DISEÑO DE CONTROL DE ACCESO INTEGRADO A LA RED LAN DE LA EMPRESA QUIMISERVI SAS IMPLEMENTADO SOBRE RASPBERRY

CARLOS FERNANDO BARRERA MORENO

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS FACULTAD DE INGENIERIA
PROYECTO CURRICULAR DE INGENIERIA ELECTRÓNICA
COLOMBIA, BOGOTÁ
2017

DISEÑO DE CONTROL DE ACCESO INTEGRADO A LA RED LAN DE LA EMPRESA QUIMISERVI SAS IMPLEMENTADO SOBRE RASPBERRY

PROPONENTE:

CARLOS FERNANDO BARRERA MORENO

DIRECTOR:
JULIAN ROLANDO CAMARGO LÓPEZ

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS FACULTAD DE INGENIERIA
PROYECTO CURRICULAR DE INGENIERIA ELECTRÓNICA
COLOMBIA, BOGOTÁ
2017

TABLA DE CONTENIDO

Contenido

TABLA DE CONTENIDO 3

INTRODUCCIÓN 1

1. RESUMEN EJECUTIVO 2

1.1. PROPUESTA DE PASANTÍA 2

1.2. TITULO DE LA PASANTÍA 2

1.3. PLANTEAMIENTO DEL PROBLEMA 2

2. OBJETIVOS: 3

2.1. GENERAL 3

2.2. ESPECÍFICOS 3

3. JUSTIFICACIÓN 4

4. ALCANCE Y LIMITACIONES 5

4.1. ALCANCE 5

4.2. LIMITACIONES 5

5. COSTOS APROXIMADOS 6

6. PLAN DE TRABAJO 7

7. RESULTADOS ESPERADOS 8

8. CRONOGRAMA 9

9. MARCO TEORICO 10

10. DISEÑO E IMPLEMENTACION 22

11. RESULTADOS OBTENIDOS 34

12. IMPACTO DEL TRABAJO DE GRADO 38

13. EVALUACION Y CUMPLIMIENTO DE LOS OBJETIVOS DE LA PASANTIA 39

14. CONCLUSIONES 40

BIBLIOGRAFIA 41

ANEXOS 42

INTRODUCCIÓN

En la actualidad la seguridad electrónica se ha posicionado como una necesidad a nivel doméstico e industrial, enfocados en la empresa, la seguridad electrónica brinda la oportunidad de tener control sobre los datos sensibles y el uso de los recursos de la empresa.

Por esta razón la ingeniería electrónica debe abrir los medios para diseñar soluciones acordes a las necesidades específicas de cada empresa.

Un sistema de control de acceso es un sistema inteligente que permite la integración de tecnologías de identificación biométrica, de tarjetas RF o de teclados matriciales, con el fin de permitir o denegar accesos a diferentes zonas de la compañía, y también permite llevar un seguimiento de horas de llegada/salida y hasta uso de los recursos.

1. RESUMEN EJECUTIVO

1.1. PROPUESTA DE PASANTÍA

El presente documento pretende definir el trabajo a desarrollar durante la pasantía a realizarse en la empresa QUIMISERVI SAS. A cargo del estudiante CARLOS FERNANDO BARRERA MORENO y bajo la dirección académica del Ingeniero JULIAN ROLANDO CAMARGO LÓPEZ y la dirección externa de la Ingeniera ANDREA DEL PILAR PARDO PINEDA, el cargo que desempeñará el estudiante en la empresa es el de diseñador de soluciones de seguridad electrónica, con el fin de enfocarse en el diseño del control de acceso de la empresa para asi obtener un documento con el soporte correspondiente a la integración de un sistema de control de acceso que se conecte a la red LAN de la empresa.

1.2. TITULO DE LA PASANTÍA

"Diseño de control de acceso integrado a la red LAN de la empresa Quimiservi SAS implementado sobre raspberry"

1.3. PLANTEAMIENTO DEL PROBLEMA

La seguridad electrónica representa no solo un ahorro de recursos dentro de una empresa, sino también una forma de control sobre las actividades de los empleados, pero los sistemas de control de accesos que se encuentran disponibles en el mercado tienen un alto costo o son poco flexibles.

Esta propuesta va encaminada a elaborar e implementar el diseño de un sistema de control de acceso con reconocimiento de tarjetas RF, que permita ser integrado y administrado a través de la red LAN de la empresa y que este montado sobre raspberry, a partir de los conocimientos adquiridos en las aulas de clase, generando una solución adaptada a las necesidades particulares de esta empresa.

2. OBJETIVOS:

2.1. GENERAL

Diseñar e implementar un sistema de control de acceso con reconocimiento de tarjetas RF, que permita ser integrado a la red LAN de la empresa Quimiservi SAS y que este montado sobre raspberry.

2.2. ESPECÍFICOS

- Estudiar y analizar las tecnologías disponibles en el mercado para tomar como base las mejores características de cada una.
- Desarrollar una solución de hardware integrando las características seleccionadas sobre la plataforma raspberry e integrarla a la red LAN de la empresa.
- Definir una solución de software que permita almacenar en una base de datos los intentos de acceso que se realizan para después generar un informe para la empresa.
- Comprobar el buen funcionamiento de la solución desarrollada y validar los datos obtenidos.

3. JUSTIFICACIÓN

Mediante los informes generados por este control de accesos la empresa Quimiservi SAS podrá revisar el cumplimiento de sus empleados lo que permitirá encontrar fallos operativos y económicos dentro de ella.

Contar con éste soporte, permitirá agilizar el proceso de diseño de futuras soluciones de control de acceso, pues se tendrá como base un programa que podrá adaptarse a los diferentes criterios encontrados.

El desarrollo del proyecto permite aplicar los conocimientos técnicos adquiridos en las áreas de telemática, programación, electrónica digital y electrónica, para a partir de éstos, integrar de la mejor manera las soluciones tecnológicas seleccionadas.

4. ALCANCE Y LIMITACIONES

4.1. ALCANCE

Durante esta pasantía se pretende diseñar e implementar la solución más adecuada de un sistema de control de acceso con reconocimiento de tarjetas RF, que permita integrarse a la red LAN de la empresa. Al final de la pasantía se entregará un documento que contenga el registro de los procedimientos realizados para el diseño y el proceso de implementación y un manual de guía rápida para el usuario.

4.2. LIMITACIONES

Se pretende entregar un documento con procesos de diseño, selección de tecnología e implementación.

Se soportará el trabajo realizado mediante registros fotográficos que demuestren la instalación de la solución diseñada.

5. COSTOS APROXIMADOS

Durante el desarrollo de la pasantía se tendrá el apoyo de la empresa en cuanto a costos.

Los costos aproximados se describen a continuación:

Costos Personal

	Valor Unitario	Cantidad	Total
Hora director interno	$120.000	16	$1.920.000
Hora director externo	$50.000	16	$800.000
Hora estudiante	$10.000	384	$3.840.000
		Total Costos Personal	$6.560.000

Costos materiales

	Valor Unitario	Cantidad	Total
Raspberry	$120.000	1	$120.000
Lector RC522	$35.000	1	$35.000
Cantonera eléctrica	$80.000	1	$80.000
Costos operativos por semana	$50.000	8	$400.000
		Total Costos Materiales	$635.000

Total proyecto: $7.195.000

6. PLAN DE TRABAJO

Lo pertinente al desarrollo de esta pasantía, se enumera por etapas:

- En una etapa inicial se estudiarán los problemas que se presentan en la empresa respecto al control de acceso por el impacto económico que esto genera.

- La siguiente etapa busca evaluar la tecnología actual sobre todo en el campo de software libre, definir características y ventajas.

- En la tercera etapa se pretende diseñar los sistemas de control de acceso, los diagramas de conexión, las características de los equipos y el modo de operación de acuerdo a los requerimientos de la empresa (tipo de bloqueo de los ingresos, cantidad de usuarios, etc.).

- La cuarta etapa será la etapa de diseño del software y la conexión a la red LAN de la empresa basado en el estudio de necesidades y tecnología al alcance.

- La siguiente etapa, consistirá en llevar a cabo las pruebas de los equipos y puesta a punto del sistema.

- Por último se debe reunir la información y los resultados obtenidos para luego organizarlos en un documento entregable que será el resultado de la pasantía.

7. RESULTADOS ESPERADOS

La empresa Quimiservi SAS espera tener una mejor organización dentro de sus instalaciones gracias a este sistema de control, pues se podrán registrar los accesos a zonas no permitidas y los incumplimientos con el horario de los trabajadores, lo cual tendrá un impacto económico positivo.

Con el desarrollo de esta pasantía se espera obtener experiencia en el campo, y dar los primeros pasos hacia el mercado laboral, desarrollando una solución apropiada a los problemas que se enfrenten en el día a día de la empresa.

Luego de la ejecución de la pasantía, se espera confirmar que los conocimientos adquiridos en la universidad, se pueden llevar a la práctica y son totalmente acordes con los retos que actualmente se presentan para los ingenieros electrónicos en el mercado actual.

Se busca obtener una solución para los problemas planteados que sea económica y eficiente y un referente, para futuros diseños de sistemas de control de acceso.

