



TECNOLÓGICO  
NACIONAL DE MÉXICO



**Tecnológico Nacional de México**  
**Campus Tuxtla Gutiérrez**

**Comisión Federal de Electricidad (Gerencia Regional de Transmisión Sureste)**

**Título del proyecto**

**Sistema de seguridad inteligente para acceso al COREFO sureste y sala de  
equipos de comunicaciones del hotel Tuxtla**

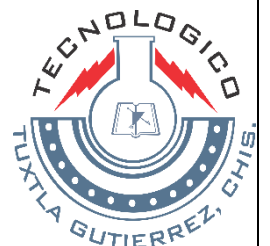
**Presenta: Reyes Palacios Williams Mauricio**

**Carrera: Ingeniería Electrónica**

**Asesor interno:** Ing. Roberto Ibáñez Cordova

**Asesor externo:** Ing. Guillermo Iván Huerta Franco

Subgerencia de Comunicaciones, Depto. Conexión de Servicios GRTSE



# Índice

<b>Capítulo 1 Generalidades .....</b>	<b>4</b>
<b>Introducción.....</b>	<b>5</b>
<b>1.2 Antecedentes .....</b>	<b>6</b>
1.2.1 Empresa.....	6
1.2.2 Visión general de la CFE .....	6
1.2.3 Fundación.....	6
1.2.4 CFE – Organigrama.....	7
1.2.5 Gerencia Regional de Transmisión Sureste.....	8
1.2.6 COREFO GRTSE .....	9
1.2.7 Ubicación geográfica.....	9
1.3 Datos técnicos.....	10
1.4 Topología de la red regional del COREFO Sureste .....	10
1.5 Problemática .....	11
1.6 Objetivo de proyecto.....	11
1.6.1 Objetivo general.....	11
1.6.2 Objetivos específicos .....	12
1.7 Hipótesis .....	12
1.8 Justificación.....	12
<b>Capítulo 2 Marco teórico.....</b>	<b>13</b>
2.1 Importancia de un control de acceso.....	14
2.2 Beneficios de un control de acceso. ....	14
2.3 Historia del Arduino .....	15
2.4 Protocolos de red .....	16
2.4.1 Protocolo SNMP .....	17
<b>Capítulo 3 Marco referencial.....</b>	<b>20</b>
3.1 Arduino mega .....	21
3.2 Sensor lector de huella digital AS608 .....	22
3.3 Pantalla LCD 16x2.....	23
3.4 Adaptador I2C.....	25
3.5 Modulo RTC.....	26
3.6 Shield Ethernet W5100 .....	28
3.7 Plataforma ZABBIX.....	29
3.8 Mensajería Telegram.....	31

<b>Capítulo 4 Diseño y desarrollo (simulación) .....</b>	<b>32</b>
4.1 Etapa 1 – Desarrollo de interfaz de enrollamiento de huellas. ....	33
4.2 Etapa 2 - Diseño de configuración de la pantalla LCD .....	34
4.3 Etapa 3 Integración del Teclado Matricial .....	36
4.4 Etapa 4 Integración de todos los componentes del dispositivo.....	37
4.5 Etapa 5 Diagrama de conexionado. ....	39
<b>Capítulo 5 Desarrollo del proyecto (físico).....</b>	<b>40</b>
5.1 Etapa 1 Montado de Componentes en protoboard.....	41
5.2 Etapa 2 Integración de la Shield Ethernet.....	44
5.3 Etapa 3 Diseño de las placas en PCB. ....	46
5.4 Etapa 4 Diseño en 3D de la carcasa física del dispositivo. ....	48
5.5 Etapa 5 Montado de componentes sobre la carcasa física.....	50
<b>Capítulo 6 Implementación del protocolo SNMP. ....</b>	<b>51</b>
6.1 Etapa 1 Integración del código del SNMP al código general del control de acceso. ....	52
6.2 Etapa 2 Registro del sistema en la plataforma de ZABBIX. ....	53
6.3 Etapa 3 Envió notificaciones vía Telegram.....	55
6.3 Etapa 4 Recepción de notificaciones vía Telegram. ....	58
<b>CONCLUSIONES.....</b>	<b>59</b>
<b>Bibliografía.....</b>	<b>60</b>
<b>Anexos .....</b>	<b>61</b>

# Capítulo 1 Generalidades

## Introducción

El control de acceso se ha venido realizando tradicionalmente en grandes edificios y lugares en los cuales hay gran afluencia de personas. Hoy en día estos sistemas representan un extra bastante importante de seguridad para cualquier tipo de empresa.

Desde la puesta en operación del Centro Regional de Fibra Óptica, mejor conocido como COREFO y que forma parte de la Gerencia Regional de Transmisión Sureste (GRTSE), perteneciente al corporativo de la Empresa Productiva Subsidiaria CFE Transmisión, no contaban con un control de acceso capaz de impedir la entrada a personas ajenas al lugar, por tal razón el presente reporte tiene como objetivo dar a conocer el programa de trabajo y actividades realizadas para poder realizar el proyecto denominado: Sistema de seguridad inteligente para acceso al COREFO sureste y sala de equipos de comunicaciones del hotel Tuxtla.

El sistema tiene como objetivo principal el controlar el acceso a dicho edificio, así como notificar en caso de que alguien quiera ingresar sin tener la autorización y de igual manera en el caso que ocurra algún acceso sin autorización.

El sistema tiene como objetivo secundario el envío de notificaciones de alertas vía intranet al sistema de monitoreo local ZABBIX por medio del protocolo SNMP y envío de mensajería a teléfonos celulares usando la aplicación de Telegram.

En el capítulo 1 veremos de manera general los datos de la empresa donde se desarrollará el proyecto, conjunto con la problemática y la hipótesis planteada para el cumplimiento de los objetivos y la justificación del porqué se va a desarrollar el mismo.

En el capítulo 2, se presenta la investigación de la importancia que tienen los sistemas de seguridad, así como los beneficios y una introducción breve de los protocolos a utilizar.

En el capítulo 3, se habla del marco referencial, donde se plasma la información de las especificaciones de los materiales que se utilizarán en el proyecto.

El capítulo 4 se presenta el desarrollo del proyecto en su parte simulada para comprender y observar las correctas respuestas y conexiones del sistema. Este mecanismo de pruebas es necesario antes de la integración física de cada componente.

En el capítulo 5, se realiza la integración de todos los componentes, así como las pruebas de operación y puesta en servicio del Sistema de seguridad inteligente para acceso al COREFO sureste y sala de equipos de comunicaciones del hotel Tuxtla

## 1.2 Antecedentes

### 1.2.1 Empresa

Comisión Federal de Electricidad, Empresa Productiva del Estado

Actualmente, Comisión Federal de Electricidad (CFE) es una Empresa Productiva del Estado, propiedad exclusiva del Gobierno Federal, con personalidad jurídica y patrimonio propio, que goza de autonomía técnica, operativa y de gestión, conforme a lo dispuesto en la Ley de la Comisión Federal de Electricidad.

El objetivo general de Comisión Federal de Electricidad tiene como fin el desarrollo de actividades empresariales, económicas, industriales y comerciales en términos de su objeto, generando valor económico y rentabilidad para el Estado Mexicano como su propietario.

En la ejecución de su objeto, Comisión Federal de Electricidad debe actuar de manera transparente, honesta, eficiente, con sentido de equidad, y responsabilidad social y ambiental, procurando el mejoramiento de la productividad con sustentabilidad para minimizar los costos de la industria eléctrica en beneficio de la población y contribuir con ello al desarrollo nacional.

Asimismo, Comisión Federal de Electricidad garantizará el acceso abierto a la Red Nacional de Transmisión y a las Redes Generales de Distribución, la operación eficiente del sector eléctrico y la competencia.

### 1.2.2 Visión general de la CFE

*“Para 2025, CFE tiene la visión de ser una de las empresas líderes en el sector eléctrico y energético, con presencia internacional, fortaleza financiera, e ingresos adicionales por servicios relacionados con su capital intelectual e infraestructura física y comercial.”*

### 1.2.3 Fundación

Fue fundada el 14 de agosto de 1937 por el Gobierno Federal y sus primeros proyectos se realizaron en Teloloapan, Guerrero; Pátzcuaro, Michoacán; Suchiate y Xía, en Oaxaca, y Ures y Altar, en Sonora. CFE abastece cerca de 26.9 millones de clientes e incorpora anualmente más de un millón. Desde octubre de 2009, se hace cargo de las operaciones de la compañía Luz y Fuerza del Centro. CFE es la empresa más grande del sector eléctrico de Latinoamérica. Asimismo es propietaria de la única central nucleoelectrónica existente en el país, la Central Nuclear de Laguna Verde ubicada en el estado de Veracruz, misma que usa dos reactores de tipo BWR construidos por General Electric.

## 1.2.4 CFE – Organigrama

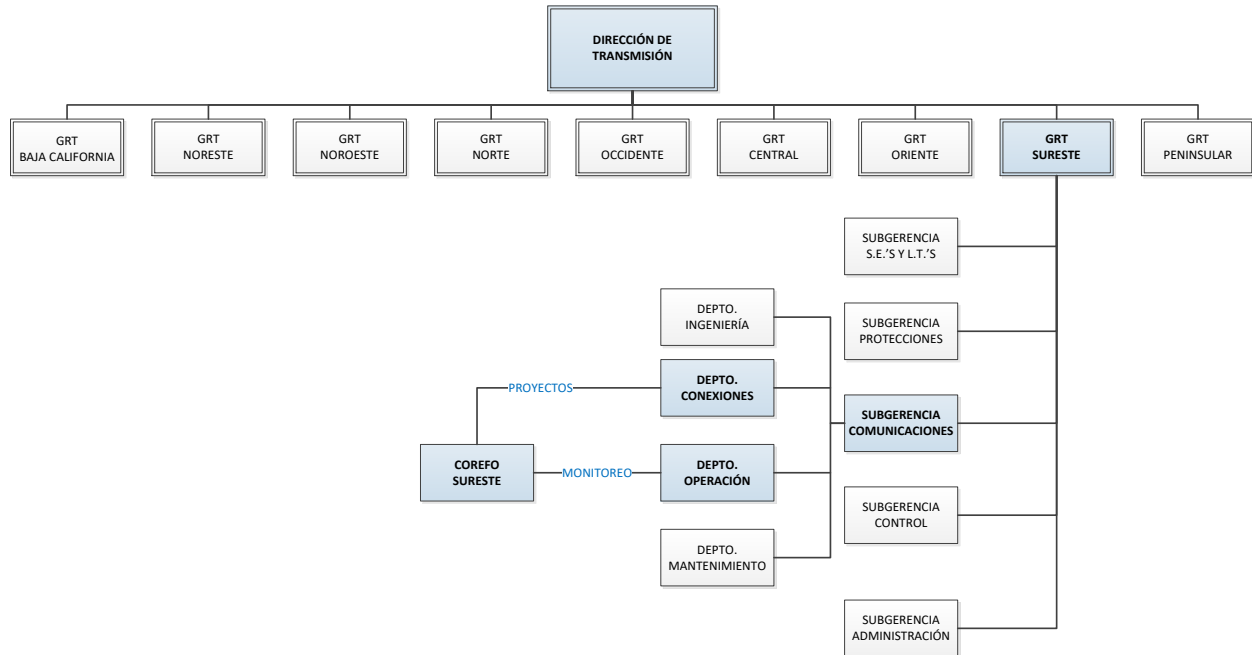
CFE Transmisión es una Empresa Productiva Subsidiaria que forma parte del corporativo de Comisión Federal de Electricidad, la cual tiene por objeto realizar las actividades necesarias para prestar el servicio público de transmisión de energía eléctrica, así como de llevar a cabo, entre otras actividades, el financiamiento, instalación, mantenimiento, gestión, operación y ampliación de la infraestructura necesaria para prestar el servicio público.

Ilustración 1. Organigrama CFE



Fuente: (CFE, 2019)

## Ilustración 2. Organigrama DT - GRTSE



Fuente: Elaboración propia, 2019

### 1.2.5 Gerencia Regional de Transmisión Sureste

La Gerencia Regional de Transmisión Sureste (GRTSE) es una de las nueve gerencias que conforman la Dirección de Transmisión, y su ámbito de influencia abarca los Estados de Chiapas, Oaxaca, Tabasco y parte de Veracruz. La responsabilidad de la GRTSE es prestar el servicio público de transmisión de Energía Eléctrica, mediante la operación, mantenimiento, expansión y modernización de la Red Nacional de Transmisión, garantizando un acceso abierto y no indebidamente discriminatorio y cumpliendo con condiciones reguladas de disponibilidad, continuidad y eficiencia, para crear valor económico y rentabilidad para el Estado Mexicano.

Geográficamente está constituida por 5 Zonas de Transmisión, Villahermosa, Tuxtla, Tapachula, Istmo y Malpaso y una Zona de Operación Sureste.



## 1.2.6 COREFO GRTSE

Es el Centro de Operación Regional de Fibra Óptica de la Gerencia Regional de Tuxtla Gutiérrez y tiene bajo su responsabilidad el monitoreo de todos los servicios de comunicaciones que transitan en nodos SDH, MPLS y BG30.

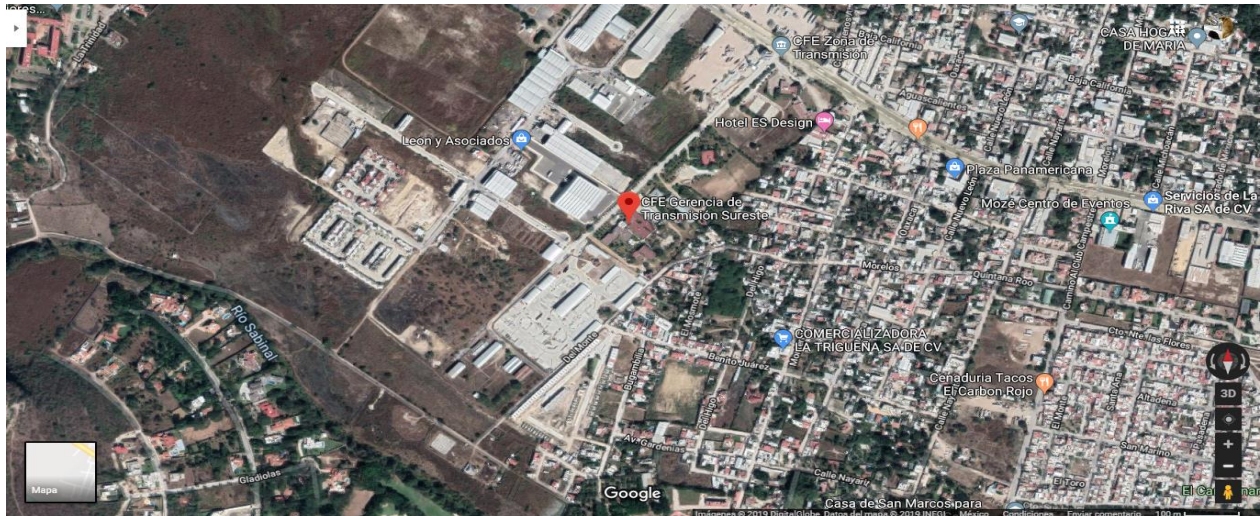
### Ilustración 3. COREFO Sureste



Fuente: Imagen propia, 2019

## 1.2.7 Ubicación geográfica

Coordenadas: 16.761099, -93.190841. Mapa 50km:



Ubicación de residencia: Carretera Panamericana 4, plan de Ayala, 29020 Tuxtla Gutiérrez, chis.



## 1.5 Problemática

El centro del COREFO (Centro Regional de Operaciones de Fibra Óptica) es un área de la GRTS responsable del control y monitoreo de las telecomunicaciones en el ámbito de la gerencia.

Sin embargo, hoy 14 de agosto del 2019 no se cuenta con un sistema inteligente capaz de controlar el acceso de los trabajadores y visitantes del área.

Es importante resaltar que tiene que existir un control de acceso al COREFO dado que desde este sitio se monitorea y controla el tráfico de los servicios de voz y datos de la GRTS monitoreando las 24 horas del día, los 365 días del año el siguiente equipamiento.

