UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES

TEMA: Diseño e implementación de un sistema electrónico de seguridad para retiro de alumnado de un jardín de infantes.

AUTOR: Jorge Antonio Acosta Benavides

TUTOR: Ing. David Cando, Mg.

AÑO: 2016

INFORME FINAL DE RESULTADOS DEL PIC

CARRERA:	Electrónica y Telecomunicaciones
AUTOR/A:	Jorge Antonio Acosta Benavides
TEMA DEL TT:	Diseño e implementación de un sistema electrónico de seguridad para retiro de alumnado de un jardín de infantes.
ARTICULACIÓN CON LA LÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	Tecnología Aplicada a la Producción y Sociedad
SUBLÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	Desarrollo de Sistemas Automáticos para la Mejora de Seguridad y Movilidad en la Ciudad de Quito
ARTICULACIÓN CON EL PROYECTO DE INVESTIGACIÓN INSTITUCIONAL DEL ÁREA	Implementación de sistema de seguridad para retiro de niños en centros de educación inicial.
FECHA DE PRESENTACIÓN DEL INFORME FINAL:	Quito, 24 de Octubre del 2016

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El actual proyecto tiene como objetivo general el diseño e implementación de un control de registro biométrico para la entrada y el retiro de niños de educación inicial del jardín de infantes ECUADOR MAGIC LAND. Con la implementación de los resultados se evita que personas ajenas puedan retirar un pequeño sin la debida autorización. Por eso se empleó el uso de tecnología biométrica y el método de huellas dactilares, ya que es uno de los más utilizados en sistemas de seguridad. A la hora de retirar a los infantes, sus representantes pasarán su huella dactilar por el biométrico e inmediatamente se accionará un seguro que se encuentra situado en el torniquete de paso. Al validar la información el sistema se activa y el niño puede pasar por el torno; al mismo tiempo el sistema envía un SMS al padre o madre de familia que fue registrado en un inicio en la base de datos. La programación de este sistema se realizó a través del prototipo Arduino, por lo que se presenta su forma de programación como parte esencial de este proyecto. También se explican las partes que conforman el sistema biométrico donde se guardará la información dactilar de las huellas autorizadas. Finalmente se muestran las conclusiones y las respectivas recomendaciones.

DESCRIPTORES:

Seguridad, Tecnología, Diseño, Investigación, Biométrico, Dactilar.

SUMMARY

This project deals with the design and implementation of a biometric access control for the removal of children from a kindergarten, implementation of this project prevents outsiders can remove a child without his permission, the method used with the use of biometrics was the fingerprint because it is a system in terms of economic cost compared to other security systems and that also provides a high level of security because it has a unique feature in each of the people as is the fingerprint, representatives of each of the students spend their fingerprint for biometric and this activates a safe which is located in the turnstile way to validate the information the system is activated and the child can go through the turnstile step while the system sends a text message to the father or mother who was initially registered. In addition, the microcontroller Arduino, a slight introduction and way of programming, which is an essential part of the project is presented, the implementation done in the kindergarten in the outlet portion of children with the parties that make up the system explained biometric where the fingerprint information of the fingerprint authorized to activate the control system and thus meet the security requirement is needed for children in kindergarten will be saved, finally the conclusions obtained from the objectives and their present recommendations.

Descriptors:

Security, Technology, Design, Research, Biometric, Fingerprint

1. INTRODUCCIÓN

En la actualidad el secuestro a menores de edad es una situación que aumenta, debido al incremento de las organizaciones criminales. Los delincuentes emplean el rapto de personas, principalmente de niños, con la finalidad de obtener grandes sumas de dinero.

Ante la situación de criminalidad aumenta el uso de equipos de acceso biométrico en proyectos que se enfocan hacia la seguridad de un determinado grupo de personas o empresas. Al utilizar ciertos rasgos que son únicos en las personas, se reconoce su eficiencia, ya que propicia la seguridad de ciertas áreas y así se evita que personas no autorizadas ingresen a lugares restringidos.

Por ejemplo, en países como Estados Unidos y Alemania, el empleo de acceso biométrico se generaliza en establecimientos educativos, ya que crecen los índices de secuestros a estudiantes. Las instituciones utilizan métodos de seguridad como el monitoreo a través de cámaras, dispositivos removibles en las mochilas de los alumnos, tras el interés de controlar el acceso a ciertos puntos del inmueble, así como sistemas de registro de acceso a áreas.

La tendencia del escenario internacional no se generaliza en el Ecuador. Los centros educativos no instalan cámaras de seguridad, ni implementan otros sistemas. Tampoco se gestionan los recorridos de la Policía Nacional en el tiempo de retiro de los estudiantes.

1.1 Planteamiento del problema

En el primer cuatrimestre del 2015 se trataron alrededor de 56 casos de secuestro expréss; 46 de ellos se resolvieron inmediatamente y los restantes están en proceso de indagación. En Quito “el 70% de estos secuestros ocurre en taxis amarillos, mientras que el 30% suceden en taxis piratas”. (El Telégrafo, 2012)

El Vicealcalde del Distrito Municipal de Quito, Señor Jorge Albán, manifestó que: “en los últimos dos años aumentó a un 62% el secuestro exprés en la capital”. Según el Ministerio del Interior, la Unidad Antisecuestros de la Policía Nacional (UNASED) en los cuatro años anteriores evitó el pago de $ 12,6 millones por concepto de extorsiones y resolvió el 97% de los casos denunciados. (El Universo, 2015)

A pesar de las acciones realizadas para que no exista el secuestro express, las áreas comunes son, por lo general, menos seguras en la actualidad. Hoy los niveles de rapto a menores de edad o su desaparición ascienden, pues las organizaciones criminales concurren con mayor frecuencia a las instituciones educativas, debido a las vulnerabilidades existentes en estos centros.

Ante la presencia de factores de riesgos, se hace necesario velar por la seguridad durante el momento de entrada y salida de los alumnos de educación inicial del jardín de infantes ECUADOR MAGIC LAND. Al retiro, los niños solo deben ser entregados a sus padres o personas que fueron expresamente autorizadas por los representantes legítimos. Cualquier cambio que se produzca debe ser comunicado inmediatamente a los docentes del jardín.

Ante la ola de delincuencia que persiste en el país y específicamente en Quito, su capital, son necesarios escenarios educativos seguros; principalmente en aquellos centros ubicados en áreas de altos índices de delito de extorción, como Carcelén. En esta zona norte de la urbe se reportan casos de secuestro y rapto de niños, por lo que toda la comunidad y principalmente los padres de familia se encuentran muy preocupados al reconocer que la seguridad de sus hijos es frágil.

1.2 Objetivos

1.2.1 Objetivo General

Diseñar e implementar un sistema electrónico de seguridad para la entrada y el retiro de los alumnos de educación inicial del jardín de infantes ECUADOR MAGIC LAND.

1.2.2 Objetivos Específicos

- Realizar una investigación sobre métodos electrónicos para el control de acceso de personas.
- Diseñar un control de acceso biométrico mediante una placa electrónica de arduino mega que a su vez proporcione mensajes de alerta a través de la red celular.
- Implementar el circuito electrónico a la entrada del jardín de infantes para garantizar la seguridad en la llegada y retiro de los niños de la institución educativa.

- Evaluar el correcto funcionamiento del sistema electrónico de seguridad y de sus componentes.

1.3 Justificación

La institución ECUADOR MAGIC LAND inició sus actividades el 27 de mayo del año 2013. El centro educativo se encuentra en el sector de Carcelén, Av. Isidro Ayora N-8217 y Gaspar Cañero.

La idea de fundar este centro infantil de educación inicial, parvulario y pre kínder respondió a un proyecto de tesis titulado CUENTO ECUADOR MAGIC LAND que se encuentra archivado en la biblioteca de la ESPE.

La institución educativa tiene en la actualidad un claustro conformado por 8 profesores y 60 niños. Pone a disposición aulas con computadores, internet, pizarra digital interactiva y un sistema curricular enfocado al aprendizaje de idioma inglés, expresión corporal, y donde se incluyen cursos de verano.

El jardín de infantes no tiene un sistema de seguridad, debido a ello se hace necesario instalar un sistema de control, con el interés de que exista la seguridad necesaria con la finalidad de evitar secuestros.

2. MARCO TEÓRICO

2.1 Control de acceso

El control de acceso requiere de un mecanismo o dispositivo que se utiliza con la finalidad de reconocer los rasgos o caracteres. Una vez que se identifiquen se permite el acceso a datos o recursos restringidos. Básicamente existen múltiples formas que cumplen con esta función, las cuales se generalizan y aplican en todo el mundo (InfoWeek, 2009).

Los softwares, con opción de digitar una contraseña y abrir determinados dispositivos, son los sistemas más difundidos; otros ejemplos son: la colocación de la huella dactilar. No obstante, en el presente proyecto se inclina por el empleo de sistemas de seguridad electrónica (Machut, 2000).

El control de acceso de interés se basa en sistemas electrónicos que restringen o permiten la entrada de usuarios, registrados previamente, a un espacio determinado. Para otorgar la posibilidad de acceso se ejecuta una verificación de la identificación mediante diferentes tipologías de lectura como por ejemplo claves por teclado, tags de proximidad o biometría (Ramos, 2014). De conjunto, se lleva un control a través de puertas, torniquetes o seguros de paso que emplean una variedad de dispositivos eléctricos o electromagnéticos como un electroimán, cantonera, pestillo o motor.

2.2 Biometría

Es la ciencia tecnológica que se dedica a estudiar y analizar los factores personales que se dividen en fisiológicos y de comportamiento. Por el interés de esta investigación solo se ampliará el factor fisiológico, donde la biometría se encarga de estudiar los rasgos en las personas, como son el iris de los ojos, el ADN, huellas dactilares, reconocimiento facial o de voz (Sistemas Biometría, 2010). Cada uno de estos rasgos son únicos en el ser humano y por ello se hace un reconocimiento veraz de las identidades.

2.2.1 Biometría ocular-iris

Es una prueba diagnóstica que permite obtener las medidas exactas del globo ocular. Gracias a esta prueba se reconocen los siguientes parámetros: tamaño y estructura característica del globo ocular. Con la determinación de estos elementos se disminuye el riesgo de que se confunda con el iris de otro individuo. Además, en el reconocimiento se utilizan imágenes de alta resolución que son capturadas con una

fina iluminación infrarroja y que elimina casi en su totalidad las interferencias que imposibilitan la elaboración detallada de imágenes de la estructura del iris. Estas tomas se convierten en plantillas digitales y proporcionan una representación matemática del iris que coincide con una identificación positiva e infalible de un individuo (Garzón, 2015).

2.2.2 Biometría facial

Según EcuRed (2016) la biometría facial permite determinar la identidad de una persona y verificar su rostro. “A diferencia de otras biometrías tipo iris o huella dactilar esta tecnología no es intrusiva y no necesita de colaboración por parte del usuario. Sólo es necesario que su rostro sea adquirido por una cámara web” (pág. 1).

De lo anterior se interpreta que en esta técnica no se necesita que los usuarios operen el sistema. Debido a esa particularidad de operación es muy empleada en el control de accesos, ya que propicia una alta confiabilidad al evitar las vulnerabilidades que suelen surgir con la colaboración del usuario.

2.2.3 Biometría por voz

La voz de las personas se utiliza con la finalidad de realizar un reconocimiento. La identificación de las palabras a medida que son articuladas por el humano depende de las características que presente la estructura física del tracto vocal de una persona, así como también del tipo de comportamiento vocal (Andrade, 2014). Por tanto, tienen rasgos muy particulares por lo que esa información se puede emplear también para el acceso a lugares restringidos.

El reconocimiento por voz no es de identificación instantánea; puede durar segundos en correspondencia con el tiempo que la persona realiza un discurso. Este tipo de sistema biométrico es muy común en la red telefónica y micrófonos de las computadoras.

2.2.4 Biometría por ADN

Esta técnica es útil en la diferenciación entre dos individuos de la misma especie con la utilización de sus muestras de ADN. Su invención ocurrió en el año 1984 y se usó en áreas de medicina forense, con la finalidad de determinar casos de homicidio.

La técnica se basa en comparar dos seres humanos que tienen una gran cadena de ADN en común. En su distinción se analiza la repetición de secuencias altamente variables que se identifican como micro satélites (InfoWeek, 2009).

La huella genética se utiliza con mayor frecuencia en la medicina forense al tomar muestras de sangre, cabello, semen o saliva. Esta técnica también ayuda a salvar a personas condenadas por error y es común en pruebas de paternidad, identificación de restos humanos y estudios de compatibilidad en la donación de órganos. Las muestras se toman fácilmente de artículos de aseo personal como: cepillo de dientes, afeitadora, cabello, sangre o también muestras de su saliva (Andrade, 2014).

2.2.5 Biometría dactilar

Es la más conocida y se utiliza desde hace más de un siglo para el reconocimiento humano. En la actualidad su funcionamiento se automatiza gracias a los avances tecnológicos de la computación y la electrónica (Ramos, 2014).

Esta técnica se usa en el registro de la asistencia de trabajadores en las empresas o en el control de acceso. Con esa finalidad se emplea el procedimiento que se visualiza en la figura 1.

Figura 1: Biometría dactilar
Fuente: (Consejo Nacional de Ciencia y Tecnología, 2006)

En consecuencia con los objetivos del proyecto, este método se ajusta a la implementación del sistema de control porque es económico, de fácil adquisición en el mercado y porque la identificación de huellas dactilares permite una solución efectiva de la situación problemática expuesta, ya que proporciona un alto porcentaje en cuanto a seguridad.

2.2.6 Lector de huella digital

Es un sensor del tipo biométrico de huella digital que se convierte en un dispositivo perfecto, para efectuar un procedimiento de control conveniente. Con su empleo se protegen o activan diferentes funciones, que se orientan a la seguridad, al utilizar el análisis dactilar (Ramos, 2014).

El biométrico realiza una evaluación interna de imágenes con la ayuda de un Procesador Digital de Señales (DSP). Este análisis permite una contrastación de datos, es decir, se valida si la información que se provee se corresponde con la que se registró con anterioridad en la base de datos (Andrade, 2014).

Según esta funcionalidad, en la figura 2 se visualiza el lector donde se almacenarán las huellas dactilares que se registrarán y que propiciarán la activación del sistema de seguridad de entrada y retiro de los alumnos en el jardín de infantes.

Figura 2: Lector de huellas dactilar
Fuente: (Informática Moderna, 2008)

2.3 Arduino

Se trata de una compañía que diseña placas electrónicas que se programan por medio de código abierto. Entre sus fundamentos principales está la particularidad de poseer software y hardware de fácil uso que se apoyan en una placa electrónica con un microcontrolador. Además poseen un entorno de desarrollo, diseñado tras el interés de viabilizar el uso de la programación y la electrónica en proyectos interactivos de carácter innovador y multidisciplinario (Barrett, 2010).

2.3.1 Arduino Mega

El Arduino presenta un microcontrolador ATMEGA 2560 que en la actualidad tiene la capacidad de realizar múltiples operaciones de control o proyectos electrónicos de tipo experimental. Tiene pines digitales que funcionan como entrada y salida; también cuenta con 16 entradas análogas, un cristal de oscilación de 16 MHz, un conector USB, un botón de reset y una entrada de corriente directa que alimenta la placa. Seguidamente se presentan las partes del Arduino en la figura 3.

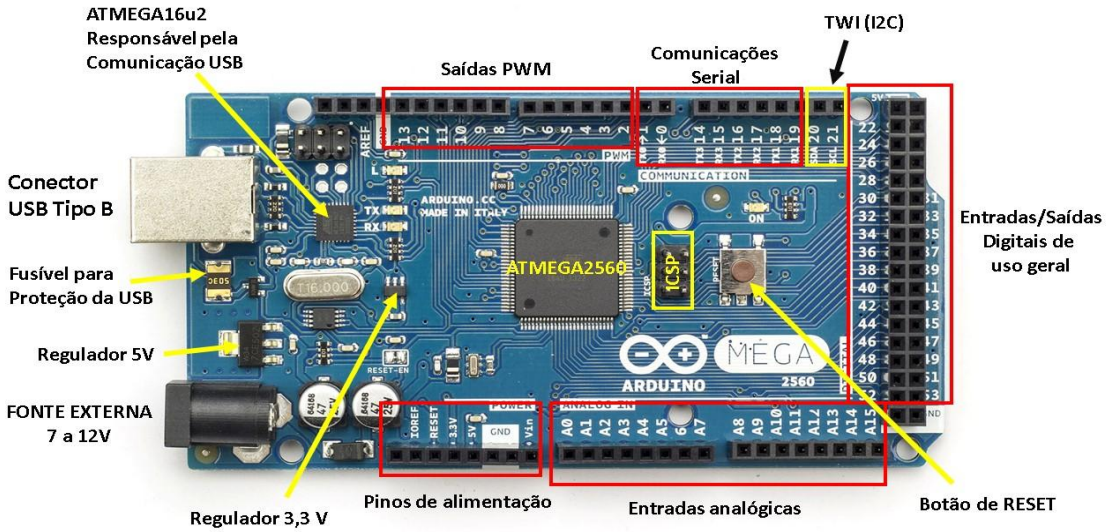


Figura 3: Placa Arduino

Fuente: (García González, Navarro, & Montenegro, 2013)

2.4 Display

Es un dispositivo que permite mostrar información gráfica o alfanumérica al usuario de manera visual. Actualmente, los displays presentan pantallas de cristal líquido o LED que se diferencian por sus formas de iluminación (Ramos, 2014). En la figura 4 se aprecian los caracteres que presentan información en correspondencia con la programación que se realiza en el Arduino.

