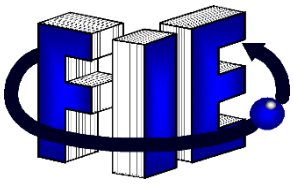
UNIVERSIDAD MICHOACANA DE SAN NICOLAS DE HIDALGO



FACULTAD DE INGENIERIA ELECTRICA

SISTEMA DE ACCESO Y REGISTRO AUTOMÁTICO

CON TECNOLOGÍA NFC Y WIFI

TESIS

PARA OBTENER EL TITULO DE

INGENIERO EN ELECTRONICA

Presenta:

JULIO CESAR LEYVA ZUÑIGA

Asesor de tesis:

M.C ISRAEL LUNA REYES

Morelia Mich. Diciembre 2019

Dedicatoria

A mi padre José Roberto Leyva Espinoza, por enseñarme a siempre dar lo mejor de mí, por darme el ejemplo de la persona que debo ser, por ser mi mayor inspiración, por darme todo el apoyo que necesito, por darme el amor de padre, por todo esto y más te la dedico papá.

A mi madre Leticia Zúñiga Moreno, por inculcarme los valores, por cuidarme cuando estuve enfermo, por preocuparse por mí, por apoyarme en todas las decisiones que he tomado, por darme ese amor de madre, te la dedico mamá.

A mi hermana Brenda Karina Leyva Zúñiga, por exigirme, por creer en mí, por apoyarme en momentos difíciles, por quererme, te la dedico hermana.

A mis padrinos Vero y Armando por motivarme, orientarme y darme apoyo y cariño.

A mi familia Leyva y Zúñiga por el apoyo brindado.

Agradecimientos

A Dios por permitirme llegar a esta etapa de mi vida con mis seres queridos al lado mío.

A mis padres Roberto y Leticia que siempre me apoyaron y gracias a ellos he podido llegar a esta etapa de mi vida, gracias por sus consejos, por su amor, por su apoyo y por estar conmigo en todas mis decisiones, gracias.

A mi hermana Kary quien siempre creyó en mí y siempre me apoyo cuando más lo necesite.

A mis amigos dentro y fuera del aula, quienes me apoyaron y me dieron sus consejos.

A mi asesor y gran amigo Israel quien siempre me compartió sus conocimientos y me apoyo para llevar a cabo esta tesis.

A mi Mariela por ayudarme, apoyarme y brindarme de sus conocimientos para la elaboración de este trabajo.

A mi profesor y gran amigo Feliche, quien busco siempre exigirme un poco más de lo que estaba dando.

A mi amigo Mauricio, por compartirme sus conocimientos.

A mi familia por apoyarme.

A la facultad por formarme durante la carrera y convertirse en mi segunda casa.

A todos los profesores de la facultad por su paciencia y enseñanzas.

Contenido

Capítulo 1: Introducción 1

1.1 Antecedentes 1
1.2 Objetivos 4
1.2.1 Objetivo general 4
1.2.2 Objetivo particular 4
1.3 Justificación 5

Capítulo 2 Marco teórico 6

2.1 Tipos de sistemas de control de acceso electrónico 7
2.1.1 Sistemas autónomos 7
2.1.2 Sistemas gestionados 8
2.1.3 Sistemas corporativos 9
2.2 Dispositivos actuales de identificación 11
2.2.1 Identificación Numérica 12
2.2.2 Lectores biométricos 13
2.2.3 RFID 14
2.2.4 Bandas magnéticas 16
2.3 Descripción general del sistema SCARE 17

Capítulo 3 Hardware 19

3.1 Modulo CARE 20
3.2 Modulo RAB 23
3.3 Placas de desarrollo para Microcontroladores 24
3.3.1 Placa de desarrollo “NodeMCU V3 lollin” 25
3.3.2 Arduino 28
3.4 NFC 29
3.4.1 TAGS 32

Capítulo 4 Software desarrollado 36

4.1 Introducción 36
4.2 Software de PC 37
4.2.1 Login 40
4.2.2 Registro de altas 41
4.2.3 Configuración avanzada 45
4.2.4 Registros 49
4.3 Servidor y base de datos 50

4.4 Php y HTML 54
4.5 Software RAB 56
4.6 Software CARE 63

Capítulo 5 Pruebas y Resultados 65
Conclusiones 67
Referencias 68

Resumen

El sistema de control de acceso tradicional permite obtener control sobre áreas específicas, sin embargo, con el avance tecnológico que se presenta a través de los años, el sistema tradicional ha quedado obsoleto en cuestión de seguridad debido a la facilidad de duplicación de llaves, además de carecer de un sistema de identificación.

En el presente trabajo se desarrolla un sistema de control de acceso electrónico, este sistema permite gestionar el acceso de usuarios a distintas áreas; además, crea un registro de operaciones.

Para facilitar la gestión de este sistema se realiza el diseño y desarrollo de un software con interfaz gráfica, este se encarga de gestionar la base de datos de sistema, además de programar tarjetas electrónicas con tecnología NFC, las cuales son requeridas para obtener acceso.

Para tener control de área se desarrolla un módulo lector de tarjetas NFC, el cual se conecta mediante Wi-fi al servidor para realizar la consulta de usuario y obtiene una respuesta de autorización o negación, al realizar esta consulta genera un registro el cual depende en su totalidad de la respuesta emitida por la base de datos alojada en el servidor.

A continuación, se presentan los capítulos en los que se divide el presente trabajo:

Capítulo 1: Introducción. – Se presentan algunos antecedentes históricos de los sistemas de acceso controlados, el uso, creación y modificación de la llave, solución propuesta, los objetivos generales y particulares y la justificación del presente trabajo.

Capítulo 2: Marco Teórico. – Describe los diferentes tipos de sistemas de acceso electrónico, los sistemas de identificación electrónica, los riesgos de estos sistemas, así como las ventajas y desventajas.

Capítulo 3: Diseño y descripción de Hardware. – Se presenta el diseño y construcción de los dos módulos que componen el sistema SCARE los cuales son CARE y RAB en sus componentes físicos.

Capítulo 4: Diseño y descripción del Software. – En este capítulo se desarrollan los códigos de los módulos RAB y CARE en lenguaje “C”, además de la configuración de la base de datos MARIADB, los programas del servidor web (HTML, PHP) y el gestor del sistema programado (java).

Capítulo 5: Pruebas y resultados. –Este capítulo describe y analiza las pruebas realizadas para determinar posibles fallos en el equipo y cuestiones de seguridad, así como sus posibles soluciones.

Capítulo 6: Conclusiones. – Se presentan las conclusiones personales del presente trabajo.

Abstract

The traditional access control system allows to obtain control over specific areas, however, with the technological progress that has been presented over the years, the traditional system has been obsolete in terms of security due to the ease of key duplication, in addition of lacking an identification system.

In this work an electronic access control system is developed, this system allows users to manage access to different areas; Also, create an operations log.

To facilitate the management of this system, the design and development of a software with graphic interface is carried out, this is responsible for managing the database of the system, in addition to programming electronic cards with NFC technology, which are required to obtain access.

To have area control, an NFC card reader module is developed, which is connected via the Wi-Fi server to perform the user's query and obtains an authorization or denial response, when making this query it generates a record which depends on its completeness. of the response issued by the database hosted on the server.

Below are the chapters in which the present work is divided:

Chapter 1: Introduction. - Some historical antecedents of the controlled access systems, the use, creation and modification of the key, proposed solution, the general and particular objectives and the justification of the present work are presented.

Chapter 2: Theoretical Framework. - Describe the different types of electronic access systems, electronic identification systems, the risks of these systems, as well as the advantages and disadvantages.

Chapter 3: Design and description of Hardware. - The design and construction of the two modules that make up the SCARE system, which are CARE and RAB in their electronic components, is presented.

Chapter 4: Design and description of the software. - In this chapter you will find the codes of the RAB and CARE modules in "C" language, in addition to the configuration of the MARIADB database, the web server programs (HTML, PHP) and the programmed system manager (java) .

Chapter 5: Tests and results. –This chapter describes and analyzes the tests performed to determine possible equipment failures and safety issues, as well as their possible solutions.

Conclusions: The personal conclusions of this work are presented.

Palabras clave

Sistema, Control, Software, Interfaz gráfica, Base de datos, Módulo, Wi-fi, Servidor, Acceso electrónico, llaves electrónicas, Tecnología, Componentes, Sistema Gestionado, Sistema Corporativo, Sistema Autónomo, Clave Global, Clave Personal, Usuario, Servidor, Biometría, Tag, Radiofrecuencia, Encriptación, Banda Magnética, Microcontrolador, Placa de Desarrollo, Chip, Super Usuarios, NodeMCU, SDA, SCL, Optoacoplador, Regulador de Voltaje, Permisos, Monitor Serie, Software, Hardware, Velocidad de Transmisión, Standby, Java, NetBeans, MariaDB, Apache, Puerto COM, Combo Box, XAMPP

Abreviaturas

NFC	Near Field Communication
SCARE	Sistema de Control de Acceso y Registro Electrónico
RAB	Registro de Altas y Bajas
CARE	Control de Acceso y Registro Electrónico
WI-Fi	Wireless Fidelity
RFID	Radio Frequency IDentification
I2c	Inter Integrated Circuits
HTML	HyperText Markup Lenguage
PHP	HyperText Preprocessor

Lista de Figuras

Figura 1 Primera cerradura [3] 2
Figura 2 Cerradura de palanca [3] 3
Figura 3 TAG NFC para incrustación en la piel. [6] 6
Figura 4 Sistema Autónomo [7] 8
Figura 5 Sistema gestionado 9
Figura 6 Sistema corporativo [8] 10
Figura 7 Teclado de identificación numérica [9] 12
Figura 8 Escáner de retina y huella dactilar 14
Figura 9 Sistema RFID y etiquetas RFID 15
Figura 10 Diagrama modulo CARE 20
Figura 11 Pines de selección de comunicación NFC 21
Figura 12 Representación física sistema CARE 22
Figura 13 Conexión Arduino nano -NFC module v3 24
Figura 14 Esquema NodeMCU 25
Figura 15 Mapa de pines NodeMCU v3 lollin 26
Figura 16 Mapa de pines de ESP8266-12E 27
Figura 17 Mapa de pines de salida de Arduino Nano 28
Figura 18 NFC module v3 ELECHOUSE 30
Figura 19 Organización de memoria MIFARE Classic 1k 32
Figura 20 Login RAB sin base de datos activa 38
Figura 21 Software RAB 39
Figura 22 Login RAB 40
Figura 23 Interfaz RAB con botones de ejecución 41
Figura 24 Gestión de Registros de usuarios 43
Figura 25 Modificación de usuario 44
Figura 26 RAB configuración avanzada 45
Figura 27 Botón Leer NFC y tabla de lectura 46
Figura 28 RAB lector especifico 47
Figura 29 RAB nueva contraseña 48

Figura 30 RAB texto manual 48
Figura 31 RAB registro de ingresos 49
Figura 32 RAB Registro de intentos 50
Figura 33 XAMPP 51
Figura 34 PHP myAdmin 52
Figura 35 Base de datos y tablas 53
Figura 36 Pagina HTML de SCARE 55
Figura 37 Respuesta del sistema 56

Lista de tablas

Tabla 1Estados de operación 23

Tabla 2 Tabla de Resgistros base de datos 53

Tabla 3 Tabla de Usuarios 54

Capítulo 1: Introducción

Desde la antigüedad, el control de acceso fue requerido con la finalidad de salvaguardar los bienes fueran estos de una comunidad o personales, es por esto que los sistemas de control de acceso han evolucionado con el paso de los años proveyendo mayor seguridad hasta llegar a la actualidad.

En el presente documento se diseña y desarrolla un sistema de control de acceso electrónico utilizando tecnología NFC para identificación de usuarios, así como la tecnología Wi-Fi para transmisión de datos.

El sistema que se desarrolla en este trabajo lleva por nombre SCARE el cual tiene por significado Sistema de Control de Acceso y Registro Electrónico, y consta de dos módulos físicos, el primer módulo se encarga de elaborar Registros de Altas y Bajas por lo que se denomina RAB, mientras que el segundo realiza el Control de Acceso y Registro de manera Electrónica por lo que se denomina CARE. Ambos módulos son indispensables para el sistema a desarrollar.

1.1 Antecedentes

Primeras cerraduras

En la antigüedad la fabricación de cerraduras era costosa debido a la cantidad de tiempo que llevaba fabricarlas y la carencia de materiales para hacerlas, por lo que solo las personas con una condición económica alta podían adquirir estos dispositivos. [1]

El primer cerrojo del que se tiene un registro es un dispositivo egipcio fabricado de madera, la manera en la que funcionaba este dispositivo es al ingresar la llave la cual era un rodillo de madera con perforaciones, este al girar recorre dos pistones y libera la chapa, dicho cerrojo fue encontrado con su llave en las ruinas de Nínive en la antigua Asiria figura 1. [1]

Figura 1 Primera cerradura [2]

Los romanos crearon un sistema de seguridad en los cierres: la vuelta de llave. Ellos fueron también quienes consiguieron disminuir el tamaño de las llaves de forma increíble por lo que la cerradura y la llave metálica son realmente una aportación romana.

Las cerraduras tuvieron poca evolución duran el periodo romano, hasta el siglo XVIII, en Inglaterra, con la aparición de la cerradura de puerta, es en ese momento cuando comienzan a tecnificarse los sistemas de seguridad. Fueron Linus Yale y su hijo quienes revolucionaron el mundo de las cerraduras; Linus desarrollo el modelo de tambor de pines, y su hijo la cerradura de combinación, ambos fueron los fundadores de la famosa compañía de llaves y cerraduras Yale Lock Manufacturing Company.

A lo largo del siglo XIX se fue mejorando los sistemas de seguridad tales como el cerrojo de pestillo, también se inventaron y perfeccionaron los cerrojos de palanca o clavija, los cilíndricos o de dientes de clavija y los cerrojos sin llave (Figura 2).

Figura 2 Cerradura de palanca [3]

Poco a poco las llaves fueron evolucionando, cambiando sus diseños y formas, ofreciendo cada vez mayor seguridad. Se comenzaron a producir cerraduras en serie, se mejoraron los materiales y se fue incrementando la complejidad de los mecanismos de funcionamiento hasta llegar a la electrónica, con llaves y cerraduras codificadas.

En la era digital se sigue requiriendo de seguridad y privacidad, es por esto que los creadores de software diseñaron un tipo de llave que denominaron “contraseña”, que es la clave o llave que algunos programas tienen como sistema de seguridad para poder ingresar a las funciones de estos.

Las llaves tradicionales muestran la evolución que ha tenido el control de acceso, al ser modificadas en su forma, tamaño, dientes, etc.; pretenden proveer mayor seguridad, sin embargo, aún con las modificaciones son fáciles de duplicar. Para solucionar este problema los hoteles, empresas y bancos han optado por reemplazar dichas llaves por llaves electrónicas que no pueden duplicarse con tanta facilidad, y en caso de pérdida no representen un gasto mayor.

Combinando los muros de protección y el uso de cerraduras se obtiene un sistema de control de acceso básico, ya que solo los usuarios poseedores de llave podrán ingresar a las áreas protegidas por el sistema, un ejemplo de estos sistemas básicos fueron los castillos, prisiones, calabozos, etc. Los cuales en su momento fueron sistemas de alta seguridad pero que hoy en día están obsoletos.

Hoy en día no contar con un sistema de control de acceso electrónico representa varios problemas, entre los cuales destaca, la falta de seguridad ya que no existe un control de llaves debido a la facilidad de duplicación; al no contar con un registro de usuarios es prácticamente imposible determinar quién ingresa y a qué área se dirige, además al perder una llave se requiere reemplazar la chapa lo cual genera costo.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar y desarrollar un sistema de seguridad que permita gestionar el control de acceso de usuarios en áreas y horarios específicos para cada uno de estos.

1.2.2 Objetivo particular

Dentro de los objetivos particulares se tienen los siguientes:

- Desarrollar una aplicación para la gestión del sistema de control de acceso.
- Controlar el acceso en áreas específicas.
- Registrar los accesos autorizados y no autorizados.
- Desarrollar e implementar los módulos para registro e identificación de usuarios.
- Aplicar los conocimientos adquiridos durante mi proceso de formación profesional.

1.3 Justificación

Los sistemas de acceso básicos (chapa y llave) permiten un control de baja seguridad ya que no cuentan con un sistema de registro, sus llaves son fáciles de duplicar y si estas se pierden se requiere remplazar la chapa lo cual genera un costo. Para solucionar algunos de estos problemas se opta por contratar personal capacitado para incrementar el nivel de seguridad, ya que estos elaboran un registro que permite un control de entradas y salidas, aun así, no se logra eliminar los problemas principales; Por lo tanto, el presente trabajo diseña un sistema para control de accesos, este provee una solución a los problemas de identificación ya que utiliza la tecnología NFC como llaves, además de un registro de usuarios, lugares y horarios de trabajo. Al contar con tecnología NFC como llaves de seguridad basta con dar de baja estas para evitar el acceso en caso de pérdida o duplicado, por lo que propone una solución inmediata a los problemas de seguridad de los sistemas no electrónicos.