8. CRONOGRAMA

Objetivo	Actividad	Semanas										
		1	2	3	4	5	6	7	8	9	10	11
Estudiar los problemas que se presentaban en la empresa, y seleccionar el que genere mayor impacto.	Observación	X										
	Estudio de los problemas	X										
	Selección	X										
Estudiar las tecnologías libres disponibles y analizar sus características para así escoger la mejor opción de desarrollo.	Recopilación de fuentes	X										
	Estudio de las tecnologías		X									
	Análisis de las características		X									
Diseñar los sistemas de control de acceso, los diagramas de conexión, las características de los equipos y el modo de operación.	Comprobación de características		X									
	Diseño de la solución			X	X	X						
	Procesos técnicos						X					
Desarrollo de la interfaz	Conexión a la red						X					
	Desarrollo del software de interfaz						X					
Prueba de equipos y adquisición de datos de funcionamiento	Puesta en funcionamiento							X				
	Pruebas finales							X				
	Adquisición de datos								X			
Creación del documento entregable a la universidad	Organización de datos								X			
	Entrega final								X			

Tabla 1. Cronograma

9. MARCO TEORICO

9.1. CONTROL DE ACCESO

El control de acceso consiste en un mecanismo que permite verificar la identidad de un usuario con el fin de autorizar el ingreso o acceso a recursos físicos.

Determinar el acceso a dichos recursos es fundamental, ya que permite que su manejo responda a las finalidades con que fueron destinados; para la implementación de esto, se identifican tres componentes:

- **Mecanismo de autenticación:** Puede ser una clave, lector biométrico, mapa o contraseña.
- **Mecanismo de autorización:** Tras la autenticación es la que permite o no el acceso.
- **Mecanismo de trazabilidad:** Complementa el mecanismo de autorización en los casos que este puede fallar.

La definición más generalizada de un **sistema de control de acceso** hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos.

Claro está, que la definición que nos interesa debe estar dada en términos de seguridad electrónica:

Un **sistema de control de acceso** es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tags de próximidad o biometría) y a su vez controlando el recurso (puerta, torniquete o talanquera) por medio de un dispositivo eléctrico como un electroimán, cantonera, pestillo o motor.

Básicamente los controles de acceso se clasifican en dos tipos:

- Sistemas de Control de Acceso Autónomos
- Sistemas de Control de Acceso en Red

Los **Sistemas de Control de Acceso Autónomos** son sistemas que permiten controlar una o más puertas, sin estar conectados a un PC o un sistema central, por lo tanto, no guardan registro de eventos. Aunque esta es la principal limitante, algunos controles de acceso autónomos tampoco pueden limitar el acceso por horarios o por grupos de puertas, esto depende de la robustez de la marca. Es decir, los más sencillos solo usan el método de identificación (ya sea clave, proximidad o biometría) como una "llave" electrónica.

Los **Sistemas de Control de Acceso en Red** son sistemas que se integran a través de un PC local o remoto, donde se hace uso de un software de control que permite llevar un registro de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. Van desde aplicaciones sencillas hasta sistemas muy complejos y sofisticados según se requiera.

9.2. BIOMETRIA

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos.

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. Biometría es el conjunto de características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad del individuo, lo cual incluye huellas digitales, reconocimiento del iris, geometría de la mano, reconocimiento visual y otras técnicas. La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana.

9.2.1. Funcionamiento de un sistema biométrico

Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad.

La tecnología biométrica se basa en la comprobación científica de que existen elementos en las estructuras vivientes que son únicos e irrepetibles para cada individuo, de tal forma que, dichos elementos se constituyen en la única alternativa, técnicamente viable, para identificar positivamente a una persona sin necesidad de recurrir a firmas, passwords, pin numbers, códigos u otros que sean susceptibles de ser transferidos, sustraídos, descifrados o falsificados con fines fraudulentos.

La identificación biométrica es utilizada para verificar la identidad de una persona midiendo digitalmente determinados rasgos de alguna característica física y comparando esas medidas con aquéllas de la misma persona guardadas en archivo en una base de datos o algunas veces en una tarjeta inteligente que lleva consigo

la misma persona. Las características físicas utilizadas son huellas digitales, huellas de la voz, geometría de la mano, el dibujo de las venas en la articulación de la mano y en la retina del ojo, la topografía del iris del ojo, rasgos faciales y la dinámica de escribir una firma e ingresarla en un teclado.

El funcionamiento de estos sistemas implica de la necesidad de un potente software con unas fases diferenciadas en las cuales intervienen diferentes campos de la informática, como son: el reconocimiento de formas, la inteligencia artificial, complejos algoritmos matemáticos y el aprendizaje. Éstas son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptografía se limita a un uso secundario como el cifrado de los datos biométricos almacenados en la base de datos o la trasmisión de los mismos.

Los escáners de huellas digitales y equipos de medición de geometría de la mano son los dispositivos más corrientemente utilizados. Independiente de la técnica que se utilice, el método de operación es siempre la verificación de la identidad de la persona para una comparación de las medidas de determinado atributo físico.

9.2.2. Sensores Biométricos

En lo que a sensores para sistemas biométricos se refiere, aunque hay diferentes fabricantes, hablando en términos generales se utiliza el mismo sistema de captación de la característica deseada, es decir, para reconocimiento de iris se emplea una cámara o para reconocimiento de voz un micrófono. El único campo donde parece existir una mayor variedad de métodos es en el de captación de huella dactilar.

A continuación se muestran diferentes tipos de sensores:

• Sensores Ópticos

El método óptico es uno de los más comunes que suele estar formado por cámaras de vídeo de tipo CCD. Estos sensores se emplean tanto en reconocimiento de huella dactilar como de ojo.

El corazón de la cámara es un circuito integrado tipo CCD (Dispositivo de Carga Acoplada). Este dispositivo consiste de varios cientos de miles de elementos individuales (píxeles) localizados en la superficie de un diminuto CI.

Cada píxel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la cámara), almacenando una pequeña carga de electricidad. Los píxeles se encuentran dispuestos en forma de malla con registros de transferencia horizontales y verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). Esta transferencia de señales ocurre 6 veces por segundo.

• Sensores Termoeléctricos

El método termoeléctrico es menos común. Actualmente sólo existe en el mercado el Atmel Fingerchip™ para reconocimiento de huella dactilar.

El Fingerchip™ utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas (slices) y se pone en marcha un software especial que reconstruye la imagen del dedo. Este método permite al Fingerchip™ obtener una gran cualidad, 500 puntos por imagen impresa de la huella dactilar con 256 escalas de gris.

El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este método proporciona una imagen de gran cualidad incluso cuando las huella dactilares presentan alguna anomalía como sequedad o desgaste con pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua.

Además, también cuenta con la ventaja de autolimpiado del sensor, con lo que se evitan las huellas latentes. Se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores sino que permite que se copie la huella para falsificarla y acceder así al sistema. De hecho, este método de arrastre que utiliza la tecnología basada en el calor hace que el Fingerchip esté por encima de otras tecnologías. El Fingerchip™ funciona con bajas temperaturas, alto porcentaje de humedad, etc.

Otra ventaja es la reproducción de una imagen grande de alta cualidad y siempre un sensor limpio. La desventaja es que la cualidad de la imagen depende un poco

de la habilidad del usuario que utiliza el escáner. La segunda desventaja es el calentamiento del sensor que aumenta el consumo de energía considerablemente.

Este calentamiento es necesario para evitar la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar.

El elevado volumen de diseño del escáner permite que su precio sea bajo ya que en el proceso de manufacturación se necesita menos silicona.

• Sensores Capacitivos

El método capacitivo es uno de los más populares para reconocimiento de huella dactilar. Al igual que otros escáner, genera una imagen de las cresta y valles del dedo. En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos conductores cubiertos por una capa aislante. La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato.

Una ventaja de este diseño es su simplicidad. Una desventaja es que debido a la geometría esférica del campo eléctrico generado por el plato sensor, tendremos un efecto de solapamiento sobre los platos (píxel) vecinos, lo que provocará que el área sensor aumente de tamaño, trayendo como consecuencia un efecto de información cruzada entre los sensores adyacentes, reduciendo considerablemente la resolución de la imagen.

Para dedos jóvenes, saludables y limpios, este sistema trabaja adecuadamente. Los problemas comienzan a presentarse cuando se tienen condiciones menos optimas en la piel. Cuando el dedo esta sucio, con frecuencia no existirá aberturas de aire en valles. Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a soltarse trayendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento.

Entre las empresas líderes en este sector se encuentran: Infineon, Verdicom, Sony y ST Microelectronics.

• Sensores E-Field (de Campo Eléctrico)

El sensor de campo eléctrico funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). La tecnología basada en los campos eléctricos afirma ser útil para cualquiera y poder trabajar bajo cualquier condición, por dura que ésta sea, del "mundo real", como por ejemplo piel húmeda, seca o dañada.

Esta tecnología para reconocimiento de huella dactilar origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Se utiliza un amplificador under-píxel para medir la señal. Los sensores reproducen una imagen clara que se corresponde con mucha exactitud a la huella dactilar y que es mucho más nítida que la producida por sensores ópticos o capacitivos. Esto permite a la tecnología de campo eléctrico la lectura de huellas que otras tecnologías no podrían.

