ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DESARROLLO DE UN SISTEMA ALTERNATIVO DE ACCESO A LAS ÁREAS RESTRINGIDAS DE LA FIEC MEDIANTE EL USO DE DISPOSITIVOS MÓVILES"

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del Título de:

INGENIERO EN TELEMÁTICA

KEVIN XAVIER ÁVALOS EDUARTE

DANIEL RICARDO SANTACRUZ ALVAREZ

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

Agradezco en primer lugar a Dios, a mis compañeros y amigos que colaboraron de manera directa e indirecta para llevar a cabo este objetivo aportando cada uno con sus experiencias y conocimientos. De igual manera agradezco a mi familia por haber estado presente en múltiples maneras, apoyándome en todo momento. A todos los docentes que en mi vida estudiantil supieron guiarme por este largo camino.

KEVIN AVALOS

Agradezco a Dios que me dio perseverancia para continuar en este arduo camino que parecía interminable, a mis padres, por su constante apoyo, sus consejos siempre sabios que me guiaron por un buen camino, siempre inculcándome el sentido de la responsabilidad, y sobre todo agradezco todo el sacrificio que han hecho por darme todos estos estudios a lo largo de mi vida académica, a mis hermanos que también me dieron su palabra de aliento cada vez que lo necesitaba. A mi enamorada que siempre me animó a seguir adelante, a pesar de la adversidad siempre me motivo a llegar hasta el final.

DANIEL SANTACRUZ

DEDICATORIA

El presente proyecto lo dedico a mi madre y a mis tíos por haber sido un soporte durante toda mi carrera, por brindarme su apoyo económico y emocional en todo momento, de igual manera me han sabido guiar para ser un hombre de bien y de valores.

KEVIN AVALOS

Esta tesis y título obtenido se la dedico a mis padres y hermanos, quienes siempre me daban palabras de aliento para jamás desistir de mi decisión de estudiar en esta universidad, me hicieron comprender que la vida siempre está llena de sacrificios y problemas, pero que un hombre de bien siempre sabe cómo afrontarlos.

DANIEL SANTACRUZ

TRIBUNAL DE EVALUACIÓN

Rebeca Estrada, Ph.D.

PROFESOR EVALUADOR

Ing. Vladimir Sánchez

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Kevin Avalos E.

Kevin Xavier Ávalos Eduarte

Daniel Santacruz

Daniel Ricardo Santacruz Alvarez

RESUMEN

En la Facultad de Ingeniería en Electricidad y Computación (FIEC) de la ESPOL, se experimenta pérdida, deterioro u olvido de las tarjetas magnéticas de los sistemas de acceso, dejando al docente sin un método de autenticación hasta la reposición de la misma, lo cual conllevará a cierto periodo de espera.

El presente proyecto integrador ofrece una solución alternativa a los sistemas de acceso existentes en la FIEC para sus docentes. Se propone usar el sensor Near Field Communication (NFC) de los dispositivos móviles [2,3]. Este sensor utiliza tecnología inalámbrica de corto alcance y una frecuencia muy alta para el intercambio de datos [3] basados en tecnología RFID[12], el único dato que se necesita obtener es el identificador único (UID).

Dicho proyecto se centra en la necesidad de tener un sistema alternativo de acceso (que no reemplazará al sistema de acceso actual -con tarjetas magnéticas-) usando su dispositivo móvil (por ejemplo, teléfono celular o tablet) que cuente con el sensor NFC. Para aquellos docentes que no cuenten con este sensor, se propone la alternativa de usar su carnet institucional de ESPOL, el mismo que cuenta con la tecnología de identificación por radiofrecuencia (RFID) [12,16], también se puede usar etiquetas NFC adheridas en la parte posterior de su celular, simulan el sensor NFC que carecen en su dispositivo móvil.

Este sistema de acceso consta de un prototipo de bajo costo que se encarga de leer el campo UID del sensor NFC, se lo envía (mediante bus de datos) a una Raspberry Pi (RPI) [9], la cual es una mini computadora que hará las veces de servidor de bases de datos y de servidor web, comparándolo con los datos registrados; si dicho UID se encuentra en la base de datos, se le otorga el acceso a dicha área restringida; caso contrario, se lo deniega.

Debido a que el desarrollo de este proyecto es solo un prototipo, éste posee ciertas limitaciones, con opciones a posibles mejoras en trabajo a futuro.

ÍNDICE GENERAL

CAPÍTULO 1

1. SISTEMA DE CONTROL DE ACCESO.

1.1 Antecedentes.

La tecnología ha dado un gran avance en esta última década, y con ellos los dispositivos móviles también han dado pasos de gran alcance tecnológico, surgiendo el nacimiento de gran cantidad de dispositivos entre ellos los dispositivos que implementan la llamada tecnología wearables[17, 18] que incluyen diferente cantidad de sensores de acuerdo al elemento que se esté usando.

Hoy en día son muchos los usuarios que cuentan con uno de estos dispositivos (NFC Ring, o pulseras con tecnología RFID, smartphones, tarjetas o carnets) y muy pocos los que no cuentan con un dispositivo de tales características (pero esto es casi nulo, ya que ahora un elemento de éstas características está asequible para el alcance económico de la familia ecuatoriana promedio). Debido a que se ha incrementado de manera exponencial este mercado, la seguridad en los datos del usuario ha sido todo un reto. Poco a poco han salido a la venta dispositivos móviles que ofrecen cada vez más una mayor seguridad para el usuario, entre ellos, han incorporado un sensor NFC[2,3] (Comunicación inalámbrica que están basados en radio frecuencia de manera cifrada <esta tecnología es utilizada para sistemas de pago móvil debido a la gran seguridad que ofrece >), en base a este sensor se desarrollará este proyecto.

1.2 Descripción del problema.

Las personas tienen la tendencia natural de extraviar u olvidar las cosas, entre ellos sus tarjetas o credenciales de acceso. En este caso el espacio de estudio es la FIEC, facultad la cual está ubicada dentro de la Escuela Superior Politécnica del Litoral. Se tiene conocimiento de la existencia de un sistema para el control de acceso a áreas restringidas el cuál funciona con tarjetas de proximidad, a lo largo del tiempo que este sistema lleva implementado se han registrado pérdidas

de tarjetas o la incomodidad que conlleva el uso de las mismas. Para tratar este inconveniente o limitación se ha realizado encuestas que permiten tener conocimiento de la opinión de los docentes de esta facultad respecto del uso de esta tecnología, y de esta manera nos permita desarrollar una solución que acabe con las limitaciones que implica el uso de este sistema.

Los resultados de estas encuestas convergen a que efectivamente el sistema actual es limitado respecto a la forma de acceso a las áreas, existiendo un solo dispositivo de identificación.

Esta información obtenida nos permite identificar un principal objetivo el cuál permita flexibilidad al momento de identificarse dentro de las áreas restringidas, para esto se usará etiquetas NFC los cuáles están incluidos dentro de la tecnología para wearables, dado que estos etiquetas son adhesivos, y permiten a su vez ser colocados sobre dispositivos convencionales de uso diario dando así la flexibilidad que se desea dar a los usuarios del sistema.

Sin descuidar los aspectos de seguridad también se podrá dar de baja o inactivar alguna etiqueta o tag en caso de ésta caer en manos equivocadas.

1.3 Objetivos.

1.3.1 Objetivo General.

Implementar un sistema alternativo de acceso (a manera de prototipo) para que los docentes de FIEC puedan acceder a las áreas restringidas usando dispositivos móviles que contengan etiquetas o etiquetas NFC.

1.3.2 Objetivos Específicos.

- Recopilar información acerca de los problemas y necesidades de los usuarios para así conocer más a detalle las características que el sistema debe adoptar.
- Habilitar y permitir el uso de phpMyAdmin para poder contar con una interfaz sencilla y amigable de administración de la base de datos y

manejo de usuarios del sistema para el administrador de la red interna de FIEC.

- Diseñar una base de datos para albergar la relación entre el docente y su respectivo dispositivo para acceso, tomando en cuenta el registro, modificación y eliminación de datos. Agregando a esto el tener que relacionar los accesos que se registran de un docente a un área.

- Implementar un sistema físico para la lectura y envío de información desde las etiquetas NFC.

1.4 Justificación.

En la actualidad el sistema para control de acceso con el que cuenta la FIEC está en funcionamiento y es considerado un sistema confiable, pero a su vez se considera que este sistema no es lo suficiente flexible limitando a sus usuarios al uso de tarjetas de proximidad dejando una única vía de acceso por persona, la misma que en caso de su pérdida dejaría sin acceso al docente. La idea principal es dar redundancia y permitir el acceso de una persona por más de una vía.

Es necesario además para esto que se le pueda asignar a un mismo docente más de una identificador o tag NFC, dando más de una forma de identificarse ante el lector de la puerta, haciendo una analogía se podría decir que se desea que los identificadores de una misma persona sean equivalentes de la misma manera que son equivalentes una cédula y una licencia al momento de identificarse cómo mayor de edad en varios lugares.

1.5 Alcance y limitaciones.

El sistema a implementarse es un prototipo el cuál podría ser mejorado o adaptado a las necesidades vigentes de los usuarios.

La persona encargada que tendrá el control total de administrar este sistema será el administrador de la red de la Facultad, encargándose de agregar, eliminar o consultar los docentes que tendrán acceso a dicha área restringida, en caso que la FIEC decide implementar este proyecto.

Entre las funciones principales del sistema está el poder registrar a un docente o en su lugar si el docente ya existe asignarle un identificador adicional, otra funcionalidad es la de poder registrar los datos del docente, añadido a esto se podrá obtener reportes acerca de los accesos al área o acceso por docente dentro del área.

Al tratarse de un prototipo está limitado a una sola área para efectos de muestra se usará una puerta pequeña que simule los efectos sobre una puerta de tamaño real.

No todos los dispositivos móviles contarán con esta ventaja debido a que es necesario que los dispositivos implementen o usen tecnología NFCa. Para realizarle test al sistema se ha procedido a realizar el método de prueba y error tomando en cuenta diversidad de dispositivos logrando considerar como utilizables los siguientes:

- Etiquetas o etiquetas NFC.
- Tarjetas del sistema de transporte Metrovía de la ciudad de Guayaquil (solo usado para pruebas del proyecto).
- Carnets otorgados por la ESPOL (a partir de agosto 2014).
- Tablet Samsung Galaxy Tab Active.