Capítulo 2 Marco teórico

En el presente capítulo se describen los conocimientos fundamentales para realizar el desarrollo del sistema SCARE, además se mencionan los tipos de sistemas de control de acceso, los dispositivos de identificación electrónicos de usuarios, ventajas y desventajas, además del funcionamiento del sistema.

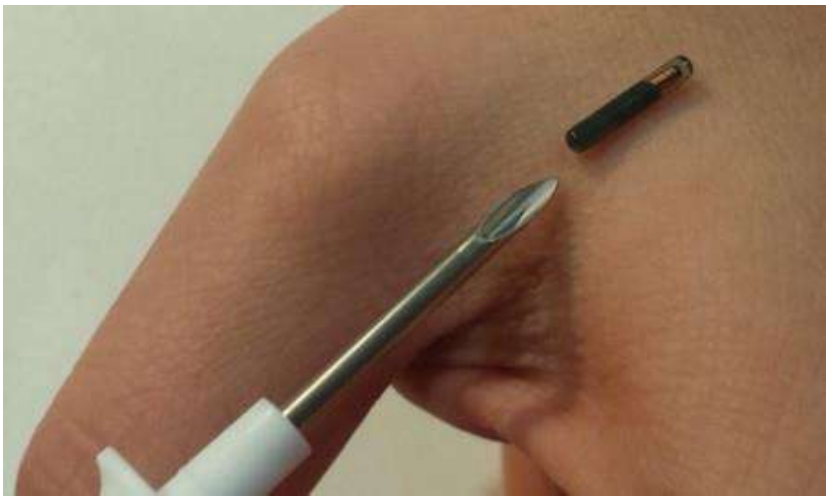


Figura 3 TAG NFC para incrustación en la piel. [6]

Dado los avances tecnológicos en los últimos 20 años, se ha implementado la electrónica en los sistemas de seguridad, y esto ha llegado a los sistemas de acceso, lo que provee una seguridad extra al sistema de acceso tradicional; Por lo tanto, los sistemas de control de acceso electrónico al igual que los sistemas tradicionales se clasifican por el nivel de seguridad que poseen.

2.1 Tipos de sistemas de control de acceso electrónico

La clasificación de los sistemas de control de acceso electrónico está organizada por las características de sus componentes y el nivel de seguridad que proveen, es por esto que se clasifican de la siguiente manera:

- Sistema autónomo
- Sistema gestionado
- Sistema corporativo

2.1.1 Sistemas autónomos

Los sistemas autónomos(figura 4) se caracterizan por proveer una seguridad electrónica baja, esto se debe a que están diseñados para negar o autorizar acceso mediante una clave global, es decir, un sistema tradicional de chapa y llave pero con llaves electrónicas, tal es el caso de las cajas fuertes con teclados numéricos, donde solo los usuarios conocen su clave, sin embargo, en este tipo de sistemas es imposible determinar quién ingresa pues no cuentan con gestión de usuarios; estos sistemas controlan cada acceso en el que son montados de manera independiente, es decir, no tienen comunicación ni relación entre sistemas.

Estos sistemas son fáciles de identificar ya que cuentan generalmente con 3 componentes principales los cuales son:

- Módulo de identificación general
- Una fuente de alimentación para los dispositivos
- Dispositivo de acceso (chapa eléctrica, abre puerta, chapa magnética, motor, etc.)

Figura 4 Sistema Autónomo [7]

2.1.2 Sistemas gestionados

El siguiente a describir es el sistema gestionado el cual se muestra un ejemplo en la figura 5; este permite tener un control de accesos preciso, restringido y de mayor seguridad que el sistema autónomo, debido a que aumentan la seguridad pues los módulos de acceso cuentan con registros de datos que permite saber quién o que ingresa, en que área y a en horario, además, los diferentes accesos de este sistema se encuentran conectados a una red lo que permite desde un solo punto la gestión de todos los accesos.

Las principales funciones que realizan estos sistemas son: la identificación única de usuario (clave personal), a diferencia de los sistemas autónomos este tipo de sistemas contiene un registro de los usuarios u objetos que ingresan a las áreas protegidas por el sistema, también cuentan con una base de datos donde se consultan los usuarios y registra los ingresos, además provee el control de diferentes accesos. Todo esto hace que los sistemas instalados en diferentes accesos estén conectados en una red de comunicación.

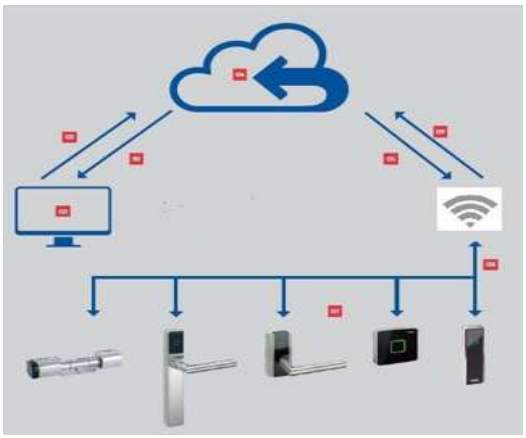


Figura 5 Sistema gestionado

Los sistemas gestionados cuentan con distintos componentes que se encargan de aumentar la seguridad del control de acceso, los cuales se mencionan a continuación:

- Módulo de identificación personal: estos módulos permiten identificación personal.
- Servidor: al contar con un servidor se puede tener el control de múltiples accesos controlados desde un solo componente
- Módulo de conexión con servidor: este puede ser de manera alámbrica, inalámbrica, bluetooth, wifi, radiofrecuencia, etc.
- Gestor de usuarios y accesos: cuentan con una base de datos que permite registrar usuarios y accesos.
- Fuente de alimentación: se encarga de alimentar a los componentes necesarios para el funcionamiento del sistema.
- Dispositivo de acceso: al ser un sistema electrónico el dispositivo de bloqueo tiene que ser electrónico (chapas eléctricas, contra chapas, motores, etc.).

2.1.3 Sistemas corporativos

El sistema que provee mayor seguridad es el corporativo; este sistema se caracteriza por tener diversos equipos de identificación de usuarios u objetos lo que proporciona un

incremento de seguridad, además, proveen el control de accesos múltiples conectados a una red, esto permite tener control de manera local, remota y monitorizada en cualquier momento, además incorpora el uso de cámaras de seguridad y alarmas (figura 6).

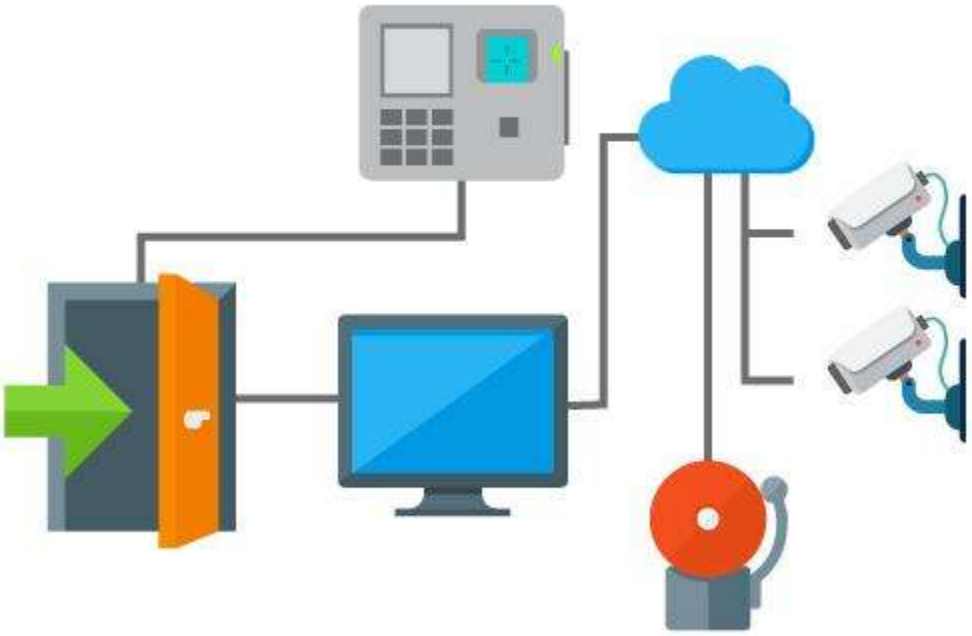


Figura 6 Sistema corporativo [8]

Al integrar en el sistema cámaras de seguridad, servidores, alarmas e identificación de alta seguridad. El sistema corporativo incrementa el nivel a un grado alto, y por lo tanto más costoso.

Si bien estos sistemas proveen más seguridad que los tipos de sistema anteriormente mencionados muchos de sus componentes son similares, la principal diferencia suele estar en que están programados para otorgar mayor seguridad y provén más funciones. Los principales componentes de los sistemas corporativos son:

- Módulos de identificación personal
- Cámaras de seguridad
- Servidores

- Conexión modulo-modulo
- Gestor de usuarios y accesos
- Fuentes de alimentación
- Dispositivos de acceso
- Dispositivos de acceso remoto
- Alarmas de seguridad

2.2 Dispositivos actuales de identificación

La identificación para el control de acceso es necesaria, con el paso de los años y el avance de la tecnología esta ha evolucionado a un grado casi imposible de duplicar, ahora se utilizan diferentes métodos o dispositivos para llevar a cabo esta tarea por lo que es importante definir que un dispositivo de identificación es aquel que mediante un lector permite la identificación de usuarios, objetos, animales, etc. Estos dispositivos pueden identificar características biológicas, claves personales, contraseñas, registros, etc.

Para el reconocimiento de usuarios en cualquier tipo de sistema de control de acceso electrónico, es necesario contar con al menos un dispositivo de identificación, por lo tanto, estos son fundamentales para el desarrollo de sistemas.

Los dispositivos de identificación más comunes son:

- Numéricos
- Biométricos
- Radiofrecuencia
- Magnéticos

2.2.1 Identificación Numérica

De los primeros dispositivos de identificación electrónica usados para sistemas de seguridad se encuentran los de identificación numérica, estos proporcionan una seguridad media-baja debido a algunos huecos o fallas de seguridad en el sistema. Estos dispositivos asocian un código numérico el cual puede ser un código personal o un código global para el acceso; Y debido a esto se producen los huecos de seguridad, al ser un código numérico asociado, cualquier persona con conocimiento del código podrá ingresar, lo cual no permite precisión en el control de usuarios.

Físicamente estos dispositivos cuentan con un teclado numérico de mínimo 10 caracteres esto depende del modelo de teclado que se use, además de un microcontrolador que almacena las contraseñas (figura 7).

Figura 7 Teclado de identificación numérica [9]

Actualmente este tipo de dispositivos se utiliza en cajas de seguridad electrónicas, accesos electrónicos, checadores de tiempo, etc. Estos dispositivos son compatibles con otros sistemas de identificación, se usan como manera de respaldo en caso de fallo del primer sistema.

2.2.2 Lectores biométricos

Hoy en día los dispositivos biométricos tienen fama de ser difíciles de corromper por que proveen una seguridad que ningún otro dispositivo puede ofrecer, sin embargo, generan un riesgo a la integridad física de los usuarios, ya que toman datos biológicos como medida de identificación.

Por ocuparse de la distinción, análisis y reconocimiento de rasgos biológicos mediante patrones de código, la biometría pertenece a una rama de las matemáticas estadísticas; esta tecnología se clasifica en dos tipos:

El primer tipo es la biometría estática, este tipo de biometría consiste en la medición de las características físicas de un individuo. Los sistemas biométricos más comunes de este tipo son el reconocimiento por huella dactilar, geometría de la mano, análisis de iris, retina y reconocimiento facial. Incluso en la actualidad es común encontrar los lectores de huella dactilar y el software de reconocimiento facial en dispositivos móviles como laptops y celulares.

Figura 8 Escáner de retina y huella dactilar

El segundo tipo es la biometría dinámica la cual consiste en la medición de rasgos de comportamiento del individuo (voz, movimientos corporales, etc.), se suelen encontrar en sistemas de reconocimiento de voz y manuscrito.

Los dispositivos de identificación biométrica suelen ser costosos, debido al alto grado de seguridad que proporcionan, estos dispositivos funcionan tomando una o varias muestras físicas, estas muestras son transformadas en una secuencia numérica cifrada, permitiendo la autenticación y verificación del usuario.

2.2.3 RFID

Los siguientes a describir son los dispositivos de identificación por radio frecuencia RFID (figura 9)por sus siglas en ingles Radio Frequency IDentification, estos más que dispositivos son sistemas ya que para funcionar se requiere un lector y un objeto a leer, el objeto a leer se le conoce como TAG, estos cuentan con la capacidad de almacenar datos en su memoria y suelen estar ocultas en tarjetas, celulares, incluso se pueden ingresar en la piel; por otra parte el lector es un receptor de datos, lo que los hace útiles para la identificación de usuarios

El modo de funcionamiento de los sistemas RFID se describe de la siguiente manera: La etiqueta TAG, que contiene los datos de identificación previamente grabados del objeto o usuario, genera una señal de radiofrecuencia al detectar el campo magnético del lector. Esta señal ya con información encriptada es captada por un lector RFID, este se encarga de leer la información, desencriptarla y pasarla en formato digital a la aplicación específica que utiliza RFID.

Figura 9 Sistema RFID y etiquetas RFID

El sistema RFID consta de los siguientes componentes:

- Etiqueta RFID: compuesta por una antena, un transductor radio y un chip. El propósito de la antena es permitirle al chip, transmitir la información de identificación de la etiqueta de manera encriptada.
- Lector de RFID: contiene una antena, un transceptor y un decodificador. El lector envía periódicamente señales para ver si hay alguna etiqueta en sus inmediaciones. Cuando capta la señal de una etiqueta, comprueba el password de esta, si es correcto, extrae la información la cual es enviada al subsistema de procesamiento de datos.
- Subsistema de procesamiento de datos o middleware RFID: proporciona los medios de proceso y almacenamiento de datos.

Basándose en la comunicación que establecen los dispositivos RFID se crea una tecnología la cual pretende acortar el rango de distancia de operación entre TAG y lector,

esto se hizo debido al phishing generado para decodificar la información de los tags, así es como nace la tecnología NFC que se describen a continuación.

NFC (Near Field Communication) es una tecnología inalámbrica de corto alcance (aprox. 5cm) que permite conectar dos dispositivos al emitir una señal, y que al mismo tiempo puede también recibir una señal (figura 3). Por lo que permite una lectura-escritura en ambos sentidos.

La tecnología NFC puede funcionar de dos formas diferentes:

- Activa: Los dos elementos que intervienen en la comunicación generan un campo electromagnético e intercambian los datos necesarios. Como sucede entre dos teléfonos celulares, celular smartwatch, llaves de presencia.
- Pasiva: Solo un dispositivo es capaz de generar un campo electromagnético. El otro dispositivo aprovecha el campo generado por el primero para recuperar la energía necesaria para enviar los datos. El ejemplo típico sería el del intercambio de datos entre un lector y una etiqueta NFC.

2.2.4 Bandas magnéticas

Una banda magnética es una banda oscura y está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina, las cuales almacenan cierta cantidad de información mediante una codificación determinada que polariza dichas partículas.

Los dispositivos de identificación que contienen banda magnética generalmente son tarjetas, esta banda lleva un código de identificación, para ser descifrado se requiere el contacto de esta con un lector de bandas y su uso actual es:

- Tarjeta de crédito y de débito.
- Cerraduras electrónicas.
- Vale como pago de un servicio.
- Tiempo de juego en una máquina.

En la actualidad las empresas están dejando de usar este tipo de tarjetas, debido a la facilidad para duplicar o robar la información de estas, otro problema es que la banda magnética suele dañarse con facilidad además de tener un desgaste considerable debido a su uso.

2.3 Descripción general del sistema SCARE

El sistema SCARE corresponde al tipo de sistemas gestionados, debido a que sus módulos de acceso están conectados a una red, se asignan claves personales y cuenta con un registro de usuarios. SCARE se diseña para funcionar con al menos un módulo RAB y un módulo CARE, sin embargo, el sistema puede soportar múltiples módulos CARE y uno o varios módulos RAB.