Figura 4: Display de 16 caracteres

Fuente: (García González, Navarro, & Montenegro, 2013)

2.5 Reloj

Este dispositivo mide el tiempo natural (días, meses y años) en unidades convencionales (horas, minutos y segundos). La tarjeta Arduino no posee este dispositivo, por lo que se debe colocar un módulo con la finalidad de que exista en el microcontrolador un registro minucioso en lapsos de tiempos (AV Electronics, 2016).

Este módulo facilitará realizar proyectos que normalmente necesitan de un registro del tiempo natural transcurrido. Esta medición, como ya se planteó no se puede obtener solamente con el uso de arduino, ya que el sistema no se encuentra en capacidad. Por eso es necesario contar con un módulo que garantice el registro del conteo de las horas, aunque el microcontrolador se encuentre apagado (García González, Navarro, & Montenegro, 2013).

El módulo reloj que interactuará con Arduino está compuesto por el circuito integrado DS3231; incluye un regulador de tensión y adicionalmente presenta una batería de respaldo de 3.6 voltios de la serie CR2631.

La figura 5 muestra un módulo de reloj, necesario para actualizar los registros.

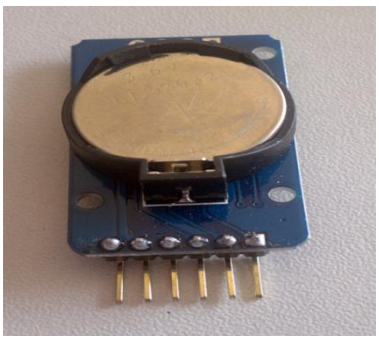


Figura 5: Módulo de reloj

Fuente: (García González, Navarro, & Montenegro, 2013)

2.6 Telefonía móvil

Ondas electromagnéticas son la base de la telefonía móvil o celular. Su desarrollo revolucionó las comunicaciones de voz y con el paso del tiempo se hizo cada vez más accesibles, debido a la reducción de sus costos. La generalización de la telefonía móvil se debe a las investigaciones que realizaron las empresas, con la intención de ganar en optimación, capacidad y así lograr que la fabricación de equipos responda al consumo masivo (Pachón, 2012).

La idea principal de la telefonía nace en el año de 1843 gracias al estudio del químico Michael Faraday sobre la posibilidad de conducción de electricidad en el espacio. Sobre la base de esas investigaciones, Alexander Graham Bell en 1876 inventó el primer teléfono, al cual sucedieron otros equipos cada vez más perfeccionados (Ramos, 2014).

En el año 1983 en Chicago, Washington D.C y Baltimore ocurrieron los primeros lanzamientos de sistemas comerciales del uso de teléfonos móviles en Estados Unidos.

En sus inicios empezó con el sistema de teléfono avanzado. Luego, la AMPS (Sistema Avanzado de Telefonía Móvil) introdujo la utilización de frecuencias de banda de 800 MHz y 900 MHz; así como 30 KHz de ancho de banda para cada canal (Pachón, 2012).

2.6.1 1G, primera generación

A partir de un conjunto de celdas interconectadas que suministran servicio a los dispositivos que están ubicados dentro de una zona de amplia cobertura se realizó la primera generación de telefonía móvil (Fernández, 2012).

Esta tecnología no garantizó la transmisión de mensajería, pues en un inicio fue solo voz. Empleó múltiples celdas en la transferencia de comunicaciones verbales de un espacio a otro, sin la necesidad de que el usuario se mantuviera estático.

La comunicación entre los distintos usuarios fue posible gracias a la utilización de una torre de cobertura que interconectó celdas cercanas. Hoy se conoce que la tecnología empleada por esta generación fue el Sistema Avanzado de Telefonía Móvil; también conocido como Advanced Mobile Phone System (AMPS) (Pachón, 2012).

Esta primera generación presentó demasiadas falencias en su funcionamiento debido a la calidad de la voz y el alto consumo de sus baterías. A pesar de esos inconvenientes, la telefonía móvil arrancó de forma global, lo cual se confirma con el registro de casi veinte millones de usuarios en 1999 (Fernández, 2012).

Ese registro masivo se debió fundamentalmente a la modernización realizada por Ericsson en la década del ochenta del siglo XX, la cual incidió en el aumento de las frecuencias superiores a 900 MHz (Ramos, 2014).

2.6.2 2G y primer standard, Global System for Mobile (GMS)

Conocido como GMS (Sistema Global para Comunicaciones Móviles o Global System for Mobile Communications); con este protocolo se persigue el interés de interconectar un mismo terminal a diferentes redes, con lo cual surgió el primer acercamiento al concepto roaming (Fernández, 2012).

A diferencia de 1G, en esta generación todo el proceso es digital; por lo tanto la transmisión no se realiza de manera analógica. Esta tecnología también incluyó la presentación de desarrollados equipos, con dimensiones más pequeñas y una mayor facilidad de conexión (Pachón, 2012).

Con ese desarrollo, la tecnología móvil alcanzó una mayor aceptación; además surgieron los servicios prepagos y se incrementaron prestaciones muy eficaces en la comunicación, como son los mensajes de texto, el buzón de voz o los servicios de gestión de llamadas.

La introducción de estos servicios respondió a la generalización de tecnologías como el GPRS (Servicio general de paquetes vía radio). El empleo de los avances tecnológicos propició que se consolidaran los servicios de mensajería con él:

- EMS que permite una mejora en el servicio al propiciar que se inserten en el mensaje melodías o íconos.
- MMS (Sistema de Mensajería Multimedia) que permite que se envían mensajes con texto audio e imágenes (Fernández, 2012).

Con la 2G también se consiguió una mejor calidad de voz al eliminar los ruidos y las interferencias, una mayor velocidad en la transmisión de datos y se introdujo el envío de e-mail.

La introducción de los servicios y mejoras provocó una revolución en esta generación que poco a poco modificó su concepto, tanto que algunos autores como Ramos (2014) hacen referencia a generaciones 2.5G y 2.75G, que preparan el trayecto de iniciación de la generación posterior, debido a la generalización de tecnologías como la siguiente.

2.6.2.1 El Servicio general de paquetes vía radio (GPRS)

Conocido como General Packet Radio Service (GPRS), surgió a finales del siglo XX. Se conoce que la conexión GPRS está instituida por “la referencia a su nombre de punto de acceso o Access Point Name (APN). Se pueden utilizar servicios como los de Wireless Application Protocol (WAP), servicio de mensajería cortos, Multimedia Messaging System, Internet y también servicios de comunicación”. (García González, Navarro, & Montenegro, 2013, pág. 2)

La elección de los servicios depende de los intereses del usuario y se debe colocar un login y una clave opcional. El operador de red propicia la información necesaria para la gestión de datos, cuya transferencia se llega a cobrar por el volumen de la información transmitida en kilo o megabytes; en contraposición, la comunicación que se realiza por datos a través de la conmutación de circuitos tradicionales se factura según los minutos que el usuario consumió del servicio (Pachón, 2012).

El estándar GPRS incorporó servicios de punto a punto, de punto a multipunto y servicios de mensajes cortos. Además popularizó el criterio de calidad de servicio en correspondencia con la factibilidad y las exigencias de las aplicaciones. En la determinación de esa calidad se identifican criterios como la prioridad y la fiabilidad, ya sea en servicio con el tiempo o el rendimiento (Ramos, 2014).

Además, GPRS detalla esquemas de codificación que establecen el nivel de protección en correspondencia con las interferencias que intervienen y en relación con la distancia que existe entre las terminales móviles y las estaciones. La protección y el rendimiento son inversamente proporcionales, es decir, si aumenta el uno, disminuye el otro.

2.6.2.2 Módulo GSM GPRS SIM 800L

El módulo GSM Modelo ARM32-0125 funciona en un rango de 3.7 voltios a 4.4 voltios; algo muy importante a tomar en cuenta, ya que se necesita de un regulador de voltaje para proporcionar el voltaje correcto. Este módulo se recomienda alimentar con un voltaje de 4 voltios, sin ninguna variación, con el fin de evitar fallos y permitir un óptimo funcionamiento (Pachón, 2012).

Es un módulo cuatribanda Quadband 850/900/1800 / 1900 MHz que se conecta a cualquier red mundial GSM con una SIM de 2G. Su dimensión es muy pequeña, casi del tamaño de la tarjeta mini SIM. Su hardware posee dispositivos como modem,

diferentes pines de CPIO, opción de conexión al Arduino vía hardware o software (Ramos, 2014).

Con la incorporación de este módulo, el Arduino puede funcionar como un teléfono móvil. Con la combinación del GSM y el GPRS no solo se transmite voz, sino también datos. Entre las funcionalidades especiales de módulo está el envío de mensajes de texto que es parte primordial del presente proyecto. Su uso se generaliza en zonas de tercera y cuarta generación donde no existe mucha cobertura (AV Electronics, 2016).

En la figura 6 se observa el módulo GSM Modelo ARM32-0125 y sus respectivas conexiones.

Figura 6: Módulo GSM GPRS SIM 800L
Fuente: (AV Electronics, 2016)

2.6.3 3G, internet móvil

Al conservar el principio básico de mantener un estándar y continuar con su desarrollo, esta nueva generación llevó a una evolución más clara que la anterior. Permitió más conexiones, al contar con una potencia mayor en sus antenas, una mayor velocidad en la transferencia de datos con un alcance de 2 Mbps bajo ciertas condiciones y además aumentó la calidad de voz (Fernández, 2012).

El incremento de su velocidad favoreció en la aparición de aplicaciones como comunicación de voz, video e imágenes en tiempo real que con anterioridad no existían, debido a la capacidad de la red y de las antenas, por las cuales se conectan los dispositivos móviles.

2.6.4 4G, alta velocidad

A medida que pasa el tiempo, la evolución continúa y da lugar a otras mejoras que se relacionan con la calidad de la señal y, de hecho, con la capacidad de las antenas.

La conexión a internet es posible a través de fibras ópticas y por tanto, la velocidad de transferencia de datos es mucho mayor. Debido a los adelantos tecnológicos se navega con los dispositivos a velocidades de 20 megabits por segundo, ver videos, películas, o los partidos de futbol en tiempo real y con muy buena calidad (Ramos, 2014).

2.7 Relé

Es un interruptor que está formado por un electroimán y una bobina. Al controlarse por una corriente acciona un grupo de contactos, ya sea para cerrarlos o abrirlos. Se considera en muchos casos como un amplificador, pues permite el manejo de potencias mayores que las de sus circuitos de entrada (PROMETEC, 2016).

2.7.1 Relé para arduino

El relé va montado sobre un pequeño módulo que se inserta en la placa arduino. Este relé cuenta con un juego de contactos normalmente cerrado y normalmente abierto y el contacto común; disponible al uso a través de tres bornes roscados y con la posibilidad de manejar hasta 10A (Arduino Genuino, 2016). Además, el módulo posee una señalización de activación del relé mediante un LED. La figura 7 presenta una muestra de relé.

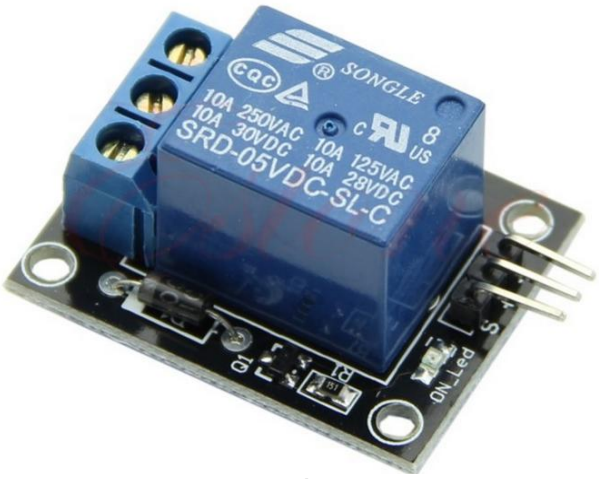


Figura 7: Relé para arduino
Fuente: (PROMETEC, 2016)

3. RESULTADOS OBTENIDOS

3.1 Diseño General del sistema Automático

El diseño e implementación de un sistema electrónico de seguridad en la institución educativa requiere que se tengan en cuenta estas directrices:

- Alimentación energética del circuito
- Circuitos de entrada
- Control electrónico que incluye una placa arduino MEGA.
- Implementación del sistema

También se contempló lo que se muestra seguidamente:

- Funcionamiento de sistemas biométricos dactilar con el uso de arduino.
- Construcción de placa.
- Implementación del sistema de seguridad.

La figura 8 representa la conexión que tiene el prototipo Arduino con los componentes del sistema de seguridad electrónico.

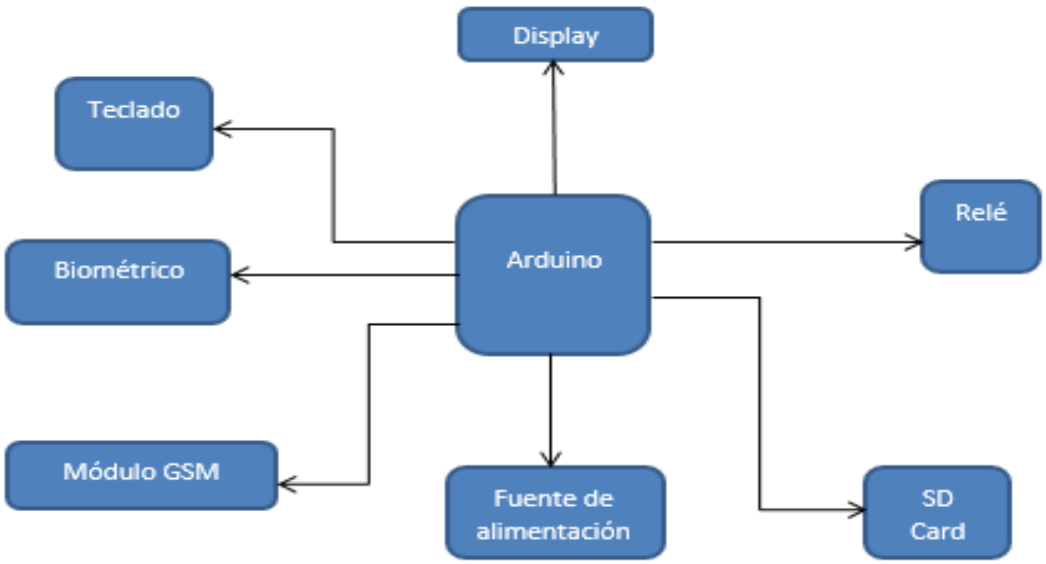


Figura 8: Interacción del microcontrolador con los componentes electrónicos

Fuente: Autor

3.2 Características de los elementos usados para el sistema de seguridad

3.2.1 Display

En este dispositivo se muestra toda la información que procesa el Arduino, al estar el sistema electrónico de seguridad en funcionamiento. En la figura 9 se observa el display de arduino con información que ejemplifica su funcionamiento.

Figura 9: Display para Arduino

Fuente: Autor

3.2.2 Teclado

Por medio del teclado se registra la información de cada representante de los alumnos del jardín de infantes. Arduino determina cuál es la tecla que se pulsa, al aplicar un voltaje en las filas y posteriormente se identifican las columnas, con el interés de determinar en cuál de estas se pone la señal en HIGH.

Todos los teclados que son matriciales usan filas y columnas de forma combinada, en donde se determina la situación de sus botones. Las teclas son un pulsador que está conectado a una columna y a una fila. Al momento que una tecla se presiona, se determina la posición del elemento de la matriz y por tanto, el botón correspondiente.

En la figura 10 se puede observar el teclado 4 x 4 matricial.

Figura 10: Teclado

Fuente: Autor

3.2.3 Biométrico

Para el almacenamiento de la información de la huella digital se utiliza un sensor biométrico que almacena los datos. Al momento de validar la información, el sistema será capaz de realizar el análisis de huella dactilar, en correspondencia con los datos grabados en su memoria.

El sistema se encarga de procesar las imágenes digitales con un DSP y también cuenta con una capacidad al comparar las imágenes en su base de datos y actualizarlas siempre que sea necesario.

En la figura 11 se muestra el dispositivo biométrico donde se almacenan las huellas dactilares digitales que se validarán y permitirán la entrada y el retiro de los niños.