Equipos de Fibra Óptica Monitoreados vía COREFO SURESTE	
Descripción	No.
KM de F.O. OPGW	2198
KM de F.O. ADSS	1875
Nodos SDH	36
Nodos MPLS-TP	55
Nodos IP-MPLS	23
ECI BG30	07
Convertidores Ópticos	168
Enlaces Microondas	18
Sistemas de fuerza	81
Cargadores VCD	18
Bancos de baterías	13
Inversores	20
Sistemas solares	3
Plantas de emergencia	19

## 1.6 Objetivo de proyecto

### 1.6.1 Objetivo general

Diseñar un sistema de seguridad inteligente para el COREFO y la sala de equipos de comunicación del Hotel Tuxtla, capaz de brindar el acceso solo a personal que trabaje dentro de dichas instalaciones, así como notificar cuando se registre un acceso sin autorización al sistema de monitoreo local ZABBIX.

## 1.6.2 Objetivos específicos

- Diseñar un dispositivo que se encargue de permitir el acceso a las instalaciones solo al personal que labore en dicho edificio
- Notificar en caso de haber un acceso o intento de acceso sin autorización, al sistema de monitoreo ZABBIX
- Crear una página web que se encargue de llevar un registro de los últimos accesos al COREFO.
- Enviar las notificaciones a los teléfonos celulares del personal responsable de la sala a través de la mensajería.

## 1.7 Hipótesis

¿Es posible realizar la implementación de un sistema de seguridad basado en tecnología arduino y que notifique por medio de la red de datos de CFE cuando se registre el acceso de personal o intentos accesos sin autorización a las instalaciones del COREFO?

## 1.8 Justificación

Al mes de agosto del año 2019, el ingreso al edificio del COREFO en la Gerencia Regional de Transmisión Sureste nunca ha sido controlado de ninguna manera, permitiendo que personas ajenas a las instalaciones ingresen sin ningún tipo de impedimento, quitándole la importancia que debería de brindarse a los equipos de alta vitalidad para la empresa que se encuentran dentro del edificio.

*Entrada del COREFO*



# Capítulo 2 Marco teórico

## 2.1 Importancia de un control de acceso.

Hay lugares en los que por seguridad el acceso debe estar restringido a personas no autorizadas. La vigilancia física no es ahora la única opción, gracias al desarrollo de las nuevas tecnologías, a los sistemas de control de accesos mediante aparatos electrónicos.

Hay diferentes maneras de autenticar el permiso de una persona para acceder a un área determinada. El más habitual era mediante un teclado, pero ya se está generalizando otro tipo de sistemas mediante tacs de proximidad o incluso variables biométricas, más fiables que otros sistemas.



## 2.2 Beneficios de un control de acceso.

El control de accesos es una poderosa arma de seguridad, pero no es su única ventaja. En espacios donde el paso de personas debe estar limitado, sirve de barrera para evitar accesos no autorizados, pero ejemplo en áreas sensibles de hospitales o centros diferentes tipos de lugares.

Permite, además, controlar las entradas y salidas del personal autorizado, de manera que se pueden registrar horarios y su relación con la productividad, por ejemplo, en salidas autorizadas para desayunos o comidas. Y no solo en el ámbito peatonal, hay que tener en cuenta que los controles de accesos se pueden instalar en lugares donde es posible entrar mediante vehículo privado, como, por ejemplo, en estacionamientos de personal de empresas o entidades públicas.

Todavía hay que tener en cuenta una utilidad muy particular de los sistemas de control de accesos. Es en aquellos lugares de gran afluencia de público. Un sistema de este tipo permite controlar el número de personas que entran a un determinado lugar, de modo que cabe la posibilidad de que el sistema se bloquee cuando se ha llegado al número máximo de ocupantes y no se desbloquee hasta que no haya sitio libre.

Todas estas ventajas han hecho que los sistemas de control de accesos estén cada vez más presentes en todo tipo de sitios, desde empresas a edificios públicos, centros deportivos, lugares donde se celebran eventos, etc. En forma de tornos, de barreras, de puertas abatibles, mediante lectores de tarjeta, de huella o incluso del iris, los sistemas para controlar entradas y salidas se han convertido en imprescindibles.

Y no hay que olvidar que, aunque ofrecen muchas ventajas para las empresas y entidades que los instalan en cuestiones económicas y de seguridad, también las tienen para las personas en general, que, por ejemplo, no podrán entrar por descuido en una zona que pueda ser peligrosa.

## 2.3 Historia del Arduino

Arduino es una tarjeta electrónica digital y además es un lenguaje de programación basado en C++ que es «open-source». En español se traduce como de «uso-libre». Su Hardware está construido por un microcontrolador de la familia AVR y es una de las tarjetas electrónicas más usadas para crear prototipos. Las instrucciones del lenguaje Arduino son muy fáciles de aprender y usar, incluso para personas con poco conocimiento de electrónica y/o programación. Es una herramienta muy utilizada por estudiantes y profesionales de sistemas embebidos. Dentro de las tarjetas Arduino más conocidas se encuentra el Arduino UNO R3.

Arduino Nació en el año 2005 el Instituto de Diseño Interactivo de Ivrea (Italia). Arduino apareció por la necesidad de contar con un dispositivo para utilizar en aulas que fuera de bajo coste. La idea original fue, fabricar una placa para uso interno de la escuela.

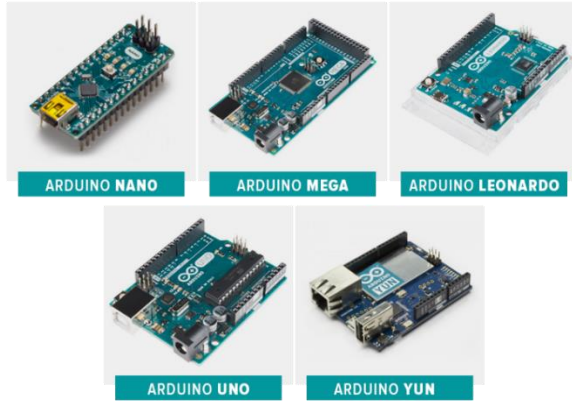
Sin embargo, el instituto se vio obligado a cerrar sus puertas precisamente en 2005. Ante la perspectiva de perder todo el proyecto Arduino en el proceso, se decidió liberarlo y abrirlo al público para que todo el mundo pudiese participar en la evolución del proyecto, proponer mejoras y sugerencias.



Los principales responsables de la idea y diseño de Arduino fueron Massimo Banzi, David Cuartielles, David Mellis, Tom Igoe y Gianluca Martino.

### 2.3.1 Evolución del Arduino

#### Ilustración 4. Tipos de Arduino existentes



Se han fabricado diferentes modelos de placas Arduino oficiales, cada una pensada con un propósito diferente y características variadas (como el tamaño físico, número de pines E/S, modelo del microcontrolador, etc). A pesar de las varias placas que existen todas pertenecen a la misma familia (microcontroladores AVR marca Atmel), esto significa que comparten la mayoría de sus características de software, como arquitectura, librerías y documentación.

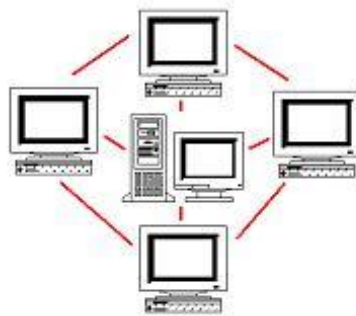
Fuente: (Arduino, 2019)

## 2.4 Protocolos de red

Es el término que se emplea para denominar al conjunto de normas, reglas y pautas que sirven para guiar una conducta o acción. Red, por su parte, es una clase de estructura o sistema que cuenta con un patrón determinado.

El concepto de protocolo de red se utiliza en el contexto de la informática para nombrar a las normativas y los criterios que fijan cómo deben comunicarse los diversos componentes de un cierto sistema de interconexión. Esto quiere decir que, a través de este protocolo, los dispositivos que se conectan en red pueden intercambiar datos.

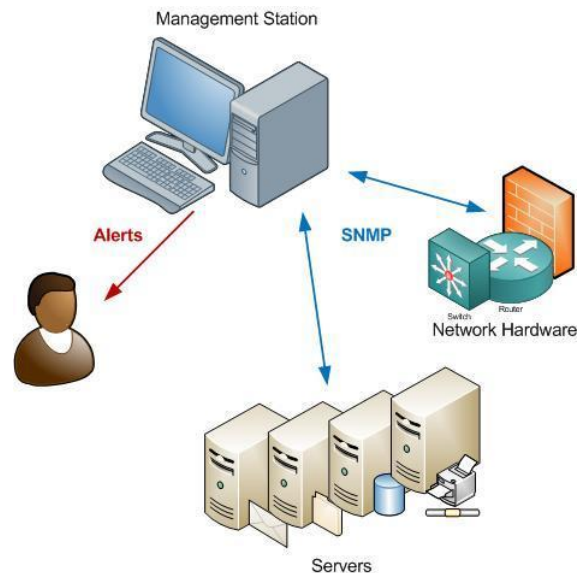
También conocido como protocolo de comunicación, el protocolo de red establece la semántica y la sintaxis del intercambio de información, algo que constituye un estándar. Las computadoras en red, de este modo, tienen que actuar de acuerdo con los parámetros y los criterios establecidos por el protocolo en cuestión para lograr comunicarse entre sí y para recuperar datos que, por algún motivo, no hayan llegado a destino.





## 2.4.1 Protocolo SNMP

El Protocolo simple de administración de red o SNMP (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.



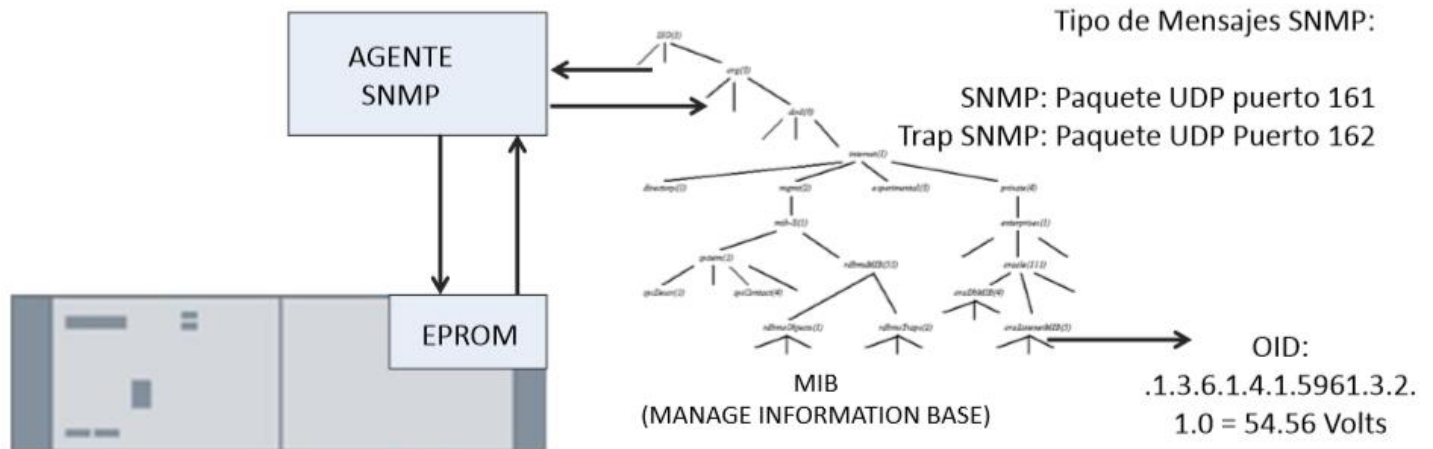
SNMP es un componente de la suite de protocolo de Internet como se define por el IETF. Se compone de un conjunto de normas para la gestión de la red, incluyendo una capa de aplicación del protocolo, una base de datos de esquema, y un conjunto de objetos de datos. Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

### Protocolo SNMP:

Uno de los protocolos más importantes que se puede utilizar en la recopilación de información de los dispositivos es SNMP.

El protocolo SNMP perteneciente a la pila de protocolos de modelo OSI ubicado en la capa de aplicación, significa Protocolo Simple de Administración de Red o SNMP (del inglés Simple Network Management Protocol).

### Ilustración 5. Estructura MIB del protocolo SNMP para equipos de Teleprotecciones, ejemplo



Fuente: Elaboración propia, 2019

Puntos para manejar por parte del Protocolo Simple de Administración de Red:

- Protocolo estándar de internet para administrar dispositivos en redes IP
- Más precisamente, es la manera estándar de monitorear hardware y software de cualquier fabricante desde Cisco a Juniper, desde Microsoft a Unix.
- Parte del protocolo de control de transmisiones / protocolo de internet (TCP / IP)
- Utiliza UDP como protocolo de transporte

El protocolo SNMP consta de una estructura de trabajo para realizar sus funciones como la que muestra a continuación:

- Componentes
  - Administrador de SNMP
  - Agente SNMP
  - Dispositivos administrados



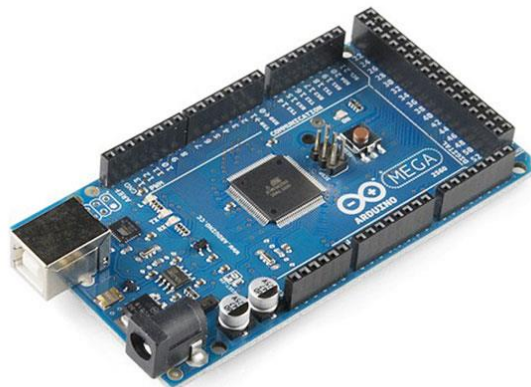
Descripción de componentes SNMP:

- **Dispositivo administrado:** Puede ser cualquier dispositivo de red como:
  - Equipos de redes unificadas (switches, routers, firewalls, servidores, acces points, etc)
  - Sistemas de alimentación (sistemas de fza 48 VCD, 12 VCD, inversores)
  - Equipos de Teleproteccion y Powerlink (acuses RX-TX
  - Puede ser cualquier servidor:

- Físico o virtual
  - cualquier SO: linux, solaris, windows, HP-UX
- 
- Cualquier dispositivo con una IP y un agente SNMP (MICROCONTROLADORES SNMP)
- **Agente SNMP:**
  - Windows SNMP
  - \*UX net-snmp
  - Cisco Cisco SNMP
  - OTROS Agent SBMP
- **Dispositivo administrado:** Cada fabricante de dispositivos, configura el agente SNMP en el dispositivo administrado para poder:
  - Recolecta información administrativa sobre su entorno local
  - Almacena y recupera información tal como se definió en la MIB
  - Indica cuando se produce un evento al administrador

# Capítulo 3 Marco referencial

## 3.1 Arduino mega



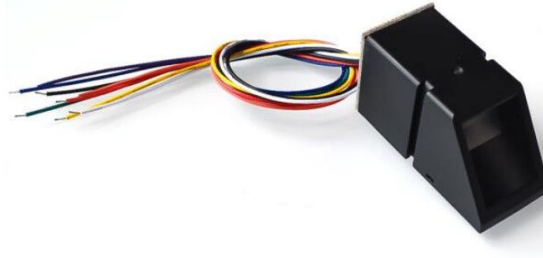
El Arduino Mega 2560 es una placa de desarrollo basada en el microcontrolador ATmega2560. Tiene 54 entradas/salidas digitales (de las cuales 15 pueden ser usadas como salidas PWM), 16 entradas analógicas, 4 UARTs, un cristal de 16Mhz, conexión USB, jack para alimentación DC, conector ICSP, y un botón de reseteo. La placa Mega 2560 es compatible con la mayoría de shields compatibles para Arduino UNO.

### Características técnicas del Arduino Mega

- Microcontrolador: ATmega2560
- Voltaje Operativo: 5V
- Voltaje de Entrada: 7-12V
- Voltaje de Entrada(límites): 20V
- Pines digitales de Entrada/Salida: 54 (de los cuales 15 proveen salida PWM)
- Pines análogos de entrada: 16
- Corriente DC por cada Pin Entrada/Salida: 40 mA
- Corriente DC entregada en el Pin 3.3V: 50 mA
- Memoria Flash: 256 KB (8KB usados por el bootloader)
- SRAM: 8KB
- EEPROM: 4KB
- Clock Speed: 16 MHz

## 3.2 Sensor lector de huella digital AS608

### Sensor AS608



El lector biométrico de huella digital es ideal para realizar un sistema capaz de proteger lo que tu requieras por medio del análisis de tu huella digital.

