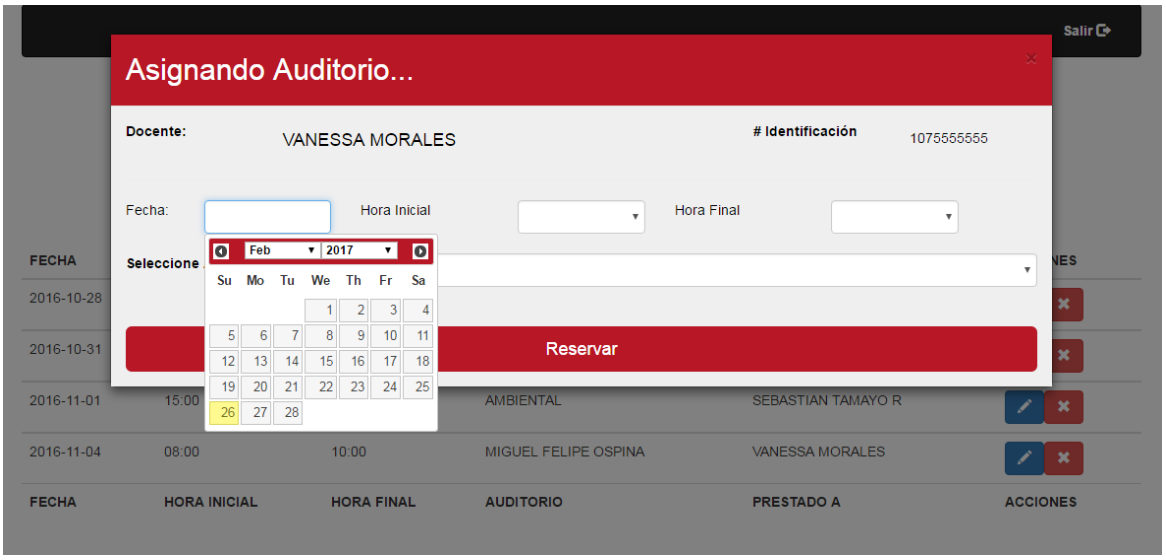


Figura 30. Asignando auditorio.
Fuente. Elaboración propia**.**

En caso de que el usuario editado no se encuentre habilitado en la base de datos proporcionada por el departamento de redes de la Universidad Surcolombiana, la página arrojara un aviso que informa que el usuario no está autorizado para realizar la reservación tal como se muestra en la figura 31.