El módulo CARE tiene como función principal la detección de usuarios, la consulta de estos en la base de datos del sistema SCARE y otorgar o niega el acceso dependiendo de la respuesta de la consulta realizada. Este módulo se encuentra en los lugares donde se requiere controlar el acceso. Para la construcción de este módulo se utiliza un microcontrolador ESP8266, el cual está montado sobre una placa de desarrollo NODEMCU v3 lollin, un chip PN532 incorporado a un módulo NFC, un relevador para conexión del módulo de acceso, un led indicador de estado además de una etapa de potencia para alimentación del sistema de control.

Por otra parte, el módulo RAB tiene la función de gestionar usuarios en la base de datos, además de asignar la llave de registro personal (TAG) a cada uno de estos, este módulo se encuentra en propiedad del administrador del sistema y basta con solo un módulo para gestionar múltiples módulos CARE. El módulo RAB cuenta con un microcontrolador ATmega168 montado sobre una placa de desarrollo Arduino nano, también cuenta con un chip PN532 incorporado a un módulo NFC.

El procedimiento para el registro de usuarios es el siguiente:

El administrador del sistema da de alta mediante el software RAB al usuario registrando nombre, dependencia, días, horas, clave de lectura, bloque y lugares a los que tendrá acceso, el nombre de usuario se graba mediante el módulo de hardware RAB en un TAG, realizado esto el software RAB registra al usuario en la base de datos. El módulo CARE al detectar un TAG realiza los procedimientos necesarios para identificar el bloque, mediante la identificación de una contraseña, de lograr la lectura de usuario el sistema CARE realiza la consulta a la base de datos, la cual regresara una respuesta de acceso correcto o acceso denegado generando un registro en ambos casos.

Si el modulo CARE no detecta red o no encuentra el servidor, este entrará en modo respaldo por lo que solo permitirá el acceso a los usuarios registrados como super usuarios

Capítulo 3 Hardware

En este capítulo se presenta el diseño y construcción de los módulos físicos que conforman el sistema SCARE; además, se describen los elementos electrónicos necesarios, así como su integración en los módulos CARE y RAB.

El sistema SCARE cuenta con dos módulos de hardware, los cuales son:

- Control de Acceso y Registro Electrónico (CARE)
- Registro de Altas y Bajas (RAB)

Los módulos del sistema SCARE pueden ser replicados las veces que sean necesarios, es recomendable contar con solo un módulo RAB y los módulos CARE para cada área que se requiera tener un control.

3.1 Modulo CARE

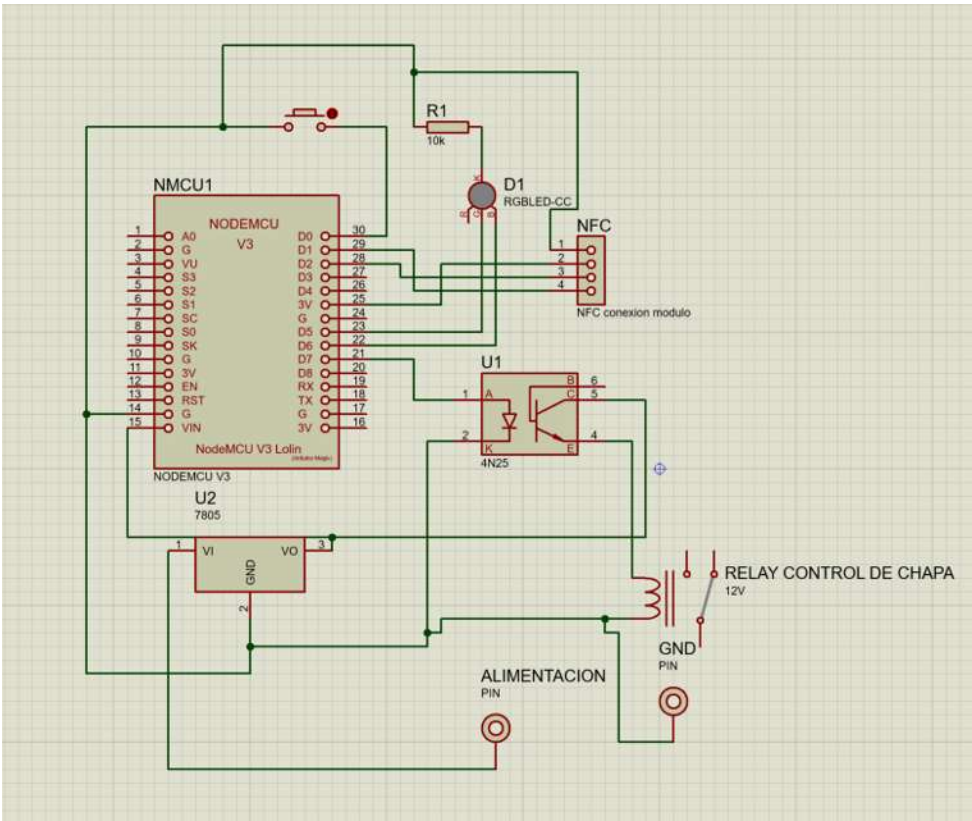


Figura 10 Diagrama modulo CARE [3]

Para el desarrollo del sistema CARE (figura 10) se diseña una etapa de potencia que acopla el voltaje a 5v, la mayoría de módulos de accesos electrónico (chapas eléctricas, contrachapas eléctricas, chapas magnéticas, etc.) funcionan con un voltaje de 12 VDC, por lo que se requiere la etapa de acoplamiento de potencia para reducir el voltaje a 5vdc debido a que es el voltaje de operación de NodeMCU, para cumplir esto se utiliza un regulador de voltaje 7805. Las entradas de alimentación de 5volts y GND ingresan a la placa por lo pines 14(G) y 15(Vin).

NodeMCU entrega a las salidas de alimentación 3.3v, este voltaje alimenta a la placa NFC module v3 en los pines 25(3v) y 14(G). Para la transmisión de información del módulo NFC a la placa de desarrollo se utilizan los pines 29(D1) este se conecta al pin 4 (SDA) y

28(D2) conectado al pin 3(SCL),esto debido a que se pueden configurar como SDA y SCL, pues la comunicación se realiza por i2c; para que sea posible la comunicación el módulo NFC cuenta con pines de selección de tipo de comunicación, estos s e configuran teniendo el switch1 en 1 es decir a la derecha mientras el switch2 en 0 es decir a la izquierda(figura 11).

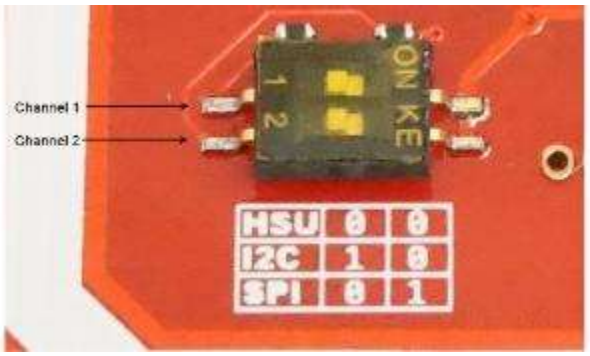


Figura 11 Pines de selección de comunicación NFC [3]

En todos los sistemas es importante saber el estado en el operan los componentes para descartar errores, es por esto queo el sistema CARE cuenta con un led RGB indicador de estado, este se conecta en los pines 23(D5) al pin correspondiente verde(G) y 22(D6) al azul (B), para protección del led se agregó una resistencia al cátodo de 330 ohm conectada a tierra.

El pin de control del módulo de acceso (chapa eléctrica) es el pin 21 (D7), debido a que el relevador utilizado se energiza a 5v para su operación y NodeMCU aporta 3.3v se utiliza un optoacoplador para ingresar el voltaje necesario.

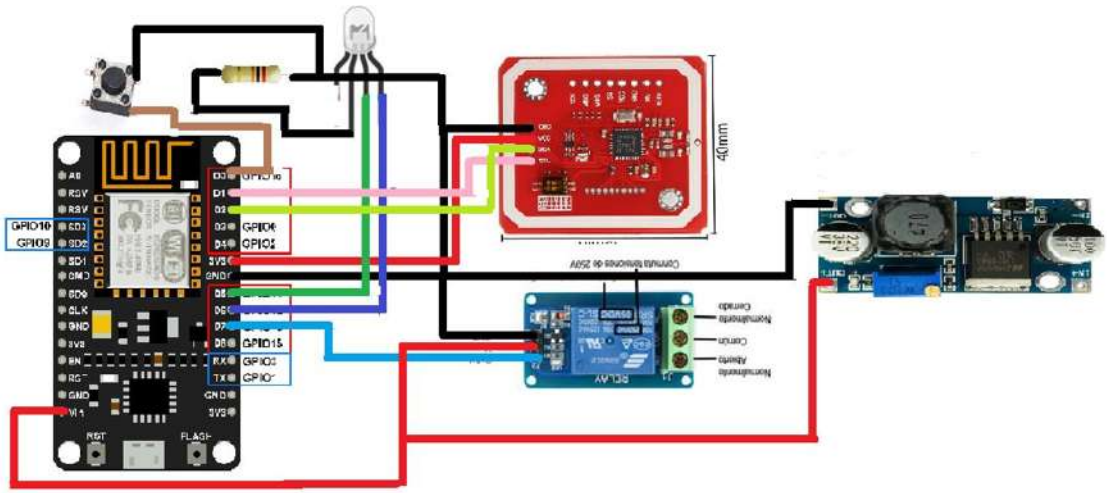


Figura 12 Representación física sistema CARE [3]

Este módulo (CARE) se debe encontrar instalado cerca del acceso del área (puerta) que se requiere controlar ya que este sistema se encarga de leer los TAGS, realizar consultas a la base de datos, y dependiendo de la respuesta determinar el ingreso de usuarios al área protegida por el sistema.

Estados de operación

Los estados de operación del modulo CARE pueden ser vistos si este es conectado a un ordenador mediante el puerto USB y utilizando el monitor serie de Arduino, sin embargo, estando instalado el modulo se ve la necesidad de instalar un indicador de estados (LED), los estados de operación son los siguientes:

ESTADO	CODIGO
Fallo del lector NFC	LED en verde parpadeante
Fallo de servidor	LED en azul constante

Fallo de red	LED en Azul parpadeante
Operación normal	LED apagado con destellos en verde

Tabla 1Estados de operación

3.2 Modulo RAB

Con el sistema CARE se obtiene el control de acceso electrónico, por lo que el sistema RAB se encarga de la gestión del sistema, es decir, asignar usuarios, horarios y áreas de ingreso, debido a que funciona como llave para el software RAB, además este módulo permite la lectura y escritura de las etiquetas NFC Mifare Classic 1k de 13Mhz.

Este módulo permite leer, modificar y borrar cualquier tag NFC Mifare Classic 1k (tag comercial), en cualquier bloque y sector específico siempre y cuando el sector cuente con permiso de lectura, escritura y se conozca la contraseña (figura 13).

La conexión de este software es sencilla pues solo cuenta con un microcontrolador Atmega169 incorporado a una placa Arduino nano para su desarrollo, ya que este cuenta con el tipo entradas requeridas para la comunicación I2C con el módulo NFC MODULE V3; RAB conecta una placa de desarrollo Arduino nano al NFC MODULE V3 mediante I2C, por lo que es necesario configurar el módulo NFC en i2c.

La conexión es la siguiente: los pines utilizados son: 5v, GND, A4 y A5 y se conectaron de la siguiente manera:

```
Arduino a NFC

5v=VCC ------- GND=GND -------- A4=SDA -------- A5=SDL
```

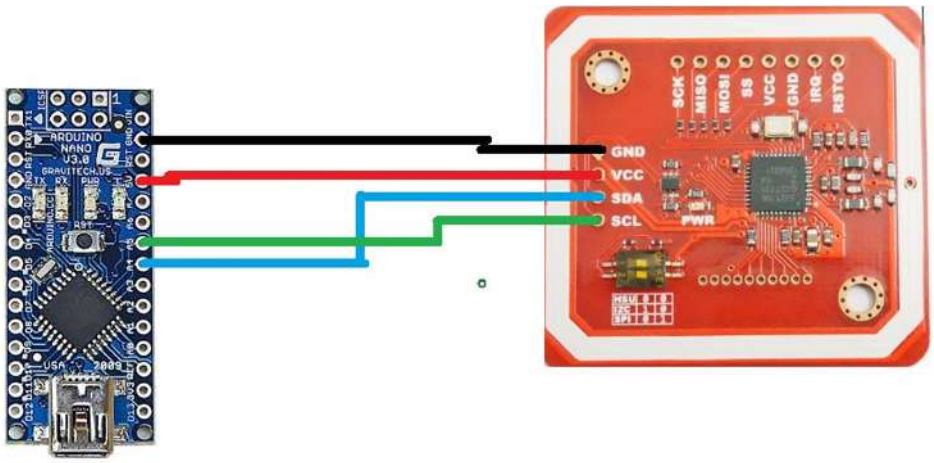


Figura 13 Conexión Arduino nano -NFC module v3 [3]

Este módulo debe de estar en posesión del administrador del sistema ya que funciona como llave para registrar nuevos usuarios, un solo modulo RAB es suficiente para el sistema SCARE.

Los procesos que realiza este modulo se pueden observar mediante el monitor serie en Arduino o en el software RAB en la pestaña de configuración avanzada.

3.3 Placas de desarrollo para Microcontroladores

Para automatizar un sistema se requiere de un componente que ejecute instrucciones específicas y es aquí donde entran los microcontroladores los cuales están montados para su programación en placas de desarrollo, las placas de desarrollo son circuitos impresos compuesto por un microcontrolador y un circuito acoplador que permite programar el microcontrolador montado. Estas placas se desarrollan para proporcionar al desarrollador la capacidad de programar el microcontrolador con funciones específicas de acuerdo a la finalidad de un proyecto, esto convierte al microcontrolador la base del proyecto.

3.3.1 Placa de desarrollo “NodeMCU V3 lollin”

Para la elaboración del módulo CARE se requiere de una conexión al servidor y debido a que el sistema SCARE es un sistema gestionado, se optó por agregar un módulo Wi-Fi ya que esta tecnología permite una conexión multipunto además de brindar mayor seguridad al sistema y una fácil instalacion. Por esta razón la placa de desarrollo será NodeMCU.

NodeMCU es una placa de desarrollo abierta, a nivel de software y de hardware, esta placa de desarrollo tiene incorporado un chip de nombre SoC (system on a Chip) que dentro contiene un microcontrolador.

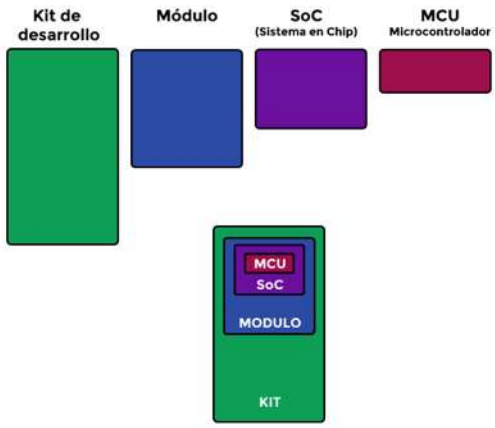


Figura 14 Esquema NodeMCU [4]

Las principales características de NodeMCU son:

- Incorpora una MCU de 32-bit de bajo consumo (Tensilica L106)
- Módulo Wifi de 2.4 GHz
- RAM de 50 kB
- 1 entrada analógica de 10-bit (ADC)
- 17 pines de entrada y salida GPIO (de propósito general)

- Conversor Serie-USB.

El módulo encargado del procesamiento de información es el ESP8266, de este existen diferentes versiones, las cuales se diferencian por permitir acceder a los pines y conectores del SoC y del microcontrolador. Estos módulos incorporan una memoria flash para almacenar los programas o sketch y una antena WIFI.

Esta placa de desarrollo cuenta con un mapa de pines elaborada por el fabricante, el mapa de pines se muestra en la imagen 3-2.

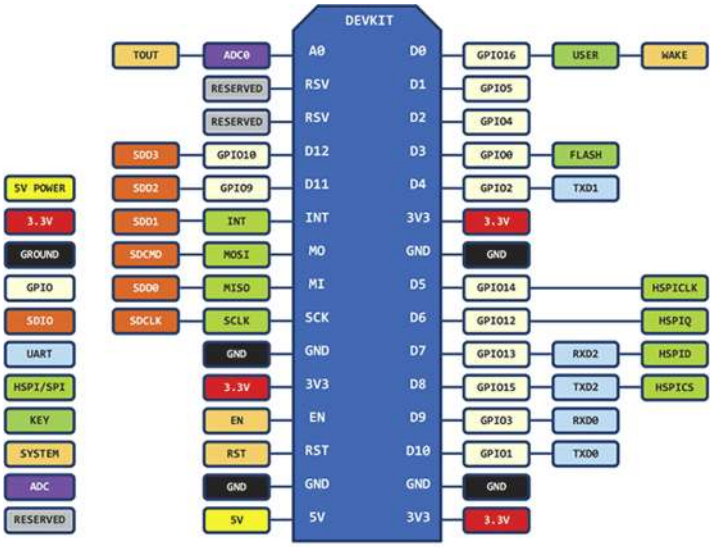


Figura 15 Mapa de pines NodeMCU v3 lollin [4]

El mapa de pines muestra las conexiones de manera indirecta con el microcontrolador ESP8266 ya que este es un chip Wi-Fi con protocolos TCP/IP completa y posee una unidad de microcontrolador MCU (Micro Controller Unit) producida por el fabricante chino Espressif Systems. En la imagen 3-3 se muestran el mapa de pines del ESP8266-12e si se realiza una comparación de la imagen 3-2 se nota la conexión que hay entre los pines de NodeMCU y ESP8266 (figura 16).

