CONTROL DE ACCESO BASADO EN TECNOLOGÍAS IOT EN INSTITUCIONES DE EDUCACIÓN SUPERIOR. PROTOTIPO APLICADO AL CONTROL DEL INGRESO A SALONES Y AUDITORÍA EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB (COLOMBIA)

JOSÉ DAVID ORTIZ CUADROS

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB
FACULTAD DE INGENIERÍA
MAESTRÍA EN TELEMÁTICA
GRUPO DE INVESTIGACIÓN EN TECNOLOGÍAS DE INFORMACIÓN
LÍNEA DE INVESTIGACIÓN EN TELEMÁTICA
BUCARAMANGA
2018

CONTROL DE ACCESO BASADO EN TECNOLOGÍAS IOT EN INSTITUCIONES DE EDUCACIÓN SUPERIOR. PROTOTIPO APLICADO AL CONTROL DEL INGRESO A SALONES Y AUDITORÍA EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB (COLOMBIA)

JOSÉ DAVID ORTIZ CUADROS

Trabajo de grado para optar al título de Magíster en Telemática, con modalidad en investigación.

Director
PhD. Cesar Darío Guerrero Santander

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA
MAESTRÍA EN TELEMÁTICA
GRUPO DE INVESTIGACIÓN EN TECNOLOGÍAS DE INFORMACIÓN
LÍNEA DE INVESTIGACIÓN EN TELEMÁTICA
BUCARAMANGA
2018

A mis padres.

AGRADECIMIENTOS

De manera muy especial agradezco al PhD. Cesar Darío Guerrero Santander por su dirección, seguimiento constante, comentarios y sugerencias durante el desarrollo de esta investigación.

A todos los docentes involucrados en mi formación de maestría por haber compartido su conocimiento.

La colaboración de todos los socios dentro del proyecto Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT). También a todas las instituciones que apoyaron este trabajo: el Ministerio de Tecnología de la Información y Comunicaciones – MinTIC de Colombia y al Departamento Administrativo de Ciencia, Tecnología e Innovación – Colciencias, a través del Fondo Nacional de Financiamiento para la Ciencia, Tecnología y la Innovación Francisco José de Caldas (ID Proyecto: FP44842-502-2015).

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

CONTROL DE ACCESO BASADO EN TECNOLOGÍAS IOT EN INSTITUCIONES DE EDUCACIÓN SUPERIOR. PROTOTIPO APLICADO AL CONTROL DEL INGRESO A SALONES Y AUDITORÍA EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB (COLOMBIA)

José David Ortiz Cuadros, Autor
PhD., Cesar Darío Guerrero Santander, Director de tesis

RESUMEN

En Colombia, la mayoría de las IES no cuentan con sistemas automatizados de control de acceso de ingreso a salones de clase. Esto impide se pueda tener información en tiempo real, que permita realizar una auditoría sobre asistencia de estudiantes a clase y cumplimiento por parte de los docentes con los horarios de clase establecidos.

En la Universidad Autónoma de Bucaramanga - UNAB, dado que es una institución de puertas abiertas que no restringe el ingreso a ningún ciudadano, llevar esa auditoría de acceso se hace aún más difícil. El registro manual a través de bitácoras de acceso está expuesto a errores por fallos humanos, información desactualizada, mayor esfuerzo logístico y, falencias en cuanto a confiabilidad de la información reportada, entre otros aspectos. Un control de acceso IoT es un sistema automatizado, que permite obtener datos confiables, donde se elimina la intervención humana e interactúa de manera ubicua.

En este trabajo de investigación se realizó un prototipo usando tecnología RFID, que permite llevar el control de acceso a un aula de clase en la UNAB. Esto permite que la información se pueda obtener en tiempo real, ayudando a mejorar procesos logísticos de las IES.

Tras identificar los requerimientos básicos de este sistema y necesidades específicas de la UNAB, se continuó a la etapa del diseño del prototipo a implementar; luego se implementó en un aula de la universidad para evaluar su uso en el entorno universitario.

Los resultados evidencian que un sistema IoT para control de asistencia y auditoría en IES, no solo posee un nivel de aceptación considerable, sino que permite reducir el tiempo que se requería; la velocidad al hacer uso de este sistema, permite usar el tiempo de clase para los temas de la misma y a su vez, cumple con los requisitos dados por el MEN.

PALABRAS CLAVES: Control de acceso, RFID, IoT, Educación superior, Telemática.

IOT BASED ACCESS CONTROL TECHNOLOGY FOR HIGHER EDUCATION. PROTOTYPE APPLIED TO ACCESS CONTROL AND AUDITORY TO CLASSROOMS AT UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB (COLOMBIA)

José David Ortiz Cuadros, Student
PhD, Cesar Darío Guerrero Santander, Thesis Director

ABSTRACT

In Colombia, the majority of Higher Education Institutions do not have automated access control systems for classrooms. This prevents to get information in real-time that allows audit of student attendance to class and compliance by teachers with established class schedules.

At the Autonomous University of Bucaramanga - UNAB, given that it is an open-door institution that does not restrict entry to any citizen, carrying that access audit becomes even more difficult. The manual registry through access binnacle is exposed to errors in the capture of data due to human failures, outdated information, greater logistical effort, and shortcomings in terms of the reliability of the reported information, among other aspects. Access control based on IoT is an automated system, which allows obtaining reliable data, where human intervention is eliminated and interacts with people in a ubiquitous manner.

In this research work, a prototype was made using RFID technology, which allows the control of access to a classroom in the UNAB. This allows the information to be obtained in real time, helping to improve IES logistics processes.

After identifying the basic requirements of this system, the specific needs of the UNAB were evaluated and so, moving on to the design stage of the prototype to be implemented; then the implementation of the same in a classroom of the university was carried out together with the tests to evaluate its use in the university environment.

The results show that the use of IoT systems for the control of assistance and audit in IES, not only has a considerable level of acceptance, but also allows to reduce the time that was required; the speed when using this system, allows to use class time for the topics of the same and in turn, meets the requirements given by the MEN.

KEYWORDS: Access control, RFID, IoT, Higher education, Telematics.

INTRODUCCIÓN

Uno de los aspectos neurálgicos en la administración de Instituciones de Educación Superior, se relaciona con la necesidad de contar con mecanismos que permitan conocer el cumplimiento de las actividades de docencia de los profesores y el registro de la asistencia de los estudiantes a las clases. Aplicaciones existentes en el ámbito universitario han usado diversas tecnologías para reducir costos de gestión y a su vez, han sido implementadas en su mayoría como medio de apoyo para proveer una herramienta tecnológica que ayude a las tareas de vigilancia de las universidades (Sowjanya & Nagaraju, 2016; K. C. Wang, Wang, Jia, & Zong, 2012).

La seguridad cobra vital importancia en cuanto a la calidad de enseñanza, ya que esta se ve afectada por los actos delincuenciales como: daños a la propiedad, robo de equipos y seguridad del ambiente estudiantil (Lozano Segura, 2013). Existen soluciones que pretenden solventar estos problemas, pero no cumplen con todas las exigencias que estas representan ya sea por exclusión a personas con problemas de capacidad reducida (Sowjanya & Nagaraju, 2016); por otro lado estos sistemas tradicionales cuentan con poco almacenamiento y no facilitan las tareas de gestión requeridas por las Instituciones de Educación Superior (K. C. Wang et al., 2012).

Una alternativa de solución al problema de control de acceso se conecta con el concepto de Internet de las Cosas - IoT. IoT hace referencia a la conexión digital de objetos que para las personas son cotidianos a Internet mediante sensores, término que fue propuesto por Kevin Ashton en el año 1999, mientras trabajaba en el MIT desarrollando actividades de investigación sobre el campo de la identificación por radiofrecuencia – RFID, haciendo uso de sensores (Ashton, 2009). Esta es la aproximación que se utiliza para el desarrollo de este proyecto.

Este proyecto está orientado a desarrollar una solución basada en RFID, utilizando como doble factor de autenticación el reconocimiento facial, evitando la falsificación de registros, capturando información fiable y real. Al utilizar un sistema IoT, este permite que se pueda crear un sistema automatizado y libre de fallos humanos, permitiendo un ambiente ubicuo entre la comunidad académica y la

tecnología propuesta. Se plantea crear un prototipo que permita controlar el acceso a las aulas de las instituciones de educación superior, donde usando la tecnología de Identificación por Radiofrecuencia - RFID se determinará si se permite el acceso a las aulas de clase, mediante un algoritmo para la toma de decisiones.

El documento se encuentra organizado de la siguiente manera: (i) Planteamiento del problema, justificación, pregunta de investigación e hipótesis, (ii) Objetivos, (iii) Antecedentes, (iv) Marco referencial, (v) Diseño metodológico, (vi) Resultados, (vii) otros resultados y (viii) conclusiones y recomendaciones.

1. PLANTEAMIENTO DEL PROBLEMA, JUSTIFICACIÓN, PREGUNTA DE INVESTIGACIÓN E HIPÓTESIS

Con el fin de garantizar la seguridad de la comunidad académica, algunas Instituciones de Educación Superior – IES implementan mecanismos de control de acceso de forma manual o semimanual en el ingreso de sus instalaciones. Estos mecanismos no llegan generalmente a replicarse en los salones y laboratorios y, se llevan a cabo con una baja eficiencia en la gestión y con costos operativos altos (Zhang, 2014). Teniendo en cuenta que el número de personas que ingresan cada día a las IES es considerable, se hace necesario contar con mecanismos efectivos de control de acceso no solo a las instituciones sino a aulas y laboratorios que minimicen el riesgo de todo tipo de actividades delictivas (Lee, Wu, Su, & Shen, 2016).

El no poseer un sistema automatizado y que permita ser actualizado a las nuevas necesidades que se presenten, hace que la gestión en el control de acceso se vea altamente afectada y la seguridad comprometida; los delincuentes son capaces de violar los sistemas tradicionales, obligando a realizar modificaciones y crear métodos para poder proporcionar la seguridad adecuada (Sowjanya & Nagaraju, 2016). Según Lozano, la delincuencia generada en las universidades, trae consecuencias directas en cuanto a la calidad de enseñanza, como a la seguridad de las instalaciones, donde la delincuencia está aumentando y expresa que la implementación de dispositivos tecnológicos es una forma de contra arrestar estos efectos (2013).

La Universidad Autónoma de Bucaramanga – UNAB, es una universidad de puertas abiertas que no restringe el acceso a ningún ciudadano. Esto no solo aplica para el campus abierto sino para el ingreso a los salones de clase. Debido a lo anterior, se hace necesario llevar una bitácora de acceso a la universidad; el no tener un control automatizado hace que se deba realizar un mayor esfuerzo en cuanto a logística y control adecuado para la seguridad.

Actualmente la universidad debe enviar personal de seguridad para abrir algunos de las aulas de clase, donde deben dejar a un lado sus labores de vigilancia para desplazarse a los salones y proceder a abrirlos o cerrarlos, sin llevar un control exacto de quien accede o no a un salón, exponiendo a errores y dando paso a falencias de seguridad en este proceso. En el momento que un profesor sale del salón al finalizar una clase, generalmente el vigilante aún no ha cerrado el aula y

queda expuesto el inventario dentro del mismo; para el caso de cambios de clase contiguos, o sea, donde se acaba una clase y luego continua otra, usualmente el salón permanece abierto desde que el docente de la clase anterior sale, hasta que el docente de la clase siguiente llega, donde los intervalos de tiempo en algunos casos pueden llegar a ser suficientes para quienes cometen actos delictivos.

Por otra parte, se cuenta con personal encargado de realizar un control de asistencia a docentes, tomando de manera manual fotografías por medio de tabletas para mantener evidencia; al ser un procedimiento humano, se está expuesto a errores humanos por cambios de salones que no fuesen avisados, confundirse de salón, entre otros. La mala manipulación de los dispositivos tecnológicos puede resultar en la pérdida de evidencia fotográfica, consumo de espacio y almacenamiento.

Generalmente un salón suele estar con las luces encendidas aunque no esté nadie en el salón, aumentando el consumo energético y reduciendo el tiempo de vida de los sistemas de iluminación, reflejándose en inversiones que se realizan en periodos más cortos para mantener la parte luminaria activa y en óptimo estado para los estudiantes (Patino, Moreno, Figueroa, Garcia, & Martin, 2017; W. Wang, Krishna, & McFerran, 2017).

Al automatizar todos los procesos, el control de acceso a los salones y la iluminación del mismo, se subyugan los errores humanos y el consumo energético generado. Al no necesitar al vigilante para abrir el salón, este puede continuar con sus labores de vigilancia sin abandonar su puesto de trabajo y así, mantener el nivel de seguridad del edificio. Para poder acceder al salón, se deberá contar con un permiso para el horario específico, eliminando falencias en cuanto que ingrese una persona que no estaba autorizada y el vigilante por error le dio acceso; de la misma manera, se puede saber quién ingresó y a qué hora. Al tener un listado de acceso, este suplanta el personal que realiza las auditorías, eliminando fallos que estos pudieran cometer y de igual manera, reduciendo costos operacionales para la universidad (Nainan, Parekh, & Shah, 2013)

Actualmente el control de estudiantes que asisten a clase está a cargo de los docentes[1], siendo una tarea que no siempre se cumple y por consiguiente, no se tiene un seguimiento riguroso y es alejado de la realidad; al igual que el control docente, se llevará a cabo un control automatizado y libre de errores humanos,

[1] La UNAB por ejemplo, hace uso del Sistema SIGA para llevar el control de asistencia a clases.

permitiendo tener estadísticas cercanas a la realidad (Silva, Filipe, & Pereira, 2008).

1.1 JUSTIFICACIÓN

Reemplazar el método actual por un sistema automatizado traería varias ventajas: (i) Bitácora de control de acceso en tiempo real, con datos confiables y libre de errores humanos; (ii) Apoyo a las unidades académicas de bienestar universitario de las IES, al poseer información en cuanto a la asistencia de estudiantes en clase, esta información puede ser usada para la detección temprana de casos de deserción estudiantil y al mismo tiempo, poder tomar a tiempo medidas preventivas en estos casos; (iii) Reducción de costo del control al no requerir de personal que desarrolle actividades de toma de asistencia a los docentes; (iv) Ofrece un uso eficiente del consumo energético de las aulas de clase; (v) Apoyo a la eficacia de los procesos de seguridad requerida en las IES; y (vi) Disminución de costos operaciones.

1.2 PREGUNTA DE INVESTIGACIÓN

¿De qué manera se podría controlar el acceso a salones de clase y llevar un registro automatizado de la información requerida para las auditorías académicas?

1.3 HIPÓTESIS

Utilizando IoT, se puede realizar controles en tiempo real y a su vez, obtener toda la información necesaria para los procesos de auditorías académicas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Construir un prototipo basado en tecnologías IoT de un sistema de control de acceso y auditoría de salones de clase en instituciones de educación superior.

2.2 OBJETIVOS ESPECÍFICOS

1. Elaborar un estado del arte sobre sistemas de control de acceso basados en tecnologías de Internet de las Cosas aplicados a instituciones de educación superior.
2. Determinar requerimientos generales, funcionales y no funcionales, para Instituciones de educación superior de los sistemas de control de acceso basados en IoT, haciendo énfasis en los específicos para el control del ingreso a salones y auditoría en la UNAB.
3. Diseñar, a nivel de hardware y software, un sistema de control de acceso basado en tecnologías IoT que atienda a los requerimientos generales de las IES y a los específicos para el control del ingreso a salones y auditoría en la UNAB.
4. Implementar, a nivel de hardware y software, un prototipo funcional de sistema de control de acceso basado en tecnologías IoT para el control del ingreso a salones y auditoría en la UNAB.
5. Realizar una prueba piloto del prototipo implementado en un aula de la UNAB para la medición de su efectividad en cuanto al control y auditoría del ingreso.

3. ANTECEDENTES

El Trabajo de Investigación titulado “Control de acceso basado en tecnologías IoT en Instituciones de Educación Superior. Prototipo aplicado al control del ingreso a salones y auditoría en la Universidad Autónoma de Bucaramanga - UNAB (Colombia)”, es un trabajo de investigación desarrollado desde las actividades investigativas del Semillero de Investigación en Telemática (SINET) en la línea de investigación en Telemática, adscrito al Grupo de Investigación en Tecnologías de Información (GTI). El proyecto está articulado con las actividades investigativas llevadas a cabo en el Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT).

El Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT) es una alianza entre universidades, líderes tecnológicos mundiales y empresas ancla para potenciar el desarrollo económico del país desde el desarrollo tecnológico y la innovación a través de las tecnologías del Internet de las Cosas, buscando resolver las necesidades de diferentes sectores productivos del país. El CEA-IoT es una iniciativa impulsada desde el Ministerio de las TIC, con el apoyo de Colciencias, y corresponde a una estrategia que busca posicionar a Colombia como líder regional en TIC. El Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT) es una alianza entre universidades, líderes tecnológicos mundiales y empresas ancla para potenciar el desarrollo económico del país desde el desarrollo tecnológico y la innovación a través de las tecnologías del Internet de las Cosas, buscando resolver las necesidades de diferentes sectores productivos del país. El CEA-IoT es una iniciativa impulsada desde el Ministerio de las TIC, con el apoyo de Colciencias, y corresponde a una estrategia que busca posicionar a Colombia como líder regional en TIC (CEA IoT, 2016).

La Universidad Autónoma de Bucaramanga[2] es una de las Universidades participantes en el CEA-IoT, que cuenta con la representación del Profesor César D. Guerrero como coordinador del Comité de Divulgación y Nuevos Negocios. Así mismo, están vinculados al CEA-IoT en representación de la UNAB tres investigadores planta, siete estudiantes de maestría y un investigador en Post-Doctorado; quienes están vinculados en las líneas del trabajo del CEA-IoT, a

[2] La Universidad Autónoma de Bucaramanga es una institución académica de orden privado del departamento de Santander. Cuenta con acreditación institucional de alta calidad por parte del Consejo Nacional de Acreditación a partir de diciembre de 2017 por un periodo de cuatro años.

saber: (i) Salud; (ii) Logística; (iii) Industria; (iv) Vestibles; (v) Seguridad; (vi) Agroindustria y Medio Ambiente y; (vii) Gobierno.

Con el desarrollo del presente trabajo de investigación “Control de acceso basado en tecnologías IoT en Instituciones de Educación Superior. Prototipo aplicado al control del ingreso a salones y auditoría en la Universidad Autónoma de Bucaramanga - UNAB (Colombia)” se pretende desarrollar una solución tecnológica basada en IoT orientada principalmente a favorecer dos procesos: (i) Ingresos a salones (docentes y estudiantes) y; (ii) Proceso de auditoría académica. Como productos esperados del proyecto se ha planteado el desarrollo de un prototipo funcional y una prueba piloto de la solución diseñada, así como la generación de artículos científicos que presenten el estado del arte, normatividades actuales, implementaciones a nivel global, nacional y departamental y, diseño metodológico de la solución propuesta.

4. MARCO REFERENCIAL

En esta sección se expondrán los principios teóricos y antecedentes que fundamentan la investigación a realizar. Contendrá todo lo concerniente a algunos antecedentes de investigación relacionados con el desarrollo del proyecto.

4.1 MARCO CONCEPTUAL

Se presentan tres conceptos base relacionados con el tema de investigación, a saber: Control de acceso, *IoT* e IES.

4.1.1 Control de acceso

Control de acceso se refiere al mecanismo que trabaja en función de la identificación que de alguna manera ya ha sido autenticada, para proveer acceso a datos, recursos o recintos (Armitage, 2014). Usualmente se encuentran diversos medios de control de acceso, por ejemplo: uso de contraseñas o huellas para desbloquear dispositivos móviles, uso de contraseñas para acceder a redes sociales, entre otros que permiten acceder a la información. Para acceder a recursos físicos, existen medios habituales como el uso de bandas magnéticas para permitir el acceso a las habitaciones de un hotel, huella digital, entre otros (Gordón Díaz, 2009).

4.1.2 *Internet of Things - IoT*

Gubbi et al, define *IoT* (*Internet of Things*) como "*cosas que tienen identidades y personalidades virtuales que operan en espacios inteligentes, usando interfaces inteligentes para conectarse y comunicarse dentro de contextos sociales, ambientales y de usuario*" (2013); tomando en cuenta lo anterior, IoT es todo objeto que pueda ser capaz de enviar y recibir datos de Internet y que a su vez, sea capaz de tomar decisiones a partir de ese intercambio de datos.

Por otra parte Guillem y Fries toman una postura similar a Gubbi et al. y adicionalmente afirma que: "IoT permite que tanto los objetos como las personas estén conectados, donde sea y cuando sea, con cualquier cosa y cualquier

persona" (2009). Esto siendo una de las razones por las que la adopción masiva de esta tecnología sea más factible.

4.1.3 Institución de Educación Superior - IES

El Ministerio de Educación Nacional dice que las IES "son las entidades que cuentan, con arreglo a las normas legales, con el reconocimiento oficial como prestadoras del servicio público de la educación superior en el territorio colombiano" (2010); Tomando como referencia lo anterior, las IES son las entidades encargadas de profundizar en una formación integral, siguiendo una serie de normas para ofrecer servicios de calidad.

Las IES se pueden clasificar según su carácter académico, (I) Instituciones Técnicas Profesionales, (II) Instituciones Tecnológicas, (III) Instituciones Universitarias o Escuelas Tecnológicas y (IV) Universidades (Ministerio de Educación Nacional de Colombia- MEN, 2010).

4.2 MARCO TEÓRICO

En este capítulo, se expondrán las teorías utilizadas en el marco de este proyecto, tales como sistemas de control de acceso, *IoT*, *RFID,* Sistemas embebidos, biometría y deserción escolar.

4.2.1 Sistemas de control de acceso.

Para el caso en particular expuesto en el proyecto, se centra en el poder conceder o denegar el acceso a un espacio físico (aulas de clase, laboratorios, entre otros espacios universitarios). El propósito principal de un control de acceso, es reducir la probabilidad de que personas no deseadas ingresen a recintos a los cuales no se quiere se ingrese y/o restringir el acceso a un número reducido de personas. Para cumplir su propósito, estos sistemas deben brindar seguridad y ofrecer un mínimo de funcionalidades dependiendo del entorno donde se aplique.

En la actualidad se están utilizando diversos métodos para realizar la identificación de personas, con la finalidad de lograr controlar el ingreso a recintos y así, crear sistemas completos que permitan el acceso a diferentes lugares. Cintas magnéticas (Sharma, Agarwal, & Singh, 2017), identificación biométrica (Banerjee & Woodard, 2012) y, RFID (Qiu, Chen, & Zhu, 2012) son los métodos más

utilizados en la actualidad. A pesar de existir diferentes métodos, el nivel de seguridad y el objetivo del sistema son los que definen cual es el indicado para realizar una implementación, pudiéndose utilizar dos métodos de manera integrada en un solo sistema.

4.2.1.1 Cintas magnéticas. Esta tecnología se basa en la lectura de una banda que se encuentra formada por un material plástico recubierto de óxido férrico, cuyo tamaño es menor a dos centímetros y sobre este, se graba la información consignada en puntos magnetizados, los cuales representas números binarios, es decir, un uno o un cero (Hernández, Valencia, & Morales).

Las cintas magnéticas permiten grabar grandes cantidades de datos siendo esta una de sus ventajas, pero por otra parte, son muy lentas (Rodríguez Mederos, Montes de Oca Sánchez de Bustamante, & Dorta Héctor, 2002).

4.2.1.2 Sistemas de identificación biométrica. Este tipo de sistema realiza una identificación de una persona utilizando características únicas de cada persona (Jain, Hong, & Pankanti, 2000; Masek, 2003). Este sistema permite ejercer un nivel de seguridad mayor frente a otros tipos de autenticación, debido que la información capturada para la identificación es única e intransferible (Sheela & Vijaya, 2010).

4.2.1.3 *Radio Frequency Identification*. Este Sistema debido a su rapidez junto con sus prestaciones ha tenido una gran acogida al no necesitar una vista directa entre el emisor y receptor, como adicional la velocidad de lectura (Meli, Gysel, Würms, & Meli). Al IoT querer identificar objetos de manera única, RFID se ve a menudo como requisito previo para el IoT ya que esta tecnología tiene la capacidad para realizar este tipo de identificación (Jia, Feng, Fan, & Lei, 2012).

4.2.2 Internet of Things

El término Internet de las Cosas fue utilizado por primera vez en 1999 por Kevin Ashton para describir un sistema en el que los objetos en el mundo físico podrían conectarse a Internet mediante sensores (Ashton, 2009). Los objetos utilizan sistemas embebidos o hardware especializado, que no solo permite se conecte a

internet, sino que permite programar eventos específicos para la ejecución de tareas que sean destinadas de manera remota.

Como valor añadido a lo propuesto por Kevin Ashton, con el cambio y la evolución de la tecnología, organizaciones como la *International Telecommunication Union* – ITU, en la Recomendación Y2060 ha ampliado el concepto de IoT acorde a la actualidad, diciendo:

> *IoT* es una Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de cosas (físicas y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras (International Telecommunication Union - ITU, 2012, p. 7).

Para el año 2011, CISCO mostró y proyectó cifras acerca de dispositivos conectados a Internet comparado con la cantidad total de la población (Evans, 2011): En el año 2003 se conectaban a Internet 500 millones de dispositivos, dando como promedio 0.08 dispositivos por persona; la cantidad de dispositivos conectados a Internet superó el número de personas hacia el 2008; y se espera que en el año 2020 se cuente con un numero de dispositivos a Internet superior a los 50 mil millones, dando como promedio, 6.58 dispositivos por persona. Lo anterior representando para las empresas más de $3 mil millones de dólares provenientes de usuarios finales y procesos industriales (Says, 2015).

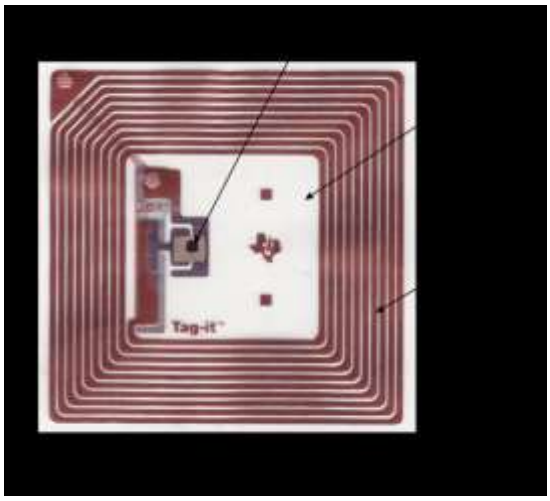
4.2.3 Identificación por Radiofrecuencia - RFID

RFID *(Radio Frequency Identification)* es una tecnología de comunicación inalámbrica que permite leer la identidad guardada en una etiqueta electrónica de bajo costo, estas etiquetas se pueden detectar sin necesidad de contacto (N. Raza, Bradshaw, & Hague, 1999; Want, 2006). RFID recolecta datos de manera automática, sin requerir intervención automática y minimizando los errores humanos (Rogers, Jones, & Oleynikov, 2007).

El sistema RFID permite que las implementaciones de gran escala, sean implementaciones de muy bajo costo haciendo que sea una solución viable para las empresas e industria donde se requiera llevar controles logísticos (Glidden et al., 2004).

4.2.3.1 Etiquetas o Tag's RFID. Son quienes reciben la señal RFID enviada por las antenas, conformados por un chip y una pequeña antena, generalmente el tag contiene la información del objeto al cual está adherido (productos, activos de empresas, personas, etc.) y estos tags pueden ser encapsulados o estar en forma de etiqueta (Ver Figura 1).

Figura 1 RFID chip y antena.



Fuente: Texas Instrument

La etiqueta por medio de señales de radio transmite la información que contiene, dicha transmisión es capturada por las antenas receptoras que se encargan de enviar la información por la red y llevarla al servidor o sistema que esté recolectando los datos (Posamentier, 2005; Strauss & Daud, 2000).

4.2.3.2 Tipos de etiquetas. Los sistemas RFID tienen tres categorías de etiquetas: de solo lectura (no se pueden modificar), etiquetas de una sola escritura (permiten múltiples lecturas) y etiquetas de lectura/escritura (se pueden leer y escribir múltiples veces) (Bohn & Mattern, 2004); sin embargo, solo dos tipos de etiquetas RFID son los principales y están contenidos en las categorías ya mencionadas:

- Etiquetas activas que están conectadas a fuentes de energía interna (pila, batería, etc.). Las etiquetas activas mejoraron la portabilidad, pero a un alto costo y con una duración restringida (Ni, Liu, Lau, & Patil, 2004).

- Etiquetas pasivas que utilizan energía que se crea a una distancia corta a través de la señal de radio del transmisor. Estas etiquetas son más económicas y, por lo general, más pequeñas y tienen una duración prácticamente ilimitada. Su aspecto negativo es que requieren una importante cantidad de energía específica de parte del lector para funcionar (Ni et al., 2004).

4.2.3.3 Frecuencias de operación. Los sistemas RFID funcionan en varias bandas de frecuencia, banda de baja frecuencia, banda de alta frecuencia y banda de frecuencia ultra alta. La banda baja de frecuencia (LF) es 124 a 135 kHz. La banda de frecuencia alta (HF) oscila entre 3 MHz a 30 MHz, siendo 13,56 MHz la frecuencia más usada. La banda de frecuencia ultra alta (UHF) que opera entre 300 MHz a 1 GHz. Generalmente, un sistema RFID opera ya sea a 2,45 GHz o 5,8 GHz, siendo la frecuencia de 2.45GHz la más común (Curty, Declercq, Dehollain, & Joehl, 2006; Juels, 2006).

4.2.4 Sistemas embebidos

Un sistema embebido es definido como un hardware que posee capacidades para el procesamiento de información, diseñado para cumplir un propósito general (Saib & Suzuki, 2002; Schoeberl, 2008). Estos sistemas tienen todos sus componentes integrados en una placa base (chip de video, memoria, entre otros), con un tamaño reducido.

Algunos de los sistemas embebidos más comunes son la Raspberry Pi, Arduino e Intel Edison, estos disponen de diferentes características diferenciales como: Memoria RAM, Capacidad del almacenamiento, dispositivos de comunicación inalámbrica incluido o con posibilidad de conexión y capacidad de procesamiento de video en algunos sistemas.

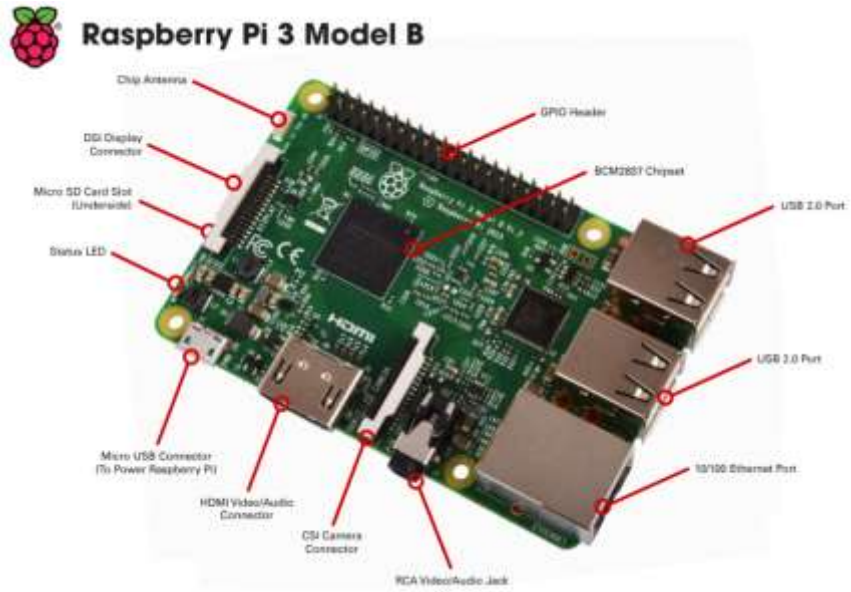
4.2.4.1 Raspberry Pi. Es una pequeña, potente y económica placa de computadora, orientada a la educación y fue lanzado al mercado en el año 2012 (Ver Figura 2). Es del tamaño de una tarjeta de crédito con mucho rendimiento y con un valor entre $35 a $45 Dólares, siendo una plataforma perfecta para interconectarse con diversos dispositivos (Vujovic & Maksimovic, 2014).

