

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-27

# **Administración de control de acceso para máquinas Vending tipo Snacks**

Andrés Alexander Ríos Uribe

David Antonio Gómez Guerra

Ingeniería Electrónica

Asesor: German Goez Sánchez

**INSTITUTO TECNOLÓGICO METROPOLITANO**

**Agosto 2018**

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## RESUMEN

---

En la actualidad las máquinas Vending tipo Snacks se han masificado significativamente, debido a que son una alternativa para satisfacer necesidades de alimentación de venta al paso en lugares donde anteriormente era difícil acceder a productos empacados. Con esto se ha incrementado el auge de la instalación de estos equipos, debido a que son un negocio rentable y prometedor para las empresas que incursionan en este campo, de aquí que existan muchas empresas que deseen explotar esta línea de negocio y sobre todo de brindar mayor seguridad a estos equipos, ya que éstos en la actualidad cuentan con un sistema de acceso convencional, compuesto de una llave metálica y un cerrojo mecánico, que son insuficientes para brindar la seguridad que requiere el equipo.

Este proyecto brinda la seguridad que requieren estos equipos, por medio de la administración de control de acceso, el cual garantiza el ingreso únicamente al personal autorizado, mediante una clave asignada por el administrador y la huella dactilar, al mismo tiempo se identifica el registro de horario de ingreso de los operarios, tiempo de apertura y la cantidad de visitas a la máquina.

La administración de claves de acceso se realiza de forma remota mediante la plataforma GPRS, que permite enviar y recibir mensajes, además de mantener una comunicación permanente con la máquina, brindando dinamismo al momento de cambiar y/o consultar las claves del equipo en cualquier momento y lugar desde que exista cobertura del operador móvil, esto brinda versatilidad y una mejor administración del sistema.

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## RECONOCIMIENTOS

---

En nuestro camino de formación profesional de Ingeniería electrónica, siempre existieron muchas personas que nos apoyaron, guiaron y compartieron sus conocimientos y sobre todo nos alentaron en los momentos difíciles, impidiendo así abandonar nuestro sueño de ser profesionales.

Por tal motivo mencionamos a nuestros padres Rosa Lía Uribe Echavarría, Fabio de Jesús Ríos García, Hernán Gómez Orozco e Idalides Guerra Martínez, a nuestras esposas Susana Zapata Quintero, y Leidy Milena Cardeño, hijas y hermanas, personas que con su amor y paciencia estuvieron siempre a nuestro lado formando así un gran pilar para alcanzar nuestro sueño.

También queremos dar un agradecimiento al docente y asesor de nuestro proyecto de grado German David Goetz Sánchez quien, con su disposición, conocimiento y experiencia, nos orientó para cumplir una a una las metas y objetivos para el desarrollo de un 100% del proyecto.

Gracias al Instituto Tecnológico Metropolitano, a su plantel administrativo, profesores y compañeros de estudio, personas con las que luchamos para llegar a una meta en común, que fue adquirir el título de profesional en Ingeniería Electrónica.

Gracias.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## ACRÓNIMOS

---

AES: Estándar de cifrado avanzado

AFIS: Criptografía de clave simétrica

AT: Tecnología avanzada

Baud Rate: Tasa de baudios

DC: Corriente directa

DSA: Algoritmo de firma digital

ETHERNET: Estándar de redes de área locales

FFT: Transformada rápida de Fourier

GPRS: General de paquetes vía radio

GSM: Sistema global para las comunicaciones móviles

IoT: Internet de las cosas

MMS: Servicio de mensaje multimedia

MS: Milisegundos

NFC: Comunicación de campo cercano

RC5: Cifrado de rivest

RFID: Identificación de frecuencia de radio

SMS: Servicio de mensajes cortos

UART: Transmisión-Receptor Asíncrono Universal

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## TABLA DE CONTENIDO

1 INTRODUCCIÓN .....	8
1.1 Planteamiento del problema.....	9
1.2 OBJETIVOS.....	10
1.2.1 Objetivo general.....	10
1.2.2 Objetivos específicos.....	10
2 MARCO TEÓRICO .....	11
2.1 Tecnologías de control de acceso.....	11
2.1.1 Control de acceso mediante teclado matricial.....	11
2.1.2 Tecnología de control de lectores de proximidad.....	11
2.1.3 Tecnología de control de acceso biométrico.....	13
2.2 Tecnologías de comunicación.....	15
2.2.1 Tecnología de comunicación GPRS.....	15
2.2.2 Tecnología de comunicación internet de las cosas.....	16
2.2.3 Tecnología de comunicación Ethernet.....	16
2.3 Cifrado de mensajes.....	16
2.4 Protección al Arduino mediante hardware o software.....	17
2.5 Base de datos.....	18

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

2.6 Especificaciones de los elementos seleccionados y utilizados.....	18
2.6.1 Plataforma de administración.....	18
2.6.2 Tecnología de comunicación.....	19
2.6.3 Control de acceso.....	20
2.6.4 Cerradura electromagnética (Solenoides).....	23
2.6.5 Reloj de tiempo real (RTC).....	24
2.7 Base de datos.....	25
3 METODOLOGÍA.....	26
3.1 Control de acceso remoto seguro .....	28
3.1.2 Documentación.....	28
3.1.3 Análisis de las tecnologías a implementar y selección de las mismas.....	28
3.2 Integración del sistema de comunicación y control de acceso.....	29
3.2.1 Implementación e integración.....	29
3.2.2 Integración y configuración de los sistemas de comunicación y control.....	32
3.2.3 Programación del sistema para la administración del proyecto.....	33
3.2.4 Integración del sistema de comunicación con la base de datos.....	33
3.3 Componentes aprovechados de la máquina Vending tipo Snacks.....	34
3.3.1 Máquina Expendidora.....	34
3.3.2 Tarjeta de control.....	34
3.3.3 Fuente de alimentación.....	35

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

3.3.4 Teclado.....	36
3.3.5 Sensor de puerta.....	36
3.4 Instalación de los componentes en la máquina.....	36
3.4.1 Instalación cerradura electromagnética.....	36
3.4.2 Instalación teclado matricial.....	38
3.4.3 Instalación sensor biométrico.....	38
3.4.5 Instalación de la plataformas de administración, sistema de comunicación y placa de conexiones.....	39
4 RESULTADOS Y DISCUSIÓN.....	41
4.1 Pruebas y validación de resultados.....	41
4.1.1 Pruebas de ingreso a la máquina.....	43
4.1.2 Prueba cambio de clave.....	44
4.1.3 Prueba base de datos.....	47
5 CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO.....	48
5.1 Problemas presentados durante la ejecución del proyecto y las pruebas realizadas.....	49
5.2 Trabajos futuros.....	51
ANEXOS.....	55

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

# 1. INTRODUCCIÓN

---

La implementación de las máquinas Vending tipo Snacks han presentado un incremento significativo en Colombia, el negocio ha crecido un 30% en los últimos 6 años. Existen aproximadamente 12.500 de estos equipos en el país, lo que significa que por cada 3.900 habitantes se encuentra una máquina dispensadora de productos, esto permite proyectar crecimientos mayores debido a que en países como Japón donde son muy populares las máquinas Vending, hay por lo menos 5.080.000 máquinas, lo que significa una por cada 25 habitantes, mientras que en Estados Unidos hay un equipo por cada 70 habitantes y la tendencia es al crecimiento. Esto con el fin de aumentar sus ingresos y poder penetrar nuevos mercados como el cuidado personal, higiene corporal, componentes electrónicos, elementos de protección personal, artículos deportivos entre otros (Dinero.com, 2017).

Entre las cifras que se manejan de este negocio en el mundo se encuentran:

En Japón las ventas totales calculadas del 2015 fueron alrededor de \$45.300 millones de dólares.

En Estados Unidos las máquinas expendedoras reciben \$22.000 millones de dólares al año, con unos 7 millones de máquinas, esto representa un promedio de \$ 3.000 dólares por máquina (Mcculloch, 2017).

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Esta industria en España facturó \$1.200 millones de euros en 2015, a través de 1.700 operadores y un número de máquinas alrededor de 368.530 lo que significa una máquina por cada 125 habitantes (Méndez, 2017).

En Colombia se habla de ventas cercanas a los \$70.000 millones de pesos anuales y según expertos del sector dependiendo de la ubicación del activo existen máquinas que logran ventas de 18 millones de pesos mensuales, con un promedio de ventas diarias de al menos \$600,000 pesos en una maquina dispensadora, esto permite pensar que estos equipos deben tener sistemas de acceso y seguridad muy confiables, debido a que el volumen de dinero almacenado en estos es significativo, sin tener en cuenta el costo de los dispositivos que se utilizan al interior del equipo que son de alto valor (Dinero.com, 2017).

### **1.1 Planteamiento del problema**

La significativa masificación de los equipos Vending en Colombia ha traído problemas de administración y seguridad a los operadores de estos equipos, entre los que se encuentran; la posibilidad de que diferentes empresas puedan tener acceso a varios equipos con una misma llave, ya sean estos propios o ajenos. Otro problema es la filtración de claves de acceso de los equipos entre personal operativo de diferentes compañías que utilizan el mismo sistema de ingreso, además de la alta dificultad en la administración de las claves, que obedece a la constante rotación del personal que experimenta este tipo de negocio. Esto permite identificar una gran oportunidad de mejora en la administración del control de acceso a estos equipos.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Desde la ingeniería se presenta un desafío a resolver, debido a que se busca una solución entre las tecnologías existentes que permitan obtener un sistema del tipo electrónico y que a su vez logre integrar los dispositivos ya disponibles en la máquina y las plataformas de desarrollo actuales, además de incorporar tecnologías que permitan tener una comunicación permanente entre un administrador y la máquina Vending.

Este trabajo propuso solucionar estos problemas mediante la implementación de una plataforma de control de acceso electrónica con conexión remota entre el operador y la máquina Vending.

## 1.2 Objetivos

### 1.2.1 Objetivo general

Desarrollar una plataforma de administración de control de acceso de bajo costo para aumentar la seguridad de las máquinas Vending tipo Snacks usando sistemas de identificación electrónica y de comunicaciones.

### 1.2.2 Objetivos específicos

- ✓ Proponer una solución de acceso remoto seguro, basada en tecnologías relacionadas con la máquina Vending tipo Snacks.
- ✓ Diseñar un sistema de comunicación utilizando tecnologías móviles para el intercambio de información entre el administrador y la máquina.
- ✓ Implementar un sistema electrónico de control de acceso para administración remota de claves.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## 2. MARCO TEÓRICO

---

En esta sección se abordan las posibles tecnologías y componentes a implementar para la administración de control de acceso. Después de analizar cada una de éstas, se realizó la selección de las más apropiadas para el desarrollo del proyecto.

### 2.1 Tecnologías de control de acceso

#### 2.1.1 Control de acceso mediante teclado matricial

Es un sistema de acceso que se basa en la utilización de una clave previamente parametrizada en el sistema y puede estar compuesta por números, letras y caracteres especiales, su principio de funcionamiento es realizar una comparación entre la clave ingresada y la almacenada, para autorizar o no el ingreso al equipo.

#### 2.1.2 Tecnología de control de lectores por proximidad

El principio de funcionamiento de esta tecnología está basado en el uso de tarjetas que almacenan información, la cual es transmitida al sistema cuando esta se acerca al lector electrónico, dando acceso o no al usuario de acuerdo con los parámetros establecidos.

Se hace referencia de algunas tecnologías de lectores de proximidad:

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

*RFID (Radio Frequency Identification)*

En español, identificación por radio frecuencia, es la tecnología que utiliza ondas de radio para identificar automáticamente personas u objetos. Hay varios métodos de identificación, pero el más implementado y común es el que almacena un número de serie que identifica a una persona u objeto en un microchip que está conectado a una antena, el chip y la antena se denominan transpondedor RFID o etiqueta RFID. La antena permite que el chip transmita la información a un lector, el cual a su vez convierte las ondas de radio reflejadas de vuelta de la etiqueta RFID en información digital, que luego puede transmitirse a ordenadores que puedan hacer uso de la misma (Deal, 2004).

En las consultas realizadas se identificaron proyectos utilizando la tecnología RFID, se quiere resaltar el proyecto “*Construcción de un prototipo de un sistema de control de acceso en instalaciones industriales utilizando tecnología RFID*”, debido a que es un proyecto que nos guía en el uso de tecnologías de proximidad y como éstas permiten aplicaciones hasta niveles industriales (Bateman, Cortés, Cruz, & Paz-Penagos, 2009).

*NFC (Near Field Communication)*

En español, comunicación de campo cercano. Esta tecnología permite que artículos, como teléfonos móviles, computadoras, etiquetas o carteles, intercambien información de forma inalámbrica a través de una pequeña distancia. Aunque principalmente asociado con el pago móvil, la comunicación de campo cercano tiene muchas aplicaciones comerciales en otros sectores como: La comercialización, nutrición, transporte, juegos y salud (McHugh & Yarmey, 2012).

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

En el año 2015 Morris William Díaz Saravia realizó un artículo donde habla de la implementación de la tecnología NFC, el artículo habla de la utilización de esta tecnología para accesos múltiples de contacto cercano frecuentemente usado en universidades, hoteles, entre otros (Saravia, 2016).

### **2.1.3 Tecnología control de acceso biométrico**

La biometría permite la identificación de individuos mediante rasgos biológicos que son perdurables en el tiempo, como las huellas dactilares, reconocimiento de retina y rasgos faciales. Los lectores biométricos se parametrizan de acuerdo a las condiciones físicas de una persona y se guardan en una base de datos, si una persona intenta ingresar y ninguna de las condiciones físicas coincide; éste no le permitirá el acceso.

En este tipo de tecnología sobresale la identificación por medio de huellas dactilares que se reconocen mediante sensores biométricos, que son dispositivos capaces de leer, guardar e identificar huellas dactilares para usos sistematizados. Existen diferentes tipos de sensores biométricos que dependiendo del principio de funcionamiento ofrecen mayor confiabilidad y ventajas, entre estos se encuentran: sensores ópticos reflexivos, ópticos transmisivos, capacitivos, mecánicos, térmicos y sensores de salida dinámica. Es importante decir que la biometría se basa en 7 pilares que permiten dar mayor respaldo a la seguridad y efectividad del sistema, estos son:

*Universalidad:* se refiere a que tan común es encontrar ese patrón en los individuos.