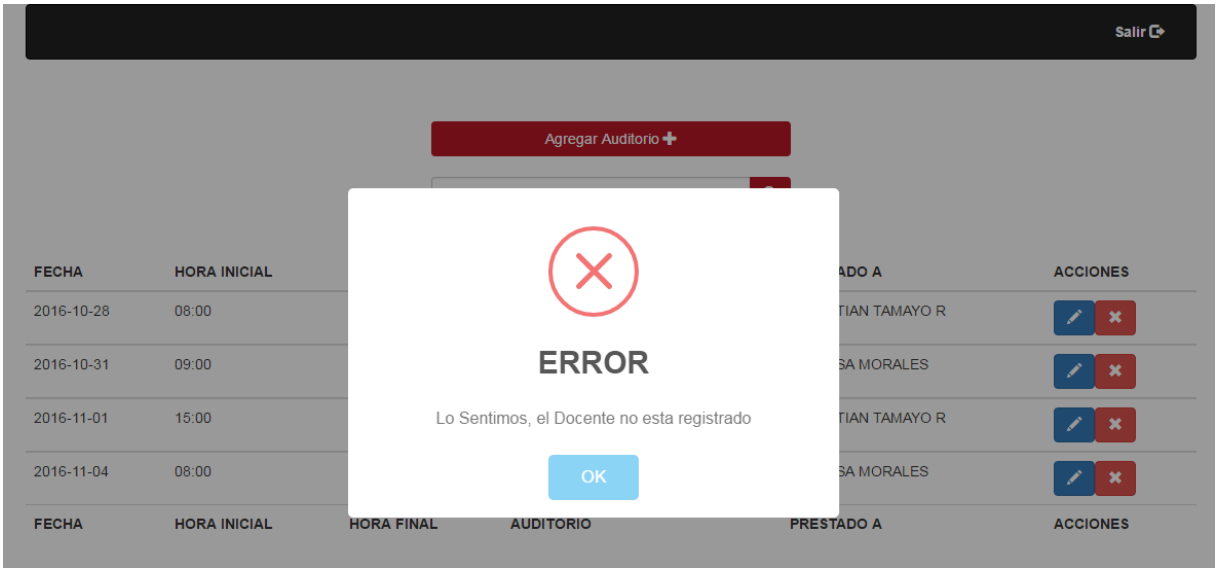


Figura 31. Alerta de usuario no encontrado.
Fuente. Elaboración propia**.**

Una vez realizada la reservación, en la parte derecha de la figura 28, se puede observar los iconos que nos permiten realizar las acciones de editar y/o eliminar dichas reservaciones, al seleccionar la opción de editar se despliega un menú el cual permite hacer cambio en la fecha, hora y/o auditorio, tal como se observa en la figura 32, donde se debe tener en cuenta que el cambio se efectuara una vez se seleccione el botón editar reserva.

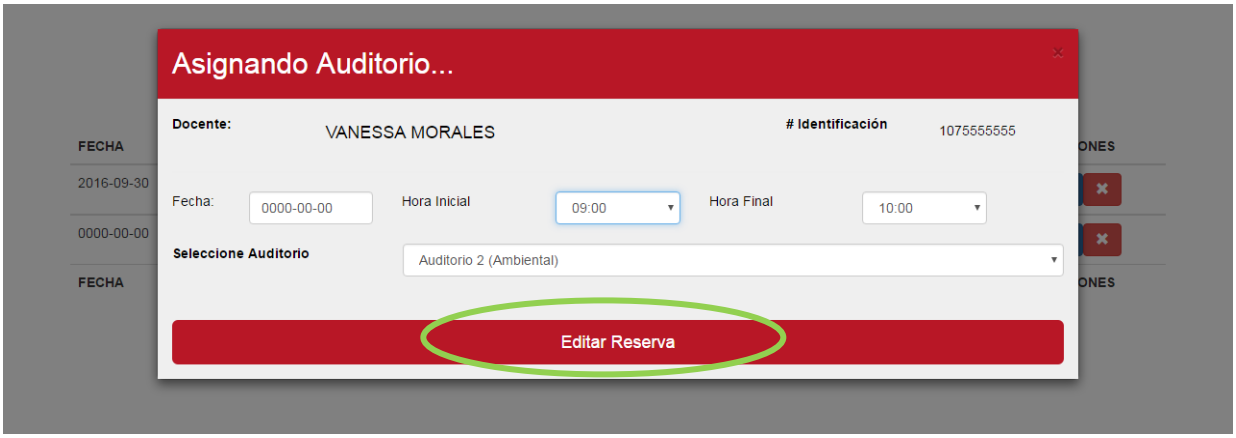


Figura 32. Editor de reservas.
Fuente. Elaboración propia**.**

Por otra parte si lo que desea es cancelar la reservación se selecciona la opción eliminar, al realizar esta operación se genera un aviso que informa que la petición fue realizada exitosamente, como se puede observar en la figura 33.