Figura 2 Placa Raspberry Pi

Fuente: raspberry.org

La Raspberry Pi tiene un procesador, chip gráfico, memoria RAM y una interfaz para conectar diferentes tipos de dispositivos o sensores (Ver Figura 3). Esta placa utiliza una memoria SD, la cual hace función de disco duro; también cuenta con un puerto Ethernet y en sus nuevas versiones WiFi (Richardson & Wallace, 2012).

Figura 3 Componentes Raspberry Pi

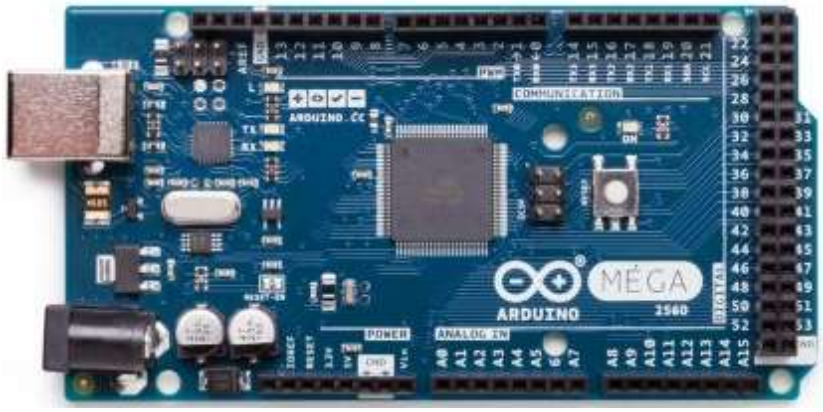


Fuente: Desing Spark

El software permitido por esta placa, hoy día es diverso gracias al auge que ha tomado IoT y la facilidad que la Raspberry ofrece para realizar despliegues de este tipo. Existen sistemas operativos como Raspbian (versión modificada del Debian), Aeros, Andriod, Kali Linux, Windows 10 IoT Core, entre otros.

4.2.4.2 Arduino. Plataforma electrónica de código abierto, para la construcción de prototipos, utilizando como lenguaje de programación el *Arduino Programming Language* y *Arduino Development Enviroment (Badamasi, 2014; Brock, Bruce, & Reiser, 2009)*. Esta plataforma lanzada al mercado en el año 2005 (ver Figura 4) posee un entorno de desarrollo flexible, con capacidad para controlar algunos dispositivos y puede leer datos enviados por diferentes sensores (Doukas, 2012).

Figura 4 Arduino MEGA 2650



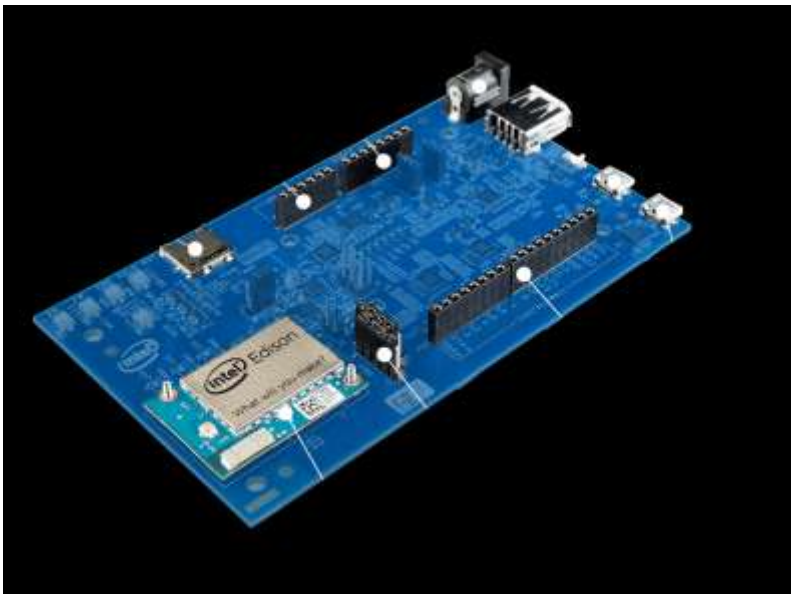
Fuente: Arduino.CC

Arduino posee varios puertos de entrada y salida que permiten la conexión a diferentes sensores para poder interactuar con el mundo físico; los microcontroladores van a comunicarse por medio de los puertos de entrada y salida, para leer la información emitida por los sensores y enviar señales hacia los actuadores (D'Ausilio, 2012).

4.2.4.3 Intel Edison. Módulo de computación desarrollado por Intel (Ver

), desarrollado para el uso en *Wereables* y en ambientes *IoT* (Dubey et al., 2015; A. Raza, Ikram, Amin, & Ikram, 2016). Al igual que el Arduino, posee puertos de entrada y salida que de la misma manera permite la comunicación con actuadores y sensores.

Figura 5 Componentes Intel Edison



Fuente: Intel Corporation

Cuenta con Sistema en Chip (SoC por sus siglas en inglés) Intel Atom de 22nm Dual Core a 500 Mhz y al mismo tiempo, con un microcontrolador de 100 Mhz, 1 GB de Ram, 4 GB de EMMC, WiFi y Bluethooth (Dubey et al., 2015).

4.2.5 Biometría

Según Serratosa, es una ciencia que utiliza técnicas para el análisis de distancias y posiciones entre partes del cuerpo, permitiendo identificar o clasificar personas (2008). Existen diferentes rasgos biométricos que pueden utilizarse con el fin de aplicar estas técnicas, tales como: huellas dactilares, reconocimiento facial, el iris, la mano, la retina y la firma (Banerjee & Woodard, 2012).

Los dispositivos biométricos consisten en un lector que permita el escaneo, un software para digitalizar la información escaneada y así, poder aplicar alguna de las técnicas de verificación y una base de datos en la cual se almacena la información biométrica que va a ser utilizada para realizar la comparación (Sabol, Nick, Earl, Shelton, & Esterline, 2016).

La biometría es robusta, ofrece gran fiabilidad y posee diversas técnicas, pero aun así, existe riesgo de falsificación (Pouryayevali, Wahabi, Hari, & Hatzinakos, 2014; Raghavendra, Raja, Surbiryala, & Busch, 2014). En la actualidad, se utiliza a gran

escala en dispositivos móviles, en donde se identifica a un usuario a través de la huella digital, siendo esta una de las técnicas con mayor aceptación por la población (Meng, Wong, Furnell, & Zhou, 2015).

4.2.6 Deserción escolar

Según el Ministerio de Educación Nacional de Colombia – MEN (2011), "l*a deserción es la interrupción o desvinculación de los estudiantes de sus estudios. Es un evento que aunque le ocurre al niño tiene causas y consecuencias en las instituciones educativas, las familias o el sistema educativo"*. Por otra parte, el MEN en su libro Deserción estudiantil en la educación superior colombiana indica que "*Aunque actualmente la definición de deserción estudiantil continúa en discusión, existe consenso en precisarla como un abandono que puede ser explicado por diferentes categorías de variables: socioeconómicas, individuales, institucionales y académicas*" (2009).

La deserción puede ser de tres tipos (Ministerio de Educación Nacional de Colombia - MEN, 2011): (i) Según su duración la deserción puede ser temporal o definitiva, donde se evidencia el abandono de un curso, pero al siguiente periodo nuevamente lo matricula o, en otros casos estos no regresan al sistema educativo; (ii) Según su alcance, en el cual se puede tener una deserción del establecimiento educativo o del sistema educativo, siendo el primero considerado como traslado; (iii) Según la temporalidad, en el cual se habla de un periodo o periodos de tiempo y esta podría reconocerse según el nivel educativo (preescolar, primaria, secundaria, media o universitaria, o incluso los grados escolares).

Según los datos del Sistema para la Prevención de la Deserción de la Educación Superior (SPADIES), para universidades e instituciones universitarias, el porcentaje de deserción por período ha venido disminuyendo (SPADIES, 2016): Para el segundo periodo de 2010 se tenía un porcentaje de 23.51%, segundo periodo de 2013 contaba con un porcentaje de 15.13%, en el primer periodo del 2014 el porcentaje estaba en 13.54% y para el primer periodo de 2016 en 11.80%, siendo este porcentaje el ultimo reportado por el SPADIES; para el primer periodo de 2016 en el departamento de Santander, el porcentaje de disertación es del 9.81%.

En la Universidad Autónoma de Bucaramanga, se denomina Seguimiento a la permanencia estudiantil a través del Sistema para la Gestión Académica – SIGA, el cual está compuesto por tres módulos (Bienestar Universitario UNAB, 2016): (i)

Caracterización del estudiante, implementado para completar toda la información básica en el sistema académico, siendo este clave para calcular variables de datos requeridas para los indicadores de riesgo académico. (ii) Control de asistencia, donde se realiza a través de tres actores; el docente, encargado de tomar lista, hacer ingreso a estudiantes que no asisten a clase y observación de posibles motivos de inasistencia; el Coordinador, ingresa observaciones y diferentes motivos dados por el estudiante, a su vez, este generara los reportes. El administrador, se encarga de asignar y habilitar a los usuarios del sistema, crear varíales de caracterización, entre otras funciones. (iii) Alerta temprana, donde se construyen los indicadores con los cuales se calcula el riesgo académico; por otra parte, genera correos automáticos a los responsables de atender riesgos tanto académicos, como los financieros.

4.3 ESTADO DEL ARTE

La revisión del estado del arte que se presenta a continuación se encuentra dividida en dos partes, una con la revisión sistemática de la literatura y otra, que contiene una compilación de resultados de otras investigaciones sobre sistemas de control de acceso utilizando la tecnología RFID.

4.3.1 Revisión sistemática de la literatura

La búsqueda fue realizada utilizando las siguientes parlabas clave: *Access Control, IoT* y *Higer Education.* El rango de búsqueda fue delimitado entre los años 2012 y 2018, realizada el 25 de febrero de 2018 por última ocasión. Para la realización del estado del arte, fueron recuperados un total de 549 documentos.

En la Figura 6, los documentos recuperados son presentados según su año de publicación. Se puede evidenciar que al paso del tiempo hay un aumento en el interés o relevancia del área de estudio; el año 2016, ha sido el año con mayor número de publicaciones (181 en total), para el transcurso del 2017, han sido publicados 83 documentos.

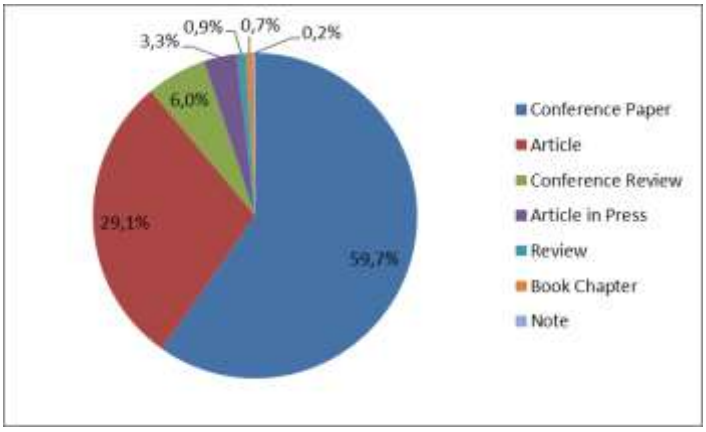
Figura 6 Documentos por año

Año	Documentos
2012	45
2013	49
2014	94
2015	97
2016	181
2017	83

Fuente: Elaboración Propia

En la Figura 7, se clasifican los documentos según su tipo. Se tiene que el 59.7% son artículos de conferencia, 29.1% son artículos publicados, 6% son revisiones de conferencias, 3.3% son artículos en proceso de impresión, 0.9% son revisiones de la temática tratada, 0.7% capítulos de libro y 0.2% son notas.

Figura 7 Tipos de Documentos



Fuente: Elaboración Propia

Los países que lideran el tema de investigación son China (102 documentos), Estados Unidos (68 documentos) y Corea del Sur (47 documentos). Ver Figura 8.

Figura 8 Número de documentos por país

Fuente: Elaboración Propia

En la Tabla 1, es presentada la síntesis del estado del arte. En total se recuperaron 13 referencias que tratan temas relacionados con *IoT, Access Control, RFID* y *Higher Education.*

Tabla 1 Referencias estado del arte

Autor	Año	Titulo	País	KeyWords	Citaciones
Risalat, et al	2017	Advanced real time RFID mutual authentication protocol using dynamically updated secret value through encryption and decryption process	Bangladesh	Encryption, Decryption, Protocol, Tag, Server, Mutual Authentication, RFID, Hash Function	0
Lee, et al	2016	A novel electronic lock using ultrasound Morse code based on FIR filter	Taiwan	Internet of Things, Morse code, FIR filter, ultrasound	1
Bagheri, et al	2016	The Effect of the Internet of Things (IoT) on Education Business Model	Reino Unido	Canvas Business Model, Classroom Access Control, Education Business Model, Energy Management and	1

Autor	Año	Titulo	País	KeyWords	Citaciones
				Ecosystem Monitoring, Higher Education, Internet of Things (IoT), Student's Healthcare, Teaching and Learning	
Sowjanya, et al	2016	Design and implementation of door access control and security system based on IOT	India	Internet of Things (IoT), biometric, password, security question, smart indication, door access	0
Shankar, et al	2016	Recognition of Faces - An Optimized Algorithmic Chain	India	Face Recognition; HCI; IoT; LBP; Neural Networks (NN).	0
Sousa, et al	2015	Wireless control and network management of door locks	Portugal	Access control, Bluetooth Low Energy, Near Field Communication, Wireless networks, Internet of Things	3
Jang, et al	2015	A Personalized Access Control Based on IoT	Corea	IoT; Personalized Access Control; Security Enhancement; Flexibility; Convenience	0
Palma, et at	2014	An internet of things example: classrooms access control over near field communication	España	Internet of Things; NFC; Arduino; sensors; smart environment; classroom access control	18
Zhang	2014	Design of a novel automatic access control system	China	RFID; embedded system; ARM; μC/OS-II; venues; access control	2
Farooq, et al	2014	RFID based security and access control system	Pakistán	Security and access control, RFID, face recognition	6
Shu, et al	2013	Dynamic Authentication with Sensory Information for the Access Control Systems	China	Authentication, sensory data, access control system, wireless rechargeable sensor	22
Wang, et al	2012	Research of RFID intelligent access control system in the internet of things	China	Internet of Things; Radio Frequency Identification (RFID); Intelligent access control system	0
Qui, et al	2012	Campus Access Control System Based on RFID	China	Campus access; control system; RFID; NCE	2

Fuente: Elaboración propia

4.3.2 Control de acceso en la actualidad

En los últimos años ha crecido el interés por RFID, debido a la fácil implementación y escalabilidad. Algunas de las aplicaciones que en la actualidad se utilizan sistemas basados en RFID son las cadenas de suministros (Chuu, 2014), venta de tiquetes de bus (Chandra, Soni, & Keshari, 2014), ventas (De Marco, Cagliano, Nervo, & Rafele, 2014), seguimiento de activos (Roper, Sedehi, & Ashuri, 2015), sistemas de control de acceso (Shu, Gu, & Chen, 2014), entre otros.

Actualmente existen otros sistemas de identificación que se utilizan para control de acceso que compiten con la tecnología RFID tales como: Sistemas biométricos y, Tarjetas magnéticas.

Sistemas biométricos. Para la identificación biométrica, se debe realizar análisis y/o mediciones de características físicas, utilizando las siguientes técnicas (Banerjee & Woodard, 2012):

- Reconocimiento de iris
- Reflexión retinal
- Geometría de la mano
- Geometría Facial
- Huellas dactilares

Una de las grandes ventajas de este tipo de identificación, se centra en el poder identificar directamente la persona y no una credencial u objeto, aunque a pesar de esto, no existen sistemas que ofrezcan una confiabilidad cercana al 100 por ciento (Banerjee & Woodard, 2012); para el caso de las huellas dactilares, estas tienden a desvanecerse con la edad y en algunos se acelera según el trabajo físico que realice con sus manos (Videla & A, 2016).

Tarjetas magnéticas. Las tarjetas magnéticas se basan en la lectura de una banda magnética, utilizando señales electromagnéticas que registran y codifican la información en una banda, esta información puede ser leída por una máquina y de esta manera se facilita una identificación instantánea (Gluck, 2015). Actualmente se utiliza esta tecnología para las tarjetas de crédito, aunque está siendo reemplaza por un chip de lectura y ahora está iniciando su uso con sistemas RFID (Sharma et al., 2017).

Su uso corresponde a la agilidad con la que trabaja el sistema, permite una identificación única y bajo costo. La mayor de las desventajas es su deterioro físico causado por la fricción; si se encuentra cerca de fuentes electromagnéticas puede modificar la información que esta contiene, haciendo perder información de utilidad.

Los sistemas RFID destinados al control de acceso que se utilizan actualmente, se implementan en lugares como bibliotecas, oficinas, centros de datos, hoteles y universidades, para llevar un control detallado de las personas que ingresan. Gracias al fácil uso, RFID permite adaptarse a diversas necesidades y así, permitiendo suplir varias necesidades que pudiesen presentarse en cuenta a todo lo que requiera logística.

En el caso de las bibliotecas, se emplea de forma que permite llevar control no solo de quien accede, sino de cual usuario está tomando prestado material bibliográfico (Pandey & Mahajan, 2012). Se pueden encontrar soluciones de este tipo implementadas en bibliotecas como la del vaticano (Biswas, 2016) que solo realiza las tareas de actualización automática de la base datos gracias a RFID; los autores Aydın & Yıldırım (2012) y Edwards & Orukpe (2014) han identificado la necesidad de no solo llevar control de inventario, llevándolos a desarrollar sistemas que permitan el control de acceso utilizando los beneficios que RFID brinda.

Umar Farooq et al, describe en su artículo un diseño de un sistema RFID para seguridad y control de acceso a implementar en hoteles de la universidad Premises (2014), donde para garantizar la fiabilidad de la información que viaja a través de la red, se propuso la utilización de protocolos orientados a la conexión, con el fin de asegurarse de tener los datos completos y sin perdidas en la base de datos.

Las oficinas y sitios de trabajo que se encuentran en un área amplia, usualmente poseen áreas que el acceso es restringido y en estos casos se ha optado por implementar sistemas de control de acceso RFID y para aumentar la seguridad del mismo, han optado por complementar con sensores para la lectura de huellas digitales (Castillo, Rojas, & Gómez, 2016; Shu et al., 2014). Obtener los datos de forma manual implica estar expuesto a fallos por errores humanos, este es uno de los factores clave por los cuales se ha optado para utilizar RFID, este permite realizar de manera automática y en tiempo real las acciones de lectura para identificar los usuarios del sistema; el modelo implementado por la mayoría de los

sistemas desarrollados por la parte académica, poseen en su diseño una base de datos, la cual contendrá los datos de los usuarios, si tienen permisos para acceder o no y de la misma manera, el momento en el que están ingresando, junto con las veces que han ingresado; el sitio web también hace parte del diseño, el cual permite la administración de los permisos, ingresar usuarios y ver la información que se encuentra en la base de datos de manera organizada.

Las soluciones comerciales que existen en el mercado, en su mayoría solo poseen un lector que está conectada a una tarjeta con instrucciones limitadas y poca memoria; la información que estas tarjetas pueden guardar es solamente la contraseña (si el sistema adicionalmente posee teclado) y el código de identificación de las tarjetas RFID, la cantidad de tarjetas a registrar puede variar según el fabricante, pero en su mayoría soportan hasta 40 diferentes usuarios en las soluciones de bajo costo. El requerir de un sistema para una cantidad de usuarios mayor suele ser costoso y en caso de requerirse otras funcionalidades, tienen un valor agregado que hace de la solución sea de difícil adquisición.

Los sistemas de embebidos tales como la Raspberry se están utilizando para integrarlo al sistema de control de acceso, permitiendo que este sea más fácil realizarle modificaciones e integrarle más funcionalidades en caso de ser necesario. El uso de esta tecnología permite realizar de manera sencilla el control de las luces del lugar en el cual se encuentre implementado que en el caso de universidades; lo anterior, reflejándose en: Reducción del consumo energético, aminorando los gastos de operaciones causados por mantenimiento, inversión en la compra de nuevas luminarias y el costo que genera el consumo eléctrico adicional y, reduciendo la emisión de CO2 (Gul & Patidar, 2015).

Lee at al, afirma que al aumentar el nivel de urbanización y la frecuencia de actividades delictivas, el fortalecer la seguridad y prevenir el robo es una tarea crítica a la cual se le debe prestar acción inmediata (2016); Sowjanya at al, argumenta que los sistemas de seguridad usualmente son violados por delincuentes y por tanto, existe la necesidad de crear nuevos métodos que proporcionen ambientes seguros (2016). Crear un lugar seguro y administrar el acceso de estudiantes a las aulas, laboratorios y otros lugares de las IES, son retos que a través de tecnologías como RFID y NFC pueden ser abordados, siendo tecnologías facilitadoras para la implementación de soluciones IoT y ayuda a mejorar la seguridad universitaria (Bagheri & Movahed, 2016).

Existen arquitecturas implementadas para el control de acceso, en el cual se implementa NFC y Bluetooth como solución para la automatización de soluciones. Sousa at al, muestra una solución en la cual se maneja la autenticación por medio de tarjetas NFC y teléfonos inteligentes, los cuales controlan una cerradura electrónica por medio del siguiente proceso: Una llave de autenticación es enviada desde la tarjeta NFC o teléfono inteligente, esta autenticación se realiza a través de la comunicación de un servidor, el cual contiene una base de datos administra y valida los permisos de acceso y, contiene un log de eventos (2015).

El bloqueo de puertas haciendo uso de llaves con cerraduras mecánicas a pesar de ser comúnmente utilizado y aceptado globalmente, suele tener problemas como la perdida de las llaves de las cerraduras, la copia no autorizada o hurto de las llaves, vulnerando la seguridad del lugar (Sowjanya & Nagaraju, 2016). Los sistemas tradicionales que cumplen funciones para controlar el acceso suelen ser simples, de baja eficiencia y con una capacidad de almacenamiento pequeña, impidiendo llevar un control óptimo que cumpla con los requisitos de seguridad como los ofrecidos por tecnologías IoT (K. C. Wang et al., 2012). Por otra parte, Jang et al, diseñó un sistema para el control de acceso basado en IoT, ya que otros sistemas comúnmente utilizados se ven afectados por problemas como: Exclusión de personas con funciones cognitivas reducidas, ancianos y niños, al requerir memorizar números secretos y, seguridad en cuanto a ingeniería social, afirmando que tanto este método de cerrojo digital, como la llave física, no son métodos seguros (2015).

Para las soluciones de control de acceso por medio de contraseñas, existen falencias en cuanto a la seguridad puesto que mantienen un control único, sin ningún registro de acceso individual (K. C. Wang et al., 2012). Sumado a lo dicho anteriormente, el uso de teclados al ser pequeños, dificultan el uso para personas mayores, personas con problemas de movilidad, al igual que suele ser incómodo el uso de este método al momento de introducir la contraseña y nombre de usuario(Sowjanya & Nagaraju, 2016).

Bagheri at al, dice que la seguridad toma un papel importante tanto en instituciones públicas como privadas, por la anterior razón, se han propuesto y desarrollado diversos sistemas de seguridad con el fin de mejorar algunos procesos que se tornan importantes y de vital importancia: Protección de la información, propiedad y la prevención contra el robo o la delincuencia (2016). La mayor parte de lugares que aún no poseen un sistema automatizado, se ven

afectados por la baja eficiencia de la gestión de control y el costo elevado de los gastos operativos, los cuales deben ser atendidos (Zhang, 2014).

En los campus universitarios se ha implementado RFID como solución para realizar el control de asistencia a los estudiantes, permitiendo llevar la información en tiempo real y sin errores con fines de toma de decisiones (Qiu et al., 2012; Silva et al., 2008). Las universidades con campus muy grandes o simplemente que mantienen sus puertas abiertas para el libre acceso a la misma, es difícil mantener un registro viable si no se cuenta con un sistema automatizado, por esto las soluciones existentes pretenden mantener en su diseño un esquema donde se refleje la gestión de la información, la cual tiene un valor importante. Zhang, tras la implementación de un sistema de seguridad y control de acceso basado en IoT, muestra en sus análisis experimentales que la eficiencia media del sistema utilizado es 38,4% mayor que otros métodos tradicionales y la precisión de control es en promedio un 48,9% mayor que las realizadas de manera manual (2014).

Palma et al, desarrollaron un sistema NFC basado en RFID, el cual les permitió administrar las aulas de clase en tiempo real, donde evidenciaron la escalabilidad de estos sistemas y la reutilización de los datos generados por el sistema (2014). Sin embargo, se han implementado otros métodos que ayudan a la autenticación de usuarios al sistema como el uso de huellas dactilares junto a RFID, el cual fue aplicado en la Universidad de Harbin para la gestión de acceso de estudiantes a los dormitorios, biblioteca y laboratorios (K. C. Wang et al., 2012).

RFID como sistema único de control de acceso, se ve expuesto a duplicaciones de las tarjetas que contienen la información de la persona y a su vez, proveen el acceso, por lo anterior, han utilizado medidas como el uso de cerraduras electrónicas usando ultra sonido (Lee et al., 2016); como medida para proteger la información del usuario que se encuentra contenida en la tarjeta, se ha implementado el uso de encriptación de los datos que se guardan en la misma, ayudando a no comprometer la seguridad del sistema (Risalat, Hasan, Hossain, & Rahman, 2017). Por otra parte, se considera el uso de herramientas biométricas como la huella digital (Sowjanya & Nagaraju, 2016), donde el reconocimiento facial se ve como herramienta de utilidad y se considera un elemento popular e importante para los sistemas que implementan la Interacción Persona-Computadora – HCI, donde se considera como aplicación critica para el control de acceso (Shankar & Udupi, 2016).

El control de acceso en gran medida, a pesar que se ha aplicado para gestionar el acceso de estudiantes a clase y llevar una bitácora, ha sido poco el uso de datos para controlar la asistencia a estudiantes y enfocándose en cosas como la seguridad de las instalaciones de las universidades. Por lo anterior, este proyecto tiene como fin, la utilización de un sistema de control de acceso enfocado en la asistencia a estudiantes y docentes por medio de la tecnología RFID y haciendo uso del reconocimiento facial como medida de factor de doble autenticación, elevando la seguridad y confiabilidad de la solución. De manera adicional, se abarcarán otras problemáticas como: apoyo a la seguridad de las IES, reducción de costos operacionales, optimización de los recursos energéticos y, tiempo de vida de elementos electrónicos en las aulas de clase y laboratorios. Como valor agregado, la información generada por este sistema de control de acceso basado en IoT, puede ser utilizada por unidades de Bienestar Universitario, en la toma de decisiones y medidas preventivas para la deserción estudiantil, siendo esta una problemática en la cual están haciendo frente tanto las IES como lo es la UNAB, al igual que Ministerio de Educación en Colombia.

4.4 MARCO LEGAL

Existen normas nacionales como internaciones que influyen en el desarrollo de este proyecto, siendo estas de vital importancia para el despliegue de la solución. Estas normas comprenden políticas de tratamiento de datos personales, uso de espectros electromagnéticos, uso de las tecnologías y decreto de educación.

4.4.1 Normas Colombianas

Para el caso de las normas colombianas, se tomaron en cuenta factores que influían directamente sobre el desarrollo de este proyecto y que era de vital importancia tomarlas en cuenta en el diseño, evitando incurrencias legales que se pudiesen aplicar.

4.4.1.1 Ley 1581 de 2012 – Habeas Data. Esta Ley dicta disposiciones del habeas data, reemplazando la antigua Ley 1266 de 2008, la cual fue sancionada en 2009. Su fin, es regular el manejo de la información que se encuentra contenida en bases de datos personales y de igual manera, este contemple integración con sistemas que ya posee la universidad y sin afectar las políticas

sobre protección de datos ya establecidas. La ley 1581 expedida por el Congreso de Colombia, determina que se debe garantizar a los usuarios el poder conocer, actualizar y rectificar la información que esta contenga (2012). El estado colombiano, del mismo modo ha dictado de manera adicional un decreto para reglamentar parcialmente la ley 1581.

4.4.1.2 Decreto 1377 de 2013. Este Decreto 1377 de 2013 (se reglamenta parcialmente la ley 1581): Define la relación contractual entre el encargado del tratamiento de datos personales y quien entrega sus datos personales, por medio de un contrato; el encargado de los datos, se obliga a mantener la confidencialidad, dar uso adecuado de los datos personales, entre otros. En caso de un mal uso, se debe indemnizar al titular (Ministerio de Comercio Industria y Turismo, 2013).

4.4.1.3 Decreto 886 de 2014 – Registro Nacional de Bases de Datos. Este decreto establece que tanto personas naturales como jurídicas del sector público o privado, deben inscribir todas las bases de datos que posean. Dichos registros, se deben hacer de manera independiente, si hay una base de datos para clientes y otra que se utilice para empleados, estas deberán ser registradas de manera individual y realizar el proceso de registro para cada una; en caso de incumplir con este decreto, acarreara a sanciones de carácter personal e institucional hasta por un valor al equivalente de 2.000 SMMVL (Ministerio de Comercio Industria y Turismo, 2014).

4.4.1.4 Ley 1341 de 2009. Se definen los principios y los conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC, se crea la Agencia Nacional de Espectro – ANE y dictan disposiciones: (i) Uso eficiente de la infraestructura y de los recursos escasos; (ii) Protección de los derechos de los usuarios y; (iii) Neutralidad tecnológica, donde se acoge la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de organismos internacionales competentes e idóneos (Congreso de la República de Colombia, 2009).

4.4.1.5 Resolución No. 711 –ANE. Establece cuales son las bandas de frecuencia para uso libre en el territorio nacional, tomando en cuenta las recomendaciones dadas por la ITU. Se definen las bandas de frecuencia que están para libre uso en el territorio nacional, parámetros técnicos, los modos en los que deben operar las bandas, aplicaciones y determina cuales son las bandas restringidas; por otra parte, *Establece que "*el espectro electromagnético es un bien público, inenajenable e imprescriptible sujeto a la gestión y control del estado, y garantiza la igualdad de oportunidades en el acceso a su uso en los términos que fije la Ley*" (Agencia Nacional del Espectro - ANE, 2016).*

4.4.1.6 Decreto Único Reglamentario 1075 de 2015. Contiene una compilación de leyes, decretos y resoluciones, permitiendo organizar en un solo texto la abundante normatividad que existe en la actualidad; El decreto trata algunos temas relevantes al proyecto, tales como (Ministerio de Educación Nacional de Colombia- MEN, 2015): (I) Seguimientos y controles de asistencia a los estudiantes e incluir en su reglamento interno los porcentajes de inasistencia máxima permitida para aprobación de un curso; (II) implementación de métodos que permitan la detección de deserción escolar y; (III) promoción al interior de las IES para la automatización de los procesos de reportes de información que se entren al Sistema Nacional de Información de la Educación Superior – SNIES, fomentando el uso de tecnologías de la información y a su vez, apoyando a la modernización del sector.