*Singularidad:* que tan único o diferente es un individuo de otro.

*Permanencia:* que tan perdurable en el tiempo es la huella sin sufrir modificaciones.

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

*Recolectable:* indica si el proceso de adquisición, medición y almacenamiento de la huella es fácil o complejo.

*Calidad:* permite medir la precisión, velocidad y confiabilidad del sistema al procesar la huella biométrica.

*Aceptabilidad:* indica la aceptación del público frente a la tecnología.

*Fiabilidad:* que tan vulnerable es el sistema de autenticación al engaño o fraude (Wikipedia.org, 2017) (Paz, 2017).

En el año 2008 Gualberto Aguilar, Gabriel Sánchez, Karina Toscano, Mariko Nakano y Héctor Pérez escribieron un documento donde hablan sobre una aplicación de la tecnología biométrica sustentado en un sistema de identificación por huellas dactilares conocido como AFIS (Sistema de Identificación Automática de Huella Dactilar), apoyados con el eficiente algoritmo: Transformada Rápida de Fourier (FFT), filtros de Gabor para aclarar la imagen de las huellas dactilares, adicional agregaron un método de reconocimiento fundamentado en tres características (coordenadas, distancia y ángulos) (Aguilar, Sánchez, Toscano, Nakano, & Pérez, 2008).

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Entre los algoritmos usados por los sensores biométricos se encuentran:

*Técnicas basadas en minucias:* Consiste en la comparación de los puntos singulares de las crestas de las huellas (minucias) que pueden ser una bifurcación o una terminación. Mediante esta técnica se genera un mapa que permite localizar la posición y orientación de una minucia, esto permite obtener un resultado sobre la similitud de dos huellas, es necesario resaltar que este método se basa en aproximaciones lo que conlleva a tener errores o lectura de falsas minucias, estos errores pueden aumentar si la calidad de la imagen no es buena.

Entre los algoritmos de comparación de minucias se encuentran Germain\_97, Tico\_03, lifeng\_04, Xundong\_00 y Lee\_02. (Muñoz, 2009).

*Técnicas de correlación:* Esta técnica se basa en la correspondencia o relación de dos imágenes y consiste en la comparación pixel a pixel del nivel de gris de la imagen, para realizar esta comparación se puede realizar de dos formas mediante la correlación directa o utilizando la correlación en el dominio de la frecuencia.

Entre los algoritmos usados para esta técnica con muy buenos resultados se encuentran [FVC 2002], [FVC 2004]. (Muñoz, 2009).

## **2.2 Tecnologías de comunicación**

### **2.2.1 Tecnología de comunicación GPRS**

Es un sistema de comunicación basado en paquetes vía radio, en inglés General Packet Radio Service. Es una tecnología de transmisión de voz y datos en terminales móviles, el principio de

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

funcionamiento esta dado mediante la conmutación de paquetes entre el terminal móvil y la antena. Esta tecnología permite compartir cada canal por varios usuarios, por ende, mejora la eficiencia en el uso de los recursos de red. Es una evolución del sistema GSM (Wikipedia.org, 2017).

### **2.2.2 Tecnología de comunicación internet de las cosas**

Internet of Things (IoT), es una red inalámbrica que permite la conectividad permanente de artículos electrónicos. Estos deben estar constituidos de sistemas embebidos y hardware especializado que permite la conectividad a internet y a la programación de eventos específicos en función de tareas que sean programadas remotamente (Ritz & Knaack, 2017).

### **2.2.3 Tecnología de comunicación Ethernet**

Es un estándar de comunicación para sistemas informáticos que se fundamenta en el uso de una red de área local. Las redes Ethernet son ampliamente usadas en las comunicaciones industriales por su alto rendimiento, sin embargo, no ha sido la solución adecuada para aplicaciones en tiempo real (Wikipedia.org, 2017).

## **2.3 Cifrado de mensajes**

El cifrado de mensajes está basado en la criptografía, ésta es la encargada de establecer los procedimientos a utilizar para proteger la información que se da entre un emisor y un receptor, es decir que la información transmitida entre dicho canal solo sea accesible al personal autorizado y que interprete dicho cifrado.

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

La criptografía tiene diferentes técnicas de cifrado, entre las cuales están:

*Criptografía clásica:* Este método de cifrado oculta los mensajes sustituyendo o cruzando las letras del mensaje por otras letras. Este método no es muy confiable debido a que existen muchas técnicas para descifrar e interpretar claramente el mensaje transmitido, adicionalmente presenta una gran dificultad ya que es muy compleja de aplicar por la longitud de la clave y el gran tiempo que ésta demanda en ser encriptado y de igual forma desencriptarlo.

*Criptografía moderna:* Es un método de cifrado avanzado que simplifica la complejidad del sistema de encriptación clásico, pero que a su vez brinda mayor seguridad a la información que se desea proteger, de ésta se deriva la criptografía simétrica y la criptografía asimétrica.

*Criptografía simétrica:* Se basa en el uso de una misma clave para cifrar y descifrar los mensajes, esto conlleva que tanto el que envía como el que recibe deban conocer esta clave, esto da como resultado mayor vulnerabilidad al tener cierto número de usuarios con la clave principal, en la criptografía simétrica tenemos los métodos RC5 y AES.

*Criptografía asimétrica:* Se caracteriza por utilizar dos claves de las cuales una es pública y otra privada, una de éstas es utilizada para cifrar y la otra para publicar. La clave pública es conocida por diferentes usuarios y la privada solo para aquel que recibe el mensaje cifrado, En la criptografía simétrica se encuentran los métodos RSA y DSA.

## **2.4 Protección al Arduino mediante hardware o software**

En la documentación de Arduino se consultó sobre los “fusibles bits” que en los microcontroladores atmel son interruptores que permiten programar los puertos del

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

microcontrolador, que para este caso limita el acceso a la información contenida en la memoria del dispositivo, mediante esta programación es posible blindar el dispositivo ante hackers que intenten realizar fraudes al proyecto que se desee producir comercialmente, además es posible vía software crear una llave o un código de programación que permita mediante una clave de acceso ingresar a la programación del Arduino y de esta forma realizar cambios al programa o código, básicamente con estas dos opciones es posible minimizar la vulnerabilidad de la plataforma (Askix.com, 2017).

## **2.5 Base de datos**

Una base de datos es un sistema de almacenamiento que permite guardar información con determinado orden, utilizando una parametrización de campos y registros, que siempre garantizan un acceso eficiente a la información depositada en ella (Wikipedia.org, 2017).

## **2.6 Especificaciones de los elementos seleccionados y utilizados**

Al inicio de este capítulo se describe de manera general las posibles tecnologías a implementar en el proyecto. En este punto se explica al detalle las tecnologías seleccionadas para el desarrollo del proyecto, teniendo en cuenta que son las más viables y efectivas.

### **2.6.1 Plataforma de administración**

Para el desarrollo de la plataforma de administración se seleccionó la tarjeta de programación Arduino Mega 2560, por lo que su software y hardware son muy flexibles y permiten realizar gran

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

cantidad de aplicaciones a muy bajo costo. Este elemento permite controlar todo el sistema de acceso a la maquina Vending tipo Snacks de una forma versátil y efectiva, entre sus características diferenciadoras podemos encontrar gran cantidad de puertos tanto análogos como digitales y un amplio espacio de almacenamiento, lo que brinda mayor capacidad de desarrollo. (*Ver anexo 1 - Comparativo especificaciones técnicas de tarjetas de programación*).

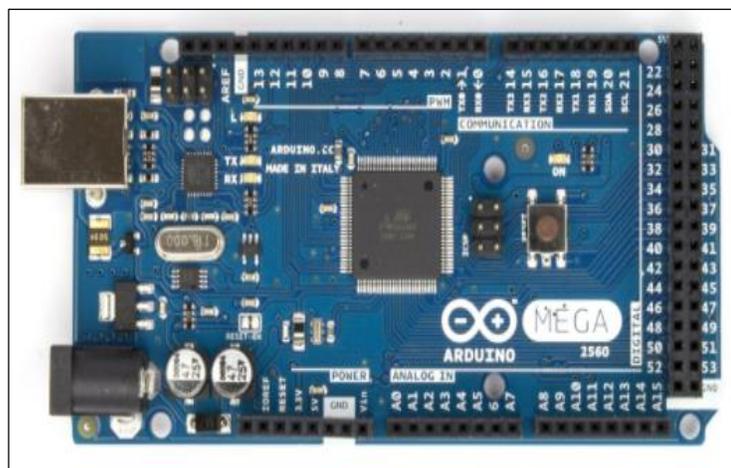


Figura 1. Tarjeta Arduino Mega 2560  
Autor: Sharebot

### 2.6.2 Tecnología de comunicación

Después de analizar diferentes tipos de tecnologías de comunicación, la seleccionada para implementar en este proyecto fue la tecnología GPRS, debido a que ésta transmite datos a altas velocidades. Adicionalmente es muy económica, dado que la facturación es en función de la cantidad de datos transferidos en lugar de tiempo de conexión, lo que permite mayor aplicación al proyecto, gracias a que la demanda de datos es muy baja.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

El criterio de selección de la tarjeta SIM900 es su compatibilidad con el módulo Arduino Mega 2560, sus características son muy similares a la SIM800, pero la diferencia más significativa es su disponibilidad y bajo costo. (Ver anexo 2 – Comparativo especificaciones técnicas de tarjetas basadas en la tecnología GPRS).



Figura 2. Tarjeta GPRS basada en el controlador SIM900  
Fuente: Prometec

### 2.6.3 Control de acceso

Luego de una revisión bibliográfica de las posibles tecnologías aplicables al proyecto, se concluye que la tecnología de teclado matricial y huella dactilar biométrica, son las más apropiadas para el desarrollo de este proyecto, la selección de estas dos tecnologías obedece a las siguientes razones:

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### Teclado matricial

Es una tecnología confiable y segura, que es ampliamente utilizada en diversos sistemas de seguridad, permite mayor versatilidad al momento de administrar las claves de forma remota y realizar cambios de clave en diversos momentos, sin necesidad de trasladarse físicamente al sitio donde se encuentra la máquina.

Se trabajó con el teclado matricial ya que la maquina Vending tipo Snacks trae incorporada esta tecnología para realizar sus funciones básicas. Además, agrega valor al proyecto debido a que permite disminuir costos asociados a su implementación. (*Ver anexo 3 - Especificaciones teclado matricial*).



Figura 3. *Teclado matricial*  
Fuente: Autor

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### Sensor de huella biométrica

Se seleccionó el sensor de huella biométrica ya que éste es un sistema ampliamente utilizado cuando se requiere mayor precisión en la identificación de un individuo, es necesario mencionar que es la única aceptada como prueba legal para la identificación de una persona. Por otra parte, los sensores de huellas dactilares además de ser efectivos, fáciles de implementar y automatizar, son eficientes debido a que la relación costo beneficio es muy buena.

El sensor utilizado es un lector óptico dactilar de huella FPM10A, debido a que posee mayor capacidad de almacenamiento, adicionalmente cuenta con un chip DSP de alta potencia. El algoritmo de identificación utilizado por este sensor se fundamenta en la técnica de minucias. (*Ver anexo 4 – Comparativo especificaciones técnicas sensor de huella biométrica*).



Figura 4. *Sensor de huella biométrica utilizado*  
Fuente: Electronilab

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

#### 2.6.4 Cerradura electromagnética (Solenóide)

Se utilizó una cerradura electromagnética Master Lock modelo HD1040-12V. Ésta fue seleccionada debido a que su funcionamiento electromecánico se adapta a las necesidades del proyecto y sus dimensiones son las adecuadas para el espacio disponible que se tenía para la instalación de ésta en la máquina, lo que permite la apertura y cierre de la puerta de la máquina adecuadamente, adicionalmente esta cerradura electromagnética opera a 24VDC, voltaje disponible en la máquina. (*Ver anexo 5 - Especificaciones cerradura electromagnética*).

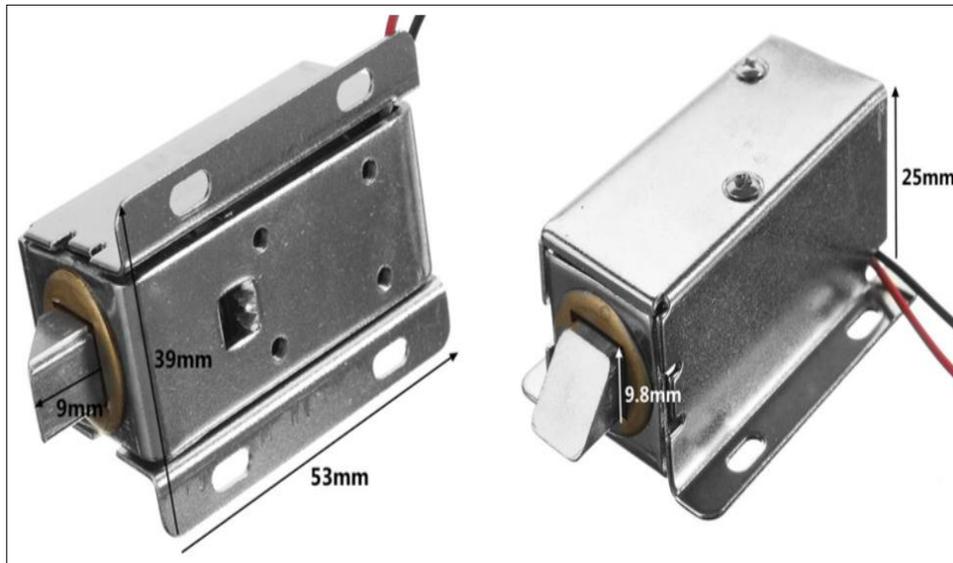


Figura 5. *Cerradura electromagnética*

Fuente: Aliexpress.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### 2.6.5 Reloj de tiempo real (RTC)

El reloj de tiempo real permite tener la fecha y hora actualizada en todo momento en el sistema, logrando así liberar al Arduino de una tarea adicional que es la de realizar estas mediciones, esto es posible gracias a la fuente de alimentación que tiene alterna, lo que hace que no se pierda las mediciones horarias; el RTC aporta grandes ventajas al proyecto al no depender de una red o conexión local para tener el horario actualizado. El RTC seleccionado es el DS3231 debido a que presenta una mayor estabilidad en su funcionamiento principal y es el más completo entre los dispositivos comparados. *(Ver anexo 6 - Especificaciones Reloj de tiempo real).*



Figura 6. *Reloj de tiempo real DS3231 (RTC)*  
Autor: Dynamoelectronics

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## 2.7 Base de datos

La base de datos implementada en este proyecto fue creada bajo el programa informático Excel de Microsoft, este programa permitió diseñar, organizar y estructurar adecuadamente la información requerida para la administración del control de acceso a las máquinas Vending tipo Snacks. Se utilizó esta base de datos debido a que es un programa informático de amplio uso y fácil de utilizar, la información que se almacenará proviene de pruebas del prototipo y no se considera necesario ahondar en sistemas más elaborados, debido a que la información será para fines netamente académicos.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

### 3. METODOLOGÍA

---

La metodología implementada fue basada en un modelo experimental la cual permitió verificar la viabilidad, aplicabilidad y confiabilidad de la plataforma de control de acceso mediante administración remota de claves. La implementación del proyecto abarcó los siguientes pasos: documentación, análisis, implementación e integración, pruebas y validación de resultados.