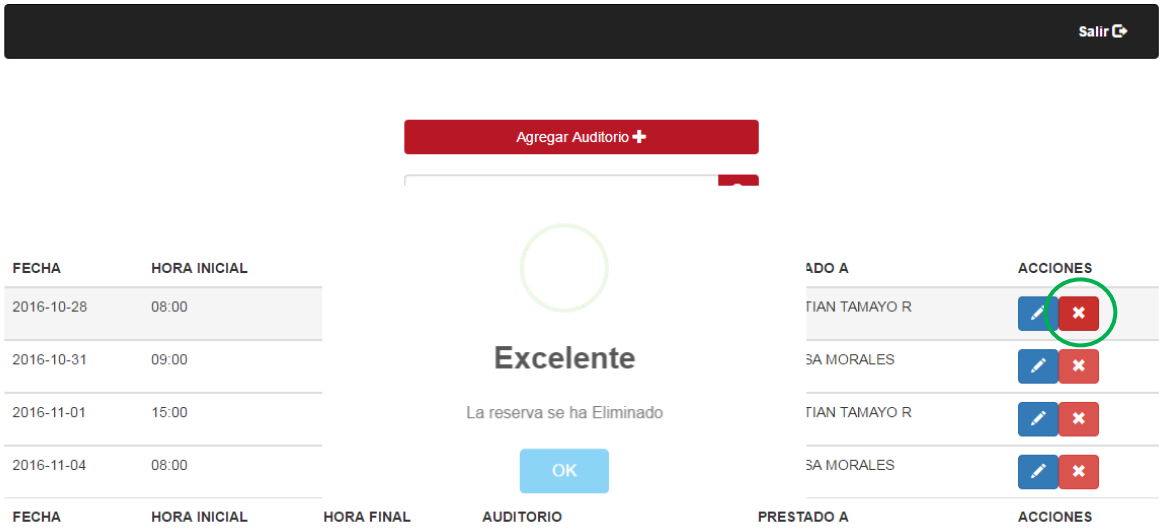


Figura 33. Cancelación de reservas.
Fuente. Elaboración propia**.**

También se consideró muy importante exaltar el motivo por el cual se va a realizar la reserva de los auditorios, ya que se puede llevar un mejor control del aprovechamiento de los mismos y evitar la saturación por cosas que se podrían desarrollar en un aula de clases.
Esto se puede encontrar en la figura 34, donde el administrador digita el motivo por el cual se va a reservar.

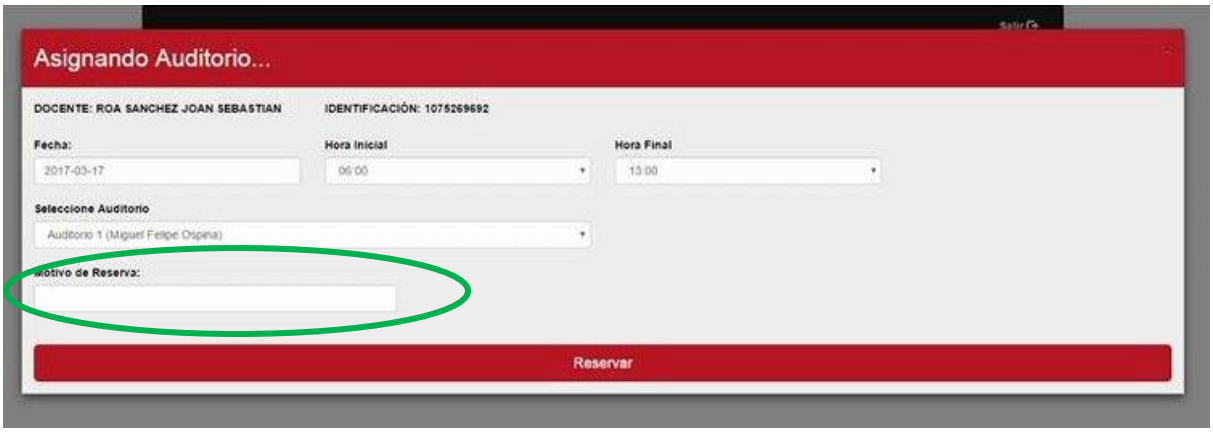


Figura 34. Motivo de Reserva.
Fuente. Elaboración propia**.**

Adicional a lo que ya se ha mencionado de nuestro aplicativo web, este nos permite generar un reporte en formato PDF, donde aparece las reservas hechas durante el mes, y las actividades por las cuales fueron ejecutadas las reservas en los respectivos auditorios junto con el nombre del docente y las horas de utilización del mismo.
En la figura 35, se representado una plantilla de cómo sería el reporte.

