UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMÁTICA

TESIS DE GRADO

SISTEMA DE SEGURIDAD BASADO EN EL INTERNET DE LAS COSAS PARA VIVIENDAS URBANAS

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMATICA

MENCION: INGENIERIA DE SISTEMAS INFORMATICOS

POSTULANTE: LIZETH CRUZ CACERES

TUTOR METODOLÓGICO: M.SC. ROSA FLORES MORALES

ASESOR: PH. D. YOHONI CUENCA SARZURI

LA PAZ – BOLIVIA

2020

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:
a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.
El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

DEDICATORIA

El presente trabajo va dedicado con mucho cariño a mis padres por el apoyo incondicional que me brindaron en cada momento de mi vida.

AGRADECIMIENTOS

A Dios por permitirme culminar este trabajo, que ha sido una meta desde el principio de esta carrera, también agradecer a mi familia ya que sin su ayuda y comprensión no hubiese sido posible salir adelante.

A mi tutora M.Sc. Rosa Flores Morales y asesor Ph. D. Yohoni Cuencua Sarzuri por su valioso tiempo y apoyo para la culminación de mi Tesis de Grado. Gracias por su colaboración.

Por ultimo quiero agradecer a todos los docentes de la carrera de Informática y también a la "Universidad Mayor de San Andrés", por los años que me cobijo en sus aulas, para adquirir conocimiento y tener una formación profesional.

Contenido

Tablas de figuras

Tablas

RESUMEN

El término del Internet de las Cosas se refiere a la conexión y manejo digital de diversos objetos por medio de dispositivos que hoy en día se aplica en la parte de seguridad de hogares. Actualmente se tienen muchos sistemas de seguridad operando en cuanto a protección de viviendas sobre robos, atentados, etc. La principal limitación de obtener estos sistemas, es el costo que tienen al ser implementados.

La presente investigación propone desarrollar un sistema de seguridad basado en el Internet de las Cosas, con los componentes básicos que debe tener cualquier vivienda de modo que esté protegido y se pueda monitorear desde cualquier ubicación que se encuentre el usuario.

Dentro la investigación se levantó un punto Wifi y se instaló los componentes hardware como: el cerco eléctrico, cámaras de seguridad, sensor PIR, sirena y el levantamiento del servidor web donde está alojada la página web para el control óptimo del sistema.

Se aplicó el método de estudio de casos para probar el funcionamiento del sistema y sus componentes descritos, realizando algunos cambios para obtener el funcionamiento más óptimo del sistema.

Finalmente el trabajo cumple con los requerimientos básicos en cuanto a seguridad de una vivienda integrado en un solo sistema que maneja la parte hardware y software.

Palabras Claves: Internet de las cosas, seguridad de vivienda, cámaras de seguridad, sensor pir, cerco eléctrico.

SUMMARY

The term of the Internet of Things refers to the digital connection and handling of various objects by means of devices that today are applied in the part of home security. Currently there are many security systems operating in terms of home protection against theft, attacks, etc. The main limitation of obtaining these systems is the cost they have when implemented.

This research proposes to develop a security system based on the Internet of Things, with the basic components that any home should have so that it is protected and can be monitored from any location the user is in.

Within the investigation, a Wifi point was built and hardware components were installed such as: the electric fence, security cameras, PIR sensor, siren and the survey of the web server where the web page is hosted for optimal control of the system.

The case study method was applied to test the operation of the system and its described components, making some changes to obtain the most optimal operation of the system.

Finally, the work complies with the basic requirements regarding the security of a dwelling integrated into a single system that handles the hardware and software part.

Key Words: Internet of things, home security, security cameras, pir sensor, electric fence.

CAPITULO I

MARCO REFERENCIAL

CAPITULO I

1. MARCO REFERENCIAL

1.1. INTRODUCCION

Hoy en día las tecnologías de información son cada vez más accesibles para la mayoría de la población. Según el ministro de Obras Publicas Oscar Coca (2018) menciono que el 78% de la población boliviana cuenta con acceso a internet, donde se observa el crecimiento acelerado de Bolivia.

Con el acceso al internet se origina a lo que se le llama el internet de las cosas (IoT). Esta tecnología se encarna en una amplia gama de productos, sistemas y sensores en red, que aprovechan los avances en la potencia del cálculo, la miniaturización de los componentes electrónicos y las interconexiones de red para ofrecer nuevas capacidades, como la seguridad en el hogar (Rose, Eldridge & Chapin,2015).

Según Saúl (2018) el robo a domicilios particulares se escucha a diario, esto crea una inseguridad ciudadana. Los antisociales aprovechan cuando los habitantes del domicilio salen a trabajar o en horas de la noche, instantes donde se producen los robos.

Las zonas muy alejadas de la ciudad no pueden ser socorridas de manera rápida esto debido a que la misma zona no cuenta con muchos pobladores, por lo que se busca medidas de protección más eficaz, de modo que los antisociales no puedan ingresar a la vivienda.

Frente a este problema, el presente proyecto propone diseñar e implementar un sistema para una vivienda implementando cámaras de seguridad que monitoreara las 24 horas del día y sensores de movimiento que detecten, alerten con notificaciones de intrusión, que se empleara cuando esté ausente el hogar y/o cuando este dentro de casa. Con la ayuda del internet de las cosas (IoT) permitirá al usuario tener acceso a la información y control de la vivienda.

En caso de que se pueda evidenciar que antisociales quieran ingresar al domicilio, se podrá controlar desde el aparato móvil (que debe estar en red con el punto WIFI) medidas de

protección como la activación del cerco eléctrico creando una barrera para que no puedan entrar a cometer actos delictivos.

1.2. ANTECEDENTES

La tesis desarrollada por Ramos (2018) titulada “Sistema de control de llave digital con Raspberry PI3”, explica el diseñó de un software para el control de cerradura con llave digital controlada mediante vía web aplicando el internet de las cosas. El producto final efectivamente cumple con lo propuesto aplicando en un prototipo de cerradura.

El trabajo de grado desarrollado por Mahecha (2018) titulada “Diseño e implementación de una aplicación domótica para iluminación usando inteligencia artificial”, explica sobre el diseño de una aplicación domótica usando un controlador con el entorno de inteligencia artificial que será controlado vía WI-FI.

La tesis desarrollada por Condori (2016) titulada “Sistema domotico de seguridad perimetral basado en arduino”, describiendo sobre la implementación de un sistema domótico de seguridad en un prototipo que tiene la funcionalidad de detectar y alertar la intrusión de personas ajenas al hogar a lo largo del perímetro establecido usando el módulo GSM en el que se puede recibir o enviar datos desde un lugar remoto

La tesis desarrollada por Villca (2016) titulada “Sistema de seguridad domiciliaria basada en tecnologia arduino y aplicación movil”, explica el desarrollo de una aplicación móvil con tecnología Bluetooth para el control automatizado del hogar con el uso de servomotores, sensores y otros medios inalámbricos para reducir costos, ofreciendo más comodidad y seguridad en el hogar.

La tesis desarrollada por Aviles y Cobeña (2015) titulada “Diseño e implementación de un sistema de seguridad a través de cámaras, sensores y alarma, monitorizado y controlado telemétricamente para el centro de acogida “Patio mi pana” perteneciente a la fundación proyecto salesiano”, diseña un sistema de seguridad utilizando el microprocesador 18F4550 para el monitoreo del centro de acogida, por medio del módulo GSM, para la comunicación desde el celular hacia el sistema.

La tesis desarrollada por Coarite (2011) titulada “Integración de sistemas domoticos multimedia y comunicacion en el hogar”, explica la implementación de un sistema domotico para el control de dispositivos como sensores, actuadores y cámara web haciendo uso del micro controlador PIC-18F4550 integrando todos los dispositivos en un solo sistema controlado por vía web, aplicado en un prototipo.

La empresa “Control House“, provee al mercado nacional sistema de casas inteligentes, que ofrece seguridad que tiene integrado cámaras de seguridad, alarmas, video porteros, control de acceso y chapas eléctricas. En la parte de automatización se tiene integrado la iluminación, cortinas, riego, climatización, audio/video. Como se muestra es un sistema completo, lo que nos limita a este servicio es el costo de la instalación que abarca entre los precios de 10000 a 15000 dependiendo el grado de complejidad en la parte de seguridad.

1.3. PLANTEAMIENTO DEL PROBLEMA

Los robos en las viviendas son sucesos inesperados que pueden ser impredecible en el momento en que pueda ser víctima de malhechores. Según fuentes policiales (2018), los ladrones prefieren cometer estos robos a horas de la noche, ya que es más probable que los dueños de la propiedad y vecinos estén durmiendo, lo que minimiza el riesgo de ser descubiertos o de que alguien los delate.

Numerosas denuncias reflejan cómo la mayoría de robos a domicilio se pudieron evitar; sin embargo, el descuido y la imprudencia es el principal aliado de los delincuentes, que esperan que las viviendas queden sin ocupantes para ingresar violentando puertas o ventanas y sustraer cuando objeto de valor encuentran en su interior.

Existen zonas de la ciudad, fronterizas con pocas casas habitadas, estos sufren de una inseguridad mayor, en el caso que antisociales estén forcejeando la puerta para entrar a cometer actos delictivos, y esta vivienda no puede ser auxiliada por los vecinos, ni por la policía en el momento preciso.

1.3.1. PROBLEMA CENTRAL

Si bien existe una amplia variedad de sistemas de seguridad en el mercado, estos no actúan de forma física interviniendo el ingreso al domicilio, solo se percata de avisar al dueño a través de la alarma antirrobo y/o mensajes, cuando antisociales traten de ingresar a la vivienda.

1.3.2. PROBLEMAS ESPECÍFICOS

- No se puede monitorear la vivienda en tiempo real desde cualquier instancia que se encuentren los dueños.
- Inseguridad y falta de tranquilidad en los dueños al dejar la vivienda ausente.
- Falta de un sistema que controle, y tome acción en el caso que antisociales estén intentando entrar a la vivienda.

1.4. DEFINICION DE OBJETIVOS

1.4.1. OBJETIVO GENERAL

Desarrollar un sistema de seguridad basado en el internet de la cosas para el resguardo de viviendas urbanas con medidas de protección.

1.4.2. OBJETIVO ESPECÍFICO

- Implementar cámaras de seguridad en lugares estratégicos de la vivienda.
- Implementar sensor de movimiento en la parte exterior de la vivienda.
- Construir una placa de circuito electrónico para la comunicación de las cámaras, del cerco eléctrico y los focos.
- Implementar el cerco eléctrico encima del muro de la vivienda donde este transmitirá corriente, y se activara por el dueño en el caso que la vivienda lo deje ausente, y en las noches.
- Implementar el prendido de luces de la vivienda de modo que no se note la ausencia de los dueños.
- Desarrollar e implementar un sistema web, para el control de todos componentes ya mencionados en caso de detección de intrusión.

1.5. JUSTIFICACIÓN

1.5.1. JUSTIFICACIÓN SOCIAL

El presente trabajo tiene un impacto social asociado, puesto que propone una herramienta con la capacidad de solucionar necesidades en cuanto a la seguridad del hogar.

Así mismo el usuario tendrá la facilidad y la tranquilidad que cuenta con un sistema de seguridad que puede ser monitoreado desde cualquier instancia en la que se encuentre.

El sistema se podrá manipular de forma sencilla para el usuario, siempre precautelando la seguridad del hogar y de la misma manera del sistema que controlara.

1.5.2. JUSTIFICACIÓN ECONOMICA

En la actualidad, no muchos ciudadanos cuentan con un sistema de seguridad en su vivienda ya sea por los altos costos que abarca entre los precios de 12000 Bs que varía de acuerdo a la calidad y beneficios, por ello el sistema de seguridad que se realizara, permitirá

fortalecer la seguridad en la vivienda permitiendo tener el control a larga distancia siempre y cuando se tenga acceso al internet.

El costo de los componentes que se utilizará en la implementación del sistema ira variando de acuerdo a la calidad y beneficios. Entre los materiales solo se utilizara los más importantes que se requiere en cuanto a la seguridad, como ser: sirena, sensor de movimiento, cámara y otros.

Precautelando de que sean los materiales más necesarios a fin de que el sistema no tenga un costo elevado.

1.5.3. JUSTIFICACIÓN TECNOLOGICA

La solución que se propone es aplicar el uso de la tecnología web que es una herramienta del internet de las cosas para adaptarlas a las necesidades que se tiene en cuanto a la seguridad del hogar.

El internet de las cosas se refiere a la interconexión y la interacción de lo digital y el mundo físico, en el que gracias a la tecnología se podra integrar cosas físicas a las redes de información a través de infraestructuras del internet.

En los últimos años unos 4.000 millones de dispositivos se han conectado a Internet según un estudio realizado por la compañía Cisco, como se puede ver hay bastante pobladores que tienen acceso al internet y que mejor aplicando la tecnología del IoT que nos ayudara en nuestro diario vivir.

1.5.4. JUSTIFICACIÓN TEORICA

Con la presente investigación, se podrá aportar con un granito de arena sobre el amplio tema que es del Internet de las Cosas y sus aplicaciones en la vida real.

El proyecto permitirá comprobar sus aplicaciones que se pueden realizar aplicando el internet de las cosas, además brindara información a estudiantes que se están formando profesionalmente en el área de la tecnología.

Gracias a estos proyectos que se realizan, de alguna manera nos ayuda a aprender un poco más y mantenernos actualizados; característica que es fundamental para la carrera, más que todo en el campo laboral.