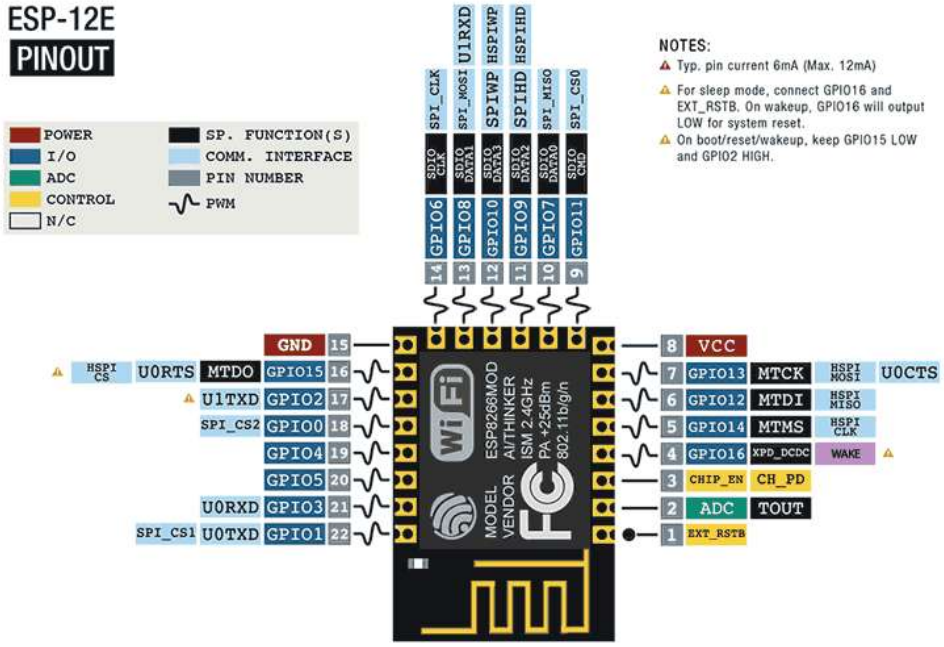


Figura 16 Mapa de pines de ESP8266-12E [5]

Algunas de las características principales del ESP8266 son:

- Utiliza un voltaje de alimentación de 3.3v de DC.
- Tiene un voltaje de entradas y salidas de 3.3v de DC.
- CPU tensilica Xtensa LX3 de (32 bits).
- Reloj interno operar a 80Mhz y 160Mhz.
- Memoria RAM de 96kb.
- Memoria flash de 4Mb.
- 17 pines digitales.
- 1 pin análogo (0v – 1v).
- Wi-fi direct (P2P).
- Soporta conexión SPI, UART, I2C.
- Soporta conectividad IPV4.
- Protocolos TCP/UDP/HTTP/FTP.

La velocidad de transmisión de paquetes del ESP8266 es menor a 2 milisegundos, esto hace que el módulo genere respuesta rápida por lo que el usuario apenas notara un ligero retardo, y su consumo de potencia es Standby es menor a 1mW, esta característica permite conectarlo a una batería de respaldo por largo tiempo, por lo tanto, es ideal para el sistema SCARE.

3.3.2 Arduino

Una de las placas de desarrollo más famosas y comerciales es Arduino, Arduino cuenta con diferentes placas de desarrollo, varían en tamaño, componentes, velocidades, tipos de conexión, puertos de conexión, pines adc, pines digitales etc. Para el sistema RAB se requiere un microcontrolador con las conexiones suficientes para soportar una comunicación i2c por lo que Arduino nano es el indicado.

Arduino nano es una placa de desarrollo de tamaño compacto. basada en el microcontrolador ATmega166. Esta placa posee las mismas capacidades que un Arduino UNO, tanto en potencia del microcontrolador como en conectividad, solo se ve recortado en su conector USB, conector jack de alimentación y los pines cambia un formato de pines header.

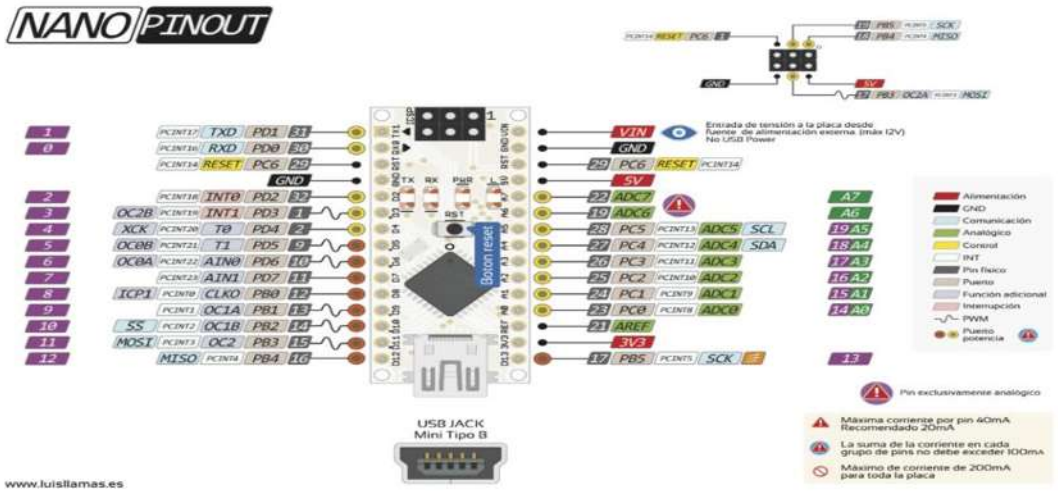


Figura 17 Mapa de pines de salida de Arduino Nano [6]

Las principales características de ATmega166 se describen a continuación:

- Fabricante: Atmel (Microchip).
- Voltaje de operación: 1.8 a 5.5 VDC.
- Arquitectura de CPU: 8 bit AVR
- Memoria flash: 32 KB.
- Memoria RAM: 2 KB.
- EEPROM: 2 KB.
- Frecuencia de operación: 16 Mhz.
- 14 pines de entrada/salida digital
- 6 entradas analógicas
- Interfaces: UART, TWI, SPI.
- Temperatura de Operación: -40° a 85° C

3.4 NFC

La identificación de usuarios es necesaria para el sistema SCARE ya que permite tener un control de los mismos, se utiliza la tecnología NFC pensando en salvaguardar la integridad física del usuario, cosa que no proporcionan los identificadores biométricos.

El módulo de identificación de usuario es un NFC-RFID V3, este está construido alrededor de un chip NXP PN532, el cual el fabricante NXP proporciona la documentación correspondiente para desarrolladores, este módulo es fabricado por la compañía ELECHOUSE.

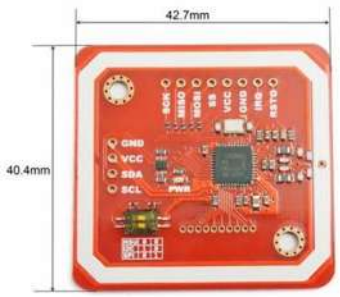


Figura 18 NFC module v3 ELECHOUSE [7]

Las características principales de NFC module v3 ELECHOUSE son:

- Dimensiones de 40.4mm x 42.7mm de largo.
- Admite conexión I2C, HSU y SPI.
- Lectura y escritura RFID, comunicación P2P entre dispositivos similares, NFC en Android.
- El lector / escritor RFID/NFC soporta:
    - Tarjetas Mifare 1k, 4k, Ultralight y DesFire
    - Tarjetas ISO / IEC 14443-4 como CD97BX, luz de CD, Desfire, P5CN072 (SMX)
    - Tarjetas Innovision Jewel como la tarjeta IRT5001.
    - Tarjetas FeliCa como RCS_860 y RCS_854
- 2 cm ~ 7 cm de distancia de lectura.
- Switch de nivel a bordo, estándar 5V TTL para I2C y UART, 3.3V TTL SPI.
- Rango de operacion3.3v hasta 5.3v

Este módulo cuenta con una antena integrada, la cual proporciona un rango de lectura de aproximadamente 5 cm, además, cuenta con 2 switch selectores de modo de comunicación.

El módulo NFC (Figura 18) incorpora un chip PN532, este es un chip transceptor diseñado para comunicación inalámbrica, está basado en un microcontrolador 80c51 y soporta 6 tipos de operaciones diferentes, las cuales son:

- ISO / IEC 14443A / MIFARE (Lectura - escritura)
- Lectura - Escritura FeliCa
- Lectura - Escritura ISO / IEC 14443B
- Emulación de Tarjeta ISO / IEC 14443A / MIFARE Classic 1K o MIFARE Classic 4K
- Emulación de tarjetas FeliCa.
- ISO / IEC 18092, ECMA 340 punto a punto

El chip PN532 implementa un demodulador y un decodificador para para señales de tags y transpondedores compatibles con ISO / IEC 14443A / MIFARE. Este chip admite modo emulación de tags MIFARE tanto classic 1k como Classic 4k, además permite una comunicación inalámbrica utilizando tags MIFARE la cual lo hace a una velocidad de trasferencia de 424kbits/s en ambas direcciones.

Algunas de las funciones del PN532 son:

- Demodular y decodificar señales codificadas FeliCa,
- Maneja los frame FeliCa
- Detección de errores
- Compatible con la comunicación inalámbrica
- Velocidades de transferencia FeliCa hasta 424 kbit / s en ambas direcciones.

Además, el PN532 admite las capas 2 y 3 de comunicación ISO / IEC 14443 B para lectura y escritura, pero no admite anticolisión. En el modo emulador de tarjeta, el Pn532 funciona como lector o escritor según la interfaz de tarjeta FeliCa o ISO / IEC 14443A / MIFARE. La comunicación en modo pasiva o activa, ofrece la posibilidad de comunicarse con otro dispositivo compatible con NFCIP-1

El Pn532 se puede conectar a una antena externa para leer como lo incorpora el módulo NFC v3, escribir o emular tags, sin ningún componente activo adicional. Los tipos de comunicación que soporta son I2C, SPI y HSU, el chip incorpora un regulador de baja caída de voltaje, gracias al cual permite conectar el chip a una batería, además de un interruptor interno de alimentación para suministrar energía al circuito integrado.

3.4.1 TAGS

Los TAGS son etiquetas ocultas en pequeños stickers, tarjetas, llaveros, etc. Estas permiten almacenar datos en distintos bloques, está información está cifrada, y se requiere un dispositivo especial para poder acceder a estos datos.

Estos dispositivos pueden configurarse con 3 modos de seguridad, 1 por bloque de manufactura, por llave A y por llave B.

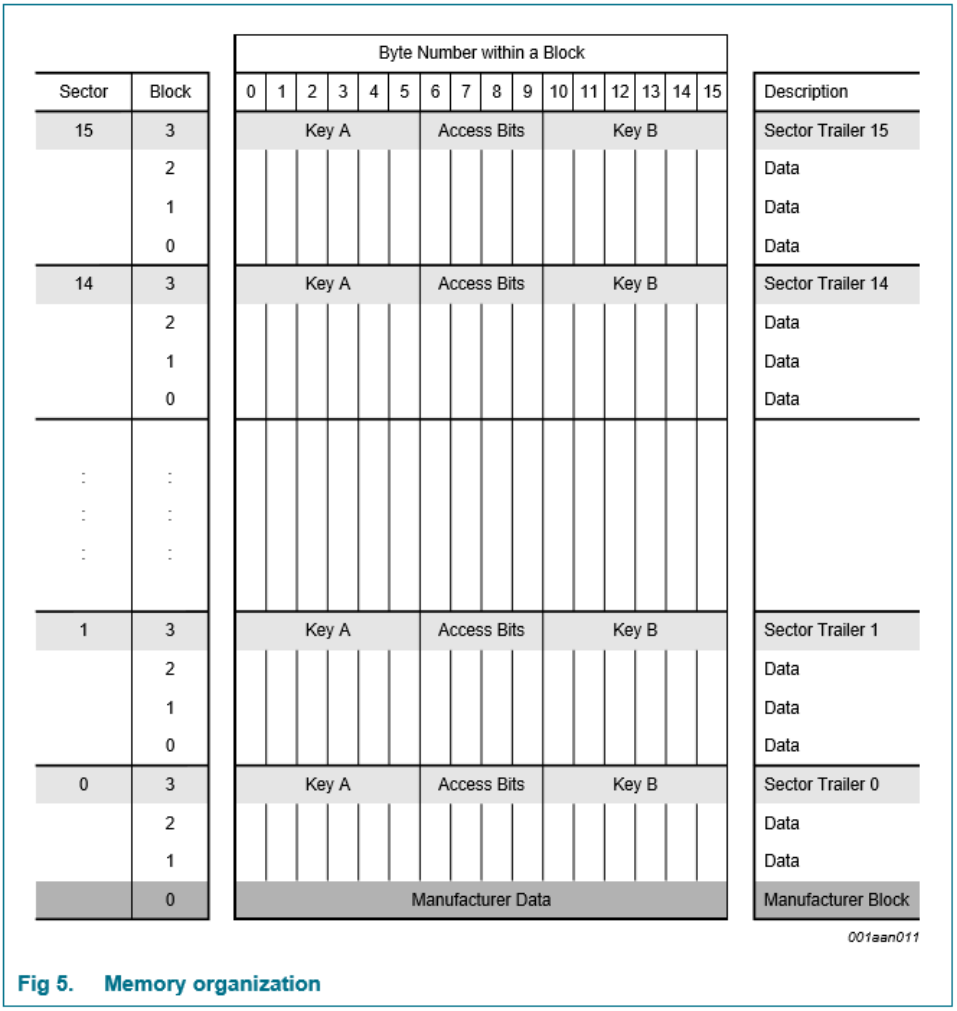


Fig 5. Memory organization

Figura 19 Organización de memoria MIFARE Classic 1k [8]

Aunque existen muchos tipos de tags, el más comercial es el que cuenta con una frecuencia de operación de 13.56MHz, MIFARE Classic 1k, este contiene internamente 16 sectores de 4 bloques cada uno, por tanto, se obtienen 64 bloques de los cuales solo 48 pueden almacenar hasta 16 bytes de información cada uno, este TAG se utiliza para el desarrollo del sistema SCARE.

Los 16 sectores tienen 6 bytes para escribir una contraseña en la llave A, 6 bytes para contraseña en llave B, y 4 bytes que se encargan de gestionar los modos de operación de los tags.

Los modos de operación son los siguientes:

- Lectura de bloque
- Escritura de bloque
- Decremento del contenido del bloque
- Incremento del contenido del bloque
- Restaurar bloque
- Transferencia de contenido.