CAPÍTULO 2

2. MARCO TEÓRICO.

2.1 Redes informáticas inalámbricas Wifi.

Para entender las redes inalámbricas WiFi, primero es necesario entender que una red informática es un conjunto de computadoras o dispositivos de red (sean smarthphones, tablets o incluso Smart TV's) comunicados entre sí, ya sea por medio de cable o no, siendo esta última la tecnología WiFi (Wireless Fidelity). Para estar conectado a una red inalámbrica WiFi solo hace falta constar con una tarjeta de red inalámbrica en las computadoras o dispositivos involucrados, configurar el dispositivo que suministra la red WiFi y todo queda listo para funcionar de forma óptima.

Este método resulta mucho más rápido, flexible y menos costoso que disponer de una red cableada; las computadoras y dispositivos de red una vez que ya forman parte de la red pueden comunicarse entre sí y compartir recursos, entre ellos: archivos, directorios, impresoras, unidades de disco, e inclusive acceso a otras redes fuera del rango de dicha red.

WiFi es un mecanismo de conexión de dispositivos electrónicos de manera inalámbrica, usando el espectro electromagnético alcanzando frecuencias de 2.4 GHz ó 5 GHz y velocidades de 11 Mbps como máximo (en la tecnología 802.11b), en versiones más recientes se pueden alcanzar de 22.54 hasta los 100 Mbps.

2.2 Identificación por radiofrecuencia.

Gracias a esta tecnología de identificación por radiofrecuencia ó RFID (por sus siglas en inglés) es uno de los sistemas más óptimos para la identificación automática (una identificación similar a la del código de barras)[4] desplazando ya a la identificación por código de barras.

Los sistemas RFID ó sistemas de identificación por radiofrecuencia ofrecen ciertas ventajas con respecto a otros sistemas de identificación[6], como por

ejemplo, tratar cada objeto o producto como único y no acepta bajo ningún concepto algún duplicado, otra ventaja es que almacena más información permitiendo así ser un sistema de almacenamiento y recuperación de datos remoto que usas dispositivos como tarjetas, etiquetas o etiquetas, el cual permiten transmitir su ID de un objeto mediante ondas de radio en cierto tipo de frecuencia.

Los sistemas RFID básicamente están compuestos de un componente que transmite y recibe señales (transponder) que se encuentra dentro de una etiqueta o tag RFID[7] y de otro componente que es el lector RFID.

2.2.1 Etiqueta/Tag RFID.

Las tarjetas o etiquetas RFID están compuestas por una antena y un chip[19] (ver figura 2.1), el cual es el encargado de almacenar el ID del objeto y ciertos tipos de campos adicionales, dichas tarjetas pueden necesitar alimentación interna o no y se clasifican en activas y pasivas.

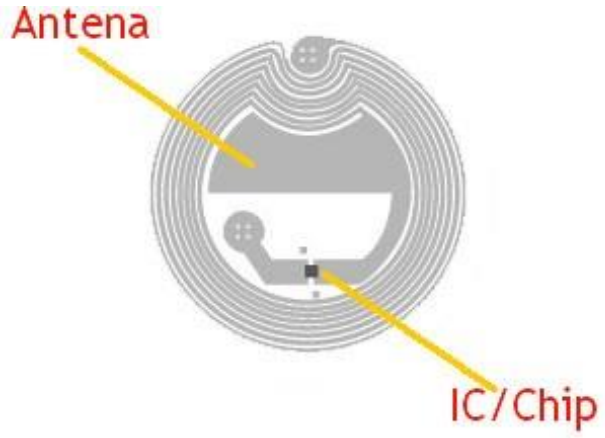


Figura 2.1 : Descripción de un tag NFC/RFID [19].

2.2.2 Identificación por radiofrecuencia activas.

Este tipo de tarjetas necesitan de alimentación de energía interna para su funcionamiento, pudiendo obtenerlas mediante celdas solares o baterías (es la comúnmente usada). La principal ventaja es que este tipo de tarjetas ofrece una mayor cantidad de almacenamiento, y la posibilidad de aumentar la distancia de comunicación entre el transponder[7] y el lector RFID previamente ya mencionados.

2.2.3 Identificación por radiofrecuencia pasivas.

Este tipo de tarjetas no requieren ningún tipo de alimentación eléctrica interna, pero poseen un menor tamaño y un menor costo. Su desventaja consiste en la distancia de comunicación con el lector[9], ya que para poder transmitir su información, entre ellas su campo ID, es necesario que el lector le induzca un campo electromagnético con la finalidad de brindar la alimentación necesaria para la transferencia de datos; esto lo logra a través de la antena, el campo electromagnético del lector provee toda la cantidad de energía requerida para energizar el transponder[7]; para que se pueda transmitir la información del chip de la tarjeta hacia el lector, el campo del lector es modulado por modulación de desplazamiento de frecuencia (FSK), que es una técnica de modulación digital por frecuencia.

2.2.4 Funcionamiento de un sistema basado en RFID.

Para entender este funcionamiento, se lo detallará en unos sencillos pasos, ilustrados en la figura 2.2; estos son[12]:

- La etiqueta o TAG RFID/NFC entra en el campo electromagnético producido por el lector RFID.
- La señal de RF (radio frecuencia) originado por la lectora energiza la etiqueta o TAG RFID/NFC.
- La etiqueta transmite su campo de identificación hacia la lectora RFID.
- La tarjeta lectora recibe el UID de la etiqueta RFID/NFC.

- La lectora envía dicho campo o campos (dependiendo del caso) hacia un computador receptor.
- La computadora procesa dichos datos de acuerdo a lo programado y genera la acción pertinente.

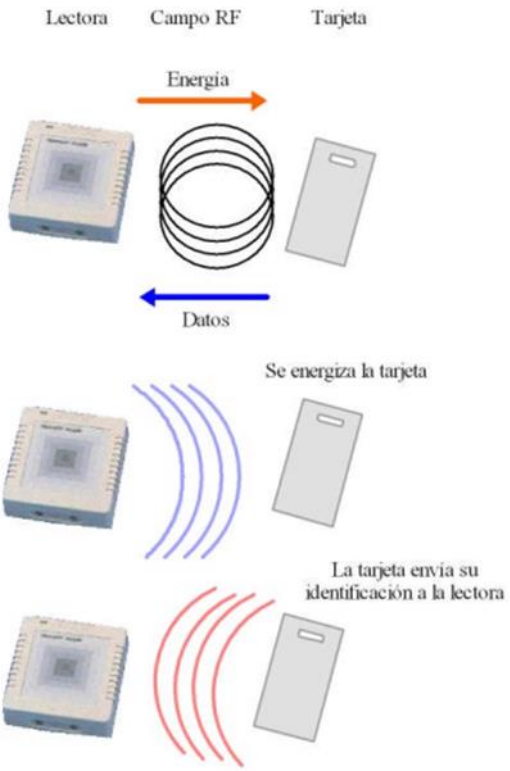


Figura 2.2: Funcionamiento de un sistema RFID[16].

2.3 Sistemas embebidos.

Para entender los componentes y fases de este proyecto, en necesario entender los componentes, aplicaciones y características que tiene un sistema embebido, y por qué se decidió usarlo en el desarrollo de este proyecto.

Un sistema embebido es un sistema informático construido para un uso específico con circuitería electrónica lo más simple y pequeña posible; dichos sistemas se usan para diversas utilidades, y por lo general vienen con dispositivos de memoria de manera integrada[20], con puertos de comunicación integrada de igual manera y con módulos de entrada/salida. De manera breve, un sistema

embebido consiste en un sistema basado en un microprocesador y/o CPU cuyos componentes de hardware y software están diseñados y optimizados de manera específica en la resolución de un problema de manera eficiente. También interactúa con el entorno para controlar o vigilar ciertos procesos mediante sensores gracias a que su hardware está diseñado principalmente a nivel de chips.

Un sistema embebido complejo puede utilizar un sistema operativo para la ejecución de programas[20] un poco más avanzados que requieran talvez una mayor cantidad de procesamiento, sobre todo cuando se requiere una ejecución de varios programas corriendo a la vez (concepto multithreads de Programación Orientada a Objetos).

Entre los principales componentes de un sistema embebido se tiene:

- CPU
- Memoria
- Actuadores
- Módulo de Reloj
- Comunicación
- Módulo de entrada y salida E/S
- Módulo de energía

2.3.1 CPU.

Es la unidad en la cual se ejecutan y procesan las instrucciones de los programas y se controla el funcionamiento de todos los distintos componentes que tiene el micro-ordenador o microcontrolador.

2.3.2 Memoria.

Existe dos tipos de memoria: interna o externa. En el subsistema de memoria se almacenan las instrucciones de los programas que controlan el buen funcionamiento de dicho sistema. Existen buffers

de memoria que almacenan varios tipos de datos, los datos de entrada que aún no han sido procesados, los resultados intermedios en procesamiento y resultados finales.

2.3.3 Actuadores.

Son los posibles componentes de origen electrónico a ser controlados por el sistema, éstos pueden ser conmutadores tipo relé o un motor eléctrico o motor hidroeléctrico.

2.3.4 Módulo de Reloj.

Es quien se encarga de generar las diferentes señales de reloj a partir de un único oscilador y generador principal. Este oscilador es importante por la frecuencia necesaria para el circuito y mantenerlo de manera estable. El mejor oscilador que existe en el mercado está basado en un resonador de cristal de cuarzo porque proporcionan estabilidad al sistema.

2.3.5 Comunicación.

Este componente es de suma importancia, ya que le da la habilidad al sistema de comunicarse mediante una interfaz, entre ellas pueden ser del tipo: DSRC, GSM, GPRS, CAN, WIFI, RS232, IP, RS485, USB, I2C, etc.

2.3.6 Módulo de entrada y salida E/S.

Estos módulos pueden ser de señales analógicas o digitales, pueden emplearse para activar diodos LED, verificar el estado de un conmutador o pulsador abierto/cerrado.

2.3.7 Módulo de energía.

Dicho módulo se encarga de generar las diferentes variaciones de voltajes o tensiones y corrientes necesarias para alimentar los diferentes componentes del circuito del sistema embebido. Normalmente se trabaja con un rango de voltaje de entrada, por lo cual a partir de conversores ac/dc o dc/dc se obtienen los diferentes valores de voltaje que necesitan los componentes electrónicos del sistema embebido.

2.4 Microcontrolador RPI.

Raspberry Pi es una computadora del tamaño de una tarjeta de crédito, de bajo costo que se conecta a un monitor de computadora o una TV y usa un mouse y teclado USB.

Hasta la fecha, existen cuatro modelos de RPI:

- Modelo A.
- Modelo B.
- Modelo B+.
- Módulo computacional.