1.6. LÍMITES Y/O ALCANCES

1.6.1. LÍMITES

El presente sistema de seguridad de control externo para una vivienda no contempla un sistema completo de seguridad, sus limitaciones se muestra a continuación:

- El sistema trabajará independientemente, solo con usuarios configurados.
- No se aplica en caso de incendios.
- El sistema solo brindara funciones principales para la seguridad de la vivienda.
- El sistema solo trabajará con dispositivos que estén conectados al Wifi.

1.6.2. ALCANCES

La implementación del sistema, propuestas por la presente tesis se realizaran de acuerdo a las siguientes consideraciones:

- Se instalara el sistema de seguridad en una vivienda real.
- Se elaborará las pruebas necesarias del funcionamiento del sistema.
- Cada usuario que manipulara el sistema tendrá una contraseña para el acceso al sistema.
- El usuario tendrá control de los componentes del sistema en tiempo real.

1.7. DISEÑO METODOLOGICO

Para la ejecución del presente proyecto, se empleara el método inductivo, el cual utiliza premisas particulares para llegar a una conclusión general. La prueba se realizara en una vivienda.

Según Perez & Merino (2008) el método inductivo es un método científico que pueden distinguirse en cuatro pasos esenciales:

1. La observación de los hechos para su registro.
2. La clasificación y el estudio de estos hechos.
3. La derivación inductiva que parte de los hechos y permite llegar a una generalización.
4. La contrastación.

Para la parte de desarrollo, en la elaboración del presente trabajo se utilizara el Modelo en V o de cuatro niveles. El modelo en V es un proceso que representa la secuencia de pasos en el desarrollo del ciclo de vida de un proyecto. Describe las actividades y resultados que han de ser producidos durante el desarrollo del producto. La parte izquierda del modelo en V representa la descomposición de los requisitos y la creación de las especificaciones del sistema. El lado derecho de la metodología en V representa la integración de partes y su verificación (Inteco, 2009).

CAPITULO II
MARCO TEORICO

CAPITULO II

2. MARCO TEORICO

2.1. INTRODUCCION

En el presente capitulo se aborda conceptos teóricos sobre seguridad de un hogar, herramientas que se emplean en hardware y software del sistema, la metodología para llevar a cabo el proyecto.

2.2. SEGURIDAD EN EL HOGAR

Según Simón (2018), cuando se habla de seguridad en el hogar se piensa en sistemas anti intrusión, en mecanismos que prevengan sufrir actos vandálicos, robos y otros percances procedentes principalmente del exterior. Se debe tener en cuenta estos asuntos, y considerar las amenazas que provienen del interior y que pueden poner en riesgo tanto a personas como a infraestructuras, bienes y componentes de cualquier vivienda, especialmente durante la ausencia del dueño.

2.3. INTERNET DE LAS COSAS

El Internet de las Cosas es una traducción de la expresión en inglés *Internet of Things (IoT),* que describe un escenario en el que diversas cosas están conectadas y se comunican. Esa innovación tecnológica tiene como objetivo conectar los ítems que se usa diariamente a internet, con el objetivo de aproximar cada vez más el mundo físico al digital (Valois, 2018).

2.3.1. Funcionamiento del IOT

Según Valois (2018), el Internet de las Cosas trata de objetos conectados entre sí por medio de la red como se muestra en la **figura 2.1**. Estos intercambian información para facilitar o crear diversas acciones, son tres factores que necesita ser combinados para que una aplicación funcione dentro del concepto de Internet de las Cosas:

- **Los Dispositivos:** Son aquellos que se conoce, como: refrigeradores, carros, lamparas, relojes, cafeteras, televisión y otros. En estos dispositivos es importante que sean equipados con los items correctos para proporcionar la comunicación con los demás elementos. Esos límites pueden ser chips, conexión con internet, sensores, antenas entre otros.
- **La Red:** Es el medio de comunicación, como Wi-Fi, Bluetooth y datos móviles (3G y 4G).
- **El sistema de control:** Es necesario que todos los datos capturados de los dispositivos a través de la red sean procesados, y enviados para un sistema que controla cada aspecto y hace nuevas conexiones.

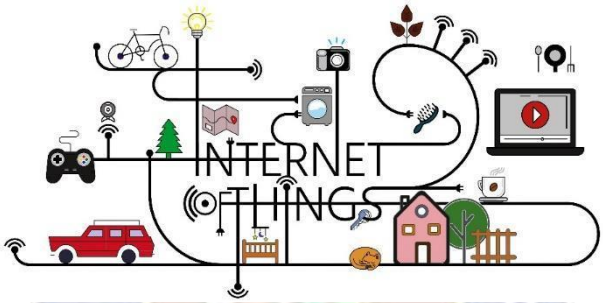


Tabla 2.1. Conexión de objetos mediante red

Fuente: (iUrban, s.f.)

2.4. HERRAMIENTAS DEL SISTEMA

Las herramientas que se emplean en el proyecto se las describe de forma independiente con sus características correspondientes.

2.4.1. ARDUINO UNO

Es una plataforma de creación de electrónica de código abierto, la cual está basada en hardware y software libre, flexible y fácil de utilizar para los creadores y desarrolladores. Esta plataforma permite crear diferentes tipos de microordenadores de una sola placa a los que la comunidad de creadores puede darles diferentes tipos de uso (Yubal, 2018).

2.4.1.1. Características

Se presenta cada una de las características que posee la placa Arduino, que debe ser revisado previo antes de implementar en el armado de la placa, de la siguiente manera:

- Micro controlador: ATmega328
- Voltaje Operativo: *5v*
- Voltaje de Entrada (Recomendado): *7 – 12 v*
- Pines de Entradas/Salidas Digital: 14 (De las cuales 6 son salidas PWM)
- Pines de Entradas Análogas: 6
- Memoria Flash: 32 KB (ATmega328) de los cuales 0,5 KB es usado por Bootloader.
- SRAM: 2 KB (ATmega328)
- EEPROM: 1 KB (ATmega328)
- Velocidad del Reloj: 16 MHZ.

2.4.1.2. Partes

Según Instructables (2020) las partes del Arduino se conforman de la siguiente manera (ver **figura 2.2.**):

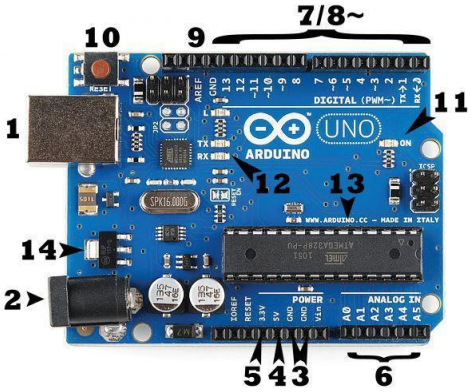


Tabla 2.2. Partes de la placa Arduino
Fuente: (Instructables, 2020)

- **Potencia - USB (1) / Conector de Adaptador (2)**

  Cada placa Arduino necesita una forma de estar alimentado eléctricamente, esta puede ser alimentada desde un cable USB que viene del ordenador o un cable de corriente eléctrica con su respectivo adaptador. La conexión USB va a cargar el código en su placa Arduino.

- **Pines (5V, 3.3V, GND, Analog, Digital, PWM, AREF)**

  Los pines en la placa Arduino es donde se conectan los cables de un circuito. El Arduino tiene varios tipos de entradas, cada uno de las cuales está marcado en el tablero y utilizan para diferentes funciones:

  • **GND (3):** Abreviatura de "tierra" (en Ingles). Hay varios pines GND en el Arduino, cualquiera de los cuales pueden ser utilizados para la conexion a tierra el circuito.

  • **5V (4)** y **3.3V (5):** Son los suministros pin 5V 5 voltios de energía, y los suministros de pin 3.3V 3.3 voltios de potencia.

  • **Analógico (6):** El área de pines en el marco del 'analógica' etiqueta (A0 a A5) son analógicas. Estos pines pueden leer la señal de un sensor analógico (como un sensor de temperatura) y convertirlo en un valor digital que se puede leer.

  • **Digital (7):** Son los pines digitales (del 0 al 13). Estos pines se pueden utilizar tanto para la entrada digital (si se oprime un botón) y salida digital (como encender un LED).

  • **PWM (8):** La tilde (~) situado al lado de algunos de los pines digitales (3, 5, 6, 9, 10 y 11), actúan como pines digitales normales.

  • **AREF (9):** Soportes de referencia analógica. La mayoría de las veces se puede dejar este pin solo, tambien se utiliza para establecer una tensión de referencia externa (entre 0 y 5 voltios) como el límite superior para los pines de entrada analógica.

- **Botón de reinicio (10)**

  Empujando el botón se conecta temporalmente el pin de reset a tierra y reinicia cualquier código que se carga en el Arduino.

- **Indicador LED de alimentación (11)**

  Este LED debe encenderse cada vez que conecte la placa Arduino a una toma eléctrica.

- **LEDs RX TX (12)**

  TX es la abreviatura de transmisión, RX es la abreviatura de recibir. Estas marcas indican los pasadores responsables de la comunicación en serie.

  Microcontrolador (13)

  Es el cerebro que controla el Arduino.

- **Regulador de Voltaje (14)**

  El regulador de voltaje controla la cantidad de tensión que se deja en la placa Arduino.

2.4.2. SHIELD ETHERNET 5100

El shield permite conectar el Arduino a Internet, está basado en el chip de ethernet Wiznet W5100 con funcionalidades de IP tanto para TCP como UDP. El Arduino Ethernet Shield soporta hasta 4 conexiones simultáneas, usa la librería Ethernet para escribir programas que se conecten a internet usando la shield (AV Electronics, 2020).

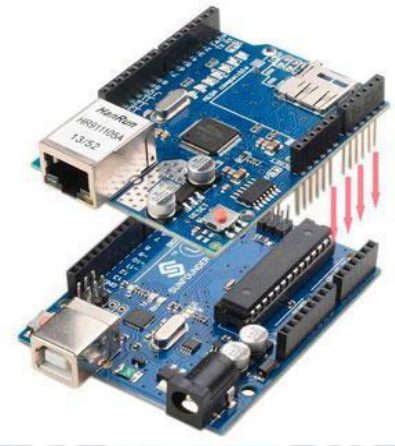


Tabla 2.3. Esquema de montaje de la placa shield al Arduino

Fuente: (luisllamas, 2020)

2.4.2.1. Componentes

Los componentes que posee la placa Shield Ethernet se las detalla a continuación:

- El shield proporciona un estándar de conector RJ45 Ethernet
- El botón de reinicio en el shield reinicia al W5100 y la placa Arduino
- El escudo contiene una serie de LEDs de información:
- **PWR**: indica que la placa y el shield son alimentados
- **LINK**: indica la presencia de un enlace de red y parpadea cuando el shield transmite o recibe datos
- **FULLD**: indica que la conexión de red dúplex está completo
- **100M**: indica la presencia de una conexión de red a 100 Mb / s
- **RX**: parpadea cuando el shield recibe datos
- **TX**: parpadea cuando el shield envía datos
- **COLL**: parpadea cuando se detectan colisiones de red

2.4.3. SENSOR INFRARROJOS (PIR)

Según (Ferrer, 2019) un sensor de movimiento es un dispositivo generalmente pensado para detectar la presencia de personas dentro de un entorno determinado. Por esta razón, estos sensores se utilizan mucho en sistemas de alarma y antirrobo, debido a que generan barreras que, cuando son cruzadas por una persona, activan la alarma. **(Figura 2.4.)**

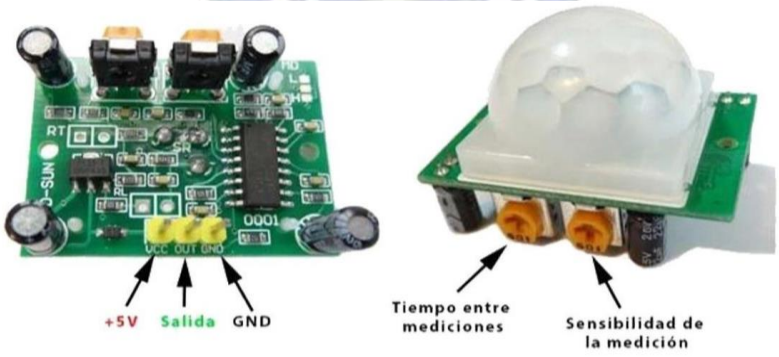


Tabla 2.4. Partes del sensor PIR

Fuente: (zonamaker.com, 2014)

2.4.3.1. Características

En el siguiente apartado se observa las características del sensor PIR.

- Sensor piroeléctrico (Pasivo) infrarrojo (También llamado PIR)
- El módulo incluye el sensor, lente, controlador PIR BISS0001, regulador y todos los componentes de apoyo para una fácil utilización
- Rango de detección: 3 m a 7 m, ajustable mediante trimmer (Sx)
- Lente fresnel de 19 zonas, ángulo < 100º
- Salida activa alta a 3.3 V
- Tiempo en estado activo de la salida configurable mediante trimmer (Tx)
- Redisparo configurable mediante jumper de soldadura

- Consumo de corriente en reposo: < 50 µA
- Voltaje de alimentación: 4.5 VDC a 20 VDC

2.4.4. SIRENA DE ALARMA

Según la página web (securitasdirect, 2018) una sirena de alarma es un dispositivo disuasorio que emite un potente aviso sonoro cuando se produce un salto de alarma por una posible intrusión. Su objetivo es disuadir al posible ladrón y alertar a los propietarios del hogar o negocio afectado. **(Figura 2.5.)**

Tabla 2.5. Sirena para alarma

Fuente: (tvc, 2019)

2.4.5. CAMARAS DE SEGURIDAD

Las cámaras de seguridad o vigilancia constituyen un sistema de seguridad que consiste en realizar vigilancia a través de cámaras de video en diferentes lugares o ambientes. Esta tecnología de video vigilancia es útil para identificar intrusos o cualquier persona que realice alguna actividad indebida que ponga en riesgo la integridad de un lugar o individuo (Ferrer, 2019).