4.4.2 Normas Internacionales

Existen normas internacionales que influyen de manera directa el proyecto, que incluyen comunicación alámbrica, el uso del espectro radioeléctrico, aplicación de IoT y uso de RFID. Para el uso de la comunicación alámbrica e inalámbrica por medio de WiFi, se tendrán en cuenta las normatividades establecidas por la Unión Internacional de Telecomunicaciones y la estandarización sugerida por IEEE. Para la comunicación entre el tag y el lector RFID, se tomará en cuenta el estándar definido por la ISO.

4.4.2.1 802.31 – IEEE. Define el funcionamiento de una red de área local (*LAN*), utilizando velocidades de operación de 1 *Mbps* hasta 100 *Gbps*, utilizando una el protocolo de control de acceso al medio (*MAC*). Las consideraciones del sistema para redes de acceso compartido multi-segmento describen el uso de repetidores

que pueden llegar a tener velocidades operativas de hasta 1000 *Mbps* (Institute of Electrical and Electronics Engineers - IEEE, 2015).

4.4.2.2 Reglamento de Radiocomunicaciones – ITU. Las frecuencias y el espectro están limitadas en el uso, con el fin de obtener un funcionamiento adecuado de los servicios necesarios. Se debe garantizar que al asignar nuevas frecuencias o realizar cambios en la misma, no creen interferencias, lo anterior, tomando en cuenta el cuadro de atribución de bandas de frecuencias dado por la ITU para no interferir de manera perjudicial y evitar la saturación del espectro. Para las bandas de uso libre, se determina una potencia y frecuencia, con el fin de garantizar que se ofrezca una calidad de servicio óptima (Unión Internacional de Telecomunicaciones - UIT, 2012).

4.4.2.3 802.11 – IEEE. Este estándar especifica todas las normas de funcionamiento para una red de área local inalámbrica (*WLAN*). Establece identificadores de canales y frecuencias; toma en cuenta las superposiciones de ondas y uso de frecuencias para establecer un nivel de calidad de servicio óptimo, preservando el rendimiento de la red. Define el protocolo *CSMA/CA* (Múltiple acceso por detección de portadora evitando colisiones) para el uso de esta como método de acceso. En caso de la existencia de dispositivos de diferentes marcas, este protocolo garantiza la interoperabilidad de la red, sin perjudicar la calidad (Institute of Electrical and Electronics Engineers - IEEE, 2016).

4.4.2.4 ISO/IEC 14443. Establece los requisitos para las tarjetas RFID que comúnmente son utilizadas con el fin de realizar tareas de identificación. Las frecuencias de operación y potencias son dadas, con el fin de no interferir con otros medios y a su vez estas son clasificadas según la distancia de operación. Define el modelo de comunicación, dispuesto de dos partes: Inicialización y anticolisión, donde se describe como se debe realizar los escaneos en busca de conexiones potenciales, al detectar esta conexión, inicia un comando para las comunicaciones; para la comunicación existe protocolos de mensajería, en el que se maneja un formato para la lectura y otro para la escritura de la tarjeta RFID (International Organization for Standardization - ISO, 2016).

4.4.2.5 Recomendación Y.2060 del 2012. Se da una definición general del significado de *IoT*, aclarando su concepto y alcances. Compatibilidad, capacidad de administración, protección de la privacidad, son parte de los requisitos de alto nivel para esta tecnología, por otra parte, en el modelo de referencia propuesto se encuentra cosas como capacidades de soporte genéricas, interacción directa con la red de comunicaciones y, gestión del tráfico y congestión (International Telecommunication Union - ITU, 2012).

5. DISEÑO METODOLÓGICO

Este proyecto está dividido en cinco fases relacionadas entre sí, los cuales permiten cumplir con los objetivos específicos, permitiendo garantizar el cumplimiento del objetivo general expuesto en este trabajo de investigación. Para el desarrollo de este proyecto, se aborda el tipo de investigación aplicada, caracterizada por generar un nuevo conocimiento o usar el ya existente para dar respuesta a un problema o necesidad identificada (Colciencias, 2016). Esta investigación aplicada, también tiene un enfoque Mixto que, implica combinar los métodos cuantitativo y cualitativo en un mismo estudio (Sampieri, Collado, & Lucio, 2014).

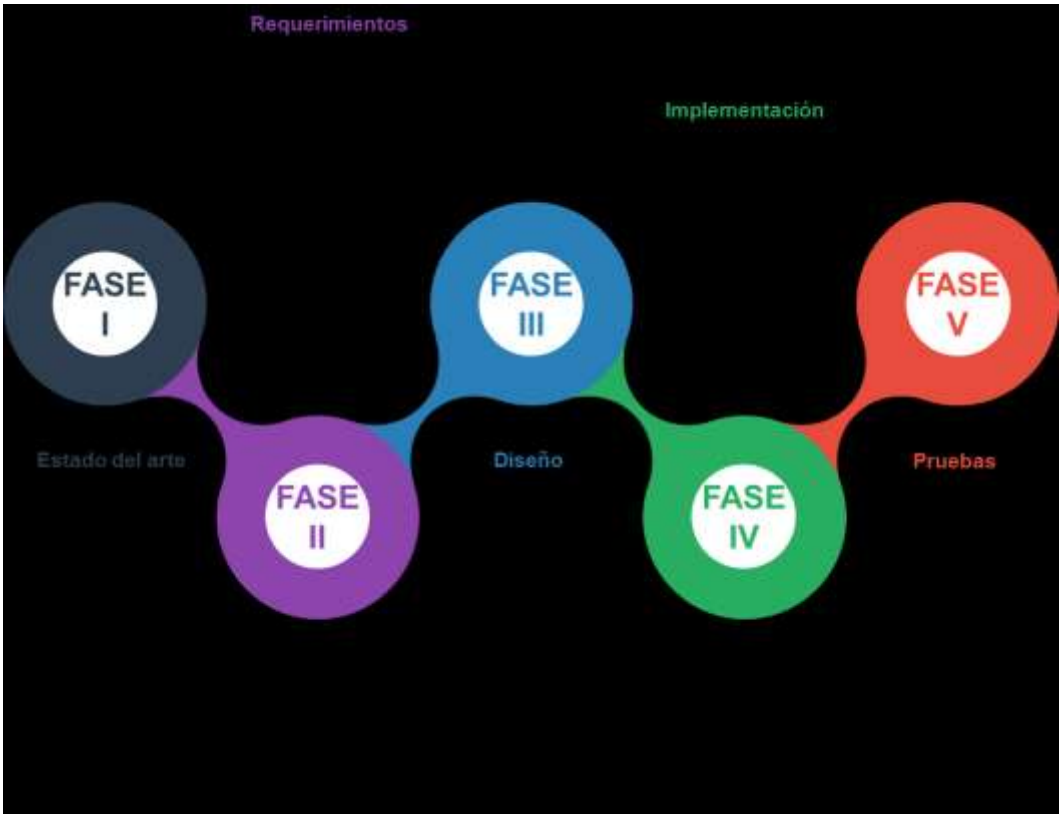
5.1 FASES DEL PROYECTO DE INVESTIGACIÓN

A continuación, se presentan a detalle las actividades y resultados correspondientes a cada fase del proyecto (Ver Figura 9).

Fase 1: Elaboración del estado del arte sobre sistemas de control de acceso basados en tecnologías de Internet de las Cosas aplicados a instituciones de educación superior. Siendo el primer resultado la revisión de la literatura sobre el uso de tecnologías basadas en IoT para las IES. Para llevar a cabo esta fase, se deben realizar las siguientes actividades:

- Búsqueda y revisión de la literatura sobre el uso de sistemas IoT para la asistencia de estudiantes en instituciones de educación superior.
- Lectura, clasificación y análisis de acuerdo a la relevancia de la información encontrada.

Figura 9 Fases del Proyecto de Investigación



Fuente: Elaboración propia.

Fase 2: Determinación de los requerimientos generales, funcionales y no funcionales, para Instituciones de educación superior de los sistemas de control de acceso basados en IoT, haciendo énfasis en los específicos para el control del ingreso a salones y auditoría en la UNAB. Como segundo resultado, se obtendrán dos documentos con los requerimientos generales, funcionales y no funcionales, uno para las IES y otro para el caso UNAB. Las actividades a realizar en esta fase son:

- Definición de procesos básicos de las IES.
- Búsqueda de datos utilizados para la realización de procesos básicos.
- Definición de los límites impuestos por el sistema.

Fase 3: Diseñar, a nivel de hardware y software, un sistema de control de acceso basado en tecnologías IoT que atienda a los requerimientos generales de las IES y a los específicos para el control del ingreso a salones y auditoría en la UNAB. Como tercer resultado, se obtendrá un prototipo funcional para el control de acceso como solución genérica para las IES y otro especifico con los requerimientos de la UNAB. Las actividades para llevar a cabo esta fase son:

- Hacer una encuesta de percepción estudiantil
- Diseño de una red, utilizando Redes Privadas Virtuales (*VPN*) que permitirá la comunicación entre la tarjeta de desarrollo y el servidor.
- Diseño de arquitectura cliente-servidor para el sistema de gestión y monitoreo.
- Diseño de un prototipo funcional de *hardware* y *software* para la comunicación, procesamiento y análisis de los datos capturados por el sensor *RFID*.

Fase 4: Implementación, a nivel de *hardware* y *software*, un prototipo funcional de sistema de control de acceso basado en tecnologías IoT para el control del ingreso a salones y auditoría en la UNAB. Como cuarto resultado, se hará la implementación del prototipo funcional en un aula de la UNAB. Como actividades para el desarrollo de esta fase están:

- Implementación del prototipo a nivel de *hardware* y *software* del sistema de control de acceso basado en *IoT*.
- Configuración de las aplicaciones.
- Pruebas del sistema

Fase 5: Realización de una prueba piloto del prototipo implementado en un aula de la UNAB para la medición de su efectividad en cuanto al control y auditoría del ingreso. Como último resultado, tomando en cuenta la fase cuatro, se tendrá una evaluación del sistema. Entre las actividades a realizar se encuentra:

- Evaluación del funcionamiento a partir de pruebas realizadas en un aula de la UNAB, teniendo en cuenta factores de gestión, seguridad y veracidad de la información.
- Socialización del rendimiento del sistema con estudiantes del Doctorado en Ingeniería de la UNAB y miembros del CEA IoT Nodo Oriente.
- Análisis de resultados.

- Documentación del trabajo de investigación.
- Hacer una encuesta de aceptación de tecnologías en IES

5.2 POBLACIÓN

La mayor parte de los usuarios del sistema son estudiantes ya que son quienes van a registrar una mayor cantidad de entradas al mismo; la población será representada por un número finito de estudiantes a quienes se les pregunta de manera aleatoria y sin preferencia en la elección de quienes participaran en la misma.

El grupo de estudiantes podrán ser de cualquier semestre, ya que cualquiera de ellos serán los potenciales usuarios de la solución. La población a tomar será de la ciudad de Bucaramanga y los casos de muestreo se centran en la UNAB ya que debe ser estudiante activo de algún programa de la universidad por el caso particular de estudio para esta tesis.

5.2 TÉCNICAS E INSTRUMENTACIÓN DE RECOLECCIÓN DE DATOS

Las técnicas definidas para realizar la recolección de datos para el sistema control de acceso basado en tecnologías IoT para las IES, es a través de encuesta por medio de un sitio web; en total se realizaron dos encuestas definidas para dos fases de desarrollo del proyecto (Fase III y Fase V) que permitan definir el diseño y ver a menor escala la viabilidad de la implementación solución en entornos reales. La primera encuesta (percepción) aplicada a estudiantes al azar durante un horario de afluencia estudiantil mayor, o sea, durante cambio de clases; para la segunda encuesta, se realizará con estudiantes de ingeniería de sistemas que estén cursando sobre los cuales se realizarán las diferentes pruebas del prototipo a desarrollar.

Para las pruebas realizadas en la implementación y la prueba piloto del prototipo, se tomarán en cuenta factores como la cantidad de captura de datos que debería realizar el sistema contra las capturas idóneas registradas; lo anterior corresponde

a la realización de mejoras del prototipo y la construcción de un prototipo que permita satisfacer los requerimientos planteados en la fase de diseño.

6. RESULTADOS

En este capítulo son presentados los resultados del proyecto de investigación, correspondientes a cada objetivo propuesto.

6.1 ESTADO DEL ARTE SOBRE SISTEMAS DE CONTROL DE ACCESO BASADOS EN TECNOLOGÍAS DE INTERNET DE LAS COSAS

Los sistemas de control de acceso realizados para el ámbito académico en las IES ha tenido un mayor interés en el paso del tiempo, para ello, desde la academia se han desarrollado diferentes mecanismos y usado diversos componentes tecnológicos; aunque existen soluciones propuestas desde la academia, no todas consideran el acceso del estudiante y el docente dentro del sistema que han propuesto, por otra parte, no todos trabajan con el dato de asistencia que se captura para generar los reportes pertinentes.

Para ampliar más información, en la Sección 4.3 es presentado el estado del arte de la investigación.

6.2 REQUERIMIENTOS GENERALES, FUNCIONALES Y NO FUNCIONALES, PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR DE LOS SISTEMAS DE CONTROL DE ACCESO BASADOS EN IOT

En esta sección se establecen los requisitos que debe tener un sistema para el control de acceso trabajado en este proyecto de investigación; atendiendo al objetivo específico dos, evidenciando los requerimientos funcionales y no funcionales, tanto de manera general para las IES, como los específicos para la UNAB.

Los requerimientos funcionales son descripciones de la interacción entre el sistema y ambiente, incluyendo al usuario y aplicaciones externas. Los requerimientos no funcionales hacen referencia a los aspectos no visibles del sistema por el usuario y que no tiene relación directa con el comportamiento funcional del sistema, incluyendo desempeño, precisión, recursos consumidos, seguridad, entre otros.

La revisión de la literatura permitió un primer levantamiento de requerimientos generales, tomando en cuenta las necesidades y aspectos evidenciados en los documentos; lo anterior, basado en las necesidades y dificultades encontradas que fueron presentadas por los autores.

6.2.1 Alcance de la solución

Esta solución está enmarcada en dos agentes, (I) *hardware* y (II) *software*; en ambos casos, se deberán realizar adecuaciones necesarias para dar cumplimiento con los requerimientos que contemplan realizar un control de ingreso a salones y auditoría en las IES, permitiendo la recolección de datos que ayudan a cumplir con los requerimientos dados por los entes normativos que rigen para estas instituciones, al igual que el cumplimiento las políticas internas.

El sistema capturará los datos a partir de una interacción por parte del usuario al acercar una tarjeta inteligente a un dispositivo lector y a partir de allí, el sistema actuará de manera automatizada.

6.2.2 Especificación de requerimientos

En esta sección se mostrarán los requerimientos funcionales y no funcionales de la solución, clasificados en requerimientos generales para la implementación en cualquier IES y los específicos para la UNAB.

6.2.3.1 Requerimientos generales. A continuación, se describirán los requerimientos generales para las IES que debe cumplir el sistema, definiendo un estándar para el ID de los requerimientos: Los Funcionales como RQ-F-S-Número_Requerimiento y los no funcionales como RQ-NF-S-Número_Requerimiento.

6.2.3.1.1 Requerimientos funcionales. El sistema deberá cumplir con diferentes aspectos que permitan un funcionamiento óptimo del sistema; a continuación, se agrupan los diferentes requerimientos funcionales tomando en cuenta módulos de funcionalidad como: Gestión de usuarios (Ver Tabla 2 hasta la Tabla 11), control administrativo (Ver Tabla 12 hasta la Tabla 21) y gestión de acceso (Ver Tabla 22 hasta la Tabla 25).

Tabla 2 Requerimiento Funcional RQ-F-S-01

RQ-F-S-01	
Requerimiento	Inicio de sesión en la plataforma web: El sistema debe permitir el ingreso a través de un usuario y contraseña.
Prioridad	Alta
Precondición	• Debe existir un administrador del sistema y será el único que existirá al momento de instalar el sistema. • La plataforma debe estar conectada a una DB relacionada.
Pos condición	El usuario creado se le asignara un Rol (Estudiante, docente o padre).

Fuente: Elaboración propia

Tabla 3 Requerimiento Funcional RQ-F-S-02

RQ-F-S-02	
Requerimiento	Cierre de sesión en la plataforma web: El sistema debe permitir al usuario finalizar su sesión activa.
Prioridad	Alta
Precondición	• El usuario debe existir en la DB. • Debe existir una sesión activa.
Pos condición	Luego de un tiempo de inactividad, la sesión debe finalizar automáticamente.

Fuente: Elaboración propia

Tabla 4 Requerimiento Funcional RQ-F-S-03

RQ-F-S-03	
Requerimiento	Recuperar contraseña: Se debe permitir al usuario tener algún mecanismo de recuperación de contraseña, diferente a contar con el administrador para que realice el cambio de la misma.
Prioridad	Alta
Precondición	• El usuario debe existir en la DB. • El usuario debe tener acceso al correo electrónico vinculado al sistema.
Pos condición	Por medio del correo electrónico el usuario recibe un vínculo que redireccionará a la plataforma, pidiéndole registrar la nueva contraseña.

Fuente: Elaboración propia

Tabla 5 Requerimiento Funcional RQ-F-S-04

RQ-F-S-04	
Requerimiento	Crear usuarios: El sistema deberá permitir al administrador crear usuarios.
Prioridad	Alta
Precondición	• Se debe tener el rol de administrador del sistema. • El usuario no debe existir en la DB. • Se debe ingresar datos personales de los usuarios.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 6 Requerimiento Funcional RQ-F-S-05

RQ-F-S-05	
Requerimiento	Rol de usuarios: El sistema deberá poseer roles de usuario.
Prioridad	Alta
Precondición	• El administrador del sistema es quien debe asignar el rol de usuario. • El rol a escoger debe ser entre administrador, docente, estudiante o padre.
Pos condición	El usuario podrá acceder a la información determinada según el rol que posea.

Fuente: Elaboración propia

Tabla 7 Requerimiento Funcional RQ-F-S-06

RQ-F-S-06	
Requerimiento	Modificar usuarios: El administrador deberá poder modificar datos personales de los usuarios del sistema.
Prioridad	Alta
Precondición	• Se debe tener el rol de administrador del sistema. • El usuario debe existir en la DB.
Pos condición	Por medio del correo electrónico el usuario recibe un vínculo que redireccionará a la plataforma, pidiéndole registrar la nueva contraseña.

Fuente: Elaboración propia

Tabla 8 Requerimiento Funcional RQ-F-S-07

RQ-F-S-07	
Requerimiento	Cifrado de contraseñas del sistema: La plataforma deberá guardar todas las contraseñas de la DB utilizando sistema de encriptación Hash.
Prioridad	Alta
Precondición	• La contraseña debe poseer un mínimo y máximo de caracteres • El campo contraseña debe ser definido como tipo de entrada *password*.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 9 Requerimiento Funcional RQ-F-S-08

RQ-F-S-08	
Requerimiento	Recuperar contraseña: Se debe permitir al usuario tener algún mecanismo de recuperación de contraseña, diferente a contar con el administrador para que realice el cambio de la misma.
Prioridad	Alta
Precondición	• El usuario debe existir en la DB. • El usuario debe tener acceso al correo electrónico vinculado al sistema.
Pos condición	Por medio del correo electrónico el usuario recibe un vínculo que redireccionará a la plataforma, pidiéndole registrar la nueva contraseña.

Fuente: Elaboración propia

Tabla 10 Requerimiento Funcional RQ-F-S-09

RQ-F-S-09	
Requerimiento	Verificar usuarios únicos: El sistema debe validar por medio del nombre de usuario que no existan usuarios duplicados.
Prioridad	Alta
Precondición	• El usuario ingresar el nombre de usuario para realizar la comparación.
Pos condición	Si el usuario existe, se le debe dar opción al administrador para generar otro nombre de usuario.

Fuente: Elaboración propia

Tabla 11 *Requerimiento Funcional RQ-F-S-10*

RQ-F-S-10	
Requerimiento	Validar campo correo electrónico: El sistema debe validar la estructura del correo electrónico cumpliendo con el formato común (example@domain.com).
Prioridad	Media
Precondición	• El usuario ingresar el correo electrónico a establecer en el sistema. • El correo no debe existir en la DB.
Pos condición	Si el correo no cumple con el formato común, se dará aviso al usuario con un ejemplo para su corrección.

Fuente: Elaboración propia

Tabla 12 Requerimiento Funcional RQ-F-S-11

RQ-F-S-11	
Requerimiento	Eliminar administradores: El sistema debe permitir eliminar un administrador.
Prioridad	Media
Precondición	• El administrador debe existir en la DB. • Si solo existe un administrador, este no se podrá eliminar.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 13 Requerimiento Funcional RQ-F-S-12

RQ-F-S-12	
Requerimiento	Consulta de información en modo privilegiado: El administrador podrá consultar a detalle la información de cada usuario.
Prioridad	Alta
Precondición	• Se debe poseer el rol de administrador.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 14 Requerimiento Funcional RQ-F-S-13

RQ-F-S-13	
Requerimiento	Consulta de información de estudiantes: Los docentes podrán consultar información no sensible de los estudiantes.
Prioridad	Alta
Precondición	• Se debe poseer el rol de docente.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 15 Requerimiento Funcional RQ-F-S-14

RQ-F-S-14	
Requerimiento	Agregar salones de clase: Los administradores podrá incluir los salones existentes en la IES.
Prioridad	Alta
Precondición	• Se debe poseer el rol de administrador. • El salón debería existir físicamente.
Pos condición	Una vez creado, se podrán asignar clases a este lugar.

Fuente: Elaboración propia

Tabla 16 Requerimiento Funcional RQ-F-S-15

RQ-F-S-15	
Requerimiento	Eliminar salones de clase: Los administradores podrán eliminar salones de clase del sistema en caso de reformas o eliminación de espacios.
Prioridad	Baja
Precondición	• Se debe poseer el rol de administrador. • El salón debería existir en la DB.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 17 Requerimiento Funcional RQ-F-S-16

RQ-F-S-16	
Requerimiento	Asignar cursos a salones: Los administradores podrán asignar clases a un salón existente en el sistema.
Prioridad	Alta
Precondición	• Se debe poseer el rol de administrador. • El salón debería existir físicamente. • Debe existir el curso que se va asignar.
Pos condición	Una vez creado, se debe definir los horarios de los cursos.

Fuente: Elaboración propia

Tabla 18 Requerimiento Funcional RQ-F-S-17

RQ-F-S-17	
Requerimiento	Crear cursos: Los administradores podrán crear cursos en el sistema.
Prioridad	Alta
Precondición	• Se debe poseer el rol de administrador.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 19 Requerimiento Funcional RQ-F-S-18

RQ-F-S-18	
Requerimiento	Asignar docentes a cursos: Los administradores podrán asignar un docente a los cursos creados en el sistema.
Prioridad	Alta
Precondición	• Se debe poseer el rol de administrador. • El curso debe tener designado un salón de clase. • El curso debe tener designado un horario.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 20 Requerimiento Funcional RQ-F-S-19

RQ-F-S-19	
Requerimiento	Asignar estudiantes a los cursos: Los administradores podrán asignar estudiantes los cursos creados en el sistema.
Prioridad	Alta
Precondición	• Se debe poseer el rol de administrador. • El curso debe existir en la DB. • El curso debe tener designado un salón de clase. • El curso debe tener designado un horario. • El estudiante debe existir en la DB
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 21 Requerimiento Funcional RQ-F-S-20

RQ-F-S-20	
Requerimiento	Eliminar estudiantes de un curso: Los administradores podrán eliminar uno o más estudiantes de curso.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador. • El curso debe existir en la DB. • El estudiante debe existir en la DB. • El estudiante debe estar inscrito en el curso.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 22 Requerimiento Funcional RQ-F-S-21

RQ-F-S-21	
Requerimiento	Revisar el control de asistencia: El sistema podrá permitir a los usuarios revisar la asistencia en tiempo real de una clase.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador, docente o estudiante. • El usuario debe existir en la DB. • El usuario debe tener un rol asignado.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 23 Requerimiento Funcional RQ-F-S-22

RQ-F-S-22	
Requerimiento	Registro de asistencia automatizado: El sistema deberá registrar al docente o estudiante al momento de activar el sistema tras un evento (colocar la tarjeta RFID sobre el sensor de lectura de la misma).
Prioridad	Alta
Precondición	• El docente o estudiante debe poseer su tarjeta RFID. • El usuario debe colocar la tarjeta sobre el sensor RFID para activar el evento. • El usuario debe existir en el sistema. • El usuario debe tener un rol asignado. • El usuario debe poseer su tarjeta RFID.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 24 Requerimiento Funcional RQ-F-S-23

RQ-F-S-23	
Requerimiento	Registro de asistencia manual: El sistema deberá permitir al administrador y al docente registrar en el sistema la asistencia del estudiante atendiendo a olvidos de la tarjeta RFID o fallos del sistema.
Prioridad	Baja
Precondición	• Se debe poseer el rol de administrador o docente en el sistema. • El usuario debe existir en el sistema.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 25 Requerimiento Funcional RQ-F-S-24

RQ-F-S-24	
Requerimiento	Reporte de asistencia en el sistema: El sistema deberá permitir visualizar tipo reporte, el estado y control de asistencia de los estudiantes, al igual que de los docentes.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador en el sistema. • El usuario debe existir en el sistema.
Pos condición	Para visualizar un curso diferente, se deberá seleccionar el siguiente curso y periodo a revisar.

Fuente: Elaboración propia

6.2.3.1.2 Requerimientos no funcionales. El sistema deberá cumplir con los aspectos de funcionalidad (ver Tabla 26) confiabilidad (ver Tabla 27), disponibilidad (ver Tabla 28), usabilidad (ver Tabla 29), seguridad (ver Tabla 30) y escalabilidad (ver Tabla 31).

Tabla 26 Requerimiento No Funcional RQ-NF-S-01

RQ-NF-S-01	
Requerimiento	Funcionalidad: El sistema debe presentar mensajes de error que indiquen al usuario si existe un error y cuál es el error ocurrido; de igual manera, debe generar al usuario mensajes de éxito que permitan identificar que la operación se hizo correctamente.
Prioridad	Media

Fuente: Elaboración propia

Tabla 27 Requerimiento No Funcional RQ-NF-S-02

RQ-NF-S-02	
Requerimiento	Confiabilidad: El sistema debe poseer un buen desempeño en el manejo de la concurrencia para todos los usuarios del Sistema.
Prioridad	Media

Fuente: Elaboración propia

Tabla 28 Requerimiento No Funcional RQ-NF-S-03

RQ-NF-S-03	
Requerimiento	Disponibilidad: El sistema debe estar disponible aproximadamente el 99,6% del tiempo, sujeto a limitaciones del centro de datos donde se almacenará toda la información.
Prioridad	Media

Fuente: Elaboración propia

Tabla 29 Requerimiento No Funcional RQ-NF-S-04

RQ-NF-S-04	
Requerimiento	Usabilidad: El sistema debe tener una interfaz que sea intuitiva y que garantice la comprensión total de los usuarios que harán uso del sistema
Prioridad	Media

Fuente: Elaboración propia

Tabla 30 Requerimiento No Funcional RQ-NF-S-05

RQ-NF-S-05	
Requerimiento	Seguridad: El acceso al sistema será restringido por uso de contraseñas, las cuales serán asignadas a cada usuario. El acceso estará limitado solo a personas que se encuentren registradas en el sistema y con un rol definido.
Prioridad	Media

Fuente: Elaboración propia

Tabla 31 Requerimiento No Funcional RQ-NF-S-06

RQ-NF-S-06	
Requerimiento	Escalabilidad: El sistema web debe ser programado bajo un lenguaje de desarrollo que permita integrar un *Framework*, para poder agregar nuevos módulos. El *software* que reside sobre los dispositivos embebidos será programado usando Python para permitir una comunicación fluida con los sensores.
Prioridad	Media

Fuente: Elaboración propia

6.2.3.2 Requerimientos específicos. A continuación, se describirán los requerimientos específicos para la UNAB que debe cumplir el sistema, haciendo uso del estándar para el ID de los requerimientos definido en el numera 6.2.3.1.

6.2.3.2.1 Requerimientos funcionales. Adicional a los requerimientos generales, el sistema deberá cumplir con los módulos de reportes (ver Tabla 32 y Tabla 33), mensajería (ver Tabla 34 hasta la Tabla 36) e importación y exportación (ver Tabla 37 y Tabla 38).

Tabla 32 Requerimiento Funcional RQ-F-S-25

RQ-F-S-25	
Requerimiento	Reporte de asistencia en formato digital: El sistema deberá permitir imprimir el reporte de asistencia de los estudiantes.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador en el sistema. • El usuario debe existir en el sistema.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 33 Requerimiento Funcional RQ-F-S-26

RQ-F-S-26	
Requerimiento	Reporte de asistencia por año: El sistema deberá permitir generar el reporte de asistencia de los estudiantes en un año específico.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador en el sistema. • El usuario debe existir en el sistema.
Pos condición	N/A.

Fuente: Elaboración propia

Tabla 34 Requerimiento Funcional RQ-F-S-27

RQ-F-S-27	
Requerimiento	Mensajes privados por el administrador: El sistema deberá permitir enviar a los usuarios mensajes por medio de la interfaz web.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador en el sistema. • El usuario debe existir en el sistema.
Pos condición	El usuario debe recibir en su interfaz web una notificación indicando un mensaje nuevo entrante.

Fuente: Elaboración propia

Tabla 35 Requerimiento Funcional RQ-F-S-28

RQ-F-S-28	
Requerimiento	Anuncios: El sistema deberá dejar agregar noticias importantes o anuncios a los usuarios del sistema.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador en el sistema. • El usuario debe existir en el sistema.
Pos condición	El usuario debe recibir en su interfaz web una notificación indicando un el nuevo anuncio o noticia.

Fuente: Elaboración propia

Tabla 36 Requerimiento Funcional RQ-F-S-29

RQ-F-S-29	
Requerimiento	Mensajes privados por usuarios: El sistema deberá permitir a los usuarios enviar mensajes a otros usuarios.
Prioridad	Media
Precondición	• El usuario debe existir en el sistema.
Pos condición	El usuario debe recibir en su interfaz web una notificación indicando un el nuevo anuncio o noticia.

Fuente: Elaboración propia

Tabla 37 Requerimiento Funcional RQ-F-S-30

RQ-F-S-30	
Requerimiento	Importar lista de alumnos: El sistema deberá permitir importar el listado de estudiantes de un archivo CSV.
Prioridad	Baja
Precondición	• Se debe poseer el rol de administrador en el sistema. • El usuario debe existir en el sistema.
Pos condición	Existiría un mensaje de éxito o error, si fue exitosa la importación, se debe poder visualizar la información.

Fuente: Elaboración propia

Tabla 38 Requerimiento Funcional RQ-F-S-31

RQ-F-S-31	
Requerimiento	Exportar lista de alumnos: El sistema deberá permitir exportar el listado de estudiantes de un curso en un archivo con extensión CSV.
Prioridad	Media
Precondición	• Se debe poseer el rol de administrador en el sistema. • El usuario debe existir en el sistema.
Pos condición	Existiría un mensaje de éxito o error y debe descargar un archivo CVS.