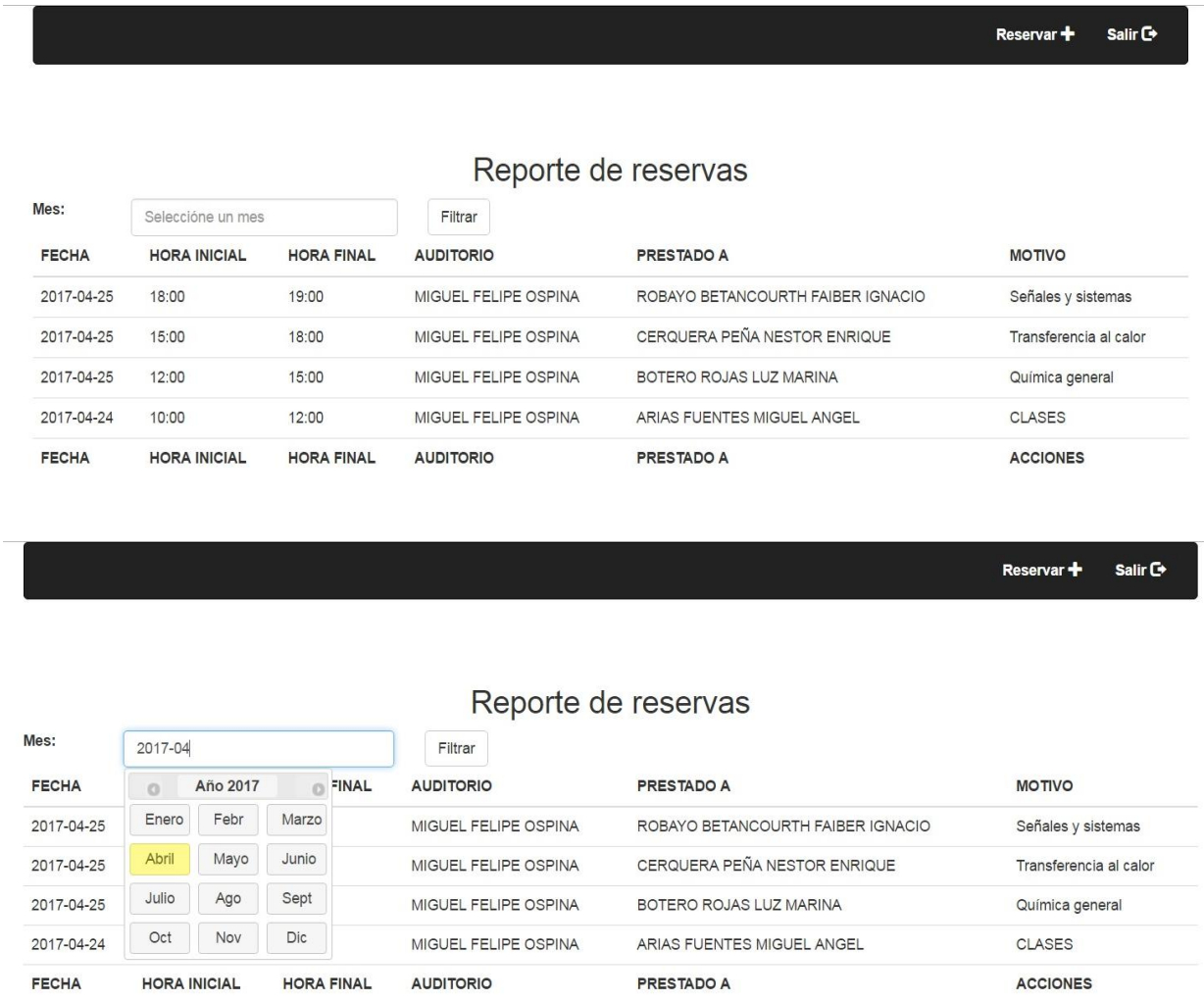


Figura 35. Reporte e historial de reservas.
Fuente. Elaboración propia**.**

Por último se debe tener en cuenta que para realizar la reservación es estrictamente necesario presentar el carné que acredita a el solicitante como profesor o administrativo, para una mayor confiabilidad a la hora de tener un control del uso de los auditorios y no permitir que terceros suplanten la identidad de un docente/administrativo.

7. CONCLUSIONES

- La implementación del sistema de control de acceso, es una solución eficiente a la problemática actual de deterioro de la infraestructura de los auditorios de la facultad de ingeniería de la universidad Surcolombiana, ya que garantiza la seguridad de las instalaciones y elementos que en ella se encuentran de una forma más controlada.

- La conexión directa a la base de datos de la Universidad Surcolombiana hace más eficiente y segura la gestión de reservas, permitiendo así que no haya ninguna anomalía en cuanto a docentes o administrativos inactivos que quieran hacer uso de los auditorios.

- El funcionamiento del módulo RFID puede verse afectado, si este es colocado sobre una superficie metálica.

- Para el correcto funcionamiento del sistema implementado para el control de acceso fue necesario hacer adecuaciones en los auditorios para un mejor aprovechamiento del sistema.

- El desarrollo de un aplicativo web para la administración de las reservas se fundamentó en ser de uso exclusivo del host del administrador, para evitar manipulación de terceros y fortalecer la seguridad del mismo.

- La implementación de la aplicación web bajo licencia de software libre, permite el mejoramiento continuo del proyecto y pueda tener adaptaciones a sistemas diversos.

8. RECOMENDACIONES Y TRABAJO FUTURO

A medida que se fue desarrollando este proyecto de grado se fueron observando una serie de modificaciones que podrían optimizar el rendimiento del sistema aún más de lo propuesto en un principio.

Una de las partes claves e importantes es instalar y adecuar un sistema de energía eléctrica de apoyo a eventuales casos de cortos y/o fallos en la red eléctrica, debido a que nuestro sistema de seguridad depende de ello en la mayor parte.

Es muy importante que al efectuar el administrador la reserva pida el documento de identificación del docente o administrativo “carnet institucional” para que se tenga la certeza que es el la persona a la cual se le va dar la reserva y sea más verídico el historial de uso de los auditorios que arroja el sistema.