A continuación se presenta la tabla 1, comparando los diferentes modelos y características de la RPI:

Característica	Modelo A	Modelo B	Modelo B+
Procesador	ARM1176JZF-S	ARM1176JZF-S	ARM1176JZF-S
Velocidad CPU	700Mhz	700Mhz	700Mhz
Memoria RAM	256Mb	512Mb	512Mb
Puertos USB	1	2	4
Almacenamiento	Full SD	Full SD	Micro SD
Ethernet 10/100	No	Si	Si
HDMI	Si	Si	Si
Pines	26	26	40
GPIO	17	17	26
Alimentación	300mA, 1.5W	700mA, 3.5W	650mA, 3W
Tamaño	85x56x15mm	85x56x15mm	85x56x15mm

Tabla 1: Tabla comparativa de los modelos del Raspberry Pi.

2.5 Sistemas de bases de datos.

Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior consulta.

Existen varios programas de bases de datos, denominados SGBD (por su acrónimo Sistema Gestor de Bases de Datos) que permiten almacenar datos y realizar consultas de los mismos de los datos de forma rápida y estructurada. Estos sistemas garantizan la integridad de los datos[11], mediante diferentes métodos y procesos que garantizan la administración y acceso de usuarios a los datos y garantizan el poder recuperar la información si el sistema se corrompe.

Por lo general para acceder a los datos, se lo hace mediante lenguajes de consulta que son lenguajes de alto nivel que simplifican la tarea al construir aplicaciones. Un SGBD permite el control total de acceso a los datos, asegura la

integridad de los mismos, gestiona el acceso concurrente a dichos datos, permite recuperar los datos tras un fallo del sistema y hacer backups[17] que son replicación de la base de datos en distintos nodos.

Los componentes de gestión de la base de datos son:

- Motor de la base de datos: es quien acepta las peticiones lógicas de otros subsistemas del SGB, las procesa y las convierte en su equivalente físico y accede a la DB en el lugar donde está almacenado.

- Subsistema de definición de datos: Es quien ayuda a crear, mantener y define la estructura del fichero de datos de la DB[17].

- Subsistema de manipulación de datos: Es quien ayuda a añadir, editar y borrar información de la DB al usuario, también gestiona la consulta para extraer información de la base de datos. Este subsistema[17] es la interfaz principal del usuario con la DB desde un punto de vista lógico.

- Subsistema de generación de aplicaciones: Es quien contiene las herramientas para gestionar el desarrollo de aplicaciones[17]. Por lo general contiene pantallas de entrada de datos, interfaces y lenguajes de programación.

- Subsistema de administración: Es quien ayuda a gestionar la DB con funcionalidades de almacenamiento y recuperación de datos, control de concurrencia, gestión de la seguridad y de cambios[17].

2.6 Control De Acceso.

A continuación la tabla 2 muestra todo el contenido resumido en este capítulo[4,6,7]:

Componente	Detalle
Etiqueta NFC/RFID	Las etiquetas o etiquetas se pueden clasificar en dos tipos: Activas o Pasivas Activas: Para poder transmitir su ID necesitan una fuente de alimentación externa, como una batería. Pasivas: Para energizarse, la energía la reciben de una antena. También las etiquetas NFC puede ser de sólo lectura o tanto de lectura como de escritura.
La antena	Estas antenas transmiten a través de objetos no metálicos y en los distintos rangos de frecuencias: 50 ≤ frecuencia ≤ 500[KHz] 0.9 ≤ frecuencia ≤ 2.5[GHz] 13.56 MHz 5.8 GHz
La lectora	Este componente permite energizar la tarjeta pasiva para capturar su UID, para posteriormente ser enviado al microcontrolador quien se encarga de procesar dicha información.
El microcontrolador	Este mini computador se encarga de capturar la información enviada por el lector, y procesar los datos pertenecientes al UID de la tarjeta o tag presentada en la lectora RC522.

Tabla 2 : Descripción de los componentes de un sistema de acceso.

CAPÍTULO 3

3. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE CONTROL DE ACCESO A MANERA DE PROTOTIPO.

En el capítulo actual se describirá o se detallará paso a paso el diseño e implementación del sistema de control de acceso usando una RPI y un lector RFID (ver Figura 20, descrita en el Anexo A).

Para desarrollar este prototipo, los componentes a usar son:

- 1 Router Inalámbrico N300 Linksys E900.
- 1 Laptop/Desktop.
- 2 cables UTP RJ-45.
- 1 Raspberry Pi 3, modelo B.
- 1 Tarjeta micro SD 16 GB.
- 1 Lector RFID Mifare RC522.
- 1 Bus de datos IDE.
- 8 Jumpers hembra-macho.
- 1 USB to Micro USB Cable.
- 1 Batería portable, salida 5V 2,1A.
- 1 Módulo de 4 Relay para Arduino.
- 1 Chapa eléctrica.
- 1 Puerta de aluminio de 50 cm de alto x 40 cm de ancho para mejor ilustración del funcionamiento del sistema de control de acceso.

A continuación se detallará una breve descripción de ciertos componentes usados en este prototipo:

3.1 Router inalámbrico N300 linksys E900.

El router inalámbrico es usado en este proyecto solo para crear una red LAN y conectar la Raspberry Pi a dicha red LAN, tener en cuenta que éste router debe contar con conexión a internet para poder descargar las librerías y paquetes que necesite la Raspberry Pi.

3.2 Laptop/Desktop.

Se necesita una computadora (laptop o desktop) que esté conectada (mediante cable UTP o Wireless Fidelity) a la misma red LAN especificada en el punto anterior, para poder acceder remotamente (ya sea por PUTTY, o por VNC-VIEWER) a la Raspberry Pi y poder configurarla de acuerdo a las necesidades de este proyecto.

3.3 Raspberry PI 3, modelo B.

Raspberry Pi no es una mini computadora de bajo costo solamente, sino que también puede ser configurado para ser un Servidor WEB, ya que brinda manejo de bases de datos a través de PHPMyAdmin y soporta casi cualquier distribución Linux.

Este microcontrolador es sumamente esencial para este proyecto, dentro de este microcontrolador es donde estará todo o casi todo el desarrollo de este proyecto, es aquí donde se establecerá la comunicación con el lector Mifare RC-522, donde se creará la base de datos que albergará los datos de los docentes con acceso a dicha área restringida, con el campo más importante, el Identificador Único (UID); también es mediante la Raspberry Pi que se podrá gestionar la base de datos como servidor Web mediante PHPMyAdmin.

3.4 Tarjeta micro SD 16 GB.

Este componente también es de gran importancia como el anterior, ya que en la tarjeta micro SD es donde se instalará el sistema operativo Raspbian, necesario para el funcionamiento del microcontrolador, es el disco duro de la Raspberry Pi, y es aquí donde se guardará todo el desarrollo del mismo.

3.5 Lector RFID mifare RC522.

Este componente es fabricado por NXP Semiconductors, trabaja con el estándar internacional ISO/IEC 14443, lo cual le permite ser un lector/escritor RFID/NFC en las frecuencias de 13.56 MHz a no más de 50mm, en base a esto, este componente solo es capaz de lograr las comunicaciones con tarjetas Mifare desarrolladas en el mismo estándar.

Los protocolos de comunicación que soporta este lector son tres:

- Protocolo Serial UART.
- Protocolo SPI (Serial Peripheral Interface).
- Interfaz I^2C.

De estos tres protocolos de comunicación se escogió trabajar con el protocolo SPI (Serial Peripheral Interface), ya que el microcontrolador o Raspberry Pi trabaja con SPI.

3.5.1 Etiqueta o tag NFC/RFID.

Las tarjetas o etiquetas RFID/NFC que se usarán en este proyecto usan el estándar internacional ISO/IEC 14443. El lector escogido (MFRC522) también se basa en este estándar de acuerdo al datasheet del fabricante, el cual se conoce como Identification cards – Proximity integrates circuit(s) cards, siendo el que describe los parámetros de operación de las Smart-cards o tarjetas inteligentes de proximidad sin necesidad de contacto.

- Se pueden mencionar ciertos beneficios y/o ventajas:
- Frecuencia de operación de 13.56 MHz.
- Algoritmo anticolisión.
- Transmisión de datos sin que estén conectados a una fuente de alimentación.
- Aplicación más usada: Control de Acceso.

3.6 Conexión lector mfrc522 y raspberry pi.

Una vez analizado todos los componentes del prototipo de este proyecto, es importante siempre tener en mente que el protocolo a utilizar es el SPI (Serial Peripherical Interface), las líneas de señal que utiliza dicho protocolo se detallan de la siguiente manera:

- SCLK, es una señal de reloj enviada desde el bus maestro hacia los esclavos; todas las señales SPI son sincronizadas con SCLK.
- SSn, es una señal de selección de esclavo por cada esclavo, es comúnmente por el máster para seleccionar el esclavo que se va a comunicar.
- MOSI (Master Out-Slave In) es una línea de datos desde el maestro a los esclavos.
- MISO (Master In-Slave Out) es una línea de datos desde los esclavos al maestro.

Para conectar el lector RC522 con la Raspberry Pi es necesario identificar los pines del lector, junto con la cabecera de pines j8 de la Raspberry Pi de acuerdo a la figura 3.1 , 3.2 , y a la tabla 3

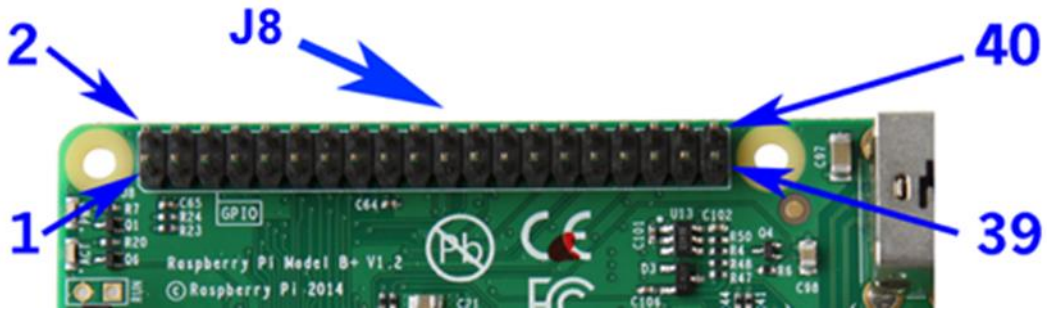


Figura 3.1: Ubicación de pines en la Raspberry Pi 3.