2.4.6. CERCO ELECTRICO

Según la página web (electronicsolutions, 2019) el cerco eléctrico es una herramienta de seguridad que se coloca en un perímetro determinado para proteger personas o instalaciones. También se le conoce con el nombre de valla electrificada. Consiste en la colocación de un alambrado conectado a un generador de alto voltaje para evitar el ingreso inapropiado de personas a través de él. **(Figura 2.6.)**

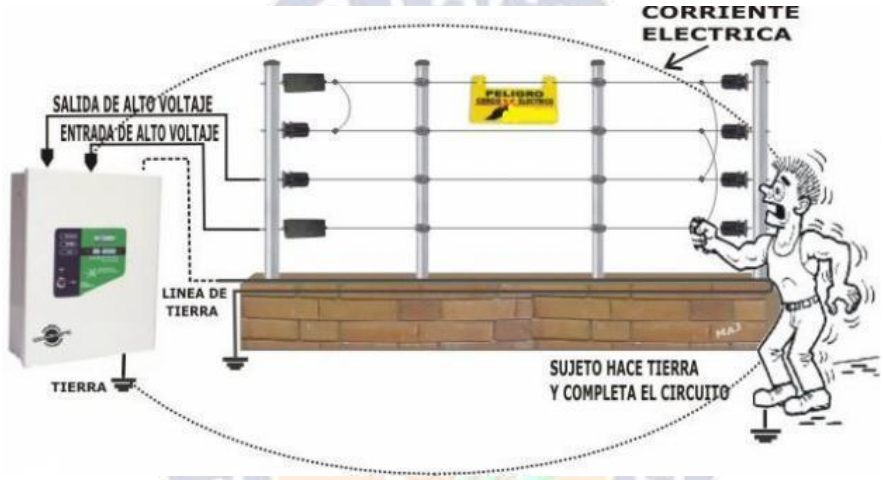


Tabla 2.6. Cerco eléctrico

Fuente: (electronicsolutions, 2019)

2.4.6.1. Partes del Cerco Eléctrico

Los componentes que son necesarios para la instalación del cerco eléctrico, tomando las precauciones necesarias para su instalación, son:

- Postes templadores
- Postes intermedios
- Alambre de acero
- Batería de reserva
- Aisladores
- Electrificador(Energizador)
- Sensores de flexion
- Argollas de caída de voltaje

- Sirena o alarma
- Letrero de advertencia
- Control de encendido/apagado que puede ser con un pulsador fijo o inalámbrico.

2.4.7. MODULO DC DC

El convertidor de voltaje DC-DC Step-Down 3A LM2596 tiene como función entregar un voltaje de salida constante inferior al voltaje de entrada frente a variaciones del voltaje de entrada o de carga. Soporta corrientes de salida de hasta 3A, voltaje de entrada entre 4.5V a 40V y voltaje de salida entre 1.23V a 37V. El voltaje de salida se selecciona mediante un potenciómetro multivuelta (NaylampMechatronics, s.f.).

2.5. HERRAMIENTAS SOFTWARE

2.5.1. PHP V7.3.9

Es un lenguaje de programación del lado del servidor gratuito e independiente de plataforma, rápido, con una gran librería de funciones y mucha documentación. Un lenguaje del lado del servidor es aquel que se ejecuta en el servidor web, justo antes de que se envíe la página a través de Internet al cliente. Las páginas que se ejecutan en el servidor pueden realizar accesos a bases de datos, conexiones en red, y otras tareas para crear la página final que verá el cliente. El cliente solamente recibe una página con el código HTML resultante de la ejecución de la PHP. Como la página resultante contiene únicamente código HTML, es compatible con todos los navegadores (desarrolloweb6, 2001).

2.5.2. XAMPP v3.2.4

XAMPP es un paquete formado por un servidor web Apache, una base de datos MySQL y los intérpretes para los lenguajes PHP y Perl, X (para cualquier sistema operativo), A (Apache), M (MySQL), P (PHP) y P (Perl) (Velasquez, 2011).

2.5.3. MYSQL v4.9.0.1

MySQL es un sistema de gestión de bases de datos relacionales de código abierto (RDBMS, por sus siglas en inglés) con un modelo cliente-servidor. RDBMS es un software o servicio utilizado para crear y administrar bases de datos basadas en un modelo relacional (B, 2019).

2.5.4. CODE IGNITER v3.1.10

Code Igniter es un framework PHP (Ionos, 2017) para la creación rápida de aplicaciones web. El diseño orientado al rendimiento de este framework de desarrollo web se revela en su parca arquitectura, pues se basa en el patrón Modelo-Vista-Controlador (MVC). El principio fundamental que sustenta a la arquitectura de desarrollo MVC es la estricta separación entre el código y la presentación, gracias a una estructura modular de software y a la externalización del código PHP. Esta separación se realiza en estos tres grupos: el modelo (model), la vista (view) y el controlador (controller), que se explica a continuación:

- **El modelo** representa la estructura de datos de una aplicación web desarrollada con Code Igniter, donde se definen las denominadas clases ("model classes") que contienen funciones especiales con las cuales se puede recibir, insertar o actualizar la información de la base de datos.

- **La vista** es aquello que se le presenta al usuario final. Por lo general, se trata de un documento HTML en el cual se ha insertado contenido de forma dinámica con PHP, convirtiéndose en una especie de plantilla. Code Igniter también permite definir fragmentos de una página web como la cabecera y el pie de página o páginas RSS como vista. Normalmente las aplicaciones web utilizan varias vistas, que toman su contenido desde el mismo modelo, de tal forma que es posible presentar diversas características del programa en vistas diferentes.

- **El controlador** media entre el modelo, la vista y cualquier otro recurso necesario para procesar una petición HTTP o generar una página web de forma dinámica. Este componente recibe las peticiones entrantes, valida la entrada,

selecciona la vista deseada y le entrega el contenido que el modelo ha cargado desde una base de datos.

2.5.5. BOOTSTRAP v3.3.7

Es un potente framework de CSS que fue creado por Twitter para simplificar el proceso de maquetación web responsive. Sin obtener grandes conocimientos en CSS, con esta herramienta se puede empezar a maquetar un sitio web adaptable a todo tipo de dispositivos (Esfera Creativa, 2019).

2.6. INGENIERIA DE SOFTWARE

La ingeniería del software en la web es la aplicación de metodologías sistemáticas, disciplinadas y cuantificables al desarrollo eficiente, operación y evolución de aplicaciones de alta calidad (isoftware, 2011)

2.6.1. METODOLOGIA EN V

Es una variación del modelo en cascada que muestra cómo se relacionan las actividades de prueba con el análisis y diseño. La letra V hace referencia a: verificación y validación.

2.6.1.1. Importancia

Según (Rodriguez, 2008) trata de un proceso ideal, por su robustez, para proyectos pequeños, con equipos de una a cinco personas. También es ideal, por su claridad, para toda esa gente que nunca ha programado siguiendo una metodología **(Figura 2.8.)**

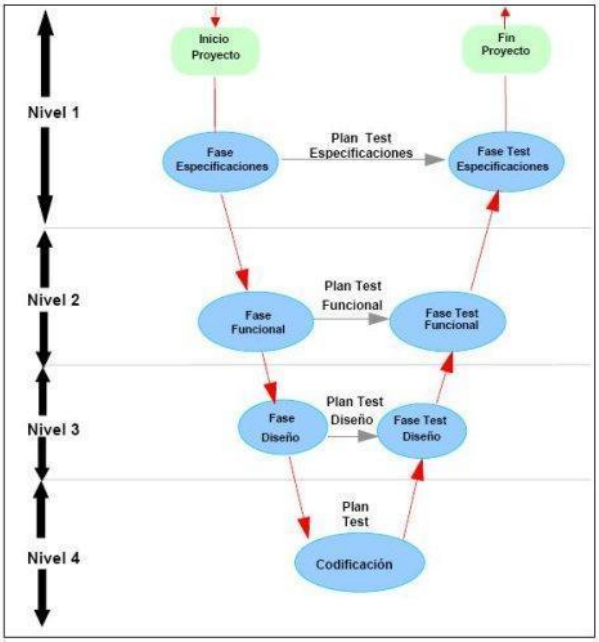


Tabla 2.7. Modelo de cuatro niveles

Fuente: (Rodriguez, 2008)

El nivel 1 está orientado al "cliente". El inicio del proyecto y el fin del proyecto constituyen los dos extremos del ciclo. Se compone del análisis de requisitos y especificaciones, se traduce en un documento de requisitos y especificaciones.

El nivel 2 se dedica a las características funcionales del sistema propuesto. Puede considerarse el sistema como una caja negra, y caracterizarla únicamente con aquellas funciones que son directa o indirectamente visibles por el usuario final, se traduce en un documento de análisis funcional.

El nivel 3 define los componentes hardware y software del sistema final, a cuyo conjunto se denomina arquitectura del sistema.

El nivel 4 es la fase de implementación, en la que se desarrollan los elementos unitarios o módulos del programa (Rodriguez, 2008).

2.6.1.2. Ventajas

- Es un modelo sencillo y fácil de aprender.
- La relación entre las etapas de desarrollo y los distintos tipos de pruebas facilitan la localización de fallos.
- Especifica bien los roles de los distintos tipos de prueba a realizar.
- Involucra al usuario en las pruebas.

2.6.1.3. Desventajas

- Las pruebas pueden ser caras y, a veces, no lo suficientemente efectivas
- El producto final obtenido puede que no refleje todos los requisitos del usuario.
- No se puede repetir la secuencia de pasos si este no sale bien. Se debe realizar nuevamente todo el proceso de validación y verificación.

CAPITULO III
MARCO APLICATIVO

CAPITULO III

3. MARCO APLICATIVO

3.1. INTRODUCCIÓN

En el siguiente capítulo se realiza el diseño y desarrollo de la parte hardware, software para la implementación del proyecto sobre la plataforma de Arduino, siguiendo cada una de las etapas de la metodología en V.

3.2. DESARROLLO DE LA METODOLOGÍA EN V

3.2.1. FASE 1: DEFINICIÓN DE ESPECIFICACIONES

Especificaciones del software

Se define las especificaciones del sistema, tomando en cuenta los siguientes puntos como requerimientos principales.

- El usuario debe loguearse en la página web.
- El sistema otorga permiso de acuerdo al rol de usuario que está autentificando.
- El sensor debe enviar datos a la base de datos, cada vez que haya captado intrusos cerca del sensor.
- La página web debe realizar él envió de una alerta al correo de todos los usuarios registrados en el sistema.
- El usuario podrá revisar la cámara de seguridad desde la página web.
- El usuario debe controlar y tomar medidas necesarias en caso de la detección de ladrones como el prendido de luces.
- El administrador podrá revisar el historial del sensor de movimiento.
- El administrador debe poder revisar el historial de todos los usuarios registrados en el sistema.

- El administrador podrá editar los permisos para los usuarios registrados en el sistema.

Especificaciones del hardware

Se define las especificaciones de la parte hardware, tomando en cuenta los siguientes puntos como requerimientos principales.

- La sirena, el cerco y las luces debe estar conectado para cualquier momento que se lo quiera manipular.
- Las cámaras de seguridad debe estar funcionando las 24 horas del día.

Diagrama De Casos De Uso

Se define los requisitos potenciales del funcionamiento del sistema según a los requerimientos planteados por el usuario en la **figura 3.1.**

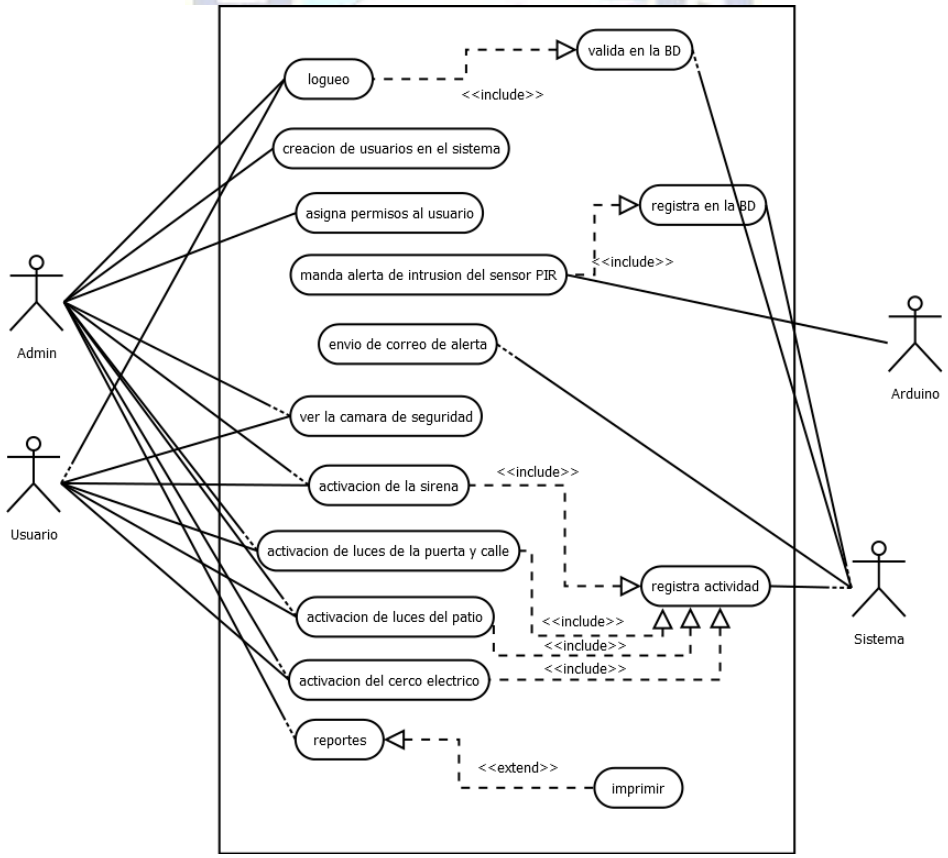


Figura 3.1. Especificación de la funcionalidad del sistema.