Para que el usuario tenga una mejor experiencia con el sistema de acceso, se recomendaría que se incluyera un display LCD donde se vaya observando la ejecución del programa.

Este sistema de acceso podría vincularse tanto a salones, laboratorios y oficinas. Siempre y cuando se rediseñe su lógica de funcionamiento al actual, ya que dentro del aplicativo web se necesitaran más elementos para llevar acabo todo este tipo de procesos.

Una mejora adicional al sistema, sería la integración de sensores de presencia, que haga que el sistema de iluminación y de aires acondicionados se encienda o se apaguen de manera autónoma, permitiendo un mayor ahorro de energía.

Este proyecto está protegido bajo la licencia de código abierto GPL y cualquier trabajo derivado de este proyecto, ya sea copia, modificación o distribución debe incluirse bajo la misma licencia de software libre, reconociendo a los autores originales.

BIBLIOGRAFÍA

Gabriel Rapetti, 27 noviembre de 2013 A., inventable.eu. Italia. URL https://www.inventable.eu/controlar-rele-con-transistor/.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Identification Cards-Contactless integrated circuit(s) cards-Proximity cards. ISO 14443, 1999.

STRONGLINK, November 2012. Version 2.6. Strong link, ee.uu. Recuperado de http://www.stronglink-rfid.com/download/SL030-User-Manual.pdf.

RaspberryPi, how to autorun a Python script on boot using system. Disponible en internet http://www.raspberrypi-spy.co.uk/2015/10/how-to-autorun-a-python-script-on-boot-using-systemd/.

SK Pang electronics, Using SL030 RFID Module with Raspberry Pi. Disponible en internet http://skpang.co.uk/blog/archives/946.

Carlos Azaustre, (2012-2016). ¡Hola! Soy Carlos Azaustre, CTO en Chefly, desarrollador web fullstack y formador de JavaScript y el ecosistema de React.js. Madrid España. URL https://leanpub.com/aprendiendo-javascript.

RFID A Guide to radiofrequency Identification, V. Daniel Hunt, Alberto Puglia, Mike Puglia, Wiley Interscience, 200, Paginas 50-52.

Jhon R. Traditional And Emerging Technologies And Applications In The Radio Frequency Identification (Rfid) Industry. Tuttle Micron Communications, Inc.2004 IEEE Radio Frequency Integrated Circuits Symposium.

ANEXOS

A. CÓDIGO PYTHON DEL MÓDULO SL030.

A1. Librerías utilizadas.

```
import rfid
import RPi.GPIO as GPIO
import time
import requests
import json
```

A2. Definición de los pines GPIO por BCM "Broadcom SOC channel" y como Pin de señal de control el GPIO18 como solo salida.

```
GPIO.setmode (GPIO.BCM)
GPIO.setup (18, GPIO.OUT)
```

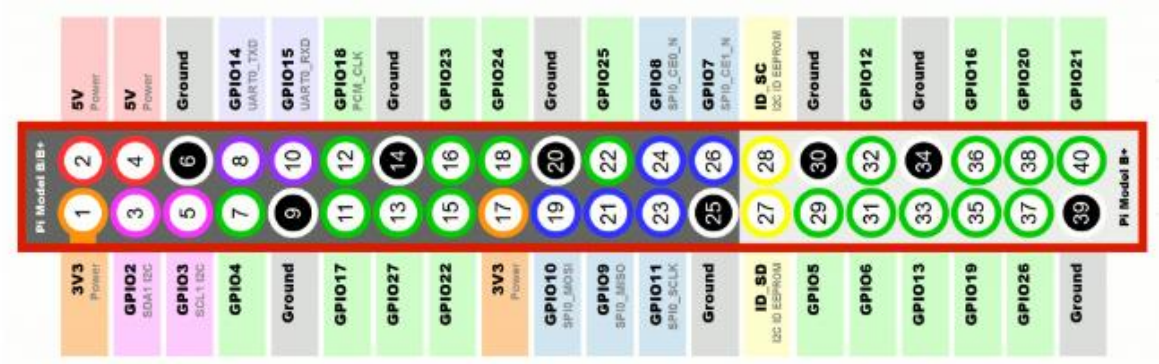


Figura 36. Pines GPIO por BCM.
Fuente. http://raspberrypi.stackexchange.com/questions/40318/raspberry-pi-2-can-gpio-pins-29-40-be-used-gpio-gen-input-output-configurable-in