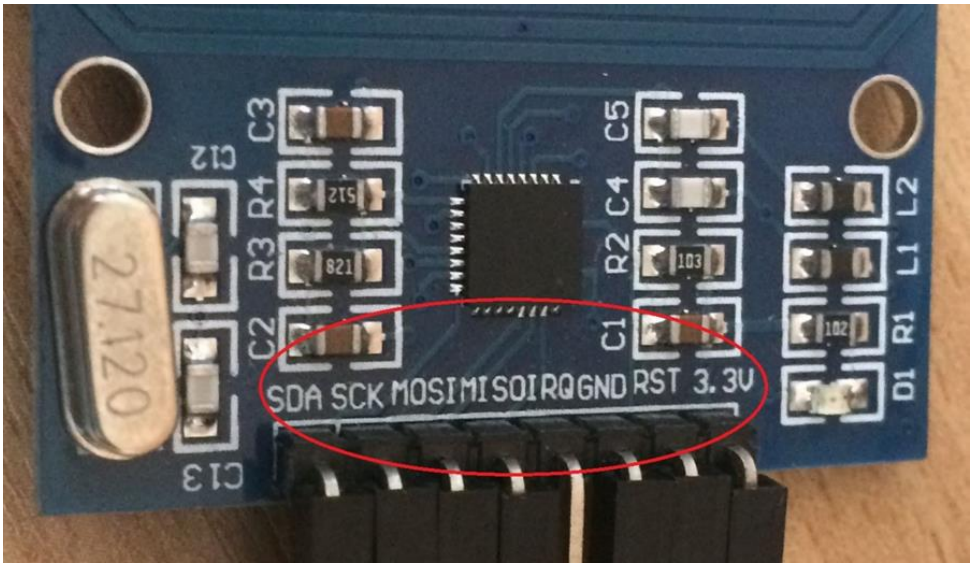


Figura 3.2: Ubicación de pines en lector RC522.

RASPBERRY PI		RC522
Nombre	Número	Nombre
GPIO 8	24	SDA
GPIO 11	23	SCK
GPIO 10	19	MOSI
GPIO 9	21	MISO
NONE	NONE	IRQ
GND	25	GND
GPIO 25		RST
3V3	1	3V3

Tabla 3: Conexión entre pines RPI y pines RC522.

CAPÍTULO 4

4. PRUEBAS Y RESULTADOS.

Una vez finalizada la fase de implementación del proyecto se procede a realizar todas las pruebas necesarias para garantizar que el sistema funcione de la manera más adecuada. A continuación, se procederá a realizar las pruebas respectivas al proyecto para determinar que los casos fueron de éxito o de fracaso, o lo que vendría a ser equivalente a los casos de acceso autorizado o no autorizado.

4.1 Escenario 1: acceso autorizado.

Este caso refleja la situación o escenario en el cual se desea acceder a un área la cual tiene asociada la etiqueta con la que se está accediendo en ese momento. Para realizar esta prueba se procederá de manera simple y sencilla a ejecutar el procedimiento almacenado asociado a este proceso llamado “registra docente”.

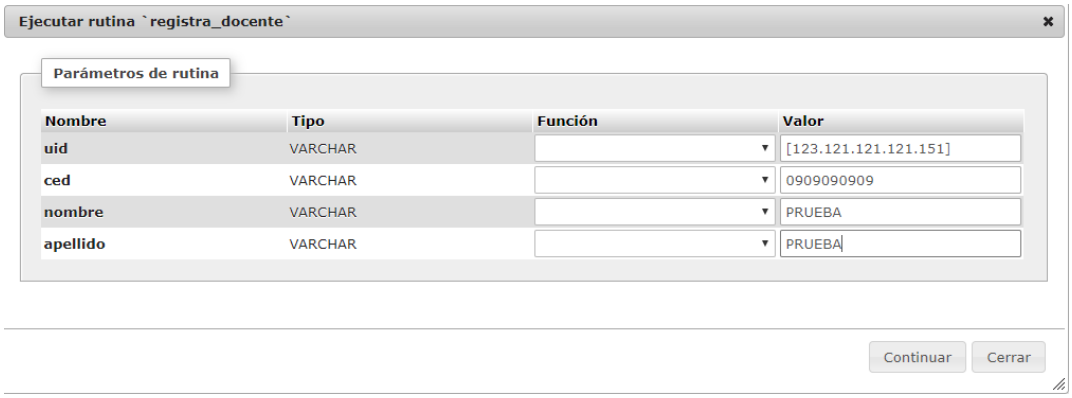


Figura 4.1: Registro de un docente en la base NFC_ACCESS.

En la figura 4.1 se puede apreciar el registro de un docente, ingresando los datos del nuevo registro.

Una vez que el docente se encuentra registrado en la base de datos de docente, se puede proceder a verificar que se encuentre registrado en la tabla de la base de datos correspondiente a los docentes.

	uid	ced	nombre	apellido	Descripción
ar	[28, 74, 198, 12, 156]	0929664845	Daniel	Santacruz	Carné ESPOL
ar	[99, 173, 212, 159, 133]	0705192623	Paola	Jordan	Carné ESPOL
ar	[234, 196, 98, 231, 171]	0929664845	Daniel	Santacruz	Metrovía
a	[123,121,121,121,151]	0930511894	Kevin	Avalos	Tag_NFC
ar	[136, 4, 16, 227, 127]	0920179017	Adriana	Collaguazo	Tag_NFC

Figura 4.2: Verificación de registro exitoso.

En la figura 4.2 se puede apreciar que el registro fue realizado correctamente.

Al haber registrado un nuevo docente en la base de datos, si se intenta acceder a alguna área con este identificador deberá permitir el acceso al área en cuestión.

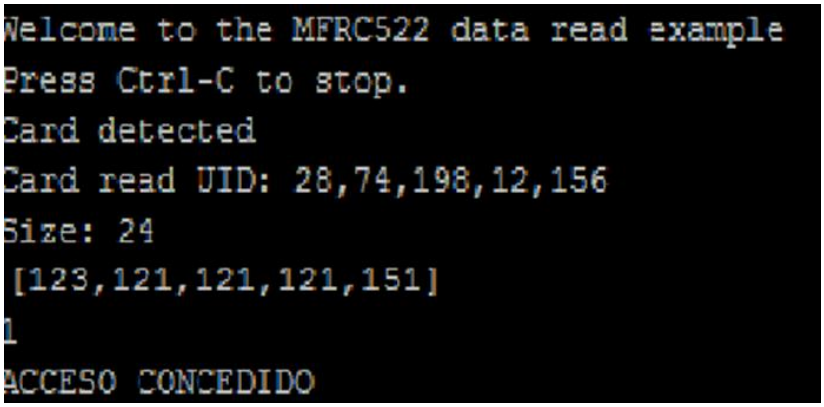


Figura 4.3: Acceso autorizado.

En la figura 4.3 se puede apreciar que dicho intento fue autorizado para ingresar de manera satisfactoria área restringida, debido que ya fue registrado previamente.

4.2 Escenario 2: acceso no autorizado.

Este caso refleja la situación o escenario en el cual se desea acceder a un área la cual no tiene asociada la etiqueta con la que se está accediendo en ese momento. Para realizar esta prueba se procederá únicamente a acercar al lector una etiqueta que no se haya registrado previamente. En la figura 4.4 se puede observar lo que sucede al intentar acceder con una etiqueta no autorizada o no registrada en la base de datos.

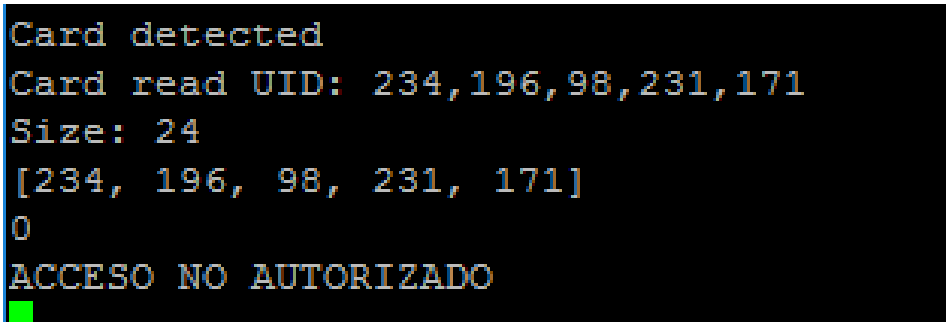


Figura 4.4: Acceso no autorizado

En la figura 4.4 se puede apreciar que dicho intento no fue autorizado para ingresar, debido a que no se encuentra en la base de datos de docentes autorizados.

4.3 Página web para consultas.

Ha sido creada y diseñado un sitio web especializado en reportes y consultas (figura B.1), está basado en tres diferentes consultas las cuáles tienen asociadas las búsquedas ya sea por apellido, por cédula o por fecha según sea el requerimiento del usuario. Adicional se permite generar un PDF para mejor presentación de los resultados.

4.3.1 Consulta por apellido.

a) Consulta apellido desde la página web.

Se procede con el ingreso del apellido a consultar, en la figura B.2 situado en el anexo B.

Se obtiene como resultado la ilustración B.3 del anexo B.

b) Archivo PDF relacionado a la consulta por apellido.

Se procede a exportar el resultado de la consulta, obteniendo el siguiente pdf ilustrado en la figura B.4 del anexo B.

4.3.2 Consulta por cédula.

a) Consulta por cédula desde la página web .

Se procede con el ingreso de la cédula a consultar, en la figura B.5 situado en el anexo B.

Se obtiene como resultado la ilustración B.6 del anexo B.

b) Archivo PDF relacionado a la consulta por cédula.

Se procede a exportar el resultado de la consulta, obteniendo el siguiente pdf ilustrado en la figura B.7 del anexo B.

4.3.3 Consulta por fecha.

a) Consulta por fecha desde la página web.

Se procede con el ingreso del rango de fechas a consultar, en la figura B.8 situado en el anexo B.

Se obtiene como resultado la ilustración B.9 del anexo B.

b) Archivo PDF relacionado a la consulta por fecha.

Se procede a exportar el resultado de la consulta, obteniendo el siguiente pdf ilustrado en la figura B.10 del anexo B.

4.3.4 Página de los autores.

En este subcapítulo se presenta una breve biografía de los autores que desarrollaron este proyecto integrador, su vida pasada y actual; así como también sus metas y aspiraciones, esta breve reseña se encuentra en la figura B.11 incluida en el anexo B de esta tesis.

CONCLUSIONES Y RECOMENDACIONES

Durante el desarrollo de este proyecto integrador se usó un sistema operativo basado en Linux, el cual es Debian, éste es un sistema operativo de código abierto (software libre), que permite hacer cambios en cualquier configuración del kernel de Linux OS, sin tener ningún tipo de restricción.

Para el desarrollo de este proyecto es importante seguir secuencialmente cada una de sus etapas: investigación, diseño, implementación y pruebas, ya que la probabilidad de éxito de cada etapa depende directamente de la etapa anterior.