Al realizar una lectura real a un TAG de los mencionados con anterioridad se obtuvieron los siguientes datos:

```
[ 00|01|02|03|04|05|06|07|08|09|0A|0B|0C|0D|0E|0F ] direcciones de memoria
[ 3E:07:6B:65:37:88:04:00:C8:34:00:20:00:00:00:15 ] Addr. 00 : UID0-UID3 / MANUFACTURER
[ 13:00:4A:51:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 01 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 02 : DATA
[ 00:00:00:00:00:00:78:77:88:C1:00:00:00:00:00:00 ] Addr. 03 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 04 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 05 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 06 : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 07 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 08 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 09 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 0A : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 0B : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 0C : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 0D : DATA
```

```
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 0E : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 0F : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 10 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 11 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 12 : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 13 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 14 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 15 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 16 : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 17 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 18 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 19 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 1A : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 1B : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 1C : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 1D : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 1E : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 1F : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 20 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 21 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 22 : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 23 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 24 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 25 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 26 : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 27 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 28 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 29 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 2A : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 2B : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 2C : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 2D : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 2E : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 2F : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 30 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 31 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 32 : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 33 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 34 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 35 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 36 : DATA
```

```
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 37 : KEYA / ACCESS / KEYB
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 38 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 39 : DATA
[ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 ] Addr. 3A : DATA
[ 00:00:00:00:00:00:FF:07:80:69:FF:FF:FF:FF:FF:FF ] Addr. 3B : KEYA / ACCESS / KEYB
```

Capítulo 4 Software desarrollado

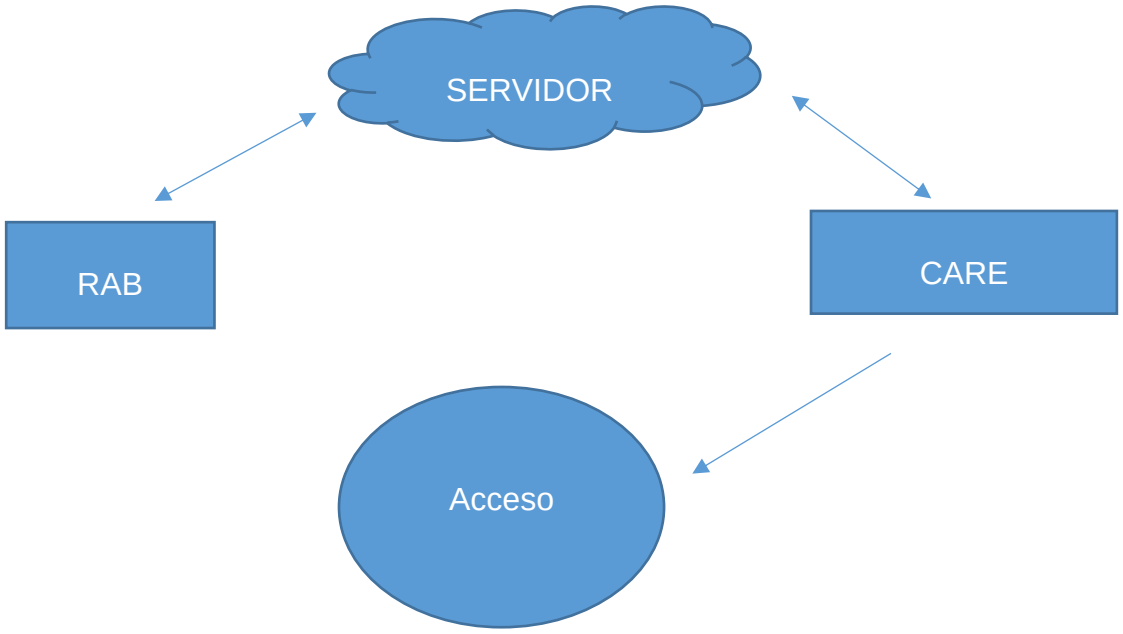
4.1 Introducción

Software se define como un conjunto de programas y rutinas que permiten a un sistema realizar distintas funciones. Por lo tanto, Para el sistema SCARE se diseña y desarrolla un software de pc en NETBEANS (java), el cual realiza una conexión a la base de datos, para otorgar permisos de usuarios, realizar consultas y al mismo tiempo permite gestionar el módulo de hardware RAB.

Para una conexión entre el módulo CARE y la base de datos se desarrolla un software HTML y un software PHP, estos permiten realizar consultas y elaborar un registro de accesos sean o no otorgados.

El módulo de hardware RAB cuenta con su propio software el cual tiene varias funciones, las cuales dependen del software de pc RAB. El módulo de hardware CARE cuenta con software específico para realizar las funciones de registro y consulta.

El sistema SCARE funciona de la siguiente manera.



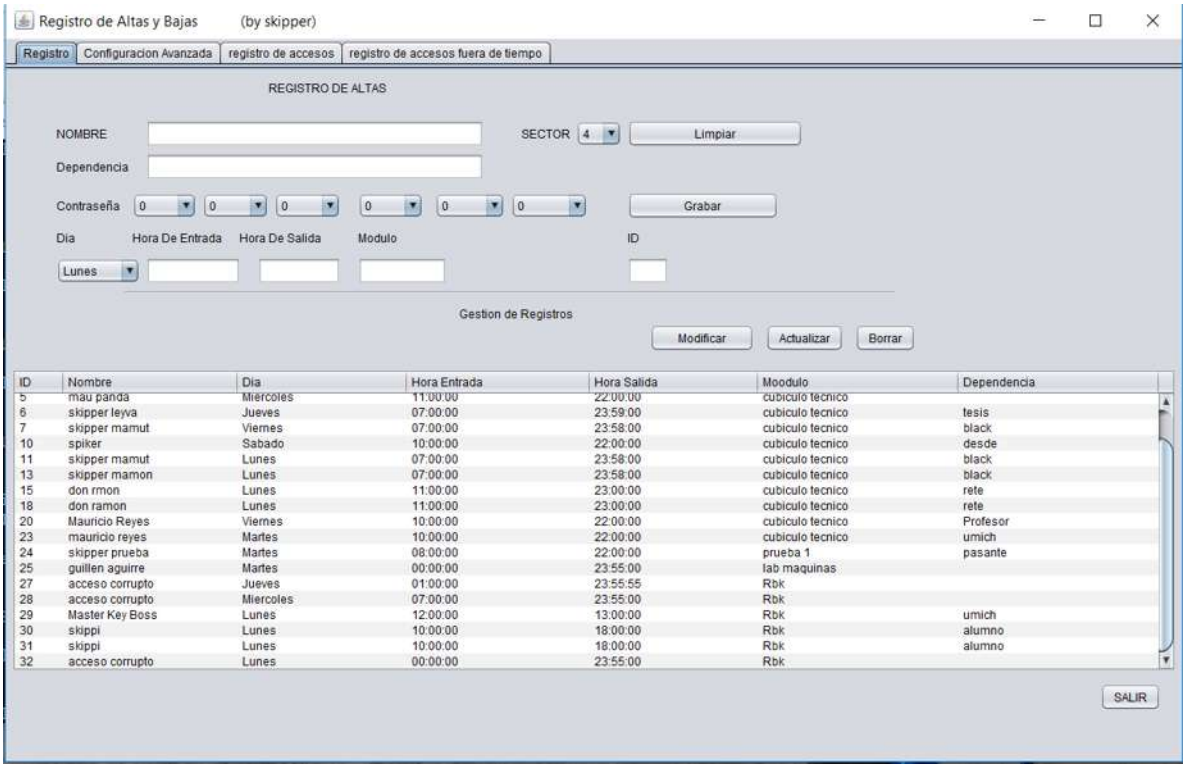
4.2 Software de PC

Debido a que el sistema está pensado para usarse por cualquier persona, SCARE cuenta con un software con interfaz grafica creado en NetBeans (java) que lo hace amigable con el usuario, este software realiza la gestión del sistema en general y cuenta con dos modos de operación, para ingresar al software es indispensable tener activo el servidor (apache) y la base de datos (MariaDB), además de conocer la dirección IP donde estos se encuentran estos.

Figura 20 Login RAB sin base de datos activa [3]

El software RAB opera en dos modos, el modo “Registro de Altas Editor” funciona cuando el sistema no detecta el módulo de hardware RAB conectado algún puerto COM del pc, este modo de operación permite bajas, modificar usuarios, horarios entrada-salida, áreas denominadas ChipID, días y dependencia, además ver y borrar registros de entrada autorizada y no autorizada.

Mientras tanto el modo “Registro de Altas” es utilizado al detectar el módulo de hardware RAB en algún puerto COM del pc, este modo permite las mismas funciones del modo editor, además permite dar altas de usuarios, leer, escribir, cualquier bloque y sector de memoria de los tags MIFARE Classic 1k, cambiar contraseñas, asignar llave A o llave B y reiniciar de fábrica los tags.



ID	Nombre	Dia	Hora Entrada	Hora Salida	Moodulo	Dependencia
5	mau panda	Miercoles	11:00:00	22:00:00	cubiculo tecnico	
6	skipper leyva	Jueves	07:00:00	23:59:00	cubiculo tecnico	tesis
7	skipper mamut	Viernes	07:00:00	23:58:00	cubiculo tecnico	black
10	spiker	Sabado	10:00:00	22:00:00	cubiculo tecnico	desde
11	skipper mamut	Lunes	07:00:00	23:58:00	cubiculo tecnico	black
13	skipper mamon	Lunes	07:00:00	23:58:00	cubiculo tecnico	black
15	don rmon	Lunes	11:00:00	23:00:00	cubiculo tecnico	rete
18	don ramon	Lunes	11:00:00	23:00:00	cubiculo tecnico	rete
20	Mauricio Reyes	Viernes	10:00:00	22:00:00	cubiculo tecnico	Profesor
23	mauricio reyes	Martes	10:00:00	22:00:00	cubiculo tecnico	umich
24	skipper prueba	Martes	08:00:00	22:00:00	prueba 1	pasante
25	guillen aguirre	Martes	00:00:00	23:55:00	lab maquinas	
27	acceso corrupto	Jueves	01:00:00	23:55:55	Rbk	
28	acceso corrupto	Miercoles	07:00:00	23:55:00	Rbk	
29	Master Key Boss	Lunes	12:00:00	13:00:00	Rbk	umich
30	skippi	Lunes	10:00:00	18:00:00	Rbk	alumno
31	skippi	Lunes	10:00:00	18:00:00	Rbk	alumno
32	acceso corrupto	Lunes	00:00:00	23:55:00	Rbk	

Figura 21 Software RAB [3]

El funcionamiento en seudocódigo es el siguiente:

```
Seleccionar IP
Seleccionar Puerto COM
Si (IP == servidor  && base de datos==DATA) {
        Si (puerto com = no disponible)
         {
                Modo editor activo
           }
        Si no {
        Modo normal}
        }

Si no {

base de datos no encontrada

Cerrar programa}
```

Para que “Registro de altas” registre un nuevo usuario, este software realiza dos conexiones, la primera es a la base de datos a través de una biblioteca llamada “mysql-connector-java-5.1.24-bin.jar”, si bien no es la versión más reciente de esta biblioteca, es útil para la base de datos, la segunda conexión que realiza es con el módulo de hardware RAB a través de las bibliotecas “PanamaHitek_Arduino-3.0.0.jar” desarrolladas por Panamá Hitek, esta biblioteca permite abrir el puerto COM que está conectado el módulo RAB.

4.2.1 Login

A modo de evitar ingreso de terceros al sistema y como medida de seguridad adicional, el software cuenta con una selección de IP y puerto COM, la cual es esencial para que RAB funcione, para IP se utiliza 4 combo box los cuales tienen una numeración de 0 a 255 para poder añadir cualquier dirección IP, para la selección del puerto COM se utiliza 1 combo box, este combo box solo muestra los puertos COM disponibles al momento de iniciar el programa

Figura 22 Login RAB [3]

4.2.2 Registro de altas

El sistema SCARE Facilita la gestión del sistema mediante la interfaz el ”Registro de altas”, este cuenta con 1 campo de texto de 16 caracteres para ingresar nombre de usuario nuevo, 1 campo de texto de 15 caracteres para ingresar la dependencia del usuario, un combo box llama sector este se encarga de selección el lugar donde se almacena la llave de lectura y asignar el lugar de escritura del nombre, la contraseña se define por 6 combo box con numeración del 0 a 255, un combo box para el selector de día y 3 campos de texto para asignar hora de entrada, hora de salida y módulo de ingreso, cuenta con dos botones de ejecución uno que permite grabar la información en la base de datos y en la tarjeta, y otro que limpia el campo de texto. Imagen 4-4.

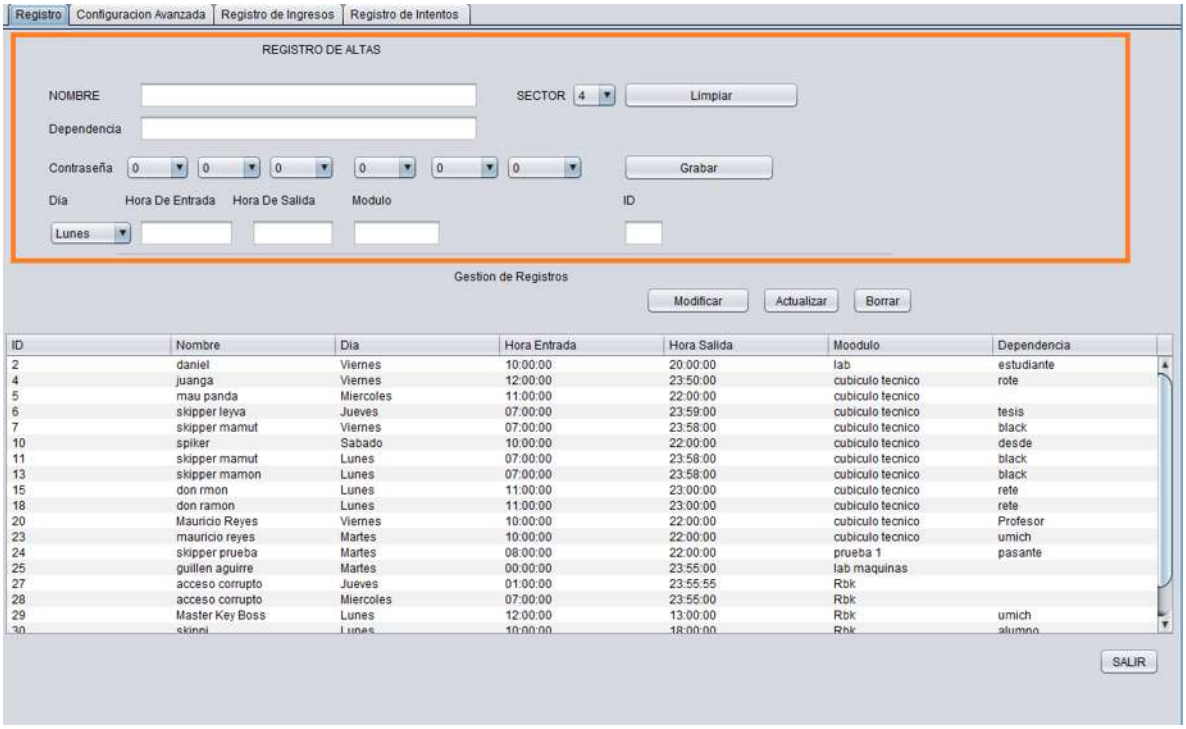


Figura 23 Interfaz RAB con botones de ejecución [3]

Los botones de la interfaz realizan las acciones siguientes:

- El botón “limpiar” envía la instrucción de escribir en los espacios de texto (nombre, dependencia, hora de entrada, hora de salida y modulo) un carácter en blanco es decir cualquier información que tengan estos espacios será sustituida por espacio en blanco, lo que da como resultado la limpieza de los espacios.

Esta instrucción no causa alteración en la base de datos ni en los tags a escribir. El botón “grabar” por su parte envía 2 instrucciones una al microcontrolador del módulo RAB y otra a la base de datos.

La primera instrucción emitida es para la base de datos, esta instrucción emite los datos de manera ordena de la siguiente manera:

```
1.-Nombre (obtenido de campo de texto nombre)
2.-Dia (obtenido del combo box día)
3.-Hora de entrada (obtenido del campo de tiempo hora entrada)
4.-Hora salida (obtenido del campo de tiempo hora salida)
5.-ChipID (nombre del lugar de acceso, obtenido del lugar modulo)
6.-Dependencia (obtenido del campo de texto dependencia)
```

Realizada la instrucción la base de datos muestra un cuadro de dialogo con el texto “Éxito”.

La segunda instrucción va dirigida al microcontrolador a través del puerto serial, esta instrucción lee el campo de texto nombre, los combos boxes de la contraseña (6 combo box de 0 a 255 cada uno) y el bloque sector.