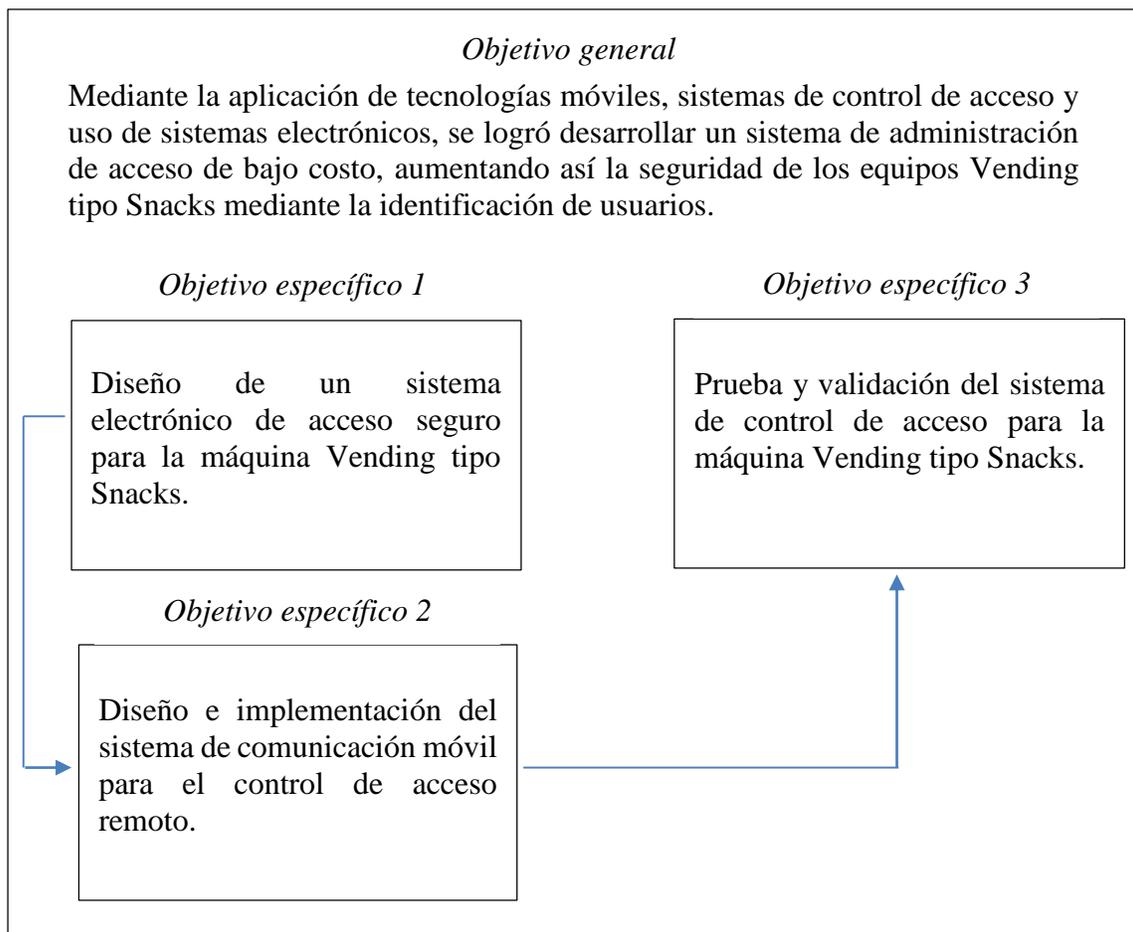


Figura 7. *Objetivo general y específicos*

Fuente: Autor

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

En la figura 2, se observa un diagrama de bloques representativo del proyecto, el cual está compuesto por dos bloques principales que articulan el funcionamiento del sistema. Donde se encuentra el módulo de comunicación que incluye la tecnología de transmisión y la plataforma administrativa, en la cual se realizan las operaciones de cambio de claves y otras rutinas asignadas al sistema. Por otra parte, en el sistema de control se encuentra el módulo de control de acceso al equipo y la cerradura electrónica que realiza la apertura de la máquina. Estos dos bloques se comunican mediante una interface que permite un intercambio permanente de información para un buen funcionamiento del proyecto.

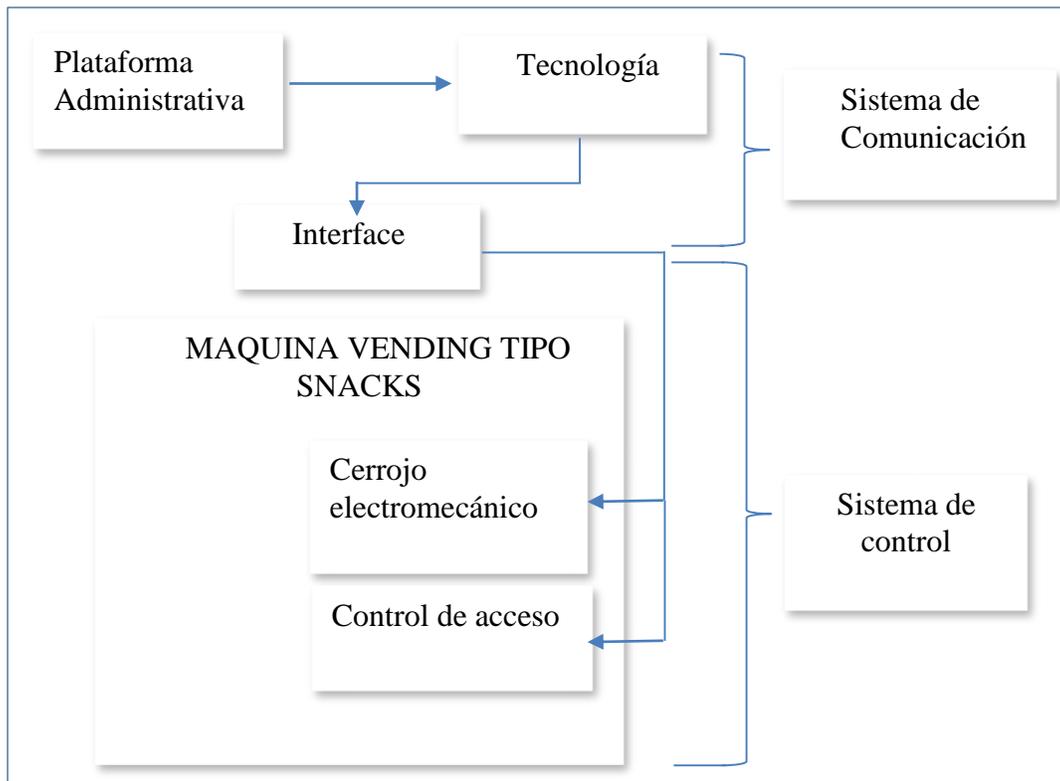


Figura 8. Esquema del sistema de control de acceso

Fuente: Autor

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### 3.1 Control de acceso remoto seguro

Para el desarrollo del control de acceso remoto seguro se consultaron diversas fuentes como: investigaciones, artículos de revista, páginas de internet, libros, educadores del área electrónica y telecomunicaciones, entre otras fuentes, que sirvieron de base para dar validez al proyecto; además de aportar conocimiento sobre los desarrollos actuales que se han llevado a cabo en el tema de controles de acceso y sistemas de comunicación, estos contenidos se encuentran con mayor detalle en el marco teórico. A continuación, se describen los pasos realizados.

#### 3.1.2 Documentación

- ✓ Se consultaron las tecnologías aplicables a la administración remota y los controles de acceso.
- ✓ Se consultaron las tecnologías que aplican a sistemas inalámbricos de transmisión.
- ✓ Se especificó el sistema de almacenamiento aplicable al proyecto de grado.

#### 3.1.3 Análisis de las tecnologías a implementar y selección de las mismas

- ✓ Se analizó y seleccionó las tecnologías para la administración, control de acceso y la comunicación entre el administrador (computador, equipo móvil, tablet entre otros) y el sistema de control.
- ✓ Se analizó y seleccionó la base de datos aplicable al proyecto.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### 3.2 Integración del sistema de comunicación y control de acceso

Para realizar una adecuada integración entre los sistemas de comunicación y control, es necesario realizar una adaptación entre los componentes propios del equipo y dispositivos externos requeridos para obtener la plataforma de administración deseada. Para lograr esta tarea primero se realiza un diagrama esquemático donde se asocian los dispositivos para su configuración y programación, por último, se realizan las pruebas que dan validez a la eficiencia del proyecto.

#### 3.2.1 Implementación e integración

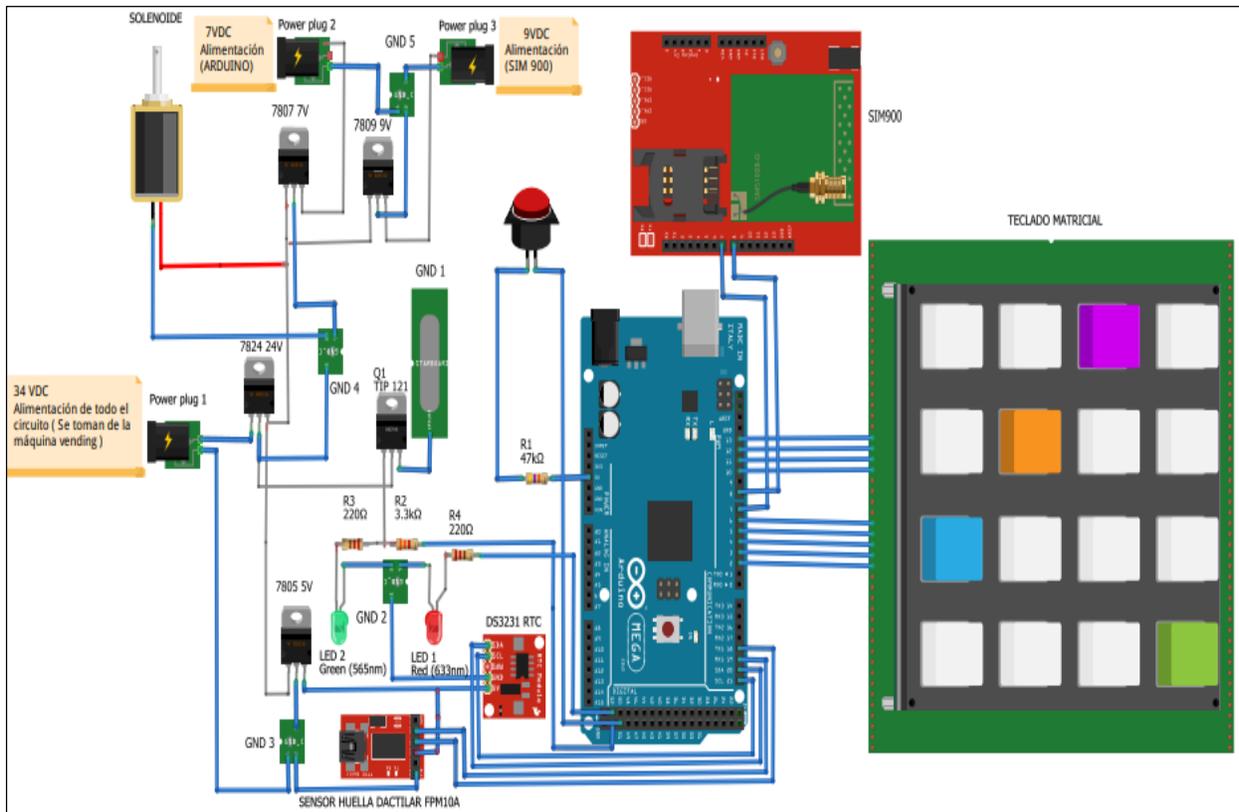


Figura 9. Sistema de comunicación y control

Fuente: Autor

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

En la Figura 11 “*Sistema de comunicación y control*” se observa el diagrama esquemático del circuito donde se conectan todos los componentes electrónicos que permiten el correcto funcionamiento del proyecto, se inicia con un transformador reductor de voltaje que permite realizar la reducción del voltaje de la red de 110 VAC 60HZ A 24VAC 60HZ, que ingresa a la tarjeta CPU de la máquina Vending tipo Snacks, ésta internamente realiza la conversión de voltaje de AC a DC y realiza la etapa de filtrado para finalmente entregar un voltaje DC para el funcionamiento normal de la CPU, siguiendo esta línea por el conector J19, se toma el voltaje DC que alimenta el Arduino Mega 2560 y el escudo GPRS SIM 900, esto se realiza mediante un regulador de voltaje que permite reducir y regular el voltaje entregado por la CPU de la máquina de 35 voltios y los regula a 24VDC, que es el voltaje requerido por el circuito para energizar los componentes que lo integran, a su vez en paralelo se conectan al circuito dos reguladores de voltaje de 9V y 7V que alimentarán al módulo SIM 900 y el Arduino Mega 2560 respectivamente.