A3. Menú del programa.

```
# MENU PROGRAMA
while True:

 print("Deslice su carnet...")
 rfid.waitTag()
 print(">> Carnet Detectado")

 # Este condicional permite solo reconocimiento de tarjetas Mifare cards
 if not rfid.readMifare():
  print("Esta no es una tarjeta MIFARE")
 else:
  print(">> Carnet Tipo: " + rfid.getTypeName())
```

```
   uid = rfid.getUniqueId()

   try:

     print("Codigo carnet")
     print(uid)

     print('Validando informacion...')

r=requests.get('https://isnos.usco.edu.co/uscop/Auditorio/Accionar?uid='+uid+'&auditorio=1'verify=False )

     json_string = r.text
     parsed_json = json.loads(json_string)
     acceso = parsed_json['mensajeTipo']
          print('carnet servidor '+acceso+' carnet local '+uid)

     if(acceso == 'SUCCESS'):

           print(">> Acceso Garantizado: ")
           GPIO.output(18, True)
           time.sleep(3)
           GPIO.output(18, False)
     else :

      GPIO.output(18, False)
      print(">> Usted no ha reservado auditorio")
   except KeyError:
     print("Carnet desconocido: " + uid)
  rfid.waitNoTag()
  print(">> Gracias....")
# END
```

B. PASOS PARA EL AUTOARRANQUE DEL PROGRAMA RASPBERRY PI.

B1.Script de Python. Tener la seguridad en la dirección donde se almaceno y su nombre completo para poder completar los siguientes pasos. En nuestro caso el script del proyecto que se almaceno en el directorio /home /pi y que se llamó (controlacceso.py).

B2. Crear un archivo de unidad. Esto se hace con el siguiente código en la terminal de la raspberry.

```
sudo nano /lib/systemd/system/myscript.service
```

Luego se añade el siguiente texto.

```
[Unit]
Description=My Script Service
After=multi-user.target

[Service]
Type=idle
ExecStart=/usr/bin/python /home/pi/myscript.py

[Install]
WantedBy=multi-user.target
```

En la parte de “Description”, ponemos el nombre de nuestro proyecto.py, luego damos [CTRL-X], [YES] después [ENTER].

Ahora para almacenar la salida de texto de la secuencia de comandos en un archivo de registro, escribimos el siguiente texto en la terminal.

```
ExecStart=/usr/bin/python /home/pi/myscript.py > /home/pi/myscript.log 2>&1
```

Tener en cuenta que el nombre (myscript.py) se reemplaza por el nombre de nuestro proyecto que deseamos que se inicie apenas se encienda la raspberry.

Luego que el permiso del archivo de la unidad debe estar configurado en 644.

```
sudo chmod 644 /lib/systemd/system/myscript.service
```

B3. Configurar el Systemd. Ahora que el archivo de unidad se ha definido, podemos llamarlo bajo systemd para iniciarlo durante la secuencia de arranque.

```
sudo systemctl daemon-reload
 sudo systemctl enable myscript.service
```

Cabe aclarar que (myscript.service), fue como se nombró el servicio donde se encuentra nuestro archivo del proyecto en .py alojado.

Por ultimo reiniciamos la raspberry Pi, escribiendo en la terminal (Sudo reboot) y listo.

C. INSTALACIÓN Y ADECUACIÓN DE LOS ELEMENTOS DE SEGURIDAD EN LOS AUDITORIOS.

Figura 37. Instalación y adecuación.
Fuente. Elaboración propia.

D. DISEÑO DE LAS CUBIERTAS PARA RASPBERRY PI, CIRCUITO DE ACONDICIONAMIENTO Y LECTOR RFID.

Para diseñar la cubierta se debió tener en cuenta las medidas del circuito acondicionador, la raspberry pi y el lector ya que estos tres elementos se encuentran ensamblados en la misma caja, que se muestra en la figura 38**.**

A continuación se mostraran las medidas de cada uno de los objetos mencionados anteriormente relacionados en las figuras 39, 40 y 41**.**

Figura 38. Caja lectora.
Fuente. Elaboración propia.