Fuente: Elaboración propia

6.2.3.2.1 Requerimientos no funcionales. Adicional a los requerimientos no funcionales generales, el sistema deberá cumplir con aspectos como respaldos (ver Tabla 39), integración (ver Tabla 40) y portabilidad (ver Tabla 41).

Tabla 39 Requerimiento No Funcional RQ-NF-S-07

RQ-NF-S-07	
Requerimiento	Respaldos: El sistema debe utilizar MySQL como motor de la DB para facilitar el exportar la base de datos y de esta manera tener un respaldo de los datos almacenados en la plataforma.
Prioridad	Alta

Fuente: Elaboración propia

Tabla 40 Requerimiento No Funcional RQ-NF-S-08

RQ-NF-S-08	
Requerimiento	Integración: El sistema debe permitir la fácil integración, a través de estructuras de código entendibles para permitir la utilización de otras plataformas de la UNAB.
Prioridad	Alta

Fuente: Elaboración propia

Tabla 41 Requerimiento No Funcional RQ-NF-S-09

RQ-NF-S-09	
Requerimiento	Portabilidad: El sistema debe permitir una fácil migración de la plataforma web. El código en los sistemas embebidos debe funcionar en plataformas similares, sin necesidad de cambios mayores.
Prioridad	Media

Fuente: Elaboración propia

6.3 DISEÑO A NIVEL DE HARDWARE Y SOFTWARE DE UN SISTEMA DE CONTROL DE ACCESO BASADO EN TECNOLOGÍAS IOT

Este capítulo presentará el desarrollo a nivel de hardware y software para el sistema, considerando los requisitos establecidos en el numeral 6.2. Por otra parte, la información está dividida en tres tópicos: (i) Situación actual; (ii) Diseño de hardware y; (iii) Diseño de software.

6.3.1 Situación actual

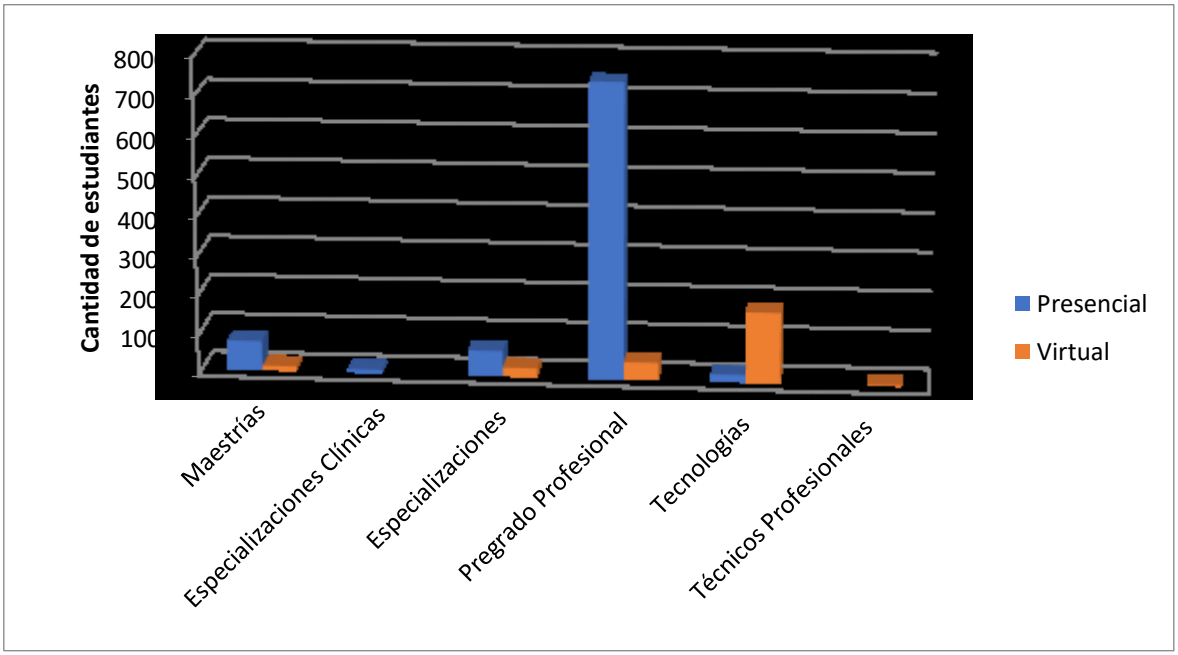
Las IES en su mayoría no cuentan con un sistema de control de acceso automatizado y se centra más en la toma de asistencia manual. Como requisito del Ministerio de Educación Nacional y atendiendo a exigencias de entes acreditadores, se debe llevar algún tipo de registro que permita obtener datos estadísticos de asistencia a clases de los estudiantes. Los datos estadísticos obtenidos suelen ser utilizados para atender a exigencias en cuanto a deserción estudiantil.

La UNAB, realiza este control de asistencia a través de los docentes, quienes son los que registran la información obtenida en la plataforma institucional SIGA. Por su parte, el control docente se realiza a partir de procedimientos de auditorías académicas, donde un grupo de personas recorren las aulas de clase y evidencia si está o no el docente, valiéndose de fotografías digitales mediante el uso de tabletas.

En la Figura 10 se muestra el número de estudiantes matriculados a diciembre del 2016, evidenciando un total de 11.680 estudiantes de los cuales 9.115 pertenecen a la modalidad presencial y 2.565 a la modalidad virtual; a lo anterior se suma la cantidad de 737 docentes en el año 2016, tal como se evidencia en la Figura 11.

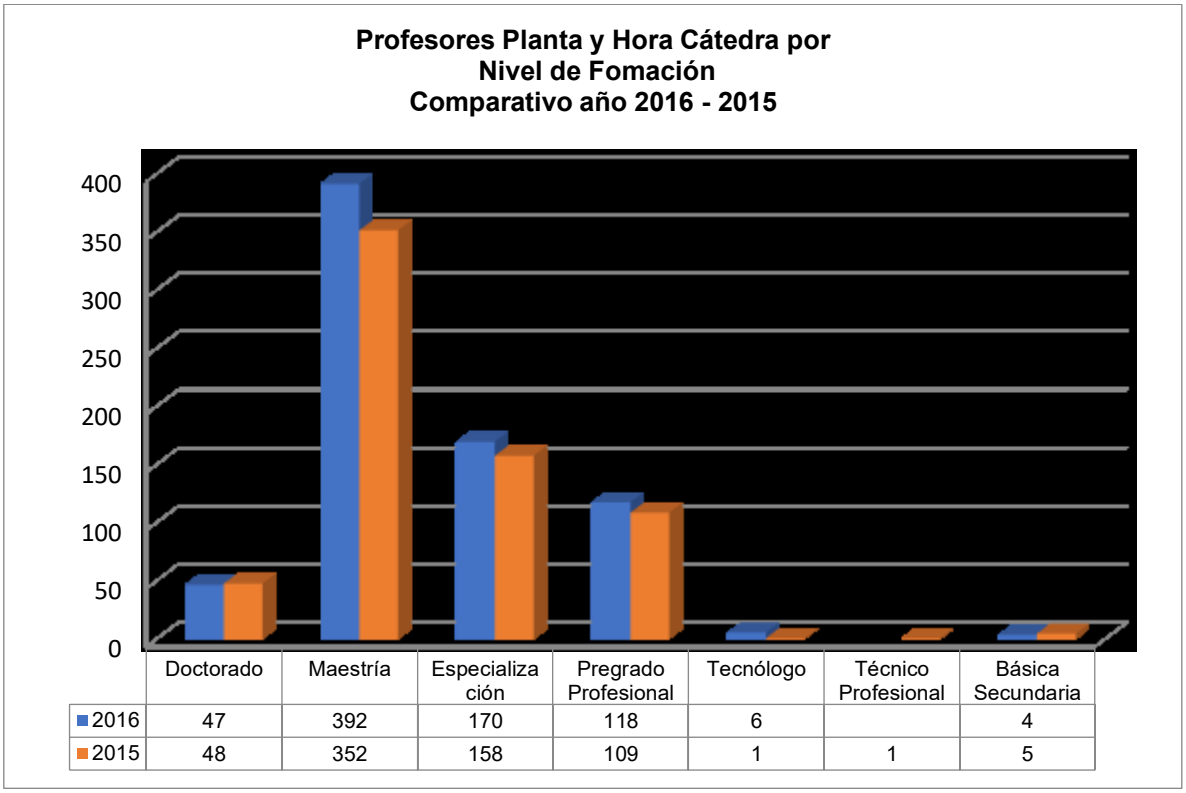
La UNAB cuenta con 239 recintos, haciendo referencia a las aulas de clase, aulas de informática y auditorios, distribuidos en los campus de la siguiente manera: Jardín 124; CSU 35, Bosque 41 y; Casona 14 (Universidad Autónoma de Bucaramanga - UNAB, 2018).

Figura 10 Población estudiantil por nivel y modalidad de formación



Fuente: Elaboración propia a partir del reporte UNAB en cifras 2016 (Universidad Autónoma de Bucaramanga - UNAB, 2017)

Figura 11 Población estudiantil por nivel y modalidad de formación



	Doctorado	Maestría	Especialización	Pregrado Profesional	Tecnólogo	Técnico Profesional	Básica Secundaria
2016	47	392	170	118	6		4
2015	48	352	158	109	1	1	5

Fuente: Reporte UNAB en cifras 2016 (Universidad Autónoma de Bucaramanga - UNAB, 2017)

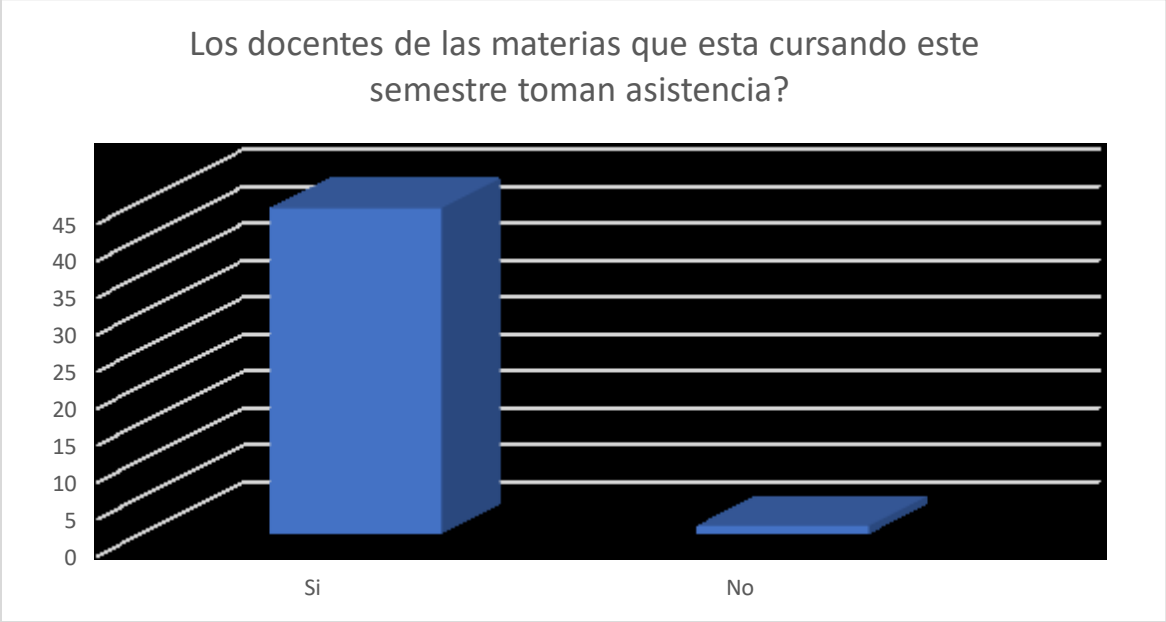
Teniendo en cuenta los datos presentados anteriormente, la labor de gestión se hace compleja y más aún, el control necesario para atender a los requerimientos interpuestos por el MEN, en lo referente a lineamientos y directrices plasmados en el Decreto 1075 de 2015, nombrado en la sección 4.4.1.5 del marco legal.

6.3.2 Encuesta de percepción estudiantil

Para la etapa del diseño, se hace importante realizar un sondeo de la percepción de los estudiantes, para detectar puntos esenciales sobre los cuales se debe trabajar en la etapa de diseño. Para esta encuesta, se tuvieron en cuenta aspecto como regularidad de los docentes en la toma de asistencia, tiempo tomado de clases para esta actividad y aceptación de un sistema para el control de asistencia (Ver Anexo C). La encuesta fue realizada a 45 estudiantes pertenecientes a diferentes programas.

En la Figura 12 se evidencia esta práctica de toma de asistencia por parte del docente. El 99% de los encuestados afirmaron que los docentes toman asistencia, representando un total de 44 personas y el 1% restante, correspondiente a una persona dijeron que no se llevaba asistencia.

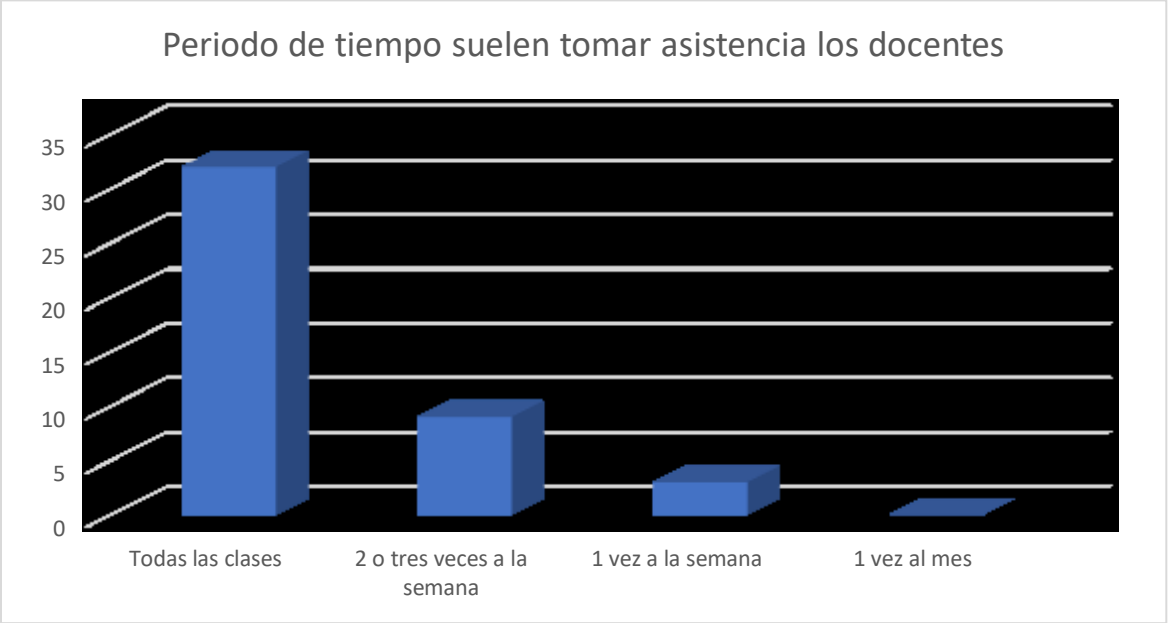
Figura 12 Encuesta 1 – Toma de asistencia



Fuente: Elaboración propia

A pesar que se practica la toma de asistencia, no todos los docentes la realizan todas las clases y por ende, hace que la captura de datos no sea fiable. En la Figura 19 se observa que aproximadamente el 72,73% de los docentes toman asistencia todas las clases, 20,45% de los docentes practican la toma de asistencia entre 2 o 3 veces a la semana y, 6,82% 1 vez a la semana.

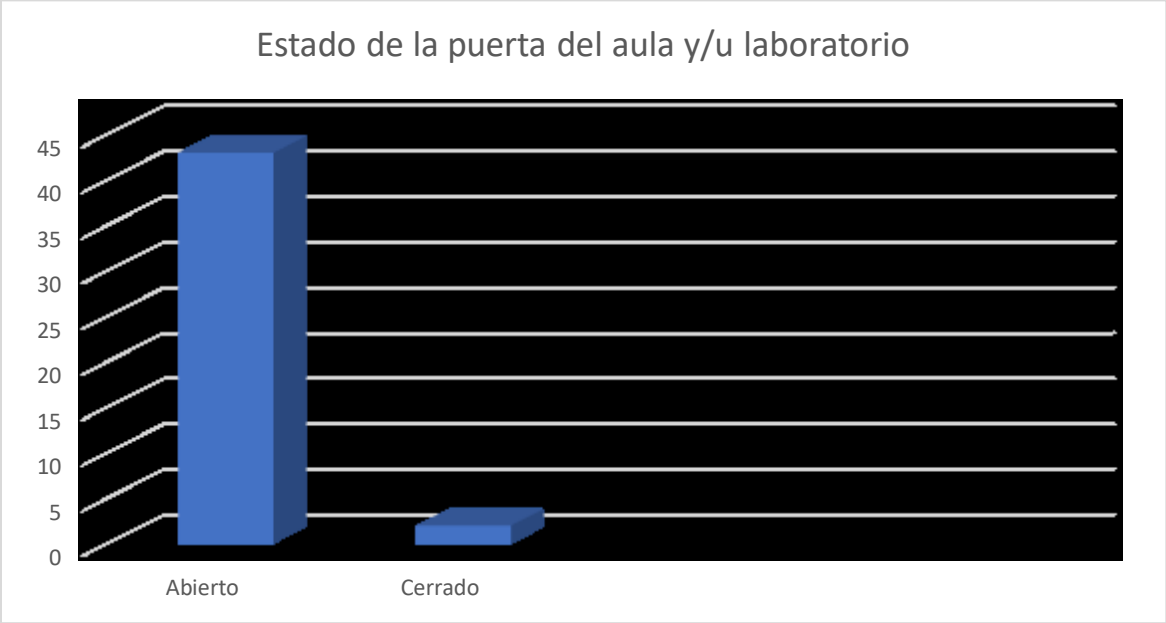
Figura 13 Encuesta 1 – Frecuencia en la toma de asistencia



Fuente: Elaboración propia

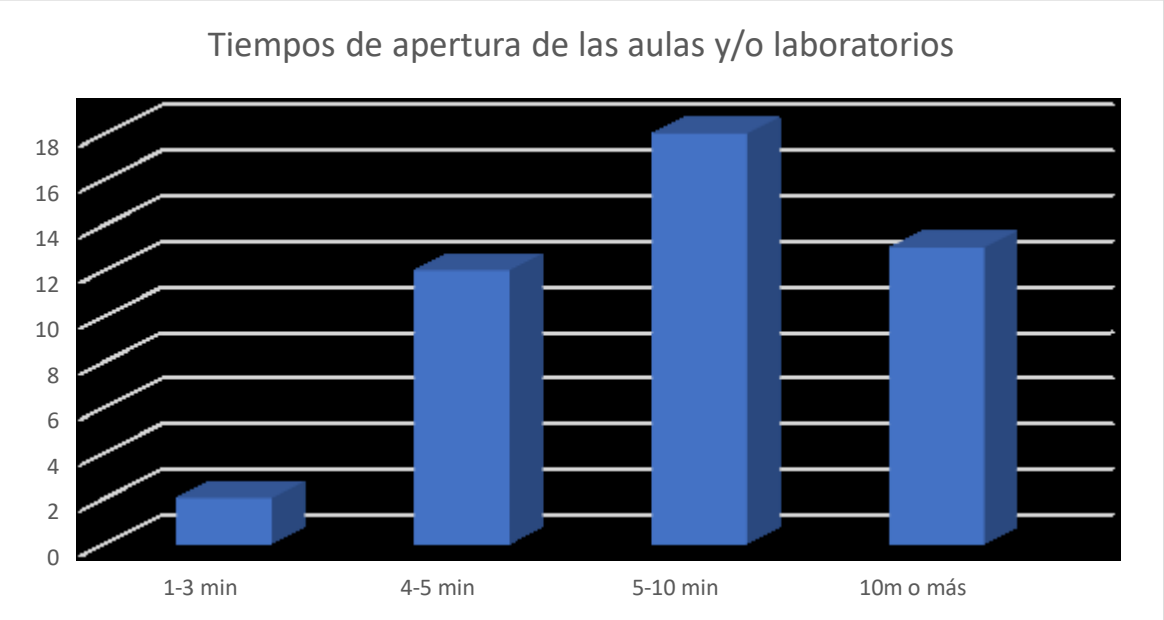
Al momento del ingreso a las aulas de clase y/o laboratorios, se encuentran generalmente cerrados tal como se ve en la Figura 14, representando el 95,56%. La Figura 15 evidencia que los tiempos de apertura en su mayoría es de 5 a 10min, representando el 40%, de 10 o más min con un valor de 28,89%, 26.67 % de 4 a 5min y, por último, con un valor de 4,44% de 1 a 3 min. Lo anterior, evidencia un tiempo de apertura prolongado, donde el 28,89%, representando 13 estudiantes encuestados.

Figura 14 Encuesta 1 – Estado de la puerta



Fuente: Elaboración propia

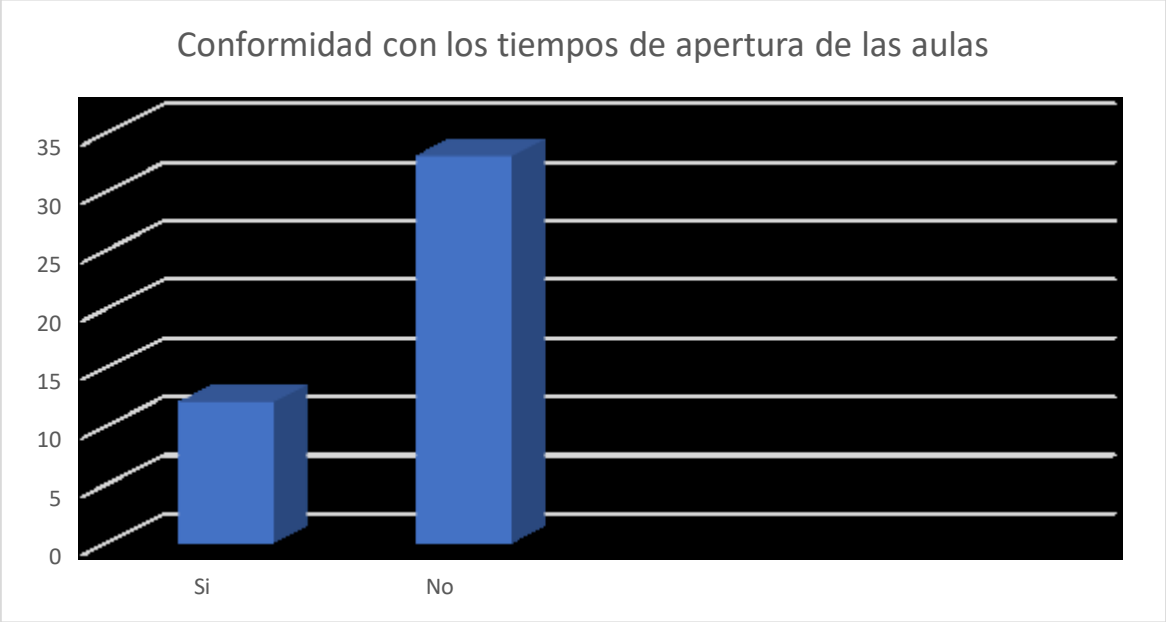
Figura 15 Encuesta 1 – Tiempos de apertura



Fuente: Elaboración propia

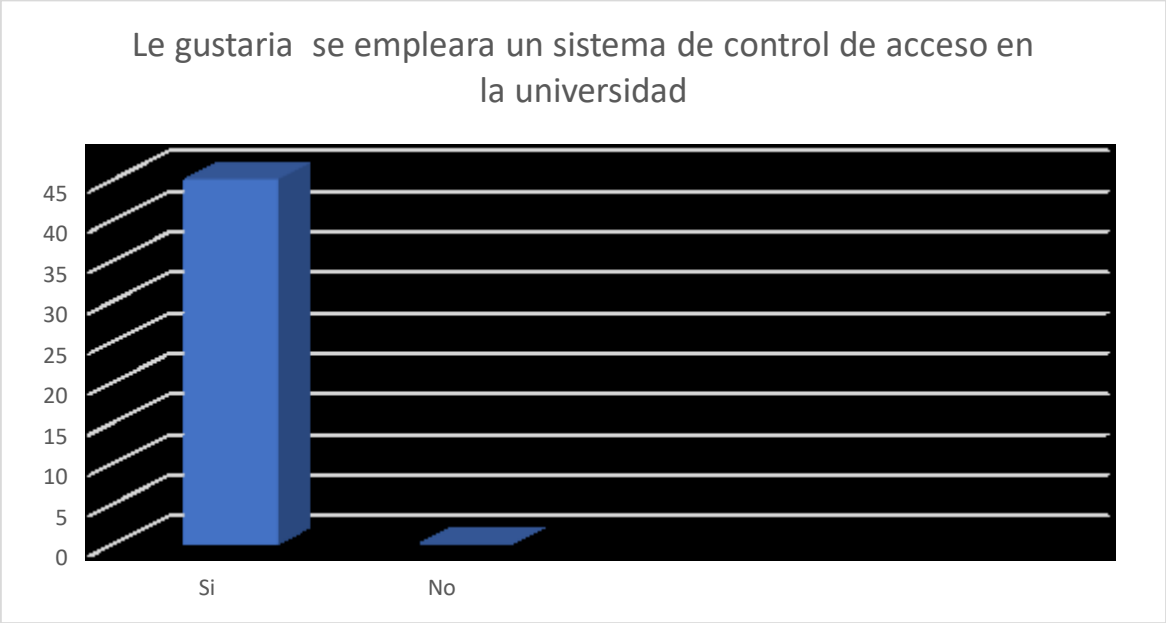
La Figura 16 evidencias problemas en la gestión de apertura en las aulas y/o laboratorios de clase, donde el 73,33% de los estudiantes están inconformes con el tiempo de apertura y tan solo el 26,67% está conforme. La Figura 17 evidencia que el 100% de los estudiantes encuestados, están de acuerdo que se implemente un sistema de control de acceso en las aulas de la universidad.

Figura 16 Encuesta 1 – Conformidad con tiempo de apertura en aulas



Fuente: Elaboración propia

Figura 17 Encuesta 1 – Aceptación de un sistema para control de acceso



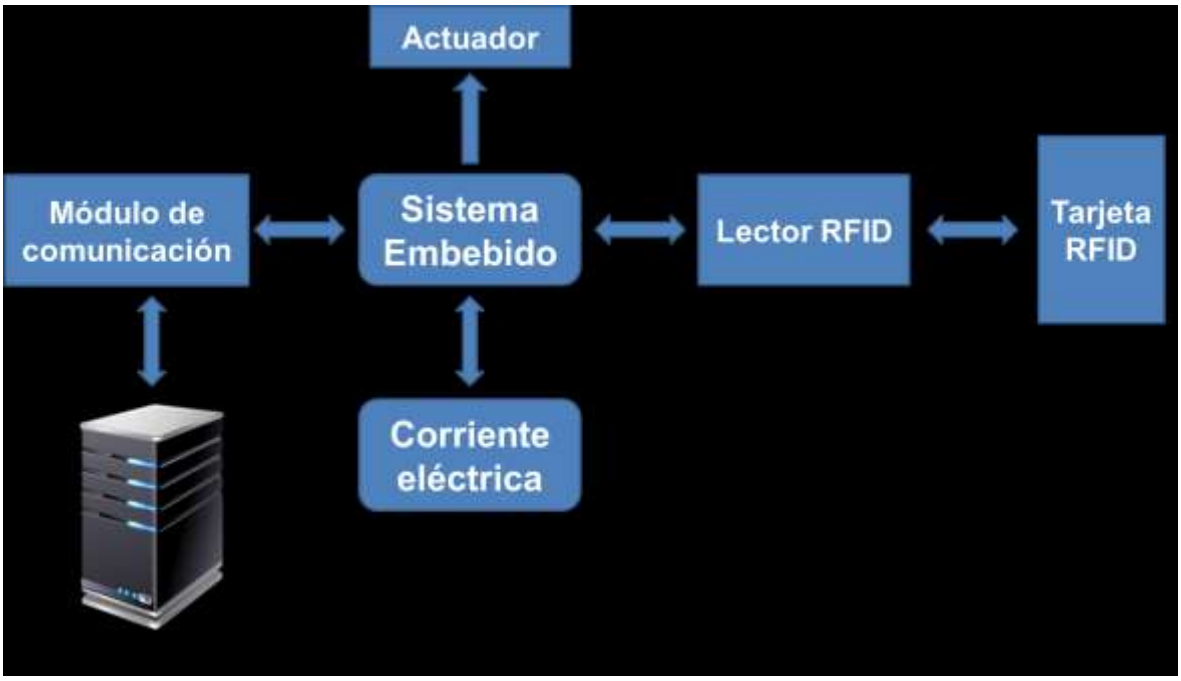
Fuente: Elaboración propia

6.3.3 Diseño de hardware

Para el diseño a nivel de hardware del sistema, se presenta una visión global del diseño de la arquitectura, teniendo en cuenta aspectos como la conexión de los módulos ya definidos y de los dispositivos que conforman el sistema. Un lector RFID, conexión a la red, interfaz de usuario y actuadores, son parte de los elementos necesarios a considerar en el sistema.

Tomando en cuenta lo anterior, en la Figura 18 se puede observar el diagrama de bloques, presentando una arquitectura genérica que permite ser adaptado a las necesidades particulares de las IES y que, a su vez, pueda dar cabida al ingreso de nuevos módulos.

Figura 18 Diagrama de bloques del hardware del sistema



Fuente: Elaboración propia

El uso de la tarjeta RFID, será el evento que activará el sistema; la tarjeta posee el identificador de cada usuario, siendo este extraído por el lector RFID y enviado al sistema embebido, quien está alimentado a través de la energía eléctrica; los datos obtenidos serán enviados por el sistema embebido, usando el módulo de comunicación para acceder al servidor, quien posee una base de datos que será consultada; las consultas realizadas por el sistema al ser respuestas por el servidor, nuevamente llegarán al sistema embebido para ejecutarse en un algoritmo de decisiones y allí, se podrá comunicar con el actuador en caso de requerirlo.

Las selecciones de los componentes del sistema deben cumplir con los requerimientos establecidos, para asegurar la calidad del producto; para la experiencia del usuario, aparece el tema de velocidad tanto de comunicación, como de procesamiento, teniendo como factor clave la ejecución en tiempo real.

6.3.3.1 Sistema embebido. La elección de la placa base del sistema embebido debe permitir la integración con sensores RFID, conexión a través de red

alámbrica o inalámbrica, escalabilidad y la integración con otros sensores. Otro factor clave es la capacidad de procesamiento, permitiendo ejecutar una serie de instrucciones en cortos periodos de tiempo, para que el usuario perciba que es una ejecución del sistema en tiempo real.

La Raspberry Pi 3 (Ver Figura 2) ofrece las exigencias necesarias para el sistema. En la Tabla 42 se pueden observar las especificaciones de esta placa de desarrollo. La compatibilidad con otras placas de desarrollo fue de igual manera uno de los elementos clave para la selección de esta tarjeta, ya que todo el desarrollo puede ser implementado en placas similares como la Banana Pi.