Por el pin 14 del Arduino Mega 2560 se envía una señal de 5V cada vez que el circuito realiza una operación exitosa, sea esta la de accionar la chapa electrónica o simplemente indicar si la huella dactilar o la clave ingresada fue la correcta, este indicador led se acopla al circuito mediante una resistencia de 220 ohmios para su adecuado funcionamiento, adicional esta señal de 5V se hace pasar por una resistencia de 3,3 kilo ohmios para reducir el voltaje que recibirá un transistor TIP121 y que a su vez realiza el control de la señal de tierra y maneja el voltaje entregado por el regulador de 24 voltios mencionado en la primera parte y que se encarga también de controlar el accionamiento de la chapa electrónica.

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Al igual que el led verde, se conectó al circuito un led rojo que permite indicar cuando existe una falla o un error, ejemplo. Cuando no llega un mensaje completo o se ingresa la clave errada. El led se alimenta mediante el pin 52 del Arduino Mega 2560 y se realiza un acoplamiento con una resistencia de 220 ohmios y por el otro extremo del led se envía a ground.

Por otra parte, se tiene el Arduino Mega 2560 y las diferentes conexiones que permiten realizar el control de los módulos incluidos en el proyecto, iniciando con el sensor de huella dactilar, debido a que entrega la alimentación de 5V y su conexión a tierra. Adicional mediante los pines 18 y 19 del Arduino Mega 2560 se envían las señales de la recepción y transmisión del módulo FPM10A, además de controlar mediante los pines 7 y 8 la recepción y transmisión del módulo SIM900.

Otra tarea del Arduino Mega 2560 consiste en alimentar con 5V y ground el módulo DS3231 que, en un RTC o reloj de tiempo real, permite tener la fecha y hora actualizada para diferentes funciones del proyecto, adicional mediante los pines 20 y 21 se conectan los pines de SDA Y SCL para su transmisión y recepción.

El circuito también cuenta con un sensor on / off que permite detectar el estado de la puerta, si está abierta o cerrada. El Arduino Mega 2560 alimenta con 5V y se conecta a una resistencia de 47 kilo ohmios para amortiguar los rebotes del sensor y a su vez realizar la entrada de la señal del sensor mediante el pin 51 del Arduino.

Por último, se observa que el teclado matricial de la máquina ingresa al puerto J12 de la CPU para realizar las operaciones normales del equipo antes mencionadas, adicional se conecta este mismo teclado en paralelo al Arduino mediante los pines del 2 al 13 con excepción de los pines 7,8 y 9 usados en otra tarea del circuito.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### 3.2.2 Integración y configuración de los sistemas de comunicación y control

Para la integración de los sistemas se inicia con la placa de conexiones que es una tarjeta de circuito impreso donde se conectan los componentes eléctricos necesarios para la interconexión entre los componentes del sistema (sistema de comunicación y control), entre los cuales se encuentran: dos reguladores de voltaje que permiten reducir los 24 voltios de la tarjeta a 9 voltios para alimentación del Arduino Mega 2560 y la tarjeta SIM900, dos leds indicadores, uno verde que permite dar indicaciones visuales del proceso del equipo, como apertura de la puerta, lectura de la huella, cambio de clave exitosa; por otra parte el led rojo permite indicar fallas del sistema, como mal ingreso de la clave, error de comunicación y cambio de clave no exitosa, bornera para conexión del teclado y sistema de acondicionamiento eléctrico del sensor.

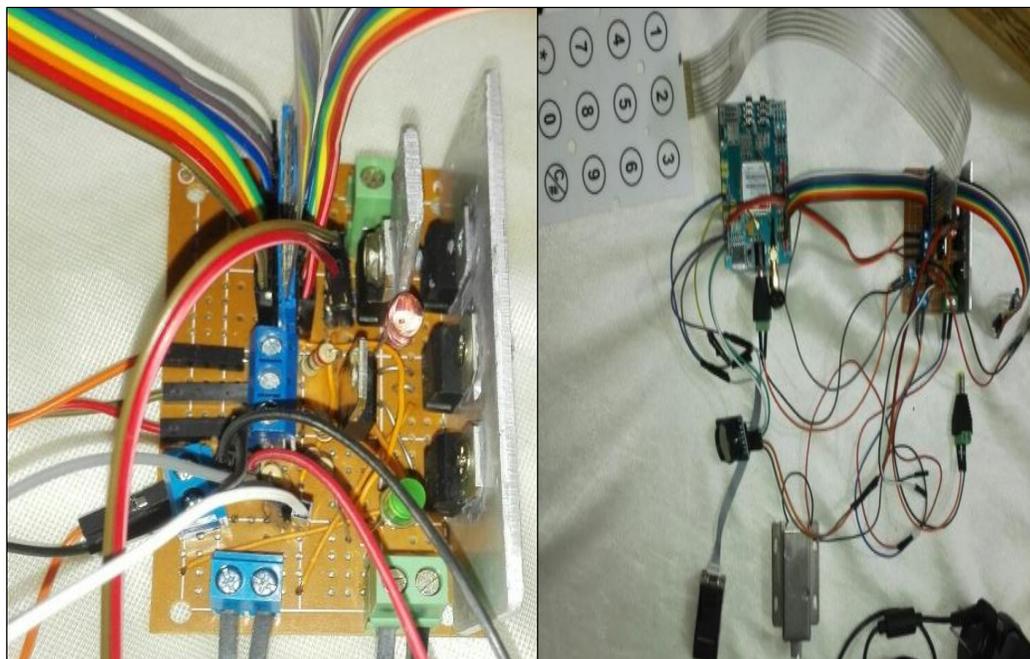


Figura 10. *Placa de conexiones*  
Fuente: Autor

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### **3.2.3 Programación del sistema para la administración del proyecto**

La programación del proyecto se realizó sobre la plataforma Arduino Mega 2560, bajo el lenguaje de programación processing, se inicia la programación incluyendo las librerías necesarias para ejecutar el proyecto, se definen variables globales y se realiza la configuración de los módulos SIM900 y Arduino Mega 2560, posteriormente se ejecutaron los comandos AT que permiten realizar la comunicación entre el administrador y el módulo GPRS, finalmente se declaran las funciones y acciones que el programa ejecutará para su correcto funcionamiento.

### **3.2.4 Integración del sistema de comunicación con la base de datos**

La información enviada por el sistema de comunicación conformado por el Arduino Mega 2560 y módulo SIM900, llegan como mensaje de texto al administrador (equipo móvil, computador, tablet, entre otros) los cuales son llevados a un archivo de Excel por medio de una herramienta gratuita llamada “SMStoExcel”, ésta permite enviar el archivo generado a la plataforma administradora de archivos Dropbox. La información es procesada, depurada y organizada por medio de una macro que se creó en Excel, que se encarga de descargar la información del archivo almacenado en Dropbox y alimentar la base datos.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### 3.3 Componentes aprovechados de la maquina Vending tipo Snacks

#### 3.3.1 Máquina Expendedora

La máquina Vending tipo Snacks utilizada en el proyecto es la expendedora de vidrio frontal modelo 35” y 39” o conocida comúnmente como máquina AMS Snacks VCB (Visi-Combo) del fabricante AUTOMATED MERCHANDISING SYSTEMS INC o Internacional A.M.S.

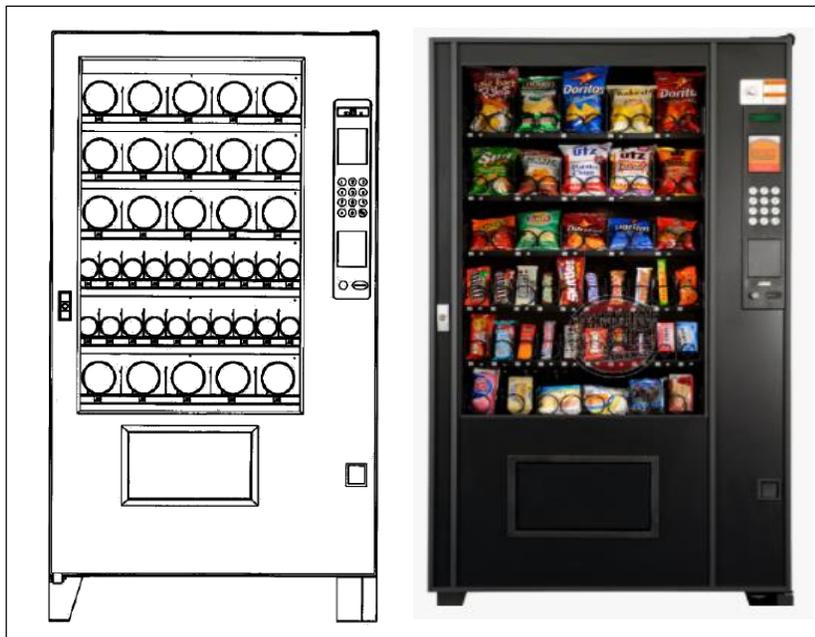


Figura 11. Foto máquina Vending Tipo Snacks

Fuente: Autor

#### 3.3.2 Tarjeta de control

La tarjeta de control es la encargada de monitorear y controlar la máquina Vending tipo Snacks, el puerto DEX y los dispositivos MDB. Está ubicada al interior de la máquina, en la esquina superior izquierda de la puerta; solo se puede acceder a ella cuando el equipo es abierto por el

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

operario. La tarjeta permite interconectar el teclado matricial, el Arduino Mega 2560 y el sensor de apertura y cierre de puerta.

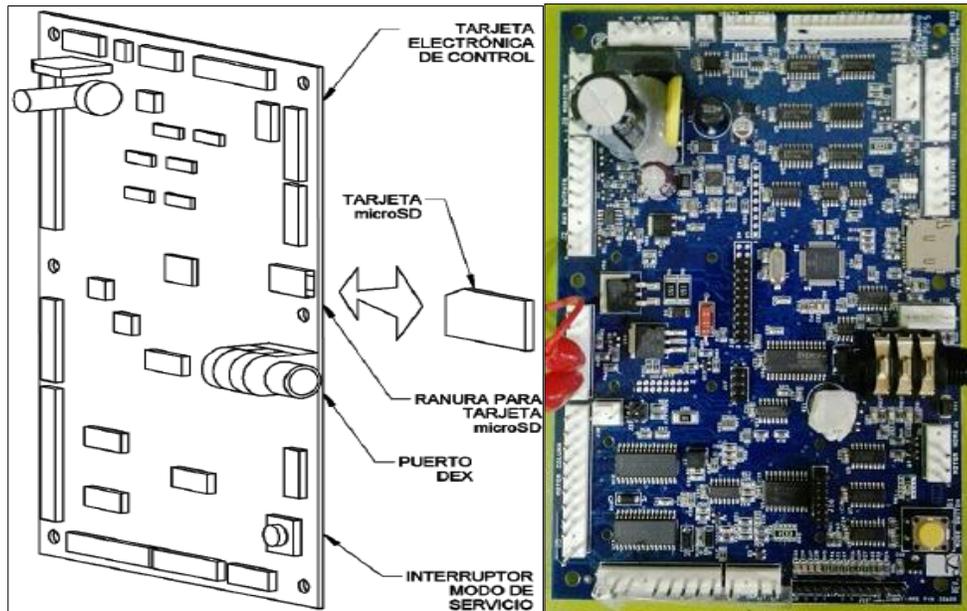


Figura 12. Tarjeta de control maquina Vending tipo Snacks  
Fuente: Autor

### 3.3.3 Fuente de alimentación

Está compuesta por un transformador que reduce el voltaje de entrada a 24 voltios AC para alimentar la tarjeta de control y un filtro RFI que elimina el ruido eléctrico de alimentación, para prevenir cualquier interferencia con el funcionamiento de la tarjeta de control y los componentes adicionales de la máquina. Este voltaje llega a la tarjeta el cual lo convierte a 24 Voltios DC, de este voltaje se toma el suministro eléctrico para alimentar los componentes del control de acceso de la máquina.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### 3.3.4 Teclado

La máquina Vending tipo Snacks tiene incorporado un teclado de tecnología matricial, éste se encuentra ubicado en la parte frontal del equipo, debajo de la pantalla. El teclado es utilizado principalmente para la selección de los productos que el usuario desea, también es usado para ingresar los parámetros en modo de servicio, en el proyecto se aprovechó para permitir el ingreso seguro del operario por medio de una clave numérica.

### 3.3.5 Sensor de puerta

El sensor de puerta (interruptor), se encuentra ubicado en la parte interna de la máquina, la función del sensor es monitorear el cambio de estado de la puerta ya sea que ésta se encuentre abierta o cerrada, paralelamente le indica a la máquina si está abierta, que se ponga en modo servicio y si está cerrada, se ponga en modo venta.

## 3.4 Instalación de los componentes en la máquina

En este punto se describe la instalación física de los diferentes componentes utilizados en el desarrollo del proyecto.

### 3.4.1 Instalación cerradura electromagnética

La cerradura electromagnética es de pequeñas dimensiones lo que permitió instalarla en la parte interna de la máquina, donde estaba ubicada anteriormente la cerradura mecánica. Ésta se instaló de tal forma que al ser energizada se contraiga el pestillo permitiendo así la apertura de la puerta

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

de la maquina Vending tipo Snacks. Al ser instalada internamente en la máquina, se garantiza que ésta no pueda ser vulnerada físicamente desde la parte externa con herramientas mecánicas como taladros, limadoras o destornilladores.



Figura 13. *Instalación chapa electromagnética*  
 Fuente: Autor

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

### 3.4.2 Instalación Teclado matricial

El teclado matricial no fue necesario instalarlo físicamente ya que se utilizó el teclado de la máquina Vending tipo Snacks, éste simplemente se enlazo con el Arduino Mega 2560 para que se comunique con el equipo administrador de las claves.



Figura 14. *Teclado en maquina Vending tipo Snacks*  
 Fuente: Autor

### 3.4.3 Instalación Sensor biométrico

Éste se instaló debajo del teclado matricial, por comodidad del operario y por espacio. Se adaptó un marco plástico con las dimensiones de la cara de lectura de la huella dactilar del sensor biométrico, se fijó internamente por medio de una lámina de aluminio y dos remaches.