En la tecnología de campo eléctrico, la antena mide las características de la capa subcutánea de la piel generando y detectando campos lineales geométricos que se originan en la capa de células de la piel situada bajo la superficie de la misma.

Esto contrasta con los campos geométricos esféricos o tubulares generados por el sensor capacitivo que sólo lee la superficie de la piel. Como resultado, huellas que con sensores capacitivos son casi imposibles de leer, se pueden reproducir con éxito por sensores de tecnología de campo eléctrico.

Desde hace poco existe también un sensor más fuerte basado en esta tecnología que saldrá al mercado en pocos meses.

Una desventaja es la baja resolución de la imagen y el área pequeña de imagen lo que produce un índice de error alto (EER).

• Sensores sin contacto

Un sensor sin contacto funciona de forma similar al sensor óptico. Normalmente con un cristal de precisión óptica a una distancia de dos o tres pulgadas de la huella dactilar mientras se escanea el dedo. La yema del dedo se introduce en un área con un hueco. Una desventaja a tener en cuenta es que a través de este hueco pueden llegar polvo y suciedad hasta el cristal óptico con la correspondiente distorsión de la

imagen. Otro punto es que las huellas escaneadas son esféricas lo que origina un complejo algorítmico mucho más complejo.

• Micrófonos ópticos unidireccionales

La luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra; cambiando así las características de la luz reflejada.

Un foto-detector registra la luz reflejada que en conjunto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido. Es utilizado en reconocimiento de voz.

9.3. TECNOLOGIA RFID

La identificación por radiofrecuencia o RFID por sus siglas en inglés (radio frequency identification), es una tecnología de identificación remota e inalámbrica en la cual un dispositivo lector o reader vinculado a un equipo de cómputo, se comunica a través de una antena con un transponder (también conocido como tag o etiqueta) mediante ondas de radio.
Esta tecnología que existe desde los años 40, se ha utilizado y se sigue utilizando para múltiples aplicaciones incluyendo casetas de peaje, control de acceso, identificación de ganado y tarjetas electrónicas de transporte.

En los últimos años, la tecnología RFID ha entrado al "mainstream" tecnológico gracias a su creciente difusión en aplicaciones de cadena de suministro motivada por las iniciativas de las cadenas de autoservicio y departamentales.

9.3.1. Funcionamiento de la tecnología RFID

El lector realiza peticiones o preguntas por radiofrecuencia al chip que integran las *etiquetas RFID*, las cuales emiten una respuesta al recibir las señales del *lector,* permitiendo la *identificación con gran seguridad y precisión en tiempo real.*

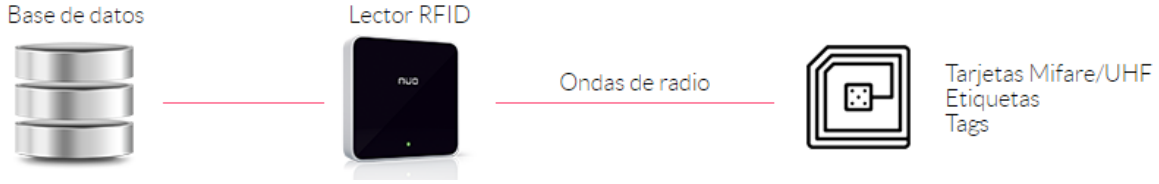


Ilustración 1 Esquema de un sistema de control RFID

El código de identificación que contienen es único y puede ser personalizado durante la fabricación de la etiqueta. Los fundamentos físicos en los que se basa la tecnología RFID, implican la aparición de varios modelos de comunicación entre los dispositivos básicos del sistema. La comunicación por radiofrecuencia, requiere la incorporación de una antena RF en cada uno de los dispositivos implicados en la comunicación cuya forma y características depende de la banda de frecuencia en la que funcionen.

La banda de 125 Khz era *utilizada* por las antiguas tarjetas de identificación en *los primeros lectores de proximidad* que salieron al mercado, lo bueno de estas frecuencias era el buen alcance conseguido para leer las tarjetas con lectores técnicamente poco complejos, y lo malo, la baja seguridad debido a la facilidad de copiar las tarjetas.

La frecuencia de 13,56Mhz es la utilizada por las *modernas tarjetas de identificación,* lo bueno de esta tecnología es la *alta seguridad de las aplicaciones y la cantidad de información que se puede guardar en su memoria,* como por ejemplo el patrón de la huella del portador de la tarjeta, también es posible incorporar en la tarjeta varias aplicaciones diferentes, como puede ser el control de accesos y monedero para máquinas de vending. Esta tecnología actualmente está extendida en todo el mundo y producida por varios fabricantes licenciados por NXP (Philips) disponen de varios modelos.
Los tags (etiquetas) incluyen en su interior un pequeño chip y una antena impresa o bobinada para comunicarse con el lector. El chip tiene grabado un número (ID) de serie único que lo identifica entre los demás, y puede disponer de una pequeña memoria para guardar datos, que los lectores son capaces de leer y escribir.

Hay tres tipos de etiquetas RFID, activas, semipasivas y pasivas.
Los tags pasivos no necesitan alimentación interna, toman la energía de la propia emisión de las antenas del lector y sólo se activan cuando se encuentran en el campo de cobertura del lector. *Las etiquetas activas utilizan alimentación propia de una pequeña batería,* y pudiendo comunicarse con el lector a una distancia mucho mayor y procesando una cantidad de datos superior. *Las etiquetas semipasivas* se parecen a las activas en que poseen una fuente de alimentación propia, aunque en este caso se utiliza principalmente para alimentar el microchip y no para transmitir una señal.



Ilustración 2 Ejemplos de tags RFID

Los tags RFID son de multitud de formas y tamaños según los diferentes entornos donde deben utilizarse, el material que se utiliza para el encapsulado de los tags varía dependiendo del uso que queramos darles, los *encapsulados en plástico* (generalmente PVC) o botones suelen tener mayor durabilidad, son perfectos para aplicaciones donde se tiene que reutilizar o en ambientes hostiles. Cuando la finalidad es identificar objetos, pueden ser cajas o palets que se mueven dentro y fuera de un almacén, lo más común es utilizar un *substrato de plástico con forma de etiqueta* que se adhiera a la superficie del objeto a identificar. También pueden estar *insertadas en tarjetas de plástico,* como las de crédito, se denominan "contactless smart cards", o en papel (sustituyendo a los conocidos códigos de barras), llamadas "smart labels".

Si el objetivo final de la aplicación es la identificación de animales, suele usarse el método de insertar el tag debajo de la piel del animal o bien en el estómago. Para hacer esto posible, el chip y la antena se encapsulan en substratos no tóxicos a modo de cápsula.

Otras aplicaciones donde podemos ver RFID son las llaves de seguridad del vehículo, o las tarjetas de control de acceso a zonas restringidas y/o edificios.

9.4. RASPBERRY PI

Raspberry Pi es un computador de placa reducida, computador de placa única o computador de placa simple (SBC) de bajo coste desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas.

El software es open source, siendo su sistema operativo oficial una versión adaptada de Debian, denominada Raspbian, aunque permite usar otros sistemas operativos, incluido una versión de Windows 10. En todas sus versiones incluye un procesador Broadcom, una memoria RAM, una GPU, puertos USB, HDMI, Ethernet (El primer modelo no lo tenía), 40 pines GPIO y un conector para cámara. Ninguna de sus ediciones incluye memoria, siendo esta en su primera versión una tarjeta SD y en ediciones poosteriore una tarjeta MicroSD.

9.4.1. Raspbian

Raspbian es una distribución del sistema operativo GNU/Linux y por lo tanto libre basado en Debian Jessie (Debian 8.0) para la placa computadora (SBC) Raspberry Pi, orientado a la enseñanza de informática. El lanzamiento inicial fue en junio de 2012.

Técnicamente el sistema operativo es un port no oficial de Debian armhf para el procesador (CPU) de Raspberry Pi, con soporte optimizado para cálculos en coma flotante por hardware, lo que permite dar más rendimiento en según qué casos. El port fue necesario al no haber versión Debian armhf para la CPU ARMv6 que contiene el Raspberry PI.

La distribución usa LXDE como escritorio y Midori como navegador web. Además contiene herramientas de desarrollo como IDLE para el lenguaje de programación Python o Scratch, y diferentes ejemplos de juegos usando los módulos Pygame.

Destaca también el menú "raspi-config" que permite configurar el sistema operativo sin tener que modificar archivos de configuración manualmente. Entre sus funciones, permite expandir la partición root para que ocupe toda la tarjeta de memoria, configurar el teclado, aplicar overclock, etc.

9.5. PROTOCOLO SSH

SSH™ (o *S*ecure *SH*ell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como telnet o rsh. Un programa relacionado, el scp, reemplaza otros programas diseñados para copiar archivos entre hosts como rcp. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

9.5.1. Características de SSH

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.

- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.

- Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

- El cliente tiene la posibilidad de reenviar aplicaciones X11 [1] desde el servidor. Esta técnica, llamada *reenvío por X11*, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada *reenvío por puerto*, como por ejemplo POP, incrementando la seguridad del sistema en general y de los datos.