Figura 11: Biométrico de huella digital

Fuente: Autor

3.2.5. Disponibilidad de las operadoras móviles en el sector de Carcelén

Las operadoras móviles de Movistar, Claro y CNT tienen fallas en cuanto a la cobertura de la señal y no solo en lugares alejados. Por ejemplo, en áreas del centro

de Quito existen inconvenientes porque la infraestructura de las construcciones no soportan las radio bases que optimizan su funcionamiento.

En el sector norte de la capital, las tres operadoras presentan una gran cobertura, ya que se implementaron radio bases en varios puntos para su mejora. La superintendencia de comunicaciones realiza supervisiones cada dos años y trata de solucionar los problemas existentes, al hacer pruebas de llamadas y monitorear el servicio de calidad de mensajería.

Las características del módulo GSM, que se utiliza en el proyecto, es Quad Band; esto hace que funcione con la mayoría de las operadoras a nivel mundial.

Por tal motivo, el sistema operará con un chip de movistar, que contrató el jardín, con un plan de mensajes ilimitados que se activará cada mes de forma automática.

No obstante, a continuación en las figuras 12, 13 se visualiza la cobertura de las compañías que prestan servicios en Carcelén.

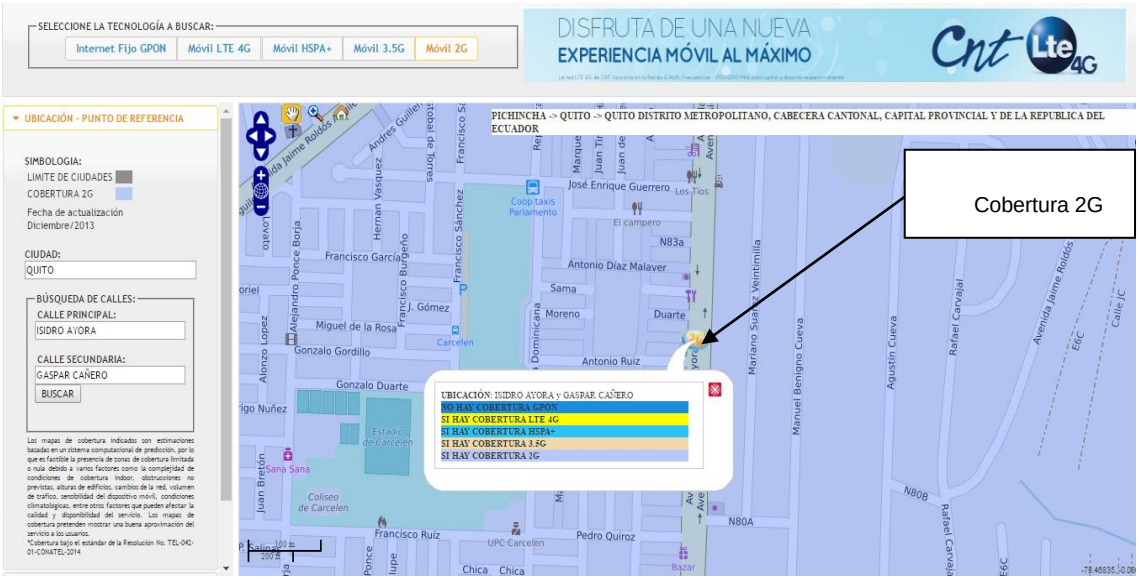


Figura 12: Cobertura CNT en sector Carcelén

Fuente: (CNT, 2016)

Como se observa seguidamente, en la figura 13 coberturas 2G compañía CLARO sector Carcelén.

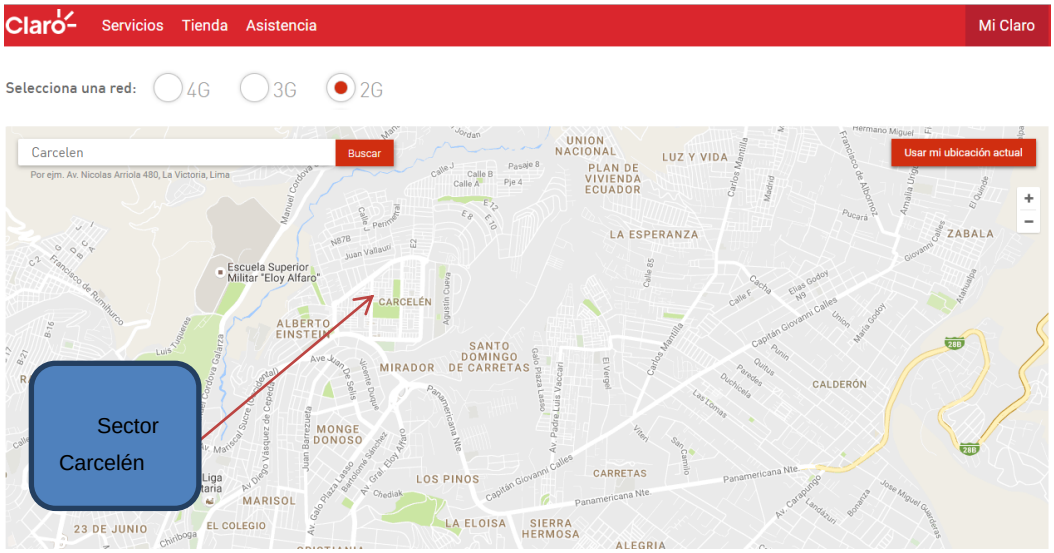


Figura 13: Cobertura Claro sector Carcelén

Fuente: (Claro, 2016)

Con la finalidad de dar cumplimiento a nuevas disposiciones establecidas en los reglamentos de la Ley Orgánica de Telecomunicaciones, Movistar informa que en proceso de elaboración los nuevos mapas de cobertura móvil, retira la información de cobertura de las tecnologías 2G y 3.5G.

3.2.4 Módulo GSM SIM 800L

El módulo trabaja en un rango de 3.3 V a 4.4 V Por esta razón el dispositivo necesita un regulador que suministre 4 V exactos. Caso contrario puede causar mal funcionamiento en el mismo.

El módulo que se seleccionó se conecta a redes mundiales GSM con cualquier mini SIM 2G; con lo cual se garantiza el envío de mensajes a los números registrados.

En la figura 14 se muestra el módulo GSM que utilizará el Arduino.

Figura 14: Módulo GSM SIM 800L

Fuente: Autor

3.2.5 Módulo micro SD

Este módulo facilita el registro de información; además amplía la capacidad de memoria del Arduino Mega. En relación con los intereses del proyecto, propicia el almacenamiento de un archivo CSV; el mismo que puede ser abierto en Excel y que permite conocer la fecha, la hora y el día de la entrada y salida de los niños.

3.2.6 Fuente de alimentación

Todo el sistema se conecta a una fuente de alimentación de 12V, 2A, donde además se encuentra un convertidor DC-DC de voltaje que alimenta a todos los componentes. Una línea de voltaje alterno de 110V que activa el solenoide del torno y su luz indicadora.

3.2.7. Solenoide

Es el elemento que activará el mecanismo del torno de paso y permite realizar el giro. El solenoide está conformado por un núcleo y una bobina que generará un campo magnético y hace que un pistón metálico destrabe dicho mecanismo.

En la figura 15 se muestra el solenoide empleado en la implementación del proyecto.

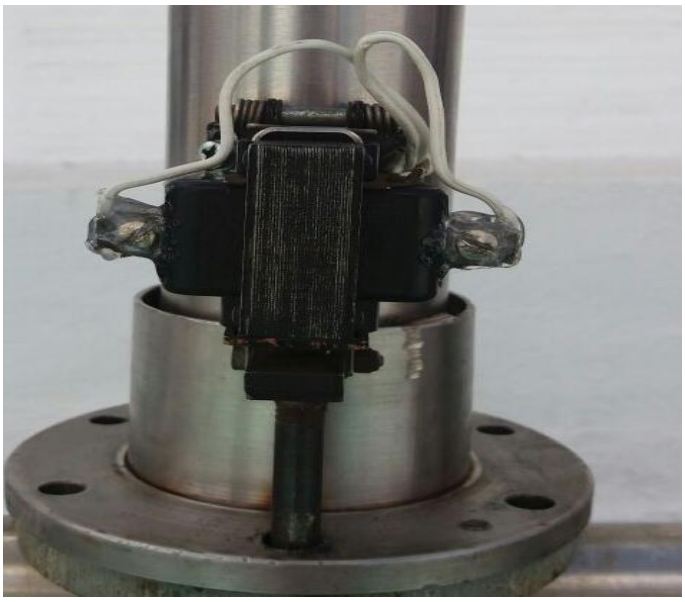


Figura 15: Solenoide

Fuente: Autor

3.2.8 Luz indicadora

Esta luz piloto se monta en la parte superior del torno. Es de color verde y se encenderá si la huella es aceptada por el sistema y, a la vez, ofrece la seguridad de que el representante fue ya registrado con anterioridad. Al no encender la luz, el docente encargado de la salida detecta inmediatamente qué intenta acceder un representante que no tiene permiso de accesibilidad al sistema.

Aceptada la huella dactilar, la luz indicadora de la figura 16 se enciende.

Figura 16: Luz indicadora

Fuente: Autor

3.3 Funcionamiento del sistema biométrico dactilar con el uso de Arduino

3.3.1 Código de administrador

La administración se delega a la directora de la institución, quien posee un código de activación del sistema que consta de 4 dígitos; el cual es 1569. Este código permite que se realice el ingreso de todos los datos de los respectivos representantes de los alumnos de educación inicial del jardín.

Al digitar el código de activación el administrador; los encargados de los niños introducen al sistema su número de celular y la huella dactilar. Solo con la validación de la huella digital registrada; será posible la entrada y salida diaria de cada infante.

Si personas no autorizadas intentan modificar algún parámetro del sistema; el display muestra un mensaje de usuario erróneo.

3.3.2 Flujograma del sistema electrónico de seguridad

En este flujograma se muestran los pasos que se siguieron para el uso idóneo del sistema de seguridad electrónico al cargar la base de datos, es decir, al momento de entrada y salida de los estudiantes de la institución educativa, una vez que se registre a cada uno de los representantes. Seguidamente se especifican los procesos.

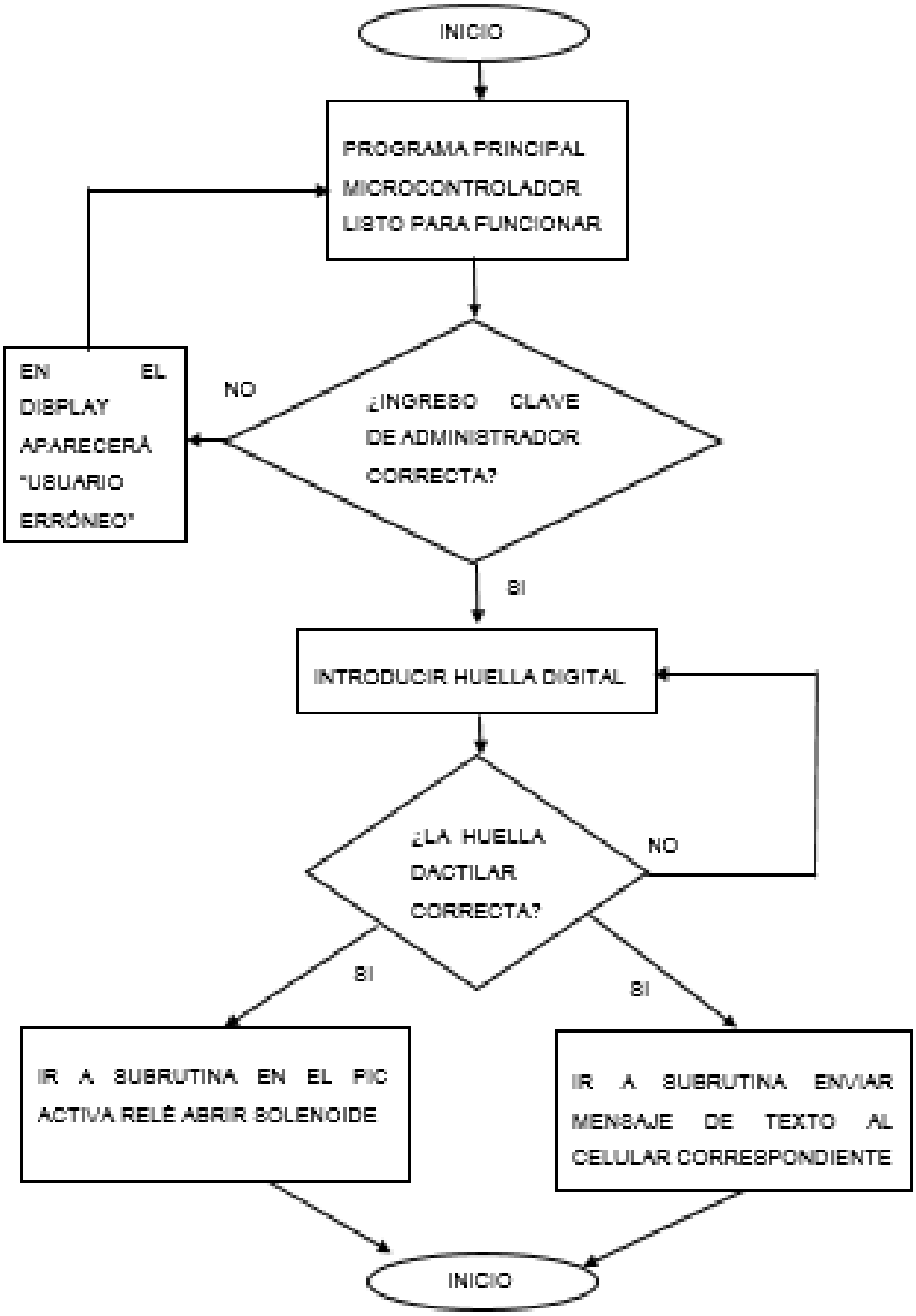


Figura 17: Flujograma para cargar base de datos

Fuente: Autor

La aceptación del usuario, es decir, la validación de la huella dactilar requiere de los siguientes procesos:

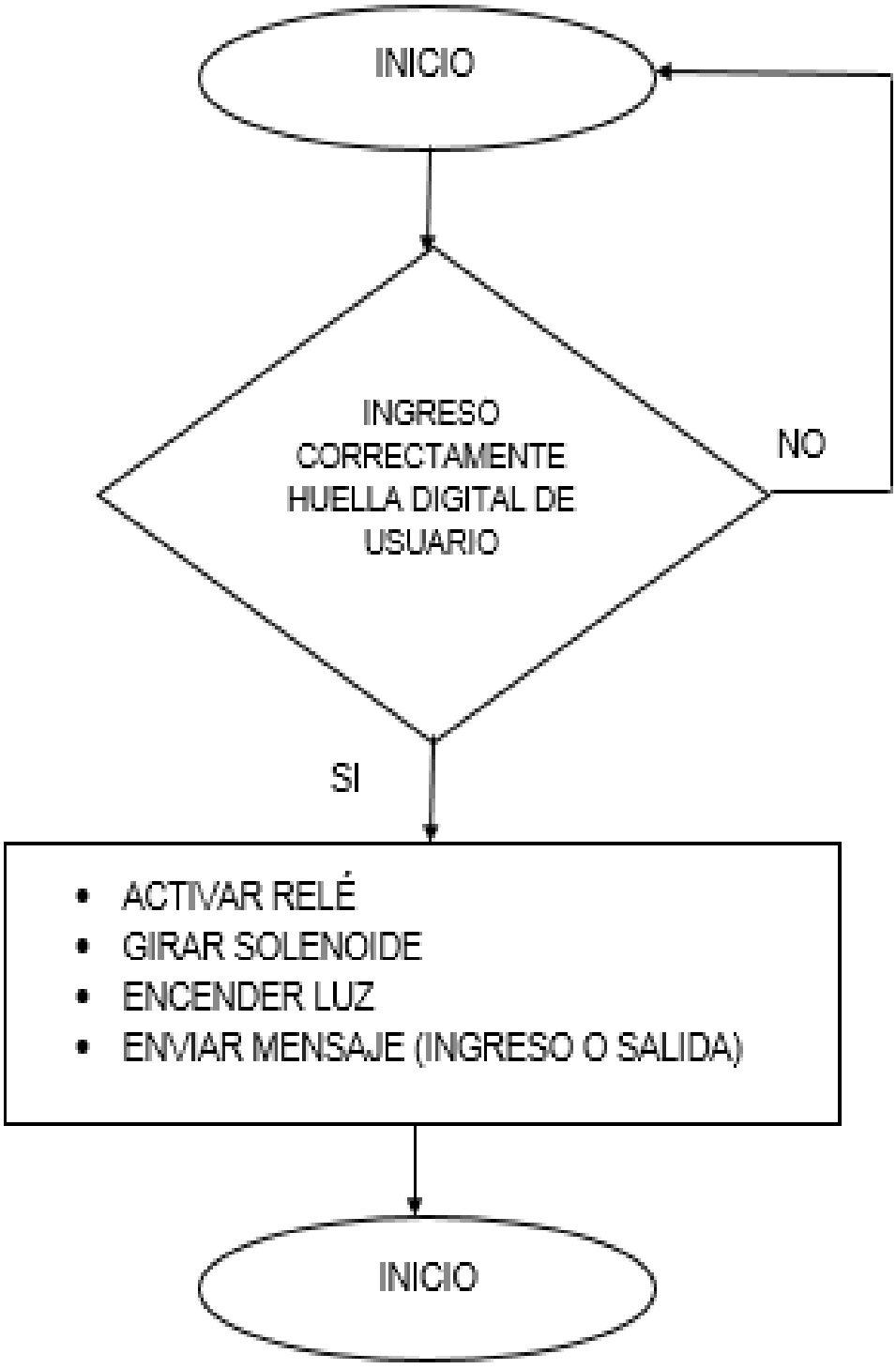


Figura 18: Flujograma para usuario

Fuente: Autor

3.3.3 Sistemas biométricos (lector de huella dactilar)

Están compuestos de un hardware y un software. El primero captura las propiedades específicas del humano que es la huella dactilar del representante y el segundo interpreta esa información y determina su aceptabilidad o negación. Todo esto depende de los datos que fueron almacenados con anticipación por el administrador durante el registro inicial de características.