El sistema realiza procesamiento digital de imágenes interno con un DSP, además de incluir capacidades de comparación en base de datos y actualización de la misma, tiene la capacidad de almacenar hasta 162 huellas dactilares en su memoria FLASH interna. El LED del dispositivo se ilumina cada que se encuentra tomando imágenes en busca de huellas digitales funcionando con el protocolo serial, por lo que puede ser utilizado con cualquier microcontrolador o tarjeta de desarrollo.

### ESPECIFICACIONES TÉCNICAS

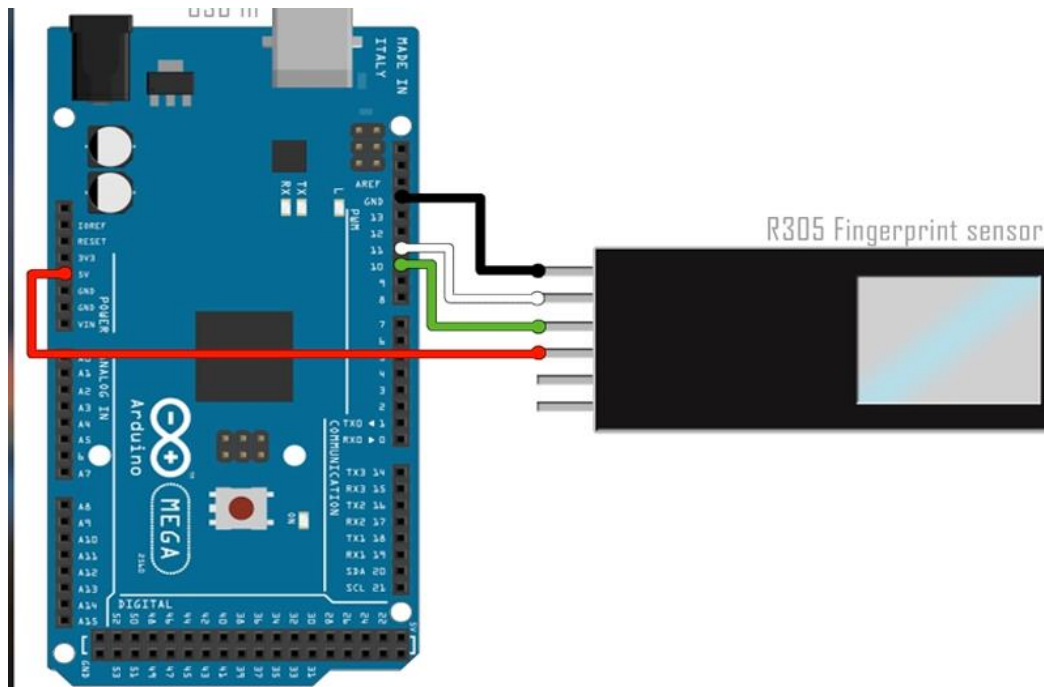
- Modelo: AS608
- Voltaje de alimentación: 3.6~6.0v
- Corriente de operación: 100mA – 150mA
- Interfaz: Serial/UART TTL
- Modo de paridad de huella: 1:1 1: N
- Baud Rate: 9600\*N
- N = 1 a 12 (Por defecto es 6)
- Tiempo de adquisición menor a 1 segundo
- 5 Niveles de seguridad
- Dimensión de la ventana: 19.5 x 15.5mm
- Temperatura de operación: -10°C a 40°C (Humedad Relativa 40% a 85%)
- Dimensiones del producto : 48 x 23.5 x 20mm

• Peso: 20g

PINES

- V+
- Tx
- Rx
- GND

Diagrama de conexión:



### 3.3 Pantalla LCD 16x2



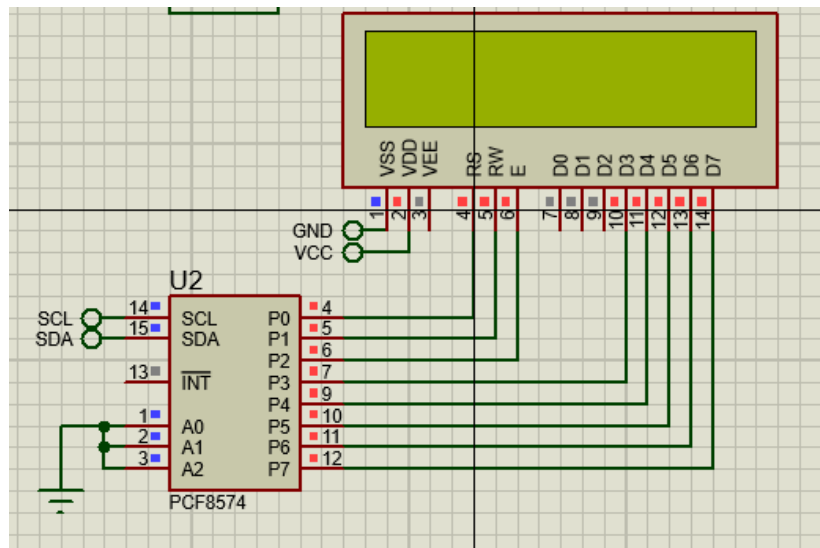
Pantalla LCD de 16x2 caracteres ideal para utilizarse en proyectos de arduino y con microcontroladores PIC. Es de 16 caracteres y 2 líneas, compatible con el controlador

HD44780 de Hitachi. Esta pantalla cuenta con iluminación de fondo azul con letras blancas. El chip controlador de esta pantalla es extremadamente común y el código necesario se encuentra disponible libremente en internet. Se puede utilizar fácilmente con cualquier microcontrolador que tenga al menos 6 pines disponibles.

### Características de la pantalla LCD de 16x2:

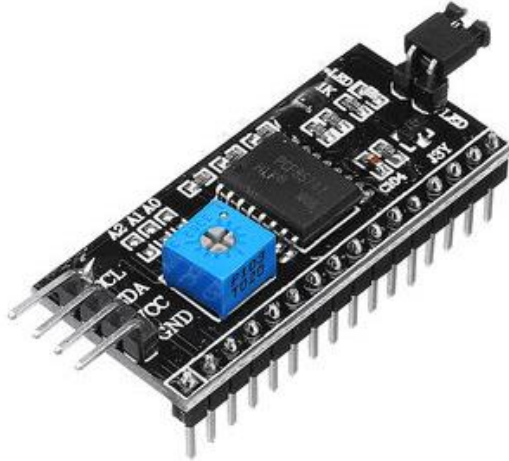
- Controlador HD44780
- Color: Fondo azul, letras blancas
- Modo de Operación: 4 y 8 bits
- Voltaje de operación: 4.5 – 5.5V

### Diagrama de conexión de la pantalla LCD 16x2:





## 3.4 Adaptador I2C



El Módulo adaptador LCD a I2C que usaremos está basado en el controlador I2C PCF8574, el cual es un Expansor de Entradas y Salidas digitales controlado por I2C. Por el diseño del PCB este módulo se usa especialmente para controlar un LCD Alfanumérico.

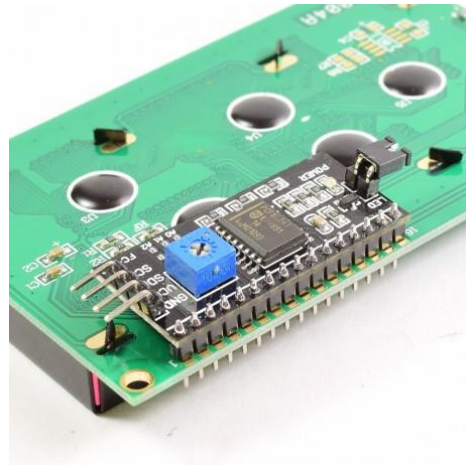
La dirección I2C por defecto del módulo puede ser 0x3F o en otros casos 0x27. Es muy importante identificar correctamente la dirección I2C de nuestro modulo, pues de otra forma nuestro programa no funcionará correctamente. Para identificar la dirección específica de nuestro módulo podemos utilizar un pequeño sketch de prueba llamado: I2C Scanner, el cual nos permite identificar la dirección I2C del dispositivo conectado al Arduino. Si en caso existiera la necesidad de trabajar con más de un LCD podemos modificar la dirección I2C del modulo adaptador.

### Características:

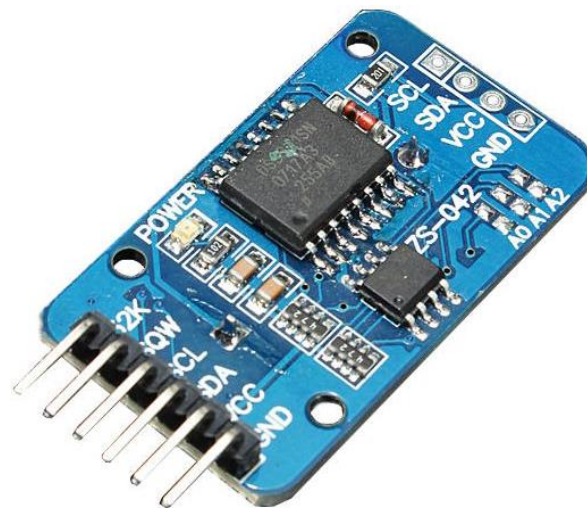
- Voltaje de Alimentación: 5V DC
- Controlador: PCF8574
- Dirección I2C: 0x3F (en algunos modelos es 0x27)
- Compatible con el protocolo I2C
- Jumper para Luz de fondo
- Potenciómetro para ajuste de contraste

### Conexiones entre Arduino y Módulo adaptador LCD a I2C

El adaptador LCD a I2C tiene los pines ordenados para conectar directamente al LCD, esto lo podemos hacer a través de un protoboard o soldando directamente al LCD.



### 3.5 Modulo RTC



El DS3231 es un reloj en tiempo real de alta precisión que cuenta con un oscilador a cristal con compensación de temperatura (TCXO). La integración del oscilador a cristal en el propio circuito integrado, en conjunto con la compensación de temperatura, asegura la precisión a largo plazo.

El RTC mantiene registro de segundos, minutos, horas, día de la semana, fecha, mes y año, la fecha es ajustada automáticamente a final de mes para meses con menos de 31 días, incluyendo las correcciones para año bisiesto.

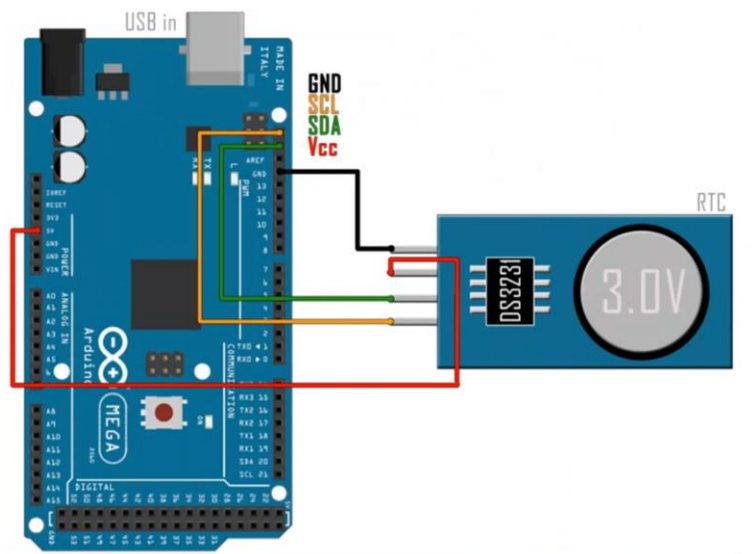
El DS3231 es capaz de generar señales de reloj cuadradas de frecuencia configurable y además cuenta con 2 alarmas programables que pueden generar interrupciones en el microcontrolador principal en tiempos específicos.

El módulo se comunica con el microcontrolador a través del bus I2C con solamente 2 pines que pueden ser compartidos por varios dispositivos como memorias EEPROM, expansores de IO, controladores PWM, etc.

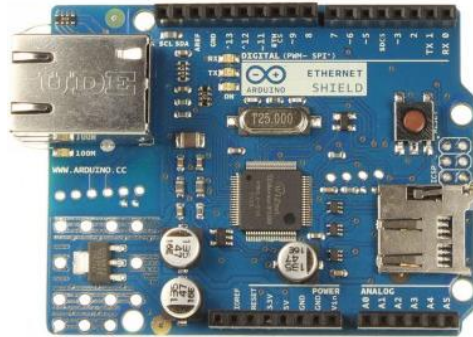
### Características de DS3231:

- Voltaje de alimentación de 3.0 a 5 volts.
- RTC de alta exactitud, maneja todas las funciones para el mantenimiento de fecha/hora.
- Exactitud de  $\pm 2\text{ppm}$  operando a una temperatura de  $0^{\circ}\text{C}$  a  $+40^{\circ}\text{C}$ .
- Módulo cuenta con reloj DS3231 y memoria EEPROM I2C.
- El módulo cuenta con batería de respaldo (incluida).
- Registro de segundos, minutos, horas, día de la semana, fecha, mes y año con compensación de años bisiestos hasta 2100.
- El DS3231 Incluye sensor de temperatura con exactitud de  $\pm 3$  grados centígrados.
- 2 alarmas programables por hora/fecha.
- Salida de señal cuadrada programable.

### Diagrama de conexión:



## 3.6 Shield Ethernet W5100



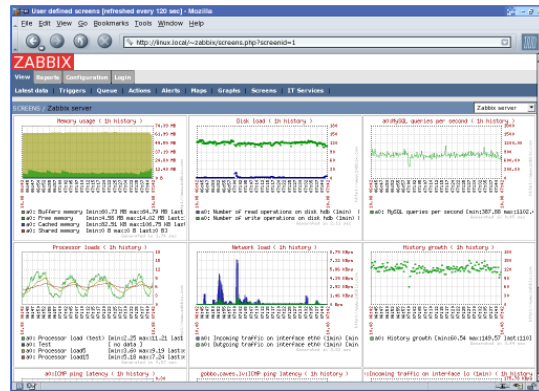
El Arduino Ethernet Shield permite a una placa Arduino conectarse a internet. Está basada en el chip ethernet Wiznet W5100. El Wiznet W5100 provee de una pila de red IP capaz de TCP y UDP. Soporta hasta cuatro conexiones de sockets simultáneas. Usa la librería Ethernet para escribir programas que se conecten a internet usando la shield.

- Es compatible con el Arduino UNO y Arduino Mega.
- El shield provee un conector ethernet estándar RJ45 y un conector lector de tarjeta Micro SD
- El botón de reset en la shield resetea ambos, el W5100 y la placa Arduino.

El shield contiene un número de LEDs para información:

- PWR: indica que la placa y la shield están alimentadas
- LINK: indica la presencia de un enlace de red y parpadea cuando la shield envía o recibe datos
- FULLD: indica que la conexión de red es full duplex
- 100M: indica la presencia de una conexión de red de 100 Mb/s (de forma opuesta a una de 10Mb/s)
- RX: parpadea cuando la shield recibe datos
- TX: parpadea cuando la shield envía datos
- COLL: parpadea cuando se detectan colisiones en la red

## 3.7 Plataforma ZABBIX



Zabbix es un Sistema de Monitorización de Redes creado por Alexei Vladishev. Está diseñado para monitorizar y registrar el estado de varios servicios de red, Servidores, y hardware de red.

Usa MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos. Su backend está escrito en C y el frontend web está escrito en PHP. Zabbix ofrece varias opciones de monitorización:

Chequeos simples que pueden verificar la disponibilidad y el nivel de respuesta de servicios estándar como SMTP o HTTP sin necesidad de instalar ningún software sobre el host monitorizado.

Un agente Zabbix puede también ser instalado sobre máquinas UNIX y Windows para monitorizar estadísticas como carga de CPU, utilización de red, espacio en disco, etc.