El usuario debe estar registrado para tener acceso a la página del sistema que se muestra en la **tabla 3.1.**

Tabla 3.1. Caso de uso, Logueo para el inicio de sesión

Caso de uso #1	Logueo
Descripción	El administrador y/o el usuario inicia sesión introduciendo su nombre de usuario y password para el ingreso del sistema.
Precondición	Debe estar en red y estar registrado en el sistema.
Actores	Admin, usuario
Condición de fracaso	Mandar datos erróneos y/o no estar registrado en el sistema
Condición de éxito	Inicio de sesión satisfactoriamente.

Creación de usuarios y asignación de roles para el ingreso al sistema en la **tabla 3.2**

Tabla 3.2. Caso de uso, Creación de usuarios en el sistema

Caso de uso # 2	Creación de usuarios en el sistema
Descripción	El administrador realiza la creación de usuarios y asignación de rol, para el ingreso del sistema, bajo las contraseñas asignadas por el administrador.
Precondición	Inicio de sesión en el sistema, y tener el rol de administrador.
Actores	Admin,

Condición de fracaso	Mandar datos invalidos al sistema
Condición de éxito	Creación de usuarios satisfactoriamente

El administrador asigna permiso al rol de usuario sobre cada módulo del sistema en la **tabla 3.3.**

Tabla 3.3. Caso de uso, Asignación de permisos a los usuarios creados.

Caso de uso # 3	Asignación de permisos a los usuarios creados.
Descripción	El administrador asigna permisos al usuario para crear, editar y borrar datos del sistema.
Precondición	Inicio de sesión en el sistema, y tener el rol de administrador.
Actores	Admin,
Condición de fracaso	Mandar datos inválidos al sistema
Condición de éxito	Asignación de permisos satisfactoriamente

Envió de datos del sensor PIR a la Base de Datos del sistema, cada que detecte intrusión cerca del hogar en la **figura 3.4.**

Tabla 3.4. Caso de uso, Envió de alerta de intrusión del sensor PIR a la BD

Caso de uso # 4	Envió de alerta de intrusión del sensor PIR a la BD.
Descripción	El sensor PIR manda alerta al sistema en caso que haya detectado intrusión cerca de la vivienda, registrando en la BD.

Precondición	Encendido del WIFI y de la placa que controla el sensor PIR, para él envió de datos a la BD. Además debe estar en red el sistema con la placa
Actores	Arduino
Condición de fracaso	Fallo de red del sistema con la placa
Condición de éxito	Envió de datos al sistema del sensor PIR satisfactoriamente a la BD.

Envió de correo electrónico a usuarios registrados en el sistema, la alerta de intrusión que se observa en la **tabla 3.5.**

Tabla 3.5. Caso de uso, Envió de alerta de intrusión a través del correo electrónico

Caso de uso # 5	Envió de alerta de intrusión a través del correo electrónico
Descripción	El sistema realiza el envió de alerta de intrusión a través del correo electrónico a todos los usuarios registrados en el sistema.
Precondición	Estar en red con el sistema.
Actores	Sistema
Condición de fracaso	No contar en red
Condición de éxito	Envio correo de alerta a los usuarios activos satisfactoriamente

Todo usuario registrado en el sistema podrá revisar las cámaras de seguridad como se describe en la **tabla 3.6.**

Tabla 3.6. Caso de uso, Revisión la cámaras de seguridad

Caso de uso # 6	Revisión de cámaras de seguridad
Descripción	Revisión de cámaras de seguridad para verificar si hubiera intrusos cerca del área.
Precondición	Todo usuario registrado y cuente con permiso de ver la cámara de seguridad.
Actores	Admin, Usuario
Condición de fracaso	Fallo de red entre la cámara con el router.
Condición de éxito	Ver la cámara de seguridad con éxito.

La sirena se activa de forma automática cuando sufre un corte el alambre tesado en el cerco eléctrico que se detalla en la **tabla 3.7.**

Tabla 3.7. Caso de uso, Activación de la sirena

Caso de uso # 7	Activación de la sirena
Descripción	Activación de la sirena para alarmar al antisocial si en caso lo fuera.
Precondición	Sufrimiento de un corte del alambre galvanizado tesado en el cerco eléctrico.
Actores	Admin, Usuario
Condición de fracaso	Fallo de red, no sufrir ningún corte de cable
Condición de éxito	Activación de la sirena con éxito.

Prendido de luces de la puerta principal de forma automática a través del sensor PIR que se observa en la **tabla 3.8.**

Tabla 3.8. Caso de uso, Activación de luces en la puerta principal

Caso de uso # 8	Activación de luces en la puerta principal
Descripción	Activación de luces en la puerta principal para alarmar al antisocial si en caso lo fuera.
Precondición	Todo usuario registrado que cuente con el permiso de activación de luces de la puerta principal.
Actores	Admin, Usuario
Condición de fracaso	Fallo de conexion el foco con la placa y/o estar en red con el router.
Condición de éxito	Activación de luces con éxito.

Prendido de luces del patio de forma manual a través de la página del sistema que se describe en la **tabla 3.9.**

Tabla 3.9. Caso de uso, Activación de luces del patio

Caso de uso # 9	Activación de luces del patio
Descripción	Activación de luces del patio para de alguna manera alarmar al antisocial (noche).
Precondición	Todo usuario registrado en el sistema, con el permiso de activación de luz del patio.
Actores	Admin, Usuario

Condición de fracaso	Fallo de conexión de luces con la placa y/o no estar en red con el Wifi.
Condición de éxito	Activación de luces con éxito.

Activación del cerco eléctrico a través de la página del sistema que se observa en la **figura 3.10.**

Tabla 3.10. Caso de uso, Activación del cerco eléctrico

Caso de uso # 10	Activación del cerco eléctrico
Descripción	Activación del cerco eléctrico para alarmar al antisocial si en caso lo fuera.
Precondición	Todo usuario registrado en el sistema y que cuente con el permiso de activación del cerco eléctrico.
Actores	Admin, Usuario
Condición de fracaso	Fallo de conexión del cerco con la placa y/o estar en red con el router
Condición de éxito	Activación de luces con éxito.

Generación de reportes en formato pdf que se observa en la **tabla 3.11.**

Tabla 3.11. Caso de uso, Generación de reportes

Caso de uso # 11	Reportes
Descripción	Generar reportes del historial del sensor PIR
Precondición	Autentificado como administrador
Actores	Admin

Condición de fracaso	No contar con el rol de administrador.
Condición de éxito	Generación de reportes exitosamente.

Para la implementación del sistema en una vivienda urbana, se emplea diversas herramientas hardware, el cual se describe cada uno de los componentes a utilizar y su costo unitario en la **tabla 3.12.**

Tabla 3.12. Componentes hardware utilizados para el sistema

Cant.	Imagen	Nombre	Voltaje	Precio(Bs.)
1		Arduino		**60**
1		Shield Ethernet	**6 V**	**70**
1		Sensor PIR		**20**
1		Módulo DC – DC	**5 V**	**20**
1		Fuente de poder	12v – 5A	**65**
2		Enchufes		**10**

2		Focos ahorrador		**15**
1		Sirena	12V	**68**
1		Router		**200**
1		Cable de red RJ45		**20**
4		KIT Cámaras de seguridad DAHUA		**600**
1		Electrificador JFL		**320**
1		Alambre galvanizado		**96**
1		Aislador para cerca eléctrica		**60**

1		Rollo de cable de alta tensión		**65**
1		Cartel de aviso de cerca eléctrica		**4**
Total costo				**1693**

3.2.2. FASE 2: DISEÑO GLOBAL

El diseño para el sistema de seguridad, se basa en la comunicación de software y hardware con la conexión de aparatos electrónicos, como ser: Arduino, Shield Ethernet, Electrificador del cerco eléctrico, sirena, como se observa en la **(Figura 3.2.)**

Tabla 3.2. Conexión del sistema con los componentes.

3.2.3. FASE 3: ARQUITECTURA DEL SOFTWARE

Diseño del software

Para el diseño del prototipo del sistema se hace uso de la herramienta Balsamiq Mockup para el entorno grafico del sistema.

Autentificación del usuario, para el ingreso del menú principal de la página web del sistema. **(Figura 3.3)**

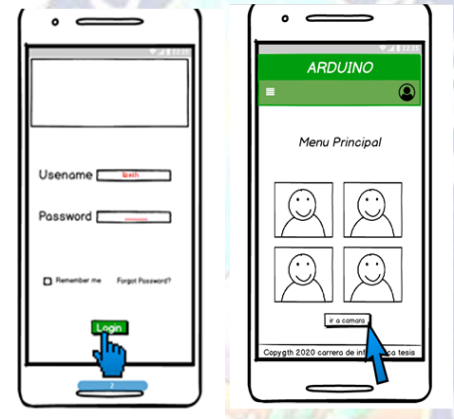


Tabla 3.3. Autentificación del usuario

El control de componentes hardware como: la sirena, cerco eléctrico y focos; son efectuados por el usuario como se observa en la **Figura 3.4.**

Tabla 3.4. Control del hardware del sistema

Registro en la base de datos, cada que el sensor PIR mande datos de intrusión cerca del área, brindando una tabla con descripción y una gráfica. **(Figura 3.5.)**

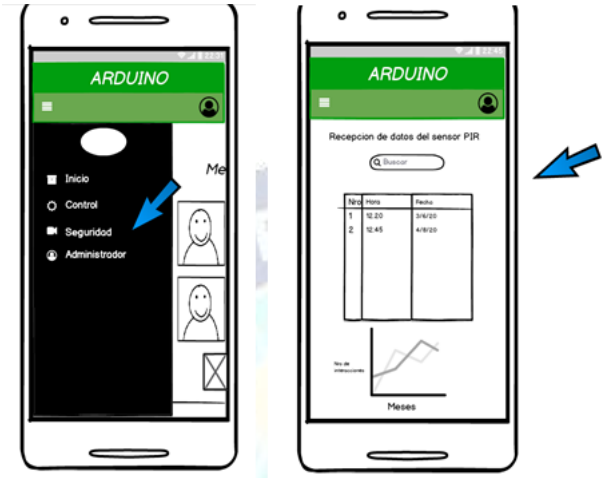


Tabla 3.5. Registro en la BD datos del sensor PIR

Listado de usuarios registrados en el sistema con su respectivo rol e información personal. **(Figura 3.6)**

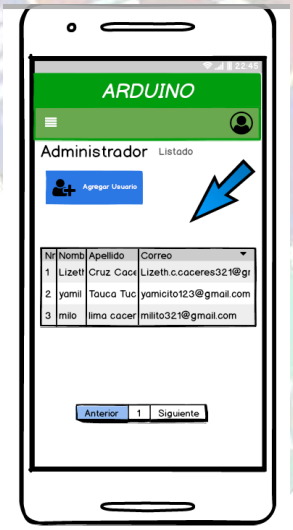


Tabla 2.6. Listado de usuarios

Permisos asignados y editables para el rol del usuario registrado en el sistema. **(Figura 3.7)**

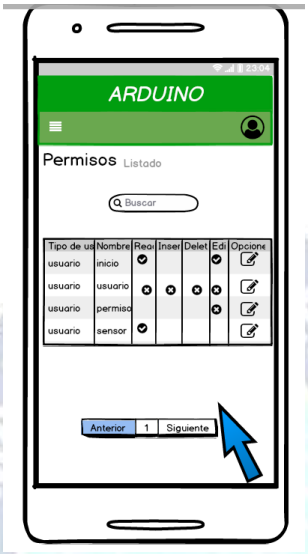


Tabla 3.7. Permisos para el rol del usuario

Diseño del hardware:

Se observa la simulación de los componentes electrónicos para el armado de la parte hardware conectado a través de los relés. **(Figura 3.8)**

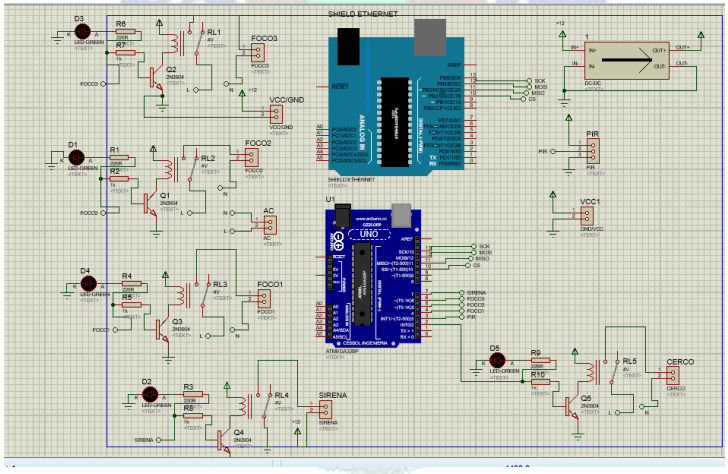


Tabla 3.8. Simulación de los componentes hardware

Se procede con el diseño de la placa de circuito impreso (PCB) que controla los componentes hardware del sistema. **(Figura 3.9)**

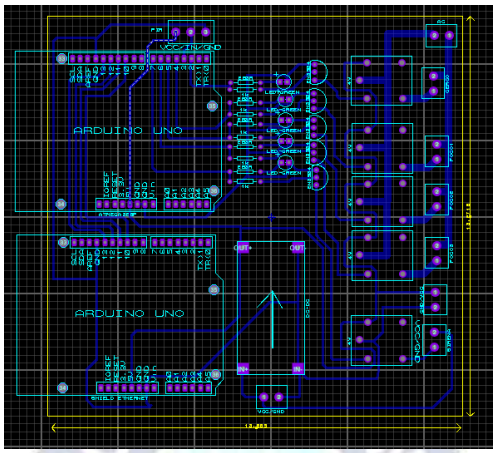


Tabla 3.9. Diseño de la placa del circuito impreso

3.2.4. FASE 4: IMPLEMENTACIÓN

En esta fase se describe el desarrollo de los módulos de la página web del sistema y los componentes hardware a utilizarse en el proyecto.