Este proyecto llamado “Desarrollo de un sistema alternativo de acceso a las áreas restringidas de la FIEC mediante el uso de dispositivos móviles”, posee ciertas limitaciones, una de ellas es el dispositivo móvil a autenticarse, ya que debe de ser compatible con la tecnología del lector Mifare RC522 descrito en el datasheet del fabricante.

El microcontrolador RPI ofrece grandes ventajas para el desarrollo de este proyecto en cuanto a otros microcontroladores o mini ordenadores, una de ellas es su versatilidad para ser usado como una computadora y como servidor, ya que posee diferentes protocolos de comunicación previamente mencionados. Cabe destacar que el protocolo de comunicación por este proyecto es el SPI.

De acuerdo a la necesidad de implementar un sistema de control de acceso en la Facultad de Ingeniería en Electricidad y Computación de la Escuela Superior Politécnica del Litoral (ESPOL), se logra la construcción de un prototipo de bajo costo que permite un control de acceso con UID como método de autenticación, se implementó además un servidor web que permitirá una administración de la base de datos de los docentes que están autorizados a dicha área de una manera muy amigable, con entorno gráfico y ya no depender del entorno de consola (aunque también se deja habilitado para hacerlo por consola si el administrador de la red lo requiere).

El aprendizaje que deja el desarrollar este proyecto es poder contar con nuevas tecnologías de autenticación por medio de un UID, en un sistema

electrónico/eléctrico por medio del sensor NFC de un dispositivo móvil o por medio de etiquetas NFC o tarjetas RFID con el campo de identificación único ya grabado previamente por el fabricante sin la posibilidad de ser cambiado. Este sistema alterno es evolución directa a los códigos QR, códigos de barras que muchos sistemas con autenticación por ID funcionan actualmente.

Se establece este prototipo de control de acceso con opción a mejoras para dichos estudiantes que tomen la materia integradora o a dichos estudiantes que muestren interés en el desarrollo de proyectos eléctricos/electrónicos, en el desarrollo de aplicaciones y en el desarrollo de proyectos de este tipo que permitan satisfacer las necesidades de la facultad.

Alimentación energía eléctrica: Procurar que el voltaje esté libre de interferencias electromagnéticas y/o perturbaciones armónicas, para evitar una inducción electromagnética no deseada y la inducción de corriente en este sistema.

BIBLIOGRAFÍA

[1] M. Benantar, Access Control Systems: Security Identity Management and Trust Models, New York: Springer, 2006

[2] V. Coskum, K. Ok y B. Ozdenizci, Professional NFC Aplication Develpment for Android, Ankara: Wrox, 2013.

[3] H. Kazmi, Security and Privacy Issues in Near Field Communication (NFC) Systems: Contactless Communication in Digital World, Publishing LAP Lambert Academic, 2012.

[4] M. Changshe y J. Weng, «Radio Frequency Identification System Security,» de Criptology and Information Security Series, Amsterdam, 2013

[5] W. Stalling, Cryptography and Network Security, Prenctice Hall, 2011.

[6] [Boukraa & Ando, 2002] Mustapha Boukraa and Shigeru Ando, Tag-Based Vision: Assiting 3D Scene Analysis with Radio-Frequency tags. Proceedings of the Fifth International Conference on Information Fusion, Vol. 1, 2002, pp. 412–418.

[7] [Chae & Han, 2005] Heesung Chae, Kyuseo Han, Combination of RFID and Vision for Mobile Robot Localization. In Proceedings of the 2005 International Conference on Intelligent Sensors, Sensors Networks and Information Processing Conference, 2005, pp. 75-80, ISBN 0-7803-9399-6.

[8] [Doerr et al., 2006] Kenneth H. Doerr, William R. Gates, John E. Mutty, A hybrid approach to the valuation of RFID/MEMS technology applied to ordnance inventory. In Int. J. Production Economics 103 (2006) 726–741.

[9] [Goodrum et al., 2006] Paul M. Goodrum, Matt A. McLaren, Adam Durfee, The application of active radio frequency identification technology for tool tracking on construction job sites. In Automation in Construction 15 (2006) 292 – 302.

[10] [Hähnel et al., 2003] D. Hähnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose, Mapping and Localization with RFID Technology, Technical Report IRS-TR-03-014, December 2003, Intel Research Institute, Seattle, WA.

[11] [Hontani et al., 2003] H. Hontani, K. Baba, T. Kugimiya, K. Sato y M. Nakagawa, Visual Tracking System using an ID- Tag and the Network. In Proceedings of SICE Annual Conference in Fukui, Japón, 4-6 Agosto, 2003.

[12] [Knight, 2006] William Knight, RFID – another technology, another security mess? Infosecurity Today, Volume 3, Issue 3, May-June 2006, Pages 35-37.

[13] [Korhonen et al., 2003] I. Korhonen, J. Parkka, and M. van Gils, Health monitoring in the home of the future, IEEE Eng. Med. Biol. Mag., vol. 22, no. 3, pp. 66–73, May/June 2003.

[14] [Kulyukin et al., 2005] Kulyukin, V.; Gharpure, C.; and Nicholson, J. 2005. Robocart: Toward robot-assisted navigation of grocery stores by the visually impaired. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). IEEE/RSJ.

[15] [Mamei & Zambonelli, 2005] M. Mamei, F. Zambonelli, Spreading Pheromones in Everyday Environments Through RFID Technology, IEEE Symposium on Swarm Intelligence, IEEE Press, pp. 281-288, June 2005

[16] [Roberts, 2006] Roberts, C.M., Radio frequency identification (RFID). Computers & Security, 25 (1). pp. 18-26. ISSN 0167-4048 (2006).

[17] [Ross, 2001] D. A. Ross, Implementing assistive technology on wearable computer orientation system, IEEE Intelligent Systems, May-June: 2-8, 2001.

[18] [Ross & Blasco, 2002] D. A. Ross and B. B. Blasch, Development of a wearable computer orientation system, IEEE Conference on Advanced Robotics, June-July 2003, Coimbra, Portugal.

[19] Ubitap.com. (n.d.). About NFC · Ubitap NFC.[online] Available at: https://ubitap.com/whatisnfc[Accessed 25 Jun. 2017].

[20] [Takemura et al., 2004] K. Takemura, K. Ohara, K. Ohba, N. Y. Chong, S. Iría, and K. Tanie, Knowledge distributed tag-based vision system. In Proceedings of 2004 Int. Workshop on Networked Sensing Systems, 2004, pp. 179-182.

ANEXOS

ANEXO A: DIAGRAMA ESQUEMÁTICO DEL SISTEMA DE CONTROL DE ACCESO USADO.

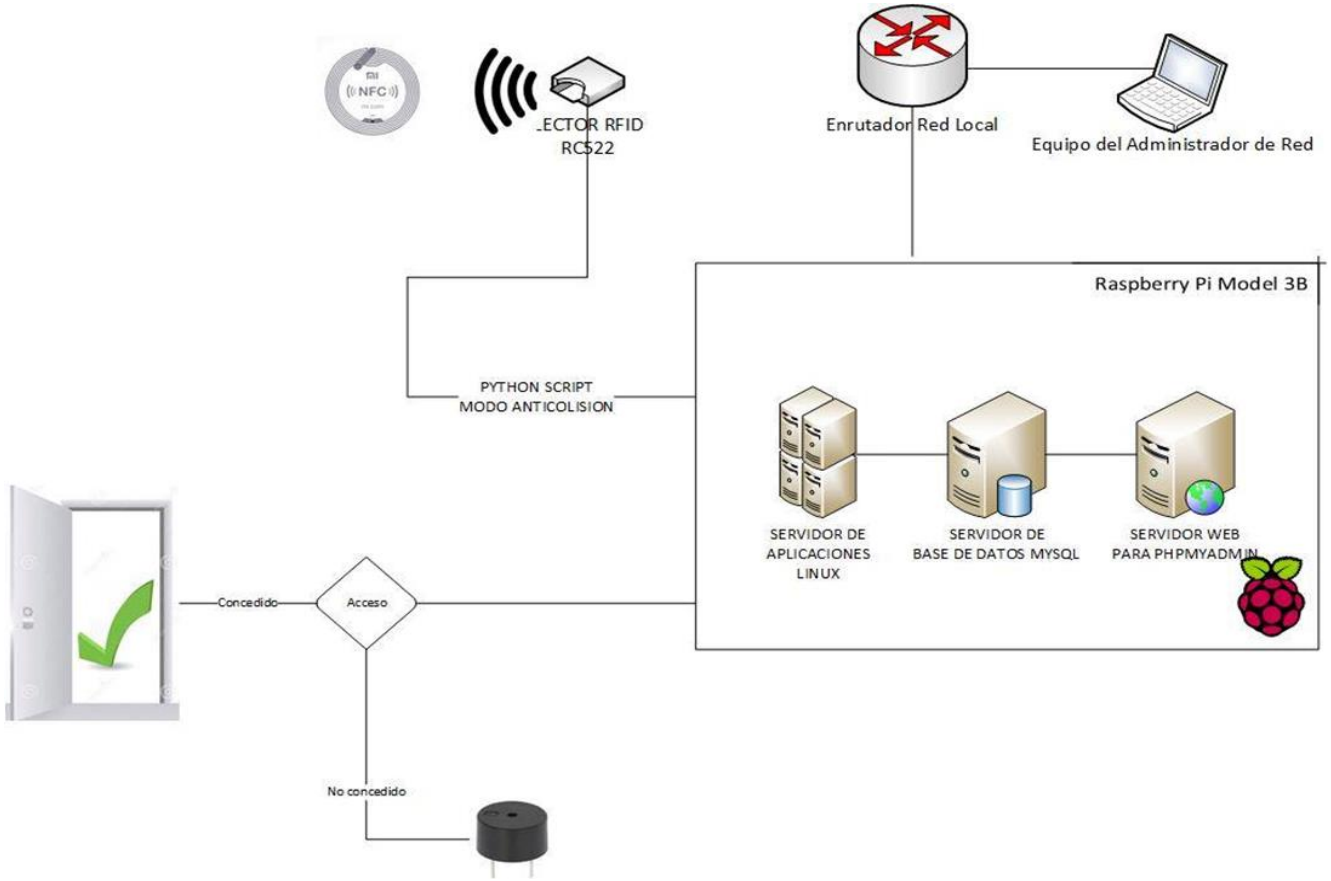


Figura A.1: Diagrama esquemático del sistema de control de acceso

ANEXO B: PÁGINA WEB PARA CONSULTAS.

Figura B.1: Página web para consultas.