Como alternativa a instalar el agente sobre los host, Zabbix incluye soporte para monitorizar vía protocolos SNMP, TCP y ICMP, como también sobre IPMI, JMX, SSH, telnet y usando parámetros de configuración personalizados. Zabbix soporta una variedad de mecanismos de notificación en tiempo real, incluyendo XMPP.

Lanzado sobre los términos de la versión 2 de la GNU General Public License, Zabbix es Software Libre.

Zabbix fue iniciado como un proyecto interno de software en 1998. Después de 3 años, en 2001, este fue lanzado al público sobre GPL. Y tomo 3 años más hasta su primera versión estable, 1.0, que fue lanzada en 2004.

Funcionalidades:

- Alto rendimiento y alta capacidad (posibilidad de monitorizar cientos de miles de dispositivos)
- Auto descubrimiento de servidores y dispositivos de red
- Monitorización distribuida y una administración web centralizada
- Agentes nativos en múltiples plataformas

- Posibilidad de monitorización sin agentes
- Monitorización JMX
- Monitorización Web
- Configuración de permisos por usuarios y grupos
- Métricas SLA y ITIL
- Sistema flexible de notificación de eventos (Email, XMPP, etc)

## Desarrollo

Hoy en día Zabbix es desarrollado principalmente por una empresa dedicada a ello, Zabbix SIA.

### Código fuente:

- Zabbix consiste en algunos módulos aislados:
- Servidor
- Agentes
- Frontend
- Proxy
- Java gateway

Mientras que el servidor, proxy y agentes están escritos en C, el frontend está implementado en PHP y Javascript.

El Java gateway, disponible desde Zabbix 2.0, está escrito en Java.

## 3.8 Mensajería Telegram



Telegram Messenger es una aplicación de mensajería y VOIP desarrollada desde el año 2013 por los hermanos Nikolái y Pável Dúrov. Está enfocada en la mensajería instantánea, envío de varios archivos y comunicación en masa. El servicio lo administra una organización autofinanciada cuya sede principal opera en Dubái, Emiratos Árabes.

Entre sus funcionalidades principales están: conversaciones entre usuarios (como mensajes guardados, opción de reenvío, sincronización, alojamiento y archivado desde la nube), envío de archivos (hasta 1.5 GB, incluyendo documentos, multimedia y animaciones gráficas), gestión de contactos (adicionando la búsqueda global), encuestas, llamadas, canales de difusión, grupos, entre otros. Adicionalmente, los usuarios pueden desarrollar bots que pueden realizar otros servicios como pagos, juegos, moderación de grupos o automatización de tareas bajo inteligencia artificial.

Inicialmente el servicio fue empleado para teléfonos móviles (Android, iOS) y el año siguiente para multiplataforma (macOS, Windows, GNU/Linux, Firefox OS, navegadores web, y otros sistemas operativos). Las aplicaciones usan la interfaz de acceso gratuito, permitiendo a los desarrolladores crear clientes externos. Parte del software está bajo software libre —excepto el lado del servidor— y recibe el apoyo de la comunidad.

# **Capítulo 4 Diseño y desarrollo (simulación)**



## 4.1 Etapa 1 – Desarrollo de interfaz de enrollamiento de huellas.

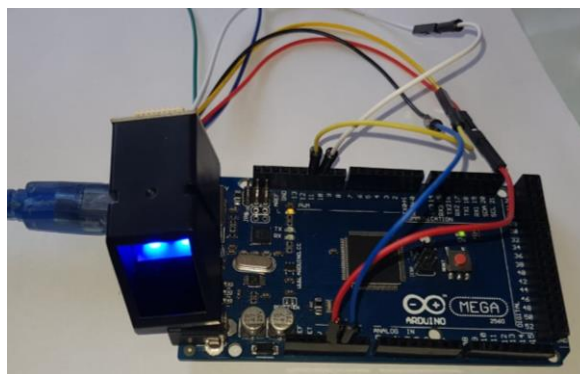
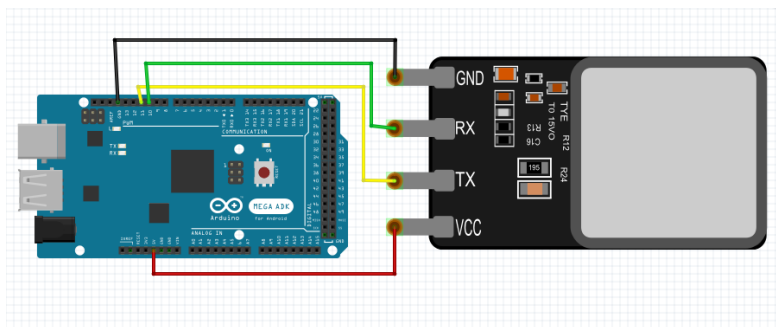
Para la primera etapa, se llevó a cabo la manipulación del sensor AS608 que es el que se utilizará para el desarrollo de este proyecto.

Se realizó la descarga de las librerías para la manipulación del sensor

### Adafruit\_Fingerprint

En esta etapa se realizará la conexión del arduino mega con el sensor (as608), es sensor cuenta con 6 salidas. Para la realización de los primeros programas de prueba se realiza la conexión de Vcc, GND, Tx y Rx conectados en la salida Vcc de arduino, GND en la respectiva salida y Tx y Rx conectados en las salidas digitales 11 y 10 respectivamente

*Ejemplo de conexionado de Lector de Huellas*



*Fuente: Elaboración Propia, 2019*

Se debe lograr el registro de huellas por medio de la memoria del AS608 en la cual podemos almacenar un aproximado de 162 huellas.

```
COM4
Fingertest
Fingerprint sensor encontrado!
Escriba numero de ID para guardar...
```

```
COM4
Fingertest
Fingerprint sensor encontrado!
Escriba numero de ID para guardar...
Enrolling ID #3
Esperando para enrollar huella correcta...
.....Capturando ImagenImagen convertida
Remueba la huella
Coloque el mismo dedo nuevamente
.....Capturando Imagen
Imagen Convertida
Huellas Similares
Huella Guardada
Escriba numero de ID para guardar...
 Autoscroll  Mostrar marca temporal
```

Una vez que guardó la imagen procedemos a realizar el reconocimiento por medio del segundo ejemplo de la librería.

```
COM4
Finger detect test
Found fingerprint sensor!
Sensor contains 7 templates
Waiting for valid finger...
Found ID #3 with confidence of 54
```

Ya que se reconoció la huella y comprobado que el sensor funciona correctamente podemos proceder al siguiente paso.

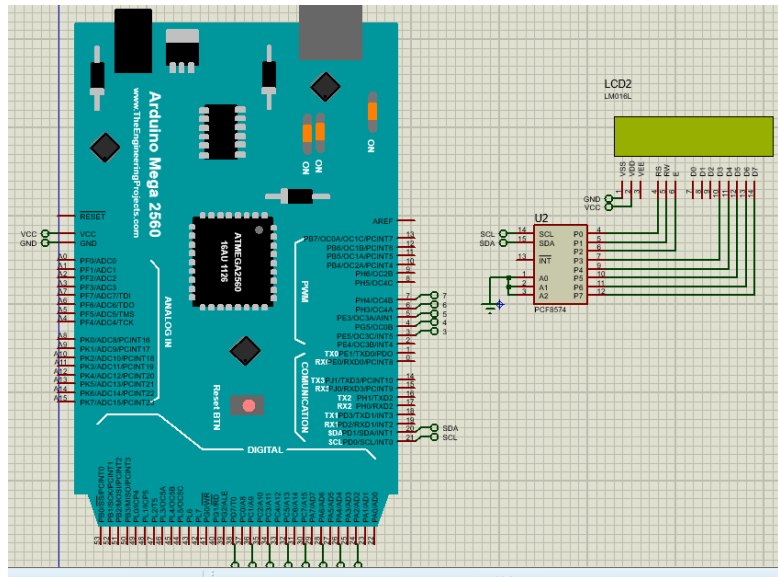
## 4.2 Etapa 2 - Diseño de configuración de la pantalla LCD

### Integración de la LCD con el sensor As608

Se utilizó una lcd de 16x2 conectada al bus I2C para reducir el uso de tantos pines para el arduino.

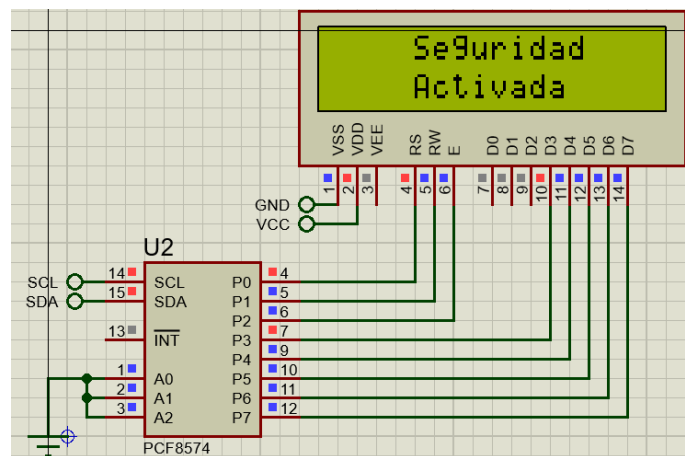
Se procedió a realizar el montaje de la LCD y el as608 sobre el Arduino Mega 2560, acompañado de la integración de 2 botones los cuales realizan la función de Escanear/OK y Agregar Usuario. También se integraron 2 leds que se encargaran de encender en verde si el acceso es permitido y el rojo si el intento de ingreso es no valido.

Ejemplo de conexionado de la LCD e I2C



Comprobado el funcionamiento de la lcd en la simulación se comenzaron a imprimir las primeras imágenes que serán la presentación de la pantalla (lo que visualizarán los usuarios) en la parte fisica.

Funcionamiento Simulado



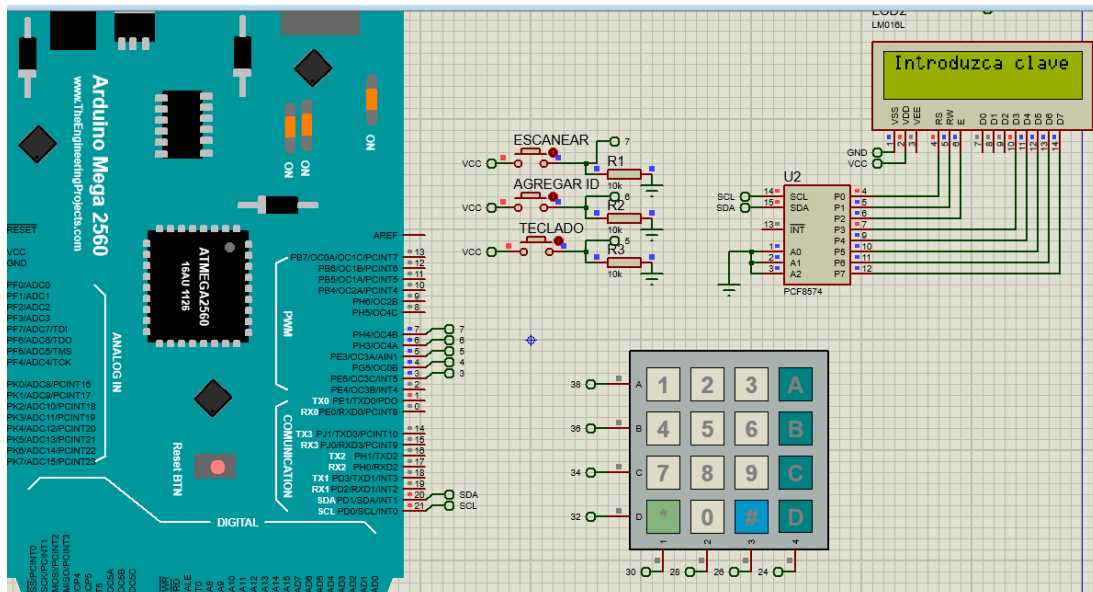


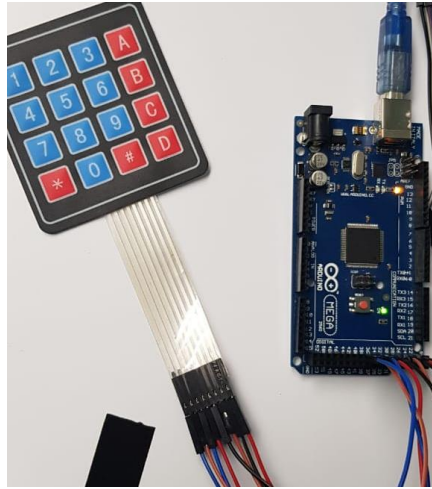
Pantalla de presentación de la LCD

### 4.3 Etapa 3 Integración del Teclado Matricial

Una vez que se integraron las partes anteriores se procedió a realizar la integración del teclado matricial para tener la certeza que la obtención de datos sea correcta así como el correcto funcionamiento del botón para activarlo y la comunicación con la LCD.

Ejemplo de conexión y funcionamiento simulado





*Teclado matricial 4X4 para pruebas*

La integración del teclado se utilizará como segundo método para poder acceder a las instalaciones, en caso que alguien no se encuentre registrado, pero conozca el PIN de acceso tendrá la posibilidad de ingresar al edificio.

Se optó por agregar un tercer botón que servirá para activar el acceso por medio del teclado, de esta manera se quedó conformado por 3 botones.

#### **4.4 Etapa 4 Integración de todos los componentes del dispositivo.**

La parte física del dispositivo quedó conformada de la siguiente manera:

Botón número 1: (Escanear / OK) se encargará de activar el escaneo del sensor para comenzar con la lectura de huellas.

Botón número 2: (Agregar ID) el botón 2 se encargará de poner en marcha la parte de registro de nuevas huellas en el dispositivo. Cabe aclarar que dentro del dispositivo se encontrarán un número determinado de huellas administradoras que serán las únicas capaces de permitir el registro de nuevas huellas.

Botón número 3: Se encargará de activar por medio del teclado la función de acceso por medio de PIN.

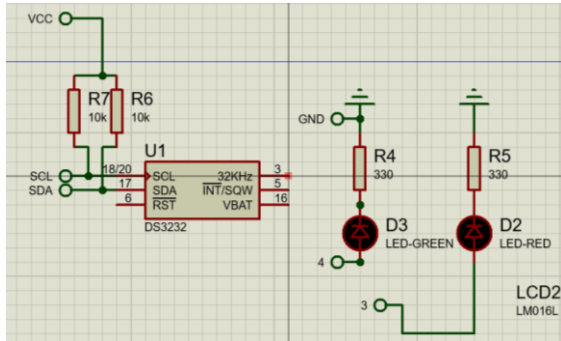
2 leds, que se encargaran de iluminar en color verde permitiendo el accionamiento de la cerradura magnética si el acceso es correcto o en color rojo si el acceso no es permitido.

Teclado Matricial encargado de brindar el acceso por medio de clave numérica.

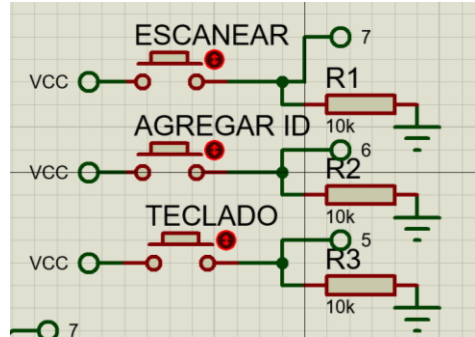
Pantalla LCD que se encargara de mostrar los mensajes para los usuarios.

También se integró un módulo RTC3231 que se encargará de llevar el registro de la hora y fecha en la que se registraron accesos tanto exitosos como fallidos.