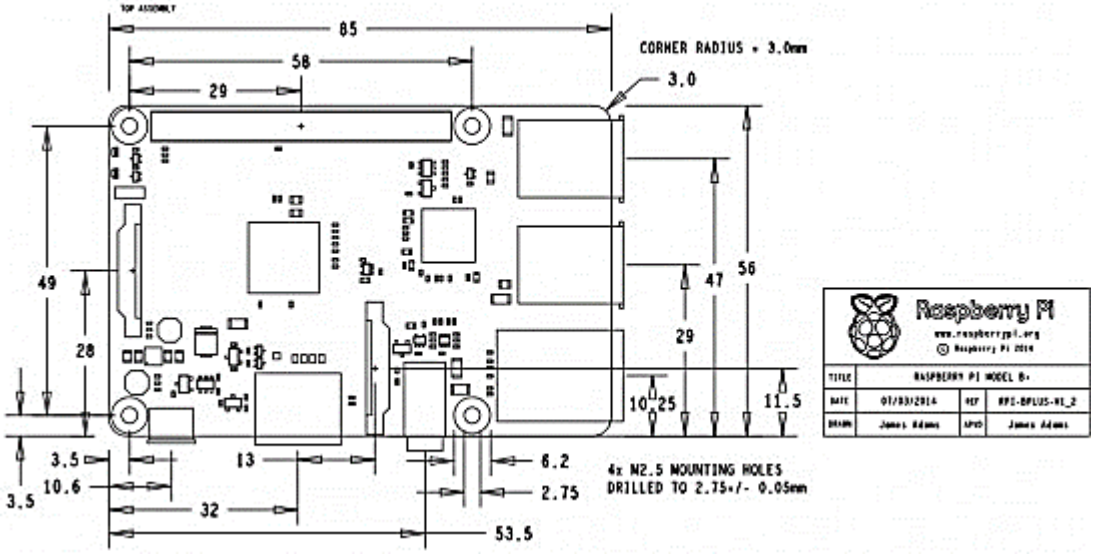


Figura 39. Dimensiones de la Raspberry Pi 3.
Fuente.https://apocusantti.files.wordpress.com/2014/07/plano-rasperry.jpg

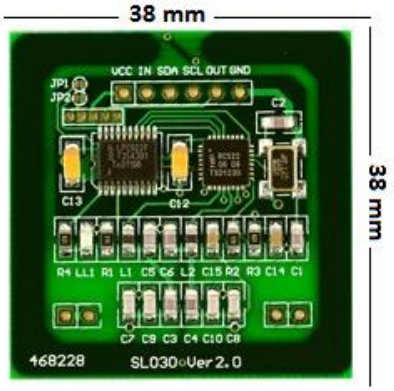


Figura 40. Dimensiones del módulo SL030 lector/escritor RFID.
Fuente. http://www.stronglink-rfid.com/es/rfid-modules/sl030.html

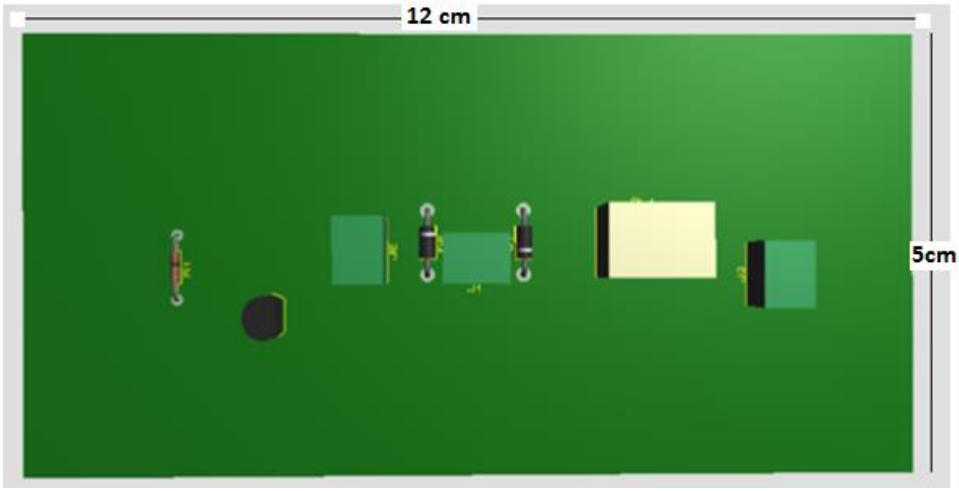


Figura 41. Dimensiones del circuito acondicionador.
Fuente. Elaboración propia.

Para el correcto funcionamiento de estos tres elementos la caja fue diseñada de tal manera que se pudiera dividir en tres secciones, la parte posterior será en la cual se ubicaría el circuito acondicionador, en la cavidad del medio se ubica la raspberry pi y en la superior se instaló el módulo RFID.

La caja está elaborada en su totalidad en acrílico de 5mm de grosor lo cual la hace realmente robusto, las divisiones fueron fijadas mediante unos rieles para que fueran removibles permitiendo que la ensamblada de cada elemento se realizara de forma fácil y sin irse a estropear entre sí.