Después de admitida la información de la huella; el Arduino envía un voltaje al relé que permite la activación del solenoide o seguro.

3.3.4 Sistema de mensajería

Al validar la información se permite la salida del alumno del jardín y simultáneamente el microcontrolador del Arduino trasmite la orden al módulo GSM para que se realice el envío del mensaje de texto hacia el número de celular del representante registrado.

3.3.5 Microcontrolador ATMEGA 2560

Es en esencia el celebro de toda la placa Arduino, que procesa todas las señales y toma de decisiones según la programación.

El microcontrolador se encarga del funcionamiento de que cada uno de los elementos asociados, es decir, controla los componentes del sistema de seguridad como el teclado, display, módulo GSM, relé y el módulo SD. Su programación independiente y su cualidad de software libre es una de las virtudes de esta tecnología.

3.3.6 Programación del microcontrolador del Arduino

La programación se muestra en los Anexo 3, 4, 5 y 6, en donde se detallan cada uno de los pasos que permiten la operación idónea del sistema electrónico de seguridad.

3.3.7. Diagrama esquemático del circuito

Seguidamente se expone la figura 19 el diagrama esquemático del circuito electrónico que se realizó en proteus.

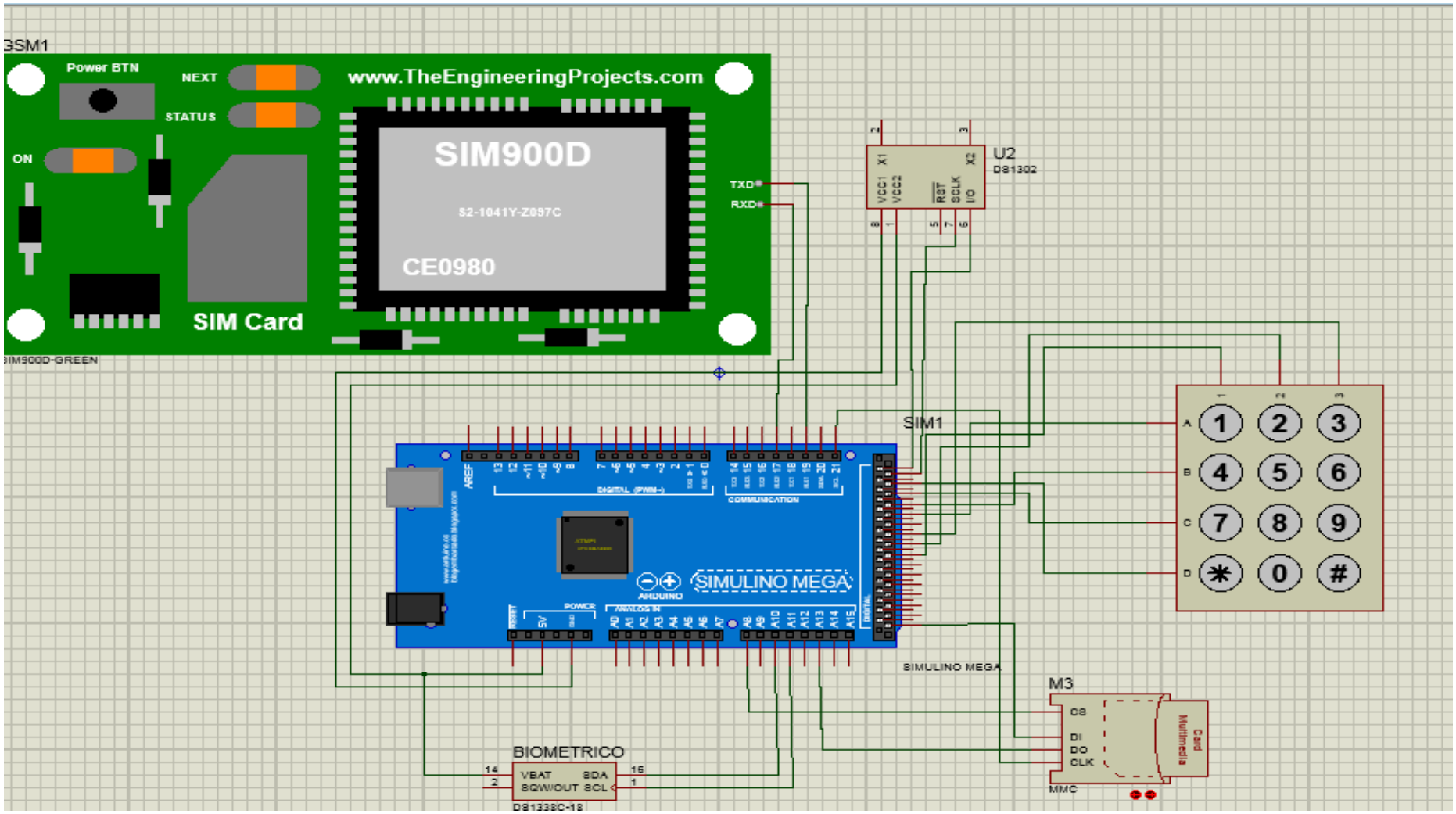


Figura 19: Diseño esquemático del sistema de seguridad

Fuente: Autor

3.3.7 Diseño de placa en el programa PCB Wizard

En esta parte se utilizará el método experimental de laboratorio, puesto que al llevar a cabo el proyecto se realizará la placa electrónica en computador con la ayuda del programa PCB Wizard.

3.3.8 PCB Wizard

PCB Wizard es un programa que permite crear esquemas de circuitos electrónicos y a partir de estos, obtener de una manera sencilla el diseño del circuito impreso a ambas caras. A continuación se presenta la pantalla principal de diseño de la placa para todas sus conecciones.

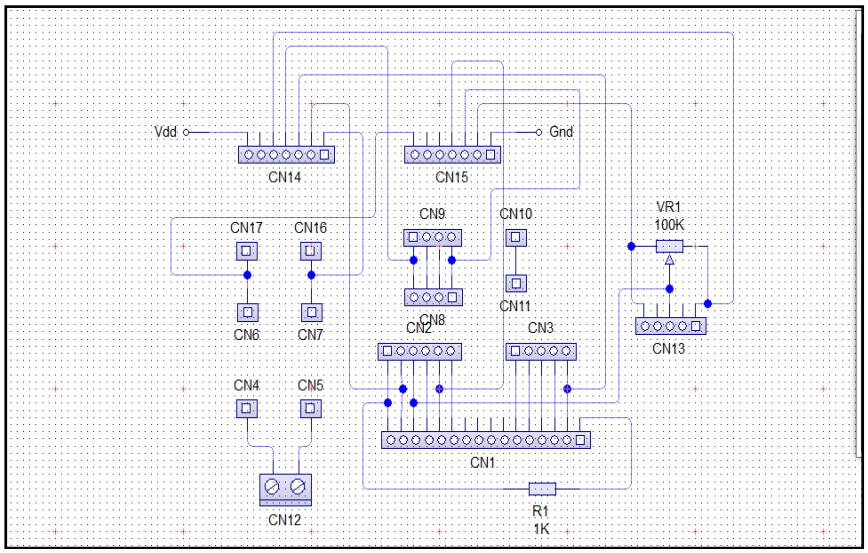


Figura 20: Programa PCB

Fuente: Autor

La figura 20 presenta el diseño de la placa que contiene los siguientes elementos:

- Potenciómetro 10 KΩ
- Resistencia 10 KΩ
- Conversor DC – DC 12V a 4V
- Conectores

El reverso de la placa generada se visualiza en la figura 21.

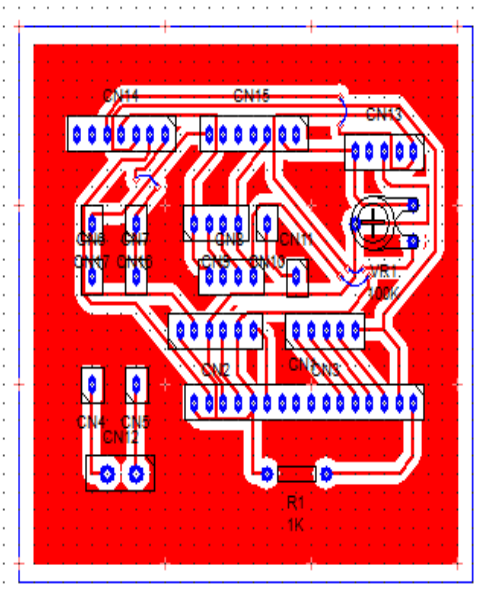


Figura 21: Reverso de placa

Fuente: Autor

A continuación (figura 22) se presenta la imagen frontal de la placa con la ubicación de los elementos que se adicionan a la misma.

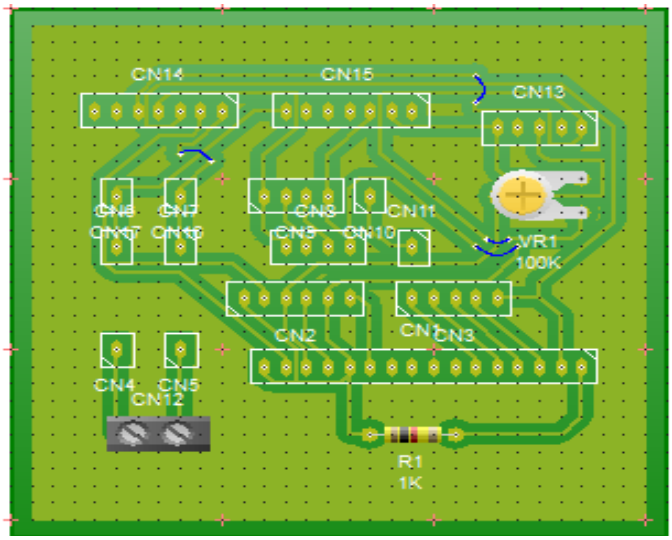


Figura 22: Parte frontal de placa

Fuente: Autor

Una vez diseñada la placa, en el mismo programa se genera el negativo para la impresión de la placa en baquelita con cobre; como se visualiza en la figura 23.

Al emplearse conexiones de paso, hay sockets en los que se conectan buses de datos. El resto de las partes contará con ubicaciones muy específicas en el sistema que se diseñó.

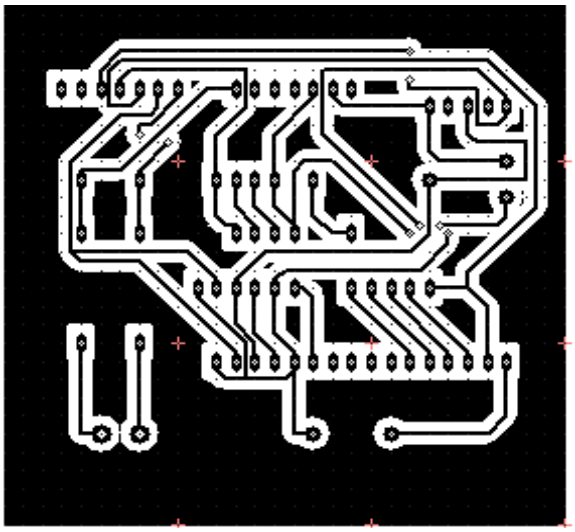


Figura 23: Negativo de la placa

Fuente: Autor

En la figura 24 se aprecia el terminado de la placa donde se montarán elementos y conexiones.

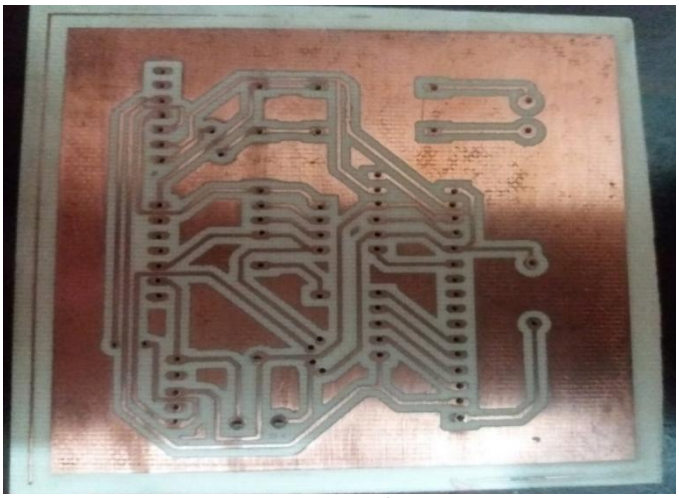


Figura 24: Confección de la placa

Fuente: Autor

Una vez que se tiene la placa y los elementos comprados que se utilizaron en su elaboración; se procede a ensamblar los componentes electrónicos como se muestra en la figura 25.

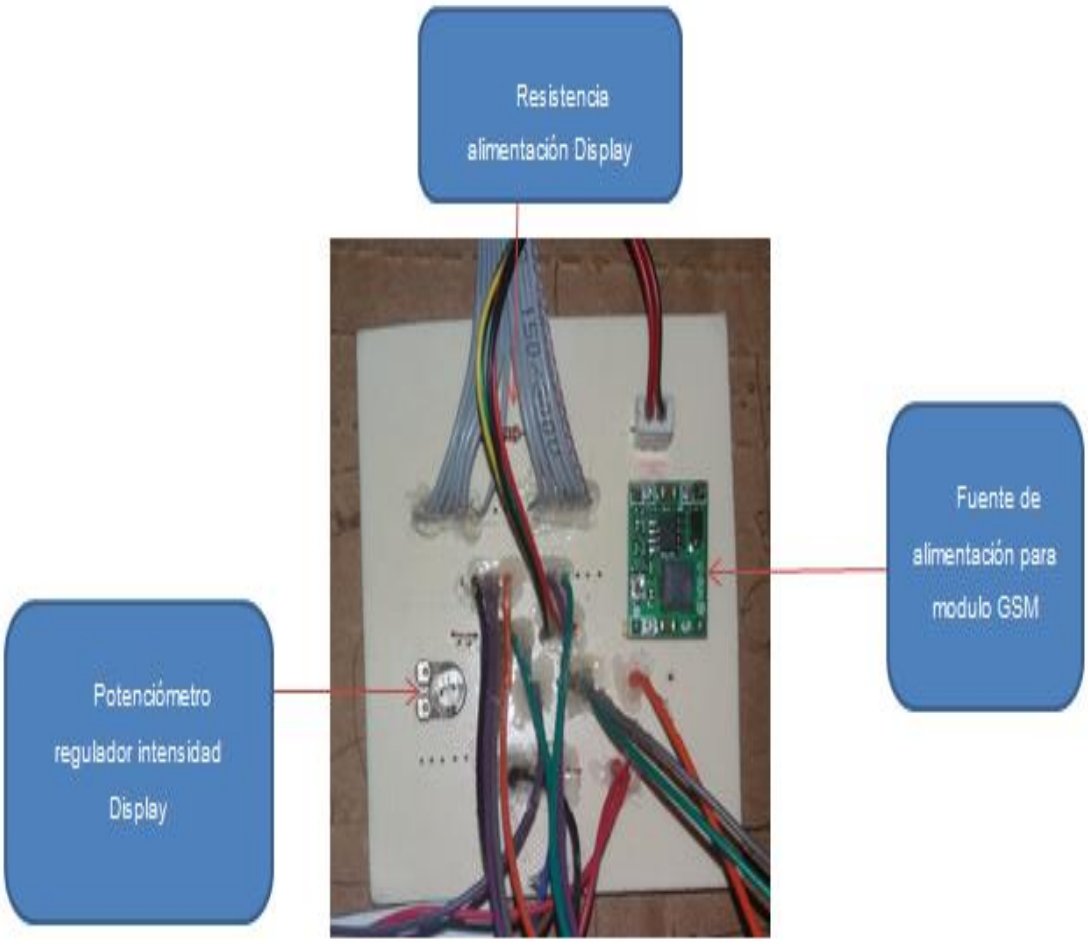


Figura 25: Ensamblado de sus componentes.