Red Hat Enterprise Linux contiene el paquete general de OpenSSH (openssh) así como también los paquetes del servidor OpenSSH (openssh-server) y del cliente (openssh-clients). Consulte el capítulo titulado ***OpenSSH*** en el ***Manual de administración del sistema de Red Hat Enterprise Linux*** para obtener instrucciones sobre la instalación y el desarrollo de OpenSSH. Observe que los paquetes OpenSSH requieren el paquete OpenSSL (openssl). OpenSSL instala varias bibliotecas criptográficas importantes, permitiendo que OpenSSH pueda proporcionar comunicaciones encriptadas.

10. DISEÑO E IMPLEMENTACION

Como se ve en el cronograma se plantearon seis fases: Estudio del problema, estudio y selección de las tecnologías a usar, diseño de la solución, integración a la red, pruebas y creación del documento entregable.

A continuación se describirá semana a semana como se llevó a cabo el proyecto, cumpliendo con las seis fases propuestas dentro del cronograma.

SEMANA 1

La primera semana en la planta se recibió orientación acerca de los procesos de seguridad en el trabajo, algo muy importante ya que al ser un planta de químicos se pueden correr ciertos riesgos, a través de entrevistas con los directivos, especialmente con la directora técnica de la planta Andrea Pardo se conocieron los problemas que tenía la planta respecto a la puntualidad, cumplimiento y orden de los colaboradores.

A lo largo de la semana se siguió teniendo reuniones con la directora técnica en las que se recalcaba la importancia de llevar un control acerca de la puntualidad del personal, ya que esto representaba una gran pérdida en la producción.

Al final de la semana se presentó la propuesta de ejecutar un sistema de control de acceso, al cual se dio vía libre esperando una presentación donde se informara que tecnologías se podrían usar, para así aprobar los presupuestos.

SEMANA 2

Durante la segunda semana del proyecto se llevó a cabo una investigación acerca de las tecnologías que estaban disponibles para ofrecer una solución al problema planteado durante la primera semana.

La investigación arrojo como resultado que se podían usar dos tipos de control para la validación del personal, mediante lector biométrico o por proximidad con algún dispositivo.

Al estudiar la primera opción con la directora técnica, se dio a entender que la validación mediante biométricos no era una opción, en primera medida por sus costos (lector de iris o facial), y también porque no se adecuaba a las condiciones de la empresa, pues todo el personal usa guantes durante su jornada, y los químicos algunas veces causan ciertas irregularidades en las huellas de los colaboradores (lector de huella dactilar).

Se tomó entonces la decisión de usar algún tipo de dispositivo para validar el acceso, el dispositivo tenía que ser personal, para que no se diera el caso de algún tipo de suplantación, por lo tanto se descartó por completo el uso de clave.

Durante la investigación se identificaron varias ventajas de los sistemas de reconocimiento RFID que se detallaran a continuación:

Seguridad. Es una tarjeta que por su diseño tecnológico, no puede duplicarse fácilmente. Cada una posee un código distinto y no permite que varios usuarios puedan tener una tarjeta duplicada. Es una diferencia fundamental cuando se le compara con otros sistemas donde la duplicación de tarjetas es bastante frecuente. Son ideales para situaciones de máxima seguridad y alta tecnología.

Sin necesidad de alineación o línea vista. De todos es el sistema más ágil y práctico, por varias razones. Una de ellas es que no necesita que la tarjeta sea pasada por una ranura o en el sentido correcto, lo que le da una mayor agilidad y practicidad de uso. Esto garantiza el éxito de la implementación de un sistema nuevo, donde, en general, los usuarios se resisten a ser controlados, pero al ser tan cómodo su uso, brinda una aceptación muy grande por parte de los usuarios.

Lectores sin mantenimiento. Los lectores son unidades sin partes móviles, lo que garantiza un correcto funcionamiento sin límite de uso y sin que haya que hacerles algún tipo de mantenimiento. También se pueden instalar a la intemperie sin que las inclemencias del tiempo, como altas y bajas temperaturas ambientales, los dañen.

Tarjetas sin desgaste. La tarjeta no tiene fricción alguna con el lector, por lo cual no se desgasta y su vida útil es prolongada. Esto permite su reutilización tras asignarlas, al personal de nuevo ingreso. El resultado es la optimización de recursos.

Se planteó entonces durante estas reuniones el uso de tarjetas RFID para poder validar la presencia del personal dentro de la planta y con la posibilidad de más adelante usar este sistema para validar la presencia no solo dentro o fuera de la planta sino de cada una de las zonas internas.

El modulo lector que se usara en la solución de este proyecto será el MFRC522

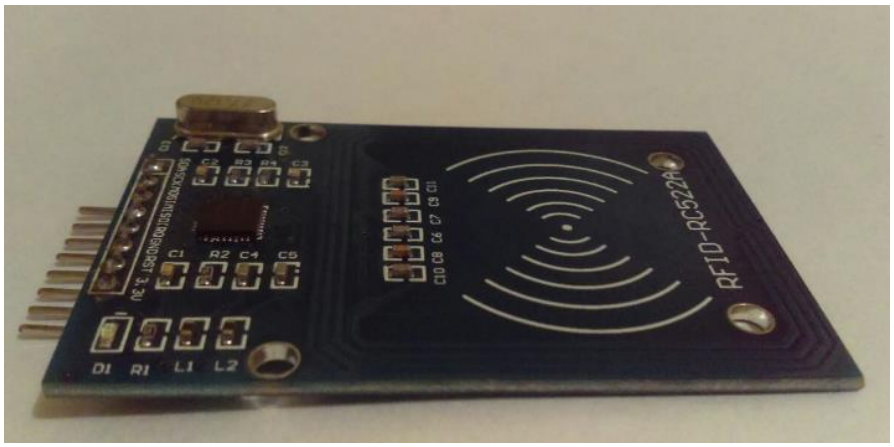


Ilustración 3 Fotografía real del módulo usado en el desarrollo

Este módulo es fabricado por NXP Semiconductors.

Su fabricante lo describe como un lector/escritor altamente integrado para comunicaciones sin contacto a 13.56 MHz y es compatible con el estándar internacional ISO/IEC 14443 por lo que se puede realizar comunicaciones con tarjetas Mifare con el mismo estándar.

Con el módulo MFRC522 podemos usar tres protocolos de comunicación distintos; el protocolo SPI, el serial UART y la interfaz I2C.

Para este desarrollo usaremos el protocolo SPI.

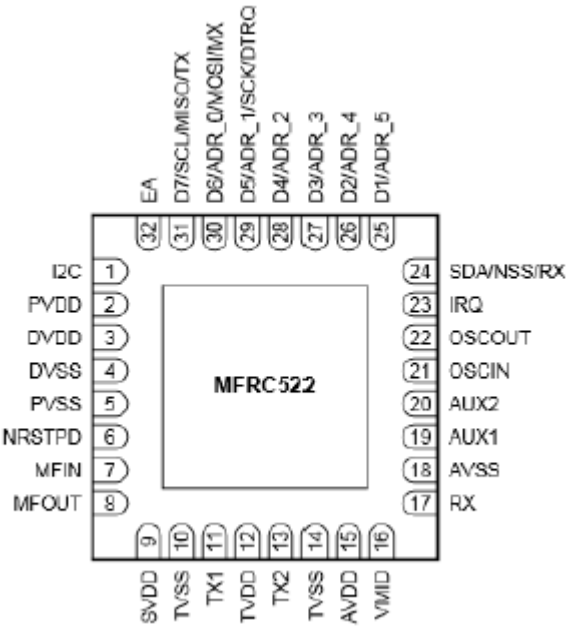


Ilustración 4 Pinout del integrado MFRC522

En cuanto al sistema de control los directivos informaron que dentro de la planta se tenía un dispositivo Raspberry PI modelo B+ que quería que se utilizara en este proyecto, por lo cual se inició una investigación acerca de esta herramienta.

Raspberry PI

La selección de un raspberry como el controlador del desarrollo se dio por las siguientes razones:

1. Uso de código abierto.
2. Hardware de bajo costo
3. Modularidad
4. La empresa insistió en el uso de un raspberry Pi modelo B+ que se encontraba en sus bodegas.

El raspberry pi modelo B+ cuenta con 26 pines GPIO lo que nos permitirá configurar algunos periféricos necesarios.