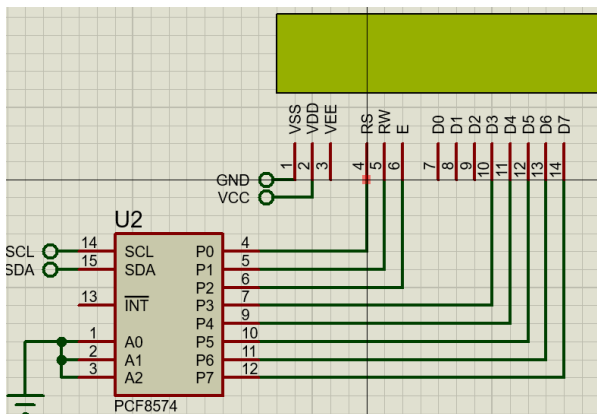
Módulo RTC Y leds indicadores



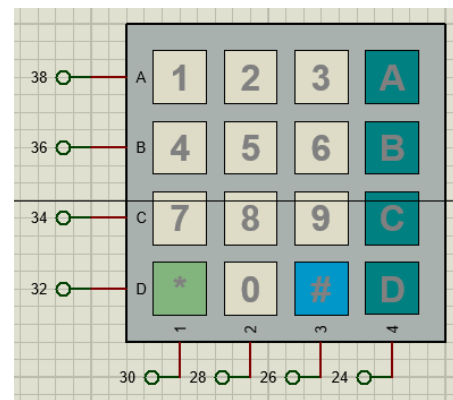
Botón escanear, agregar ID, teclado



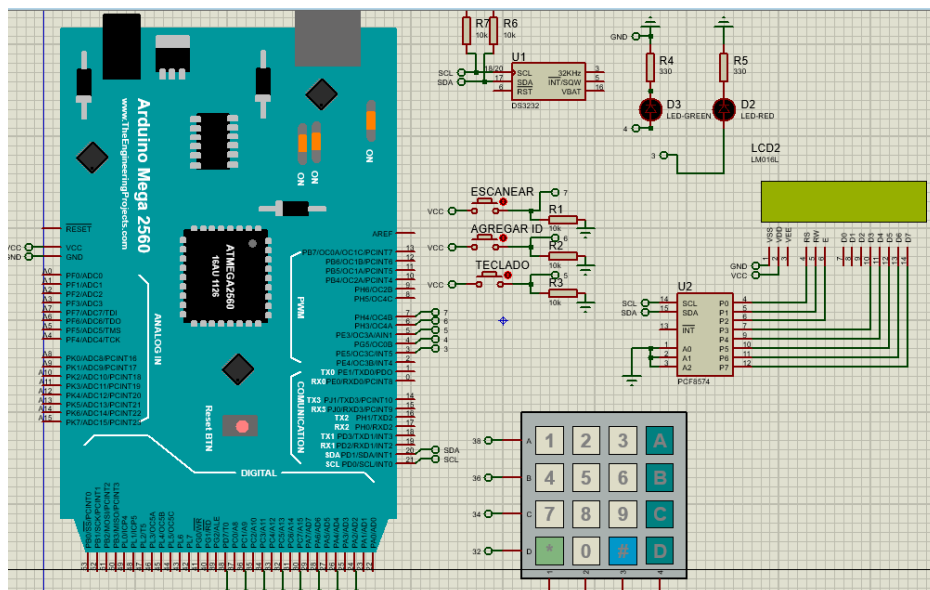
LCD



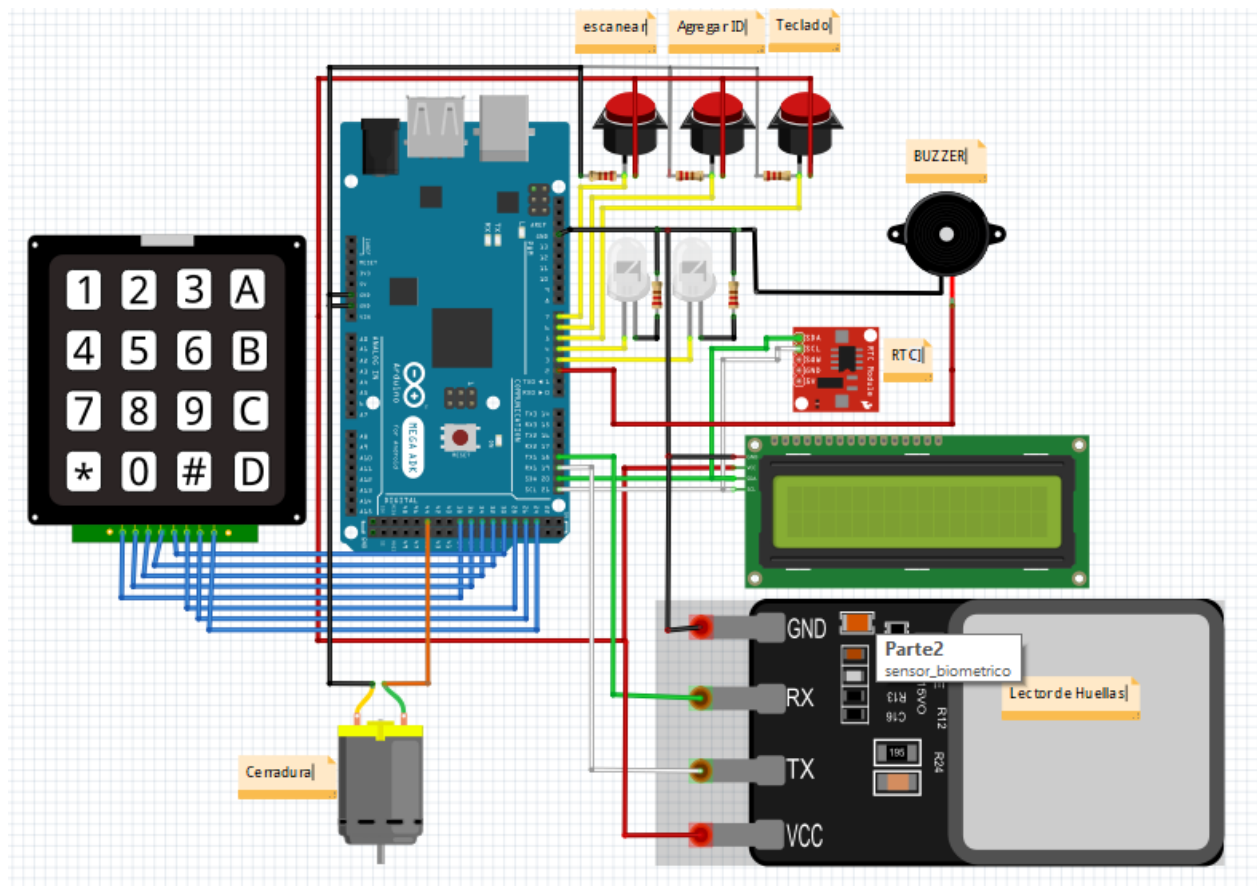
Teclado Matricial



Ejemplo de conexión y funcionamiento simulado



## 4.5 Etapa 5 Diagrama de conexionado.



Con el avance obtenido hasta el momento se obtiene el siguiente diagrama de conexionado. Es bien sabido que conforme el proyecto vaya avanzando se irán agregando detalles para cubrir necesidades que vayan surgiendo.

# Capítulo 5 Desarrollo del proyecto (físico)



## 5.1 Etapa 1 Montado de Componentes en protoboard

### Primeras pruebas:

Para el desarrollo de la primera parte con los componentes reales ya a utilizar, se realiza el proceso de conexión con la Pantalla LCD, y los botones respectivos para percatarnos de que el programa responda conforme a la lo deseado y a los resultados obtenidos en la simulación.

Pantalla de presentación



### Botón 1 – Escanear / OK

La pulsación de primer botón consiste en activar el lector de huellas entrando a la parte de reconocimiento de huellas, es decir que leerá la huella que se esté colocando sobre en sensor en ese momento y la comparará con las que tiene almacenado en su memoria. Si la huella es coincidente el programa te dirá el número de ID con el que se haya guardado en la memoria y así mismo permitir el acceso accionando la cerradura. El sistema cuenta con la capacidad de llevar un conteo de los intentos erróneos, es decir si alguna persona trata de ingresar siendo rechazada un total de 3 veces, automáticamente se emitirá una alarma visual (led rojo) y auditiva (buzzer) que durará alrededor de 10 segundos activa.

Botón de Escanear/ OK presionado



*Huella encontrada permitiendo acceso*



*Intento de acceso Huella no registrada*



## **Botón 2 – Agregar ID**

La pulsación del botón 2 consiste en activar el lector de huellas entrado a la parte de agregar nuevos ID's. Una vez aplastado el botón, el programa pedirá que se presente una huella de administrador que previamente fue guardada en la memoria del sensor, esto ayudara a que no cualquier persona pueda dar de alta más huellas en la memoria del sensor. Una vez presentada la huella del administrador el programa pedirá que escojas un número entre el 3 y el 19 para guardar el nuevo ID y de esta manera sea reconocido por el propio sensor.

**Nota 1: Los espacios para almacenar 1 y 2 no aparecen sobre la selección ya que estarán ocupados con las huellas de los administradores, es decir que se contarán con dos personas (huellas) que tendrán la capacidad de agregar nuevos ID's en el caso que sea requerido.**

**Nota 2:** El número de espacios dado para almacenar huellas en este programa es de 17, que van desde el 3 hasta el 19, esto es solo por requerimiento de la empresa, si se quisiera agrandar el número de espacios tendríamos un límite de 162 registros que es el aproximado de huellas que soporta la memoria del Sensor AS608.

*Botón Agregar ID, Pedimento de huella de administrador para validar registro*



*Espacio para almacenar la nueva huella*



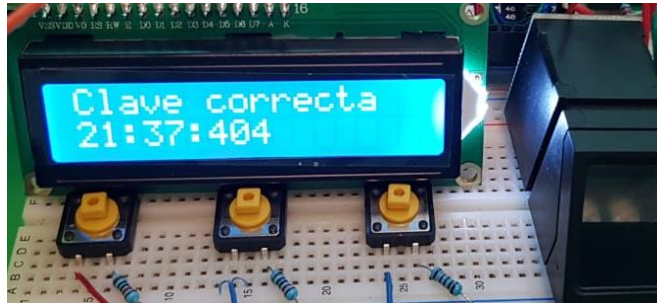
### **Botón 3 – Teclado**

La pulsación del botón 3 consiste en activar el teclado para poder ingresar la clave de acceso. Una vez aplastado el botón, el programa te pedirá que digites la clave, si la clave de acceso es correcta se activara el led verde y la cerradura para permitir el acceso, en caso contrario se activara el led rojo indicando que clave es incorrecta. De igual manera que el botón de escaneo, si se intenta accesar por más de 3 veces sin éxito se activara la alerta ya antes mencionada.

*Clave incorrecta digitada*



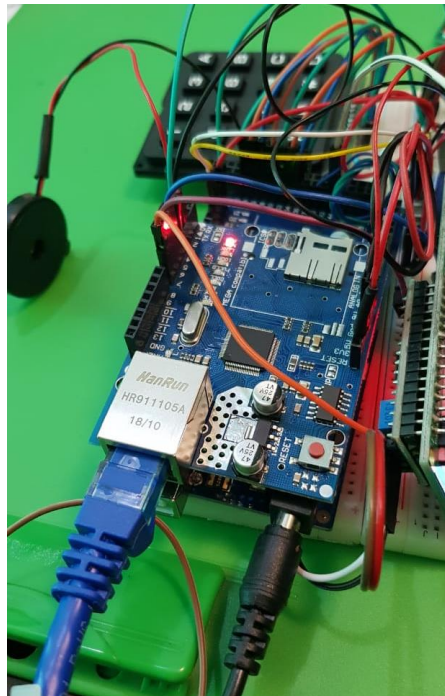
*Clave correcta puesta registrando hora*



## 5.2 Etapa 2 Integración de la Shield Ethernet

Una vez realizada la integración de todos los componentes en la parte física y demostrado que todo funciona correctamente, procedemos a la parte de la integración de la Shield Ethernet que será la encargada de mostrar la página y de recopilar los datos que obtenga el arduino.

*Shield Ethernet*



Direcciones asignadas a la tarjeta para poder establecer comunicación con la intranet de CFE.

- Dirección IP: 10.27.3.28
- Mascara de subred: 255.255.255.192
- Dirección Gateway: 10.27.3.62
- Dirección DNS: 10.27.2.134
- Numero de puerto de servidor ethernet: 80

La primera prueba que se realizó para verificar la comunicación de la Shield con la red, fue cargar una página prueba.

*Primera comunicación*

<

## Sistema de seguridad COREFO sureste

Sistema de seguridad COREFO sureste

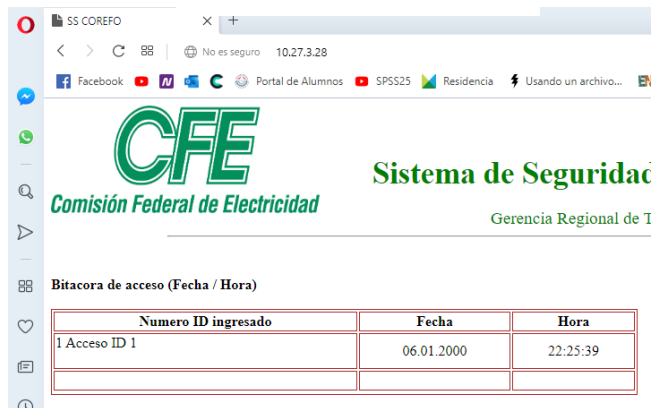
Bitacora de acceso (Fecha / Hora)

Una vez que se comprobó que la tarjeta funciona correctamente y que la incorporación al código general no causo conflictos se procedido a dar un poco más de estética a la página y comenzar a mandar los primeros valores.

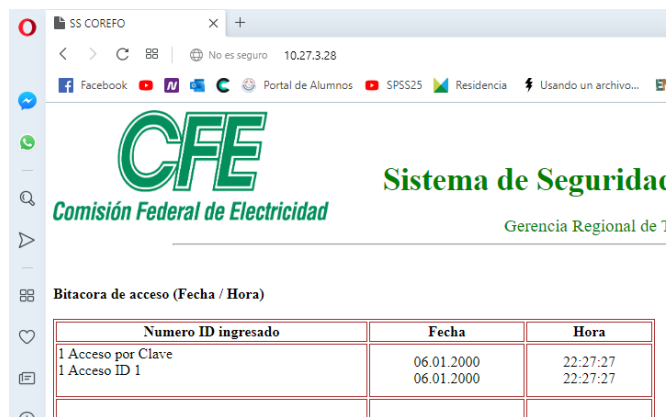
*Diseño de la Página Web*



*Registro de acceso por medio de ID*



*Registro de acceso por medio de Clave*



Bitacora de acceso (Fecha / Hora)

Numero ID Ingresado	Fecha/Hora
0 Acceso por Clave	18.12.2019 / 13:06:44
0 Acceso por Clave Acceso ID 6	18.12.2019 / 13:07:25
0 Acceso por Clave	18.12.2019 / 13:26:06

ID Registrados

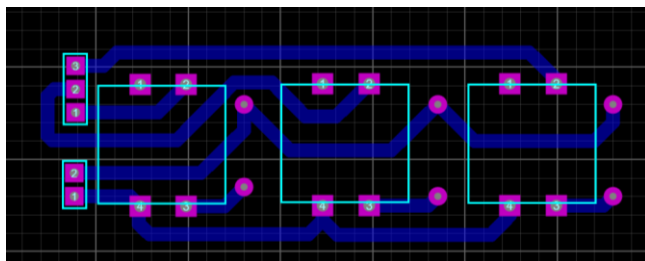
1. Ing. Guillermo Huerta Admin
2. Ing. Mario Aguilar Admin
3. Ing. Manuel Pineda
4. Ing. Rodiberto Cruz
5. Ing. Adriana de los Santos
6. Ing. Williams Reyes
7. Ing. Carlos Flores
8. Ing. Julio Valecia
9. Ing. Alejandro Pelayo
10. ....
11. Ing. Ingnacio Lopez

Tuxtla Gutiérrez, Chiapas  
Tecnológico Nacional de México  
Campus Tuxtla Gutiérrez  
Gerencia Regional de Transmisión Sureste

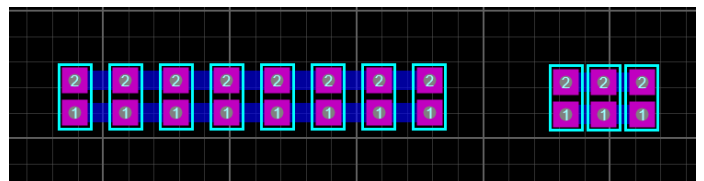
### 5.3 Etapa 3 Diseño de las placas en PCB.