Tabla 42 Especificaciones Rapsberry Pi 3

Sistema embebido	
Producto	Raspberry Pi3
Especificaciones	• Quad Core 1.2GHz Broadcom BCM2837 64bit CPU • 1GB RAM • BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board • 40-pin extended GPIO • 4 USB 2 ports • 4 Pole stereo output and composite video port • Full size HDMI • CSI camera port for connecting a Raspberry Pi camera • DSI display port for connecting a Raspberry Pi touchscreen display • Micro SD port for loading your operating system and storing data • Upgraded switched Micro USB power source up to 2.5A

Fuente: Elaboración propia a partir de información de raspberrypi.org

Las limitaciones de la Raspberry se centran en no poder ser utilizada como parte de un producto comercializable, ya que infringiría las normas y políticas de uso; todo desarrollo realizado dentro de esta placa, como ya se mencionó, puede ser utilizado en placas similares como la Banana Pi, ya que su arquitectura es similar y no implica realizar cambios adicionales. Por otra parte, la Banana Pi si puede ser utilizada dentro de una solución comercial, sin infringir las normas y políticas de uso.

6.3.3.2 Módulo lector *RFID*. El proveer un identificador único a cada estudiante y docente es uno de los aspectos de importancia para la implementación del

proyecto. Este identificador será usado por el sistema para tomar la decisión de conceder el acceso al aula o laboratorio de la IES y a través del identificador, llevar un control de ingreso. Tomando en cuenta lo anterior, la tecnología *RFID* cumple con los criterios necesarios para la ejecución del sistema.

Uno de los aspectos por los cuales se escogió *RFID* es la facilidad de uso que se le brinda al usuario, al igual que los bajos costos de implementación en soluciones tecnológicas. Su principal funcionalidad es la identificación única de objetos o personas y por consiguiente se hace adecuada su inclusión en el proyecto.

El lector RFID RC522 (Ver Figura 19) integra un circuito MFRC522, el cual le permite comunicarse inalámbricamente a una frecuencia de operación de 13.56Mh. En la Tabla 43 se pueden observar algunas características relacionadas con el dispositivo.

Figura 19 Lector RFID RC522

Fuente: Elaboración propia

Tabla 43 Lector RFID RC522

Componente hardware	
Producto	Lector RFID RC522
Especificaciones	• Tensión de alimentación 3.3V • Corriente de Operación 13-26mA • Corriente de *standby* 10-13mA • Corriente de *sleep-mode* <80µA • Corriente máxima 30mA • Frecuencia de operación 13.56Mhz • Distancia de lectura 0 a 60mm • Protocolo de comunicación SPI • Velocidad de datos máxima 10Mbit/s • Temperatura de operación -20 a 80ºC

Fuente: *NXP Semiconductors* (NXP Semiconductors, 2016)

Entre los criterios de selección de este módulo, se encuentra la eficiencia de lectura y la distancia de hasta 3cm para la lectura de tarjetas, ya que de esta manera no requiere un consumo elevado de energía e incluso, su bajo costo en el mercado.

6.3.3.3 Etiqueta *RFID*. Como se mencionó en el marco teórico sección 4.1.2.1, existen diferentes tipos de etiquetas que van a variar de tamaño según la utilidad del mismo. Se propone utilizar etiquetas tipo tarjetas, que cumplan la función y a su vez, permitan reemplazar el carnet de los estudiantes, siendo esta de tamaño similar (ver Figura 20).

Figura 20 Tarjeta RFID 4K

Fuente: Autor

En la Tabla 44 se muestran algunas especificaciones del producto, destacando la frecuencia de operación que permite la compatibilidad con el lector *RFID*, capacidad de almacenamiento, protocolo de comunicación y material.

Tabla 44 Tarjeta RFID MIFARE 4K

Componente hardware	
Producto	Tarjeta RFID 4K
Especificaciones	• Frecuencia: 13.56MHz • Protocolo: ISO14443A • ID único: 32 bits • Tamaño EEPROM: 4096 Bytes • Material: PVC • Temperatura: -20°C ~ +50°C • Dimensión: 85.6 × 54 × 0.86 (mm)

Fuente: *Strong Link* (Strong Link, 2002)

Las tarjetas pueden ser impresas, permitiendo tener sobre ellas la información requerida por las IES: Fotografía, código del estudiante, filiación institucional, entre otros; en cuanto a las dimensiones de la tarjeta, posee un tamaño similar al carnet que entregan las IES a sus estudiantes.

6.3.3.4 Cantonera eléctrica. La apertura de la puerta se debe realizar a través de un actuador, el cual va a ser una cantonera eléctrica marca Yale cuya operación será a 12v (Ver Figura 21). Esta cantonera permite que mediante un solo pulso eléctrico que debe emitir el sistema embebido, se procede a liberar la puerta y así, poder acceder al salón de clase.

Figura 21 Cantonera eléctrica 12v

Fuente: Yale Colombia (Yale Colombia, 2011)

En Tabla 45 se detallan características importantes del producto, entre ellas destacar el uso de memoria que permite el envío de un único pulso para liberar la puerta. En la cantonera, el poder hacer uso de memoria es algo importante puesto que reduce el uso del sistema y de esta manera prolonga la vida útil del mismo.

Tabla 45 Cantonera eléctrica Yale

Componente hardware	
Producto	Cantonera eléctrica 12V Yale
Especificaciones	• Voltaje de operación: 12 Vca. • Recomendada para aplicaciones comerciales ligeras que requieran apertura remota. • La placa frontal es de acero lo que permite que sea soldable. • Con memoria: apertura de puerta con un único pulso eléctrico. • Sin memoria: mantener pulso eléctrico presionado para abrir la puerta. • Requiere transformador: Entrada 110V ca 60 Hz 0.06 A mac. / 220V ca 50 Hz 0.06 A max. Salida: 12 V ca 60 HZ 1.20 A.

Fuente: Yale Colombia (Yale Colombia, 2011)

La instalación de la cantonera no implica la realización de instalaciones complejas, solo requiere ser energizada por medio de una conexión eléctrica de 12 V para accionar la cantonera y liberarla, permitiendo el acceso al lugar. Por otra parte, es posible hacer uso de cantoneras de 120 V, sin requerir cambios adicionales diferentes a ser alimentado con el voltaje de operación.

6.3.3.5 *Relay*. Para controlar el pulso enviado a la cantonera, se debe utilizar un relevo, el cual funciona como un interruptor (Ver Figura 22); al recibir el relevo la señal emitida por el sistema embebido, este debe accionar ese interruptor, que estará controlado por un circuito eléctrico.

Figura 22 Relevo Songle SRD-05VDC-SL-C

Fuente: Autor

En la Tabla 46 se muestran algunas de las características del dispositivo, indicando una expectativa de vida de vida de 100.000 accionamientos. Este relevo viene con una protección adicional, siendo un relevo optoacoplado, o sea, que separa la parte lógica de la parte de potencia, para que no exista contacto físico entre las partes y así, evitar cortos circuitos por regresos de voltaje.

Tabla 46 *Relay Songle*

Componente hardware	
Producto	*Relay* Songle SRD-05VDC-SL-C
Especificaciones	• Relé electromecánico con bobina de 5 V • Contactos NA y NC de 10A/250VAC, 10A/30VDC • 5 pines de conexión • Resistencia de la bobina: 70 Ω aprox. • Expectativa de vida: 100.000 accionamientos • Dimensiones: 19×15.5×15.3 mm aprox.

Fuente: My Com Kits (2008)

Tomando en cuenta que en la UNAB en promedio la cantidad de estudiantes por curso oscila entre los 20 a 25 estudiantes; y que para efectos del ejercicio trabajaremos con 30, con las siguientes consideraciones: si dividimos las clases en bloques de 2 horas al día y en un horario de 6am a 10pm, se activaría el uso del relevo en 7 diferentes momentos del día; cada momento del día que se active el relevo, lo haría 30 veces, una por cada estudiante, más una oportunidad adicional correspondiente al docente, se accionaria en un total de 31 veces para cada momento.

Lo anterior, en un ambiente general de uso implicaría que: de los 7 momentos del día, con 31 activaciones, se tendría un total de 217 activaciones diarias; suponiendo se utiliza 30 días al mes, incluyendo festivos y dominicales para reducir margen de error y dar mayor utilización, se tendría en el mes un total de 6.510 activaciones; en un año el promedio de activaciones seria de 78.120.

Tomando en cuenta el promedio de activaciones anuales, la expectativa de cambio y mantenimiento es de 1 año, para garantizar el funcionamiento adecuado del sistema.

6.3.3.5 Servidor. La plataforma web y los datos estarán alojados en un servidor, este debe contar con suficiente espacio de almacenamiento que permita almacenar la información que se ira almacenando al paso del tiempo; las múltiples peticiones de consultas van a requerir almacenamiento en memoria RAM, por lo que se debe requerir un mínimo disponible para el correcto funcionamiento y; capacidad de procesamiento, para poder procesar las múltiples peticiones realizadas al servidor, asegurándonos la ejecución en tiempo real.

Tabla 47 Características servidor

Componente hardware	
Característica	Parámetro
Procesador	Intel Xeon E5
Velocidad de procesamiento	2,4 Ghz
Memoria RAM	8GB
Disco Duro	500GB
Interface de red	NIC

Fuente: Autor a partir de datos de Dell

El servidor debe poseer en el sistema operativo abiertos los puertos 80 (HTTP), 8080 (HTTPS), 21 y 22 (FTP), 22 (SSH) y 3306 (MySql), al igual que debe estar abiertos dentro de los dispositivos de la red; si no se lleva a cabo la revisión de puertos, puede incurrir en la perdida de información si no es posible la comunicación a través de los puertos ya mencionados.

6.3.4 Diseño de software

En esta sección es presentado el diseño del software, donde se detallan las funciones del software teniendo en cuenta los requerimientos determinados en la sección 6.2, para asegurar el funcionamiento óptimo del sistema.

6.3.4.1 Programación del sistema embebido. Para permitir la migración entre Raspberry Pi y Banana Pi para el despliegue de una solución comercial, la compatibilidad de archivos y configuración, juegan un papel importante en la selección del sistema operativo; al ser los dos sistemas embebidos de arquitecturas similares, se puede utilizar los mismos puertos de entrada y salidas bajo la misma configuración e incluso, usar el mismo sistema operativo. Se decide por el uso de Raspbian como sistema operativo, ya que se puede hacer uso de interfaz gráfica, usa un entorno seguro basado en Linux y tiene un bajo consumo de recursos.

Para la programación de la placa de Raspberry Pi se debe utilizar código Python, por otra parte, se requiere el uso de librerías que faciliten la integración del módulo lector *RFID* (Ver Tabla 48). El uso de estas librerías permite el funcionamiento adecuado del sistema, para ayudar a cumplir con los requisitos de confiabilidad y seguridad.

Tabla 48 Librerías Raspbian

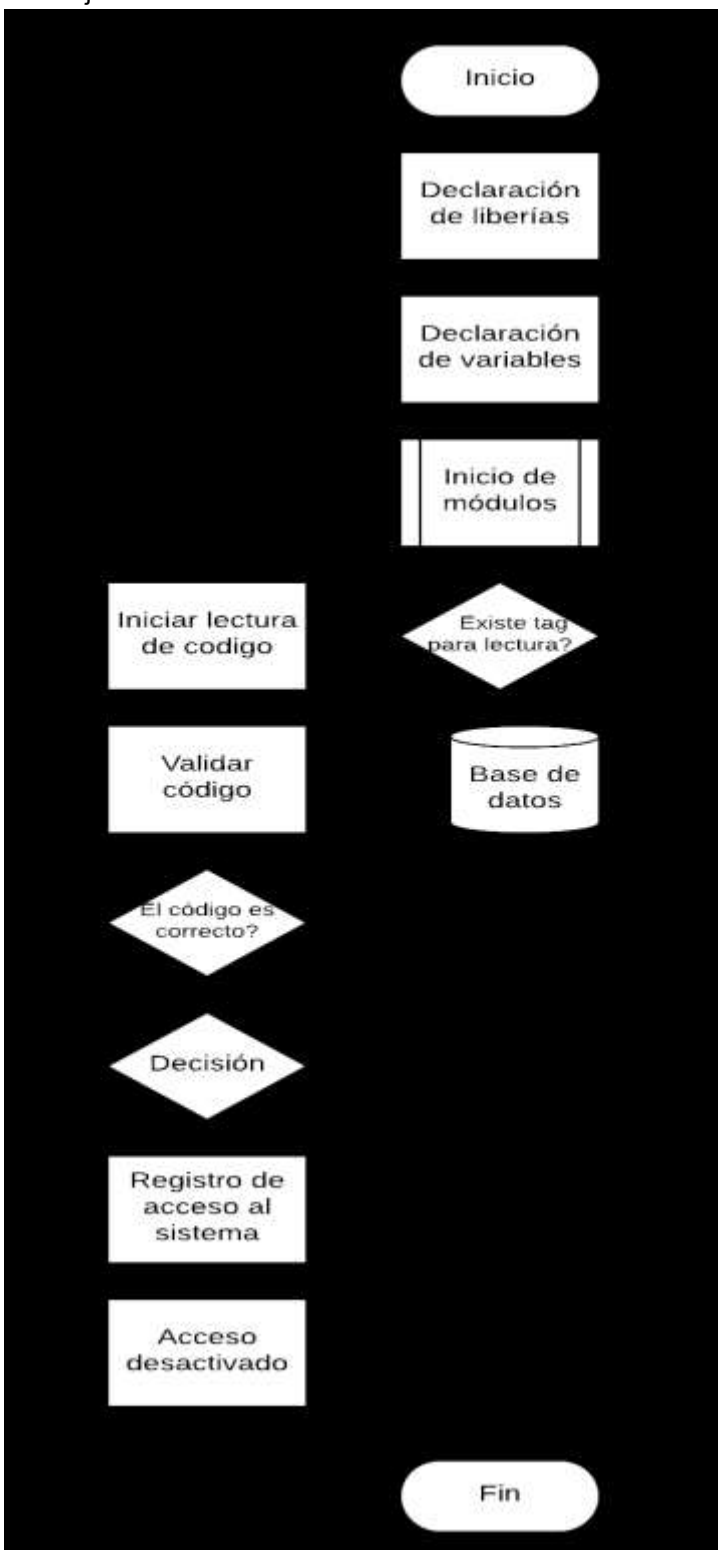
Librerías del sistema embebido	
SPI	Bus de comunicación a nivel de circuitos integrados
Librería RFID	Permite realizar y controlar la comunicación entre el sistema embebido con el sistema operativo a través de Python.

Fuente: Autor

En la Figura 27 se pueden observar los pasos que sigue el sistema para el control de acceso, donde se hace una declaración de variables (Ver Anexo B, sección 1), luego se inician los módulos requeridos para que se pueda operar la lectura *RFID*; Al iniciar el proceso de lectura del código de la etiqueta, se validará la existencia de los mismos y tras ello, se debe tomar una decisión en cuanto a la apertura de la puerta, si el proceso es exitoso, se registra en el sistema esta entrada válida.

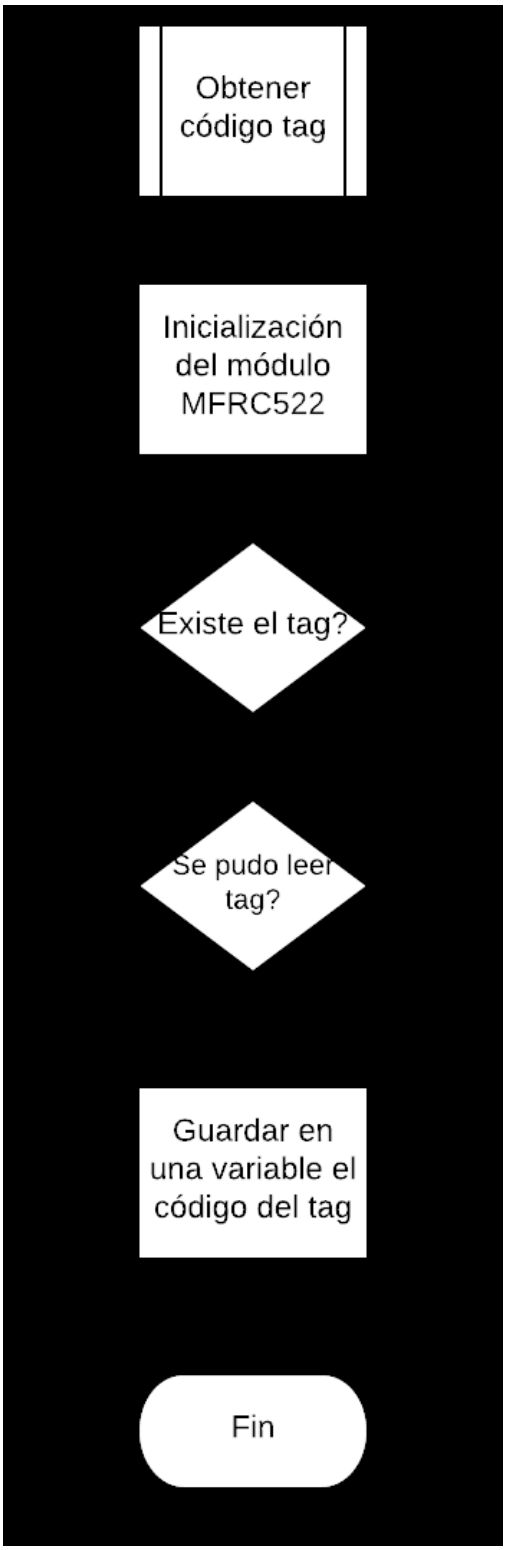
El módulo RFID RC522, el cual para su correcto funcionamiento usa la librería MFRC522 (Ver Anexo B, sección 2), también posee una estructura definida que permite proveer los mecanismos necesarios para comunicarse con el sistema embebido a través de SPI (Ver Figura 28).

Figura 23 Diagrama de flujo control de acceso



Fuente: Autor

Figura 24 Diagrama de flujo librería MFRC522



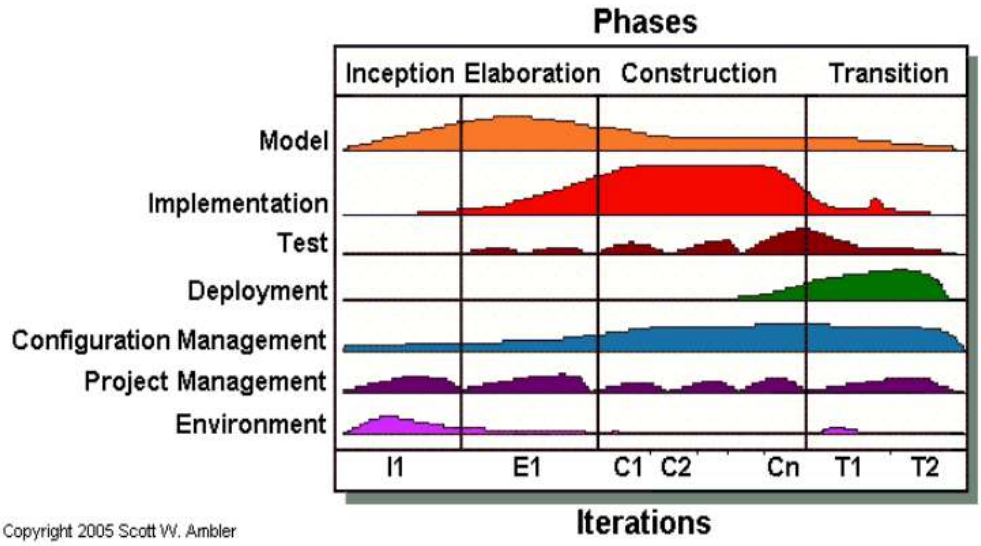
Fuente: Autor

6.3.4.2 Metodología para el desarrollo de la solución *AUP*. *Agile Unified Process – AUP*, es una metodología de desarrollo ágil, heredando funcionalidades de la Programación Extrema – *XP* y de *Rational Unifie Process RUP*. Para el desarrollo de esta metodología, se propone realizar de manera paralela la codificación del código fuente y las pruebas del sistema. Esta metodología es recomendada para equipos de proyectos con pocas personas (Ambysoft, 2005).

La selección del enfoque UAP, es porque permite la integración de buenas prácticas, a través de la ejecución de pruebas mientras se realiza la programación y se permite la fácil adición de nuevas características.

6.3.4.3 Fases de la metodología *AUP*. Esta metodología consta de cuatro fases (Ver Figura 29): Inicio, donde su meta es la identificación del alcance inicial del proyecto (sección 6.2.1); Elaboración, se realizan pruebas a la arquitectura del sistema; Construcción, se crean los entregables del sistema, priorizando las necesidades identificadas (sección 6.2) y; Transición, se valida y se hace el despliegue del sistema en un ambiente producción.

Figura 25 Ciclo de vida de UAP



Fuente: Ambysoft (Ambysoft, 2005)

6.3.4.4 Actores del sistema. El sistema cuenta con tres actores, Administrador, Estudiante y Docente, descritos a más detalle en la Tabla 49. Cada uno tiene diferentes niveles de acceso a la información de los sistemas y no todos pueden realizar las acciones que posee el sistema.

Tabla 49 Actores del sistema

Actor	Descripción
ACT1 - Administrador	La persona que tiene acceso a todo el sistema, con permisos para modificar, agregar, consultar y eliminar información.
ACT2 – Docente	La persona con acceso para agregar información limitado a partes del sistema, modificar ciertos datos del sistema. También posee acceso a través de RFID a las aulas de clase.
ACT3 - Estudiante	La persona que tiene acceso a las aulas de clase.

Fuente: Autor

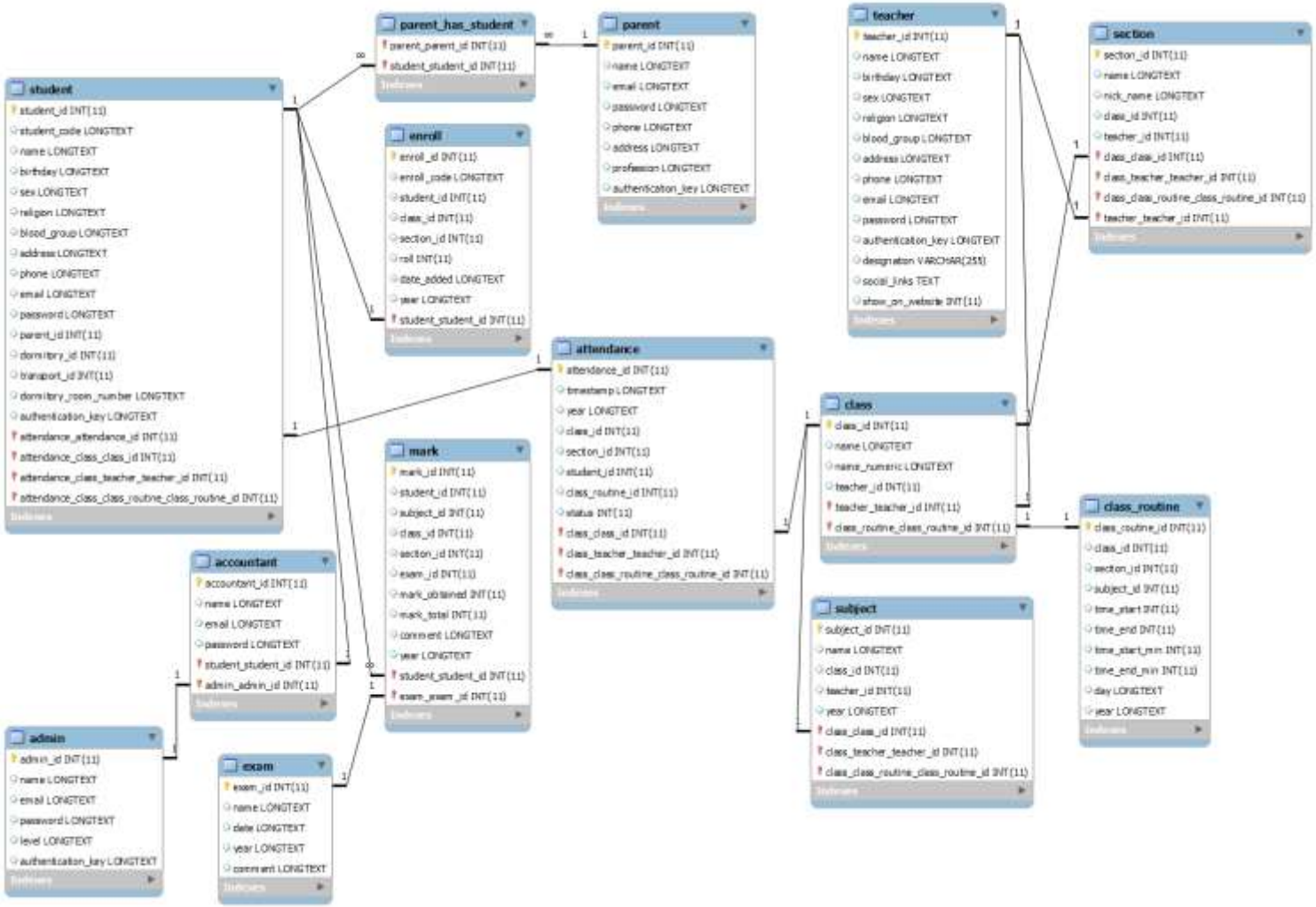
6.3.4.5 Diseño de la Base de Datos. El diseño de la base de datos, permite la búsqueda amigable de información, para que las consultas a la misma, se hagan de manera eficiente. Para que lo anterior se cumpla, se debe tomar en cuenta la escalabilidad, para permitir que el diseño pueda ser modificado, para agregar necesidades futuras.

En el diseño de la estructura se tuvieron en cuenta no existieran datos redundantes, el acceso fácil a los datos y la integridad de los datos. Los requisitos del sistema permitieron la construcción de las tablas utilizadas, haciendo uso de llaves primarias y una normalización que permitiera estandarizar las tablas.

El sistema de gestión de base de datos a utilizar es MySQL, ya que es *Open Source*, posee un buen rendimiento y a su vez, un bajo consumo de recursos. El mantener los recursos del sistema disponibles es parte esencial del sistema, ya que existirán múltiples peticiones que deben ser atendidas a la mayor brevedad.

En la Figura 26, se muestra el modelo entidad relación definido para el desarrollo del proyecto, atendiendo todo que requiere para implementar buenas prácticas en el desarrollo del software.

Figura 26 Diagrama Entidad Relación



Fuente: Autor

6.3.5 Diseño de red

Un correcto funcionamiento de la comunicación garantiza la calidad de servicio del sistema, por lo que se hace necesario realizar el diseño de la red y así, garantizar una mayor disponibilidad del sistema.

6.3.5.1 Selección de la topología. En la Tabla 50 se encuentran criterios bases, para la selección de topología a utilizar para la comunicación del sistema embebido hacia el servidor.

Tabla 50 Criterios de selección

Criterio	Razón
Distancia promedio desde un punto de red cercano a la puerta	10 metros
Protocolo de comunicación	• 802.3 IEEE • 802.11 IEEE
Velocidades de comunicación	10/100/1000 Mbps

Fuente: Autor

Los sistemas embebidos poseen en su mayoría tarjetas Ethernet que operan hasta 100 Mbps, como es el caso del seleccionado para este proyecto; también existen sistemas embebidos que poseen la capacidad de operar a 1 Gbps, como el sistema seleccionado para comercialización. Para el caso de los dos sistemas embebidos seleccionados, se cuenta con tarjeta WLAN.

Para la selección del medio de trasmisión, se debe optar por la utilización de *Ethernet y WiFi* puesto que, para edificaciones antiguas, se requiere realizar mayores modificaciones y en algunos casos, llegar a comprometer la estructura física. Para la red alámbrica y por el bajo consumo de datos generados, se debe utilizar una velocidad de transmisión de 10/100 Mbps, haciendo uso de cableado UTP categoría 5e o superior. La red inalámbrica debe operar bajo el estándar 802.11g, permitiendo velocidades hasta de 54 Mbps.

6.3.5.2 Entorno actual en la UNAB. La UNAB posee salones de clase en los diferentes edificios que la conforman y no solo eso, a pesar de ser la misma ciudad, algunos se encuentran ubicados en áreas geográficamente distantes (Campus Jardín, CSU, el Bosque y Casona). Al contar con una red muy grande, con equipos ya instalados y en operación, puede hacerse uso de los equipos de comunicación ya en funcionamiento para la trasmisión de datos.

Para el caso de despliegue a través de *WiFi* en algunas zonas, el sistema embebido puede conectarse y de esta manera, asegura su comunicación sin necesidad de un medio guiado. Para el uso de *WiFi*, se debe considerar que la señal puede verse atenuada por los muros, vidrios, objetos metálicos, entre otros, afectando la potencia de la señal y por ende, reduciendo la calidad de la misma (Shen, Xu, Sun, Wu, & Lin, 2011).

Al existir una cantidad elevada de salones, se recomienda utilizar diferentes segmentos de red para optimizar el uso de direcciones IP y de este modo, permitir escalar el sistema en caso de construir más salones de clase en la universidad.

6.3.5.3 Esquema de la solución. Como se comentó anteriormente, al ser un número elevado de aulas de clase, se requiere mantener diferentes rangos de IP para poder definir las direcciones de cada dispositivo.

Por lo anterior, y siguiendo el esquema utilizado por la UNAB, se decide utilizar direcciones clase B, siendo esta clase la usada para las redes internas en la universidad. Tomando en cuenta que existen 239 recintos (aulas y laboratorios) dispersos en los diferentes campus, se opta por definir 2 segmentos de red, para hacer uso de subredes.

Se optará por las redes privadas 172.16.200.0 y 172.16.201.0, definidas a más detalle en Tabla 51, dando un total de 253 direcciones disponibles para cada los sistemas embebidos por cada red. En la

Tabla ***52*** se puede ver la distribución de las subredes, atendiendo a la cantidad de recintos en cada campus, tomando en cuenta direcciones IP extras en caso de construirse un nuevo recinto.

Tabla 51 Direccionamiento de red clase B

ID Red	Puerta de enlace	*Broadcast*
172.16.200.0/24	172.16.200.1	172.16.200.255/24
172.16.201.0/24	172.16.201.1	172.16.201.255/24

Fuente: Autor

Tabla 52 Subredes de la solución

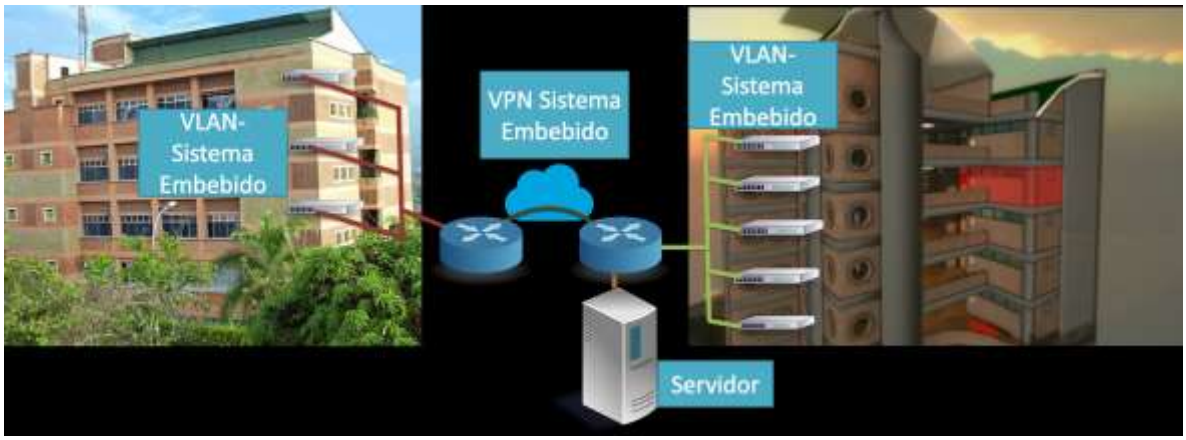
Campus	Subred	Puerta de enlace	*Broadcast*	Direcciones IP disponibles para los sistemas embebidos
Jardín	172.16.200.0/24	172.16.200.1	172.16.200.255/24	253
CSU	172.16.201.0/26	172.16.201.1	172.16.201.63/26	61
Bosque	172.16.201.64/26	172.16.201.65	172.16.201.127/26	61
Casona	172.16.201.128/27	172.16.201.129	172.16.201.159/27	29

Fuente: Autor

Para efectos de seguridad, se debe realizar el despliegue de una VLAN en cada uno de los campus que poseen salones de clase en diferentes edificios o posee una cantidad de host considerable, para separar el tráfico de los sistemas embebidos, del tráfico común de la IES. Lo anterior, para poder mantener una subred para todo el sistema a pesar de estar conectados a diferentes *switches* y a su vez, en diferentes edificios.