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22



Figura 15. *Sensor de huella biométrica en máquina Vending tipo Snacks*  
Fuente: Autor

### **3.4.4 Instalación de la plataforma de administración, sistema de comunicación y placa de conexiones**

La plataforma de administración, el sistema de comunicación y la placa de conexiones fueron instalados internamente en la máquina Vending tipo Snacks en un espacio libre y seguro que ésta posee, adicionalmente es un punto estratégico ya que dicho sistema queda cerca de la tarjeta principal de la máquina, la cual enlaza el sistema de control del proyecto con la máquina. A este compartimiento se puede acceder únicamente cuando la máquina es abierta por personal autorizado.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

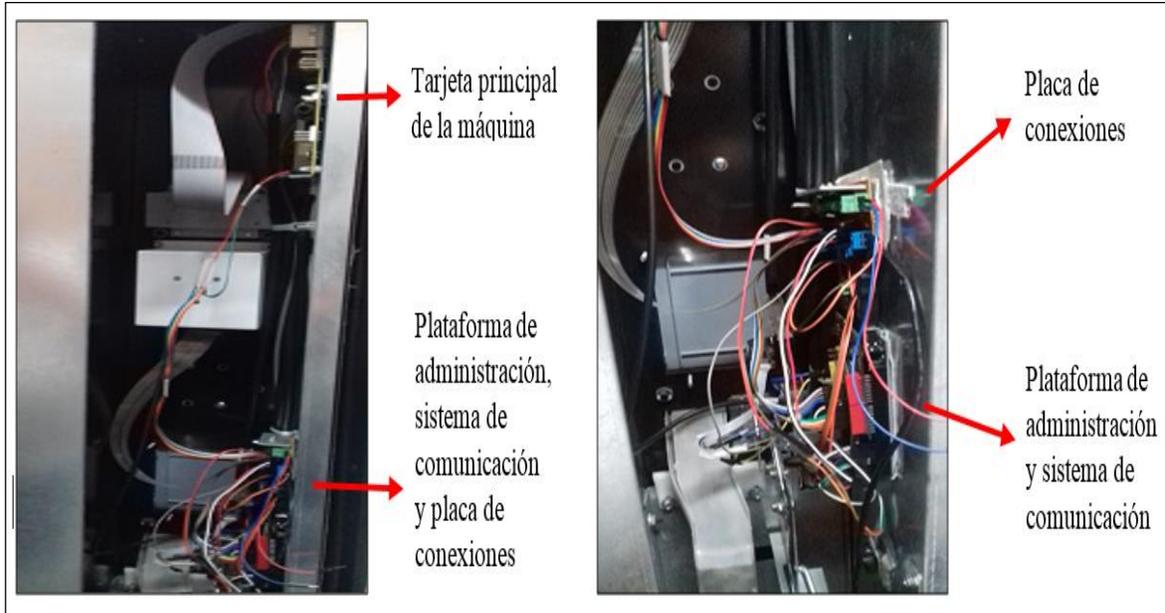


Figura 16. *Plataforma de administración, sistema de comunicación y placa de conexiones*

Fuente: Autor

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## 4 RESULTADOS Y DISCUSIÓN

---

En esta sección se realizaron las diferentes pruebas de funcionamiento de cada uno de los sistemas que integran la administración de control de acceso para máquinas Vending tipo Snack y a su vez se validaron los resultados.

### 4.1 Pruebas y validación de resultados

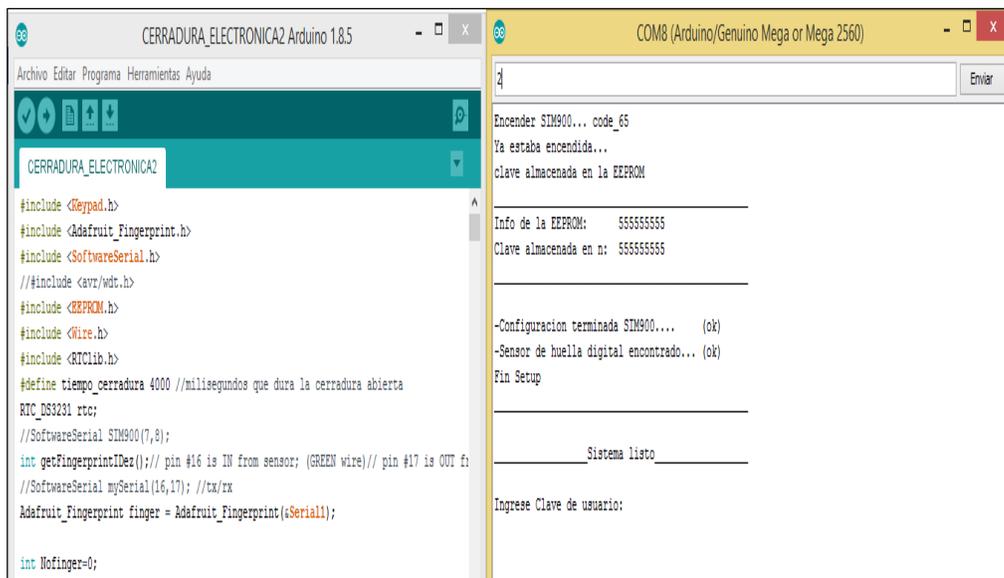
Concluida la instalación para la administración del control de acceso para la máquina Vending tipo Snacks, se procedió a realizar las pruebas con base a la siguiente lista de chequeo.

PRUEBA	PRUEBA REALIZADA	ESTADO
1	Conexiones de los dispositivos del administrador de control de acceso para máquinas Vending tipo Snacks	✓
2	Información de la clave almacenada en la EEPROM	✓
3	Configuración terminada de la SIM900	✓
4	Sensor de huella digital encontrado por el sistema	✓
5	Solicitud de ingreso de clave de usuario	✓
6	Confirmación del ingreso de clave correcta	✓
7	Solicitud de huella de usuario	✓
8	Apertura y cierre de cerradura electromagnética	✓
9	Ingreso erróneo de clave para acceso a la máquina *Bloqueo de terminal por ingreso incorrecto de la clave en 3 oportunidades	✓

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	<b>Código</b>	<b>FDE</b> 089
		<b>Versión</b>	03
		<b>Fecha</b>	2015-01-22

	*Terminal habilitada para ingresar de nuevo la clave correcta	
10	<b>Cambio de clave del usuario desde la plataforma administradora</b> *Envió de mensaje por cambio de clave exitoso de ingreso a la máquina *Envió de mensaje por ingreso de clave incorrecta para cambio de Clave	✓

Lo primero que se realizó fue la conexión de todos los dispositivos del administrador de control de acceso en la máquina Vending, posteriormente se comprobó en el programa que se cargara correctamente la información almacenada en la EEPROM, que es la clave de usuario que tiene actualmente la máquina, también se comprobó que la tarjeta SIM900 se hubiese conectado correctamente y que el sistema reconociera el sensor de huella digital. Con la configuración correcta del sistema, el administrador de control de acceso queda listo para ser operado.



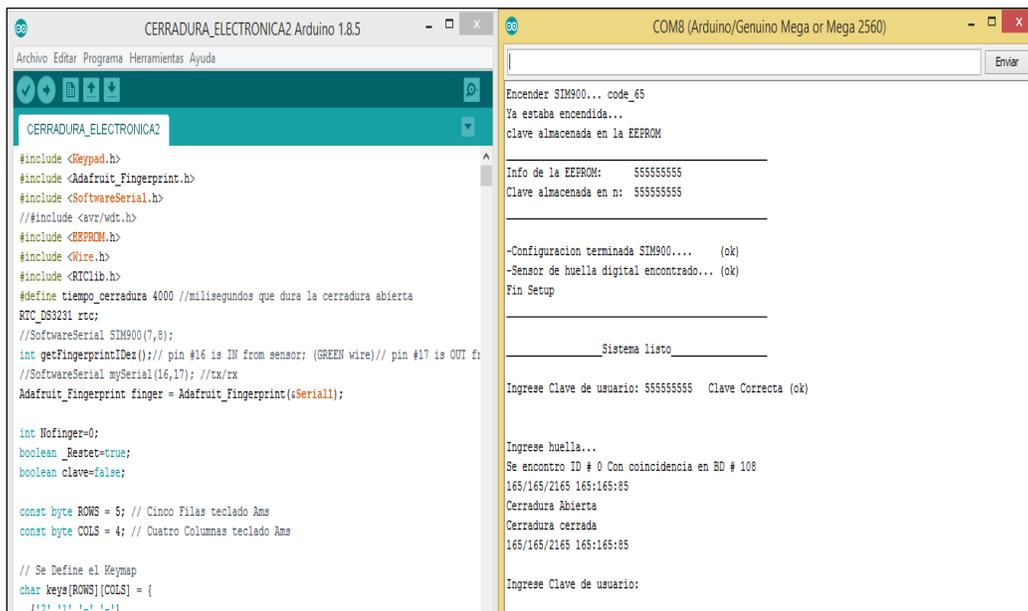
**Figura 17. Configuración sistema**  
Fuente: Autor

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Para comprobar el funcionamiento de la operación del sistema, se realizaron diferentes pruebas

#### 4.1.1 Prueba de ingreso a la máquina

Se realizaron dos pruebas, una con clave correcta y otra con clave incorrecta, las cuales se explican a continuación; en primera instancia el sistema solicita el ingreso de clave, la cual se ingresó desde el teclado de la máquina de forma correcta, posteriormente el sistema pidió la huella, al ser detectada la cerradura electromagnética se energizó contrayendo el pestillo permitiendo así la apertura de la puerta de la máquina, luego se hizo la prueba ingresando la clave de forma incorrecta, para evidenciar que el sistema no solicitará el ingreso de huella, ni se energizará la cerradura electromagnética, adicionalmente se comprobó que el sistema se bloqueea por el tiempo parametrizado en el programa, en el momento en que se ingresó la clave incorrecta tres veces.



```

CERRADURA_ELECTRONICA2 Arduino 1.8.5
COM8 (Arduino/Genuino Mega or Mega 2560)

Encender SIM900... code_65
Ya estaba encendida...
clave almacenada en la EEPROM

Info de la EEPROM:      5555555555
Clave almacenada en n: 5555555555

-Configuracion terminada SIM900.... (ok)
-Sensor de huella digital encontrado... (ok)
Fin Setup

Sistema listo

Ingrese Clave de usuario: 5555555555 Clave Correcta (ok)

Ingrese huella...
Se encontro ID # 0 Con coincidencia en BD # 108
165/165/2165 165:165:85
Cerradura Abierta
Cerradura cerrada
165/165/2165 165:165:85

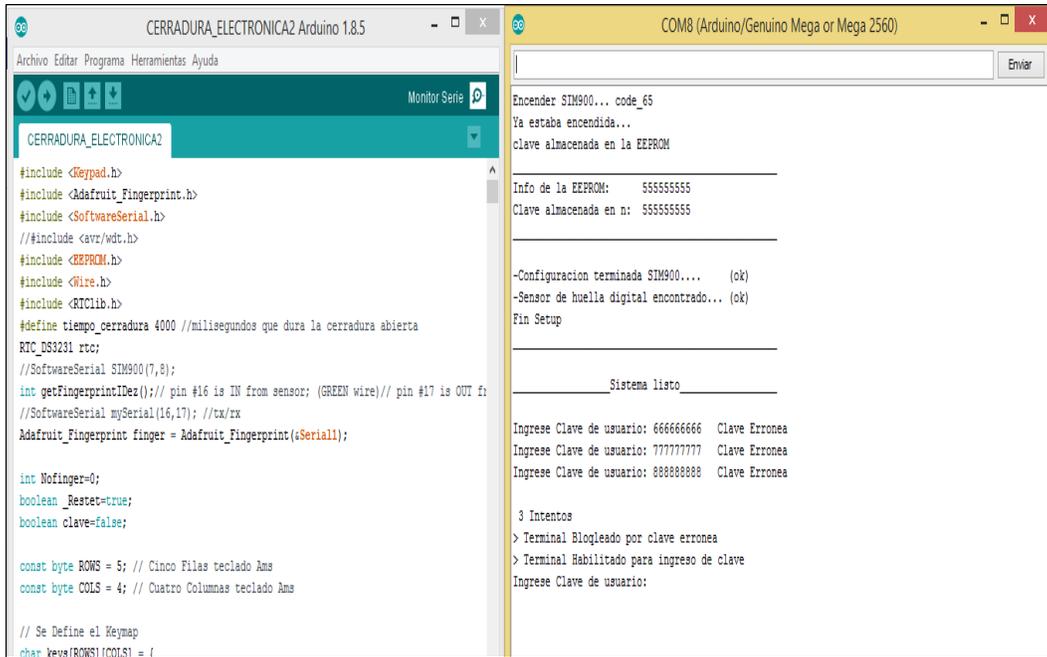
Ingrese Clave de usuario:

```

Figura 18. Prueba ingreso de clave correcta y huella dactilar

Fuente: Autor

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	<b>Código</b>	<b>FDE 089</b>
		<b>Versión</b>	<b>03</b>
		<b>Fecha</b>	<b>2015-01-22</b>



**Figura 19. Prueba ingreso de clave incorrecta**  
**Fuente: Autor**

#### **4.1.2 Prueba cambio de clave**

La prueba se inició enviando un mensaje desde la plataforma administradora (en este caso desde un celular), el mensaje enviado fue; @555555555\*111111111, el cual significa; @ indicador de clave actual, los nueve “5” son la clave actual, el \* indica la nueva clave que se asignará y los nueve “1”, es la clave nueva, en este caso fue un cambio de clave exitoso, ya que la clave inicio con el @ lo presidió la clave actual de la máquina que eran los “5” y en la cantidad correcta que es nueve caracteres, seguidamente está el \* y por último esta la nueva clave, la cual cumplió la condición de contener nueve caracteres; al cumplirse todas estas condiciones el mensaje recibido fue; “cambio de clave exitoso la nueva clave de la máquina es: 11111111”.