La instrucción ejecuta el modo de operación 1 del software programado para el hardware RAB de nombre “escritura de nombre y password” el cual envía los datos en el siguiente orden al microcontrolador:

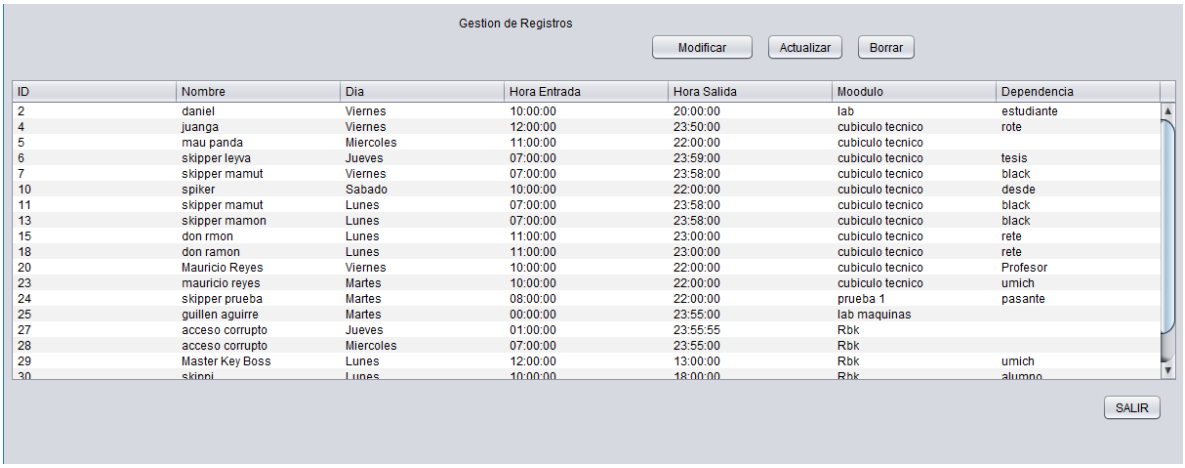
```
1.- Numero de Modo de operación para RAB (modo 1 escritura de nombre y
password).
2.- Numero de sector.
```

```
3.- Contraseña nueva de sector.
4.- Nombre de usuario.
```

Como es necesario saber los usuarios registrados la parte “Gestión de registros” muestra la tabla Users de la base de datos, esta tabla esta ordenada por fecha de ingreso y muestra nombre, día, hora entrada, hora salida, modulo, dependencia estos son parámetros modificables, además muestra 3 botones, “modificar” permite seleccionar un usuario y cambiar los datos de la tabla, “actualizar” actualiza la tabla, “borrar” borra el usuario seleccionado, por ultimo cuenta con un botón “salir” el cual cierra el programa.

El “modo editor” no permite leer, escribir, ningún tag y tampoco dar altas a la base de datos.

Por consiguiente, la tabla (figura 24) que muestra este apartado es obtenida directamente de la base de datos, al ejecutar el programa este realiza una consulta con la base de datos para obtener dicha tabla.



ID	Nombre	Dia	Hora Entrada	Hora Salida	Moodulo	Dependencia
2	daniel	Viernes	10:00:00	20:00:00	lab	estudiante
4	juanga	Viernes	12:00:00	23:50:00	cubiculo tecnico	rote
5	mau panda	Miercoles	11:00:00	22:00:00	cubiculo tecnico	
6	skipper leyva	Jueves	07:00:00	23:59:00	cubiculo tecnico	tesis
7	skipper mamut	Viernes	07:00:00	23:58:00	cubiculo tecnico	black
10	spiker	Sabado	10:00:00	22:00:00	cubiculo tecnico	desde
11	skipper mamut	Lunes	07:00:00	23:58:00	cubiculo tecnico	black
13	skipper mamon	Lunes	07:00:00	23:58:00	cubiculo tecnico	black
15	don rmon	Lunes	11:00:00	23:00:00	cubiculo tecnico	rete
18	don ramon	Lunes	11:00:00	23:00:00	cubiculo tecnico	rete
20	Mauricio Reyes	Viernes	10:00:00	22:00:00	cubiculo tecnico	Profesor
23	mauricio reyes	Martes	10:00:00	22:00:00	cubiculo tecnico	umich
24	skipper prueba	Martes	08:00:00	22:00:00	prueba 1	pasante
25	guillen aguirre	Martes	00:00:00	23:55:00	lab maquinas	
27	acceso corrupto	Jueves	01:00:00	23:55:55	Rbk	
28	acceso corrupto	Miercoles	07:00:00	23:55:00	Rbk	
29	Master Key Boss	Lunes	12:00:00	13:00:00	Rbk	umich
30	skippi	Lunes	10:00:00	18:00:00	Rbk	alumno

Figura 24 Gestión de Registros de usuarios [3]

Este apartado muestra 3 botones superiores y uno inferior de nombre “salir”, al ejecutar esta orden el programa recibe la instrucción de cerrarse.

En un sistema siempre existen las modificaciones por lo cual se añade el botón “modificar”, para usarlo es necesario seleccionar la fila, una vez seleccionada la fila, los datos

que en esta aparecen se moverán al acampo de texto permitiendo realizar las modificaciones necesarias.

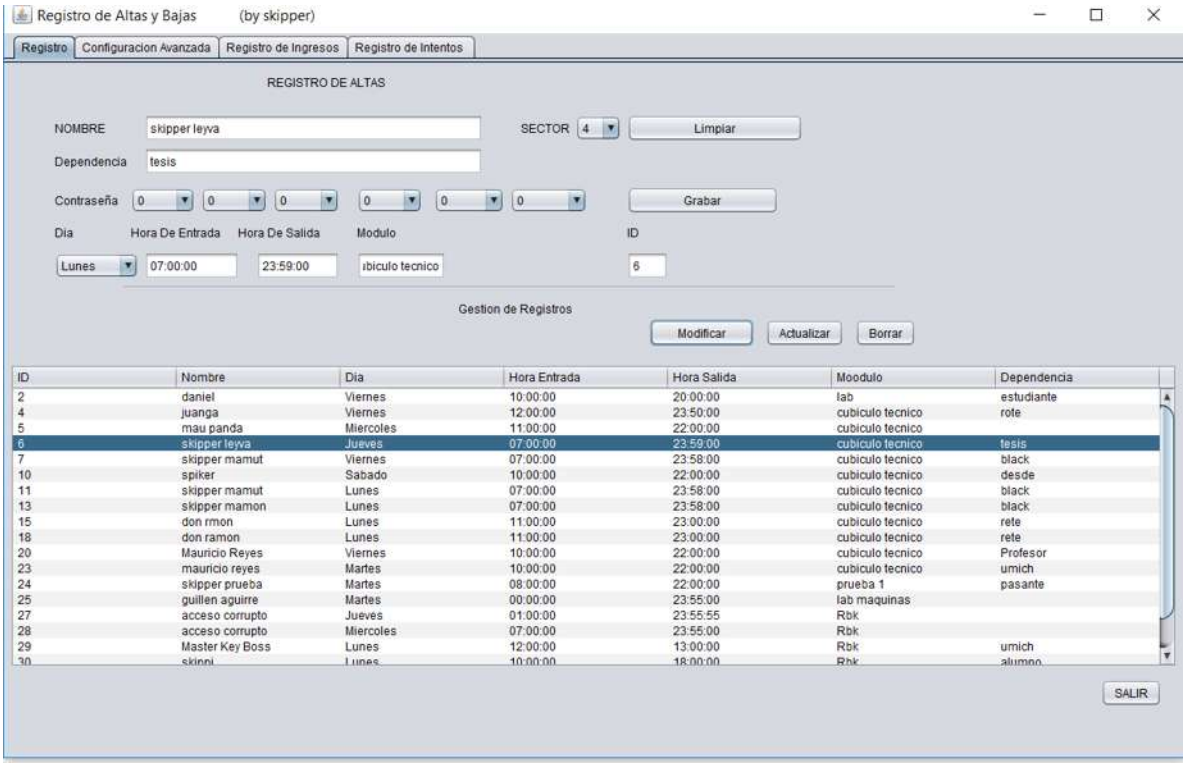


Figura 25 Modificación de usuario [3]

Para que la modificación se concrete es necesario presionar el botón “actualizar”, este enviara una instrucción en la base de datos, esta toma todos los datos de la parte “Registro de altas”, esta orden además realiza la lectura de tabla, de este modo queda la tabla de gestión de registros actualizada.

Para dar de baja un usuario se añadió el botón “borrar” esta borra el registro completo seleccionado, esta instrucción ordena a la base de datos para eliminar el registro.

4.2.3 Configuración avanzada

Existe un apartado especial para la gestión de tags a este se le denomina "Configuración avanzada" (figura 26), este solo está disponible en modo de operación normal ya que requiere el módulo de hardware RAB para operar.

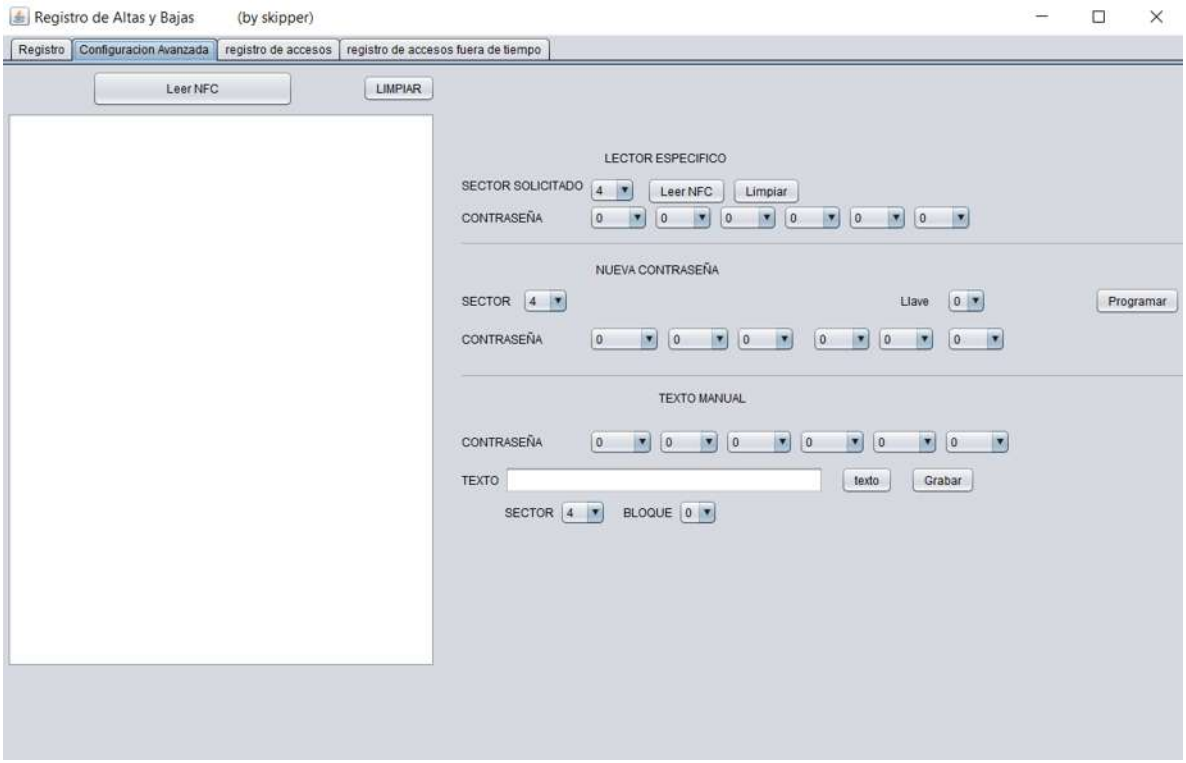


Figura 26 RAB configuración avanzada [3]

Configuración avanzada cuenta con un botón "leer NFC" (Figura 27), esta instrucción envía el modo de operación 3 "lectura completa" al módulo RAB, este se encarga de leer los 63 bloques de las tarjetas con clave por default (0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF).

Mientras tanto el botón "limpiar" se encarga de borrar todos los datos mostrados en la tabla.

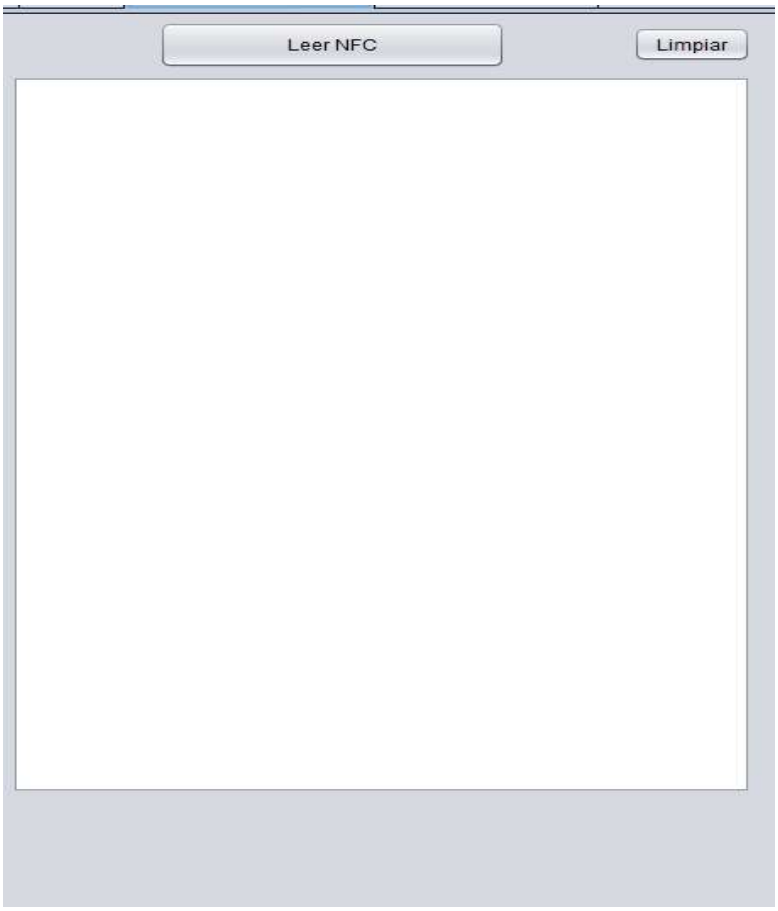


Figura 27 Botón Leer NFC y tabla de lectura

Para leer un lector especifico con una contraseña distinta esta la opción “LECTOR ESPECIFICO” (Figura 28), esta permite seleccionar el sector, ingresar contraseña, leer el sector seleccionado con sus respectivos bloques, limpiar el sector y los bloques seleccionados. Al limpiar le sector regresa su contraseña original (0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF) y los bloques se registran en 00.

Figura 28 RAB lector especifico [3]

El botón “leer NFC” envía la instrucción 5 “lectura específica”, además envía los datos de manera ordena al módulo RAB.

```
1.- Numero de Modo de operación.
2.- Numero de sector solicitado.
3.- Contraseña del sector (6 números de 0 a 255 cada uno).
```

El módulo RAB regresa como respuesta la información de cada bloque, esta información se muestra con el número del bloque leído, su información y su contraseña de bloque en el monitor del software RAB.

Este apartado cuenta con el botón “limpiar” esta instrucción permite restaurar los datos de fábrica de un sector en específico, el cual ha sido modificado, para activar esta instrucción es necesario contar con la contraseña del sector. Esta instrucción envía el número 4 de modo de operación limpieza de sector, el envió de datos es ordenado.

```
1.- Numero de Modo de operación.
2.- Numero de Sector.
3.- Contraseña (6 números de 0 a 255 cada uno).
```

El siguiente apartado es “NUEVA CONTRASEÑA” este permite asignar contraseñas a tags independientes del sistema, permite también seleccionar el sector a escribir y asignar la llave A (0) o la llave B (1).

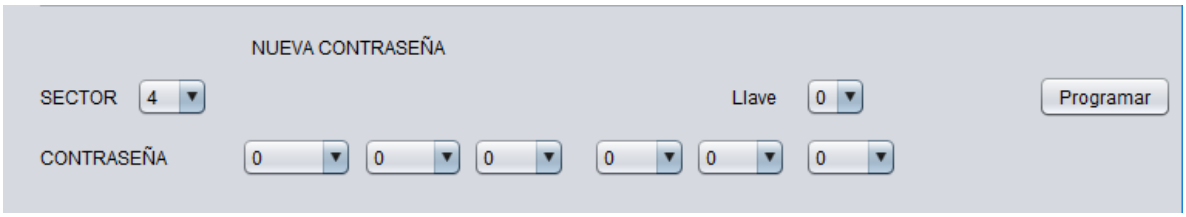


Figura 29 RAB nueva contraseña [3]

Para llevar a cabo la instrucción, este apartado tiene el botón “Programar”, este envía el modo de operación 2 “Escritura de password al módulo RAB”, además envía los datos en el siguiente orden:

```
1.- Numero de modo de operación.
2.- Numero de sector.
3.- Contraseña (6 números de 0 a 255 cada uno).
4.- Código llave A o llave B.
```

El último apartado de configuración avanzada es “TEXTO MANUAL” (figura 30) la cual requiere de la contraseña del sector a escribir, así como el sector y el bloque en el cual se escribirán los 16 caracteres.