Para poder proceder al armado del circuito de manera independiente se realizó el diseño y desarrollo de los circuitos en PCB. El diseño consto de la realización de 3 placas, una se encargará de integrar los botones correspondientes al dispositivo, la otra solo para poner la alimentación en paralelo de los 5v del arduino y de igual manera los pines SDA y SCL, y la tercera es módulo de relevador que funciona con lógica positiva.

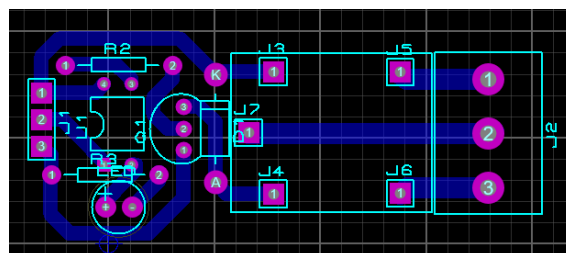
Circuito encargado de la activación de los 3 botones (Digitar Clave, Agregar ID, Escanear).



Circuito encargado de poner en paralelo la alimentación, así como los módulos SDA y SCL.

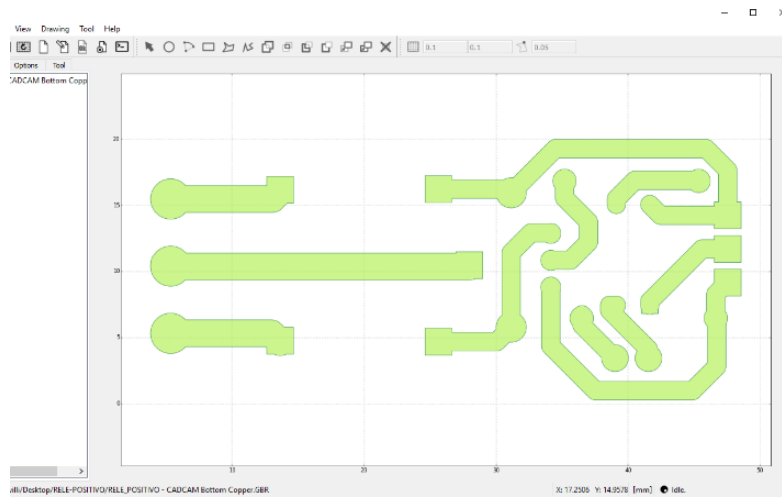


Módulo de relevador con lógica positiva

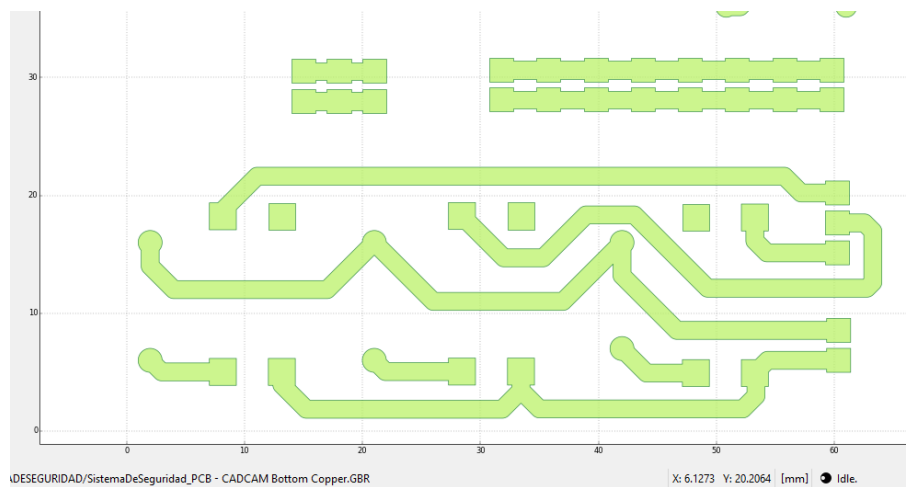


Una vez realizados los circuitos en PCB, se exportan al programa FlatCam para vectorizar las pistas y posteriormente poder imprimir con la CNC.

*Vectorización del módulo de relevador*

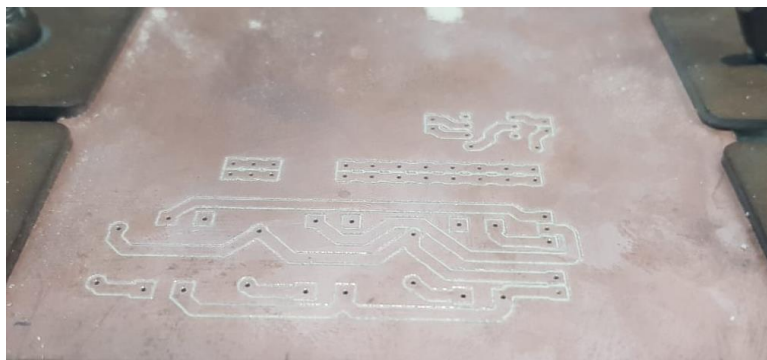


*Vectorización de la placa para los botones y alimentación en paralelo.*

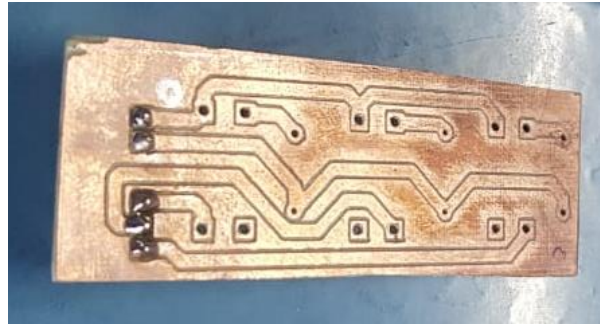


En cuanto se tienen vectorizados todos los circuitos a imprimir, se procede a realizar la impresión por medio de la CNC.

*Impresión realizada por CNC*



Impresión realizada por CNC



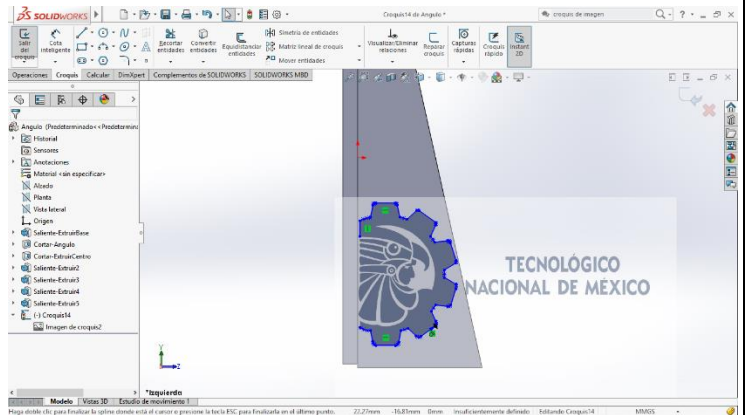
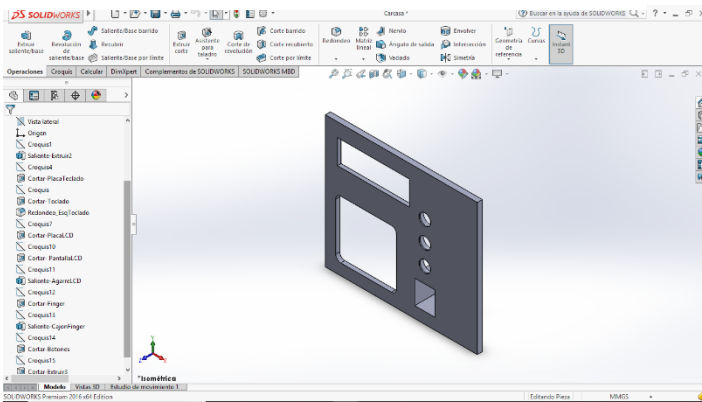
## 5.4 Etapa 4 Diseño en 3D de la carcasa física del dispositivo.

Se optó por realizar el diseño de una carcasa en 3D para colocar de la mejor manera todos los componentes del sistema y de igual manera mejorar la estética del proyecto.

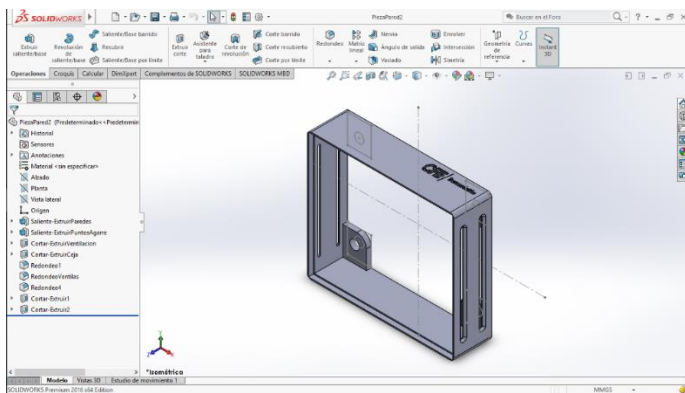
Se procedió a tomar las medidas de todos los componentes dándoles los márgenes, así como el espacio interior necesario para integrar todo de la mejor manera tomado en cuenta las placas PCB realizadas y el espacio que ocupado por el cableado interior.

Desarrollo del Angulo, con impresión del logo del Tecnológico Nacional de México

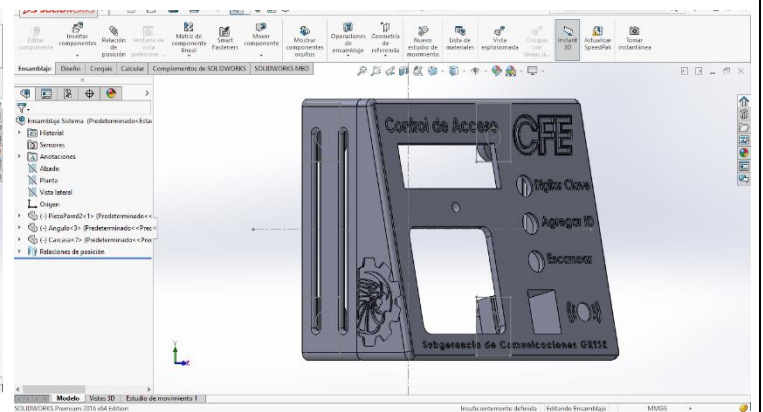
Desarrollo de la carcasa



Desarrollo de la pieza de agarre a la pared



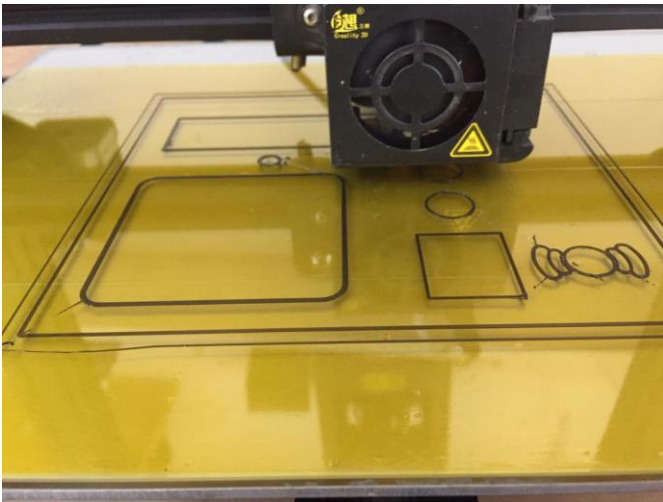
Diseño final de la carcasa del control de acceso





Aprobado el diseño final de la carcasa en 3D, se procedió a realizar la impresión.

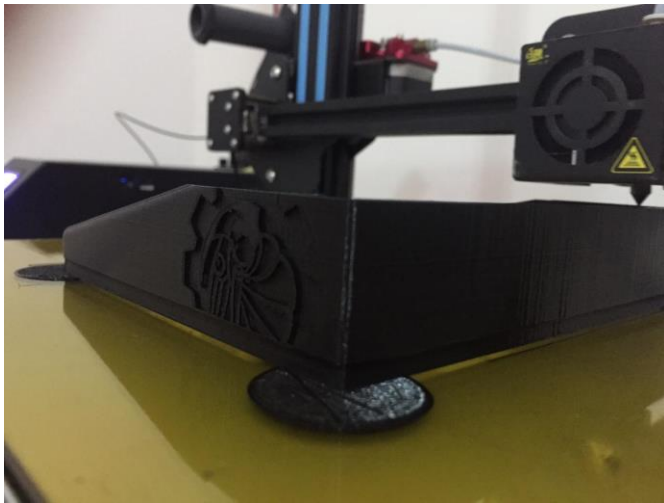
*Impresión en 3D – Inicio del proceso de caratula principal*



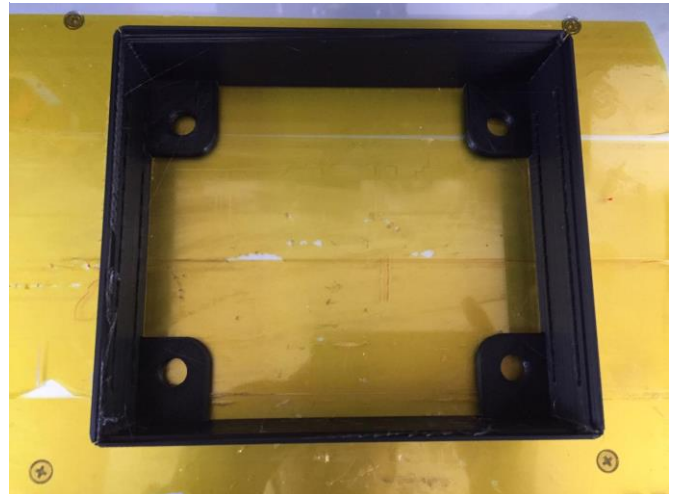
*Impresión en 3D – Final del proceso de caratula principal*



*Impresión en 3D – Proceso de realización del Angulo y logo del Tecnológico Nacional de México*



*Impresión en 3D – Pieza base de agarre a la pared terminada.*



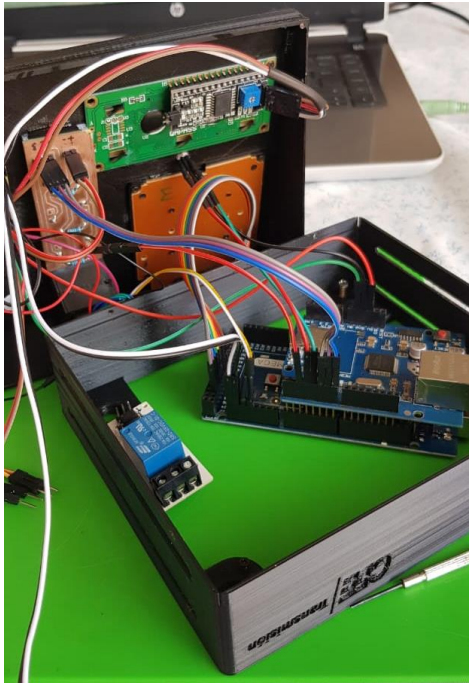
*Impresión en 3D – Resultado Final*



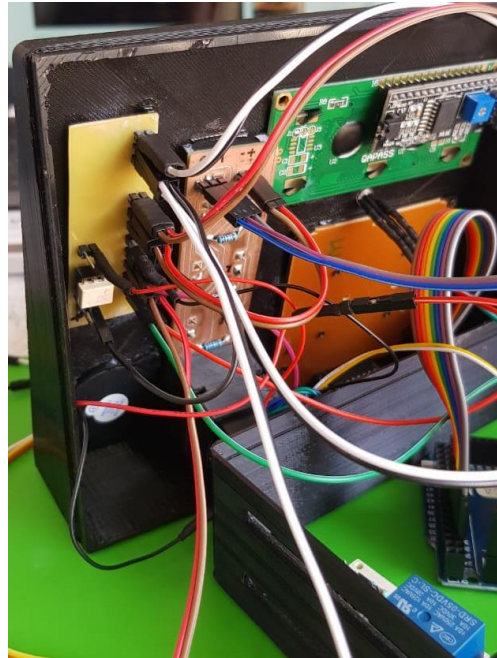
## 5.5 Etapa 5 Montado de componentes sobre la carcasa física.