	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



Figura 20. Prueba cambio de clave correcta

Fuente: Autor

Las últimas pruebas realizadas fueron el envío del mensaje con clave incorrecta, las cuales fueron de la siguiente forma; una con la clave actual de la máquina incorrecta, otra con la clave a cambiar con un número menor a 9 dígitos y por último con la clave actual menor a 9 dígitos. En todas éstas se obtuvo como retorno un mensaje con la siguiente información “clave incorrecta, ingrese de nuevo” el cual llega al celular de la siguiente manera.



Figura 21. Prueba cambio de clave correcta

Fuente: Autor

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



Figura 22. Prueba cambio de clave incorrecta  
Fuente: Autor

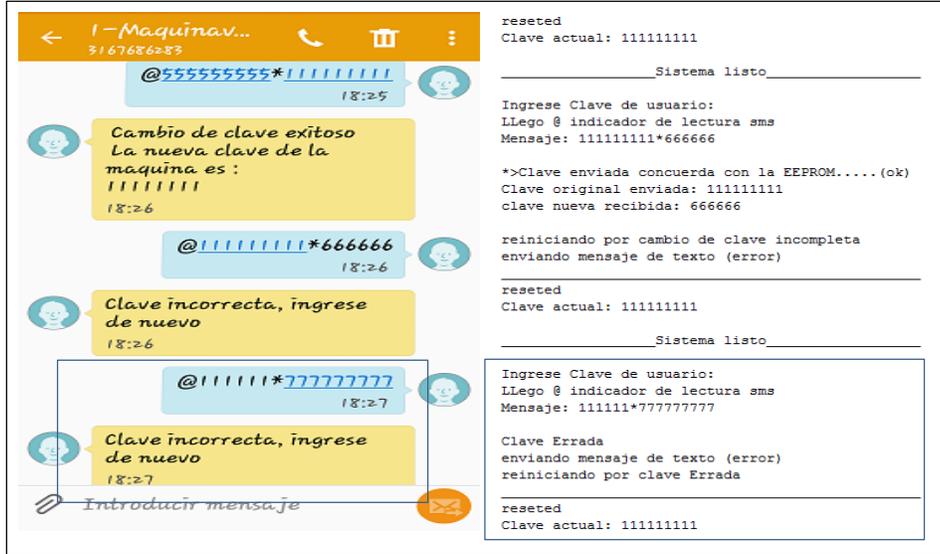


Figura 23. Prueba cambio de clave correcta  
Fuente: Autor

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

#### 4.1.3 Prueba base de datos

Después de haberse realizado las diferentes pruebas de ingreso a la máquina y los cambios de claves ya hubiese sido ésta correcta o incorrecta; se efectuó la prueba de la base de datos la cual consistió en lo siguiente:

La información enviada por el sistema de comunicación que llega como mensaje de texto al administrador (equipo móvil, computador, tablet, entre otros) se llevaron a un archivo de Excel por medio de la herramienta “SMStoExcel”, la cual envió el archivo generado a Dropbox, posteriormente se puso a correr la macro creada en Excel que tomo la información, la depuro y la organizó para alimentar así la base de datos e informar la clave actual de la máquina.

#MSM	TELEFONO	MAQUINA VENDIN	FECHA Y HORA DE LA INFORMACIÓ	TIPO MENSAJ	INFORMACION RECIBIDA O ENVIADA
1	3167686283	1-Maquinavending	2018-03-01 jue. 20:06:54	Sent	@22222222*11111111
2	3167686283	1-Maquinavending	2018-03-01 jue. 20:22:02	Sent	@22222222*11111111
3					Cambio de clave exitoso La nueva clave de la maquina es :
4	3167686283	1-Maquinavending	2018-03-01 jue. 22:33:32	Inbox	66666666
5	3167686283	1-Maquinavending	2018-03-01 jue. 20:24:01	Sent	@22222222*11111111
6	3167686283	1-Maquinavending	2018-04-27 vie. 09:48:38	Inbox	Clave incorrecta, ingrese de nuevo
7	3167686283	1-Maquinavending	2018-03-01 jue. 20:47:42	Sent	@11111111*55555555
8	3167686283	1-Maquinavending	2018-03-01 jue. 20:49:53	Sent	@11111111*55555555
9	3167686283	1-Maquinavending	2018-03-01 jue. 20:55:17	Sent	@55555555*88888888
10	3167686283	1-Maquinavending	2018-03-01 jue. 20:55:57	Sent	@55555555*88888888
11	3167686283	1-Maquinavending	2018-03-01 jue. 21:10:02	Sent	@88888888*55555555
12					Cambio de clave exitoso La nueva clave de la maquina es :
13	3167686283	1-Maquinavending	2018-03-01 jue. 21:53:26	Inbox	22222222

#MSM	TELEFONO	MAQUINA VENDING	FECHA Y HORA DE LA INFORMACION	TIPO MENSAJE	INFORMACION ENVIADA
2	321	3167686283 1-Maquinavending	2018-04-27 vie. 09:54:48	Sent	*11111111*44444444
3	320	3167686283 1-Maquinavending	2018-04-27 vie. 09:53:48	Sent	@11111111@11111111
4	318	3167686283 1-Maquinavending	2018-04-27 vie. 09:53:01	Sent	@11111111*6666
5	316	3167686283 1-Maquinavending	2018-04-27 vie. 09:52:21	Sent	@11111*66666666
6	314	3167686283 1-Maquinavending	2018-04-27 vie. 09:51:22	Sent	@22222222*33333333
7	312	3167686283 1-Maquinavending	2018-04-27 vie. 09:50:17	Sent	@55555555*11111111
8	310	3167686283 1-Maquinavending	2018-04-27 vie. 09:49:11	Sent	@55555555*11111111
9	308	3167686283 1-Maquinavending	2018-04-27 vie. 09:48:27	Sent	@55555555*11111111
10	297	3167686283 1-Maquinavending	2018-04-21 sáb. 14:55:12	Sent	@22222222*55555555
11	293	3167686283 1-Maquinavending	2018-04-19 jue. 08:19:55	Sent	Q2222222*11111111
12	292	3167686283 1-Maquinavending	2018-04-19 jue. 07:34:49	Sent	@11111111*33333333
13	291	3167686283 1-Maquinavending	2018-04-19 jue. 07:34:00	Sent	@11111111*66666666
14	290	3167686283 1-Maquinavending	2018-04-19 jue. 07:33:27	Sent	@11111111*55555555

#MSM	TELEFONO	MAQUINA VENDING	FECHA Y HORA DE LA INFORMACIÓ	TIPO MENSAJ	INFORMACION RECIBIDA
2	319	3167686283 1-Maquinavending	2018-04-27 vie. 09:53:10	Inbox	Clave incorrecta, ingrese de nuevo
3	317	3167686283 1-Maquinavending	2018-04-27 vie. 09:52:30	Inbox	Clave incorrecta, ingrese de nuevo
4	315	3167686283 1-Maquinavending	2018-04-27 vie. 09:51:30	Inbox	Clave incorrecta, ingrese de nuevo
5					Cambio de clave exitoso La nueva clave de la maquina es :
6	313				11111111
7					Cambio de clave exitoso La nueva clave de la maquina es :
8	311				11111111
9					Cambio de clave exitoso La nueva clave de la maquina es :
10	309	3167686283 1-Maquinavending	2018-04-27 vie. 09:48:38	Inbox	Clave incorrecta, ingrese de nuevo
11					Cambio de clave exitoso La nueva clave de la maquina es :
12	307				11111111
13					Cambio de clave exitoso

#MSM	TELEFONO	MAQUINA VENDING	FECHA Y HORA ULTIMA CLAVE ENVIAR	TIPO MENSAJ	INFORMACION RECIBIDA	CLAVE ACTUAL DE MAQUIN
2	307	3167686283 1-Maquinavending	2018-04-24 mar. 00:03:02	Inbox	Cambio de clave exitoso La nueva clave de la maquina es :	11111111

Figura 24. Base de datos  
Fuente: Autor

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## 5 CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

---

Con el desarrollo de este trabajo se logra realizar una plataforma de administración de control de acceso usando sistemas de identificación electrónica y de comunicación a las máquinas Vending tipo Snacks aumentando así su nivel de seguridad, de igual forma se comprobó que esta plataforma funciona eficientemente en el área metropolitana del valle de aburrá, dado que la cobertura móvil es muy amplia y el servicio que los diferentes operadores móviles ofrecen es constante y favorable.

Se concluye que es posible operar sistemas de comunicaciones móviles en las maquinas Vending tipo Snacks, debido a que permiten una gran versatilidad al ofrecer una comunicación constante con el equipo.

Se puede concluir que es factible la implementación de sistemas biométricos mediante huella dactilar en los equipos Vending tipo Snacks, debido a que aportan mayor nivel de seguridad y confiabilidad basadas en tecnologías modernas.

Es posible incorporar sistemas electrónicos de control de acceso para la seguridad física del equipo mediante la utilización de componentes electromecánicos que brindan confiabilidad y versatilidad a los sistemas de seguridad actuales.

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Se concluye que se puede modernizar los sistemas electrónicos de las maquinas Vending tipo Snacks y ampliar su capacidad operacional mediante dispositivos programables de fácil implementación y bajo costo.

### **5.1 Problemas presentados durante la ejecución del proyecto y en las pruebas realizadas**

El teclado matricial con el que se realizaron las pruebas fue un teclado matricial estándar compuesto por filas y columnas, pero al momento de realizar la integración al sistema de la máquina, se encontró que era una configuración matricial especial diseñada por el fabricante de la máquina Vending, lo que obligó a contactar al fabricante para solicitar las especificaciones técnicas del dispositivo.

En las pruebas realizadas de funcionamiento de la plataforma de administración se detectó que, al enviar un mensaje para cambio de clave, éste no se ingresaba completo, el sistema rellenaba automáticamente el vector y cambiaba la clave en la EEPROM por datos erróneos, lo que hacía que el sistema cambiara la clave, por una totalmente diferente a la enviada, por consiguiente, no se podía ingresar al equipo y se perdía la clave. Esto se corrigió mediante la programación del Arduino Mega 2560 agregando condicionales los cuales le dieron solución al problema.

Con el sensor de huellas, el problema presentado fue que cada vez que se ingresaba la clave numérica el sistema quedaba esperando un primer ingreso de la huella lo que es normal, pero si se

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

intentaba poner la huella nuevamente por segunda o tercera vez el sistema igual seguía abriendo la cerradura sin necesidad de ingresar la clave numérica, acción que no es válida para el funcionamiento del proyecto, esta novedad se corrigió mediante ajuste del código o programa.

Otro error que surgió durante las pruebas consistió en que cuando se enviaba un mensaje con la clave y por algún motivo ésta no era la correcta, el usuario administrador no tenía forma de saber si había alguna falla con la clave. Este inconveniente se solucionó mediante la modificación del código, agregando la instrucción para enviar un mensaje cada vez que había un error con la clave, para conocimiento del administrador.

Otro problema presentado fue con la instalación de la cerradura electrónica, debido a que la ubicación inicialmente planteada no se ajustaba al sistema mecánico de la máquina, este inconveniente se solucionó realizando un ajuste en la estructura de la puerta y consistió en perforar la lámina de la máquina para que la cerradura se alojara perfectamente y se ajustara al sistema mecánico.

Otro problema encontrado en las pruebas fue que cuando el proyecto se instaló en el equipo y se ingresaba la clave no se podía observar si se había ingresado los dígitos correctos o erróneos, algo indispensable para seguir con el ingreso de la huella y poder tener acceso a la máquina Vending. Para corregir esta novedad se modificó el código, de tal forma que el led verde parpadeara unos

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

segundos si se había ingresado la clave correctamente y luego poder ingresar la huella para la apertura de la máquina, de lo contrario parpadearía el led rojo indicando que la clave era errónea.

## 5.2 Trabajos futuros

Para trabajos futuros se puede implementar el censado de forma remota para el inventario de productos en la máquina Vending tipo Snacks, debido a que en la actualidad no se tiene la información de la rotación del producto, ni el momento en que se agota, esta información solo se obtiene hasta la siguiente visita a la máquina, lo que genera pérdidas de venta e información clave como: preferencias alimenticias de los clientes, franjas de consumo, vencimiento y rotación de los productos.

Otro trabajo futuro puede ser el manejo remoto de fallas presentadas en el monedero de las máquinas Vending tipo Snacks, en la actualidad hay muchas pérdidas debido a que la máquina automáticamente se bloquea y queda fuera de servicio cuando el monedero presenta fallas. El estado de bloqueo de la máquina solo se puede saber únicamente cuando el operario realiza la visita de rutina.

Cómo trabajo futuro también se puede implementar una base de datos de mayor complejidad que permita organizar de manera más avanzada los datos y personalizarla acorde a la necesidad de cada usuario.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## REFERENCIAS

---

- Aguilar, G., Sánchez, G., Toscano, K., Nakano, M., & Pérez, H. (2008). Reconocimiento de Huellas Dactilares Usando. *ESIME*, 101-109.
- Askix.com*. (13 de Agosto de 2017). Obtenido de Askix.com: <http://www.askix.com/como-cambiar-el-fusible-bits-de-avr-atmega328p-microcontrolador-de-8-bits-con-arduino.html>
- Dinero.com*. (13 de Agosto de 2017). Obtenido de Dinero.com: <http://www.dinero.com/empresas/articulo/mercado-de-las-maquinas-dispensadoras-tiene-oportunidades-en-colombia/223371>
- Mcculloch, C. (13 de Agosto de 2017). *ehowenespanol.com*. Obtenido de ehowenespanol.com: [http://www.ehowenespanol.com/cuanto-dinero-gana-promedio-maquina-expendedora-hechos\\_430490/](http://www.ehowenespanol.com/cuanto-dinero-gana-promedio-maquina-expendedora-hechos_430490/)
- McHugh, S., & Yarmey, K. (2012). Near Field Communication: Introduction and Implications. *ERIC*, 22.
- Méndez, I. G. (13 de Agosto de 2017). *Emprendedores.es*. Obtenido de Emprendedores.es: <http://www.emprendedores.es/gestion/introduccion-negocio-del-vending>
- Paz, N. d. (10 de Agosto de 2017). *Monografias.com*. Obtenido de Monografias.com: <http://www.monografias.com/trabajos56/huellas-lofoscopicas/huellas-lofoscopicas3.shtml#ixzz4qzMAXWoW>
- Ritz, J., & Knaack, Z. (2017). Internet of Things. *Technology and Engineering Teacher*, 28-33.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Saravia, M. W. (2016). Access control system using NFC and Arduino. *IEEE*, 1-6.