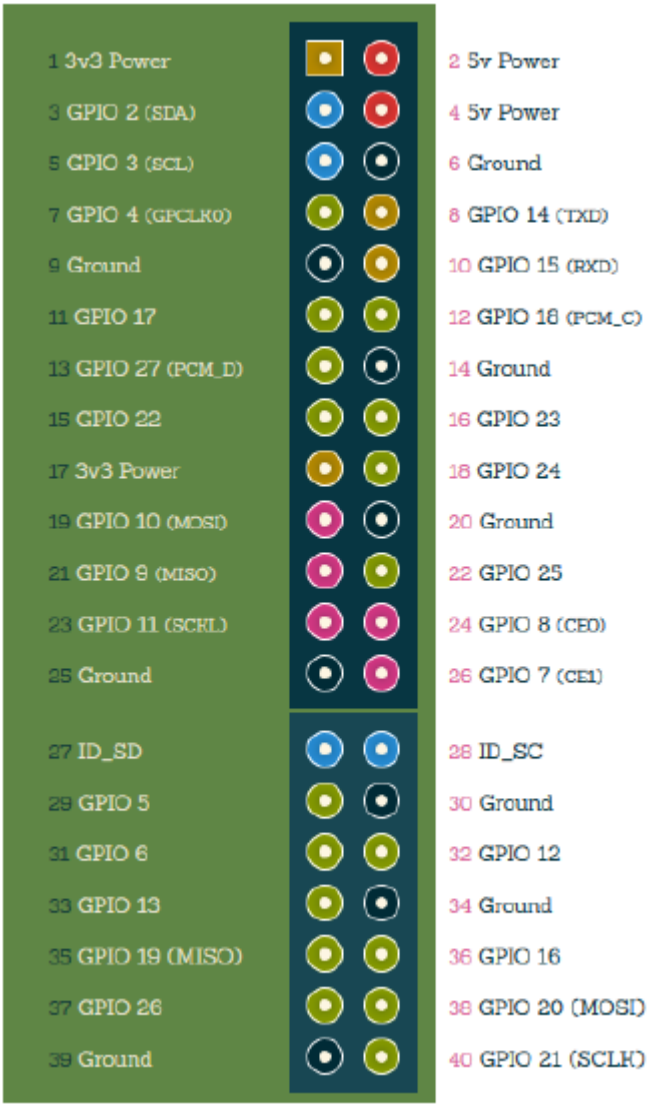


Ilustración 5 Pinout Raspberry Pi B+

Como se mencionó anteriormente la comunicación entre el raspberry y el módulo MFRC522 se llevará a cabo mediante el protocolo SPI, por lo que usaremos los pines 19, 21, 23, 24 y 26.

SEMANAS 3, 4 Y 5

Durante estas tres semanas se llevó a cabo el diseño del programa principal cuyo código se puede revisar en la sección anexos. Para una mejor comprensión del diseño del software a continuación mostramos el desarrollo de este.

Primero se instaló sobre la raspberry el sistema operativo raspbian mediante la herramienta ***NOOBS*** que se puede descargar desde la web: *www.raspberry.org*.

Tras la instalación de raspbian se hicieron algunas configuraciones específicas que son necesarias para el funcionamiento del sistema a diseñar, estas configuraciones se realizan en la pestaña advanced options y se enumeran a continuación.

-COMUNICACIÓN MEDIANTE SSH (Secure Shell): El protocolo SSH es un protocolo que facilita las comunicaciones de forma segura entre dos sistemas encriptando la sesión de conexión, haciendo imposible la intrusión de terceros.

En nuestro caso habilitamos la comunicación SSH por el puerto 22.

-SERIAL PERIPHERAL INTERFACE (SPI): Es un estándar de comunicaciones comúnmente usado para para enviar datos entre micro controladores y algunos periféricos.

Para este proyecto usamos este estándar para la comunicación entre la raspberry y el lector de tarjetas rfid.

Para completar la configuración del estándar SPI debemos editar el archivo *raspi-blacklist.conf*

Primero se abre desde terminal con la siguiente línea de código:

Sudo nano /etc/modprobe.d/raspi-blacklist.conf

Se abrirá un archivo que se debe editar para que quede comentariado de esta forma

“ # blacklist spi-bcm2708”

Así sacamos el protocolo SPI de la lista negra del raspberry para posteriormente usarlo en la comunicación con el módulo MFRC522.

Usaremos Python como lenguaje de programación, este lenguaje viene instalado por defecto en el raspberry, pero hay que descargar algunos módulos y actualizaciones para que nuestro proyecto funcione, las listaremos a continuación.

XLWT, XLRD Y XLUTILS: Son módulos para Python que se usan para copiar, escribir, modificar, actualizar, etc. Archivos de Excel, se descargan desde http://www.python-excel.org/ y se instalan ejecutando la siguiente línea:

Sudo Python setup.py install

SPI-py: Es una de las librerías mas importantes a instalar sobre Python en nuestro proyecto, pues nos permite manejar la configuración de los pines destinados a la comunicación SPI, que será el puente con nuestro lector MFRC522. La instalación se realiza con el siguiente comando en terminal:

Sudo git clone https://github.com/lthiery/SPI-Py

Sudo Python setup.py install

MFRC522: Es la librería que nos permite controlar el modulo lector/escritor MFRC522 a travez de los puertos SPI del raspberry. Su instalación se lleva a cabo mediante los siguientes comandos e terminal.

Sudo git clone https://github.com/mxgxw/MFRC522-python.git

Sudo Python MFRC522 install

RPi-GPIO: Este módulo permite el control de los GPIO del Raspberry Pi, la instalación de este modulo la realizamos mediante el siguiente comando en terminal.

Sudo apt-get install python-rpi.gpio

SEMANA 6

Durante la sexta semana de la práctica se trabajó en la planta para hacer las distintas conexiones entre los periféricos y la raspberry y entre la raspberry y el servidor de la empresa.

Conexión entre el raspberry y el lector de tarjetas

Teniendo en cuenta que se usara el protocolo SPI, es conveniente que se revise un poco más de que trata este.

El protocolo SPI es un protocolo síncrono que trabaja en modo full dúplex para recibir y transmitir información, permitiendo que dos dispositivos se comuniquen entre si al mismo tiempo utilizando canales diferentes. Al ser un protocolo síncrono el sistema cuenta con una línea extra que hace de reloj.

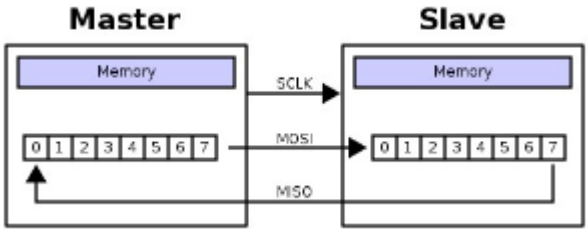


Ilustración 6 Estructura General del protocolo SPI tomada de http://panamahitek.com/como-funciona-el-protocolo-spi/

Dentro de este protocolo se debe definir un maestro que es el dispositivo que transmite información a los demás (esclavos) que son los dispositivos que transmiten y reciben información de su maestro.

Se necesitan de cuatro líneas para realizar el proceso, líneas que se corresponden con los pines que anteriormente destacamos en el raspberry.

- MOSI (Master Out Slave In)
- MISO (Master In Slave Out)
- CLK (Clock)
- SS (Slave Select)

Para nuestro caso el maestro será el raspberry y el esclavo el modulo lector/escritor RFID-RC522, entonces un esquema básico para entender la comunicación entre ellos sería el que vemos en las ilustraciones 5 y 6.

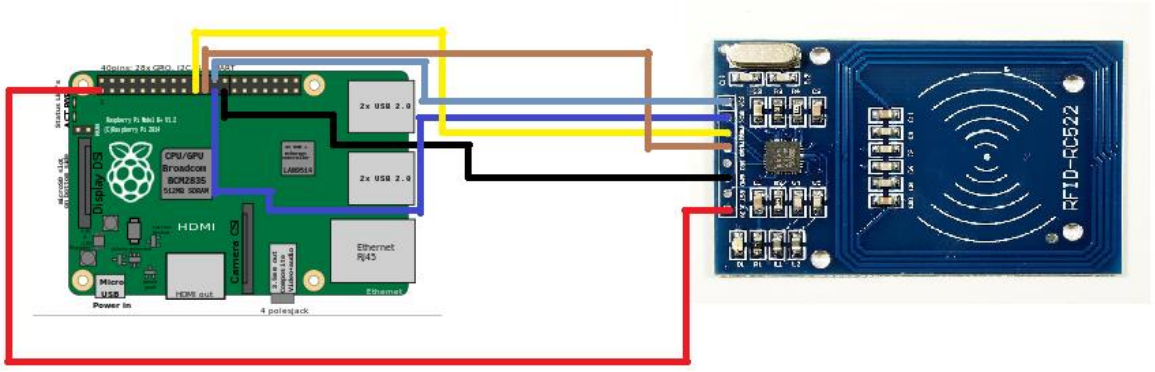


Ilustración 7 Cableado entre el raspberry y el módulo MFRC522

Otras conexiones

En nuestro sistema de control de acceso se visualizará un led azul cuando se haya leído una tarjeta, un led verde cuando el acceso sea concedido y uno rojo cuando sea denegado, al conceder el acceso, mediante un relé se activará una cantonera eléctrica que abrirá la puerta.

Estas 4 conexiones las controlaremos a través de los GPIO 2, 3, 4 y 5 que corresponden a los pines 3, 5, 7 y 29 del raspberry, tal como se puede observar en la ilustración 7.