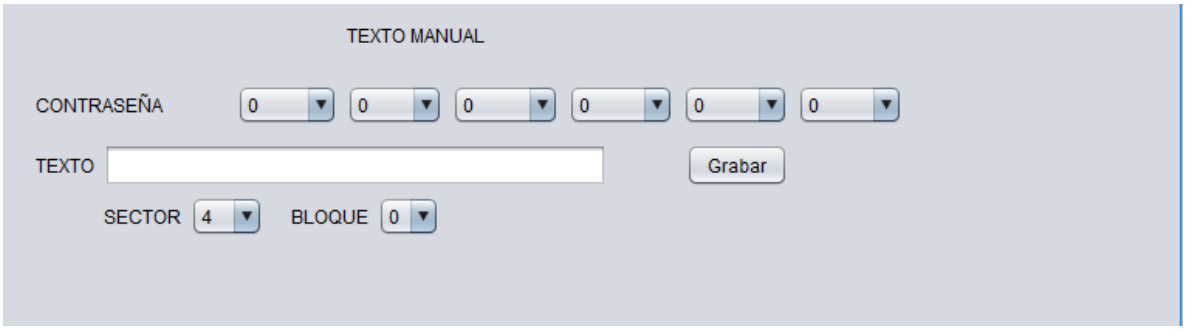


Figura 30 RAB texto manual [3]

Este apartado cuenta con el botón “Grabar”, esta instrucción envía el modo de operación 6

“texto manual”, además envía de forma ordenada los siguientes datos:

```
1.- Código de modo de operación.
2.- Numero de sector.
3.- Numero de bloque.
4.- Contraseña (6 números de 0 a 255 cada uno).
```

Una vez realiza la instrucción regresa en el monitor “proceso correcto”.

4.2.4 Registros

La pestaña denominada registro de accesos muestra la tabla de ingresos de usuarios que accedieron en tiempo, lugar y día, y esta ordena por ID, Usuario, Fecha, Hora y lugar de acceso (ChipID), esta pestaña solo permite la instrucción “borrar” la cual funciona seleccionando el registro.

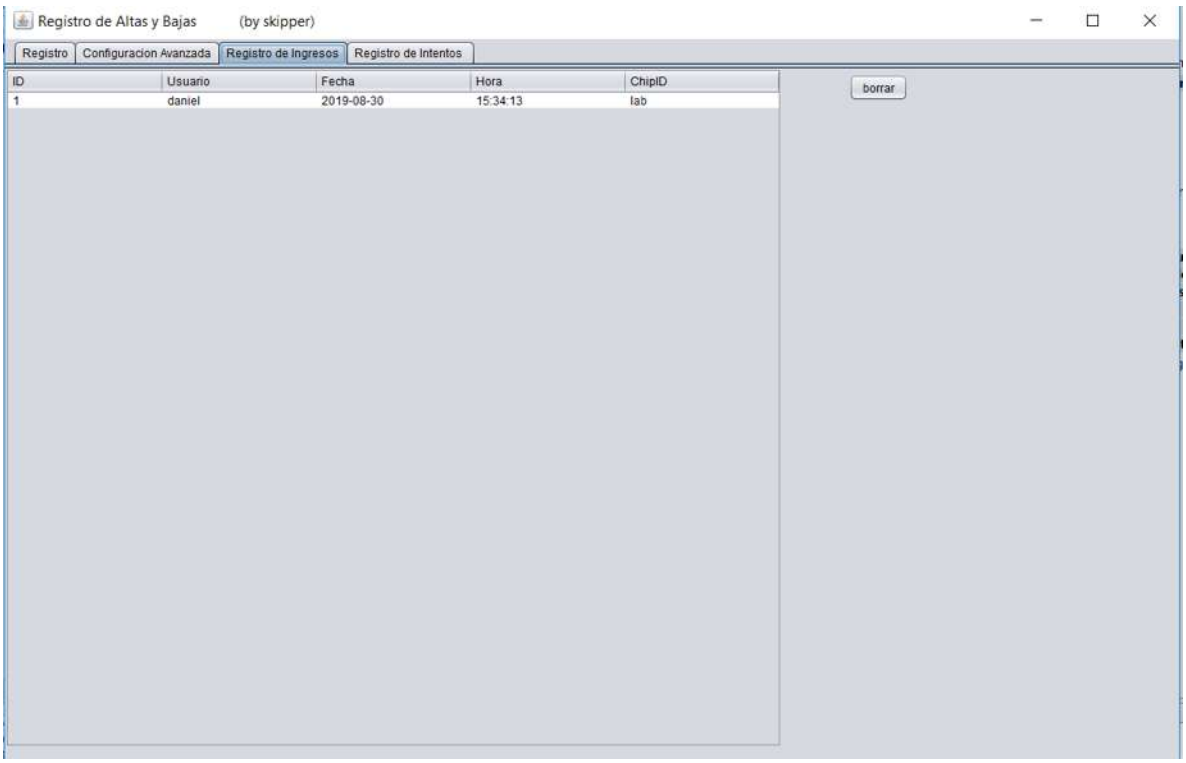


Figura 31 RAB registro de ingresos [3]

Esta instrucción envía la instrucción “DELETE” a la base de datos especificando el registro de usuario a borrar.

La pestaña de nombre Registro de intentos muestra una tabla con las mismas características que Registros de ingresos, esta tabla muestra los intentos de ingresos realizados a los módulos fuera de tiempo, día o lugar, al igual que la pestaña 3 solo permite borrar el registro una vez este sea seleccionado.

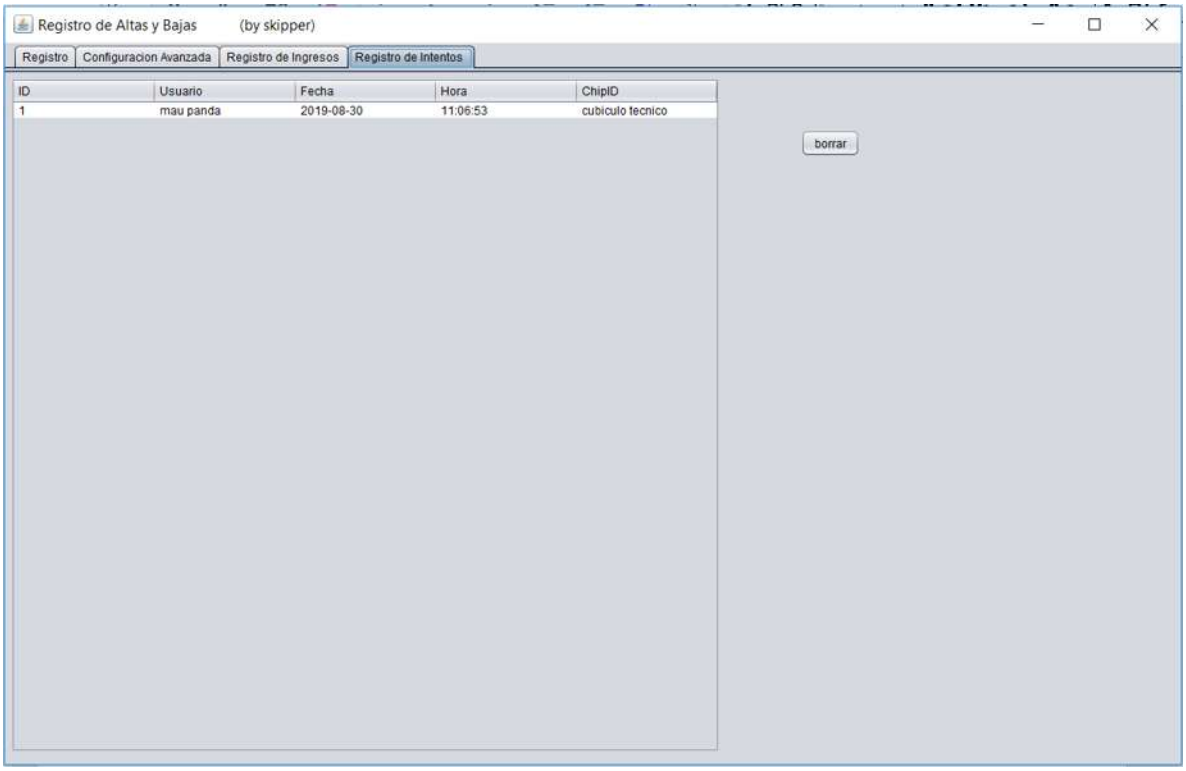


Figura 32 RAB Registro de intentos [3]

4.3 Servidor y base de datos

En la primera versión de prueba la base de datos se montó mediante XAMPP, ya que cuenta con un servidor (Apache), una base de datos (MariaDB) y un intérprete de lenguaje como lo es php.

Figura 33 XAMPP [3]

La figura 33 indica que el servidor (Apache) está operando, en ese momento está opera de manera local, por lo que no permite conexiones externas al servidor, debido a su configuración de protección.

Esta configuración se modifica en la siguiente ruta C:\xampp\apache\conf\extra\http-xampp el archivo lleva como nombre httpd-xampp.con, otra manera de ingresar al archivo es en configuración de XAMPP.

Las líneas de código que autorizan el acceso remoto son las siguientes:

```
</Directory>
 Alias /phpmyadmin "C:/xampp/phpMyAdmin/"
 <Directory "C:/xampp/phpMyAdmin">
     AllowOverride AuthConfig
```

```
    Require local
    ErrorDocument 403 /error/XAMPP_FORBIDDEN.html.var
</Directory>
Alias /webalizer "C:/xampp/webalizer/"
<Directory "C:/xampp/webalizer">
    <IfModule php7_module>
         <Files "webalizer.php">
               php_admin_flag safe_mode off
         </Files>
    </IfModule>
    AllowOverride AuthConfig
  #  Require local
    ErrorDocument 403 /error/XAMPP_FORBIDDEN.html.var
</Directory
```

Con esto se obtiene acceso desde cualquier dispositivo conectado a la red local, ingresando la IP del servidor se obtiene la imagen principal XAMPP.

Figura 34 PHPMyAdmin [3]

Para la parte de base de datos se utiliza un manejador de nombre phpmyadmin proporcionado por XAMPP. PhpMyAdmin cuenta con una lista de bases de datos creadas, SCARE trabaja con la base de datos llamada “SCARE” la cual cuenta con 3 tablas: notime, timedata, users (figura 35).

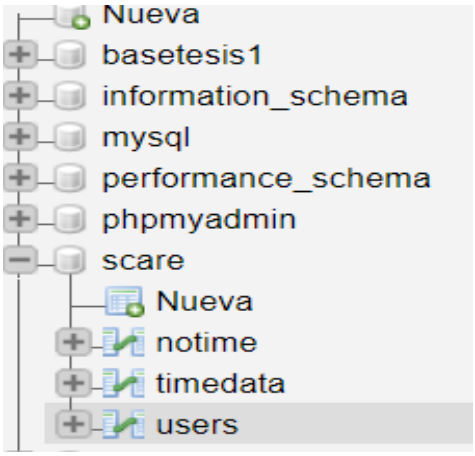


Figura 35 Base de datos y tablas [3]

La tabla notime y timedata se estructura con 4 filas, la tabla notime muestra los intentos de acceso a módulos RAB para los cuales no se tiene permiso de día, hora, usuario o lugar, la tabla timedata muestra los usuarios que accedieron al lugar en hora y día.

Numero	Nombre	Tipo	Extra
1	ID	Int(11)	Auto incrementable
2	Usuario	Varchar(20)	--
3	Fecha	Timestamp	Fecha actualizable
4	ChipID	Varchar(20)	---

Tabla 2 Tabla de Resgistros base de datos

La tabla users está compuesta de 7 filas, esta tabla es la encargada de almacenar los usuarios, módulos, días, dependencia y horas entrada-salida.

La tabla se estructuro de la siguiente manera:

Numero	Nombre	Tipo	Extra
1	ID	Int(11)	Auto incrementa
2	Nombre	Varchar(16)	--
3	Dia	Varchar(9)	--
4	HoraEntrada	Time	--
5	HoraSalida	Time	--
6	Modulo	Varchar(20)	--
7	Dependencia	Varchar(15)	--

Tabla 3 Tabla de Usuarios

4.4 Php y HTML

El módulo CARE debe comunicarse con la base de datos, por tanto, se crean 3 archivos, un HTML, un php y un archivo .ini que guarde la configuración de parámetros del servidor y base de datos, estos están alojados en el servidor Apache y realizan la consulta y registro de usuarios mediante el módulo CARE instalado en los accesos.

El archivo de nombre “index.html” permite probar la conexión remota a la base de datos desde cualquier dispositivo con wi-fi, este archivo recibe un usuario y un lugar de acceso (ChipID).

Este software es la conexión visual (frontend) entre el usuario y el software php (Figura 36).

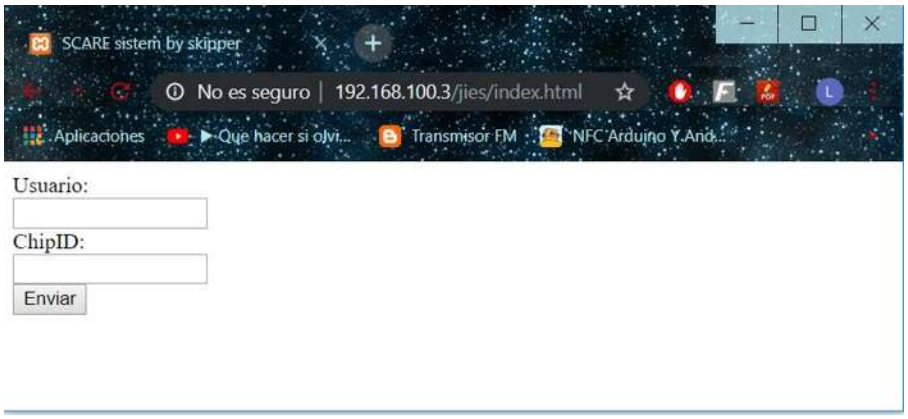


Figura 36 Pagina HTML de SCARE

El software “ejecute.php” recibe los parámetros usuario y ChipID, además agrega día y hora de la ciudad de México para realizar la consulta en la base de datos.

La consulta realizada por “ejecute.php” responde a la siguiente línea de seudocódigo

```
“Selecciona de usuarios
Donde Nombre = parámetro de usuario
Y Modulo = parámetro ChipID
Y Día = día del servidor
y hora este entre Hora de Entrada y Hora de Salida”
Si recibe una respuesta = 0 es decir no encontró ninguna coincidencia regresara en la pantalla un mensaje “Acceso Denegado\r”
```

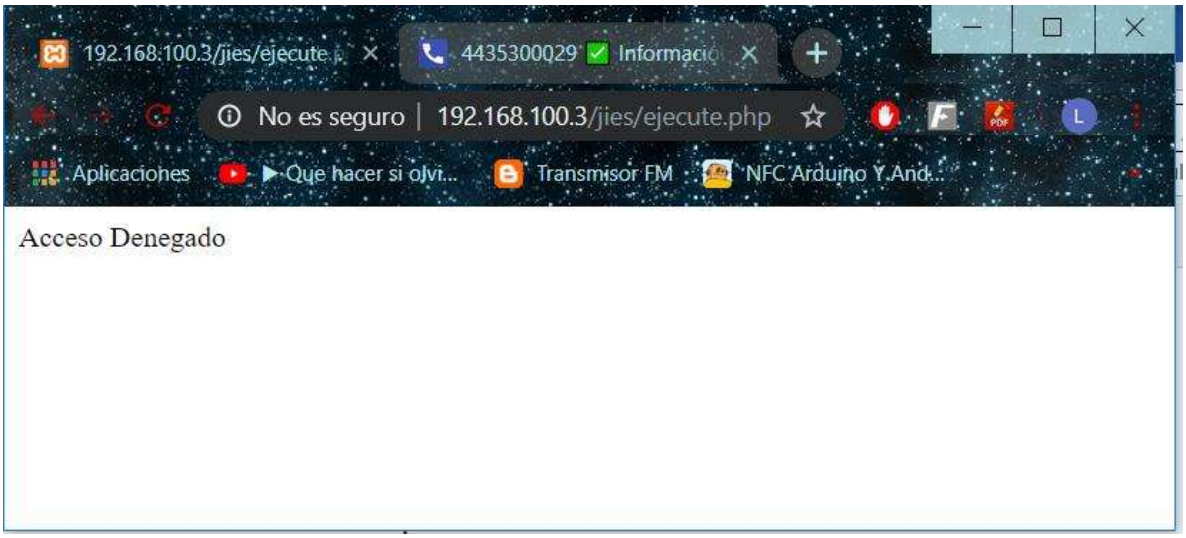


Figura 37 Respuesta del sistema

Si recibe la respuesta > 1 es decir encontró alguna coincidencia regresara en la pantalla un mensaje “Accesoo\r” es el carácter \r no lo muestra, sin embargo, es indispensable ya que el sistema CARE detecta este como carácter de terminación.

El software “config.ini” guarda la dirección id de la base de datos, nombre de la base de datos, usuario y contraseña.

4.5 Software RAB

El módulo RAB cuenta con su propio software, este software hace comunicación directa a través del puerto serial (COM) con el software de PC Registro de Altas y Bajas (RAB) para la modificación de datos en los tags NFC.

La comunicación realizada entre el software de PC RAB y el microcontrolador se describe de la siguiente manera, RAB PC da una instrucción a través del puerto serie, esta hace la selección de modo de operación, después comienza a transmitir los datos escritos o seleccionados en PC RAB al microcontrolador.