Terminado el proceso de impresión en 3D, y comprobado el correcto funcionamiento de todos los componentes que conforman nuestro sistema de seguridad, se procedio a realizar el montaje de todos los componentes dentro la carcasa final.

*Montado de componentes en carcasa final*



*Montado de componentes en carcasa final*



*Presentación final del control de acceso.*



# Capítulo 6 Implementación del protocolo SNMP.

## 6.1 Etapa 1 Integración del código del SNMP al código general del control de acceso.

Como ya vimos en la introducción del protocolo SNMP (Protocolo simple de administración de red o del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación (del modelo OSI) que facilita el intercambio de información de administración entre dispositivos de red.

Como ya contamos con la integración de la shield ethernet que se utilizó para cargar la página Web, se facilita la integración de este código ya que hasta este punto ya tenemos conexión a la red internet de CFE.

Para comprobar el correcto funcionamiento y la activación del protocolo SNMP en nuestro control de acceso debemos apoyarnos de un buscador de MIBs y OID's, y para este caso se utilizó el "MIB Browser"

*Control de acceso en línea –SNMP  
Arduino*

Name/OID	Value	Type	IP:Port
.1.3.6.1.2.1.1.9.0	0 millisecond (0)	TimeTicks	10.27.3.28:161
.1.3.6.1.2.1.1.13.0	6	Integer	10.27.3.28:161
.1.3.6.1.2.1.1.11.0	CFE AccesoCorefo	OctetString	10.27.3.28:161
.1.3.6.1.2.1.1.12.0	Chiapas	OctetString	10.27.3.28:161
.1.3.6.1.2.1.1.8.0	SNMP-Arduino-AccesoCOREFO	OctetString	10.27.3.28:161
.1.3.6.1.2.1.1.10.0	Williams	OctetString	10.27.3.28:161

Comprobada la activación del SNMP proseguimos a hacer la búsqueda de los IOD'S asignados para las notificaciones, que serán los encargados de levantar las banderas de notificación que son Apertura por huella, Apertura por clave y acceso denegado.

*Declaración de variables con sus OID'S*

```
sysapertura_huella[]      PROGMEM = "1.3.6.1.4.1.36582.5.1.0"; //oid
sysapertura_clave[]      PROGMEM = "1.3.6.1.4.1.36582.5.1.1"; //oid
sysacceso_denegado[]     PROGMEM = "1.3.6.1.4.1.36582.5.1.2"; //oid
```

*OID'S correspondientes a las banderas de notificación.*

Name/OID	Value	Type	IP:Port
sysDescr.0	SNMP-Arduino-AccesoCOREFO	OctetString	10.27.3.28:...
sysUpTime.0	0 millisecond (0)	TimeTicks	10.27.3.28:...
sysContact.0	Williams	OctetString	10.27.3.28:...
sysName.0	CFE AccesoCorefo	OctetString	10.27.3.28:...
sysLocation.0	Chiapas	OctetString	10.27.3.28:...
sysServices.0	6	Integer	10.27.3.28:...
1.3.6.1.4.1.36582.5.1.0	0.00	OctetString	10.27.3.28:...
1.3.6.1.4.1.36582.5.1.1	0.00	OctetString	10.27.3.28:...
1.3.6.1.4.1.36582.5.1.2	0.00	OctetString	10.27.3.28:...

Para que el abanderamiento funcione correctamente, la variable contenida por el OID debe realizar un cambio de estado de 0 a 1 y durar aproximadamente 5 segundos para que el cambio se vea reflejado.

Activación del OID 5 segundos aproximado

Name/OID	Value	Type	IP:Port
.1.3.6.1.4.1.36582.5.1.2	0.00	OctetString	10.27.3.28:...
.1.3.6.1.4.1.36582.5.1.2	1.00	OctetString	10.27.3.28:...
.1.3.6.1.4.1.36582.5.1.2	1.00	OctetString	10.27.3.28:...
.1.3.6.1.4.1.36582.5.1.2	1.00	OctetString	10.27.3.28:...
.1.3.6.1.4.1.36582.5.1.2	1.00	OctetString	10.27.3.28:...
.1.3.6.1.4.1.36582.5.1.2	0.00	OctetString	10.27.3.28:...
.1.3.6.1.4.1.36582.5.1.2	0.00	OctetString	10.27.3.28:...
.1.3.6.1.4.1.36582.5.1.2	0.00	OctetString	10.27.3.28:...

Como se hizo notar, se reflejó el cambio de estado de 5 segundos aproximadamente que serán suficientes para poder aplicar una acción desde el ZABBIX.

## 6.2 Etapa 2 Registro del sistema en la plataforma de ZABBIX.

El sistema de seguridad inteligente para acceso al COREFO sureste y sala de equipos de comunicaciones del hotel Tuxtla tiene la capacidad de mandar la notificaciones y alertas de forma directa a la plataforma del ZABBIX, por ende, se procede a dar el alta del equipo en la plataforma.

La plataforma del ZABBIX de encarga de leer todos los datos que son mandados desde el arduino por medio del puerto 161 que es el utilizado para mandar información al protocolo SNMP.

Alta del arduino en el ZABBIX

Host group	Critica	Severa	Intermedio	Menor	Information	Not classified
ARDUINO	0	0	2	0	0	0
ARDUINO HOTEL TUXTLA	0	0	0	0	0	0
ARDUINO SE.MPD	0	0	4	0	0	0
SIST. FZA. GRTSE	0	0	0	0	0	0
SIST. FZA. HTTUX	0	0	0	0	0	0
SIST. FZA. ZTTAP	0	0	0	0	0	0
TELEPROTECCIONES ZTISTMO	0	0	0	0	0	0
TELEPROTECCIONES ZTMALPASO	0	0	0	0	0	0
Zabbix servers	0	0	0	0	0	0

El registro del equipo en el ZABBIX se realizó de la siguiente manera.

Nombre: ARDUINO HOTEL TUXTLA

IP: 10.27.3.28

Puerto de comunicación: 161

Registro correcto del Arduino ligado al host (Control de acceso HTTUX).

The screenshot shows the 'Host groups' page in Zabbix. A table lists various host groups. The row for 'ARDUINO HOTEL TUXTLA' is highlighted with a red rectangular box. The table has columns for Name, Hosts, Templates, and Members.

Name	Hosts	Templates	Members
ARDUINO HOTEL TUXTLA	Hosts 1	Templates	Control de acceso HTTUX
ARDUINO SE.MPD	Hosts 1	Templates	DISPOSITIVO DE CONTROL Y MONITOREO DE ALARMAS ARDUINO SE.MPD
ARDUINO	Hosts 1	Templates	Dispositivo de Control y Monitoreo de Alarmas Arduino
ARDUINO SE.MPD	Hosts 1	Templates	DISPOSITIVO DE CONTROL Y MONITOREO DE ALARMAS ARDUINO SE.MPD
Discovered hosts	Hosts	Templates	
Hypervisors	Hosts	Templates	
Linux servers	Hosts	Templates	
Network devices	Hosts	Templates	
SIST. FZA. GRTSE	Hosts 1	Templates	SE.GRTSE.SFEMEISA-02
SIST. FZA. HTTUX	Hosts 2	Templates	SE.HTTUX.SFMEI-01, SE.HTTUX.SFMEI-02
SIST. FZA. ZITAP	Hosts 2	Templates	SE.THP.SFEMEISA-01, SE.THP.SFMEI-01
TELEPROTECCIONES ZTISTMO	Hosts 1	Templates	SE.OXP-93710-TMU.SWT3000-OXP
TELEPROTECCIONES ZTMALPASO	Hosts 2	Templates	SE.MPD-93940-PEA.SWT3000-PEA, SE.PEA-93910-MZW.SWT3000-PEA
Templates	Hosts	Templates 76	Template App FTP Service, Template App HTTP Service, Template App HTTPS Service, Template App IMAP Service, Template App LDAP Service, Template App MySQL, Template NNTS Service, Template App NTP Service, Template App POP Service, Template App SMTP Service, Template App SSH Service, Template App Telnet Service, Template App Zabbix Agent, Template App Zabbix Sender, Template IPMI Intel SP1630, Template IPMI Intel SP1630, Template IMV Generic, Template

Para el equipo se debe dar de alta el host que en este caso se llama Control de acceso HTTUX que alojara las variables como ítems que presentaran los cambios de estado para que a su vez la misma plataforma pueda realizar el envío de notificaciones, las cuales quedaron asignadas de la siguiente manera.

- Acceso Denegado
- Apertura por Clave
- Apertura por Huella

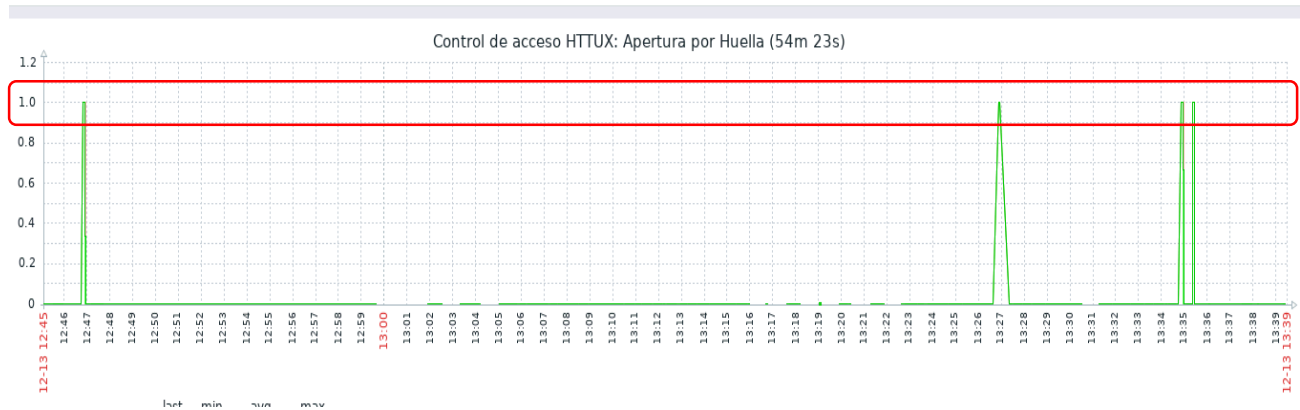
Variables habilitadas por protocolo SNMP

The screenshot shows a table of Zabbix items for the host 'ARDUINO HOTEL TUXTLA'. Four rows are highlighted with red boxes, corresponding to the items mentioned in the text above: 'Acceso Denegado', 'Apertura por Clave', and 'Apertura por Huella'. The table has columns for Name, Triggers, Key, Interval, History, Trends, Type, Applications, Status, and Info.

Name	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
ARDUINO HOTEL TUXTLA: Acceso Denegado		sysacceso_denegado	1s	90d	365d	SNMPv1 agent		Enabled	
ARDUINO HOTEL TUXTLA: Apertura por Clave	Triggers 1	sysapertura_clave	1s	90d	365d	SNMPv1 agent		Enabled	
ARDUINO HOTEL TUXTLA: Apertura por Huella		sysapertura_huella	1s	90d	365d	SNMPv1 agent		Enabled	
ARDUINO HOTEL TUXTLA: Gestion		icmping	30s	90d	365d	Simple check		Enabled	
ARDUINO HOTEL TUXTLA: No. Servicios		sysServices	1s	90d	365d	SNMPv1 agent		Enabled	
ARDUINO HOTEL TUXTLA: Nombre de contacto		sysContact	30s	90d		SNMPv1 agent		Enabled	
ARDUINO HOTEL TUXTLA: Puerta Cerrada		syspuerta_cerrada	1s	90d	365d	SNMPv1 agent		Enabled	
ARDUINO HOTEL TUXTLA: Tiempo excedido puerta abierta		sys tiempo_excedidoap	1s	90d		SNMPv1 agent		Enabled	

Una vez dadas de alta las tres variables se verifica que realice correctamente el cambio de estado, para esta prueba se realizaron 3, para la configuración del ZABBIX se estableció mandar una alerta informativa cuando el valor de la variable llegue a 1, es decir, cuando alguien ingrese por medio de la huella.

*Cambio de estado a 1 cuando se realiza ingreso.*

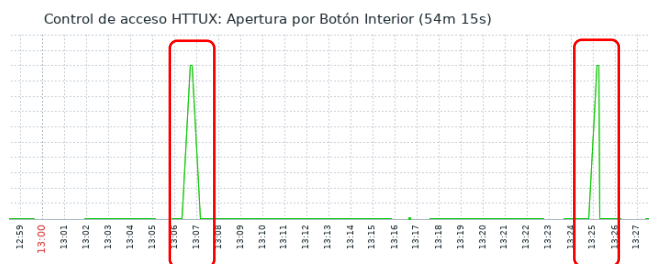


### 6.3 Etapa 3 Envió notificaciones vía Telegram.

Como ya habíamos mencionado, se procederá a realizar el envío de notificaciones por medio del ZABBIX.

En cuanto se aseguran que los cambios de estado son enviados correctamente desde el arduino es cuando se puede proceder a realizar la activación de las notificaciones.

*Cambios de estado de variables del arduino detectados*



The screenshot shows the ZABBIX configuration interface for creating a new action. The 'Name' field is filled with 'Control de Acceso Hotel Tuxtla'. Under the 'Conditions' section, a condition is added with label 'A' and name 'Host group = ARDUINO HOTEL TUXTLA'. The 'New condition' section is empty. The 'Enabled' checkbox is checked. At the bottom, there are buttons for 'Update', 'Clone', 'Delete', and 'Cancel'.

Se procede ahora sobre la configuración generar un apartado de acciones que se van a realizar con los cambios de estado. Por lo tanto, se debe crear la acción con el nombre de “Control de Acceso Hotel Tuxtla”.

Una vez configurado el apartado de acciones, se procede a agregar los contactos (que previamente ya se encontraban registrados en la plataforma del ZABBIX para el contacto por medio de Telegram), para este caso solo se encontraban como responsables del área los dos contactos ya agregados.

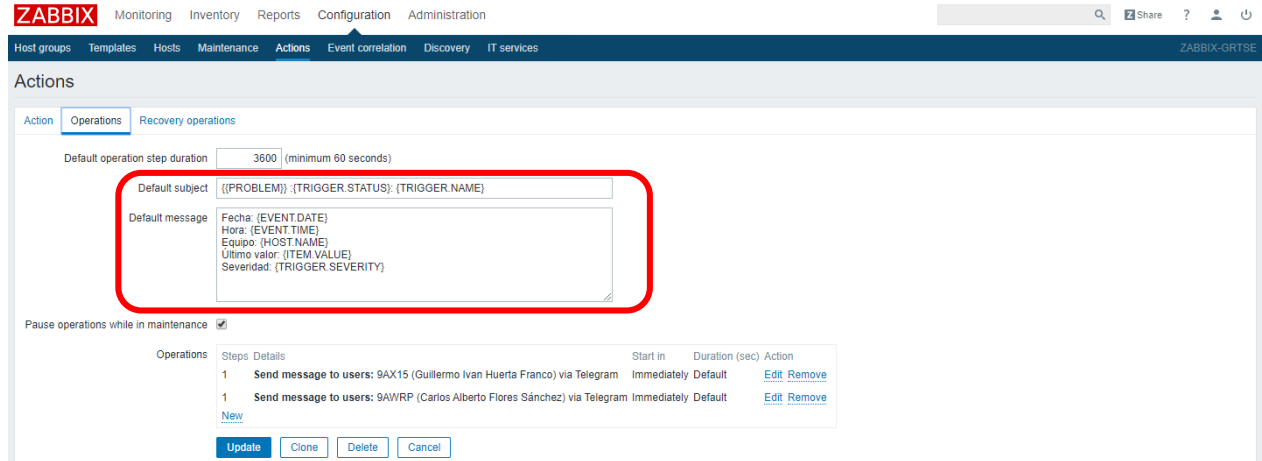
Name	Conditions	Operations	Status
ALARMAS ARDUINO	Host group = ARDUINO	Send message to user groups: Subgerencia de Comunicaciones GRTSE, Zabbix administrators via Telegram	Enabled
ALARMAS SIST. FZA. ZTTAPACHULA	Host group = SIST. FZA. ZTTAP	Send message to user groups: Subgerencia de Comunicaciones GRTSE, Zabbix administrators, ZONA DE TRANSMISIÓN TAPACHULA via Telegram	Enabled
ALARMAS SIST.FZA HTTUX	Host group = SIST. FZA. HTTUX	Send message to user groups: Subgerencia de Comunicaciones GRTSE, Zabbix administrators via Telegram	Enabled
ALARMAS SIST FZA GRTSE	Host group = SIST. FZA. GRTSE	Send message to user groups: Subgerencia de Comunicaciones GRTSE, Zabbix administrators via Telegram	Enabled
ALARMAS TELESWT3000 ZTITSMO	Host group = TELEPROTECCIONES ZTITSMO	Send message to user groups: Subgerencia de Comunicaciones GRTSE, Zabbix administrators via Telegram	Enabled
ALARMAS TELESWT3000 ZTMALPASO	Host group = TELEPROTECCIONES ZTMALPASO	Send message to user groups: Zabbix administrators via Telegram	Enabled
Control de Acceso Hotel Tuxtla	Host group = ARDUINO HOTEL TUXTLA	Send message to users: 9AX15 (Guillermo Ivan Huerta Franco) via Telegram Send message to users: 9AWRP (Carlos Alberto Flores Sánchez) via Telegram	Enabled
Report problems to Zabbix administrators		Send message to user groups: Zabbix administrators via all media	Disabled

Ya registrados los contactos ahora se procede a realizar la operación que se va realizar cuando se realizan los cambios de estados, para lo cual de establecer el mensaje que por default será enviado que en este caso engloba:

- Problem: establece el motivo del mensaje es decir si se registró el acceso por medio de huella o clave.
- Fecha
- Hora
- Equipo: Nombre con el cual se realizó el registro
- Ultimo valor: Muestra el valor que se alcanzó para generar el disparo que para este caso sería el valor de 1
- Severidad: que por defecto debe ser como mínima “intermedia” para que se pueda realizar el proceso del envío del mensaje.