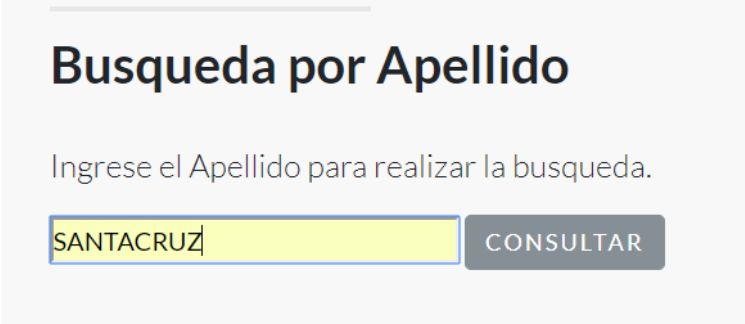


Figura B.2: Búsqueda por Apellido

Consulta por Apellido:
Apellido: SANTACRUZ

Apellido	Nombre	Cedula	UID	Descripcion
Santacruz	Daniel	0929664845	[234, 196, 98, 231, 171]	Metrovía
Santacruz	Daniel	0929664845	[28, 74, 198, 12, 156]	Carné ESPOL

Figura B.3: Consulta por Apellido

REPORTE POR APELLIDO

Apellido: SANTACRUZ

Fecha y Hora: 02-09-2017 19:56:17 PM

Apellido	Nombre	Cedula	UID	Descripcion
Santacruz	*Daniel*	*0929664845*	*[234, 196, 98, 231, 171]*	*MetrovÃ-a*
Santacruz	*Daniel*	*0929664845*	*[28, 74, 198, 12, 156]*	*CarnÃ© ESPOL*

Figura B.4: Reporte por Apellido

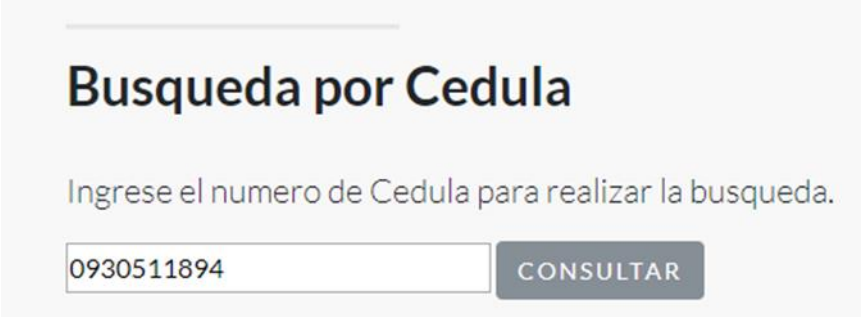


Figura B.5: Búsqueda por cédula

Se obtiene como resultado:

Figura B.6: Consulta por Cédula

REPORTE POR CEDULA

Numero: 0930511894

Fecha y Hora: 02-09-2017 19:57:54 PM

Cedula	Nombre	Apellido	UID	Descripcion
0930511894	*Kevin*	*Avalos*	*[123.121.121.121.151]*	*Tag_NFC*

Figura B.7: Reporte por Cédula

Figura B.8: Búsqueda por fecha

Consulta por Fecha:
Desde: 2017-08-01 Hasta: 2017-09-10

Fecha	Cedula	Nombre	Apellido	UID	Descripcion
2017-08-10 03:07:31	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	Metrovía
2017-08-10 03:07:35	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	Metrovía
2017-08-10 03:07:38	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	Metrovía
2017-08-10 03:10:29	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	Metrovía
2017-08-10 03:10:36	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	Metrovía
2017-08-10 03:07:54	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	Carné ESPOL
2017-08-10 03:07:57	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	Carné ESPOL
2017-08-10 03:10:32	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	Carné ESPOL
2017-08-10 03:10:40	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	Carné ESPOL
2017-08-10 03:23:24	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	Carné ESPOL
2017-08-10 03:23:43	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	Carné ESPOL

Figura B.9: Consulta por Fecha

REPORTE POR FECHA

Desde: 2017-08-01 Hasta: 2017-09-10

Fecha y Hora: 02-09-2017 20:01:25 PM

Fecha y Hora	Cedula	Nombre	Apellido	UID	Descripcion
2017-08-10 03:07:31	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	MetrovÃ-a
2017-08-10 03:07:35	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	MetrovÃ-a
2017-08-10 03:07:38	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	MetrovÃ-a
2017-08-10 03:10:29	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	MetrovÃ-a
2017-08-10 03:10:36	0929664845	Daniel	Santacruz	[234, 196, 98, 231, 171]	MetrovÃ-a
2017-08-10 03:07:54	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	CarnÃ© ESPOL
2017-08-10 03:07:57	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	CarnÃ© ESPOL
2017-08-10 03:10:32	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	CarnÃ© ESPOL
2017-08-10 03:10:40	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	CarnÃ© ESPOL
2017-08-10 03:23:24	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	CarnÃ© ESPOL
2017-08-10 03:23:43	0929664845	Daniel	Santacruz	[28, 74, 198, 12, 156]	CarnÃ© ESPOL

Figura B.10: Reporte por Fecha

Daniel Santacruz

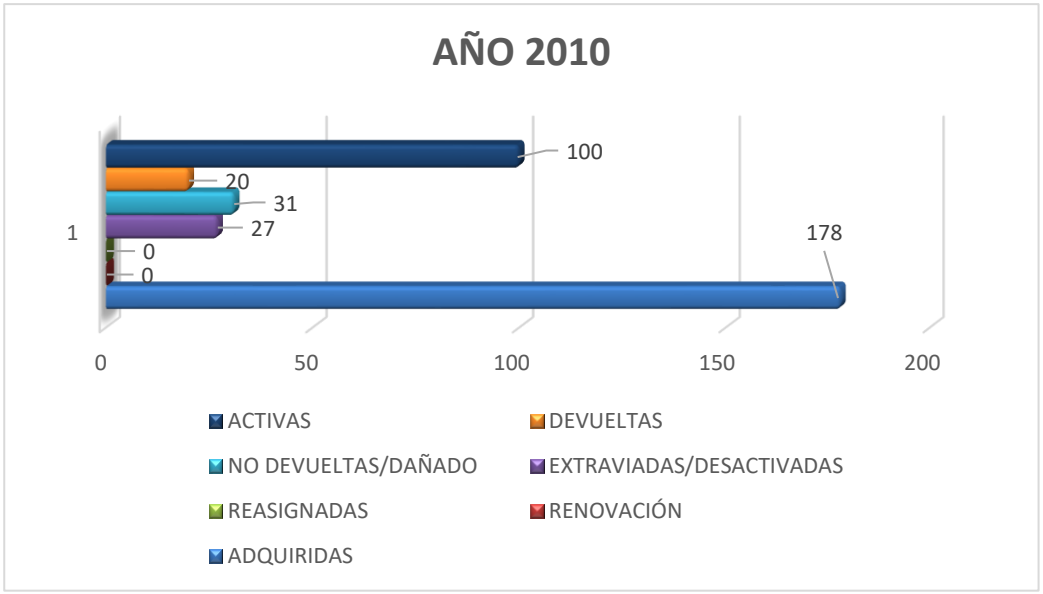
Daniel Ricardo Santacruz Alvarez nació el 26 de octubre de 1990 en la ciudad de Guayaquil-Ecuador. Actualmente está cursando la materia integradora de Telemática en la Escuela Superior Politécnica del Litoral, siendo ya esta la última materia de la carrera previo a la graduación. Fue miembro de la IEEE en el año 2015 y en la actualidad es técnico de en el departamento de HelpDesk en la empresa Telconet.

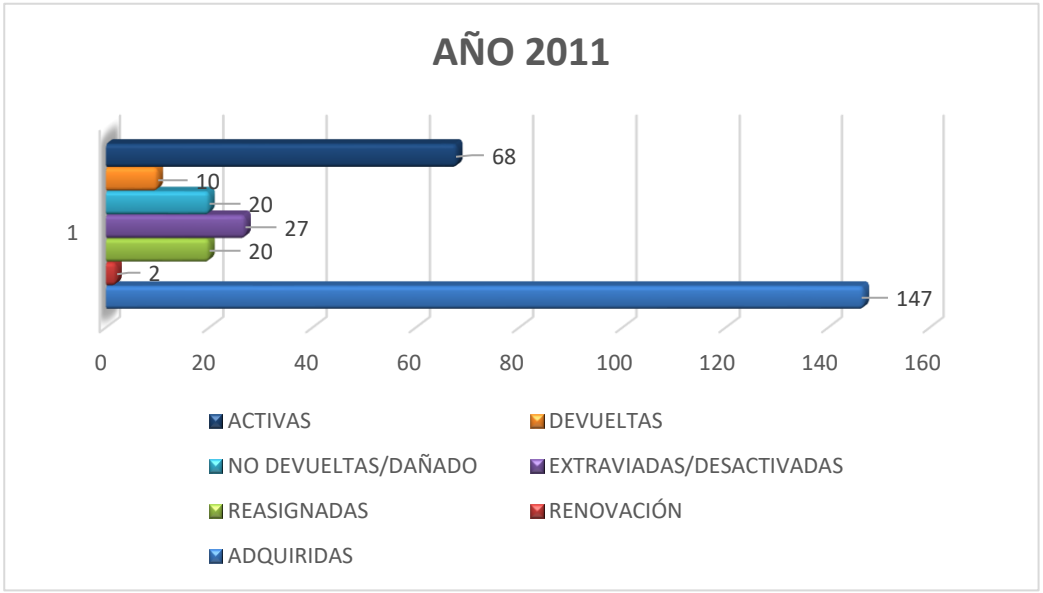
Kevin Avalos

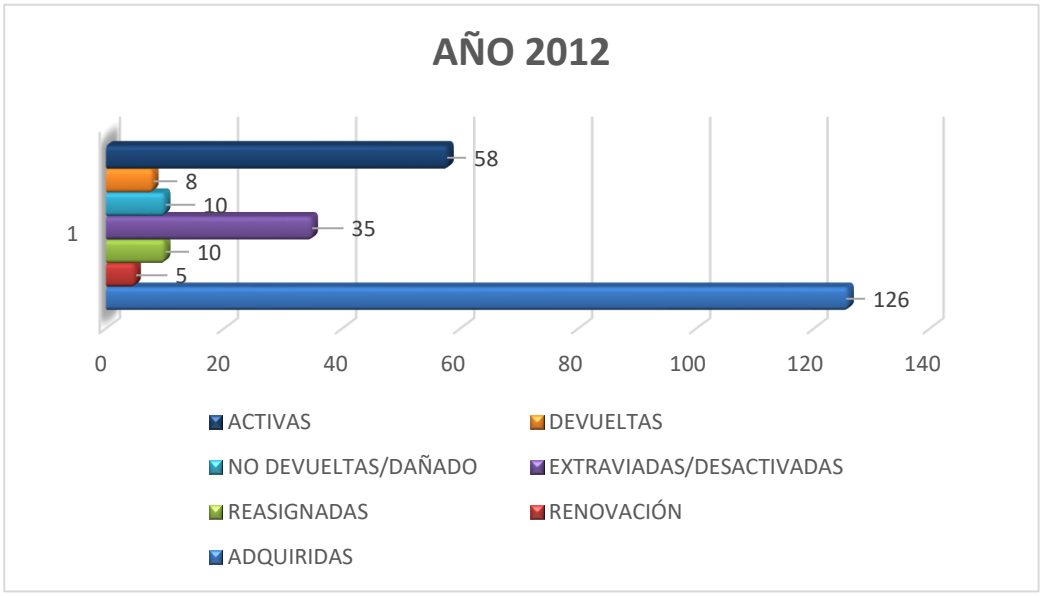
Kevin Xavier Avalos Eduarte nació el 9 de octubre de 1992 en la ciudad de Guayaquil-Ecuador. Actualmente está cursando la materia integradora de Telemática en la Escuela Superior Politécnica del Litoral, siendo ya esta la última materia de la carrera previo a la graduación. Fue miembro de la IEEE en el año 2016 y en la actualidad es Coordinador en el departamento de CDO en la empresa Unilever Andina gestionando bases de datos relacionales y generando reportes para el uso de la empresa.