Este software permanece en modo de espera hasta recibir una instruccion de operación.

El software tiene 6 diferentes modos de operación, el primer dato que recibe determina el modo de operación a seguir, estos modos de operación dependen en su totalidad del software de PC RAB.

Los modos de operación son los siguientes:

Modo 1 Escritura de nombre y password

El modo 1 de operación escribe el nombre obtenido en el campo de texto de PC RAB, el bloque seleccionado y la contraseña nueva, por tanto, el microcontrolador recibe los parámetros en el siguiente orden:

1.- Número de bloque.

```
temp=Serial.read();
```

2.-Contraseña (6 números que van de 0-255 cada uno)

```
Serial.readBytes(newpass,6);
```

3.-Nombre de usuario (máximo 16 caracteres).

```
Serial.readBytes(Name,16);
```

Obtenidos los datos se procede a la verificación del tag con contraseña de fábrica, para escribir el nombre el software realiza una resta de 3 al número de sector, esto permite escribir en el bloque 1 el nombre de usuario y la contraseña del sector en su respectivo lugar.

Este modo de operación funciona de la siguiente manera.

```
Leer sector
Leer contraseña nueva
Leer nombre
Bloque = sector – 3
```

```
Detecta tag
Si (tag = 1) {
     Identificación de sector con llave de fabrica
     Si (identificación =1) {
          Escribe contraseña nueva
          Escribe nombre
        Si (escritura = 1) {
             Limpia el buffer
            Imprime “proceso correcto”}}}
```

Los datos recibidos son almacenados en el buffer de memoria del microcontrolador para después ser usados en la escritura de tags, una vez terminada la escritura el software limpia el buffer de almacenamiento y regresa a su ciclo de espera.

Modo 2 escritura de password

El modo 2 de operación realiza la escritura de password de manera manual, es decir se puede asignar una contraseña a cualquier sector, y puede escribir en llave A o en llave B.para este modo de operación el sector a modificar contraseña tiene que contar con la contraseña de fábrica.

Los parámetros son enviados en el orden siguiente:

1. Número de Sector

```
nbloquepas=Serial.read();
```

2. Contraseña (6 números de 0-255 cada uno).

```
Serial.readBytes(newpass,6);
```

3. Llave A o llave B.

```
Cc=Serial.read();
```

El funcionamiento de este modo de operación es el siguiente

```
Leer sector
Leer contraseña
```

```
Leer llave
Si (llave =1) {
       contraseña es de llave B
}
Detecta tag
Si (tag = 1) {
     Identificación de sector con llave de fabrica
     Si (identificación =1) {
         Escribe nueva contraseña}
         Si (escritura = 1) {
             Limpia el buffer
            Imprime “proceso correcto”}}}
```

De esta manera se graba la contraseña en cualquier sector específico.

Para la selección de llave b el software hace un arreglo para ordenar los datos en bits de la llave b. Una vez realizada la escritura de la nueva contraseña realiza una limpia del buffer de almacenamiento y regresa a modo espera.

Modo 3 Lectura de tags

El modo 3 de operación se encarga de realizar una lectura completa del tag es decir lee los 63 bloques que contiene el tag, siempre y cuando la clave de cada sector este escrita de fábrica (0xFF,0xFF,0xFF,0xFF,0xFF,0xFF), este modo de operación solo soporta los tags MIFARE_CLASSIC 1k.

Los bloques de memoria con contraseña distinta a la de fabrica aparecen como “contraseña distinta xx” y su número de bloque.

Este modo de operación solo recibe la orden de ejecución y su funcionamiento es el siguiente:

```
Contador n = 0
Si (contador es <=63) {
       Lee bloque n
       Imprime bloque
       Imprime contenido
       N+1}
```

Este modo de operación no recibe más datos por el puerto serie, por tanto, no es necesario limpiar el buffer

El modo 4 limpieza de sector

El modo de operación 4 se encarga de borrar un sector y los 3 bloques que lo conforman de manera específica, es decir, regresa los parámetros a su estado de fábrica. para realizar esta función es indispensable saber la contraseña del sector a borrar.

Los datos recibidos por el puerto serie del microcontrolador son los siguientes

1. Numero de sector.

```
nbloquepasold=Serial.read();
```

2. Contraseña de sector específico (6 números de 0-255 cada uno).

```
Serial.readBytes(verifica,6);
```

El orden de operación es el siguiente:

```
Lee sector
Lee contraseña
detecta tag
 Si (tag =1) {
       Escribe contraseña de fabrica
       Escribe en el bloque 1 (0x00,0x00,0x00, 0x00,0x00,0x00)
       Escribe en el bloque 2 (0x00,0x00,0x00, 0x00,0x00,0x00)
       Escribe en el bloque 3 (0x00,0x00,0x00, 0x00,0x00,0x00)
       Si (escrituras =1) {
              Limpia buffer ();
              Imprime “proceso correcto”;
       }}
```

Ya borrado el sector, procede a limpiar el buffer de almacenamiento de datos recibidos mediante el puerto serie.

Modo 5 lectura especifica de sector

Modo de operación 5 es una lectura especifica de sector, para este modo se requiere contar con la contraseña de dicho sector, la función realiza la lectura de los 3 bloques que la componen más el bloque de sector donde se almacena la contraseña.

Este modo recibe los siguientes datos

1.-Número de sector.

2.- Contraseña de sector (6 números de 0 a 255 cada uno).

El modo de operación es el siguiente:

```
Lee sector
Lee contraseña
Bloque = sector – 3
Mientras (bloque <= sector) {
       Detecta tag
       Si (tag = 1) {
       Lee bloque
       Si leer bloque = 1) {
              Imprime bloque y numero
       }}
       Bloque + 1
}
```

Una vez termina la lectura, la función limpia el buffer de almacenamiento y regresa a modo espera.

Modo 6 texto manual

El ultimo modo de operación es la escritura en un bloque específico de un sector, este modo permite escribir texto en cualquier bloque de cualquier sector sin modificación de parámetros del sector, es decir sin alterar permisos o contraseñas.

Este modo se utiliza para grabar bloque de sectores específicos externos al sistema SCARE, es necesario contar con la contraseña del sector a escribir.

Los datos que recibe en orden son los siguientes:

1.- Numero de sector.

```
nSector=Serial.read();
```

2.- Numero de bloque.

```
nBloque=Serial.read();
```

3.- Contraseña de sector (6 números de 0-255 cada uno).

```
Serial.readBytes(verificacion,6);
```

4.- Texto (máximo 16 caracteres).

```
Serial.readBytes(Texto,16);
```

El modo de operación es el siguiente

```
Leer sector
Leer bloque
Leer contraseña
Leer texto
Detectar tag
Si (tag = 1) {
      Escribir texto
      Si (escribir = 1) {
      Imprime proceso correcto
```

```
Limpia buffer

}}
```

Una vez terminada la función limpia el buffer de almacenamiento y regresa a modo espera.

4.6 Software CARE

El software CARE cuenta con 2 modos de operación, uno llamado modo configuración, al cual la manera de acceder es mediante el hardware y otro llamado modo cliente.

El modo configuración al ser llamado crea una red Wi –Fi de nombre “CARE”, esta red cuenta con una contraseña. Una vez conectado a la red permite entrar a una dirección para configurar parámetros utilizados en el sistema.

Estos parámetros son almacenados en la memoria EEPROM del microcontrolador.

Los parámetros que son modificables en el modo configuración son los siguientes:

1. Nombre de la red wifi a conectar SSID.
2. Contraseña de red.
3. IP del servidor.
4. Numero de bloque a leer de tag.
5. Nombre de ChipID.
6. Contraseña de tag (6 numero de 0 a255 cada uno).

Una vez escrito todos los parámetros hay una orden de nombre “Guardar”, esta orden almacena los datos en la memoria EEMPROM del microcontrolador, realizada la orden genera un mensaje “configuración guardada”.

Estos parámetros son configurables de cualquier dispositivo conectado al módulo vía Wi-FI.

El modo cliente realiza la configuración del Lector NFC, la conexión a la red wifi asignada en el modo configuración, la lectura del tag, la consulta a la base de datos y el registro del acceso sea o no en lugar y tiempo.

Este modo es el que está programado por defecto en el microcontrolador y funciona de la siguiente manera:

Configuración de NFC

```
Si (NFC = 1) {
       Conexión a la red wifi
       Si (conexión =1) {
              Esperar tag
              Si (tag=1){
                     Envía tag a php
                     Envía ChipID a php
                     Si (respuesta=1) {
                            Abrir puerta
                     }
                     Si no {
                     Puerta cerrada}
              }
       }
       Si no {
       Leer clave de súper usuario
              Si (clave=1) {acceso}
              Si no {acceso incorrecto}
       }
Si no {Reiniciar Sistema}.
```

Los utilizados como el SSID de la red, contraseña, bloque de lectura, clave de lectura, IP del servidor, ChipID son leídos directamente de la memoria EEPROM configurada en modo configuración.

Capítulo 5 Pruebas y Resultados

Al sistema SCARE se le realizaron múltiples pruebas de las cuales se obtuvieron distintos resultados.

Una de las pruebas arrojo un error en la comunicación i2c, este error era que al permanecer en espera de recepción de datos en el módulo CARE se quedaba colgado y dejaba de funcionar, este problema se solucionó reiniciando el módulo cada determinado tiempo y añadiendo una función de configuración específica para limpiar la comunicación i2c, esto evita que la comunicación se quedara colgada.

Con los tags, las pruebas fueron de modificación de permisos, varios bloques quedaron dañados por la incorrecta programación, por desgracia estos bloques ya no se pueden recuperar.

Otra prueba fue el tiempo que tardaba el sistema CARE en recibir los datos de la base, este tiempo era de aproximadamente 6 segundos, la solución a este problema fue enviar una cadena corta de caracteres con uno de terminación, el resultado fue pasar de 6 segundo a 1 en obtener la respuesta desde el servidor.

Como prueba final se instaló el sistema SCARE en el edificio de posgrado de la facultad de ingeniería eléctrica, como primera prueba se instalaron 2 módulos en los accesos al laboratorio de máquinas y al laboratorio de instrumentación, se presentó falla al intentar conectar al servidor instalado también se presentó una falla en la comunicación wi-fi. Para corregir el problema del servidor se actualizo los conectores del software RAB, y los conectores de la base de datos, para corregir la comunicación wi-fi se utilizó un modem distinto, al cual se le aplicó una configuración especifica.

En el edificio ya existía un sistema de control de acceso mediante dígitos, este sistema se remplazó por SCARE, para esto se utilizó el banco de baterías adaptando la salida de 12v a 5v para el uso de CARE, también se utilizaron las chapas eléctricas previamente instaladas.

Se diseñó una caja especial para el módulo CARE y se fabricó con el uso de impresora 3D.

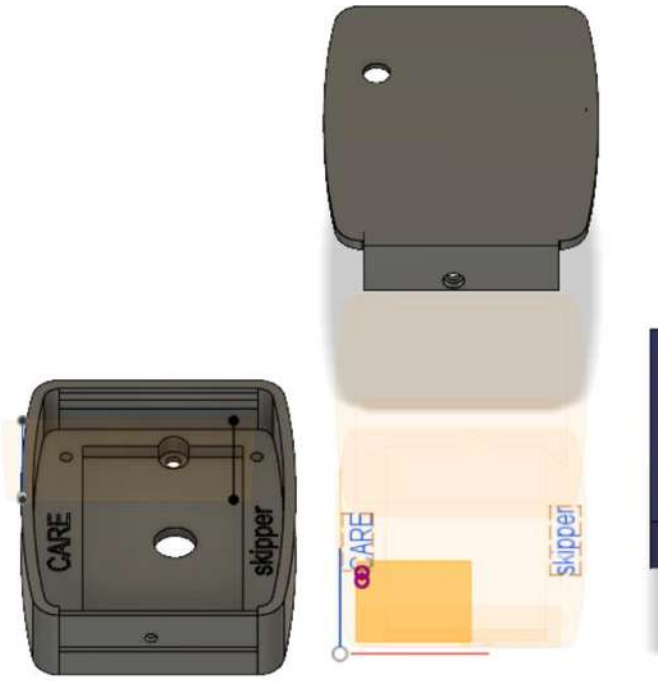


Imagen 5-1 Diseño de impresión 3d modulo CARE

Al día de 15 de noviembre de 2019, cumpliendo 4 meses el sistema SCARE no ha presentado fallas.

Conclusiones

Se cumple con el objetivo general al diseñar y desarrollar un sistema de seguridad que permite tener una gestión de usuarios a distintos accesos, incorporando tecnología wifi para la transmisión de datos y NFC para la identificación de usuarios, además de contar con un sistema de registro de horarios.

Se desarrollo un software para facilitar la gestión del sistema de control de acceso y registro de usuarios, esto permite que el sistema sea fácil de gestionar, además se agrego un registro de accesos autorizados y no autorizados; permitiendo saber quiénes ingresan a distintas áreas.

Se desarrollo un sistema físico (hardware) para registro de usuarios y otro para identificación de estos.

Para el desarrollo del presente trabajo se aplicaron los conocimientos adquiridos durante los años de formación en la Facultad de Ingeniería Eléctrica.

Referencias

[1] «wikipedia,» 18 Septiembre 2019. [En línea]. Available: https://es.wikipedia.org/wiki/Electr%C3%B3nica_de_control. [Último acceso: 13 Noviembre 2019].

[2] M. F. Sendin, «fernandezsendin,» blogspot, 2 junio 2011. [En línea]. Available: http://fernandezsendin.blogspot.com/2011/06/historia-de-las-llaves-y-cerraduras.html. [Último acceso: 31 octubre 2019].

[3] J. C. Leyva, *Fuente Propia*, Morelia: Propia, 2019.

[4] L. d. Valle, «https://programarfacil.com/podcast/nodemcu-tutorial-paso-a-paso/,» progrmarfacil, 2019. [En línea]. Available: https://programarfacil.com/podcast/nodemcu-tutorial-paso-a-paso/. [Último acceso: 26 11 2019].

[5] S. Schneider, «repo,» [En línea]. Available: https://repo.sesc.eu/doc/esp-toniesp/commit/a3ff43cd5e5cda37b02b0cd99623adb43b66a17a. [Último acceso: 24 11 2019].

[6] L. Llamas, «luisllamas,» [En línea]. Available: https://www.luisllamas.es/esquema-de-patillaje-de-arduino-pinout/. [Último acceso: 19 11 2019].

[7] todoelectronica, «todoelectronica,» [En línea]. Available: https://www.todoelectronica.com/es/1516-control-de-accesos. [Último acceso: 4 noviembre 2019].

[8] datasheet, «alldatasheet,» [En línea]. Available: alldatasheet.com. [Último acceso: 2 10 2019].

[9] https://reparacionesvalencia.com/blog/historia-la-cerradura/, «https://reparacionesvalencia.com/blog/historia-la-cerradura/,» [En línea]. Available: https://reparacionesvalencia.com/blog/historia-la-cerradura/.

[10] wikipedia, «Gran Muralla China,» Fundacion Wikimedia, inc., 7 septiembre 2016. [En línea]. Available: https://es.wikipedia.org/wiki/Gran_Muralla_China. [Último acceso: 31 octubre 2019].

[11] Grainger, «grainger,» grainger, 2019. [En línea]. Available: https://www.grainger.com.mx/producto/STANLEY-COMMERCIAL-HARDWARE-Cerradura-de-Palanca%2CNíquel-Plata/p/45DH65. [Último acceso: 31 octubre 2019].

[12] R. Alvarez, «xataka,» xataka, 24 junio 2016. [En línea]. Available: https://www.xataka.com/medicina-y-salud/de-la-ficcion-a-la-realidad-chips-nfc-implantados-en-la-piel-para-ayudar-en-tareas-diarias. [Último acceso: 4 noviembre 2019].

[13] Desconocido, «visioptech,» 11 Agosto 2017. [En línea]. Available: https://www.visiotechsecurity.com/es/noticias/207-tipos-de-control-de-accesos.. [Último acceso: 5 Noviembre 2019].

[14] bricomart, «bricomert,» [En línea]. Available: https://www.bricomart.es/teclado-control-de-acceso.html. [Último acceso: 5 Noviembre 2019].

[15] n. liu, «viaje-a-china,» china highlights, [En línea]. Available: https://www.viaje-a-china.com/gran-muralla/historia/. [Último acceso: 13 Noviembre 2019].

[16] J. Carrillo, «reserchgate.net,» [En línea]. Available: https://www.researchgate.net/figure/Figura-8-Sistema-de-control-en-lazo-abierto_fig4_259678412. [Último acceso: 13 Nobiembre 2019].