Las resistencias asociadas a los leds que usaremos se calculan mediante la siguiente formula:

$$V_{cc} - V_{LED} = I.R$$

El voltaje que ofrecen los pines GPIO es de 3.3V y el voltaje promedio en el led es de 2.4V con una corriente de alrededor de 5 mA, asi reescribimos la anterior ecuación de esta manera.

$$3.3V - 2.4V = 5mA.R$$

De donde despejamos el valor de la resistencia así:

$$R = \frac{3.3V - 2.4V}{5\ mA}$$

Y obtenemos el valor:

$$R = 180\Omega$$

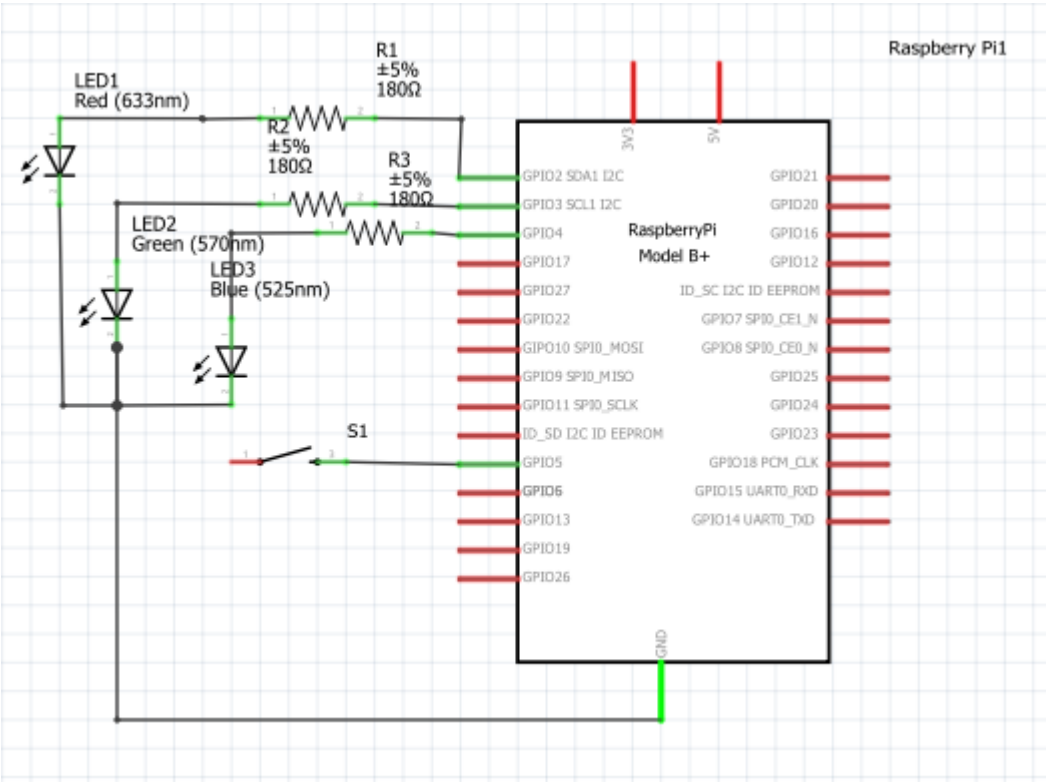


Ilustración 8 Conexión del Raspberry con los LED indicadores de acceso

SEMANA 7

En la séptima semana de la práctica se realizó un seguimiento de los datos que se iban generando en el archivo alojado en el servidor, se hicieron también pruebas de continuidad en las conexiones entre periféricos, para asegurar que todo estuviera en correcto funcionamiento, de esto podemos dar cuenta con las imágenes relacionadas en el apartado resultados obtenidos.

También se revisó un diagrama de flujo del funcionamiento o lógica del sistema final, este diagrama se muestra a continuación.

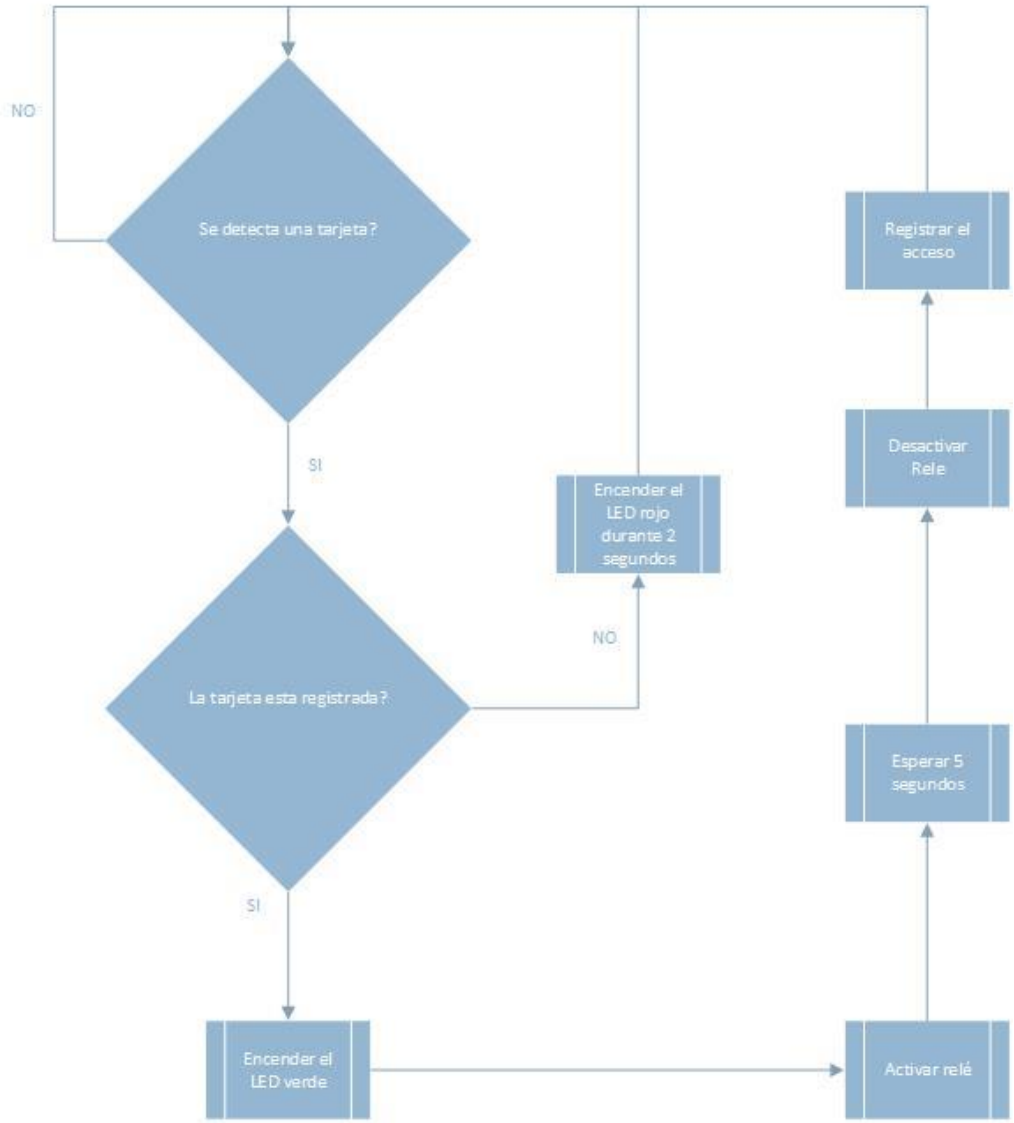


Ilustración 9 Diagrama de flujo del sistema

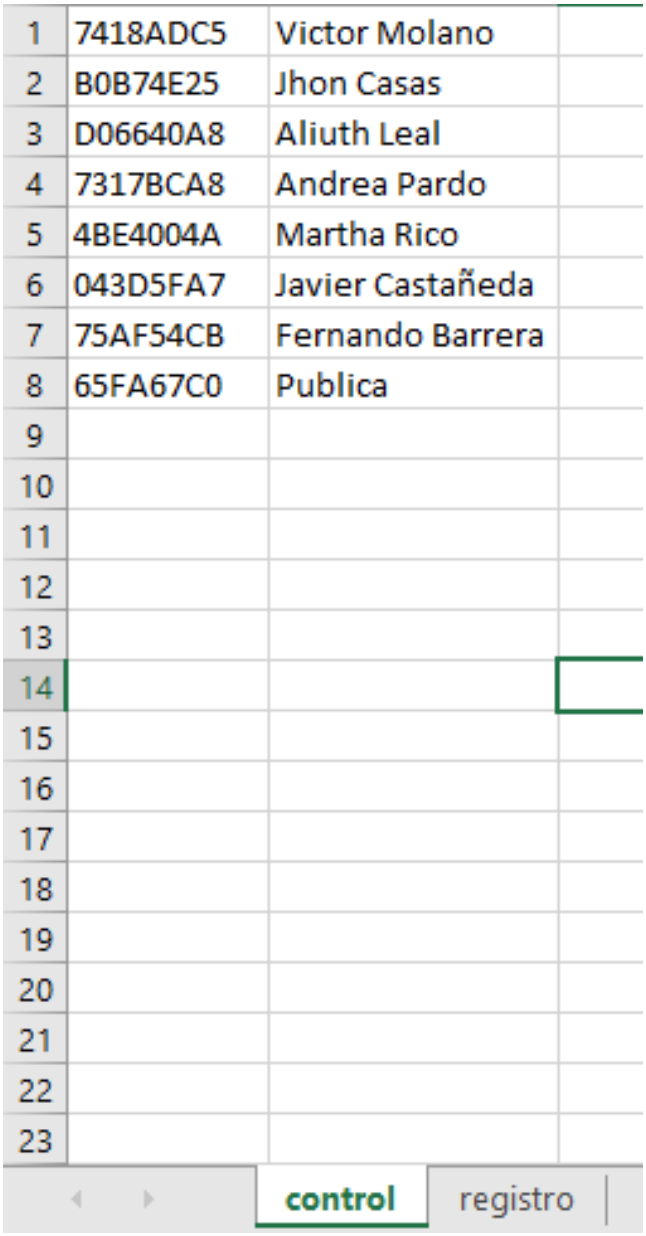
El sistema estará en espera hasta que se detecte una tarjeta en el lector, en ese momento se leerá el id de la tarjeta y se comparara con la base de datos, si el id coincide con algún registro se encenderá el LED verde y se activara el relé que da paso a la energía para que la cantonera eléctrica libere la puerta durante 5 segundos, se registra en la base de datos fecha y hora de acceso. Después de esto el sistema vuelve a la espera.