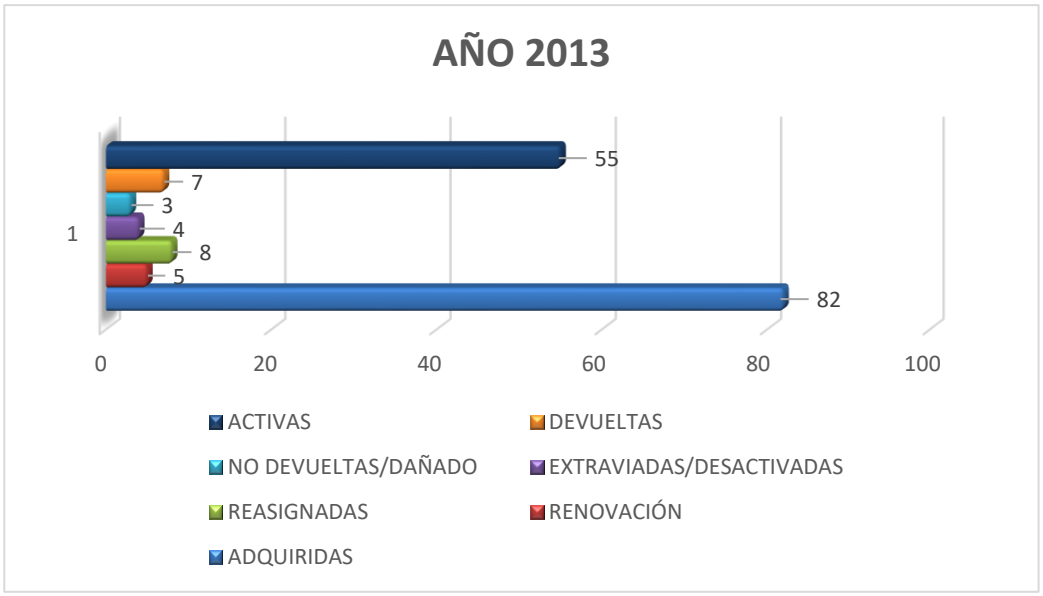
Figura B.11: Breve biografía de los autores.

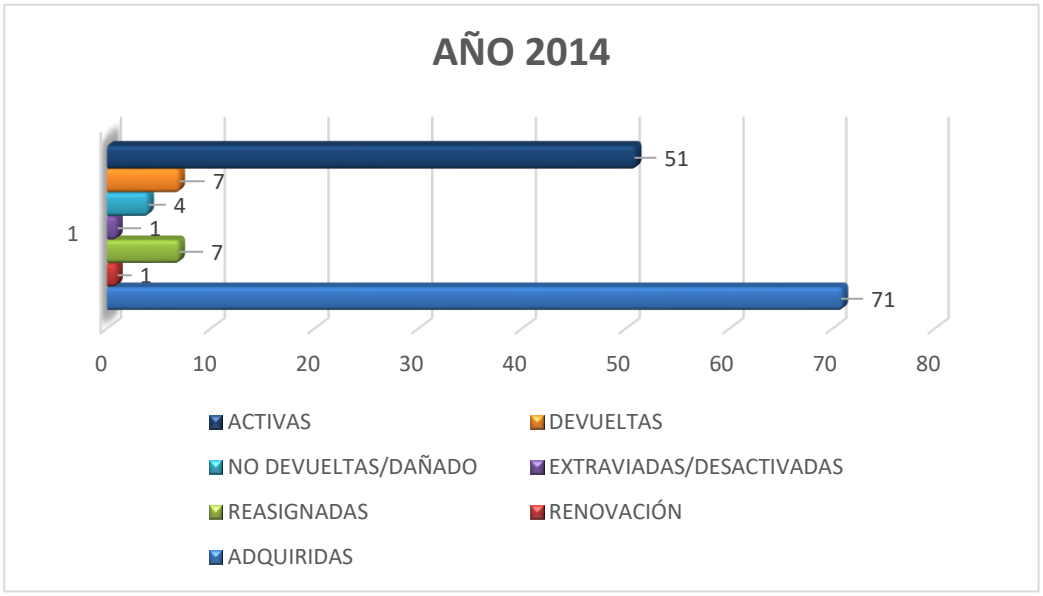
ANEXO C: REPORTE DE TARJETAS ANUAL DEL SISTEMA DE CONTROL DE ACCESO YA EXISTENTE EN LA FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN.

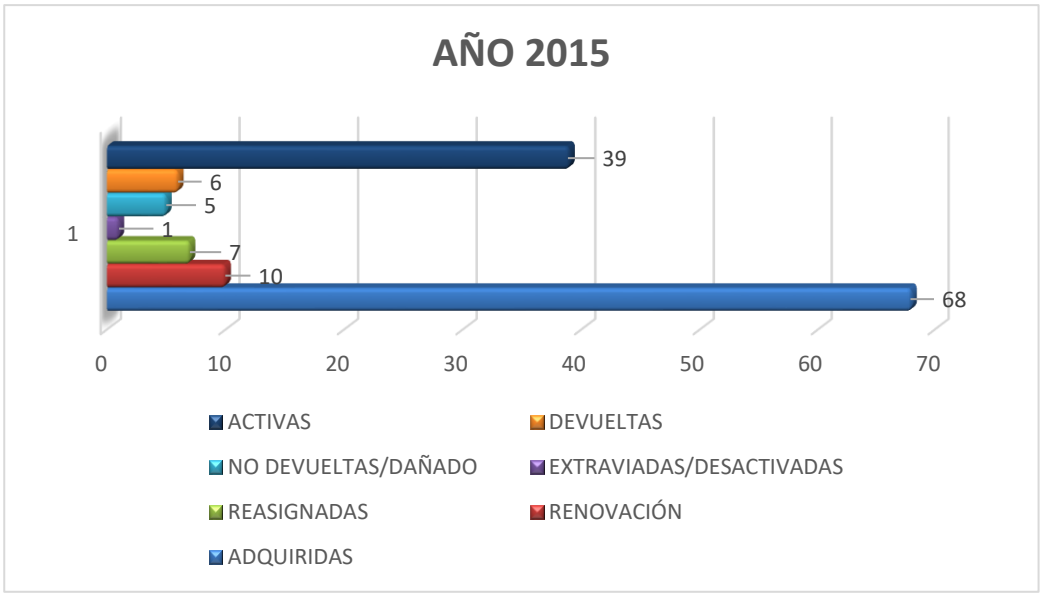


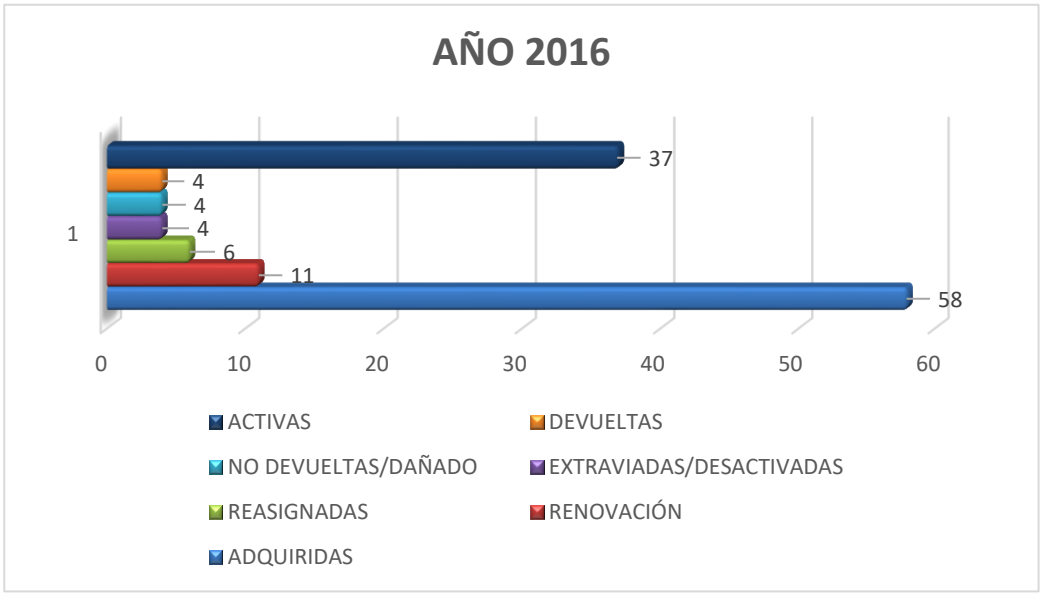


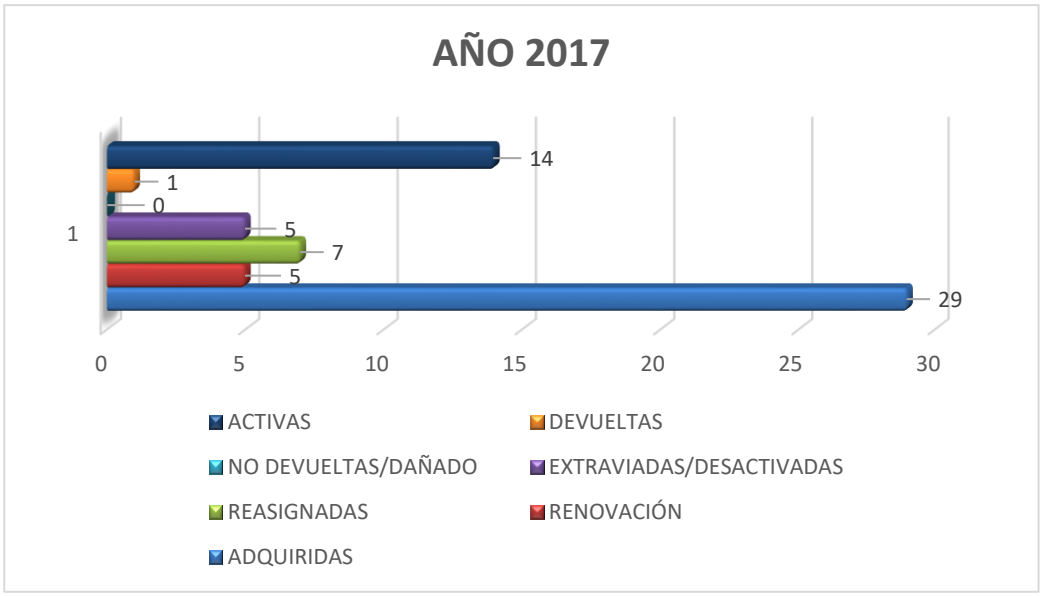

AÑO 2012
58
8
10
35
10
5
126
1
0
20
40
60
80
100
120
140
ACTIVAS
DEVUELTAS
NO DEVUELTAS/DAÑADO
EXTRAVIADAS/DESACTIVADAS
REASIGNADAS
RENOVACIÓN
ADQUIRIDAS