Configuración del Arduino

El código de Arduino importa librerías para la comunicación de datos y conexión al Wifi mediante el Shield Ethernet, realizando la asignación de una ip estática a la placa Arduino, como se observa en la **Figura 3.10.**

out | Source Code

in.ino

```
#include <SPI.h>//libreria para el spi del ethernet
#include <Ethernet.h>//libreria del shield etherne

byte mac[] = { 0xDE, 0xAD, 0xBE, 0xEF, 0xFE, 0xED }; //direccion mac ethernet
IPAddress ip(192,168,20,2);//ip del ethernet
EthernetServer server(80);//puerto para el acceso web http
char est1=0;
int foco1=4,foco2=5,foco3=6,sirena=7,pir=3,cerco=2;
String cadena;//variable para la recepcion de datos de la pc
void setup ()
{
  pinMode(foco1,1);
  pinMode(foco2,1);
  pinMode(foco3,1);
  pinMode(sirena,1);
  pinMode(pir,0);
  pinMode(cerco,1);
  Serial.begin(9600);
  SPI.begin();//abre la conexion spi
  Ethernet.begin(mac, ip);//inicializa ethernet
  server.begin();//se habilita el servidor
  Serial.print("Servidor en la IP:");
  Serial.println(Ethernet.localIP());
  delay(2000);
}
```

Tabla 3.10. Declaración de variables y configuración de ip en el arduino.

Proceso que sigue el ciclo del programa Arduino, cada vez que el sensor PIR envié datos de intrusión, como se observa en la **Figura 3.11.**

```
void loop()
{
delay(12000);
  if (digitalRead(pir)==1 && est1==0)
  {
//delay(12000);
    //digitalWrite(sirena,1);
    digitalWrite(cerco,1);
    digitalWrite(foco2,1);

  }
  else if(est1==0)
  {
    //digitalWrite(sirena,0);
    digitalWrite(cerco,0);
    digitalWrite(foco2,0);
  }
  EthernetClient client = server.available();//verifico peticion de un cliente
  if (client) //si existe cliente
  {
    boolean currentLineIsBlank = true;//para controlar los espacios en blanco
    cadena="";
    while (client.connected())//mientras esta conectado el cliente
    {
      if (client.available())//si el cliente pide el webserver
      {
        char c = client.read();//lee la peticion

        cadena+= c;//alamcena la peticion
        if (c == '\n' && currentLineIsBlank)//verifica si existe \n
```

Tabla 3.11. Proceso del ciclo que realiza el Arduino

Envió de datos del sensor y demás componentes hardware a una página exterior que se observa en la **Figura 3.12.**

```
      {
        //web para enviar a la pc cada elemento tiene un id para reconocer
        //el dato en la pc
        client.print("<!DOCTYPE HTML>");
        client.print("<html>");
        client.print("<head><title>Ethernet</title>");
        client.print("<meta http-equiv=\"Content-Type\" content=\"text/html; charset=utf-8\" ></head>");
        client.print("<body>");
        client.print("<form action=\"http://192.168.20.3/seguridad_php/index.php\" method=\"post\" name=\"seguridad\" id=\"seguridad\" >");
        client.print("<br /><input name=\"pir\" value=\"");
        client.print(digitalRead(pir));
        client.print("\" />");
        client.print("<br /><input name=\"foco1\" value=\"" );
        client.print(digitalRead(foco1));
        client.print("\" />");
        client.print("<br /><input name=\"foco2\" value=\"" );
        client.print(digitalRead(foco2));
        client.print("\" />");
        client.print("<br /><input name=\"foco3\" value=\"" );
        client.print(digitalRead(foco3));
        client.print("\" />");
        client.print("<br /><input name=\"cerco\" value=\"" );
        client.print(digitalRead(cerco));
        client.print("\" />");
        client.print("<br /><input name=\"sirena\" value=\"" );
        client.print(digitalRead(sirena));
        client.print("\" />");
        client.print("</form>");
        client.print("<script> document.seguridad.submit();</script>");
        // Buscar campo data
```

Tabla 3.12. Envió de datos a la pagina exterior

En la **Figura 3.13** se observa la comparación de id, que controla cada botón de la página web para el prendido de focos y del cerco eléctrico.

main.ino

```
86          // Buscar campo data
87          if (cadena.indexOf("dato=a")>-1)
88          {
89            digitalWrite(foco1,1);
90          }
91          else if (cadena.indexOf("dato=b")>-1)
92          {
93            digitalWrite(foco1,0);
94          }
95          else  if (cadena.indexOf("dato=c")>-1)
96          {
97            digitalWrite(foco2,1);
98          }
99          else if (cadena.indexOf("dato=d")>-1)
100         {
101           digitalWrite(foco2,0);
102         }
103          else  if (cadena.indexOf("dato=e")>-1)
104         {
105           digitalWrite(foco3,1);
106         }
107         else if (cadena.indexOf("dato=f")>-1)
108         {
109           digitalWrite(foco3,0);
110         }
111          else  if (cadena.indexOf("dato=g")>-1)
112         {
113           digitalWrite(cerco,1);
114           est1=1;
115         }
116         else if (cadena.indexOf("dato=h")>-1)
117         {
```

Tabla 3.13. Comparación de id para el manejo de los botones

Armado de componentes del Arduino

Placa impresa que conecta los componentes hardware con la página web del sistema. **(Figura 3.14)**

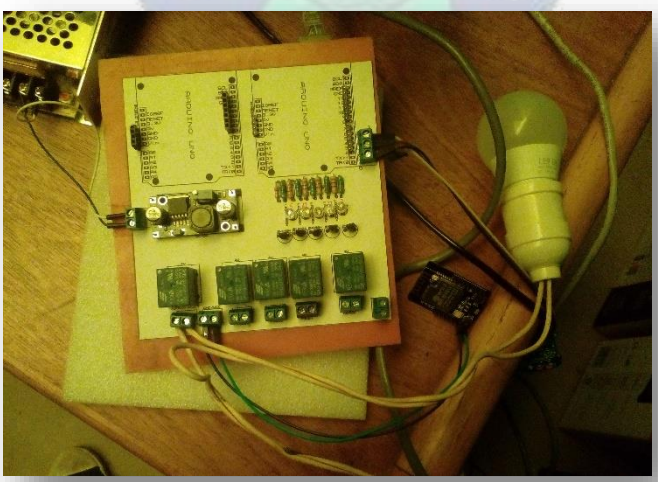


Tabla 3.14. Placa que controla los componentes hardware

Configuración del framework Code Igniter

En la **(Figura 3.15)** se observa la conexión de la base de datos MySql con el framework Code Igniter.

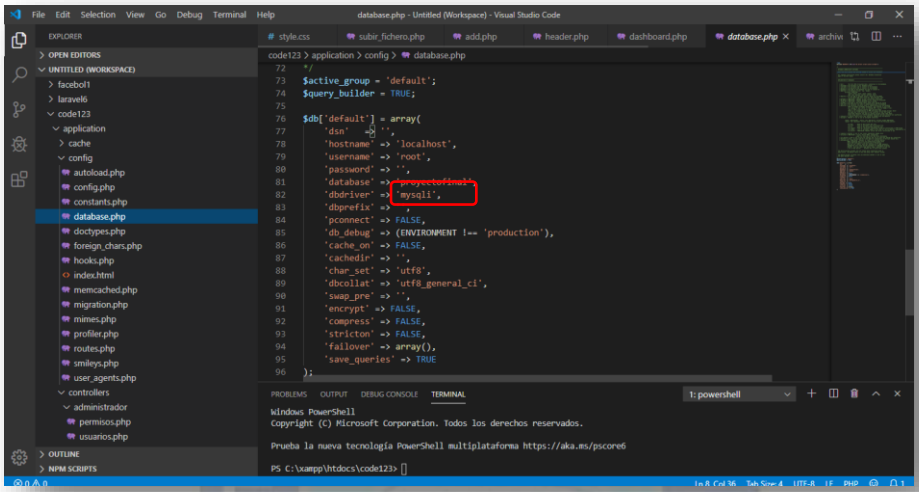


Tabla 3.15. Conexión del framework con la base de datos

Asignación de una ip estática a la página web, para la conexión con la placa base que maneja los componentes hardware y las cámaras de seguridad. **(Figura 3.16)**

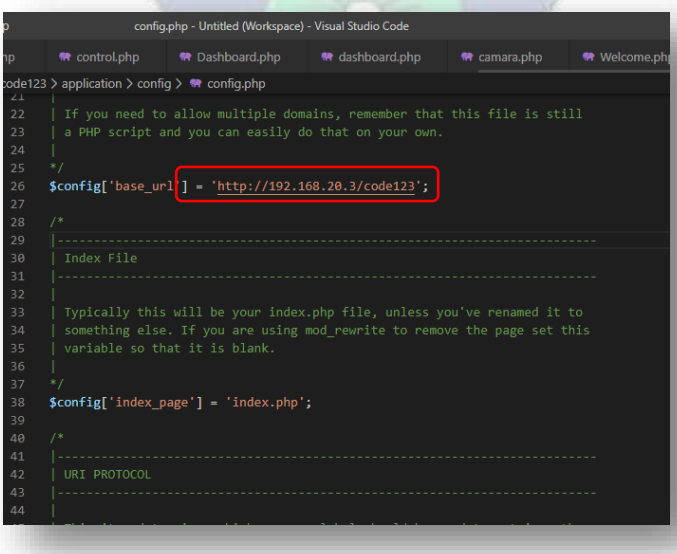


Tabla 3.16. Asignación de ip a la pagina web del sistema.

Herramienta para el modelado de datos de la Base de Datos, aplicando el modelo de Entidad Relación. **(Figura 3.17.)**

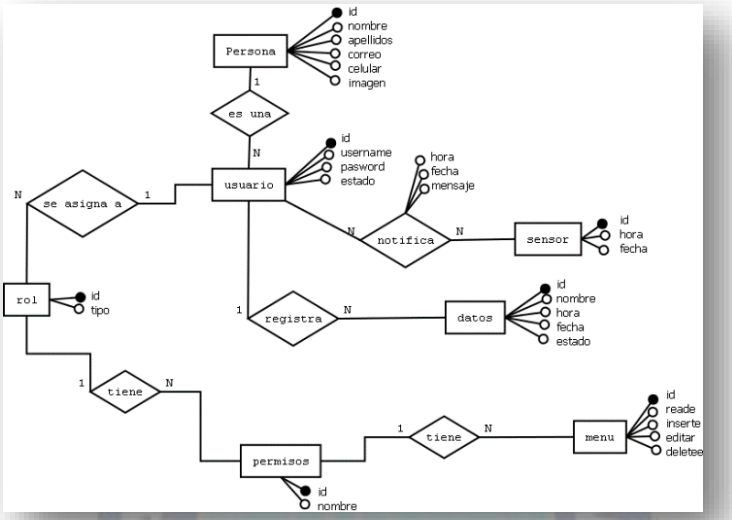


Tabla 3.17. Modelo Entidad – Relacion

Tablas de la base de datos de Mysql que se aplica para el funcionamiento del sistema de seguridad. **(Figura 3.18)**

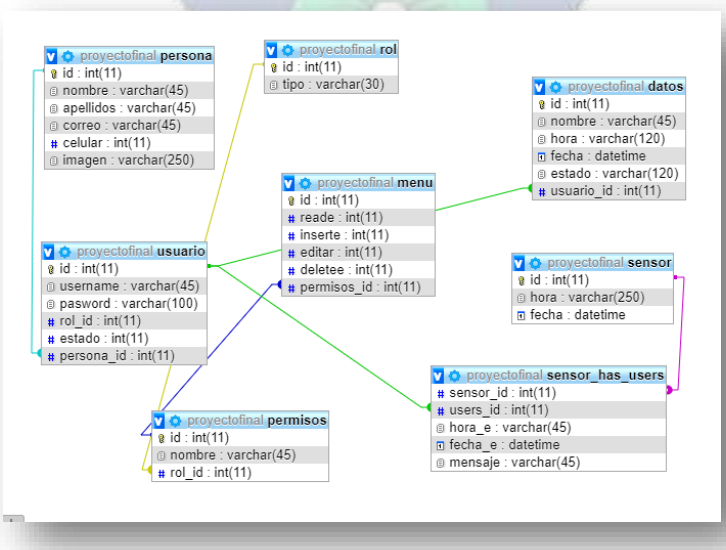


Tabla 3.18. Modelo relacional de la base de datos del sistema

Configuración del router

Se realiza la creación de un punto Wifi en el router para la conexión de la placa base, la página web y las cámaras de seguridad a través de ip estática.