Para la conexión entre los diferentes campus, del mismo modo se requiere garantizar la seguridad de la información, por lo cual se deben crear Redes Virtuales Privadas – *VPN*, evitando así, exponer los datos sensibles que deben viajar a través de Internet. Por lo anterior, se define en la Figura 27 el esquema lógico de la red.

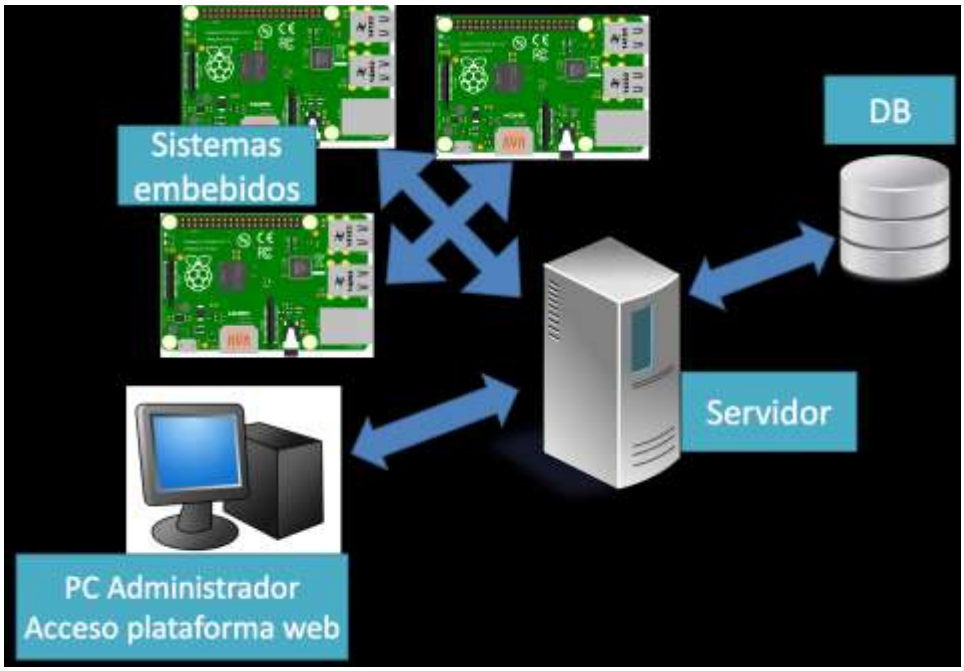
Figura 27 Esquema de red



Fuente: Autor

La arquitectura cliente servidor es definida en la Figura 28, mostrando una arquitectura distribuida, para permitir que los usuarios puedan tener acceso a la información; esta arquitectura es definida para permitir la fácil integración con nuevas tecnologías y que, a su vez, permite el crecimiento de infraestructura.

Figura 28 Arquitectura Cliente/Servidor



Fuente: Autor

El administrador accederá al servidor a través de la plataforma web, donde consultará la información guardada por los sistemas embebidos. Estos sistemas embebidos solo consultan el servidor al momento de utilizar una tarjeta *RFID* sobre el módulo de lectura.

6.3.6 Diseño físico del prototipo

Tomando en cuenta los materiales requeridos para la construcción del prototipo, se define un diseño del mismo (ver Figura 29); este diseño base se compone de una puerta con su marco, un sistema embebido, el relevo y el módulo lector *RFID*.

Figura 29 Diseño prototipo

Fuente: Autor

Este diseño base es realizado para la elaboración del prototipo funcional a escala que permite realizar las pruebas necesarias, para la puesta en marcha de la solución antes de la implementación en un ambiente real.

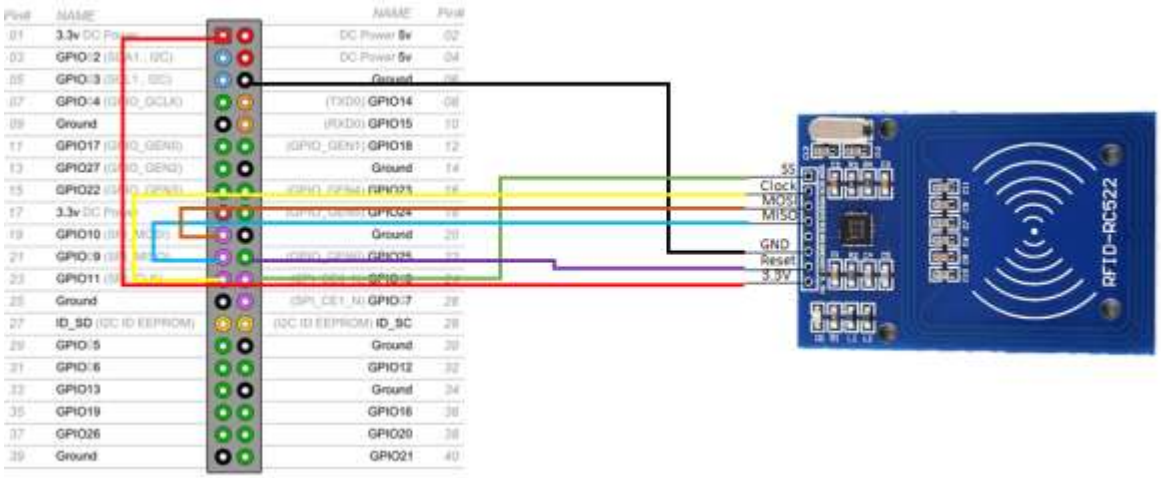
6.3.7 Construcción del prototipo funcional

Tomando en cuenta los materiales requeridos para la construcción del prototipo y el diseño propuesto en la sección 6.3.4, se construyó un sistema a escala que permitiera realizar las pruebas antes de hacer una implementación.

El módulo RFID RC522 posee 8 conexiones posibles en él, estas son: SDA (señal de datos en serie), SCK (reloj en serie), MOSI (Maestro de entrada esclava), MISO (maestro en salida esclava), IRQ (Petición de interrupción), GND (*Ground Power*), RST (*Reset-Circuit*) y 3.3v (3.3v Voltaje de entrada). Se conectan a los pines GPIO de la Raspberry Pi todas las salidas descritas anteriormente, excepto el IRQ.

La conexión entre el RFID RC522 y la Raspberry Pi es bastante simple, solo requiere que conecte 7 de los pines GPIO directamente al lector de RFID. En la Figura 30, se observa las posiciones de los pines GPIO a los que necesita conectar el módulo RC522.

Figura 30 Esquema de conexión



Fuente: Autor

Una vez realizado el montaje (Ver Figura 31), se realizó la instalación y configuración del sistema embebido (Anexo A), al igual que la del servidor donde se aloja el sitio web y *DB*. Inicialmente se configuró un sistema web de menores funcionalidades que cumpliera con lo requerido, para realizar una primera etapa de pruebas del funcionamiento del prototipo (Ver Figura 32).

Figura 31 Prototipo construido

Fuente: Autor

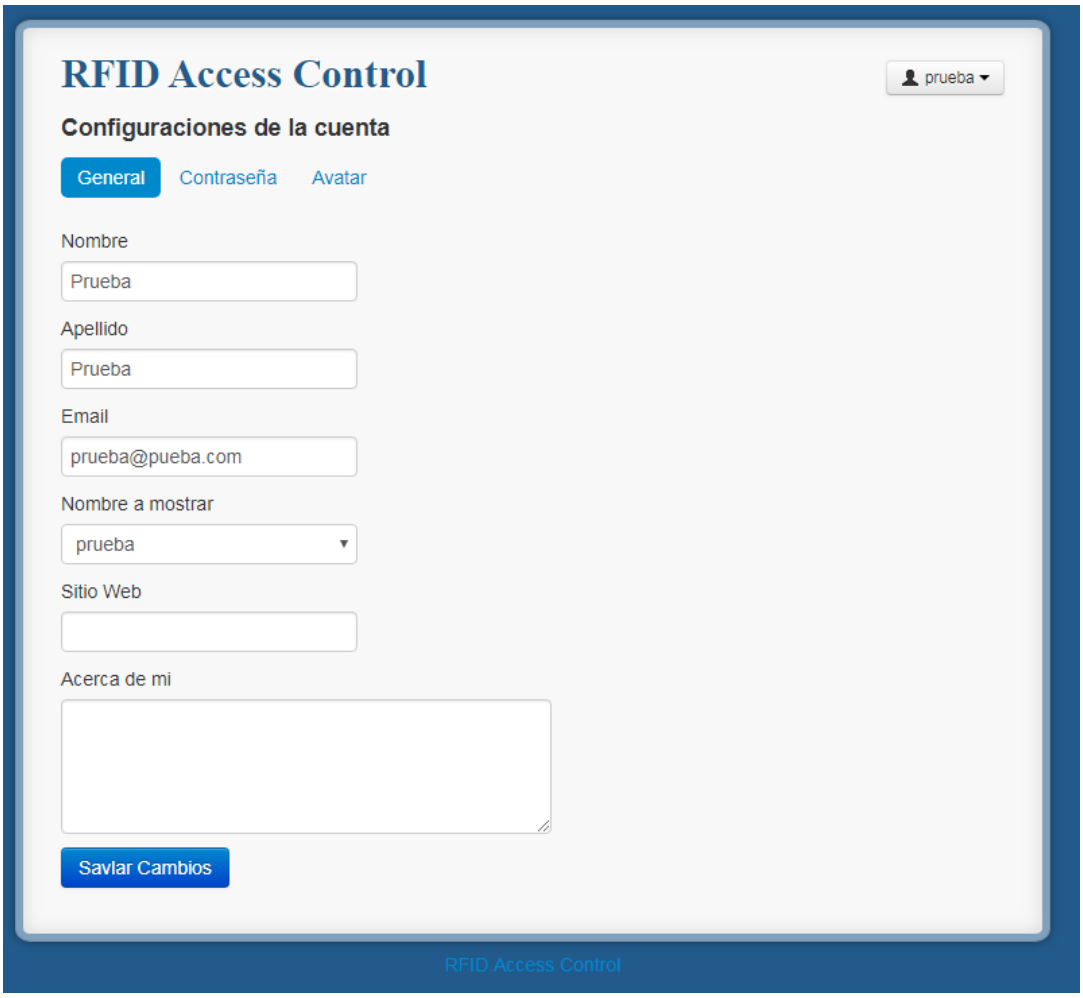
Figura 32 *Login User Control Panel* V1.0

Fuente: Autor

Este sistema web está posee un gestor de usuarios accedido por un administrador y un panel de usuarios. Este sistema solo permite manejar datos básicos del perfil del usuario y, el administrador cuenta con opciones de dar acceso o no a una persona.

Desde el panel de usuario se puede cambiar nombres, correos, contraseñas (Ver Figura 33) y, por otra parte, cuenta con un perfil de usuario que indica los datos básicos registrado de la cuenta (Ver Figura 34).

Figura 33 Panel de usuario del sistema *User Control Panel* V1.0



Fuente: Autor

Figura 34 Perfil de usuario del sistema *User Control Panel* V1.0

Fuente: Autor

Desde la parte administrativa se permite el rol de usuario, el status (indica si tiene o no acceso), el ultimo día accedido y una serie de acciones para controlar datos del usuario y, por otra parte, se permite ver el un registro de quienes han accedido (Ver Figura 35).

Figura 35 Panel administrativo del sistema *User Control Panel* V1.0

Fuente: Autor

6.4 IMPLEMENTACIÓN A NIVEL DE HARDWARE Y SOFTWARE, DE UN PROTOTIPO FUNCIONAL DE SISTEMA DE CONTROL DE ACCESO BASADO EN TECNOLOGÍAS IOT

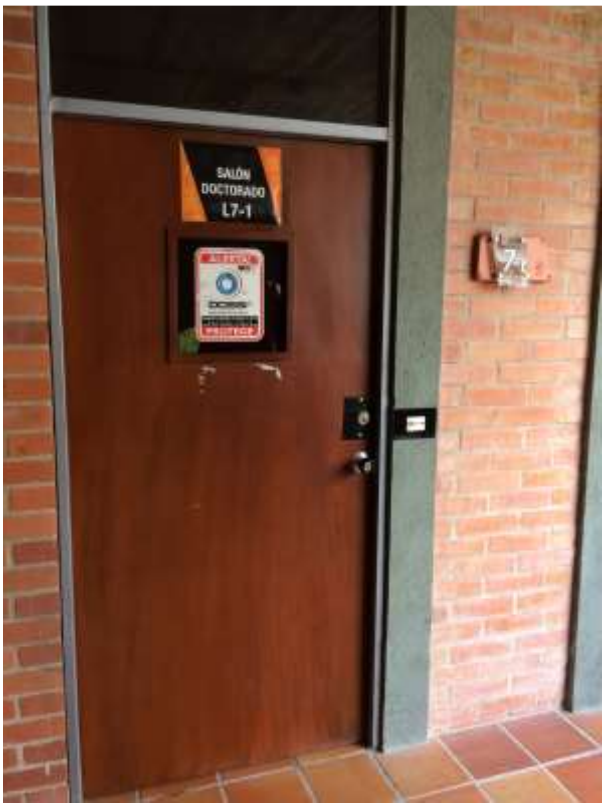
Para la implementación, se realizaron previamente pruebas sobre el prototipo funcional descrito en la sección 6.3.7 para verificar la funcionalidad del sistema y comunicación del mismo.

6.4.1 Sitio de instalación

El montaje e instalación del sistema demanda una serie mínima de requerimientos para su funcionamiento óptimo que deben ser tomados en cuenta antes entrar en funcionamiento: Adecuaciones del lugar para el montaje del dispositivo lector, instalación de un punto eléctrico con corriente regulada y anclaje del lector RFID.

El prototipo funcional fue instalado en el salón 7-1, del séptimo piso del edifico de ingenierías de la UNAB (Ver Figura 36), sobre el cual se realizaron las modificaciones pertinentes para el uso adecuado del sistema.

Figura 36 Salón 7-1 edificio de ingenierías UNAB



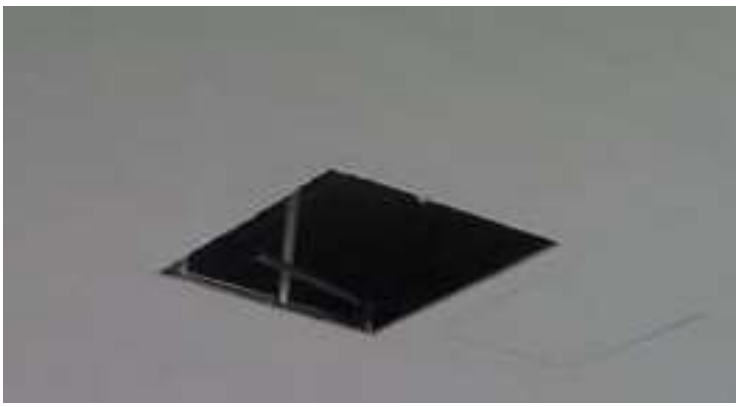
Fuente: Autor

Para el montaje del lector, se realizó una perforación al muro que permitiera realizar un anclaje del mismo, evitando sufriera daños el dispositivo o que fuera sustraído (Ver Figura 37). El montaje del sistema embebido se realizó en el techo falso, quedando oculto a la vista de quien entrara al lugar (Ver Figura 38 y Figura 39). Para el cableado, se utilizó el marco hueco de la puerta, manteniendo seguro el prototipo.

Figura 37 Vista de anclaje en el muro

Fuente: Autor

Figura 38 Vista techo falso



Fuente: Autor

Figura 39 Chasis Raspberry Pi

Fuente: Autor

6.4.2 Comunicación a internet

Para la conexión a *Internet*, se estableció comunicación a través de *WiFi*, haciendo uso de una red establecida por la UNAB que opera bajo el estándar IEEE 802.11n y de esta manera, asegurando la comunicación la Raspberry Pi hacia Internet (Ver Figura 40).

Figura 40 *Air Port Express*

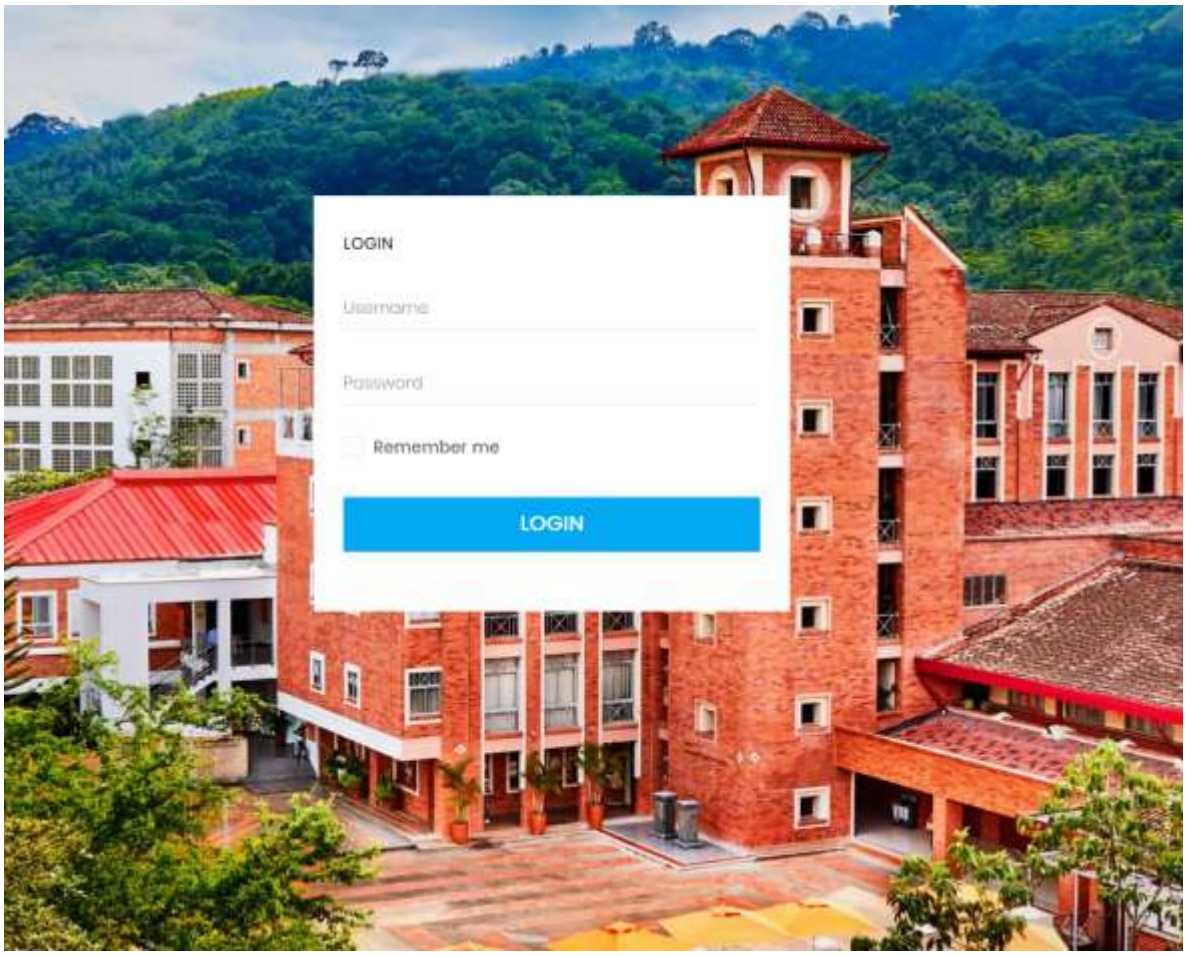
Fuente: Autor

La Raspberry se comunica al servidor web, por medio de consultas que se realizan a la base datos, usando el protocolo *TCP* y de esta manera se asegura la integridad de la información. Para acceder a la plataforma Web, se puede realizar por medio de cualquier navegador *web* (Compatibilidad con Chrome, Mozilla, Internet Explorer, Safari, Microsoft Edge y Opera), el cual, para garantizar la seguridad en el uso de contraseñas, utiliza protocolo HTTPS.

6.4.3 Plataforma web General

La plataforma web empleada corresponde a los requisitos generales para las IES (Ver Figura 41). Una de las características de funcionalidad de la plataforma, es el ser *Responsive*, o sea, se ajusta a cualquier tamaño (resolución de pantalla) y lo hace ideal para su uso en computadoras, tabletas y celulares. Esta plataforma permite el ingreso de usuarios con el rol de Administradores, Estudiantes, Docentes y Padres.

Figura 41 Login plataforma general



Fuente: Autor

Desde la parte administrativa, se cuenta con un módulo que permite conocer la cantidad de personas registradas en la plataforma (Ver Figura 42). El reporte de asistencia hace parte de los requisitos funcionales, por lo que se puede generar el reporte diario o mensual por cada curso que se esté impartiendo; en la Figura 43 se puede ver uno de los reportes generados por la plataforma, en uno de los cursos en los cuales se realizaron pruebas al sistema.

Figura 42 Usuarios registrados por rol de la plataforma general

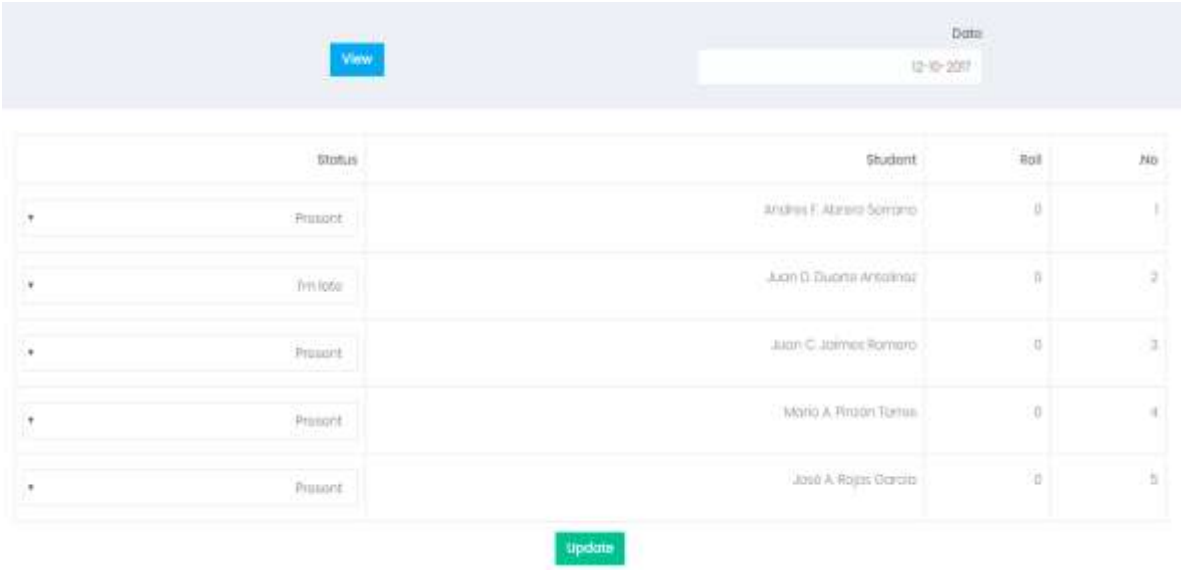
Fuente: Autor

Figura 43 Reporte de asistencia de la plataforma general

Fuente: Autor

Se detectó que en algunas ocasiones los estudiantes olvidaban traer la tarjeta RFID otorgada, por lo cual, como apoyo al docente se creó un módulo donde se permite el registro manual de la asistencia en la plataforma (Ver Figura 44).

Figura 44 Reporte de asistencia de la plataforma general



Fuente: Autor

6.4.4 Datos capturados a partir de la implementación

Durante las pruebas de la plataforma, se detectó que el material utilizado para el módulo RFID y el grabado adicional atenuaban la señal, disminuyendo en aproximadamente 15 mm el alcance lectura, un 25% menos del rango normal de lectura. Se realizaron 181 intentos de registro, de 179 que debieron realizarse, los 2 intentos adicionales, se debieron a una lectura incompleta de la tarjeta. Los 179 intentos fueron registrados exitosamente en la *DB.* Lo anterior, indicando una efectividad de registro del 100% y de lectura en un valor aproximado al 99%, evidenciando eficiencia de la solución.

6.5 PRUEBA PILOTO DEL PROTOTIPO IMPLEMENTADO EN UN AULA DE LA UNAB

En base en las pruebas y la implementación a nivel de hardware y software, se determinó que se debían modificar los diseños físicos del producto. Del mismo modo, se detectaron mejoras a realizar en la plataforma web. Por efectos de la prueba piloto, la implementación se vio afectada por remodelaciones en el lugar

donde se encontraba y de igual manera, se realizó un diseño nuevo para y se creó un nuevo método para llevar a cabo la prueba piloto.

6.5.1 Diseño y marca del producto

Para el nuevo producto se creó la marca *Classroom Access Surveillance System – CLASS*, sobre la cual se diseñó el logo que le representaría (Ver Figura 45). El *chassis* sobre el cual reposan los elementos del producto se personalizó, de manera tal que mantuviera un diseño propio y contuviera la marca del producto (Ver Figura 46, Figura 47 y Figura 48).

Figura 45 Logo CLASS

Fuente: Autor

Figura 46 Módulo portátil

Fuente: Autor

Figura 47 Módulo estacionario

Fuente: Autor

Figura 48 Módulo lector *RFID*

Fuente: Autor

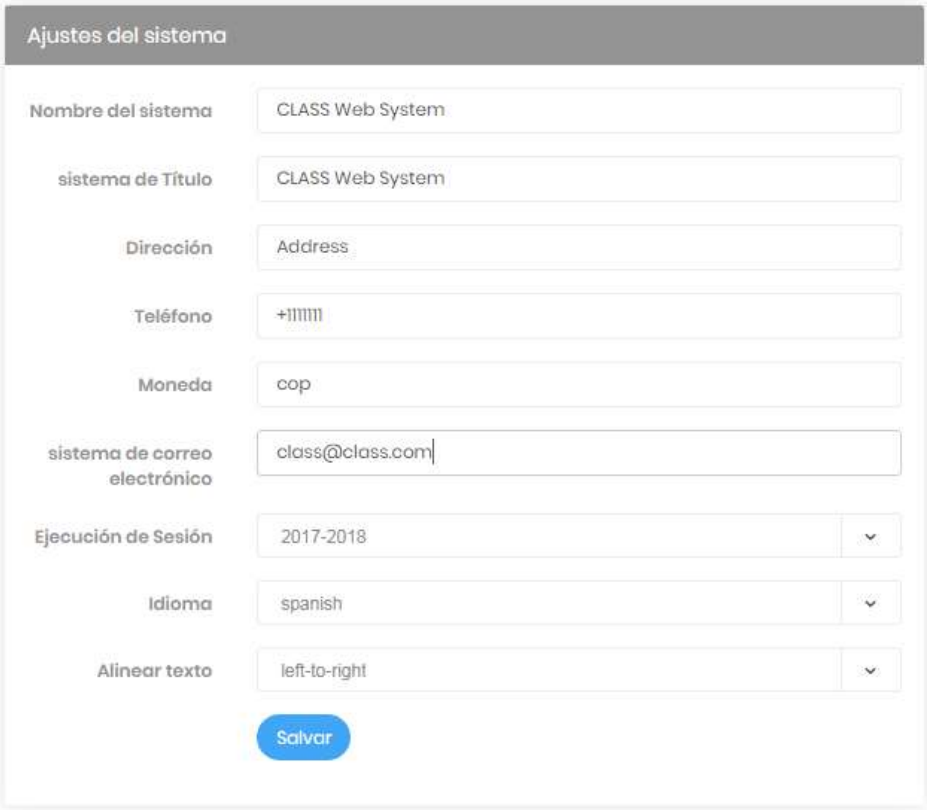
La plataforma web se integró un portal, donde se puede mostrar información institucional, manejar una lista de eventos y noticias; por otra parte, se cuenta con un módulo para admisiones.

Figura 49 *Home page CLASS Web System*

Fuente: Autor

La UNAB usualmente recibe estudiantes extranjeros, por lo que se habilito la función de cambiar idioma (Figura 50), de esta manera, el sistema CLASS facilita el aprendizaje de la plataforma y brinda comodidad al usuario.

Figura 50 *Cambio de idioma - CLASS Web System*



Fuente: Autor

Al igual que lo argumentado en la fase de diseño, se dejó activa la opción para que los docentes pudieran marcar de forma manual la asistencia en caso de olvido del carnet estudiantil o por cuestiones externas al producto, tal como se ve en la Figura 51.

Figura 51 Asistencia desde la vista del docente - *CLASS Web System*

Fuente: Autor

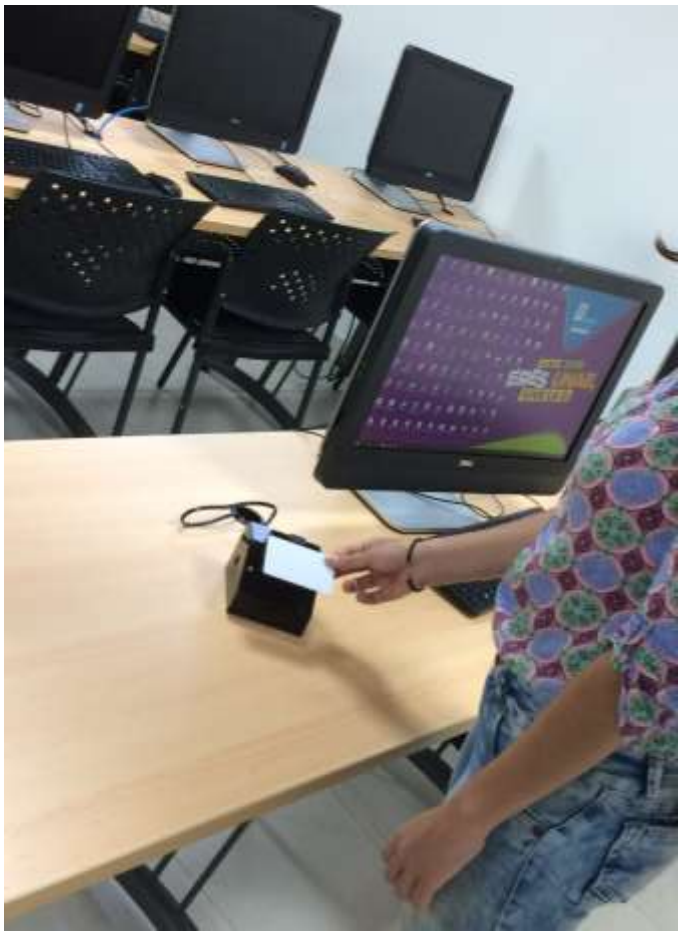
6.5.2 Ejecución de la prueba piloto

Haciendo uso del módulo portátil, durante el inicio de clases del primer semestre de 2018 se realizaron las pruebas del producto. A 65 estudiantes de cuatro cursos diferentes se les otorgó una tarjeta *RFID*, la cual utilizaron durante las dos últimas semanas de enero y durante todo febrero.