AÑO 2013
55
7
3
4
8
5
82
1
0
20
40
60
80
100
ACTIVAS
DEVUELTAS
NO DEVUELTAS/DAÑADO
EXTRAVIADAS/DESACTIVADAS
REASIGNADAS
RENOVACIÓN
ADQUIRIDAS


AÑO 2014
51
7
4
1
7
1
71
0
10
20
30
40
50
60
70
80
ACTIVAS
DEVUELTAS
NO DEVUELTAS/DAÑADO
EXTRAVIADAS/DESACTIVADAS
REASIGNADAS
RENOVACIÓN
ADQUIRIDAS


AÑO 2015
39
6
5
1
7
10
68
0
10
20
30
40
50
60
70
ACTIVAS
DEVUELTAS
NO DEVUELTAS/DAÑADO
EXTRAVIADAS/DESACTIVADAS
REASIGNADAS
RENOVACIÓN
ADQUIRIDAS


AÑO 2016
37
4
4
4
6
11
58
1
0
10
20
30
40
50
60
ACTIVAS
DEVUELTAS
NO DEVUELTAS/DAÑADO
EXTRAVIADAS/DESACTIVADAS
REASIGNADAS
RENOVACIÓN
ADQUIRIDAS

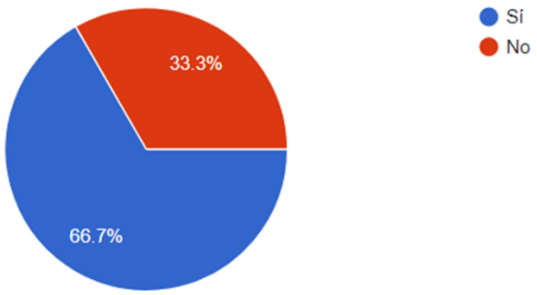

AÑO 2017
14
1
0
5
7
5
29
1
0
5
10
15
20
25
30
ACTIVAS
DEVUELTAS
NO DEVUELTAS/DAÑADO
EXTRAVIADAS/DESACTIVADAS
REASIGNADAS
RENOVACIÓN
ADQUIRIDAS

ANEXO D: RESULTADOS DE LA ENCUESTA EN LÍNEA A LOS DOCENTES DE LA FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN.

De 12 docentes que realizaron la respectiva encuesta, se obtienen los siguientes resultados:

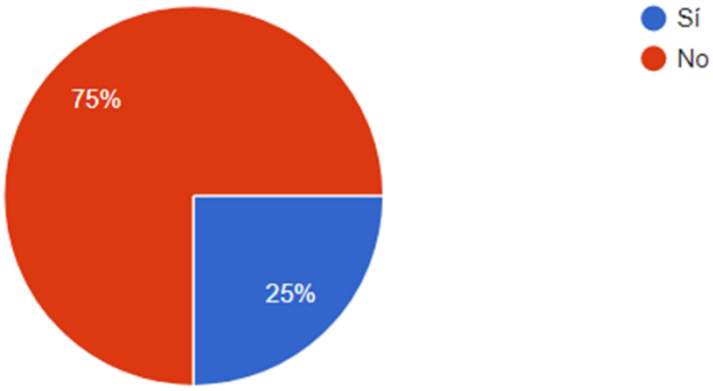
¿Usa usted tarjetas (de proximidad o magnéticas) para el ingreso a las áreas restringidas?

12 respuestas



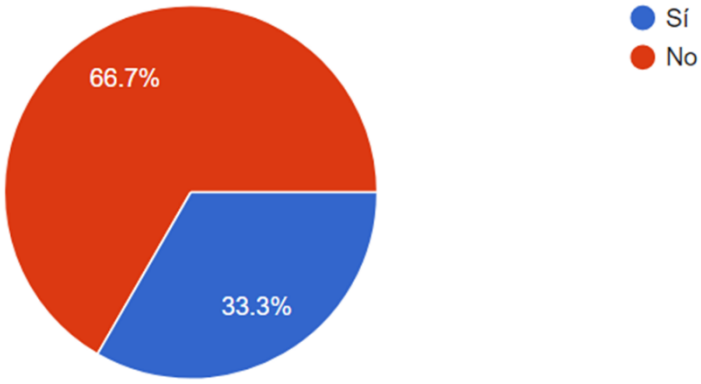
¿Alguna vez se le ha perdido su tarjeta de ingreso?

8 respuestas



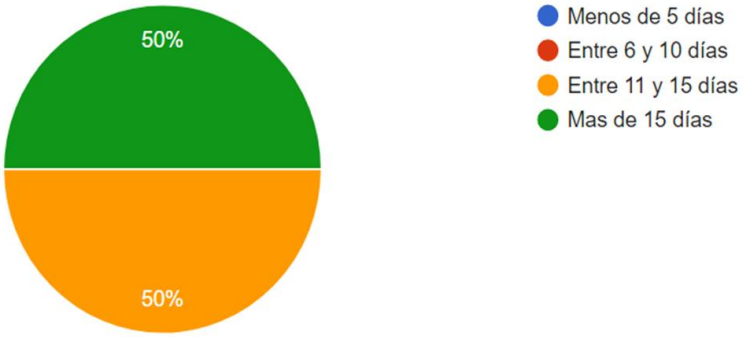
¿Alguna vez se le ha olvidado su tarjeta de ingreso?

6 respuestas



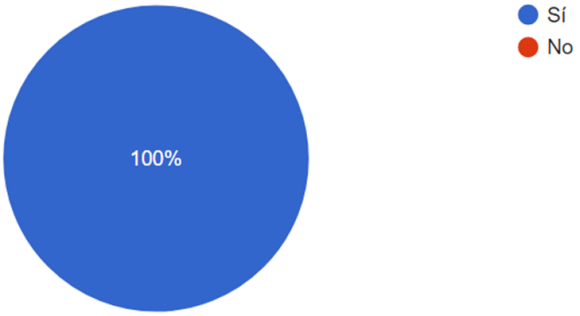
¿Cuánto tiempo le ha tocado esperar para la reposición de su tarjeta?

2 respuestas



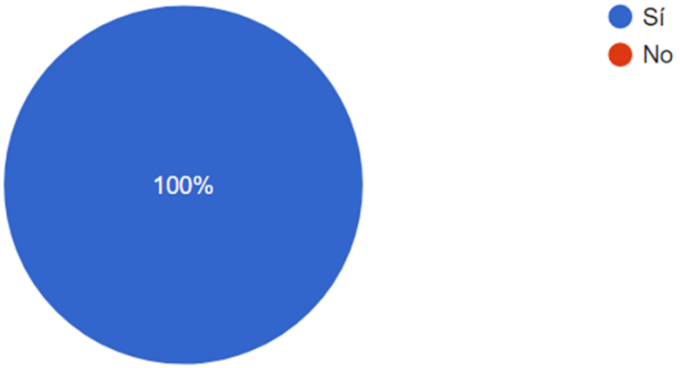
¿Le gustaría contar con una vía alternativa (adicional a la existente) de ingreso a las áreas restringidas?

12 respuestas



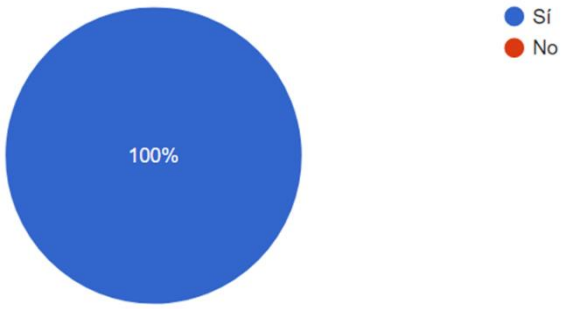
¿Cuenta usted con un teléfono inteligente?

12 respuestas



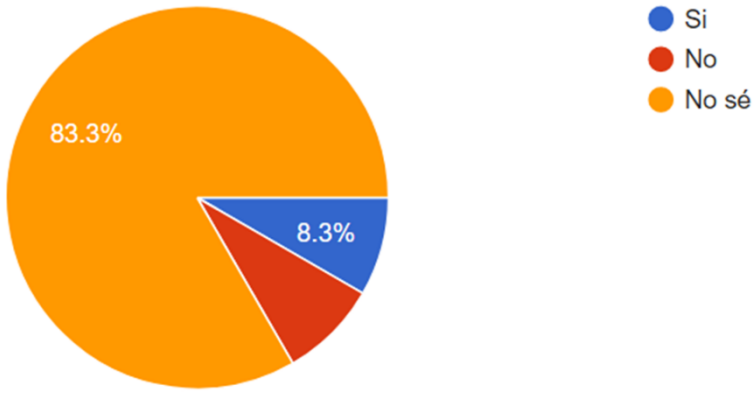
¿Le gustaría usar su teléfono inteligente para poder ingresar a las áreas restringidas?

12 respuestas



¿Su dispositivo celular cuenta con sensor NFC?

12 respuestas



Por favor ingrese la marca y su modelo de celular

10 respuestas

Samsung galaxy s4 mini
Samsung
Samsung S5
samsung j5
samsung
Sony Xperia Z3
Samsung
Samsug DUOS
samsung Galaxy Grand Prime
Samsung galaxi s3 mini