*Wikipedia.org*. (10 de Agosto de 2017). Obtenido de *Wikipedia.org*:

[https://es.wikipedia.org/wiki/Sensor\\_de\\_huella\\_digital](https://es.wikipedia.org/wiki/Sensor_de_huella_digital)

*Wikipedia.org*. (20 de Abril de 2017). Obtenido de *Wikipedia.org*:

[https://es.wikipedia.org/wiki/Servicio\\_general\\_de\\_paquetes\\_v%C3%ADa\\_radio](https://es.wikipedia.org/wiki/Servicio_general_de_paquetes_v%C3%ADa_radio)

*Wikipedia.org*. (20 de Abril de 2017). Obtenido de *Wikipedia.org*:

<https://es.wikipedia.org/wiki/Ethernet>

*Wikipedia.org*. (20 de Abril de 2017). Obtenido de *Wikipedia.org*:

[https://es.wikipedia.org/wiki/Base\\_de\\_datos](https://es.wikipedia.org/wiki/Base_de_datos)

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

## ANEXOS

Anexo A. Tabla comparativa especificaciones técnicas de tarjetas de programación

DESCRIPCIÓN	ESPECIFICACIONES			
				
Modelo	Uno	Mega / Mega 2560	Stellaris Launchpad LM4F120	Raspberry Pi Mod.B
Microcontrolador	AVR Atmega 328 8 bits	AVR ATmega2560 8bits	ARM LM4F120H5QR Cortex-M4 32bits	ARM Broadcom BCM2835
Frecuencia	16Mhz	16Mhz	80Mhz	700mHz
Memoria RAM	2KiB	8KiB	32KiB	512MiB
Memoria EEPROM	1KiB	4KiB	-	-
Memoria FLASH	32KiB	128 ó 256KiB	256KiB	-
Pines digitales entradas/salidas	14/14	54/54	43/43	8/8
Tensión/corriente pines digitales	5v 40Ma	5v 40mA	5v	-
Pines analógicos entradas/salidas	6/0	16/0	-	-
Tensión/resolución pines analógicos	5v 10bits (1024 valores)	5v 10bits (1024 valores)	-	-
Pines con interrupción externa	2	6	-	-
Pines PWM	6	15	-	-
Conexiones serial/UART	1	4	8	Si

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO			Código	FDE 089
				Versión	03
				Fecha	2015- 01-22

Conexiones I2C/TWI	1	1	4	Si
Conexiones ISP/ICSP	1	1	-	Si
Conexión USB	Si, USB-B	Si, USB-B	Si, Nativa, MicroUSB	Si, MicroUSB
Corriente en el pin de 5v	500~800Ma	500~800mA	-	-
Corriente en el pin de 3.3v	50Ma	50mA	-	-
Voltaje de alimentación por el USB	5v	5v	5v	5v
Voltaje de alimentación recomendado por el Jack	7 ~12v	7~12v	-	-
Voltaje de alimentación limite por el Jack	6~20v	6~20v	-	-

Anexo B. Tabla comparativa especificaciones técnicas de tarjetas basadas en la tecnología

GPRS

CARACTERÍSTICAS	ESPECIFICACIONES	
	SIM800	SIM900
Voltaje de Alimentación	3.4~4.4V	3.2~4.8V
Voltaje On/Off	VBAT	3V
Voltaje de reloj de tiempo real	1~2.8V	2~3.15V
Corriente de salida	50mA	10mA
Corriente de respaldo	100mA	No soportado
Voltaje de activación On/Off	<1.7V	<0.42V

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Voltaje de entrada de alto nivel (VIH)	2.1<VIH<3.1	2.4<VIH
Voltaje de entrada de bajo nivel (VIL)	-0.3<VIL<0.7	VIL<0.4
Voltaje de salida de alto nivel (VOH)	>2.4V	>2.7V
Voltaje de salida de bajo nivel (VOH)	<0.4V	<0.1V
Tiempo de reseteo	>105mS	>20uS
Velocidad máxima de transmisión	85.6 Kbps	85.6 kbps
Codificación	CS 1, 2, 3, 4	CS 1, 2, 3, 4
Protocolo	TCP/IP	TCP/UDP
Temperatura de operación	40°C to +85 °C	40°C to +85 °C

#### Anexo C. Tabla especificaciones técnicas teclado matricial

DESCRIPCIÓN	ESPECIFICACIÓN
Vida útil	Aproximadamente 1,000,000 ciclos de operaciones
Conector estándar	2.54 mm (0.1")
Dígitos	0-9 símbolos * y #
Tamaño	70 x 77 x 0.8 mm
Longitud de cables	85 mm (incluyendo el conector)
Conector	Tipo hembra de 8 pines, espaciamento 0.1"
Capacidad máxima	35 vdc, 100 ma
Aislamiento	100M Ohm, 100V
Rigidez dieléctrica	250 vrms (60Hz, 1 min)
Contacto de rebote	<= 5 ms
Temperatura de funcionamiento	-20 a +40 °C

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Anexo D. Tabla comparativa especificaciones técnicas sensor de huella biométrica

DESCRIPCIÓN	DESCRIPCIÓN	
	ZFM-20 Módulo de identificación de huellas dactilares	FPM10A Módulo de identificación de huellas dactilares
Voltaje de suministro	3.6 - 6.0VDC	3.6 - 6.0VDC
Corriente de funcionamiento	120mA max	120mA max
Corriente máxima	150mA max	150mA max
Tiempo de imagen de huellas dactilares	<1.0 segundos	<1.0 segundos
Área de la ventana	14 mm x 18 mm	14 mm x 18 mm
Archivo de firma	256 bytes	256 bytes
Archivo de plantilla	512 bytes	512 bytes
Capacidad de almacenamiento	162 plantillas	1000
Calificaciones de seguridad	5 (siendo 5 la calificación más alta)	5 (siendo 5 la calificación más alta)
Tasa de aceptación falsa	<0.001% (Nivel de seguridad 3)	<0.001% (grado de seguridad 3)
Interfaz	serie TTL	serie TTL
Velocidad en baudios	9600, 19200, 28800, 38400, 57600 (por defecto es 57600)	9600, 19200, 28800, 38400, 57600 (por defecto es 57600)
Clasificación de temperatura de trabajo	-20C a + 50C	-20C a + 50C
Humedad de trabajo	40% -85% HR	40% -85% HR
Dimensiones completas	56 x 20 x 21.5 mm	56 x 20 x 21.5 mm
Peso	20 gramos	Peso: 22 gramos

 <b>Institución Universitaria</b>	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Anexo E. Tabla especificaciones técnicas cerradura electromagnética

DESCRIPCIÓN	ESPECIFICACIONES
Voltaje	12V - 24V dc
Consumo de corriente	12V/ma
Estado	Normalmente abierto
Longitud de extensión	9.8 mm
Tamaño de la cerradura	53 x 39 x 25 mm
Dimensión del perno	9.8 x 9 mm
Peso	150g
Tiempo de desbloqueo	1 seg
Tiempo energizado	10 seg
Potencia	5W

Anexo F. Tabla comparativa especificaciones técnicas Reloj de tiempo real

CARACTERÍSTICAS	ESPECIFICACIONES		
	DS3231	DS1307	DS1302
El reloj en tiempo real cuenta segundos, minutos, horas, fecha del mes, mes, día de la semana y año, con una compensación de año bisiesto válida hasta 2100	SI	SI	SI
Señal de salida de onda cuadrada programable	SI	SI	X
Batería de respaldo	De entrada, para la hora normal continua	De respaldo con el oscilador funcionando	Utiliza menos de 300nA a 2.0V
Voltaje de operación	3.3V	3V	De 2.0V a 5.5V
Rangos de temperatura de funcionamiento	-40 °C a + 85 ° C	-40 °C a + 85 ° C	-40 °C a + 85 ° C

 Institución Universitaria	<b>INFORME FINAL DE TRABAJO DE GRADO</b>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

Precisión $\pm$ 2ppm	De 0 ° C a + 40 ° C	X	X
Precisión $\pm$ 3.5ppm	De -40 ° C a + 85 ° C	X	X
Salida del sensor de temperatura digital	$\pm$ 3 ° C de precisión	X	X
Dos alarmas de hora del día	SI	SI	SI

Anexo G. Código de programación para la administración de control de acceso para máquinas Vending tipo Snacks

```
#include <Keypad.h>
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
//#include <avr/wdt.h>
#include <EEPROM.h>
#include <Wire.h>
#include <RTClib.h>
#define tiempo_cerradura 4000 //milisegundos que dura la cerradura abierta
RTC_DS3231 rtc;
//SoftwareSerial SIM900(7,8);
int getFingerprintIDez();//
//SoftwareSerial mySerial(16,17); //tx/rx
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&Serial1);

int Nofinger=0;
boolean _Restet=true;
boolean clave=false;
```

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

const byte ROWS = 5; // Cinco Filas teclado Ams

const byte COLS = 4; // Cuatro Columnas teclado Ams

// Se Define el Keymap

```
char keys[ROWS][COLS] = {
    {'2','1','-','-'},
    {'4','3','-','-'},
    {'6','5','-','-'},
    {'8','7','-','-'},
    {'0','9','#','*'}
};
```

byte rowPins[ROWS] = {2,3,4,5,6}; //Filas

byte colPins[COLS] = {10,11,12,13}; //Columnas

// Creamos el Keypad

Keypad keypad = Keypad( makeKeymap(keys), rowPins, colPins, ROWS, COLS );

char customKey;

int led =52;

int led2 =53;

int i=0,j=0;

int z,s,ok,error;

char n[10];

char r[10];

int DATO[10]; //ingresa por teclado

char a,b;

int memoria=0;

boolean condicion=true;

char infoserial[20];

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```
const int suichepuerta = 7;
```

```
int valor = 0;
```

```
int contador=0;
```

```
int key;
```

```
int v=0;
```

```
int SW=51;
```

```
void setup()
```

```
{
```

```
// wdt_disable(); //perro guardian
```

```
Serial.begin(19200);
```

```
finger.begin(57600);//57600
```

```
Serial2.begin(19200);//configuracion serial sim900
```

```
pinMode(led,OUTPUT);//led indicador de sensado
```

```
pinMode(led2,OUTPUT);//led indicador de sensado
```

```
pinMode(9,OUTPUT);//Encender tarjeta GSM
```

```
pinMode(51,INPUT);
```

```
pinMode(suichepuerta , INPUT);
```

```
pinMode(7 , INPUT);
```

```
pinMode(8 , INPUT);
```

```
SIM900Encender();// encender tarjeta GSM
```

```
Huella_sensor();
```

```
delay(6000);
```

```
Serial.println("Fin Setup");
```

```
Serial.println("_____");
```

```
}
```

```
void loop(){
```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial.println();
Serial.println("_____Sistema listo_____");
Serial.println();
Serial.print("Ingrese Clave de usuario: ");
_Restet=true;

while(_Restet){
  leer_teclado();
  leer_mensaje();

  //
  if(clave){
    Serial.println();
    Serial.print("Ingrese huella...");
  }
  while(clave){
    lector_de_huellas();
  }
  //////////////////////////////////////
  while(digitalRead(SW)==HIGH){

  }
  }
  }

  void Reset(){
for( int i = 0; i < sizeof(infoserial); ++i){
  infoserial[i] = (char)0;
}

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

for( int i = 0; i < sizeof(DATO); ++i ){
DATO[i] = (char)0;
}
for(int m=0; m<=8; m++){
  n[m] = EEPROM.read(m);
}
  _Restet=false;
  clave=false;
  Serial.println("_____");
  Serial.println("reseted");
  Serial.print("Clave actual: ");
  for(i=0; i<=8; i++){
  Serial.print( n[i]);
  }
  Serial.println();
  delay(800);
}
void SIM900Encender()// encender la tarjeta sim
{
  Serial.print("Encender SIM900...");
  Serial2.println("AT+");
  delay(80);
for(int i=0; i < 100; ++i ){
  if(Serial2.available(>0)
  {
    Serial.print(" code_");
    Serial.println(Serial2.read());
    Serial.println("Ya estaba encendida...");

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

goto salto;
}

}

//delay(1000);
digitalWrite(9,HIGH);
delay(800);
digitalWrite(9,LOW);
delay(7000);
Serial.print(".....");
Serial.println("");
salto:
//////////comprueba eeprom//////////
EEPROM.update(0,'2');
EEPROM.update(1,'2');
EEPROM.update(2,'2');
EEPROM.update(3,'2');
EEPROM.update(4,'2');
EEPROM.update(5,'2');
EEPROM.update(6,'2');
EEPROM.update(7,'2');
EEPROM.update(8,'2');
Serial.println("clave almacenada en la EEPROM");
Serial.println("_____");
Serial.print("Info de la EEPROM:  ");
Serial.print(char(EEPROM.read(0)));
Serial.print(char(EEPROM.read(1)));
Serial.print(char(EEPROM.read(2)));

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial.print(char(EEPROM.read(3)));
Serial.print(char(EEPROM.read(4)));
Serial.print(char(EEPROM.read(5)));
Serial.print(char(EEPROM.read(6)));
Serial.print(char(EEPROM.read(7)));
Serial.println(char(EEPROM.read(8)));
//////////////////////////////////Imprime fecha //////////////////////////////////
//////////////////////////////////leer eeprom //////////////////////////////////
for(int m=0; m<=8; m++){
  n[m] = EEPROM.read(m);
}
Serial.print("Clave almacenada en n: ");
for(i=0; i<=8; i++){
  Serial.print( n[i]);
}
Serial.println();
Serial.print("_____");
Serial.println();
delay(5000);
configuracion_inicial();
}
void configuracion_inicial();//configura los codigos de lectura de mensajes
{
  Serial2.println("AT+CMGF=1\r");// modo mensajes para celulares
  delay(200);
  Serial2.println("AT+CPAS");//Chequeo actividad SIM900
  delay(200);
  Serial2.print("AT+CLIP=1\r");// Activamos la identificación de llamadas

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial.println("");
delay(200);
Serial2.println("AT+CNMI=2,2,0,0,0\r");//se envia mensajes al arduino via comunicacion
serial
delay(200);
Serial2.println("AT+CMGL=?");//muestra mensajes recibidos
delay(200);
Serial2.println("AT+CMGD=4\r");//borra mensajes en el programa
delay(200);
Serial2.println("AT+CSCS=IRA\r");//borra mensajes en el programa
delay(200);
//finger.begin(57600);
Serial.println("-Configuracion terminada SIM900.... (ok)");
}
////////////////////////////////////
void leer_mensaje()
{
  salir:
  if(Serial2.available(>0)
  {
    a = Serial2.read();

    if(a=='@')//el arroba hace detectar el inicio del codigo
    {
      //If arroba
      Serial.println();
      Serial.println("LLego @ indicador de lectura sms");//para verificar si lo detecto
      //////////////////////////////////
      error=0;

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

while(true)//ingresa en un while para leer solo los codigos futuros que estan por llegar despues de la arroba