Configuración de la cámara de seguridad

La instalación de las cámaras de seguridad, se la realiza en el patio y en la puerta principal de la vivienda. **(Figura 3.19)**

Tabla 3.19. Instalación de la cámara de seguridad en el patio de la vivienda

Para la visión de cámaras vía web en una PC o laptop, se procede con la instalación del siguiente plugin para el navegador chrome. **(Figura 3.20)**

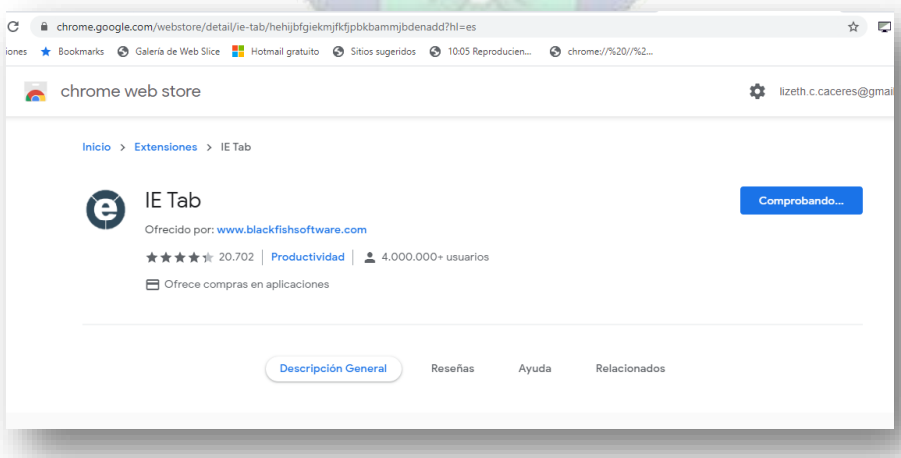


Tabla 3.20. Instalación del plugin IE Tab para chrome

Terminada la instalación del plugin, se procede con el ingreso de la ip asignada por el Wifi a la cámara, q siguiente pantalla. **(Figura 3.21)**

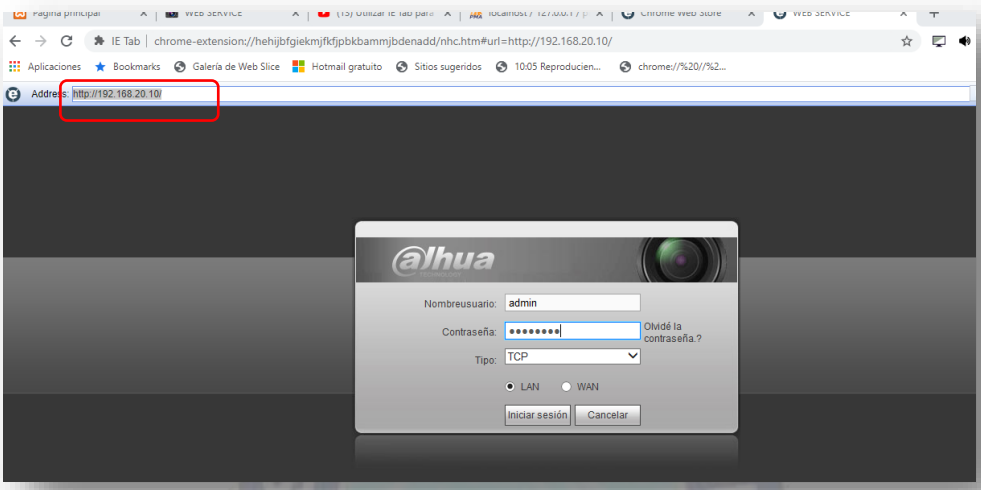


Tabla 3.21. Autentificación para el acceso de la cámara con el usuario y password que viene por defecto.

Dispositivo android

Para los dispositivos android se realiza instalación de la aplicación gDMSS Lite. **(Figura 3.22)**

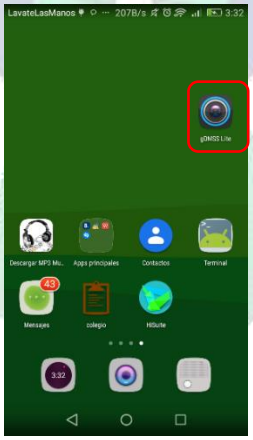


Tabla 3.22. Aplicación gDMSS descargada de Play Store

Terminada con la instalación de la aplicación, se procede con la conexión al Wifi que se observa en la **Figura 3.23.**

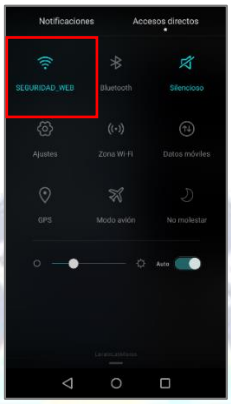


Tabla 3.23. Conexión del teléfono con el WiFi del router.

Una vez ingresado a la aplicación, se procede con el pinchado de la siguiente pestaña e ingreso de datos del usuario y la ip asignada a la cámara de seguridad. **(Figura 3.24)**

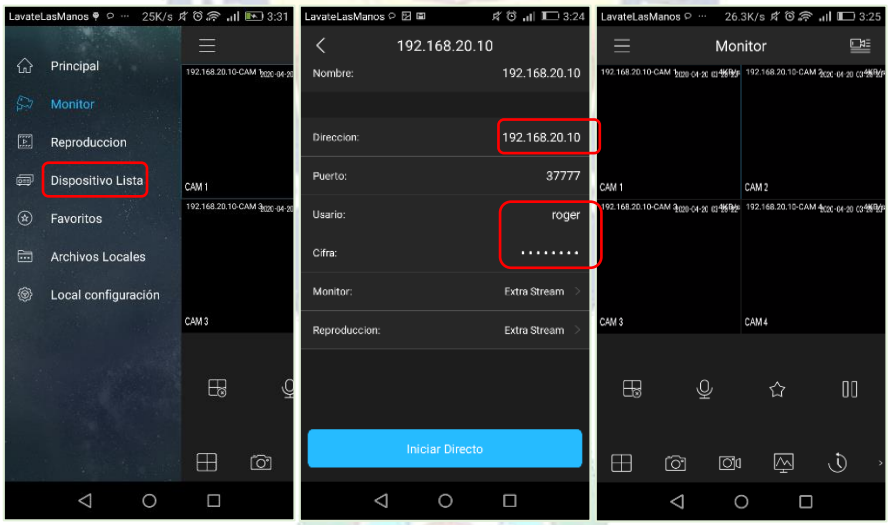


Tabla 3.24. Conexión en red con la cámara de seguridad desde un dispositivo Android

Instalación del cerco eléctrico

Las herramientas que se observa en la **Figura 3.25** se aplica en la instalación del cerco eléctrico

Tabla 3.25. Herramientas del cerco eléctrico

Tesado del alambre galvanizado sobre los postes, donde se transmite corriente desde su central. **(Figura 3.26)**

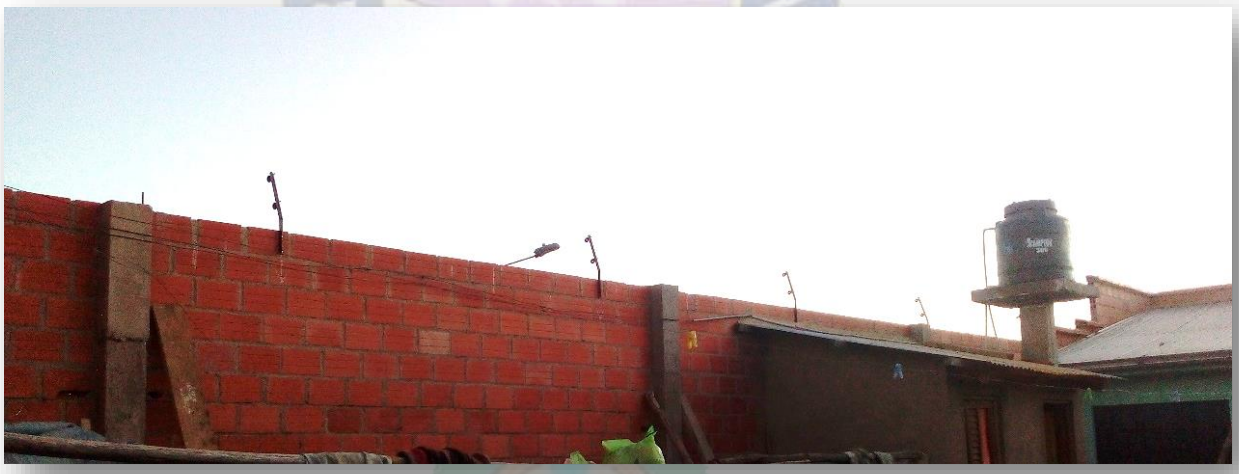


Tabla 3.26. Tesado del alambre sobre los postes

3.2.5. FASE 5 TEST UNITARIO

Se procede con la verificación de cada módulo tanto en la parte de software y hardware de forma unitaria, comprobando su funcionamiento adecuado para la comunicación del sistema.

Software

El software realizado con el framework Code Igniter **(ver Figura 3.27)**, inicia con la autentificación del usuario registrado en la base de datos.

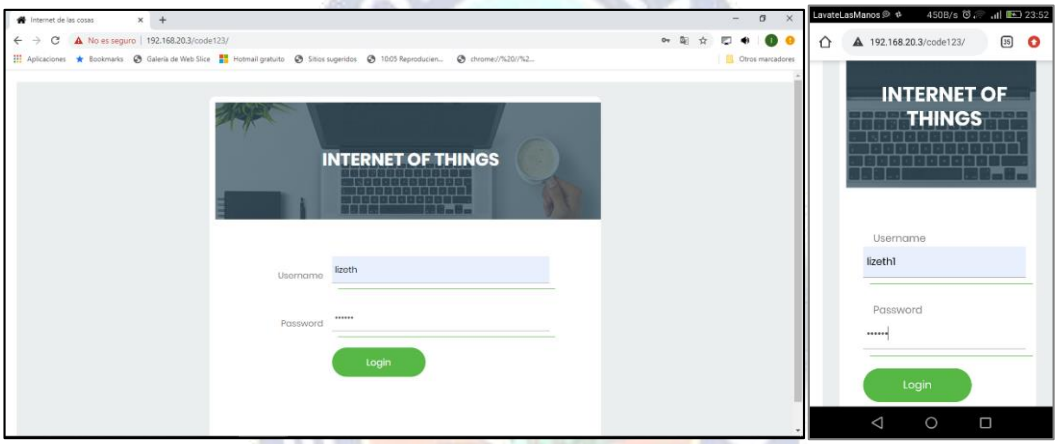


Tabla 3.27. Loguin desde un móvil y una PC

En el menú principal **(ver Figura 3.28)** se observa un acceso directo a cada módulo del sistema, adicionalmente un gráfico del historial del sensor PIR.