El módulo portátil era instalado en el salón y conectado a la corriente eléctrica (el único requerimiento de acción manual), este se conectaba a la red inalámbrica de la universidad, la cual había sido previa mente configurada. Esta operación se debía llevar a cabo para todas las clases, puesto que se debía contar con adecuaciones mínimas del lugar, permitiendo brindar seguridad al sistema; estas adecuaciones requerían interrumpir el transcurso normal de las clases y por ese motivo principalmente se optó por trabajar el módulo portátil.

Una vez realizado el montaje, se procedía con el ingreso de los estudiantes al aula de clase, registrando el acceso a clase (Ver Figura 52, Figura 53, Figura 54 y Figura 55). El realizar la toma de asistencia tomaba alrededor de 40 min, máximo 1 min.

Figura 52 Prueba 1 de uso de *CLASS Web System*

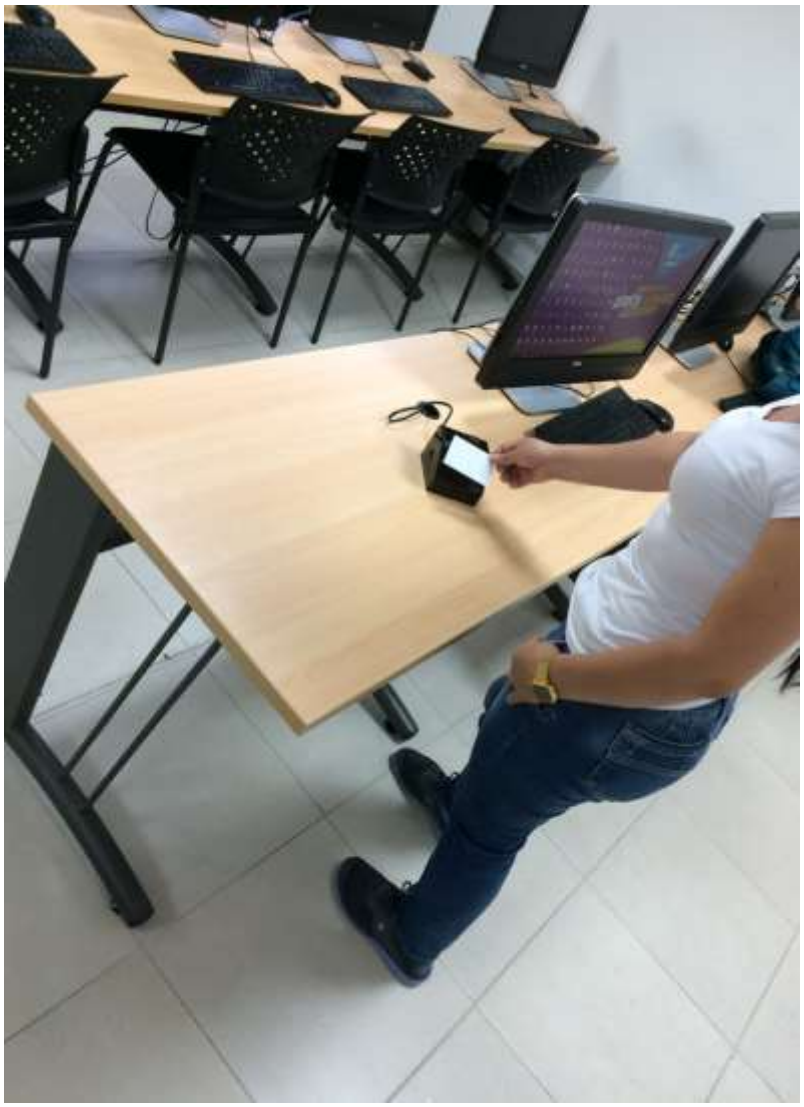


Fuente: Autor

Figura 53 Prueba 2 de uso de *CLASS Web System*

Fuente: Autor

Figura 54 Prueba 3 de uso de *CLASS Web System*



Fuente: Autor

Figura 55 Prueba 4 de uso de *CLASS Web System*

Fuente: Autor

6.4.3 Datos capturados a partir de CLASS

A diferencia de la plataforma usada anteriormente, el acrílico utilizado para el *chassis* del lector *RFID* no se veía afectado por la atenuación de la señal y su rango de lectura se mantenía muy próximo a los 60mm. Durante el transcurso de las pruebas, se realizaron 3350 iteraciones con el lector *RFID*, de las cuales 3350 fueron registradas y marcadas como exitosas, indicando que la efectividad del sistema se encuentra en un 100%.

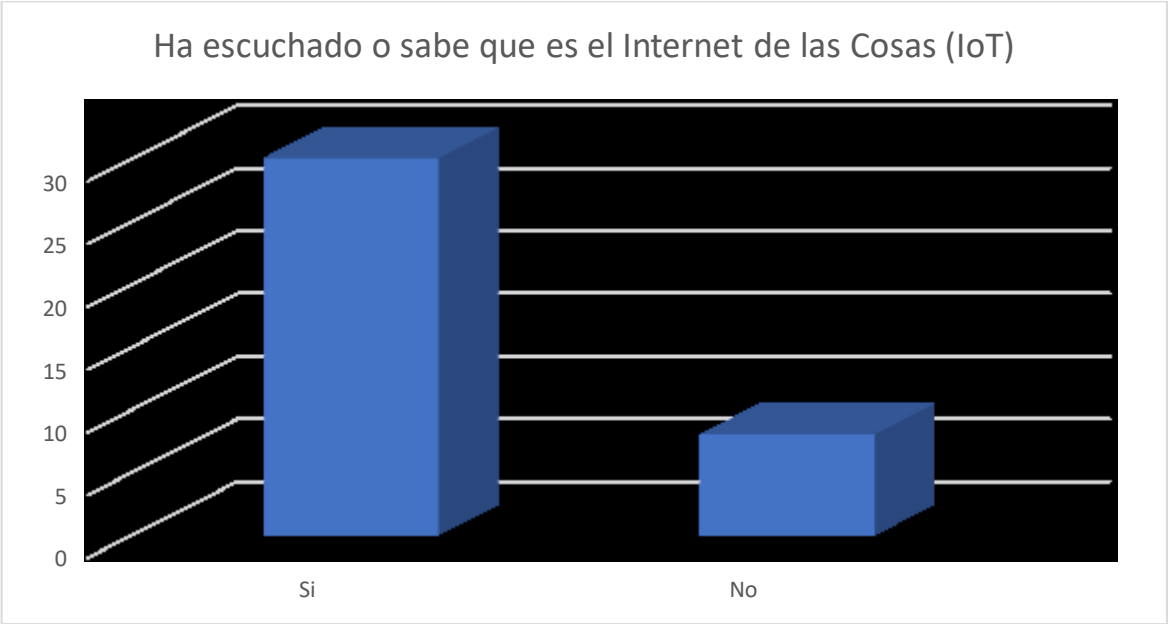
6.5.4 Encuesta de aceptación de tecnologías en IES

A diferencia de la encuesta de percepción, esta encuesta se enfoca en saber la opinión de los estudiantes en la implementación de un sistema que permita llevar el control de asistencia de los estudiantes y de esta manera, determinar su aceptación (Ver anexo D). Esta encuesta fue aplicada a 38 estudiantes, de diferentes programas de la UNAB.

Respecto al conocimiento de la tecnología *IoT*, se tiene que el 78,95% de los encuestados conoce o ha escuchado hablar sobre *IoT*, mientras que el 21,05% no conoce que es *IoT* (Ver Figura 56). Por otra parte, el termino *RFID* es conocido por

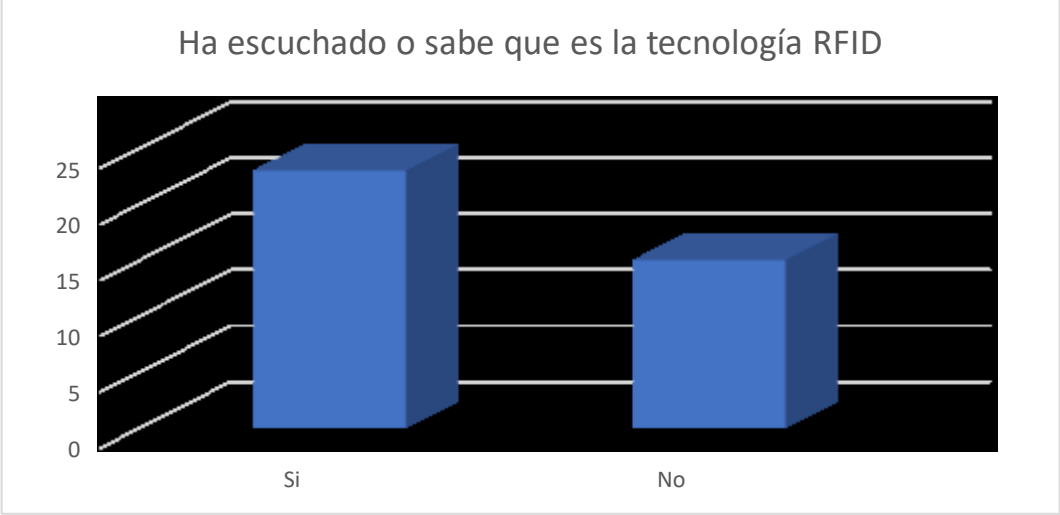
el 60,52% y no han escuchado sobre *RFID* el 39,48% de los encuestados (Ver Figura 57).

Figura 56 Encuesta 2 – Conocimiento sobre *IoT*



Fuente: Elaboración propia

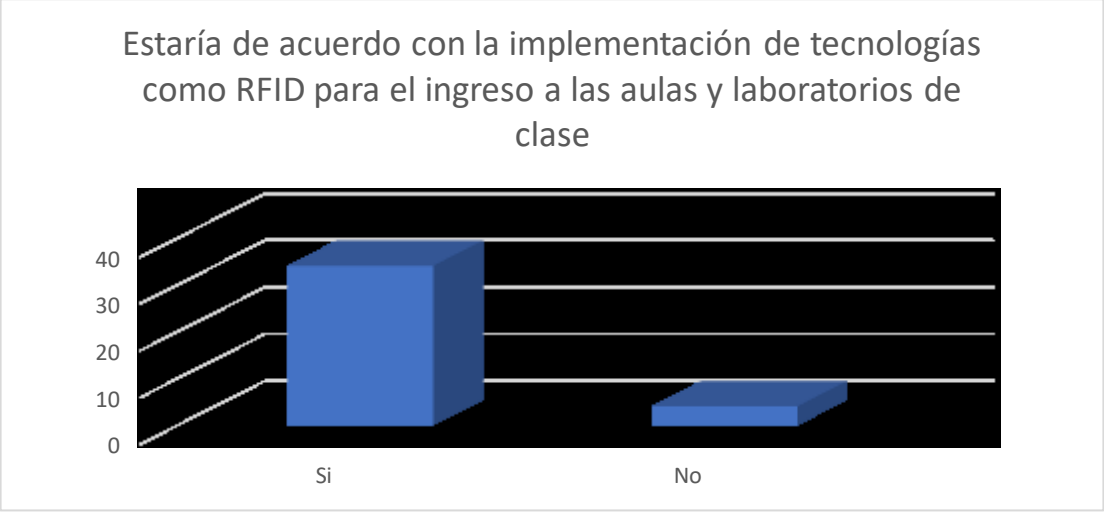
Figura 57 Encuesta 2 – Conocimiento sobre *RFID*



Fuente: Elaboración propia

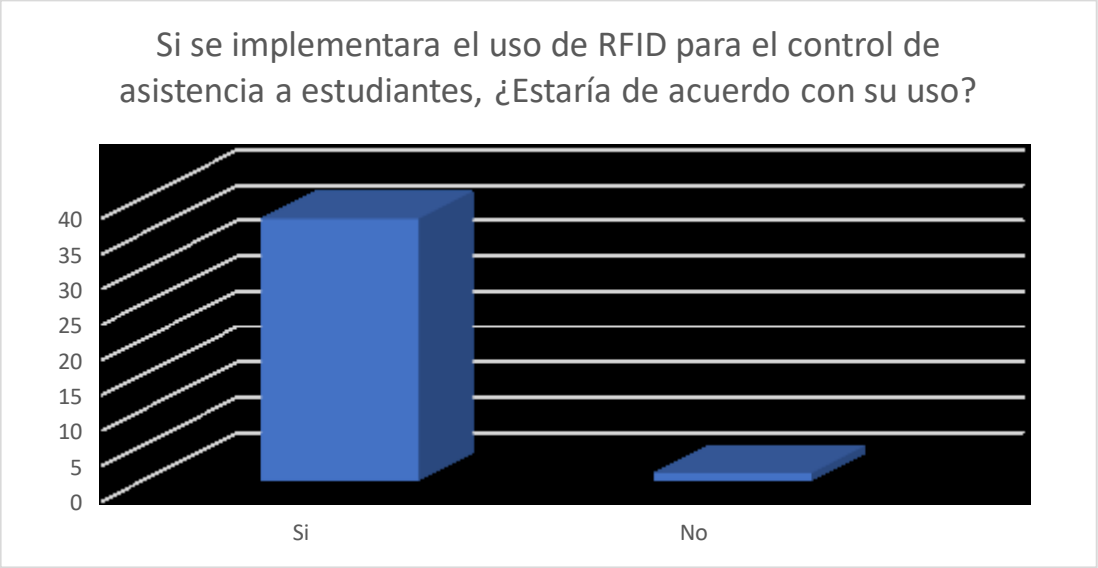
La implantación de un sistema para el control de acceso es aceptado por los estudiantes, donde el 89,47% está de acuerdo y solo el 10,53% está en desacuerdo (Ver Figura 58). Por otra parte, la implementación un control de acceso y control de asistencia a estudiantes es fuertemente aceptado por las personas encuestadas, representando un 97,36% de estudiantes de acuerdo y únicamente un 2,64% están en desacuerdo, argumentando que el sistema actual está bien (Ver Figura 59).

Figura 58 Encuesta 2 – Aceptabilidad de un sistema de acceso



Fuente: Elaboración propia

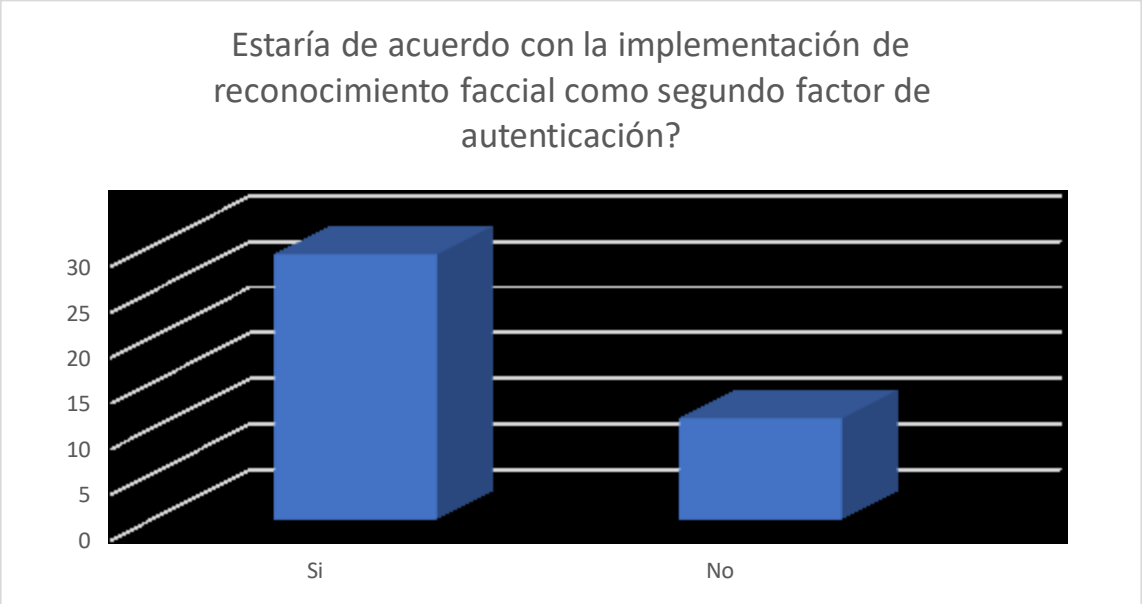
Figura 59 Encuesta 2 – Aceptabilidad de un sistema de control de asistencia estudiantil



Fuente: Elaboración propia

Como adicional, se preguntó acerca de la implementación de reconocimiento facial para autenticar el acceso al aula de clase, determinando que el estudiante realmente es quien solicita el ingreso. EL 76,31% está de acuerdo con el uso del reconocimiento facial, frente al 26,69% que no están de acuerdo (Ver Figura 60). Algunas de las razones del rechazo, están entre la privacidad y uso de datos, mientras que otros argumentan que el gasto de implementarlo sería elevado.

Figura 60 Encuesta 2 – Aceptabilidad de un sistema de control de asistencia estudiantil



Fuente: Elaboración propia

7. OTROS RESULTADOS

Como resultados adicionales, se realizaron registros de software ante la Dirección Nacional de Derecho de Autor - DNDA y sobre los que se relacionan los siguientes productos:

- Registro de software de la plataforma web implementada en la etapa de diseño del prototipo.
- Registro software de código Python implementado en la etapa de diseño del prototipo.
- Registro software de plataforma web implementada en la etapa de construcción del prototipo
- Registro software del código Python implementado en la etapa de construcción del prototipo
- Registro software de la plataforma web CLASS

Por otra parte, también se realizó el registro ante el ente internacional Copyright.es, quien utiliza protocolos y convenciones internacionales de derechos de autor.

- Registro de marca Classroom Access Surveillance System – CLASS
- Registro de logo CLASS

8. CONCLUSIONES

En la actualidad existen diversos estudios científicos y aplicaciones realizadas por la academia, pero que no tienen una solución integral, aspecto que fue resuelto en la elaboración de este proyecto. La eficiencia y efectividad de la plataforma, no solo debería ser utilizada como un sistema común en las IES que, a su vez, sirva de plataforma para los reportes que se deben realizar ante MEN y así, permitiendo obtener datos en tiempo real.

La pregunta de investigación fue resuelta, respondiendo la hipótesis planteada; IoT permite llevar de forma automatizada la obtención de datos en tiempo real, del mismo modo, se permite a través de esa captura de datos, poder diseñar nuevos métodos que permitan controlar la deserción estudiantil.

La selección de los implementos adecuados para la construcción del prototipo hace parte clave de la efectividad, en cuanto a comunicación, sensor de lectura y chasis. Una mala elección puede atenuar la señal, reduciendo efectividad en la lectura de las tarjetas y de esta manera, afectando la confiabilidad del sistema.

Es importante el uso de VPN para asegurar la integridad de la información y a su vez, asegurarse de mantener un canal de comunicación con un ancho de banda disponible para la comunicación hacia el servidor. Si la conexión se hace a través de redes compartidas, la tormenta de Broadcast puede reducir la capacidad del canal y si hay mucho tráfico en la red, puede generar pérdidas de paquetes, provocando retardos ajenos a la solución.

El construir un software que permita la integración con otras plataformas, toma un papel muy importante ya que las universidades poseen sistemas implantados; uno de los factores de éxito que fue detectado es la compatibilidad y simplicidad para la integración entre plataformas, por otra parte, las buenas prácticas de programación permiten la adición de nuevas funcionalidades.

Se espera implementar el sistema en las aulas de doctorado, permitiendo su uso oficial e impactar sobre este programa, facilitando los controles pertinentes para garantizar un nivel de calidad superior, siendo un elemento diferenciador.

REFERENCIAS

Agencia Nacional del Espectro - ANE. (2016). *Resolución No. 711 de 2016*. Diario Oficial No. 50.061: Agencia Nacional del Espectro Retrieved from http://www.ane.gov.co/images/COMUNICACIONES2016/RESOLUCION_711_2016.pdf.

Ambysoft. (2005). AUP, Agile Unified Process. from http://www.ambysoft.com/scottAmbler.html

Armitage, R. (2014). Crime prevention through environmental design *Encyclopedia of criminology and criminal justice* (pp. 720-731): Springer.

Ashton, K. (2009). I could be wrong, but I'm fairly sure the phrase “Internet of Things” started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. *RFID Journal, 22*.

Aydın, K., & Yıldırım, S. (2012). Case study about RFID System in Library Services. *Technology, 1*, 2.

Badamasi, Y. A. (2014). *The working principle of an Arduino.* Paper presented at the Electronics, computer and computation (icecco), 2014 11th international conference on.

Bagheri, M., & Movahed, S. H. (2016). *The Effect of the Internet of Things (IoT) on Education Business Model.* Paper presented at the Signal-Image Technology & Internet-Based Systems (SITIS), 2016 12th International Conference on.

Banerjee, S. P., & Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research, 7*(1), 116-139.

Bienestar Universitario UNAB. (2016). Informe de deserción estudiantil: Universidad Autónoma de Bucaramanga.

Biswas, A. (2016). Applicability and usability of RFID technology in library. *Learning Community: An International Journal of Educational and Social Development, 7*(1), 53.

Bohn, J., & Mattern, F. (2004). *Super-distributed RFID tag infrastructures.* Paper presented at the European symposium on ambient intelligence.

Brock, J. D., Bruce, R. F., & Reiser, S. L. (2009). Using Arduino for introductory programming courses. *Journal of Computing Sciences in Colleges, 25*(2), 129-130.

Castillo, E. O., Rojas, H. E., & Gómez, E. J. (2016). Modulo RFID de Acceso para oficinas. *Tekhnê, 13*(2), 19-26.

CEA IoT. (2016). CEA-IoT | Centro de Excelencia y Apropiación en Internet de las Cosas. Retrieved 06/06/2017, 2017, from http://www.cea-iot.org/

Colciencias. (2016). Tipología de proyectos calificados como de carácter científico, tecnológico e innovación. Colciencias: Colciencias.

Congreso de Colombia. (2012). *LEY ESTATUTARIA 1581 DE 2012*. Diario Oficial de la Republica de Colombia: Diario Oficial 48587 Retrieved from http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf.

Congreso de la República de Colombia. (2009). *LEY 1341 DE 2009*. MINTIC: Diario Oficial 47426 Retrieved from http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf.

Curty, J.-P., Declercq, M., Dehollain, C., & Joehl, N. (2006). *Design and optimization of passive UHF RFID systems*: Springer Science & Business Media.

Chandra, P., Soni, P., & Keshari, R. K. (2014). RFID-based Ticketing for Public Transport System: Perspective Megacity. *International Journal of Advance Research in Computer Science and Management Studies, 2*(5).

Chuu, S.-J. (2014). An investment evaluation of supply chain RFID technologies: A group decision-making model with multiple information sources. *Knowledge-Based Systems, 66*, 210-220.

D'Ausilio, A. (2012). Arduino: A low-cost multipurpose lab equipment. *Behavior research methods, 44*(2), 305-313.

De Marco, A., Cagliano, A. C., Nervo, M., & Rafele, C. (2014). Modeling the effectiveness of radio frequency identification (RFID) technologies in improving sales performance in fashion retail outlets. *Fashion Supply Chain Management Using Radio Frequency Identification (RFID) Technologies*, 203.

Doukas, C. (2012). *Building Internet of Things with the ARDUINO*: CreateSpace Independent Publishing Platform.

Dubey, H., Yang, J., Constant, N., Amiri, A. M., Yang, Q., & Makodiya, K. (2015). *Fog data: Enhancing telehealth big data through fog computing.* Paper presented at the Proceedings of the ASE BigData & SocialInformatics 2015.

Edwards, E., & Orukpe, P. (2014). Development of a RFID based library management system and user access control. *Nigerian Journal of Technology, 33*(4), 574-584.

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper, 1*(2011), 1-11.

Farooq, U., ul Hasan, M., Amar, M., Hanif, A., & Asad, M. U. (2014). RFID based security and access control system. *International Journal of Engineering and Technology, 6*(4), 309.

Glidden, R., Bockorick, C., Cooper, S., Diorio, C., Dressler, D., Gutnik, V., . . . Humes, T. (2004). Design of ultra-low-cost UHF RFID tags for supply chain applications. *IEEE Communications Magazine, 42*(8), 140-151.

Gluck, A. (2015). Multi-purpose credit card reader apparatus: Google Patents.

Gordón Díaz, N. Y. (2009). *Control de acceso en la entrada del Instituto Geofísico utilizando tecnología RFID.* QUITO/EPN/2009.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems, 29*(7), 1645-1660.

Guillemin, P., & Friess, P. (2009). Internet of things strategic research roadmap. *The Cluster of European Research Projects, Tech. Rep*.

Gul, M. S., & Patidar, S. (2015). Understanding the energy consumption and occupancy of a multi-purpose academic building. *Energy and Buildings, 87*, 155-165.

Hernández, J. L. H., Valencia, R. E. C., & Morales, A. F. ADMINISTRACIÓN DE ARCHIVOS.

Institute of Electrical and Electronics Engineers - IEEE. (2015). *IEEE 802.3: Standard for Ethernet*. IEEE Standards Association.

Institute of Electrical and Electronics Engineers - IEEE. (2016). IEEE 802.11: Wireless LANs. IEEE: IEEE Standards Association,.

International Organization for Standardization - ISO. (2016). ISO/IEC 14443-1. ISO. International Organization for Standardization - ISO: ISO.

International Telecommunication Union - ITU. (2012). *SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN*. ITU.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2), 90-98.

Jang, J. J., Moon, J., & Jung, I. Y. (2015). *A Personalized Access Control Based on IoT.* Paper presented at the Dependable Computing (PRDC), 2015 IEEE 21st Pacific Rim International Symposium on.

Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). *RFID technology and its applications in Internet of Things (IoT).* Paper presented at the Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on.

Juels, A. (2006). RFID security and privacy: A research survey. *IEEE journal on selected areas in communications, 24*(2), 381-394.

Lee, C.-T., Wu, C.-C., Su, B.-R., & Shen, T.-C. (2016). *A novel electronic lock using ultrasound Morse code based on FIR filter.* Paper presented at the Advanced Materials for Science and Engineering (ICAMSE), International Conference on.

Lozano Segura, J. A. (2013). Estudio documental del aporte de la tecnología para la generación de ambientes seguros en las instituciones de educación superior (IES) colombianas.

Masek, L. (2003). Recognition of human iris patterns for biometric identification.
Meli, M., Gysel, M., Würms, M., & Meli, M. Low cost solutions to pairing issues in IEEE 802.15. 4 networks.

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials, 17*(3), 1268-1293.

Ministerio de Comercio Industria y Turismo. (2013). *DECRETO 1377 DE 2013*. Diario Oficial de la Republica de Colombia: Diario Oficial 48834 Retrieved from http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf.

Ministerio de Comercio Industria y Turismo. (2014). *Decreto número 886 de 2014*. Diario Oficial de la Republica de Colombia: Diario Oficial 49150 Retrieved from http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf.

Ministerio de Educación Nacional de Colombia- MEN. (2009). *Deserción estudiantil en la educación superior colombiana*.

Ministerio de Educación Nacional de Colombia- MEN. (2010). *Instituciones de Educación Superior (IES)*. Retrieved from https://www.mineducacion.gov.co/1621/article-217744.html

Ministerio de Educación Nacional de Colombia- MEN. (2015). *Decreto Único Reglamentario 1075 de 2015*. Ministerio de Educación Nacional de Colombia- MEN: Ministerio de Educación Nacional de Colombia- MEN, Retrieved from https://www.mineducacion.gov.co/1759/w3-article-351080.html.

Ministerio de Educación Nacional de Colombia - MEN. (2011). El ABC de la Deserción. Retrieved 25/05/2017, 2017, from http://www.mineducacion.gov.co/1621/articles-293659_archivo_pdf_abc.pdf

My Com Kits. (2008). Songle SRD Relay. Retrieved 01/02/2018, 2018, from http://www.mycomkits.com/reference/Songle_SRD(T73)_Relay.pdf

Nainan, S., Parekh, R., & Shah, T. (2013). RFID technology based attendance management system. *arXiv preprint arXiv:1306.5381*.

Ni, L. M., Liu, Y., Lau, Y. C., & Patil, A. P. (2004). LANDMARC: indoor location sensing using active RFID. *Wireless networks, 10*(6), 701-710.

NXP Semiconductors. (2016). MFRC522 - Standard performance MIFARE and NTAG frontend. Retrieved 02/02/2018, 2018, from https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf

Palma, D., Agudo, J. E., Sánchez, H., & Macías, M. M. (2014). An Internet of Things example: Classrooms access control over near field communication. *Sensors, 14*(4), 6998-7012.

Pandey, P., & Mahajan, K. (2012). *Application of RFID technology in libraries and role of librarian.* Paper presented at the 12th MANLIBNET Convention 2010, Jaipur.

Patino, J. M., Moreno, F. I., Figueroa, M. A. H., Garcia, J. M. L., & Martin, H. G. (2017). A modified analysis of electrical energy consumption in University buildings. *IEEE Latin America Transactions, 15*(3), 408-414.

Posamentier, J. (2005). RFID tag with separate transmit and receive clocks and related method: Google Patents.

Pouryayevali, S., Wahabi, S., Hari, S., & Hatzinakos, D. (2014). *On establishing evaluation standards for ECG biometrics.* Paper presented at the Acoustics, speech and signal processing (icassp), 2014 ieee international conference on.

Qiu, Y., Chen, J., & Zhu, Q. (2012). *Campus access control system based on RFID.* Paper presented at the Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on.

Raghavendra, R., Raja, K. B., Surbiryala, J., & Busch, C. (2014). *A low-cost multimodal biometric sensor to capture finger vein and fingerprint.* Paper presented at the Biometrics (IJCB), 2014 IEEE International Joint Conference on.

Raza, A., Ikram, A. A., Amin, A., & Ikram, A. J. (2016). *A review of low cost and power efficient development boards for IoT applications.* Paper presented at the Future Technologies Conference (FTC).

Raza, N., Bradshaw, V., & Hague, M. (1999). Applications of RFID technology.

Richardson, M., & Wallace, S. (2012). *Getting started with raspberry PI*: " O'Reilly Media, Inc.".

Risalat, N. A. M., Hasan, M. T., Hossain, M. S., & Rahman, M. M. (2017). *Advanced real time RFID mutual authentication protocol using dynamically updated secret value through encryption and decryption process.* Paper presented at the Electrical, Computer and Communication Engineering (ECCE), International Conference on.

Rodríguez Mederos, M., Montes de Oca Sánchez de Bustamante, A., & Dorta Héctor, J. (2002). Utilización y conservación de los soportes electrónicos. *Acimed, 10*(6), 7-8.

Rogers, A., Jones, E., & Oleynikov, D. (2007). Radio frequency identification (RFID) applied to surgical sponges. *Surgical endoscopy, 21*(7), 1235-1237.

Roper, K. O., Sedehi, A., & Ashuri, B. (2015). A cost-benefit case for RFID implementation in hospitals: adapting to industry reform. *Facilities, 33*(5/6), 367-388.