Fuente: Autor

3.4 Implementación de los equipos a emplearse

Para la implementación y armado de los componentes electrónicos se ejecutaron varios procesos de prueba, con la finalidad de determinar la calidad de funcionamiento y así garantizar la operatividad correcta del sistema electrónico de seguridad.

Luego, se realizó el armado e instalación de componentes en una caja de protección. Seguidamente se representa en la figura 26 parte del sistema en funcionamiento. Se observa también la fecha y hora del registro de la huella dactilar del encargado del niño. Esta muestra del circuito armado en el protoboard constituye un paso de los procesos de prueba, con el fin de evitar desperfectos.

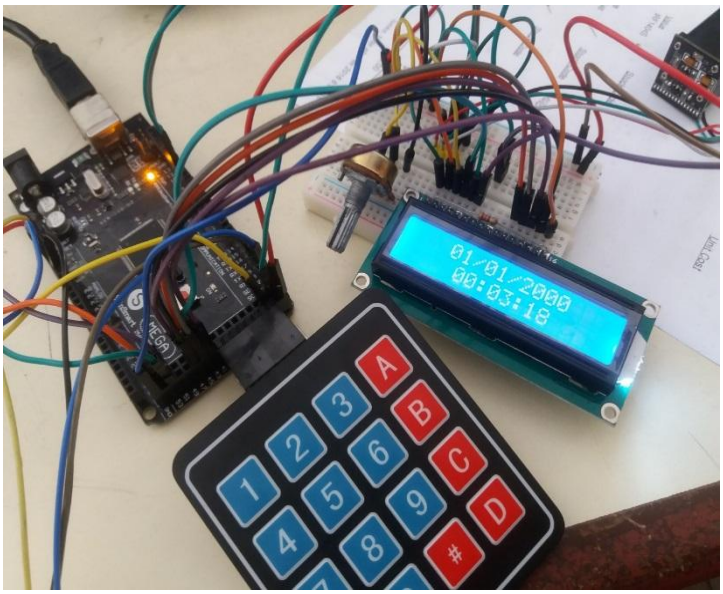


Figura 26: Armado en Protoboard

Fuente: Autor

En la construcción de sistema de seguridad electrónico se usaron los siguientes elementos:

- Placa Electrónica
- Microcontrolador Arduino
- Módulo GSM
- Módulo de reloj
- Módulo de Micro SD
- Antena para GSM
- Display
- Teclado
- Biométrico de huella digital
- Relé
- Solenoide

Al comprobarse la funcionalidad práctica de los dispositivos electrónicos, se montó el circuito diseñado en el protoboard. Luego se realizaron pruebas y se determinó la eficiencia de cada una de las operaciones. Finalmente se detectó que el sistema se encuentra óptimo. A continuación se observa en la figura 27 la parte del biométrico donde se verificó el funcionamiento, con la activación del relé.

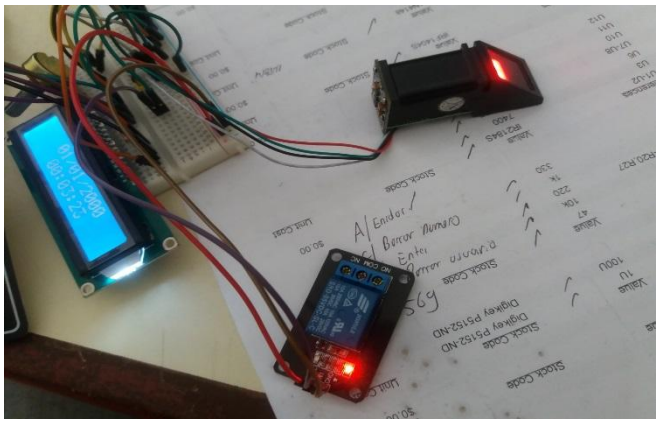


Figura 27: Armado en Protoboard

Fuente: Autor

Al realizar las pruebas respectivas se procedió a ensamblar los elementos en la caja de seguridad que se construyó, con la finalidad de proteger el equipo. La figura 28 muestra la ubicación de los componentes usados, es decir, el relé, reloj, lector biométrico, módulo GSM, y pantalla LDC y la tarjeta Arduino.

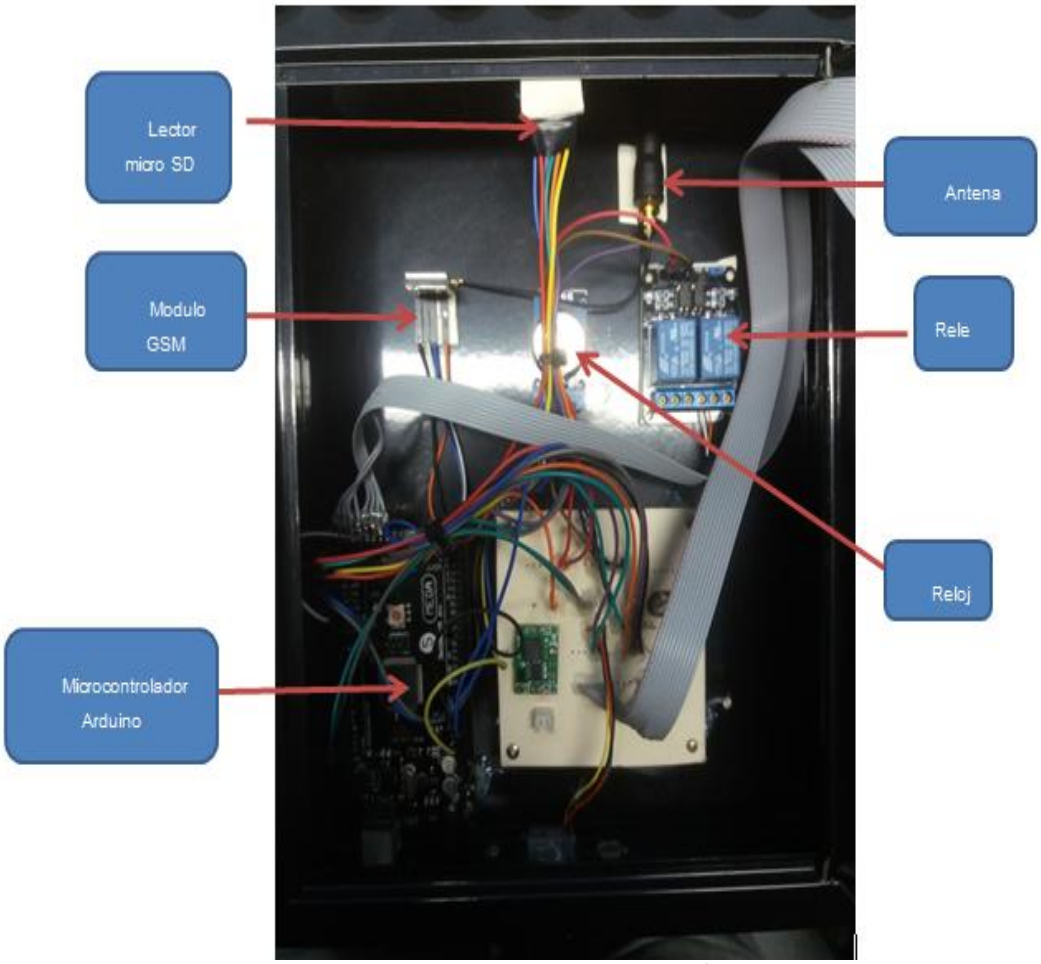


Figura 28: Armado en Caja metálica

Fuente: Autor

Como se visualiza en la figura 29 se consideró necesario hermetizar algunas secciones con la intencionalidad de extender la vida útil de los elementos y el correcto funcionamiento del sistema.

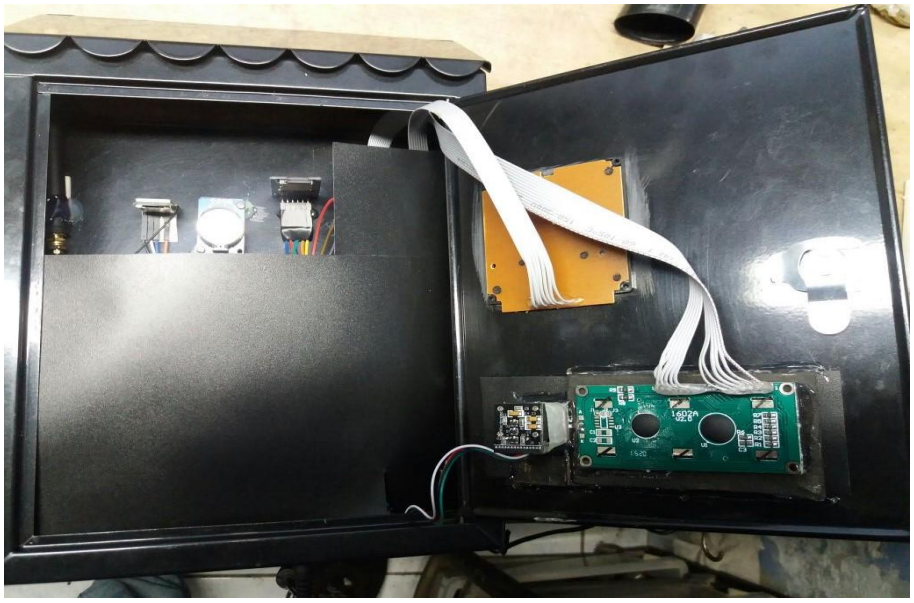


Figura 29: Colocación de placa para hermeticidad

Fuente: Autor

Seguidamente se visualiza el sistema de control, que ya se encuentra listo en la figura 30.

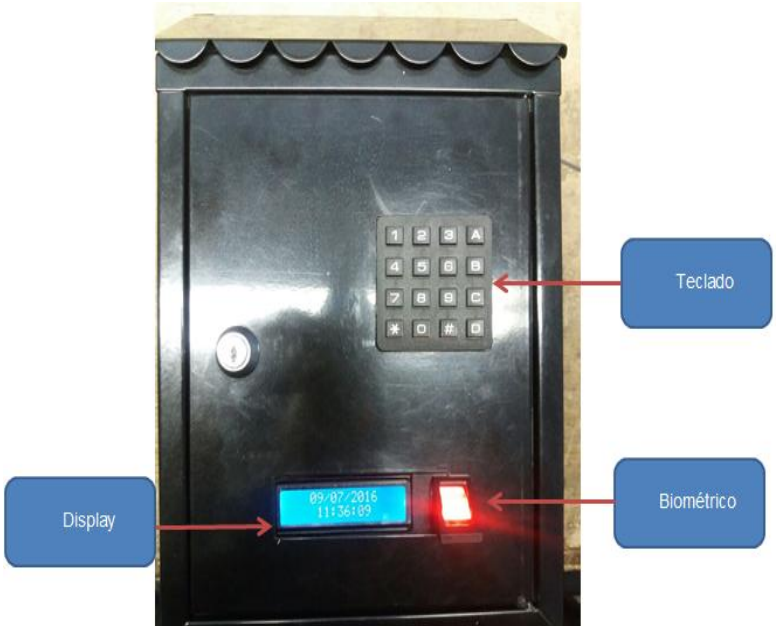


Figura 30: Panel frontal del sistema de seguridad

Fuente: Autor

El torno giratorio se realizó en Acero Inoxidable disponible en el mercado. En el torno se implementó el solenoide que permitirá la salida de los alumnos si la huella digital de la persona registrada es correcta. A continuación se muestra la posición de solenoide en el torno giratorio. El Anexo 2 muestra la forma de construcción del torno giratorio y la figura 31 expone el solenoide que asegura el mecanismo del torniquete.

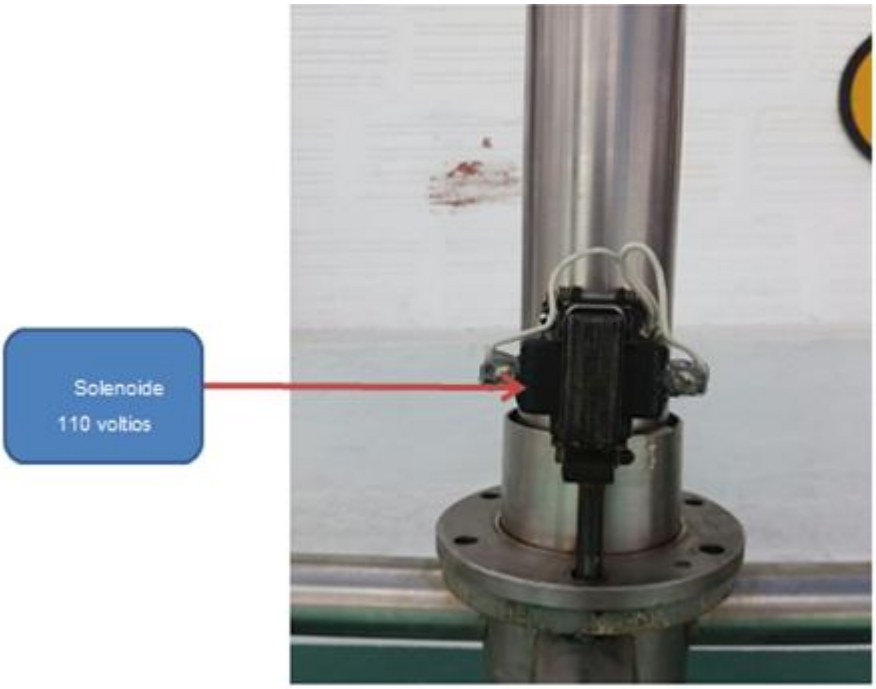


Figura 31: Ubicación de solenoide en el torno giratorio

Fuente: Autor

3.5 Implementación del sistema en la institución educativa

La institución educativa posee dos entradas principales, la primera entrada es de uso exclusivo del personal que trabaja en la institución, mientras que la segunda puerta es salida de emergencia y salida de las y los niños.

El sistema se implementó en la segunda entrada. A continuación, la figura 32 presenta el torniquete de paso instalado en la salida.

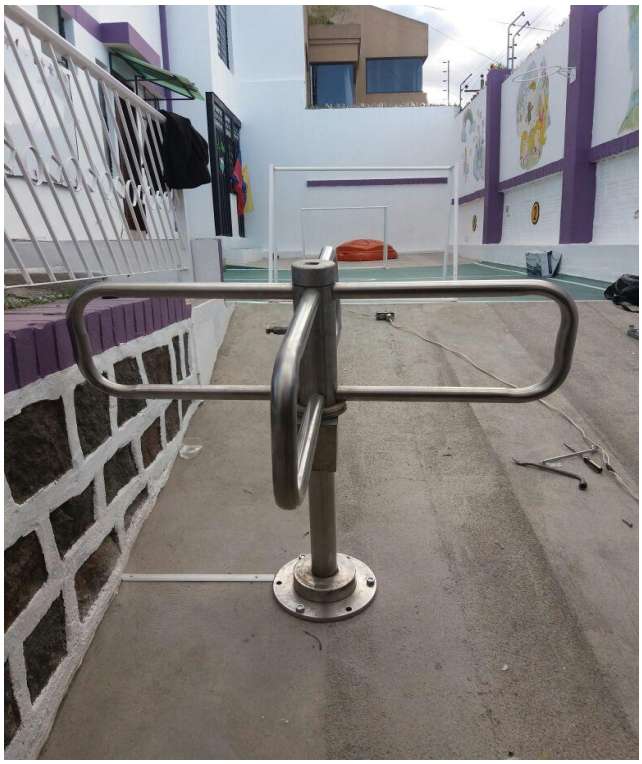


Figura 32: Ubicación del torno giratorio en la institución educativa

Fuente: Autor

Las partes que conforman el sistema de seguridad se visualizan en la figura 33.

Figura 33: Ubicación del sistema de seguridad en la institución educativa

Fuente: Autor

3.6 Pruebas de funcionamiento para el administrador

El funcionamiento del sistema empieza con el registro de usuarios en el biométrico a partir del almacenamiento inicial de las huellas de cada persona autorizada a retirar un alumno. Luego, a los usuarios se les asigna un número de ID en el biométrico que permitirá el ingreso de datos como huella del representante y número de celular del padre o madre de familia.

El registro y validación de las huelas dactilares seguirá estos pasos:

Primer paso: Ingreso de clave de administrador

En la figura 34 se muestra la pantalla donde se le indica al administrador que debe introducir su clave, la cual es única.

Figura 34: Ingreso de clave del administrador

Fuente: Autor

Ante el ingreso de la clave del usuario, se visualizará esta orden:

Figura 35: Ingreso clave del administrador

Fuente: Autor

Segundo paso: en el ingreso del ID se utilizará una numeración, la cual se distribuye de la siguiente manera: el grupo A tendrá ID del 1 al 15; el grupo B, del 16 al 30; el Grupo C del 31 al 45; el Grupo D del 46 al 60. La figura 36 muestra la solicitud de ingreso del id del usuario.