Si el id no coincide con ningún registro se encenderá el LED rojo y el sistema volverá a estar en espera.

11. RESULTADOS OBTENIDOS

Base de datos

Imágenes tomadas del archivo de Excel alojado en el servidor de la empresa Quimiservi S.A.S. y que funciona como base de datos del control de accesos.



1	7418ADC5	Victor Molano
2	B0B74E25	Jhon Casas
3	D06640A8	Aliuth Leal
4	7317BCA8	Andrea Pardo
5	4BE4004A	Martha Rico
6	043D5FA7	Javier Castañeda
7	75AF54CB	Fernando Barrera
8	65FA67C0	Publica
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		

control registro

Ilustración 10 Hoja "Control"

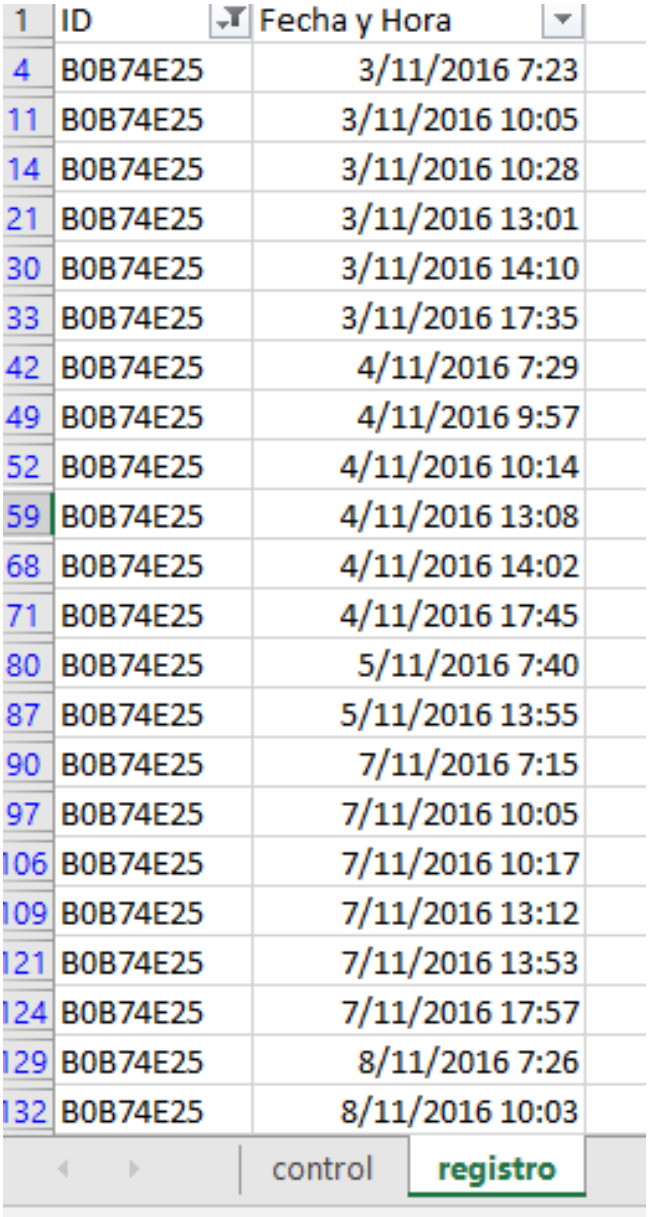
En la ilustración 10 vemos la hoja “control” del libro de Excel llamado control que se usa como base de datos para el sistema de control de accesos, en esta hoja se listan los ID de los tags entregados a los colaboradores de la empresa Quimiservi S.A.S.

	ID	Fecha y Hora
2	7418ADC5	3/11/2016 7:04
3	7317BCA8	3/11/2016 7:21
4	B0B74E25	3/11/2016 7:23
5	75AF54CB	3/11/2016 7:24
6	D06640A8	3/11/2016 7:25
7	043D5FA7	3/11/2016 7:25
8	4BE4004A	3/11/2016 9:36
9	043D5FA7	3/11/2016 10:01
10	75AF54CB	3/11/2016 10:05
11	B0B74E25	3/11/2016 10:05
12	7317BCA8	3/11/2016 10:06
13	D06640A8	3/11/2016 10:06
14	B0B74E25	3/11/2016 10:28
15	7317BCA8	3/11/2016 10:28
16	75AF54CB	3/11/2016 10:28
17	D06640A8	3/11/2016 10:29
18	043D5FA7	3/11/2016 10:29
19	4BE4004A	3/11/2016 12:53
20	7418ADC5	3/11/2016 12:55
21	B0B74E25	3/11/2016 13:01
22	D06640A8	3/11/2016 13:02
23	75AF54CB	3/11/2016 13:05

control registro

Ilustración 11 Algunos registros de acceso

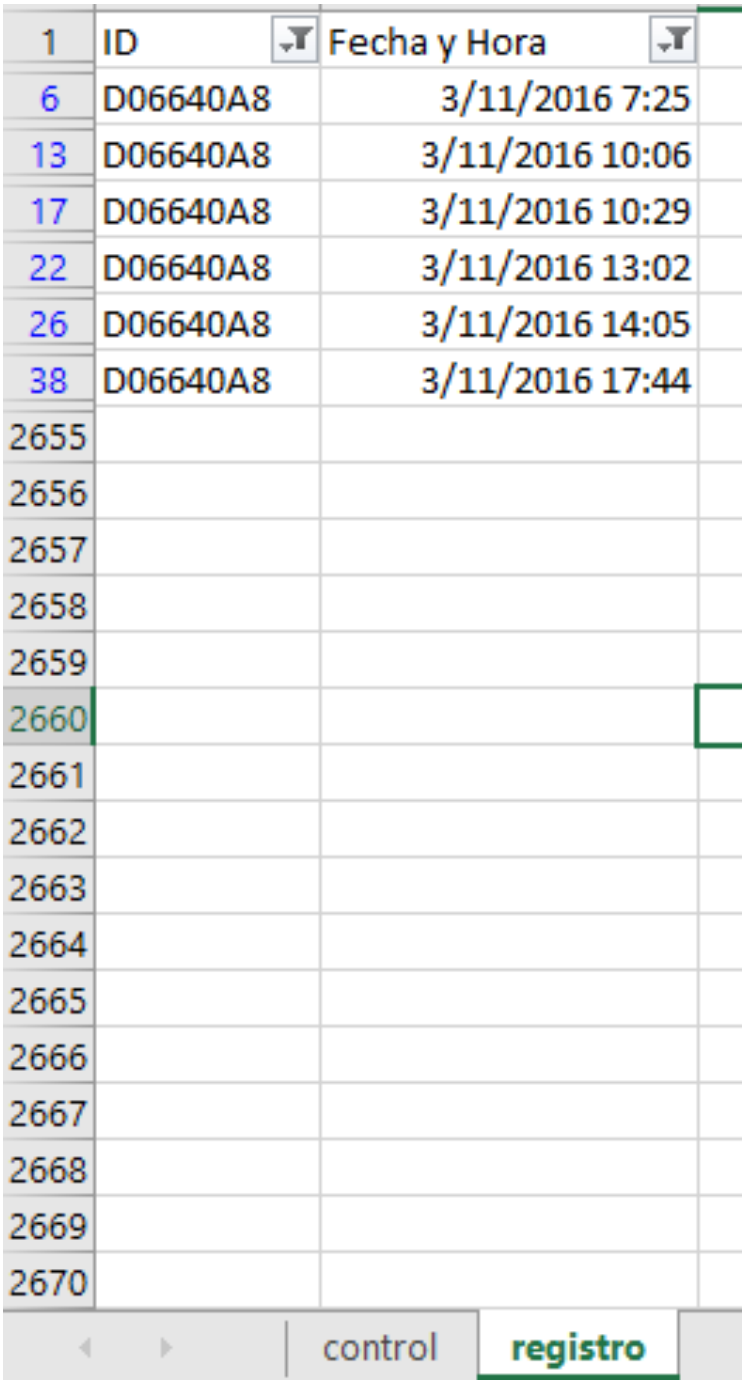
En la ilustración 11 se observa cómo se almacenan los registros en la hoja “registro” del libro de Excel llamado “control”, estos registros corresponden al primer día de pruebas, noviembre 3 de 2016.