Sabol, C., Nick, W., Earl, M., Shelton, J., & Esterline, A. (2016). The WebID Protocol Enhanced With Group Access, Biometrics, and Access Policies.

Saib, J., & Suzuki, A. (2002). GUI resource editor for an embedded system: Google Patents.

Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2014). *Metodología de la investigación* (Vol. 5): Mcgraw-hill México.

Says, G. (2015). 6.4 billion connected "Things" will be in use in 2016, up 30 percent from 2015. *Gart. Inc*.

Schoeberl, M. (2008). *Jop: A java optimized processor for embedded real-time systems*: VDM Publishing.

Serratosa, F. (2008). La biometría para la identificación de las personas. *Universitat Oberta de Catalunya*, 8-20.

Shankar, S., & Udupi, V. (2016). Recognition of Faces–An Optimized Algorithmic Chain. *Procedia Computer Science, 89*, 597-606.

Sharma, R., Agarwal, A. K., & Singh, P. (2017). Comparing Different Methodologies Used To Ensure the Security of RFID Credit Card: A Comparative Analysis. *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 7*(1).

Sheela, S., & Vijaya, P. (2010). Iris recognition methods-survey. *International Journal of Computer Applications, 3*(5), 19-25.

Shen, X., Xu, K., Sun, X., Wu, J., & Lin, J. (2011). *Optimized indoor wireless propagation model in WiFi-RoF network architecture for RSS-based localization in the Internet of Things.* Paper presented at the Microwave Photonics, 2011 International Topical Meeting on & Microwave Photonics Conference, 2011 Asia-Pacific, MWP/APMP.

Shu, Y., Gu, Y. J., & Chen, J. (2014). Dynamic authentication with sensory information for the access control systems. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 427-436.

Silva, F., Filipe, V., & Pereira, A. (2008). *Automatic control of students' attendance in classrooms using RFID.* Paper presented at the Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on.

Sousa, P. J., Tavares, R., Abreu, P., Quintas, M., Reis, A., & Restivo, M. T. (2015). *Wireless control and network management of door locks.* Paper presented at the Experiment@ International Conference (exp. at'15), 2015 3rd.

Sowjanya, G., & Nagaraju, S. (2016). *Design and implementation of door access control and security system based on IOT.* Paper presented at the Inventive Computation Technologies (ICICT), International Conference on.

SPADIES. (2016). Tabla de deserción estudiantil. Retrieved 06/06/2017, 2017, from https://spadies.mineducacion.gov.co/spadies/JSON.html

Strauss, K. F., & Daud, T. (2000). *Overview of radiation tolerant unlimited write cycle non-volatile memory.* Paper presented at the Aerospace Conference Proceedings, 2000 IEEE.

Strong Link. (2002). Standard 4 kByte Card IC MF1 IC S70 - Data Sheet. Retrieved 26/01/2018, 2018, from http://www.stronglink-rfid.com/download/M043531.pdf

Unión Internacional de Telecomunicaciones - UIT. (2012). Reglamento de Radiocomunicaciones. ITU: Unión Internacional de Telecomunicaciones - UIT.

Universidad Autónoma de Bucaramanga - UNAB. (2017). UNAB en cifras 2016. UNAB: Universidad Autónoma de Bucaramanga - UNAB.

Universidad Autónoma de Bucaramanga - UNAB. (2018). Sistema de Préstamos y Reservas. Retrieved 03/03/2018, 2018

Videla, C., & A, O. (2016). Adermatoglifia: Una mutación genética que impide la formación de huellas dactilares. *Archivos de Criminología, Criminalística y Seguridad Privada, 6*.

Vujovic, V., & Maksimovic, M. (2014). *Raspberry Pi as a wireless sensor node: performances and constraints.* Paper presented at the Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on.

Wang, K. C., Wang, T. T., Jia, Z. F., & Zong, M. K. (2012). *Research of RFID Intelligent Access Control System in the Internet of Things.* Paper presented at the Advanced Materials Research.

Wang, W., Krishna, A., & McFerran, B. (2017). Turning Off the Lights: Consumers' Environmental Efforts Depend on Visible Efforts of Firms. *Journal of Marketing Research, 54*(3), 478-494.

Want, R. (2006). An introduction to RFID technology. *IEEE pervasive computing, 5*(1), 25-33.

Yale Colombia. (2011). Cantonera Eléctrica. Retrieved 06/02/2018, 2018, from https://www.yalecolombia.com/es/yale/yale/productos/cerraduras-electromecanicas/contra-larga/

Zhang, L. J. (2014). *Design of a Novel Automatic Access Control System.* Paper presented at the Advanced Materials Research.

ANEXO A – Preparación para instalación del sistema embebido

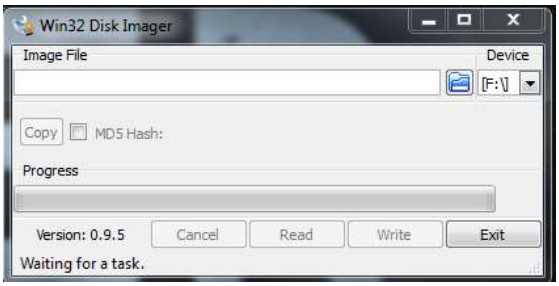
Requerimientos para la instalación:

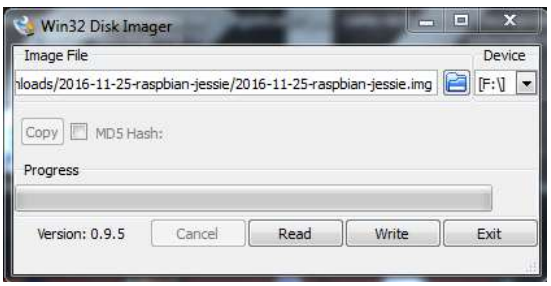
- Descargar última versión de Raspbian desde el sitio oficial de Raspberry Pi https://www.raspberrypi.org/downloads/raspbian/
- 

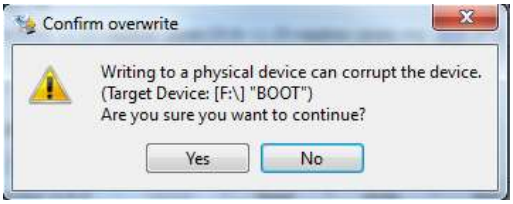
- Tener Win32DiskImager, se puede descargar la última versión desde https://sourceforge.net/projects/win32diskimager/
- Memoria SD de al menos 8GB

Pasos para la instalación:

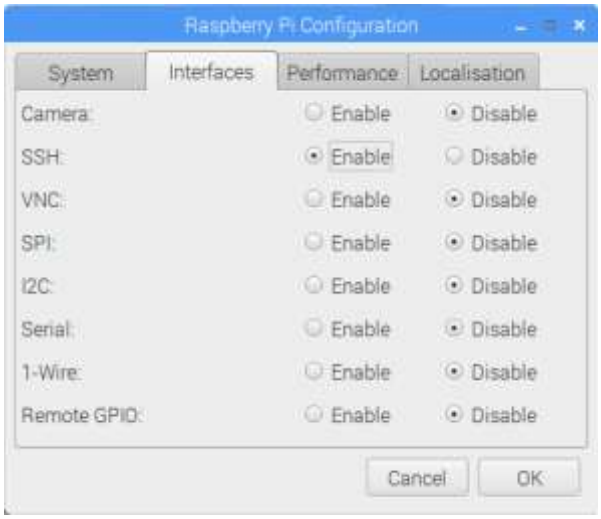
1. Ejecutar win32diskimager y seleccionar la ubicación donde se encuentra la imagen descargada de Raspbian junto con la unidad a la que se va a cargar la misma. Tras realizar lo anterior, seleccionar la opción de escribir sobre la memoria (write) y aceptar la escritura de la tarjeta para continuar. Al finalizar la copia, en la esquina inferior izquierda aparecerá un aviso diciendo ha finalizado el proceso (Done.) junto con una ventana emergente indicando si la escritura fue satisfactoria o no. Teniendo los pasos anteriores completados, se podrá conectar a la Raspberry Pi para iniciar el sistema operativo.



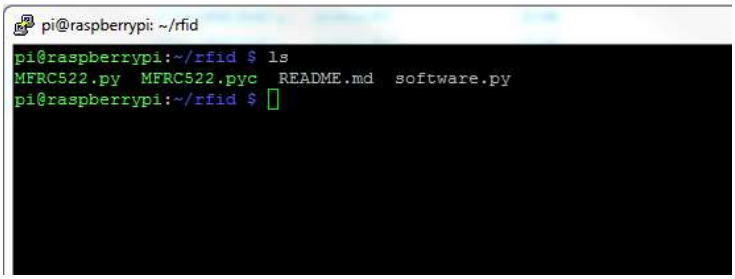




2. Una vez insertada la tarjeta SD en la Raspberry, procedemos a encenderla. Luego del primer inicio, se debe utilizar la conexión cableada o WiFi según su preferencia u uso que desee realizar. Recuerde habilitar en la herramienta de configuraciones de la Rapsberry la interface SPI, si se desea tener acceso SSH se debe habilitar de igual manera y en caso de usarse, habilitar el acceso remoto al GPIO.



3. Ingrese a la terminal y acceda como root utilizando el comando *sudo su* (para el acceso SSH el usuario es ***pi*** y la contraseña ***Raspberry***). Estando en el terminal, se creará una carpeta, donde se copiarán los archivos necesarios para ejecutar el programa (software.py, README.md, MFRC522.pye y MFRC522.py).

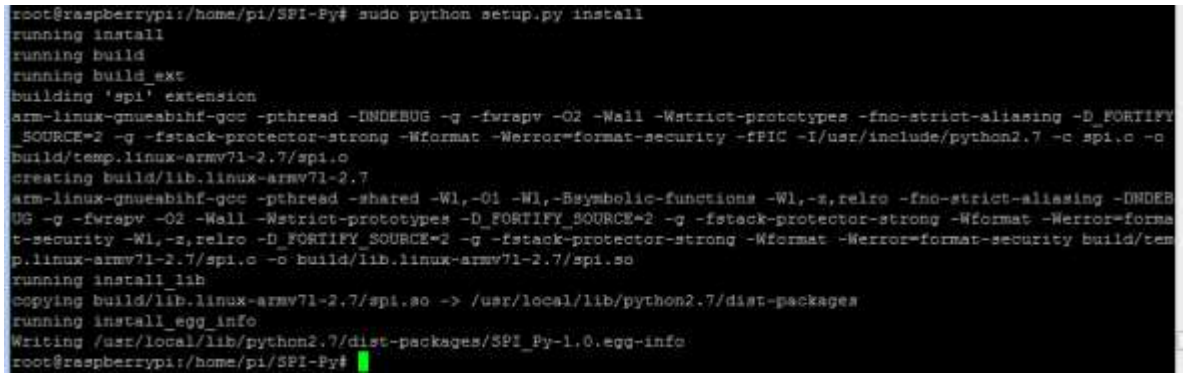


Se procederá a instalar ahora los módulos necesarios para la ejecución del software. Para esto saldremos del folder utilizando el comando cd .. y ejecutaremos las siguientes instrucciones:

sudo apt-get install python-dev

```
Reading state information... Done
The following extra packages will be installed:
  libpython-dev libpython2.7-dev python2.7-dev
The following NEW packages will be installed:
  libpython-dev libpython2.7-dev python-dev python2.7-dev
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 18.2 MB of archives.
After this operation, 25.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrordirector.raspbian.org/raspbian/ jessie/main libpython2.7-dev armhf 2.7.9-2+deb8u1 [17.9 MB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ jessie/main python-dev armhf 2.7.9-1 [1,188 B]
Get:3 http://mirrordirector.raspbian.org/raspbian/ jessie/main libpython-dev armhf 2.7.9-1 [19.6 kB]
Get:4 http://mirrordirector.raspbian.org/raspbian/ jessie/main python2.7-dev armhf 2.7.9-2+deb8u1 [287 kB]
Fetched 18.2 MB in 26s (699 kB/s)
Selecting previously unselected package libpython2.7-dev:armhf.
(Reading database ... 122302 files and directories currently installed.)
Preparing to unpack .../libpython2.7-dev_2.7.9-2+deb8u1_armhf.deb ...
Unpacking libpython2.7-dev:armhf (2.7.9-2+deb8u1) ...
Selecting previously unselected package libpython-dev:armhf.
Preparing to unpack .../libpython-dev_2.7.9-1_armhf.deb ...
Unpacking libpython-dev:armhf (2.7.9-1) ...
Selecting previously unselected package python2.7-dev.
Preparing to unpack .../python2.7-dev_2.7.9-2+deb8u1_armhf.deb ...
Unpacking python2.7-dev (2.7.9-2+deb8u1) ...
Selecting previously unselected package python-dev.
Preparing to unpack .../python-dev_2.7.9-1_armhf.deb ...
Unpacking python-dev (2.7.9-1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up libpython2.7-dev:armhf (2.7.9-2+deb8u1) ...
Setting up libpython-dev:armhf (2.7.9-1) ...
Setting up python2.7-dev (2.7.9-2+deb8u1) ...
Setting up python-dev (2.7.9-1) ...
root@raspberrypi:/home/pi/SPI-Py#
```

git clone https://github.com/lthiery/SPI-Py.git
cd SPI-Py
sudo python setup.py install



apt-get update
apt-get install python-pip python-dev libmysqlclient-dev
pip install MySQL-python

ANEXO B – Código fuente Python y librería MFRC522

Sección 1 – Código de funcionamiento del sistema

```
import MFRC522
import signal
import MySQLdb
import os
import time
import RPi.GPIO as GPIO

GPIO.setwarnings(False)
GPIO.setmode(GPIO.BOARD)


continue_reading = True
MIFAREReader = MFRC522.MFRC522()

os.system('cls' if os.name == 'nt' else 'clear')


access = 1
db = MySQLdb.connect(host="localhost", user="username_here",
passwd="password", db="dbname_here")
cur = db.cursor()
cardid = 0
cdb = 0
autorizacion = 0
user = "clear"

#GPIO.setup(8, GPIO.OUT)
GPIO.setup(18, GPIO.OUT)
#GPIO.output(8, False)

number = 0.001
timer = 150

time.sleep(1)
```

```
os.system('cls' if os.name == 'nt' else 'clear')

def end_read(signal, frame):
  global continue_reading
  continue_reading = False
  print "Ending read."
  MIFAREReader.GPIO_CLEEN()

signal.signal(signal.SIGINT, end_read)

while continue_reading:
  (status,TagType) =
MIFAREReader.MFRC522_Request(MIFAREReader.PICC_REQIDL)
  if status == MIFAREReader.MI_OK:
    os.system('cls' if os.name == 'nt' else 'clear')
  (status,backData) = MIFAREReader.MFRC522_Anticoll()
  if status == MIFAREReader.MI_OK:

    back =
str(backData[0])+str(backData[1])+str(backData[2])+str(backData[3])+str(backData[
4])
    back2 = str (back)
    print "        Cheking User and Card"
    cur.execute("SELECT cardid FROM users WHERE cardid= %s", (back2,) )
    cardid = cur.fetchone()

    if cardid != None:
      cdb = cardid[0]

      cur.execute("SELECT first_name FROM users WHERE cardid= %s", (back2,) )
      nombre = cur.fetchone()
      if nombre != None:
        user = nombre[0]

      cur.execute("SELECT last_name FROM users WHERE cardid= %s", (back2,) )
      nombre = cur.fetchone()
      if nombre != None:
        user = user + " " + nombre[0]
```

```
  cur.execute("SELECT status FROM users WHERE cardid= %s", (back2,) )
  status = cur.fetchone()
  if status != None:
    acs = status[0]



print "               Wait....."
time.sleep(1)
if  back2  == cdb:
  if access == acs:
        os.system('cls' if os.name == 'nt' else 'clear')
        #GPIO.output(26, True)
        GPIO.setup(36, GPIO.OUT)
        while timer != 0 :
                GPIO.output(18, True)
                time.sleep(number)
                GPIO.output(18, False)
                time.sleep(number)
                timer = timer - 1
        timer = 150
        #GPIO.output(26, 0)
        GPIO.setup(36, GPIO.IN)
        time.sleep(2)
        os.system('cls' if os.name == 'nt' else 'clear')
        reader"

  else:
        os.system('cls' if os.name == 'nt' else 'clear')

        for x in range (0, 4):
          while timer != 0 :
              GPIO.output(18, True)
              time.sleep(number)
              GPIO.output(18, False)
              time.sleep(number)
              timer = timer - 1
          timer = 150
```

```
            time.sleep(0.3)
          time.sleep(2)
          os.system('cls' if os.name == 'nt' else 'clear')
          reader"

    else:
          os.system('cls' if os.name == 'nt' else 'clear')
          for x in range (0, 4):
            while timer != 0 :
              GPIO.output(18, True)
              time.sleep(number)
              GPIO.output(18, False)
              time.sleep(number)
              timer = timer - 1
            timer = 150
            time.sleep(0.3)
          time.sleep(2)
          os.system('cls' if os.name == 'nt' else 'clear')
```

Sección 2 – Librería

```
import RPi.GPIO as GPIO
import spi
import signal

class MFRC522:
  NRSTPD = 22

  MAX_LEN = 16

  PCD_IDLE       = 0x00
  PCD_AUTHENT    = 0x0E
  PCD_RECEIVE    = 0x08
  PCD_TRANSMIT   = 0x04
  PCD_TRANSCEIVE = 0x0C
  PCD_RESETPHASE = 0x0F
  PCD_CALCCRC    = 0x03

  PICC_REQIDL    = 0x26
  PICC_REQALL    = 0x52
```

```
PICC_ANTICOLL  = 0x93
PICC_SEIECTTAG = 0x93
PICC_AUTHENT1A = 0x60
PICC_AUTHENT1B = 0x61
PICC_READ      = 0x30
PICC_WRITE     = 0xA0
PICC_DECREMENT = 0xC0
PICC_INCREMENT = 0xC1
PICC_RESTORE   = 0xC2
PICC_TRANSFER  = 0xB0
PICC_HALT      = 0x50

MI_OK       = 0
MI_NOTAGERR = 1
MI_ERR      = 2

Reserved00     = 0x00
CommandReg     = 0x01
CommIEnReg     = 0x02
DivlEnReg      = 0x03
CommIrqReg     = 0x04
DivIrqReg      = 0x05
ErrorReg       = 0x06
Status1Reg     = 0x07
Status2Reg     = 0x08
FIFODataReg    = 0x09
FIFOLevelReg   = 0x0A
WaterLevelReg  = 0x0B
ControlReg     = 0x0C
BitFramingReg  = 0x0D
CollReg        = 0x0E
Reserved01     = 0x0F

Reserved10     = 0x10
ModeReg        = 0x11
TxModeReg      = 0x12
RxModeReg      = 0x13
TxControlReg   = 0x14
TxAutoReg      = 0x15
```

```
TxSelReg       = 0x16
RxSelReg       = 0x17
RxThresholdReg = 0x18
DemodReg       = 0x19
Reserved11     = 0x1A
Reserved12     = 0x1B
MifareReg      = 0x1C
Reserved13     = 0x1D
Reserved14     = 0x1E
SerialSpeedReg = 0x1F

Reserved20        = 0x20
CRCResultRegM     = 0x21
CRCResultRegL     = 0x22
Reserved21        = 0x23
ModWidthReg       = 0x24
Reserved22        = 0x25
RFCfgReg          = 0x26
GsNReg            = 0x27
CWGsPReg          = 0x28
ModGsPReg         = 0x29
TModeReg          = 0x2A
TPrescalerReg     = 0x2B
TReloadRegH       = 0x2C
TReloadRegL       = 0x2D
TCounterValueRegH = 0x2E
TCounterValueRegL = 0x2F

Reserved30      = 0x30
TestSel1Reg     = 0x31
TestSel2Reg     = 0x32
TestPinEnReg    = 0x33
TestPinValueReg = 0x34
TestBusReg      = 0x35
AutoTestReg     = 0x36
VersionReg      = 0x37
AnalogTestReg   = 0x38
TestDAC1Reg     = 0x39
TestDAC2Reg     = 0x3A
```

```
TestADCReg      = 0x3B
Reserved31      = 0x3C
Reserved32      = 0x3D
Reserved33      = 0x3E
Reserved34      = 0x3F

serNum = []

def __init__(self,spd=1000000):
  spi.openSPI(speed=spd)
  GPIO.setmode(GPIO.BOARD)
  GPIO.setup(22, GPIO.OUT)
  GPIO.output(self.NRSTPD, 1)
  self.MFRC522_Init()

def MFRC522_Reset(self):
  self.Write_MFRC522(self.CommandReg, self.PCD_RESETPHASE)

def Write_MFRC522(self,addr,val):
  spi.transfer(((addr<<1)&0x7E,val))

def Read_MFRC522(self,addr):
  val = spi.transfer((((addr<<1)&0x7E) | 0x80,0))
  return val[1]

def SetBitMask(self, reg, mask):
  tmp = self.Read_MFRC522(reg)
  self.Write_MFRC522(reg, tmp | mask)

def ClearBitMask(self, reg, mask):
  tmp = self.Read_MFRC522(reg);
  self.Write_MFRC522(reg, tmp & (~mask))

def AntennaOn(self):
  temp = self.Read_MFRC522(self.TxControlReg)
  if(~(temp & 0x03)):
    self.SetBitMask(self.TxControlReg, 0x03)

def AntennaOff(self):
```

```
  self.ClearBitMask(self.TxControlReg, 0x03)

def MFRC522_ToCard(self,command,sendData):
  backData = []
  backLen = 0
  status = self.MI_ERR
  irqEn = 0x00
  waitIRq = 0x00
  lastBits = None
  n = 0
  i = 0

  if command == self.PCD_AUTHENT:
    irqEn = 0x12
    waitIRq = 0x10
  if command == self.PCD_TRANSCEIVE:
    irqEn = 0x77
    waitIRq = 0x30

  self.Write_MFRC522(self.CommIEnReg, irqEn|0x80)
  self.ClearBitMask(self.CommIrqReg, 0x80)
  self.SetBitMask(self.FIFOLevelReg, 0x80)

  self.Write_MFRC522(self.CommandReg, self.PCD_IDLE);

  while(i<len(sendData)):
    self.Write_MFRC522(self.FIFODataReg, sendData[i])
    i = i+1

  self.Write_MFRC522(self.CommandReg, command)

  if command == self.PCD_TRANSCEIVE:
    self.SetBitMask(self.BitFramingReg, 0x80)

  i = 2000
  while True:
    n = self.Read_MFRC522(self.CommIrqReg)
    i = i - 1
    if ~((i!=0) and ~(n&0x01) and ~(n&waitIRq)):
```

```
      break

    self.ClearBitMask(self.BitFramingReg, 0x80)

    if i != 0:
      if (self.Read_MFRC522(self.ErrorReg) & 0x1B)==0x00:
        status = self.MI_OK

        if n & irqEn & 0x01:
          status = self.MI_NOTAGERR

        if command == self.PCD_TRANSCEIVE:
          n = self.Read_MFRC522(self.FIFOLevelReg)
          lastBits = self.Read_MFRC522(self.ControlReg) & 0x07
          if lastBits != 0:
            backLen = (n-1)*8 + lastBits
          else:
            backLen = n*8

          if n == 0:
            n = 1
          if n > self.MAX_LEN:
            n = self.MAX_LEN

          i = 0
          while i<n:
            backData.append(self.Read_MFRC522(self.FIFODataReg))
            i = i + 1;
      else:
        status = self.MI_ERR

    return (status,backData,backLen)


  def MFRC522_Request(self, reqMode):
    status = None
    backBits = None
    TagType = []
```

```
    self.Write_MFRC522(self.BitFramingReg, 0x07)

    TagType.append(reqMode);
    (status,backData,backBits) = self.MFRC522_ToCard(self.PCD_TRANSCEIVE,
TagType)

    if ((status != self.MI_OK) | (backBits != 0x10)):
      status = self.MI_ERR

    return (status,backBits)


  def MFRC522_Anticoll(self):
    backData = []
    serNumCheck = 0

    serNum = []

    self.Write_MFRC522(self.BitFramingReg, 0x00)

    serNum.append(self.PICC_ANTICOLL)
    serNum.append(0x20)

    (status,backData,backBits) =
self.MFRC522_ToCard(self.PCD_TRANSCEIVE,serNum)

    if(status == self.MI_OK):
      i = 0
      if len(backData)==5:
        while i<4:
          serNumCheck = serNumCheck ^ backData[i]
          i = i + 1
        if serNumCheck != backData[i]:
          status = self.MI_ERR
      else:
        status = self.MI_ERR

    return (status,backData)
```

```
  def CalulateCRC(self, pIndata):
    self.ClearBitMask(self.DivIrqReg, 0x04)
    self.SetBitMask(self.FIFOLevelReg, 0x80);
    i = 0
    while i<len(pIndata):
      self.Write_MFRC522(self.FIFODataReg, pIndata[i])
      i = i + 1
    self.Write_MFRC522(self.CommandReg, self.PCD_CALCCRC)
    i = 0xFF
    while True:
      n = self.Read_MFRC522(self.DivIrqReg)
      i = i - 1
      if not ((i != 0) and not (n&0x04)):
        break
    pOutData = []
    pOutData.append(self.Read_MFRC522(self.CRCResultRegL))
    pOutData.append(self.Read_MFRC522(self.CRCResultRegM))
    return pOutData

  def MFRC522_SelectTag(self, serNum):
    backData = []
    buf = []
    buf.append(self.PICC_SElECTTAG)
    buf.append(0x70)
    i = 0
    while i<5:
      buf.append(serNum[i])
      i = i + 1
    pOut = self.CalulateCRC(buf)
    buf.append(pOut[0])
    buf.append(pOut[1])
    (status, backData, backLen) = self.MFRC522_ToCard(self.PCD_TRANSCEIVE,
buf)

    if (status == self.MI_OK) and (backLen == 0x18):
      print "Size: " + str(backData[0])
      return  backData[0]
    else:
      return 0
```

```
  def MFRC522_Auth(self, authMode, BlockAddr, Sectorkey, serNum):
    buff = []
    buff.append(authMode)
    buff.append(BlockAddr)
    i = 0
    while(i < len(Sectorkey)):
      buff.append(Sectorkey[i])
      i = i + 1
    i = 0
    while(i < len(serNum)):
      buff.append(serNum[i])
      i = i +1
    (status, backData, backLen) = self.MFRC522_ToCard(self.PCD_AUTHENT,buff)
    if not(status == self.MI_OK):
      print "AUTH ERROR!!"
    if not (self.Read_MFRC522(self.Status2Reg) & 0x08) != 0:
      print "AUTH ERROR(status2reg & 0x08) != 0"

    return status

  def MFRC522_Read(self, blockAddr):
    recvData = []
    recvData.append(self.PICC_READ)
    recvData.append(blockAddr)
    pOut = self.CalulateCRC(recvData)
    recvData.append(pOut[0])
    recvData.append(pOut[1])
    (status, backData, backLen) = self.MFRC522_ToCard(self.PCD_TRANSCEIVE,
recvData)
    if not(status == self.MI_OK):
      print "Error while reading!"

    print "Got data size: "+str(backLen)
    i = 0
    if len(backData) == 16:
      print "Sector "+str(blockAddr)+" "+str(backData)

  def MFRC522_Write(self, blockAddr, writeData):
```

```
    buff = []
    buff.append(self.PICC_WRITE)
    buff.append(blockAddr)
    crc = self.CalulateCRC(buff)
    buff.append(crc[0])
    buff.append(crc[1])
    (status, backData, backLen) = self.MFRC522_ToCard(self.PCD_TRANSCEIVE,
buff)
    if not(status == self.MI_OK) or not(backLen == 4) or not((backData[0] & 0x0F)
== 0x0A):
      status = self.MI_ERR

    print str(backLen)+" backdata &0x0F == 0x0A "+str(backData[0]&0x0F)
    if status == self.MI_OK:
        i = 0
        buf = []
        while i < 16:
          buf.append(writeData[i])
          i = i + 1
        crc = self.CalulateCRC(buf)
        buf.append(crc[0])
        buf.append(crc[1])
        (status, backData, backLen) =
self.MFRC522_ToCard(self.PCD_TRANSCEIVE,buf)
        if not(status == self.MI_OK) or not(backLen == 4) or not((backData[0] & 0x0F)
== 0x0A):
          print "Error while writing"
        if status == self.MI_OK:
          print "Data writen"


  def MFRC522_Init(self):
    GPIO.output(self.NRSTPD, 1)

    self.MFRC522_Reset();


    self.Write_MFRC522(self.TModeReg, 0x8D)
    self.Write_MFRC522(self.TPrescalerReg, 0x3E)
```

```
  self.Write_MFRC522(self.TReloadRegL, 30)
  self.Write_MFRC522(self.TReloadRegH, 0)

  self.Write_MFRC522(self.TxAutoReg, 0x40)
  self.Write_MFRC522(self.ModeReg, 0x3D)
  self.AntennaOn()

def GPIO_CLEEN(self):
  GPIO.cleanup()
```

Anexo C - Encuesta de percepción estudiantil

Bienvenidos, por favor respondan las preguntas a consideración.

Sección A: General

A1. ¿Ha escuchado o sabe que es el Internet de las Cosas (IoT)?

- Si ☐
- No ☐

A2. ¿Ha escuchado o sabe que es la tecnología RFID?

- Si ☐
- No ☐

A3. ¿Estaría de acuerdo con la implementación de tecnologías como RFID para el ingreso a las aulas y laboratorios de clase?

- Si ☐
- No ☐

A4. El tomar asistencia a clase es parte de la labor docente durante el transcurso de la clase; si se implementara el uso de RFID para el control de asistencia a estudiantes, ¿Estaría de acuerdo con su uso?

- Si ☐
- No ☐

A5. ¿Por qué no estaría de acuerdo?

A6. Si la universidad implementara RFID para el control de asistencia y como segundo factor de autenticación empleara el reconocimiento facial, ¿Estaría de acuerdo?

- Si ☐
- No ☐

A7. **¿Por qué no estaría de acuerdo?**

Tu opinión es valiosa, gracias por contestar la encuesta.

Anexo D - Encuesta de aceptación de tecnologías en IES

Bienvenidos, por favor respondan las preguntas a consideración.

Sección A: General

A1. **Los docentes de las materias que esta cursando este semestre toman asistencia?**

- [ ] Si
- [ ] No

A2. **Si la anterior pregunta fue SI, responda: Por lo general, en que periodo de tiempo suelen tomar asistencia los docentes con los cuales esta cursando materias durante este semestre:**

- [ ] Todas las clases
- [ ] 2 o 3 veces a la semana
- [ ] 1 vez a la semana
- [ ] 1 vez al mes

A3. **El tomar asistencia toma parte del tiempo de la clase, ¿Le gustaría que ese tiempo fuese utilizado para tratar temas del curso y no ejecutando esta acción?**

- [ ] Si
- [ ] No

A4. **Usualmente andes de iniciar una clase, las aulas y/o laboratorios se encuentran:**

- [ ] Abierta
- [ ] Cerrada

A5. **Cuando un aula de clase se encuentra cerrada, el tiempo de apertura de la misma es:**

- [ ] 1-3 min
- [ ] 4-5min
- [ ] 5-10 min
- [ ] 10m o más

A6. **¿Está conforme con los tiempos de apertura de las aulas y/o laboratorios de clase?**

Si ☐

No ☐

A7. **Le gustaría que la universidad implementara algún sistema para automatizar el proceso de apertura de las aulas y laboratorios de clase?**

Si ☐

No ☐

Tu opinión es valiosa, gracias por contestar la encuesta.