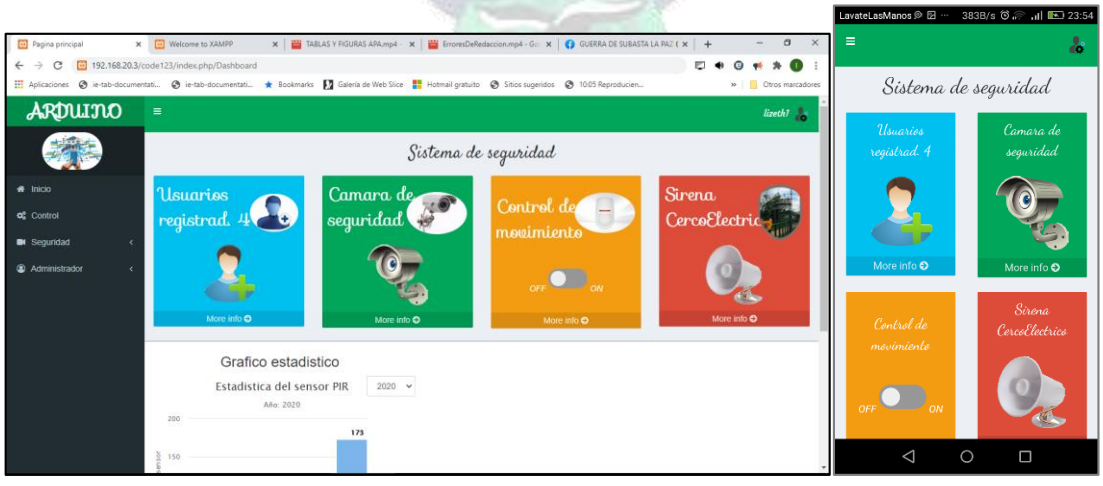


Tabla 3.28. Menú principal del sistema

Pantalla donde se realiza la comunicación del sistema con el hardware a través de los botones con el activado y desactivado. **(Figura 3.29)**

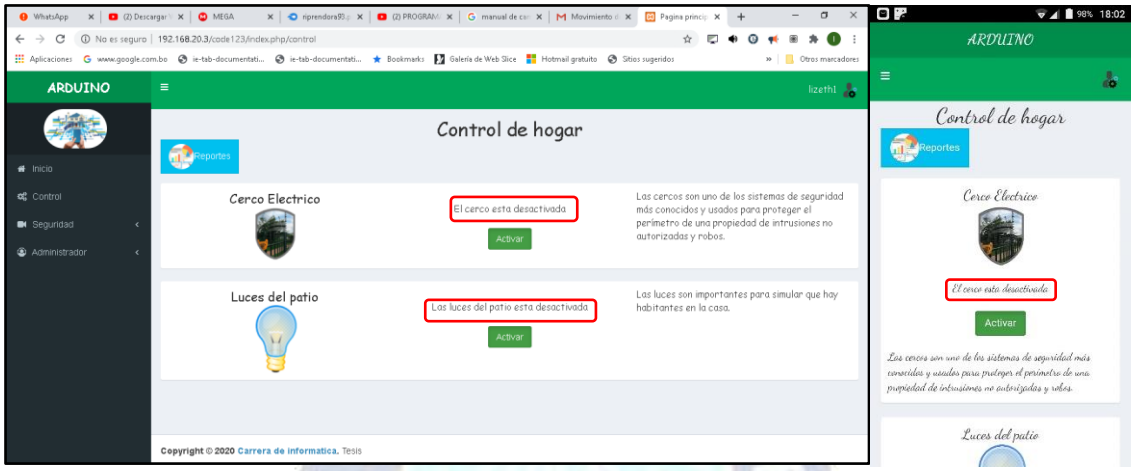


Tabla 3.29. Comunicación del sistema con los componentes hardware.

En la **Figura 3.30** se observa un reporte sobre el manejo de cada uno de los componentes hardware registrando el usuario y hora que se activó o desactivo dichos componentes.

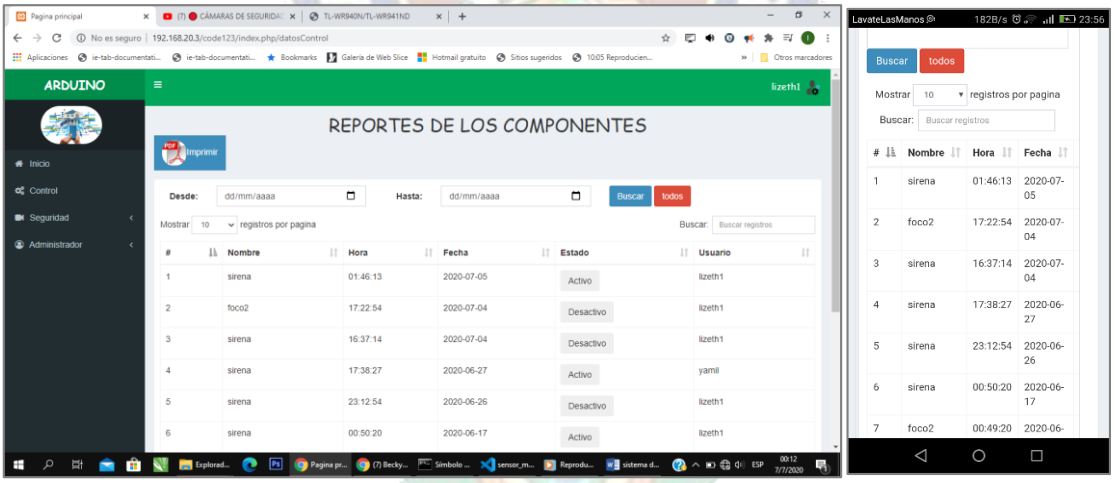


Tabla 3.30. Reporte de componentes hardware

Envió de datos de intrusión almacenando en la BD del sistema, adicionalmente un gráfico del reporte clasificado por mes. **(Figura 3.31)**

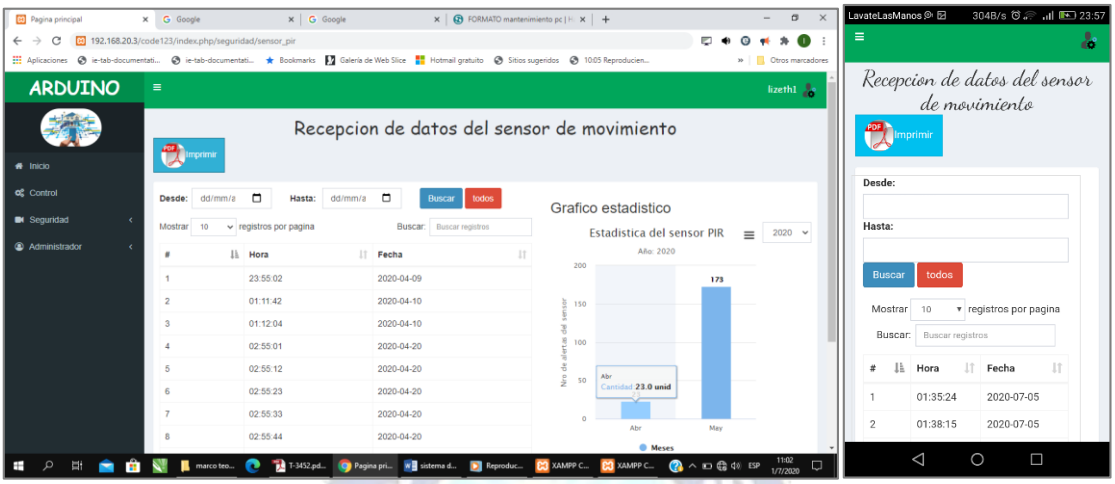


Tabla 3.31. Reporte del sensor PIR

Envió de alerta a usuarios registrados en el sistema, a través del correo electrónico. **(Figura 3.32)**

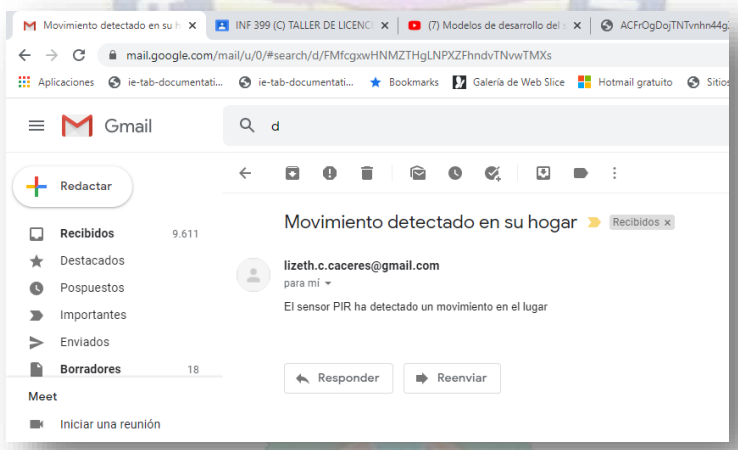


Tabla 3.32. Mensaje al correo electrónico

Administrador de usuarios

En la **figura 3.33** se observa los usuarios registrados en el sistema, creación de un nuevo usuario, y otorgación de permisos para el uso sistema.

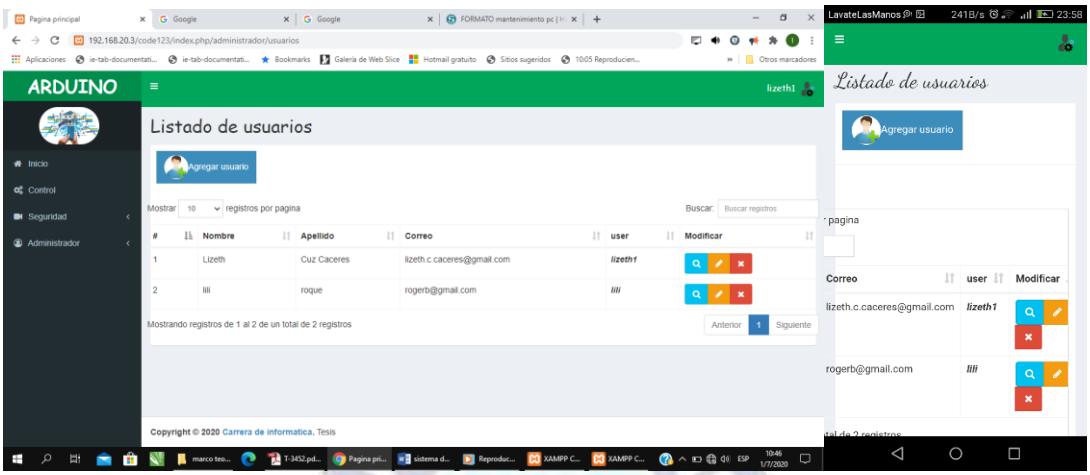


Tabla 3.33. Administración de usuarios

Datos básicos del usuario registrado y el rol que ocupa en la base de datos del sistema. **(Figura 3.34)**

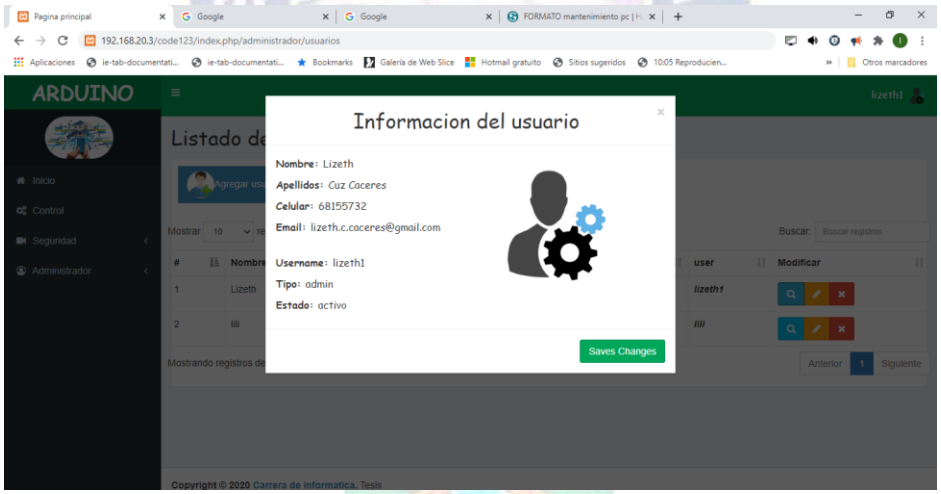


Tabla 3.34. Información del usuario registrado en la base de datos del sistema.

La agregación de usuarios para el manejo del sistema, lo realiza el administrador como se observa en la **Figura 3.35.**

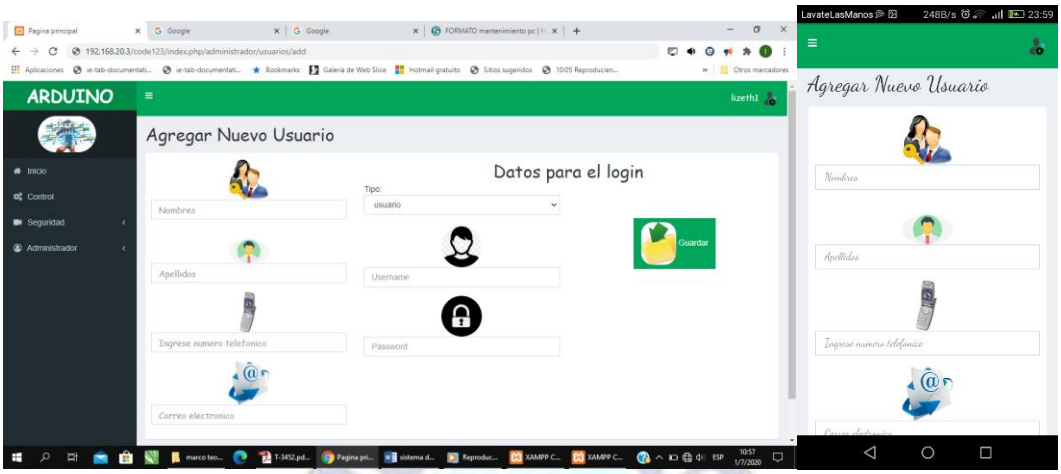


Tabla 3.35. Adición de usuarios

Asignación de permisos para el rol de usuario en cada uno de los módulos del sistema. **(Figura 3.36)**