```

{
if(Serial2.available()>0)
{//cierre del segundo if
b =Serial2.read();// Lectura de mensaje
infoserial[j]= b;//almacena en cadena de caracteres, suma de caracteres
j++;
////////////////////////////////////
if (b=='\n')//cuando termine de entregar todos los datos dara un enter
//garantizando el final del codigo
{
Serial.print("Mensaje: ");//IMPRIME LOS CARACTERES ALMACENADOS PARA
VER SI TODO ESTA OK
for(int i=0;i<j;i++)
{
Serial.print(infoserial[i]);//IMPRIME TODO EL CODIGO GUARDADO EN EL
ARRAY
}
Serial.println();

// Serial.print("lectura previa eeprom: ");
// Serial.print(n[0]);
// Serial.print(n[1]);
// Serial.print(n[2]);
// Serial.print(n[3]);
// Serial.print(n[4]);
// Serial.print(n[5]);

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```
// Serial.print(n[6]);
// Serial.print(n[7]);
// Serial.println(n[8]);
// Serial.println("Termina verificacion de datos EEPROM Y Serial");
```

```
led_cambio_on(); // encender led si guarda clave nueva en eeprom
```

```
b=0;
```

```
a=0;
```

```
j=0;//borra el puntero o acumulador si no se hace esto no detecta los siguientes
```

codigos

```
goto salir;//sale de todos los ciclos y va al inicio para volver a leer codigo
```

```
}//CIERRA AL /N
```

```
////////////////////////////////////
```

```
} //cierre del segundo if
```

```
}//while
```

```
}//arroba
```

```
}//serial available
```

```
}
```

```
////////////////////////////////////
```

```
void led_cambio_on(){
```

```
if(infoserial[0]==n[0] && infoserial[1]==n[1] && infoserial[2]==n[2] &&
infoserial[3]==n[3] && infoserial[4]==n[4] && infoserial[5]==n[5]&& infoserial[6]==n[6] &&
infoserial[7]==n[7] && infoserial[8]==n[8])
```

```
{
```

```
Serial.print(char(infoserial[9]));
```

```
Serial.print(">Clave enviada concuerda con la EEPROM.....(ok) ");Serial.println();
```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

//////////leer clave nueva que se almacenara en eeprom //////////

```

Serial.print("Clave original enviada: ");
    Serial.print(infoserial[0]);
    Serial.print(infoserial[1]);
    Serial.print(infoserial[2]);
    Serial.print(infoserial[3]);
    Serial.print(infoserial[4]);
    Serial.print(infoserial[5]);
    Serial.print(infoserial[6]);
    Serial.print(infoserial[7]);
    Serial.println(infoserial[8]);

Grabar_eeprom();

}
else
{
digitalWrite(led2,HIGH);
Serial.println("Clave Errada ");

mensaje_clave_incorrecta();
Serial.println("reiniciando por clave Errada");
digitalWrite(led2,LOW);
Reset();
}
}

//////////grabar eeprom //////////
void Grabar_eeprom()
{

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

if(InfoSerial[9]== '*')
{
Serial.print("clave nueva recibida: ");
for(i=10; i<=18; i++){
Serial.print( char(InfoSerial[i]) );
}
Serial.println();
if(j<21){
Serial.println("reiniciando por cambio de clave incompleta");
mensaje_clave_incorrecta();
Reset();
}

if(InfoSerial[18]>47 && InfoSerial[18]<58 && _Restet==true){

EEPROM.update(0, InfoSerial[10]);
delay(20);
EEPROM.update(1, InfoSerial[11]);
delay(20);
EEPROM.update(2, InfoSerial[12]);
delay(20);
EEPROM.update(3, InfoSerial[13]);
delay(20);
EEPROM.update(4, InfoSerial[14]);
delay(20);
EEPROM.update(5, InfoSerial[15]);
delay(20);
EEPROM.update(6, InfoSerial[16]);

```

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

delay(20);
EEPROM.update(7, infoserial[17]);
delay(20);
EEPROM.update(8, infoserial[18]);
delay(20);
digitalWrite(led2, HIGH);
Serial.println();
Serial.println( ">>>Clave nueva actualizada<<<<");
// Serial.print("verificacion datos almacenados EEPROM: ");
// Serial.print(char(EEPROM.read(0)));
// Serial.print(char(EEPROM.read(1)));
// Serial.print(char(EEPROM.read(2)));
// Serial.print(char(EEPROM.read(3)));
// Serial.print(char(EEPROM.read(4)));
// Serial.print(char(EEPROM.read(5)));
// Serial.print(char(EEPROM.read(6)));
// Serial.print(char(EEPROM.read(7)));
// Serial.println(char(EEPROM.read(8)));
mensaje_cambio_exitoso();
digitalWrite(led2,LOW);
Serial.println();
Serial.println( "Reiniciando el sistema, para actualizar clave");
Reset();

}
}
}

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

void leer_teclado()
{
if(error <3){

char key = keypad.getKey();
if (key != NO_KEY){
Serial.print(key);
DATO[z]=key;
Serial.print("");
z++;
if (z==9){
for (int j=0;j<=8;j++){
if (n[j]==DATO[j]){
ok++;
}
}
}

//Serial.println("");
/*
Serial.print(n[0]);
Serial.print(n[1]);
Serial.print(n[2]);
Serial.print(n[3]);
Serial.print(n[4]);
Serial.print(n[5]);
Serial.print(n[6]);

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial.print(n[7]);
Serial.println(n[8]);
Serial.println("");
Serial.print(DATO[0]);
Serial.print(DATO[1]);
Serial.print(DATO[2]);
Serial.print(DATO[3]);
Serial.print(DATO[4]);
Serial.print(DATO[5]);
Serial.print(DATO[6]);
Serial.print(DATO[7]);
Serial.println(DATO[8]);

```

\*/

```

if(ok==9){
error=0;
Serial.println(" Clave Correcta (ok)");
Serial.println();
for (int j=0;j<=8;j++){
DATO[j]=0;
}
clave=true;
//digitalWrite(led, HIGH); // encendemos el verde
//delay(3000);
//digitalWrite(led, LOW);
}
if(ok<9){
error++;
if (error == 3){

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial.println(" Clave Erronea");
Serial.println(" ");
Serial.println(" 3 Intentos");
Serial.println("> Terminal Bloqueado por clave erronea");
digitalWrite(led2,HIGH); // apagamos el LED rojo
delay(2000);
Serial.println("> Terminal Habilitado para ingreso de clave");
digitalWrite(led2,LOW);
Serial.print("Ingrese Clave de usuario: ");
error=0;
}
else{
Serial.println(" Clave Erronea");
Serial.print("Ingrese Clave de usuario: ");
//delay(1000);
}
}
ok=0;
z=0;
}
}
}
}

void mensaje_clave_incorrecta(){
Serial.println("enviando mensaje de texto (error)");
Serial2.print("AT+CMGF=1\r");
delay(100);

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial2.println("AT + CMGS = \"+573043878802\"); // numero del usuario
delay(100);
Serial2.println("Clave incorrecta, ingrese de nuevo");//mensaje a enviar
delay(100);
Serial2.println((char)26);//termino la comunicaciÃ³n
delay(100);
Serial2.println();
delay(2000);
Serial2.flush();
}
void mensaje_cambio_exitoso()
{
Serial.println("enviando mensaje de texto (exitoso)");
Serial2.print("AT+CMGF=1\r");
delay(100);
Serial2.println("AT + CMGS = \"+573043878802\");// numero del usuario
delay(100);
Serial2.println(" Cambio de clave exitoso ");//mensaje a enviar
Serial2.println(" La nueva clave de la maquina es : ");//mensaje a enviar
for(int m=0; m<=8; m++){
n[m] = EEPROM.read(m);
}
for(i=0; i<=8; i++){
Serial2.print( n[i] );//clave enviada al coordinador
}
delay(200);
Serial2.println((char)26);//termino la comunicaciÃ³n
delay(100);

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial2.println();
delay(4000);
Serial2.flush();
}

void Huella_sensor(){
if (finger.verifyPassword()){
Serial.println("-Sensor de huella digital encontrado... (ok)");
}
else
{
Serial.println("No se encontro el sensor de huellas dactilares :(");
delay(10000);
//while (1);
}
}

void lector_de_huellas()
{

getFingerprintIDez();
Nofinger += getFingerprintIDez();
if(Nofinger == -30 || Nofinger == -60){
Serial.print("Esperando Huella...");
}
if(Nofinger == -90){
Serial.println();
Serial.println("Tiempo superado");
Serial.print("....Reiniciando sistema . . .");
}
}

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

Serial.println();
delay(800);
Nofinger =0;
Reset();
}
}

uint8_t getFingerprintID(){
uint8_t p = finger.getImage();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Imagen tomada");
break;
case FINGERPRINT_NOFINGER:
Serial.println("Sin dedos detectados");
return p;
case FINGERPRINT_PACKETRECEIVEERR:
Serial.println("Error de comunicación");
return p;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Error de imagen");
return p;
default:
Serial.println("Error desconocido");
return p;
}
// OK exitoso!
p = finger.image2Tz();
switch (p) {

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```
case FINGERPRINT_OK:
```

```
    Serial.println("Imagen convertida");
```

```
    break;
```

```
case FINGERPRINT_IMAGEMESS:
```

```
    Serial.println("Imagen demasiado sucia");
```

```
    return p;
```

```
case FINGERPRINT_PACKETRECIEVEERR:
```

```
    Serial.println("Error de comunicacion");
```

```
    return p;
```

```
case FINGERPRINT_FEATUREFAIL:
```

```
    Serial.println("No se pudieron encontrar las características de huellas dactilares");
```

```
    return p;
```

```
case FINGERPRINT_INVALIDIMAGE:
```

```
    Serial.println("No se pudieron encontrar las características de huellas dactilares");
```

```
    return p;
```

```
default:
```

```
    Serial.println("Error desconocido");
```

```
    return p;
```

```
}
```

```
// OK convertida!
```

```
p = finger.fingerFastSearch();
```

```
if (p == FINGERPRINT_OK) {
```

```
    Serial.println("Se encontro coincidencia de impresion");
```

```
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
```

```
    Serial.println("Error de comunicacion");
```

```
    return p;
```

```
} else if (p == FINGERPRINT_NOTFOUND) {
```

```
    Serial.println("No se encontro una coincidencia");
```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```

return p;
} else {
Serial.println("Error desconocido");
return p;
}
}
}
//devuelve -1 si falló, de lo contrario devuelve ID #

int getFingerprintIDez() {
uint8_t p = finger.getImage();
if (p != FINGERPRINT_OK) return -1;

p = finger.image2Tz();
if (p != FINGERPRINT_OK) return -1;

p = finger.fingerFastSearch();
if (p != FINGERPRINT_OK) return -1;
Serial.println();
Serial.print("Se encontro ID # "); Serial.print(finger.fingerID);
Serial.print(" Con coincidencia en BD # "); Serial.println(finger.confidence);
if(clave){
digitalWrite(led, HIGH);
Guardar_fecha();//debe ir en leer teclado
//Sensado_suiche();// leer el sensor e puerta
Serial.println("Cerradura Abierta");
delay(tiempo_cerradura);
digitalWrite(led, LOW);
Serial.println("Cerradura cerrada");

```

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

```
Guardar_fecha();//debe ir en leer teclado
```

```
clave=false;
```

```
Serial.println();
```

```
Serial.print("Ingrese Clave de usuario: ");
```

```
return finger.fingerID;
```

```
}
```

```
}
```

```
void Guardar_fecha(){
```

```
    DateTime now = rtc.now();
```

```
    //Serial.print("");
```

```
    //(daysOfTheWeek[now.dayOfTheWeek()]);//no se puede mostrar por serial sale error
```

probar con el envio del mensaje

```
    //Serial.print(" ");
```

```
    Serial.print(now.day(), DEC);
```

```
    Serial.print('/');
```

```
    Serial.print(now.month(), DEC);
```

```
    Serial.print('/');
```

```
    Serial.print(now.year(), DEC);
```

```
    Serial.print(' ');
```

```
    Serial.print(now.hour(), DEC);
```

```
    Serial.print(':');
```

```
    Serial.print(now.minute(), DEC);
```

```
    Serial.print(':');
```

```
    Serial.print(now.second(), DEC);
```

```
    Serial.println();
```

```
}
```

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015- 01-22

FIRMA ESTUDIANTES ANDRÉS PIOS VEJIBE  
DAVID A GÓMEZ

FIRMA ASESOR *[Handwritten Signature]*

FECHA ENTREGA: 2018/08/16

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD \_\_\_\_\_

RECHAZADO\_\_\_      ACEPTADO\_\_\_      ACEPTADO CON  
MODIFICACIONES\_\_\_\_\_

ACTA NO. \_\_\_\_\_

FECHA ENTREGA: \_\_\_\_\_

FIRMA CONSEJO DE FACULTAD \_\_\_\_\_

ACTA NO. \_\_\_\_\_

FECHA ENTREGA: \_\_\_\_\_