Figura 36: Ingreso clave de usuario

Fuente: Autor

Ante el ingreso del id del usuario se visualiza esta orden:

Figura 37: Ingreso del ID del usuario

Fuente: Autor

Tercer paso: una vez registrado el id se introducirá la huella dactilar del representante. En tal sentido, la figura 38 muestra la orden para el registro de la huella dactilar mediante el biométrico.

Figura 38: Ingreso del ID del usuario

Fuente: Autor

Cuarto paso: una vez guardado el dato huella se prosigue con el número celular del representante registrado. El ingreso del número celular por medio del teclado ocurre al visualizarse la siguiente orden en la figura 39.

Figura 39: Ingreso del número celular del usuario

Fuente: Autor

En la figura 40 se presenta el registro del número celular.

Figura 40: Registro del numero celular del usuario

Fuente: Autor

Quinto paso: el usuario será guardado en la base de datos del sensor biométrico y será el único que podrá realizar la entrada y el retiro del alumno.

Una vez registrado los datos de todos los representantes el sistema funciona de la siguiente manera: el representante se acercará al sensor biométrico y al colocar su dedo pulgar la base de datos del sensor biométrico validará la información y se activará el solenoide del torno de paso y así el alumno podrá salir del jardín.

Simultáneamente el Arduino enviará una orden al módulo GSM, a partir de la cual se emite el siguiente mensaje de texto al celular que fue registrado: “su hijo es retirado del jardín”, con un anuncio de hora fecha y día. Al finalizar este proceso, el equipo nuevamente se encuentra disponible al siguiente registro.

El funcionamiento del sistema requiere de un check list de cada paso, como se expone en la tabla 1.

Tabla 1. Check list de funcionamiento

Pasos	**Cumple**	**Cumple**	**Observación**
	Sí	No	
Registro ID	✓		ID guardado
Registro ID		✓	ID no registrado
Grabar huella dactilar	✓		Imagen de la huella dactilar guardada en biométrico
Grabar huella dactilar		✓	Sistema inactivo
Huella dactilar registrada	✓		Activa el sistema
Huella dactilar registrada		✓	Sistema inactivo
Registro del número de celular	✓		Número celular registrado
Registro número de celular		✓	Sistema inactivo no guarda información
Huella dactilar registrada	✓		Activa el sistema, permite la salida del niño y envía mensaje al número celular
Huella dactilar registrada		✓	Sistema inactivo

Fuente: Autor

3.7 Pruebas de funcionamiento para los usuarios

Al introducirse los datos del usuario correctamente, el sistema electrónico de seguridad funcionará correctamente. Como ya se explicó; el proceso inicia con la introducción de la huella digital que permitirá el ingreso del menor al centro educativo. Así se visualiza en las Figuras 41 y 42.

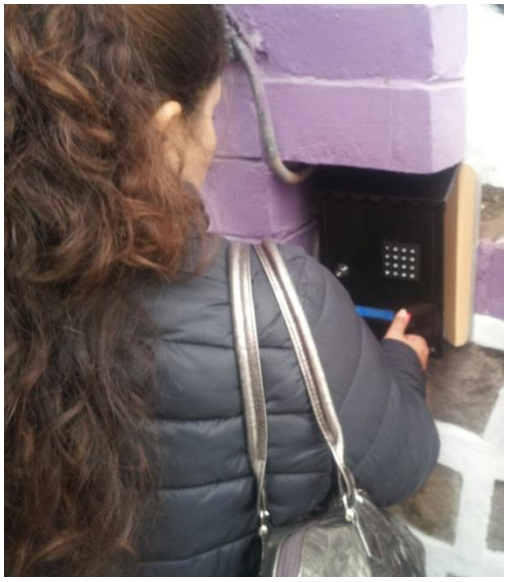


Figura 41: Prueba del ingreso de la huella dactilar del representante

Fuente: Autor

Figura 42: Retiro de los niños una vez validada la huella dactilar

Fuente: Autor

En la imagen de la figura 43 se muestra la luz indicadora, la cual se encenderá si se valida la huella dactilar del representante. Simultáneamente se enviará un mensaje de texto al celular del representante, registrado previamente por el administrador.

Figura 43: Luz indicadora prendida una vez validada la huella dactilar

Fuente: Autor

En la figura 44 se observa la salida del infante por el torno, una vez que se valida la huelle dactilar.

Figura 44: Retiro del niño, una vez validada la huella dactilar

Fuente: Autor

En la figura 45 se muestra un registro de mensajes de ingreso de entrada que se envían al usuario. Específicamente se indica el mensaje de texto que se envía al número que se registró previamente.

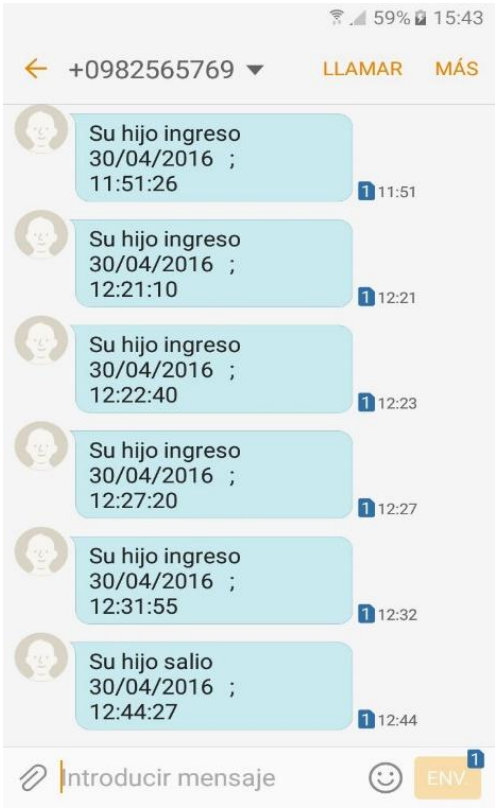


Figura 45: Registro de ingreso al celular del usuario

Fuente: Autor

Al momento de retirar al infante de la institución el encargado del menor debe pasar su huella dactilar por el biométrico, si la huella es correcta el torno giratorio se activará. Encenderá una luz y se enviará un mensaje de texto que, como ya se explicó, confirma al representante que el menor es retirado del centro educativo.

La figura 46 indica el SMS de salida enviado por el sistema para confirmar el retiro del menor.

Figura 46: Registro de salida al celular del usuario

Fuente: Autor

3.8 Costos de la implementación del sistema de seguridad electrónico

En este ítem se describe todos los componentes que se usaron en la implementación del sistema; los cuales son elementos electrónicos, mecánicos y de construcción civil. Los costos de cada uno se muestran en la tabla 2:

Tabla 2: Costos de la implementación del sistema

Costos de materias primas	
Módulo relé	$ 6,00
Biométrico	$ 77,00
Arduino mega	$ 36,00
LCD 16 x 2	$ 6,50
Sim 800L	$ 55
Conversor DC – DC	$ 5
Teclado 4 x 4	$ 8
Cables	$7
Tubos acero inoxidable	$ 120
Dobles tubos	$ 30
Trabajo torno	$ 395
Construcción del Torno	$ 300,00
Implementación en la institución	$ 300,00
Improvistos (5%)	$ 30,00
TOTAL	$ 1375

Fuente: Autor

Como se muestra en la tabla 2, el costo del diseño y la implementación del sistema no implican grandes gastos. Por tanto, es importante reconocer que el sistema tiene futuro, ya que puede ser un proyecto de implementación masiva en instituciones educativas del país. Además, serán mayores los beneficios, pues hasta el momento las propuestas similares no incluyen la parte electrónica y mecánica; elementos que sí se tuvieron en consideración en este proyecto.

CONCLUSIONES

- Los métodos de seguridad existentes en las instituciones educativas del país son escasos. No obstante, existen opciones sencillas que se pueden generalizar, como la instalación de un botón de pánico conectado directamente con la unidad de policía comunitaria más cercana; los sensores biométricos y el circuito cerrado de cámaras de seguridad. El método que se presenta en el proyecto, el uso de un sensor biométrico, hace que el sistema tenga un grado de seguridad mayor al tratarse de reconocer huellas dactilares; un elemento de carácter único en cada persona.
- Se diseñó un sistema electrónico de seguridad que está conformado de dos partes, una electrónica, y una mecánica, con la finalidad de controlar la entrada y el retiro de infantes de educación inicial de la institución ECUADOR MAGIC LAND, mediante la aplicación de tecnología biométrica de huella dactilar sobre la base de un microcontrolador arduino, y un módulo GSM para envío de mensajes de texto al momento de llegada o salida del alumno.
- Se implementó el sistema de seguridad en la puerta de salida de los infantes, que a su vez permite el orden; pues la parte mecánica cuenta con un torno de paso, que se activa por medio de un solenoide, cuando se valida la huella dactilar del representante registrado.
- Para la evaluación del sistema electrónico de seguridad, se capacitó a la persona de confianza que se encargará de la administración, sobre la introducción de la información que requiere el equipo para la actualización de la base de datos, es decir, se explicó el correspondiente registro de huella digital por medio del biométrico y el número telefónico celular que permite la comunicación al momento del retiro del infante. Los padres y madres de familia aprendieron a utilizar el equipo de manera correcta, con lo cual se evitan daños por mal uso, como presionar muy fuerte el sensor biométrico.

RECOMENDACIONES

- Capacitar a los usuarios del sistema, con la finalidad de evitar fallas y extender la vida útil de los componentes.
- Ubicar la caja de componentes del microcontrolador Arduino en un lugar seco, libre de humedad y distante del contacto directo; ya que son componentes frágiles que pueden dañarse fácilmente.
- Brindar mantenimiento a la parte mecánica del torno, por lo menos dos veces en el año, con la finalidad de extender la vida útil.
- La operadora requerida para el funcionamiento del sistema es la Compañía Móvil Movistar por su amplia cobertura en el sector y costo accesible en cuanto a paquetes ilimitados de mensajes.
- Se requiere de la cooperación de docentes, autoridades y progenitores de los alumnos de la institución educativa, debido a que las personas inescrupulosas siempre encuentran vulnerabilidades.

BIBLIOGRAFÍA

Andrade, C. (2014). Sistemas biométricos. *Robótica*, 4-10.

Arduino Genuino. (2016). *Genuino MEGA 2560*. Recuperado el 16 de Junio de 2016, de Genuino MEGA 2560: https://www.arduino.cc/en/Main/ArduinoBoardMega2560

Arthur Lemuel, A. (2005). *Electrónica y dispositivos electrónicos.* Barcelona: Editorial Reverté.

AV Electronics. (mayo de 2016). *Módulo GSM/GPRS SIM800L*. Recuperado el 5 de Junio de 2016, de Módulo GSM/GPRS SIM800L: http://avelectronics.co/productos-2/modulo-gsmgprs-sim800l/

Barrett, S. (2010). *Arduino Microcontroller Procesing for everyone.* Morgan and Claypool Publishers.

Consejo Nacional de Ciencia y Tecnología. (Agosto de 2006). *Biometría*. Recuperado el 5 de Mayo de 2016, de Biometría: http://www.biometria.gov.ar/metodos-biometricos/dactilar.aspx

Díaz Orueta, G., Alzorriz Armendáriz, Sancritobal Ruiz, E., & Castro Gil, M. (2014). *Procesos y herramientas para la seguridad en redes.* Madrid: Universdad Nacional de Educación a distancia.

EcuRed. (2016). *EcuRed Conocimiento con todos y para todos*. Recuperado el 23 de Mayo de 2016, de http://www.ecured.cu/Biometr%C3%ADa_facial: http://www.ecured.cu/Biometr%C3%ADa_facial

El Telégrafo. (27 de Septiembre de 2012). Secuestro exprés creció 62% en dos años en Quito. *El Telégrafo*. Recuperado el 15 de Agosto de 2016, de http://www.eltelegrafo.com.ec/noticias/judicial/13/secuestro-expres-crecio-62-en-2-anos-en-quito

El Universo. (19 de Mayo de 2015). Ministro advierte a sospechoso de rapto con incluirlo en más buscados. *El Universo*. Recuperado el 24 de Agosto de 2016, de http://www.eluniverso.com/noticias/2015/05/19/nota/4889586/ministro-advierte-sospechoso-rapto-incluirlo-mas-buscados

Electrónica Básica. (2004). *Diodos Transistores*. Recuperado el 14 de Agosto de 2016, de Diodos Transistores: https://www.electronicafacil.net/tutoriales/El-rele.php

Fernández, A. (2012). Telefonía Móvil. *Ciencia y Tecnología*, 10-12.

García González, A., Navarro, K., & Montenegro, R. (2013). *Arduino*. Recuperado el 7 de Mayo de 2016, de Sensores de Proximidad: http://panamahitek.com/arduino/

Garzón, N. (2015). Biometría Ocular. *Tecnología*, 2-12.

Goilav, N., & Loi, G. (2016). *Aeduino Aprender a desarrollar para crear objetos inteligentes.* Barcelona: Ediciones ENI.

Hermosa , A. (2011). *Proncipios de electricidad y electrónica II.* Barcelona: Marcombo.

Informática Moderna. (2008). *InformaticaModerna.com*. Recuperado el 3 de Mayo de 2016, de Lector de huella digital: http://www.informaticamoderna.com/Lect_huella.htm

InfoWeek. (2009). Uso de la Biometría. *INFOWEEK Líder en negocios y tecnología*, 14.

Machut, J. F. (2000). *Selección de componentes en electrónica.* Paris: Maarcombo Editores.

Pachón, Á. (2012). Evolución de los sistemas móviles celulares GSM. *Sistemas y telemáticas*, 13-45.

PROMETEC. (2016). *Reles*. Recuperado el 5 de Junio de 2016, de Reles: http://www.prometec.net/reles/

Ramos, T. (2 de junio de 2014). *Tecnología.* Obtenido de Tecnología: http://radioespoch.galeon.com/MATERIA/generacion2.pdf

Schueler, C. (2002). *Electrónica Principios y aplicaciones.* California: Editorial Reverté.

Sistemas Biometría. (14 de Diciembre de 2010). *Biometria*. Recuperado el 24 de Junio de 2010, de Biometria: http://sistemasbiometria.blogia.com/temas/definicion-biometria/

Warren, J., Adams, J., & Molle, H. (2010). *Arduino Robotics.* Friendsof.

ANEXOS

Anexo 1: Manual de usuario del sistema electrónico de seguridad para la entrada y el retiro del alumnado de educación inicial del jardín de infantes.

MANUAL DE USUARIO

Sistema electrónico de seguridad para retiro de alumnado de un jardín de infantes.

1. Precauciones de seguridad

La puesta en funcionamiento del sistema electrónico requiere que primeramente se cumplan las siguientes instrucciones.

No introducir objetos metálicos en su interior que ocasionan daños en sus módulos electrónicos.

La alimentación de energía para el equipo es de 12 VDC.

Por ningún motivo se deben manipular los elementos internos al estar el equipo conectado, ya que ocasiona daños.

Si el equipo presenta un daño se exige que se revise por el personal autorizado.

2. Encendido del dispositivo

Varios componentes conforman el sistema. Sin embargo, su encendido solo depende de la pulsación del SW de ON/OFF que se ubica en la parte frontal y que se muestra en la imagen.

Figura: SW de ON-OFF

Fuente: Autor

3. Conexión/desconexión del dispositivo

El sistema posee un adaptador de 110V AC a 12V DC de alimentación para su conexión y desconexión como indica la figura 2. Por favor, asegurarse que la toma de voltaje alterno sea de 110 voltios AC.

Figura: Adaptador 110 AC-12 DC

Fuente: Autor

4. Torniquete de paso

El torniquete que se fabricó en acero inoxidable permite la entrada y salida de los niños.

Figura: Torniquete de paso

Fuente: Autor

5. Instrucciones de seguridad

Respete las instrucciones que se presentan seguidamente y así evitará accidentes:

- No vierta líquidos sobre el equipo.
- No modifique las partes del equipo. Al abrir la tapa de la caja protectora, expondrá al sistema a varios factores de riesgos, como la humedad o el contacto directo.
- Ante fallas, espere por la asistencia técnica
- Durante una tormenta no manipule el equipo, ni su sistema de cableado.

6. Partes del sistema

El sistema consta de las siguientes partes:

1. **Relé:** activa el seguro del torniquete de paso.

2. **Biométrico:** propicia el reconocimiento de huellas dactilares
3. **Teclado:** permite la introducción de las claves de acceso.
4. **Display:** muestra los datos, hora y día del registro.
5. **Placa Arduino Mega:** activa los dispositivos.
6. **Tarjeta electrónica:** permite la alimentación y conexión de todos los componentes.
7. **Reloj:** tiempo real
8. **Módulo GSM:** propicia que se envíen los SMS de confirmación de entrada o salida del niño.