También fue necesario diseñar, dos carcazas en las cuales se ubicaron los botones “no touch”, como los que se muestran en la figura 42 y dos más para los botones que nos accionaran las cantoneras como se muestra en la figura 43.

Figura 42. Botón de emergencia NoTouch.
Fuente. Elaboración propia.

Figura 43. Botón de cantonera eléctrica.
Fuente. Elaboración propia.

E. PRUEBA Y FUNCIONAMIENTO DEL SISTEMA DE CONTROL DE ACCESO

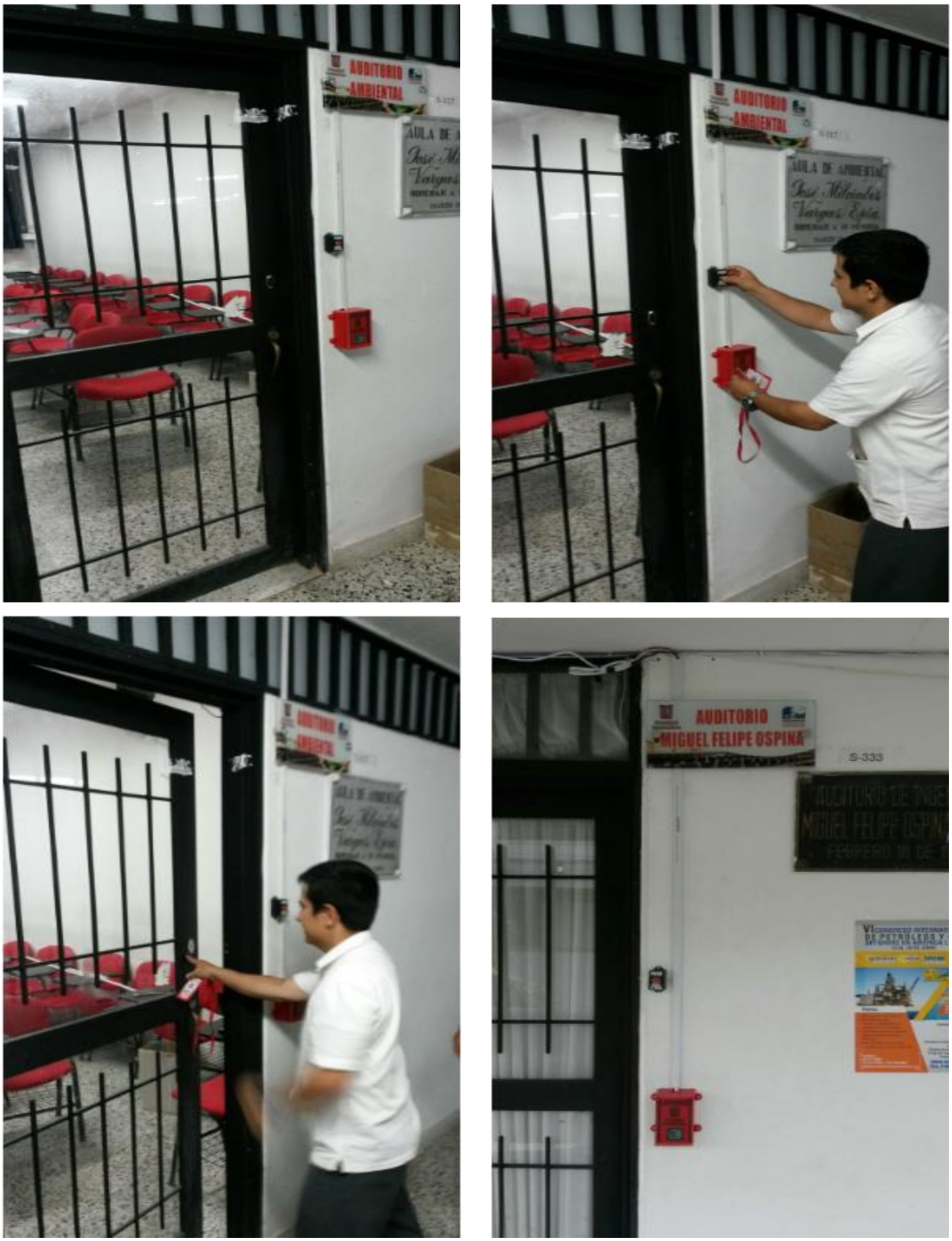


Figura 44. Funcionamiento del sistema de control de acceso.
Fuente. Elaboración propia.