1	ID	Fecha y Hora
4	B0B74E25	3/11/2016 7:23
11	B0B74E25	3/11/2016 10:05
14	B0B74E25	3/11/2016 10:28
21	B0B74E25	3/11/2016 13:01
30	B0B74E25	3/11/2016 14:10
33	B0B74E25	3/11/2016 17:35
42	B0B74E25	4/11/2016 7:29
49	B0B74E25	4/11/2016 9:57
52	B0B74E25	4/11/2016 10:14
59	B0B74E25	4/11/2016 13:08
68	B0B74E25	4/11/2016 14:02
71	B0B74E25	4/11/2016 17:45
80	B0B74E25	5/11/2016 7:40
87	B0B74E25	5/11/2016 13:55
90	B0B74E25	7/11/2016 7:15
97	B0B74E25	7/11/2016 10:05
106	B0B74E25	7/11/2016 10:17
109	B0B74E25	7/11/2016 13:12
121	B0B74E25	7/11/2016 13:53
124	B0B74E25	7/11/2016 17:57
129	B0B74E25	8/11/2016 7:26
132	B0B74E25	8/11/2016 10:03

Ilustración 12 Registros filtrados

En la ilustración 12 se observan los registros filtrados para el ID B0B74E25 correspondiente al colaborador Jhon Casas



1	ID	Fecha y Hora
6	D06640A8	3/11/2016 7:25
13	D06640A8	3/11/2016 10:06
17	D06640A8	3/11/2016 10:29
22	D06640A8	3/11/2016 13:02
26	D06640A8	3/11/2016 14:05
38	D06640A8	3/11/2016 17:44
2655		
2656		
2657		
2658		
2659		
2660		
2661		
2662		
2663		
2664		
2665		
2666		
2667		
2668		
2669		
2670		

Ilustración 13 Registros con dos filtros

En la ilustración 13 se observa el registro filtrado con el ID D06640A8 correspondiente al colaborador Aliuth Leal para el día 3 de noviembre de 2016.

12. IMPACTO DEL TRABAJO DE GRADO

Como se ha planteado en todo el desarrollo del proyecto el mayor impacto es generar un beneficio a la compañía a través del manejo más exacto del personal, situación que mejorara la producción y eficiencia dentro de la planta.

Por otra parte, el sistema que se generó es completamente replicable y modular, lo que permite más adelante llevar un control específico sobre diferentes zonas que son de especial atención dentro de la planta como los laboratorios de pruebas.

A nivel personal este trabajo cambio mi perspectiva, al situarme bajo una experiencia nueva y real de la vida laboral, aportándome conocimientos que me hicieron crecer a nivel profesional y académico.

13. EVALUACION Y CUMPLIMIENTO DE LOS OBJETIVOS DE LA PASANTIA

13.1. Cumplimiento del objetivo general

Se diseñó un sistema de control de acceso sobre la herramienta Raspberry con sistema de reconocimiento RFID (MFRC522) que arroja informes a través de un libro de Excel alojado en el servidor de la empresa QUIMISERVI S.A.S.

13.2. Cumplimiento de los objetivos generales

Como se evidencia en este documento se estudiaron y pusieron en discusión con los representantes de la empresa las diferentes tecnologías que estaban disponibles para el desarrollo de la solución.

Se desarrolló una solución de hardware con los requerimientos de la empresa usando las tecnologías investigadas anteriormente

A través de las preferencias de la directora técnica se diseñó el programa principal para el control del hardware especificado.

A través de una semana de prueba se confirmó el buen funcionamiento de la solución entregada.

14. CONCLUSIONES

Mediante la implementación de este proyecto se logró mejorar el control sobre la asistencia de los colaboradores en la empresa Quimiservi S.A.S. lo que después de algunas reuniones con ellos, incremento la productividad en las instalaciones.

El uso de software libre para el desarrollo del proyecto bajó los costos del mismo, también se encontró una gran cantidad de documentación para este, lo que lo facilito.

Se observó la necesidad de implementar sistemas de control de acceso en diferentes organizaciones.

Se proyectan diferentes mejoras al sistema y nuevos desarrollos con la empresa, lo que permite estabilidad laboral para el pasante en el futuro inmediato.

BIBLIOGRAFÍA

1. **Byte Paradigm,** Introduction to I2C and SPI protocols. http://www.byteparadigm.com/applications/introduction-to-i2c-and-spi-protocols/?/article/AA-00255/22/Introduction-to-SPI-and-IC-protocols.html, [Fecha de consulta:2016-10-21]
2. **Raspberry Pi Foundation,** What is a Raspberry Pi?, https://www.raspberrypi.org, [Fecha de consulta:2016-10-15]
3. **Egomexico,** ¿Cómo funciona la tecnología de identificación por radio frecuencia RFID?, http://www.egomexico.com/tecnologia_rfid.htm, [Fecha de consulta:2016-10-15]
4. **Tolosa Cesar,** Sistemas Biométricos, https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf, [Fecha de consulta: 2016-10-14]

ANEXOS

Accesos.py

Este es el código con el que funciona el raspberry como control de acceso, está escrito en Python, lenguaje seleccionado como se ha dicho antes por ser libre y estar preinstalado en el raspberry.

```
1   #!/ usr/bin/Python
2
3
4       #Importar modulos
5       import openpyxl
6       import sys
7       import time
8
9       import RPi.GPIO as GPIO #Importamos la librería RPi.GPIO que permite el control de los pines del raspberry
10      import MFRC522#Importa la libreria que permite el manejo del lector/escritor de tarjetas RFID MFRC522

11      import subprocess
12
13
14
15
16 #Encender y apagar Led rojo
17 def denegado():
18              GPIO.output(3,True)#Pone el pin 3(gpio 2) en alto
19              time. sleep (2)#espera dos segundos
20              GPIO.output(3,False) #Pone el pin 3(gpio 2) en bajo
21 #Encender y apagar el LED verd y el rele
22 def concedido():
23              GPIO.output(5,True)#Pone el pin 5(gpio 3) en alto
24              GPIO.output(29,True) #Pone el pin 29(gpio5, rele) en alto
25              time.sleep(5)#Espera cinco segundos
26              GPIO.output(5,False) #Pone el pin 5(gpio 3) en bajo
27              GPIO.output(29,False) #Pone el pin 29(gpio5, rele) en bajo
28 #Encender y apagar  el LED azul
29 def noleida():
30              GPIO.output(7,True) #Pone el pin 7 en alto
```

```
31              time.sleep(1)#Espera un
segundo
32              GPIO.output(7,False) #Pone el
pin 7 en bajo

33def validaracceso(tagID): #Revisa en el archivo de Excel usado como base de datos si el id esta
registrado
34
        bdd=openpyxl.load_workbook('\\Servidor\bodega\Administrativa\Personal\Control.
xls')
35      hoja=bdd.get_sheet_by_name('control')
36      z=hoja.get_highest_row()
37      for i in range(1,z+1):
38      vbdd=hoja.cell(row=i,column=1).value
39      if(vbdd==tagID):
40              control=1
41              return control
42      else:
43              control=0
44      bdd.close()
45      return control
46
47
48def registraracceso(tagID):
49
        bdd=openpyxl.load_workbook('\\Servidor\bodega\Administrativa\Personal\Control.
xls')
50      hoja=bdd.get_sheet_by_name('registro')
51      hoja.append([tagID,time.strftime("%c")])
52      bdd.save('\\Servidor\bodega\Administrativa\Personal\Control.xls')
53      bdd.close()


54def inicializarGpio():
55      GPIO.setwarnings(False)#Se colocan   las advertencias en falso
56      GPIO. setmode(GPIO.BOARD)
57      GPIO.setup(3,GPIO.OUT) #Configura el pin 3 como salida
58      GPIO.setup(5,GPIO.OUT) #Configura el pin 5 como salida
59      GPIO.setup(7,GPIO.OUT) #Configura el pin 7 como salida
60      GPIO.setup(29,GPIO.OUT) #Configura el pin 29 como salida
61
62#Esta función se mantiene comprobando si se leyó una tarjeta y devuelve el valor id de esta
```

```
63
64def ciclo():
65      ingreso=True
66      contador=10
67      while (espera==True and contador!=0) :
68              lectura = MFRC522.MFRC522()
69              (estado,tipo)=lectura.MFRC522_Request(lectura.PICC_REQIDL)
70              (estado,dato)=lectura.MFRC522_Anticoll()
71              contador=contador−1#Disminuye el valor del contador en uno
72              if (estado==lectura.MI_OK):
73                      lectura.AntennaOff()
74                      ingreso=False
75                      contador=0
76                      return str(dato[0])+str(dato[1])+str(dato[2])+str(dato[3])+str(dato[4])
77                      time.sleep(0.2)
78#Funcion leerTag() permite obtener los datos obtenidos en ciclo y almacenarlo para su
manejo
79def leerTag():
80      global tagId#Variable  tagId global
81      tagId=0#Valor inicial 0
82      tagId=ciclo()#llamamos a la función ciclo y almacenamos el valor del id
83      return tagId
84#En esta función se define si el usuario tiene permiso para entrar
85
86def permiso():
87      leerTag()#Llama a la funcion leerTag para obtener el valor de la tarjeta
88      global tagId
89      if (tagId==None):# Si el id es nulo
90      noleida()#Encender LED azul
91      else:#Verifica  si el usaurio esta en la lista de admitidos
92              auto=validaracceso(tagid)
93              if (auto==0):#Si el id no esta registrado
94              denegado()#Enciende el led rojo
95
96              permiso ()
97              else:
98                      registraracceso(tagId)
99                      concedido()
100     GPIO.cleanup()
101     accesos()
```