Específicamente, en la figura siguiente se observa el relé, módulo de reloj, módulo GSM, tarjeta electrónica y placa Arduino Mega.

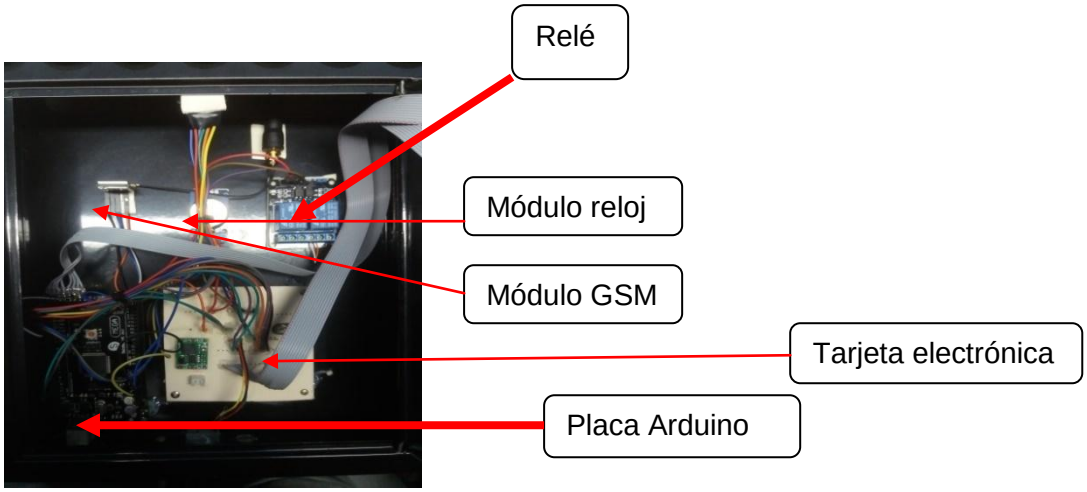


Figura: Partes del sistema

Fuente: Autor

A continuación se muestra el teclado, el display y el biométrico.

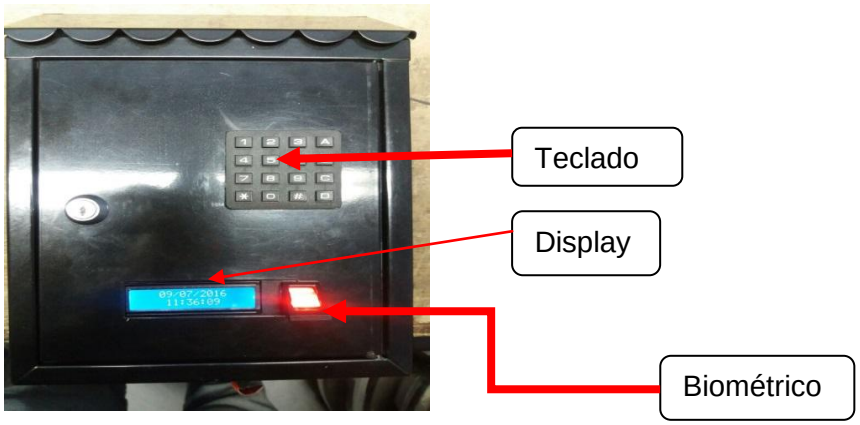


Figura: Partes del sistema

Fuente: Autor

8. Instrucciones de funcionamiento del sistema

Este sistema electrónico se diseñó, con la finalidad de realizar el control de entrada y salida de los niños del jardín de infantes y evitar que personas ajenas accedan a retirar un alumno, sin previa autorización.

Este sistema cuenta con otros elementos que garantizan la seguridad al disponer de un biométrico, torniquete de paso módulo GSM y seguro solenoide.

- Una placa Arduino
- Un seguro mecánico solenoide
- Un sensor biométrico
- Un torniquete de paso
- Una luz verde de acceso
- Cables de conexión.

9. Requisitos necesarios para usar el sistema

- Su funcionamiento exige de una instalación y programación correcta.
- Su programación e instalación requiere de personal calificado.

10. Conocimientos mínimos del usuario

No hay necesidad de recurrir constantemente a servicio técnico, el sistema se diseñó para uso diario.

11. Requisitos técnicos previos

Una placa Arduino MEGA permite el funcionamiento del equipo.

12. Capacidades técnicas del equipo

Trabaja con 12V (CC) de corriente continua que alimenta la placa Arduino, el módulo GSM se alimenta con 4V, entregados por un convertidor 12VDC A 4VDC, así como el resto de sus dispositivos.

13. Software necesario

Es un lenguaje de programación, que funciona como enlace de comunicación serial, a través un convertidor de niveles RS-32 a TTL.

14. Instalación y configuración

En la instalación es necesario que el microcontrolador se programe con los parámetros de cada dispositivo, ya que así cada uno cumple con sus requisitos de funcionamiento.

15. Guía de las principales funciones del sistema

Una vez que se coloca la huella dactilar inicia su funcionamiento. Al validarse se activa un Relé que quita el seguro del solenoide del torno de paso. Al mismo tiempo, ocurre el envío del SMS al número celular que se registró.

16. Sección de solución de problemas que detalla los posibles errores o problemas que pueden surgir, junto con la forma de solucionarlos.

Ante problemas en la operación del sistema pulse el botón de reseteo que tiene la placa del Arduino. Así se reiniciará el programa y se restablecerá el funcionamiento del equipo.

17. Dónde encontrar más ayuda, y datos de contacto

Ante fallas del dispositivo, contacte con el servicio técnico, pues son los responsables del análisis y la reparación del sistema.

17.1 Datos de contacto del soporte técnico

RESPONSABLE

JORGE ACOSTA	jorg.acos@hotmail.com	0983384004

Anexo 2: Manual de detección y solución de problemáticas

Conozca los problemas más comunes que se suelen presentar; los cuales son:

Problema	Solución
Con el encendido	Verificar la toma de alimentación
Con la activación del seguro que destraba el torno.	Confirmar el registro del usuario Confirmar que la bobina se alimenta con el voltaje correcto. Verificar el estado de las conexiones
No se enciende la luz indicadora de aceptación	Comprobar si el voltaje de entrada al foco es el adecuado. Verificar el estado del foco
No envía mensaje de texto	Verificar que el chip este bien colocado Verificar que este activo el plan de mensajes
No desactiva el torno de paso	Verificar el voltaje del solenoide Verificar que el torno no esté trabado Verificar que representante este registrado

Si no se obtienen soluciones, se debe contactar con los operadores del servicio técnico.

Anexo 3: Programación del arduino (Programación datalogger)

```
#include <SD.h>

File dataFile;
int led = 24;

void setup(){
  Serial.begin(9600);
  Serial.print("Iniciando SD card...");
  pinMode(led, OUTPUT);
  if (!SD.begin(led)) {
  Serial.println("Fallo comunicacion o no existe SD");
  return;}
  Serial.println("SD Iniciada.");
  dataFile = SD.open("datalog.txt", FILE_WRITE);

  /////////
  if (dataFile) {
    Serial.println("Escribiendo Informacion...");
    dataFile.println("Escribiendo Informacion...");

    Serial.println("");
    dataFile.println("");

    Serial.println("Programo: Jorge Acosta ");
    dataFile.println("Programo: Jorge Acosta ");

    Serial.println("");
    dataFile.println("");

    Serial.println("<<< Datalogger >>>");
    dataFile.println("<<< Datalogger >>>");

    dataFile.close();}
    else {

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

```
}

    void loop(){

      String dataString = "";
      for (int analogPin = 0; analogPin < 3; analogPin++) {
        int sensor = analogRead(analogPin);
        dataString += String(sensor);
        if (analogPin < 2) {
          dataString += ";"; }}

    dataFile = SD.open("datalog.csv", FILE_WRITE);

      if (dataFile) {
        dataFile.println(dataString);
        delay(1000);
        dataFile.close();
        Serial.println(dataString);
      }
      else {
        Serial.println("Fallo comunicacion.txt");
        Serial.println("Revise conecxion");
        delay(1000); }
    }
```

Anexo 4: Programación del arduino (Programación del reloj)

Programación DS3231 o reloj

```
DS3231_SIMPLE
// CONNECTIONS:
// DS3231 SDA --> SDA
// DS3231 SCL --> SCL
// DS3231 VCC --> 3.3v or 5v
// DS3231 GND --> GND
#if defined(ESP8266)
#include <pgmspace.h>
#else
#include <avr/pgmspace.h>
#endif
#include <Wire.h> // must be incuded here so that Arduino library object file references work
#include <RtcDS3231.h>
RtcDS3231 Rtc;
void setup ()
{
    Serial.begin(9600);
    Serial.print("compiled: ");
    Serial.print(__DATE__);
    Serial.println(__TIME__);
    //--------RTC SETUP ------------
    Rtc.Begin();
  // if you are using ESP-01 then uncomment the line below to reset the pins to
    // the available pins for SDA, SCL
    // Wire.begin(0, 2); // due to limited pins, use pin 0 and 2 for SDA, SCL
    RtcDateTime compiled = RtcDateTime(__DATE__, __TIME__);
    printDateTime(compiled);
    Serial.println();
    if (!Rtc.IsDateTimeValid())
    {
        // Common Cuases:
```

```
        Serial.println("RTC lost confidence in the DateTime!");
        // following line sets the RTC to the date & time this sketch was compiled
        // it will also reset the valid flag internally unless the Rtc device is
        // having an issue
        Rtc.SetDateTime(compiled);
    }

    if (!Rtc.GetIsRunning())
    {
        Serial.println("RTC was not actively running, starting now");
        Rtc.SetIsRunning(true);
    }

    RtcDateTime now = Rtc.GetDateTime();
    if (now < compiled)
    {
        Serial.println("RTC is older than compile time!  (Updating DateTime)");
        Rtc.SetDateTime(compiled);
    }
    else if (now > compiled)
    {
        Serial.println("RTC is newer than compile time. (this is expected)");
    }
    else if (now == compiled)
    {
        Serial.println("RTC is the same as compile time! (not expected but all is fine)");
    }
    // never assume the Rtc was last configured by you, so
    // just clear them to your needed state
    Rtc.Enable32kHzPin(false);
    Rtc.SetSquareWavePin(DS3231SquareWavePin_ModeNone);
}
void loop ()
{
```

```
        // Common Cuases:
        //    1) the battery on the device is low or even missing and the power line was disconnected
        Serial.println("RTC lost confidence in the DateTime!");
    }
    RtcDateTime now = Rtc.GetDateTime();
    printDateTime(now);
    Serial.println();

    RtcTemperature temp = Rtc.GetTemperature();
    Serial.print(temp.AsFloat());
    Serial.println("C");
    delay(10000); // ten seconds
}
#define countof(a) (sizeof(a) / sizeof(a[0]))
void printDateTime(const RtcDateTime& dt)
{
    char datestring[20];
    snprintf_P(datestring,
            countof(datestring),
            PSTR("%02u/%02u/%04u %02u:%02u:%02u"),
            dt.Month(),
            dt.Day(),
            dt.Year(),
            dt.Hour(),
            dt.Minute(),
            dt.Second() );
    Serial.print(datestring);
}
```

Anexo 5: Programación del arduino (Programación del sensor biométrico)

```
/*************************************************
  This is an example sketch for our optical Fingerprint sensor

  Designed specifically to work with the Adafruit BMP085 Breakout

  ----> http://www.adafruit.com/products/751

  These displays use TTL Serial to communicate, 2 pins are required to
  interface
  Adafruit invests time and resources providing this open source code,
  please support Adafruit and open-source hardware by purchasing
  products from Adafruit!

  Written by Limor Fried/Ladyada for Adafruit Industries.
  BSD license, all text above must be included in any redistribution
 *************************************************/

#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>

uint8_t getFingerprintEnroll(uint8_t id);


// pin #10 is IN from sensor (GREEN wire)
// pin #11 is OUT from arduino  (WHITE wire)
SoftwareSerial mySerial(10, 11);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup()
{
  Serial.begin(9600);
  Serial.println("fingertest");
```

```
  // set the data rate for the sensor serial port
  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1);
  }
}

void loop()                     // run over and over again
{
  Serial.println("Type in the ID # you want to save this finger as...");
  uint8_t id = 0;
  while (true) {
    while (! Serial.available());
    char c = Serial.read();
    if (! isdigit(c)) break;
    id *= 10;
    id += c - '0';
  }
  Serial.print("Enrolling ID #");
  Serial.println(id);

  while (! getFingerprintEnroll(id) );
}

uint8_t getFingerprintEnroll(uint8_t id) {
  uint8_t p = -1;
  Serial.println("Waiting for valid finger to enroll");
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {

case FINGERPRINT_NOFINGER:

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

```
break;

  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    break;
  case FINGERPRINT_IMAGEFAIL:
    Serial.println("Imaging error");
    break;
  default:
    Serial.println("Unknown error");
    break;
  }
}

// OK success!

p = finger.image2Tz(1);
switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image converted");
    break;
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Image too messy");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return p;
  default:
    Serial.println("Unknown error");
    return p;
```

```
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
  p = finger.getImage();
}

p = -1;
Serial.println("Place same finger again");
while (p != FINGERPRINT_OK) {
  p = finger.getImage();
  switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Image taken");
    break;
  case FINGERPRINT_NOFINGER:
    Serial.print(".");
    break;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    break;
  case FINGERPRINT_IMAGEFAIL:
    Serial.println("Imaging error");
    break;
  default:
    Serial.println("Unknown error");
    break;
  }
}

// OK success!

p = finger.image2Tz(2);
switch (p) {
  case FINGERPRINT_OK:
```

```
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Image too messy");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Communication error");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    return p;
  default:
    Serial.println("Unknown error");
    return p;
}


// OK converted!
p = finger.createModel();
if (p == FINGERPRINT_OK) {
  Serial.println("Prints matched!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
  Serial.println("Fingerprints did not match");
  return p;
} else {
  Serial.println("Unknown error");
  return p;
}

p = finger.storeModel(id);
```

```
    Serial.println("Stored!");
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return p;
  } else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Could not store in that location");
    return p;
  } else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Error writing to flash");
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }
}
```