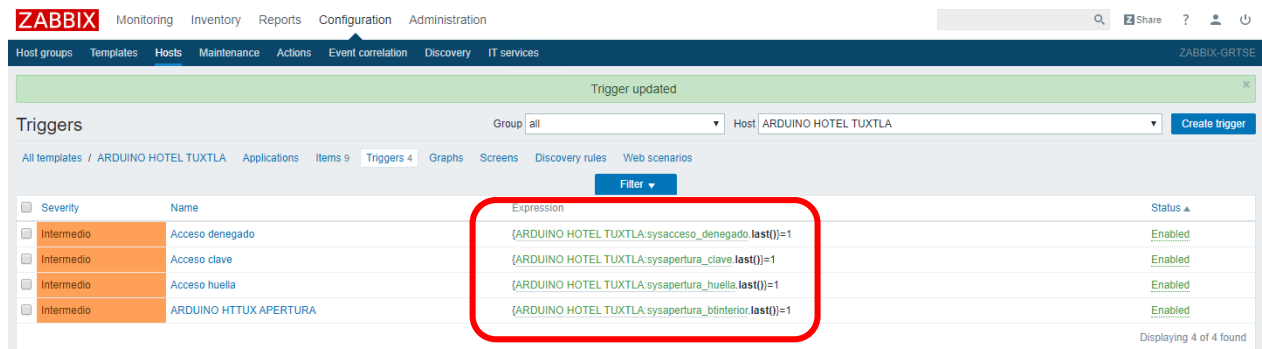
## Estructura del mensaje que será enviado por defecto



The screenshot shows the ZABBIX configuration interface for an Action. The 'Default subject' field contains the expression: `{{(PROBLEM)}}: {{(TRIGGER.STATUS)}}: {{(TRIGGER.NAME)}}`. The 'Default message' field contains the following text: `Fecha: (EVENT.DATE)  
Hora: (EVENT.TIME)  
Equipo: (HOST.NAME)  
Último valor: (ITEM.VALUE)  
Severidad: (TRIGGER.SEVERITY)`. A red box highlights these two fields. Below them, there is a 'Pause operations while in maintenance' checkbox which is checked. At the bottom, there is a table of 'Operations' with two entries, each with a 'Send message to users' action.

Steps	Details	Start in	Duration (sec)	Action
1	Send message to users: 9AX15 (Guillermo Ivan Huerta Franco) via Telegram	Immediately	Default	<a href="#">Edit</a> <a href="#">Remove</a>
1	Send message to users: 9AWRP (Carlos Alberto Flores Sánchez) via Telegram	Immediately	Default	<a href="#">Edit</a> <a href="#">Remove</a>

Por ultimo solo quedaría por establecer que cuando se realice el disparo y el valor preestablecido en el registro sea igual a en las variables descritas como Acceso denegado, Acceso clave, Acceso clave y Acceso denegado, es cuando se realizara el envío de notificaciones.



The screenshot shows the ZABBIX configuration interface for Triggers. A notification banner at the top says 'Trigger updated'. The 'Triggers' section shows a list of triggers for the host 'ARDUINO HOTEL TUXTLA'. A red box highlights the 'Expression' column for four triggers: 'Acceso denegado', 'Acceso clave', 'Acceso huella', and 'ARDUINO HTTUX APERTURA'. The expressions are: `{(ARDUINO HOTEL TUXTLA:sysacceso_denegado.last())}=1`, `{(ARDUINO HOTEL TUXTLA:sysapertura_clave.last())}=1`, `{(ARDUINO HOTEL TUXTLA:sysapertura_huella.last())}=1`, and `{(ARDUINO HOTEL TUXTLA:sysapertura_btinterior.last())}=1`.

Severity	Name	Expression	Status
Intermedio	Acceso denegado	<code>{(ARDUINO HOTEL TUXTLA:sysacceso_denegado.last())}=1</code>	Enabled
Intermedio	Acceso clave	<code>{(ARDUINO HOTEL TUXTLA:sysapertura_clave.last())}=1</code>	Enabled
Intermedio	Acceso huella	<code>{(ARDUINO HOTEL TUXTLA:sysapertura_huella.last())}=1</code>	Enabled
Intermedio	ARDUINO HTTUX APERTURA	<code>{(ARDUINO HOTEL TUXTLA:sysapertura_btinterior.last())}=1</code>	Enabled

### 6.3 Etapa 4 Recepción de notificaciones vía Telegram.

Ya estando en el Smartphone podemos recibir las notificaciones cuando se realicen los cambios de estado y cómo podemos ver en las capturas, cuando se accesa por medio de la clave se realiza el abanderamiento de la variable que por ende toma el valor de 1, el ZABBIX manda el mensaje de advertencia con el signo de admiración en rojo y te arroja el mensaje haciendo mención que se hizo un acceso por medio de la clave, e inmediatamente te manda el siguiente mensaje reportando que la variable ya bajo el abanderamiento y su regreso a su estado normal que es 0, de igual manera se realiza con el acceso por huella, con el botón interior y con el acceso denegado.



## CONCLUSIONES

El sistema de seguridad inteligente denominado como control de acceso que se diseñó para hotel Tuxtla de la GRTSE, es un dispositivo de bajo costo comparado contra los que se encuentran en el mercado, y tomando en cuenta que además de controlar el acceso a dicho edificio también tiene la capacidad de notificar cuando se realicen accesos fuera de horarios establecidos. El principal sensor que se utilizó fue el Lector de huellas AS608 que es el encargado de guardar todas las huellas registradas.

El hecho de que el sistema de seguridad cuente con una página web establecida para su propio uso es de gran importancia y de gran ayuda en caso de que se requiera saber quién fue la última persona en ingresar a las instalaciones o también para saber que medio se utilizó para el ingreso (huella o clave alfanumérica). Sin embargo, cabe aclarar que el montado de la página web sobre el mismo arduino y sin contar con una base de datos externa hace realizar un trabajo extra, así como de uso de mayor memoria dinámica del microcontrolador que como consecuencia puede ocasionar que en algunos casos se sature y congele el mismo arduino. Para corregir este pequeño error se procedió a realizar la activación del WatchDog de nuestra placa para generar un reinicio automático cuando la placa este congelada.

La implementación del protocolo SNMP en conjunto con la plataforma ZABBIX es de gran importancia ya que con esto se permite al ZABBIX realizar un monitoreo constante del dispositivo, y el cual será el encargado de gestionar las notificaciones que se enviarán al personal responsable del área en caso de accesos autorizados o intentos de accesos en horarios no laborales.

El envío de notificaciones vía telegram por medio del ZABBIX representa una gran ventaja ya que no es necesario ingresar a la página para recolectar información de nuestro sistema de seguridad, ya que la plataforma se encarga de estar monitoreando las 24hrs, los 365 días del año, notificando de manera inmediata en cuanto se registran los accesos en horarios no establecidos.

## Bibliografía

Pandora FMS team, S. N. M. P. (2019, 17 julio). Monitorización SNMP: claves del Protocolo Simple de Administración de Red. Recuperado 13 diciembre, 2019, de <https://pandorafms.com/blog/es/monitorizacion-snmp/>

History, A. R. (s.f.). Historia. Recuperado 14 diciembre, 2019, de <https://arduinodhtics.weebly.com/historia.html>

Yralys Sulbaran, O. S. I. m. (1970, 1 enero). Evaluación de los dispositivos a nivel de la capa 2, 3 y 4 del modelo OSI. Recuperado 14 diciembre, 2019, de <https://dialnet.unirioja.es/servlet/articulo?codigo=5157998>

(MLA 8th Edition)

Romeiro, W., and F. Costa. "MONITORAMENTO RESIDENCIAL UTILIZANDO O ZABBIX E O PADRAO IEEE 802.15.4." *Holos*, vol. 2016, no. 1, 2016, p. 253+. Gale OneFile: Informe Académico, Accessed 13 Dec. 2019.

Pereira Varela, Juan Antonio, T. E. L. E. G. R. A. M. chat. (2018, 22 octubre). Aplicación web para el diseño de chatbots de telegram. Recuperado 14 diciembre, 2019, de <https://addi.ehu.es/handle/10810/29205>

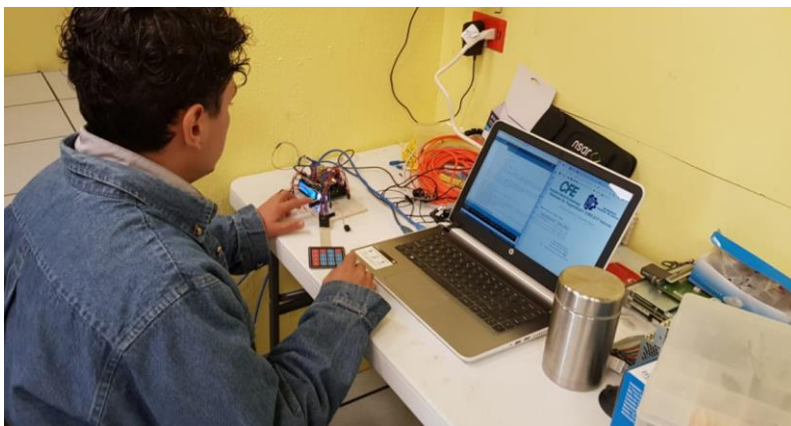
Rosales Briceño Caryuly, S. N. M. P. Monit. (1970, 1 enero). Protocolo snmp (protocolo sencillo de administración de redes). Recuperado 14 diciembre, 2019, de <https://dialnet.unirioja.es/servlet/articulo?codigo=2967489>

Redacción, W. A. T. C. H. D. O. G. AR. (2019, 11 abril). Cómo funciona Watchdog Timer en Arduino. Recuperado 18 diciembre, 2019, de <https://descubrearduino.com/watchdog-timer/>

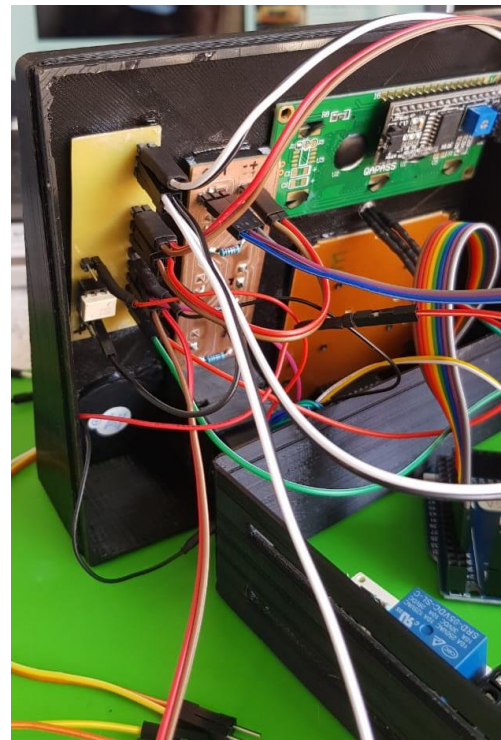
## Anexos

No.	ETAPA	COSTO	BENEFICIO
1	Microprocesador Arduino Mega	\$ 365.00	<ul style="list-style-type: none"> <li>• Aumentar la seguridad del edificio.</li> <li>• Limitar el ingreso al edificio solo trabajadores.</li> <li>• Obtener registros de quienes ingresan capturando hora y fecha exacta.</li> <li>• Recibir notificaciones en tiempo real en caso de violaciones de seguridad o ingresos en horas no laborales vía mensajería de texto Telegram.</li> </ul>
2	Lector biométrico (huellas)	\$550.00	
3	Teclado matricial	\$100.00	
4	Modulo ethernet	\$180.00	
5	Pantalla LCD	\$40.00	
6	Modulo RTC	\$350.00	
7	Modulo Relay	\$28.00	
8	Chapa Magnética	\$700.00*	
9	Buzzer	\$20.00	
10	Caja (Impresión 3D)	\$700.00*	
11	Extras(Cables, botones, estaño, pineras)	\$88.00	
<b>Totales</b>		<b>\$ 3121.00</b>	

*Desarrollo de la interfaz de visualización*



*Montado de componentes físicos*



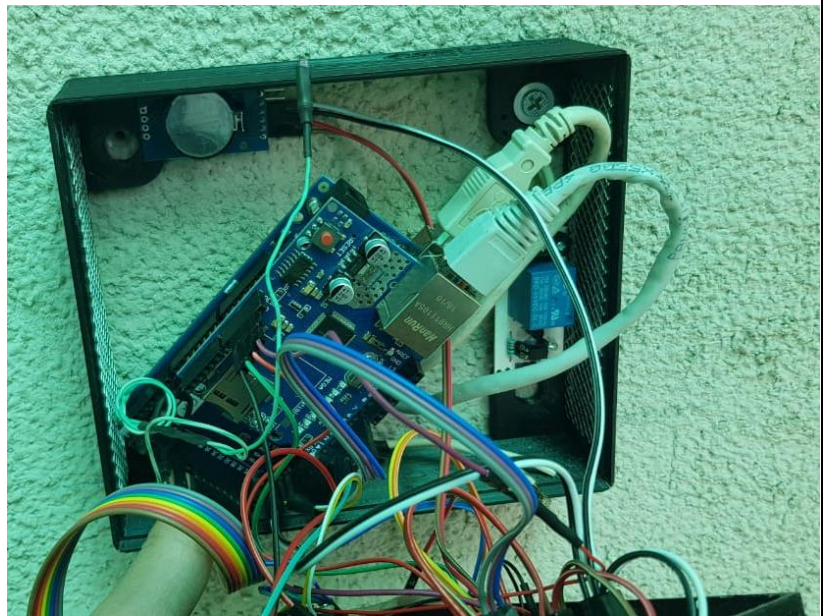
*Prueba para detección de errores y pruebas de la shield ethernet*



*Cableado para próximo empotramiento del dispositivo*



*Empotrado de la base para establecer cableado*



*Fijado de la chapa magnética y pruebas de alimentación*



*Cableado interno para alimentación de la chapa con alimentación respaldada.*



*Fijado final de la chapa magnética*



*Alimentación respaldada con botón de apertura interior*



*Presentación final del control de acceso*



*Pruebas finales y uso diario del control de acceso*



*Pruebas finales y uso diario del control de acceso*