Anexo 6: Programación del arduino (Programación del Teclado y LCD)

```
#include <Keypad.h>
#include <LiquidCrystal.h>


LiquidCrystal lcd(40, 41, 42, 43, 44, 45);

const byte Filas = 4;     //Cuatro filas
const byte Cols = 4;    //Cuatro columnas

byte Pins_Filas[] = {25, 27, 29, 31};  //Pines Arduino a los que contamos las filas.
byte Pins_Cols[] = { 33, 35, 37, 39};   // Pines Arduino a los que contamos las columnas.
char Teclas [ Filas ][ Cols ] =
{
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};

int hall = 3;

int addr = 0;
String inString = "";    // string to hold input
String inString2 = "";    // string to hold input
int inChar;
char pulsacion;
long int velocidad;
float Sp=0;
int pwmM = 9;      // LED connected to digital pin 9
int contP = 0;
int t = 0;
long int to = 0;
long int ta = 0;
```

```
long int taux = 0;
float RPMs = 0;
float RPMs1 = 0;
float RPMs2 = 0;

int tt=0;
float kc=1.0;
float ki=0.2;
float kd=0.03;
float T=0.05;
float ek=0;
float mk=0;
float pdy=0;
float pd1y=0;
float sdy=0;
float mk1=0;
float m = 0;

int ttt = 0;
int buzz = A0;
int cBuzz = 0;
int bt = 0;

int corr = 1;
float is = 0;
float is2 = 0;
float ism1 = 0;

float rel = 3.5;
int iErr = 3;
long int tfin = 0;
long int tcur = 0;

int pausa = 0;
```

```
int eCorr = 0;
Keypad Teclado1 = Keypad(makeKeymap(Teclas), Pins_Filas, Pins_Cols, Filas, Cols);

void setup() {
  /** Empty setup. **/

  pinMode(pwmM,  OUTPUT);   // sets the pin as output
  pinMode(buzz, OUTPUT);   // sets the pin as output
  Serial.begin(9600);

  // set up the LCD's number of columns and rows:



  lcd.begin(16, 4);
  lcd.print("SP = ");
  lcd.setCursor(5, 0);
  lcd.print(int(Sp/rel));

  lcd.setCursor(0, 2);
  lcd.print("T  = ");
  lcd.setCursor(5, 2);
  lcd.print(int(tfin/60));

}


void loop() {
  pulsacion = Teclado1.getKey() ;

  if (pulsacion == '*'){
      cT = 1;
      lcd.setCursor(0, 1);
      lcd.print("T  > 0");
```

```
      lcd.setCursor(0, 0);
      lcd.print("SP = ");

      inString2 = "";
      contP=0;
    }
/*  if (pulsacion == '#'){
      cT = 0;
      lcd.setCursor(0, 0);
      lcd.print("SP > 0");
      lcd.setCursor(0, 2);
      lcd.print("T  = ");

      inString2 = "";
      contP=0;
    }

      if (isDigit(pulsacion)) {
        if(cT == 0){
          inString2 += (char)pulsacion;
          if(contP == 0){
            lcd.setCursor(0, 0);
            lcd.print("          ");
            lcd.setCursor(0, 0);
            lcd.print("SP > 0");
          }
          lcd.setCursor(5+contP, 0);
          lcd.print((char)pulsacion);
          contP++;
        }
        if(cT == 1){
          if (isDigit(pulsacion)) {
            inString2 += (char)pulsacion;
```

```
          lcd.setCursor(0, 2);
          lcd.print("T  > 0");
        }
        lcd.setCursor(5+contP, 2);
        lcd.print((char)pulsacion);
        contP++;
      }
    }
}
if (pulsacion == 'C') {
  if(cT==0){
      if(contP>0){
        lcd.setCursor(5+contP-1, 0);
        lcd.print(" ");
        inString2=inString2.substring(0,contP-1);
        contP--;
      }
    }
   if(cT==1){
      if(contP>0){
        lcd.setCursor(5+contP-1, 2);
        lcd.print(" ");
        inString2=inString2.substring(0,contP-1);
        contP--;
      }
    }
}

if (pulsacion == 'A') {
  if(pausa==1){
    pausa =0;
    lcd.setCursor(11, 3);
    lcd.print("   ");
    eCorr=0;
```

```
  }else{
    pausa =1;
    m=0;
 }
}

if (pulsacion == 'B') {
    pausa =0;
    lcd.setCursor(11, 3);
    lcd.print("   ");
    eCorr=0;
    cBuzz = 0;
    tfin = 0;
    tcur = 0;

  }



if (pulsacion == 'D') {
  if(cT == 0){
    if(contP != 0){
      Sp = inString2.toInt();
      contP = 0;
      if(Sp>100)
        Sp=100;
      if(Sp<10)
        Sp=10;
      lcd.setCursor(0, 0);
      lcd.print("          ");
      lcd.setCursor(0, 0);
      lcd.print("SP =    ");
      lcd.setCursor(5, 0);
      lcd.print(int(Sp));
```

```
        inString2 = "";
        cT = 2;
      }
      }

    if(cT == 1){
      if(contP != 0){
        tfin = inString2.toInt();
        contP = 0;
        if(tfin>2000)
          tfin=2000;
        if(tfin<0)
          tfin=0;
        lcd.setCursor(0, 2);
        lcd.print("          ");
        lcd.setCursor(0, 2);
        lcd.print("T  =    ");
        lcd.setCursor(5, 2);
        lcd.print(int(tfin));
        tfin = tfin*60;
        eT(int(tfin));
        inString2 = "";
        cT = 2;
      }
      }
  }

analogWrite(pwmM, int(m));
if(ttt == 20){
  lcd.setCursor(0, 1);
  lcd.print("RPM=            ");
  lcd.setCursor(5, 1);
  RPMs2 = RPMs2/20;
  lcd.print(int(RPMs2/rel));
```

```
lcd.setCursor(0, 3);
lcd.print("I  =      ");
lcd.setCursor(5, 3);
is2 = is / 20;
lcd.print(is2);
if(is2>iErr){
  pausa = 1;
  m=0;
  eCorr = 1;
  lcd.setCursor(11, 3);
  lcd.print("ERR");
  }

if(tfin>tcur){
  lcd.setCursor(11, 2);
  lcd.print(tcur/60);
  if(pausa==0){
    tcur++;
    eTC(int(tcur));
  }
  if(eCorr == 0){
    lcd.setCursor(11, 0);
    lcd.print("PRC");
    }
  }
else{
  Sp = 0;
  eSP(0);
  lcd.setCursor(11, 0);
  lcd.print("FIN");
  lcd.setCursor(0, 0);
  lcd.print("SP = 0    ");
  lcd.setCursor(0, 2);
```

```
      tfin = 0;
      eT(0);
      tcur = 0;
      eTC(0);
      }

    if(eCorr == 1){
       lcd.setCursor(11, 0);
       lcd.print("EMG");
       if(cBuzz == 0){
        cBuzz = 1;
        digitalWrite(buzz, LOW);
        }
      else{
        cBuzz = 0;
        digitalWrite(buzz, HIGH);
        }
      }


    RPMs2 = 0;
    is = 0;
    ttt=0;
  }
  delay(10);
}

void RPM() {
    taux++;
    digitalWrite( 13, digitalRead( 13 ) ^ 1 );
}

void timerIsr()
{
```

```
  ism1 = 0;
is = ism1+is;


ttt++;
RPMs = 10*taux;
RPMs2 = RPMs + RPMs2;
taux=0;

  if((Sp >= 20)&(pausa == 0)){
    ek=Sp-RPMs;
    if (tt==0){
        pdy=RPMs/T;
        sdy=pdy/T;
        mk=T*(-kc*pdy+ki*ek-kd*sdy);
        tt = 1;
    }else{
        pdy=(RPMs-RPMs1)/T;
        sdy=(pdy-pd1y)/T;
        mk=mk1+T*(-kc*pdy+ki*ek-kd*sdy);
    }
    if(mk>900)
       mk=900;
    if(mk<0)
       mk=0;
    mk1=mk;
    pd1y=pdy;
    RPMs1=RPMs;
    m = (mk)*255/900;
  }else{
    tt=0;
    ek=0;
    mk=0;
    pdy=0;
```

Anexo 7: Construcción del Torno Giratorio

Figura: Corte de tubos para el torno giratorio

Fuente: Autor

Figura: Doblado de los tubos

Fuente: Autor

Figura: Ensamble del torno

Fuente: Autor

Figura: Prueba del funcionamiento

Fuente: Autor

Anexo 8: Data sheet GSM

2.3. Functional Diagram

The following figure shows a functional diagram of SIM800L:

- GSM baseband
- GSM RF
- Antenna interface
- Other interface

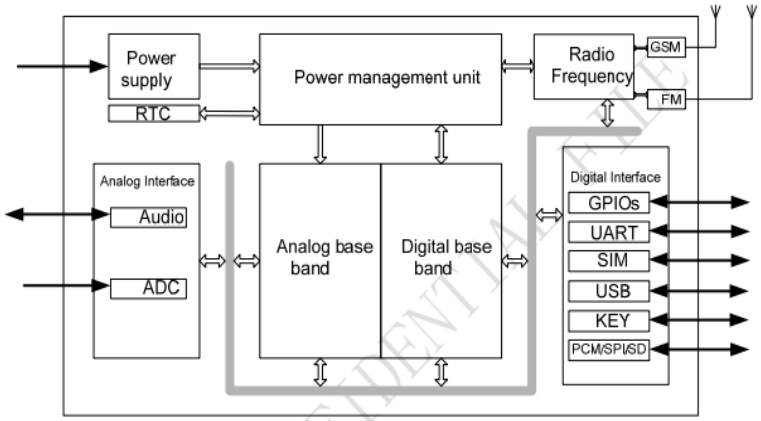
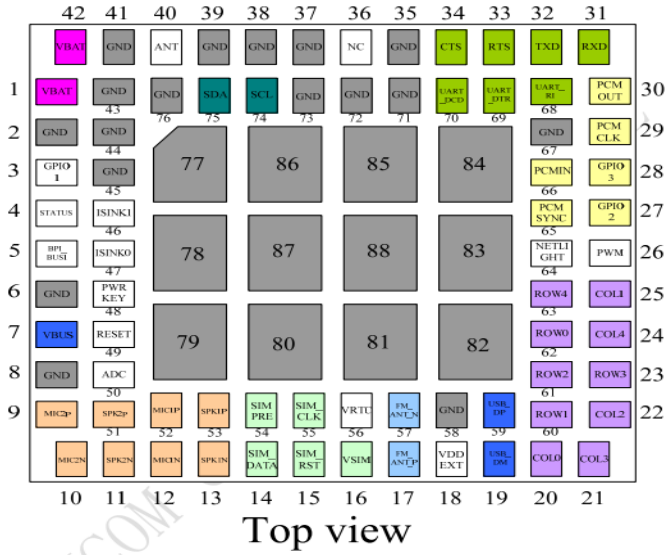


Figure 1: SIM800L functional diagram

3. Package Information

3.1. Pin out Diagram

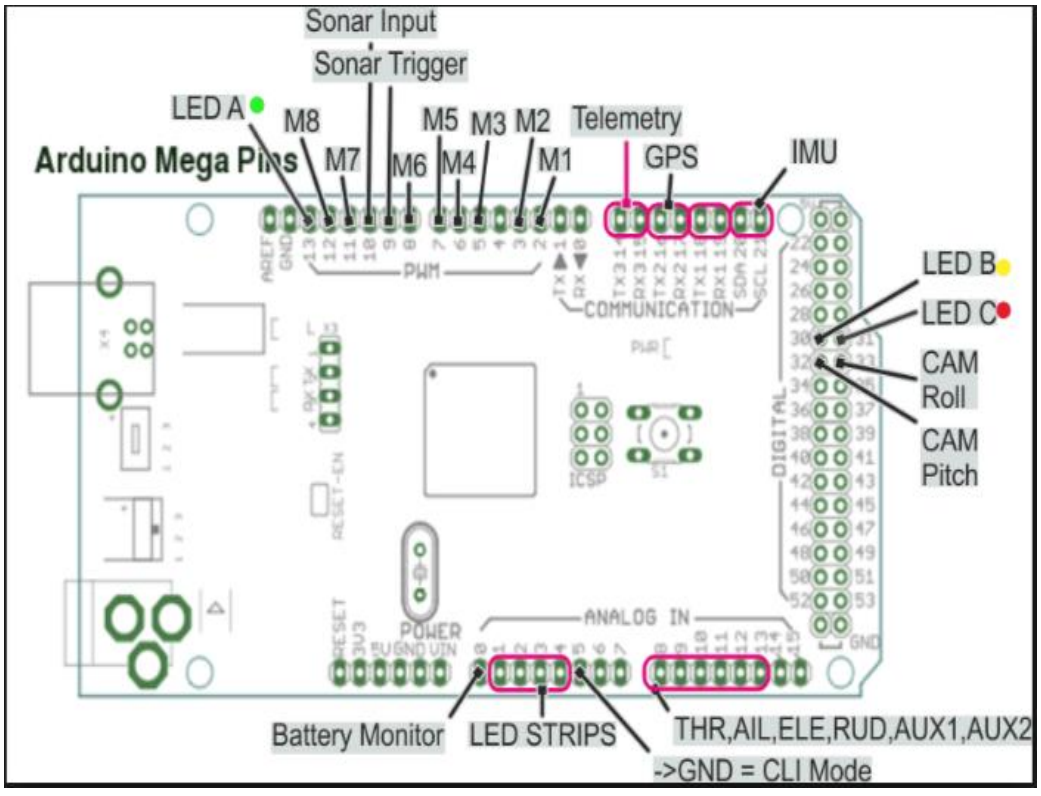


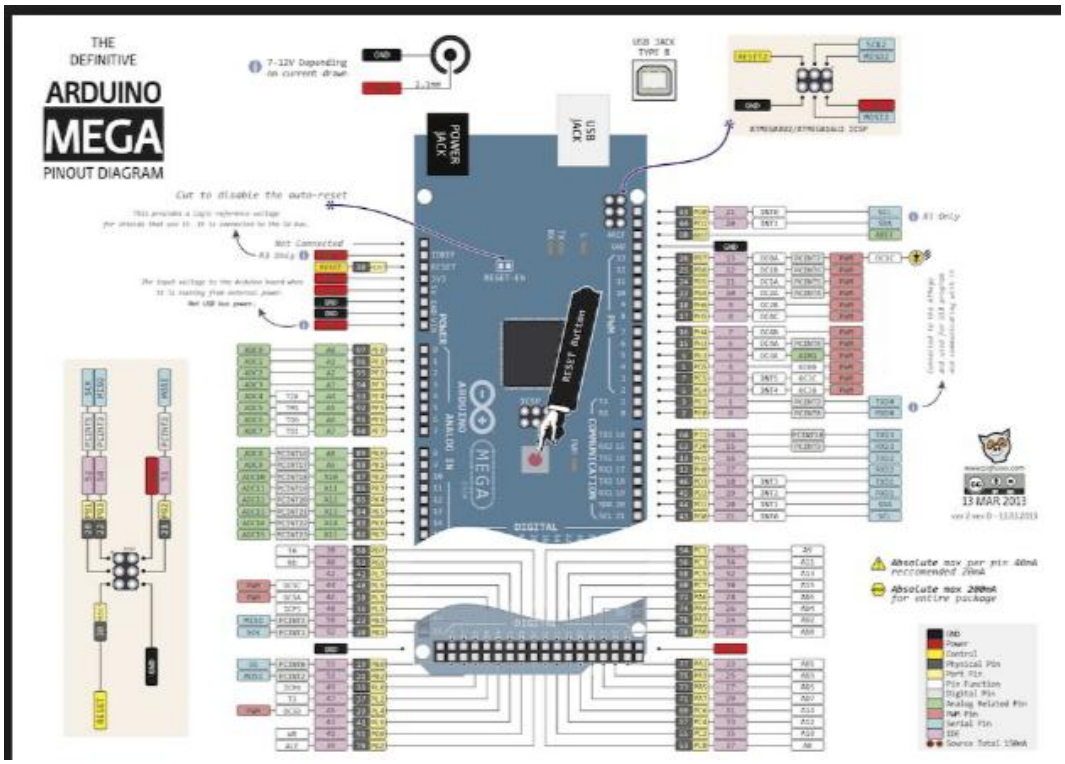
Anexo 9: Data sheet arduino

Overview
Get Inspired
Technical Specs
Documentation

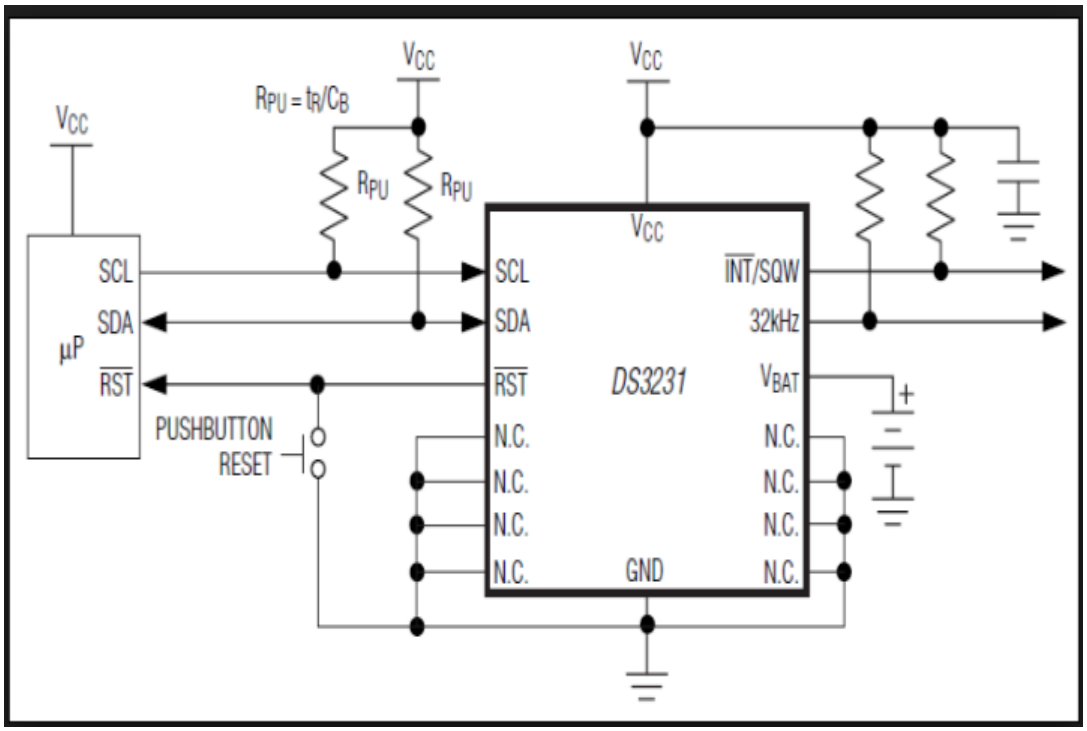
Technical specs

Microcontroller	ATmega2560
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O Pins	54 (of which 15 provide PWM output)
Analog Input Pins	16
DC Current per I/O Pin	20 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	256 KB of which 8 KB used by bootloader
SRAM	8 KB
EEPROM	4 KB
Clock Speed	16 MHz
LED_BUILTIN	13
Length	101.52 mm
Width	53.3 mm
Weight	37 g




THE
DEFINITIVE
ARDUINO
MEGA
PINOUT DIAGRAM
7-12V Depending on current draw
POWER JACK
USB JACK
Cut to disable the auto-reset
Not Connected
Atmega 2560
13 MAR 2013

Anexo 10: Data sheet reloj 3131



Anexo 11: Data sheet teclado