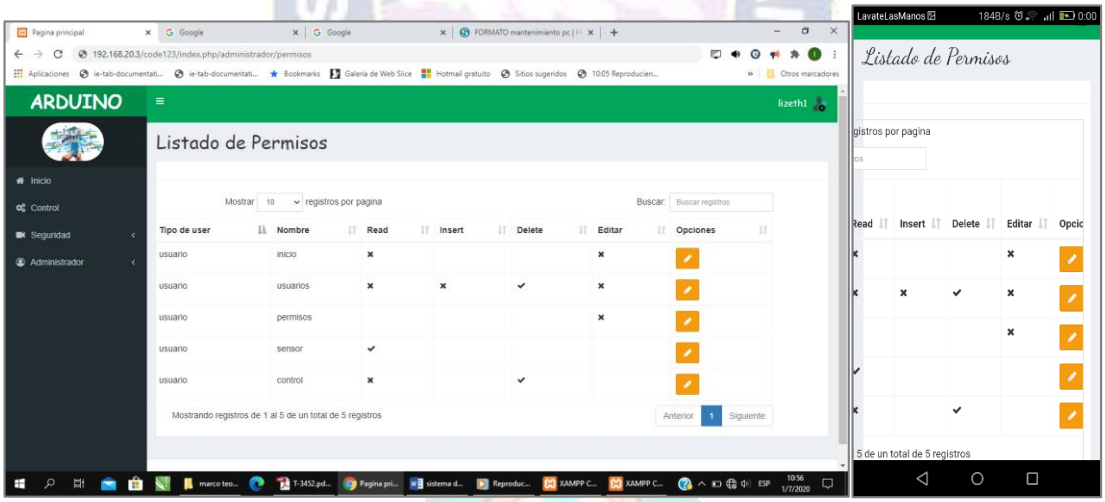


Tabla 3.36. Otorgación de permisos

Editar permisos según vea conveniente el administrador del sistema, para cada módulo del sistema. **(Figura 3.37)**

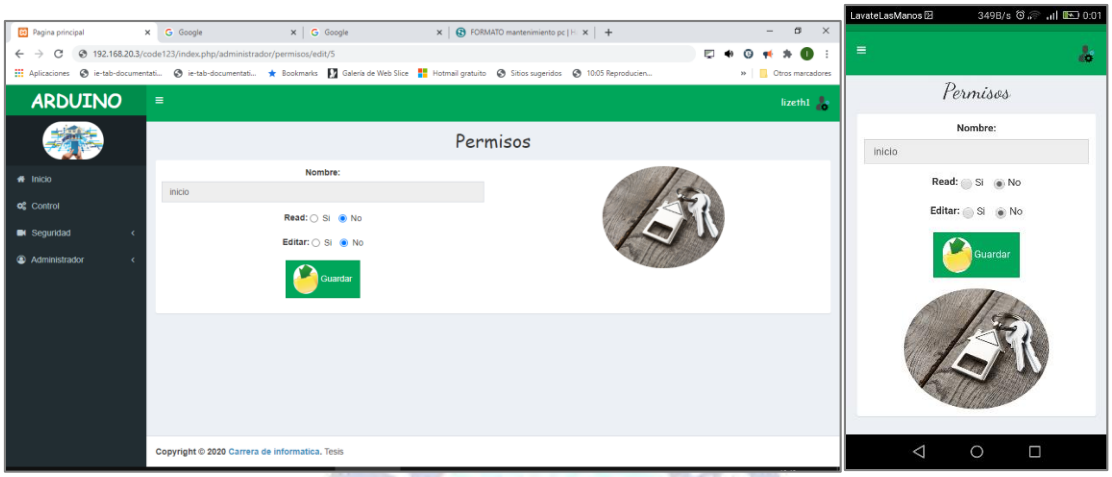


Tabla 3.37. Editar permisos del rol usuario

Hardware

Prueba de visibilidad de cámaras de seguridad desde la página web según a la ip asignada desde el punto Wifi. **(Figura 3.38)**

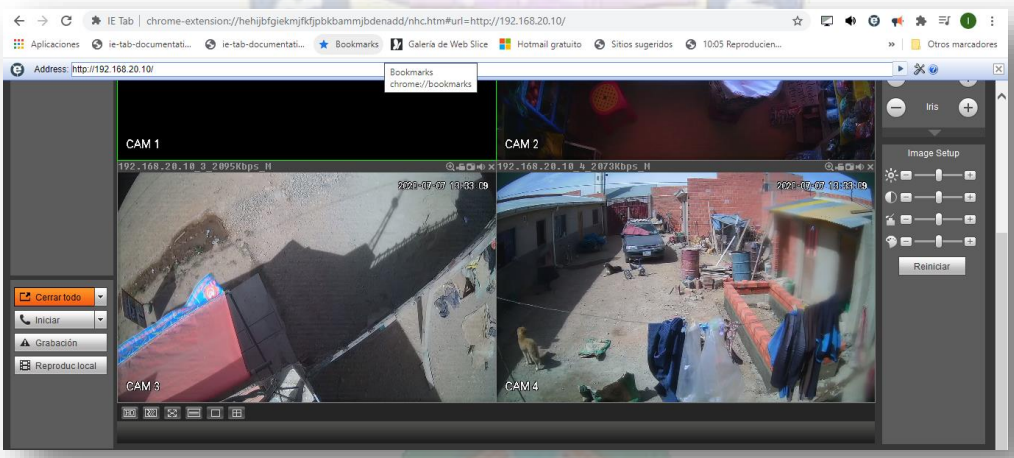


Tabla 3.38. Cámaras de seguridad

3.2.6. FASE 6: INTEGRACIÓN

En esta fase se integran los distintos módulos que forman de manera conjunta el sistema.

Integración de focos con la placa base del proyecto como se muestra en la **tabla 3.13.**

Tabla 3.13. Integración de los focos en la placa

Prueba realizada	Integración de los focos con la placa del circuito
Detalle	A través de los cables positivo y negativo se conecta los cables con el relay del circuito, el cual se monitorea con los botones de la pagina.
Resultado	Al presionar el botón de prendido, se activa el foco de manera correcta

Conexión del cerco eléctrico a través de cable con la sirena como se muestra en la **tabla 3.14.**

Tabla 3.14. Conexión de la placa con la sirena.

Prueba realizada	Conexión del cerco con la sirena
Detalle	El cerco se conecta con la sirena a través del relay con los colores blanco(-) y naranja(tono1)
Resultado	Conexión de forma satisfactoria de la placa con la sirena de forma directa

Conexión del cerco eléctrico con la placa base que utiliza el sistema que se detalla en la **tabla 3.15.**

Tabla 3.15. Conexión de la placa con el cerco electrico.

Prueba realizada	Conexión de la placa con el cerco electrico.
Detalle	La placa se conecta con el cerco eléctrico a través de su electrificador, conectado al relay de la placa.
Resultado	Conexión de forma satisfactoria de la placa con el electrificador del cerco electrico.

3.2.7. FASE 7: TEST OPERACIONAL DEL SISTEMA

En esta última fase se realiza las últimas pruebas del sistema como producto final, basados en sus objetivos planteados en el Capítulo I.

En el Capítulo IV (Resultados) se muestra las pruebas realizadas y los resultados obtenidos del sistema web y su funcionamiento.

CAPITULO IV
RESULTADOS

4. RESULTADOS

El diseño y desarrollo del software adoptó la metodología en V, citada en el Capitulo II de la presente tesis, a partir de esta se siguen las fases correspondientes para obtener el sistema.

4.1. PRUEBAS

Para realizar las pruebas del sistema se optó por el método de estudio de casos el cual Rovira (2018) lo describe como una herramienta de investigación y una técnica de aprendizaje que puede ser aplicado en cualquier área de conocimiento, y además es considerada como una técnica de investigación cualitativa.

La implementación del sistema y las pruebas se la realizó en un domicilio particular ubicado en la Zona Tilata Jnas (ver **figura 4.1**.) donde los usuarios que manipulan el sistema, serán los miembros del hogar. La zona donde se ubica la vivienda, no existe cobertura WIFI de ninguna empresa, por lo que se optó levantar un punto WIFI desde un router e instalando todos los dispositivos como se describe en el Capítulo III.

Tabla 4.1. Vivienda donde se implementó el sistema de seguridad

Los componentes que se instaló en la vivienda fueron mencionadas en el anterior capitulo, el circuito que conecta todos los componentes hardware, el router y el DVR de las cámaras de seguridad, se observa en la **figura 4.2**.

Figura 4.2. Circuito del sistema, el router y el DVR de las cámaras

Las cámaras de seguridad funcionan las 24 horas del día, monitoreando de forma continua junto al sensor PIR y el foco que se muestra en la **figura 4.3.**

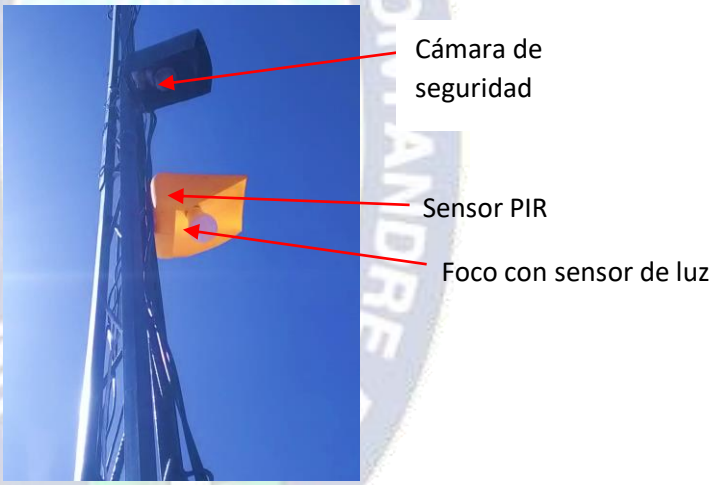


Figura 4.3. 2da cámara de seguridad junto con el foco y sensor PIR

4.2. INICIO DEL SISTEMA

La prueba del sistema se realizó cerca al mediodía, con una simulación de intrusión cerca del área del sensor PIR de la siguiente manera:

El sensor PIR cada que capta presencia cerca de la puerta principal procede con el prendido del foco que está a la altura del sensor, el foco independiente cuenta con un sensor de luz (solo en las noches se activa) y además realiza el envío de un mensaje al correo electrónico de los usuarios registrados en la base de datos, como se ve en la **figura 4.4.**

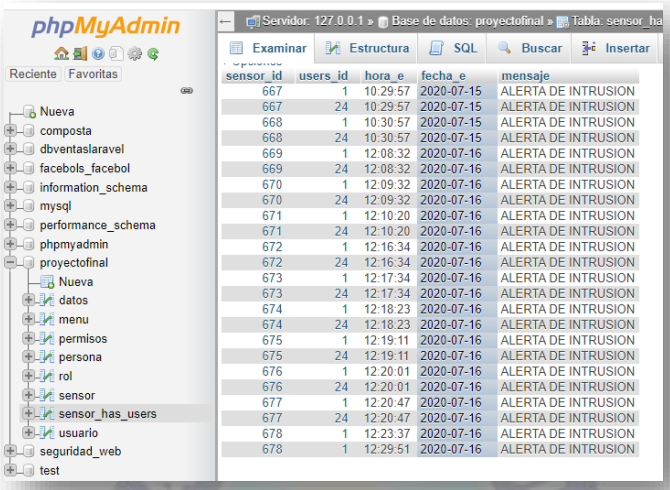


Tabla 4.4. Envió de alerta al correo electrónico de los usuarios registrados.

Siendo un usuario registrado en el sistema, llega al correo electrónico la alerta de intrusión con un acceso directo para el ingreso de la página web, como se ve en la **figura 4.5.**

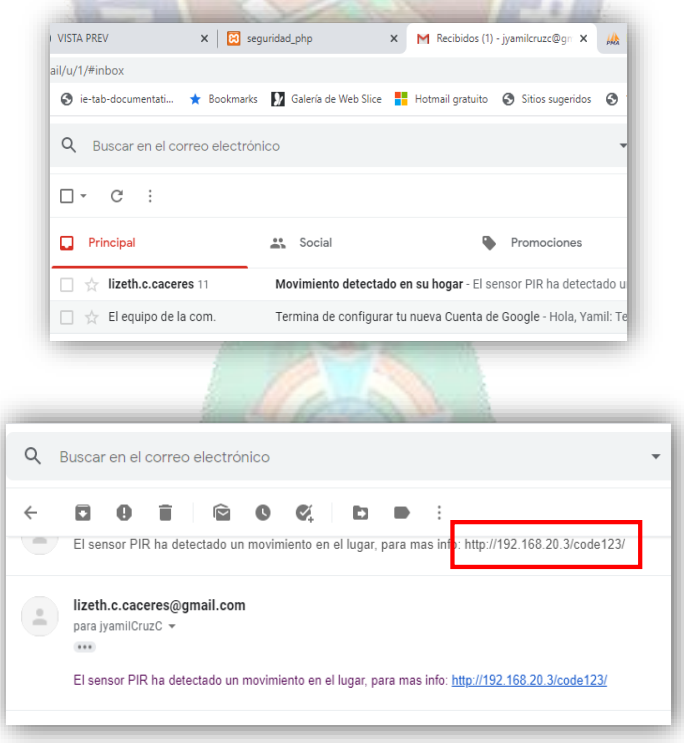


Tabla 4.5. Correo de alerta de intrusión

Una vez ingresado al link que se menciona anteriormente, se procede con la autentificación del usuario y se observa el menú principal como se muestra en la **figura 4.6.**

Tabla 4.6. Menú principal de la página web

Una vez dentro del sistema se procede a la verificación de intrusion cerca del área donde está situada el sensor PIR a través de las cámaras de seguridad como se ve en la **Figura 4.7.**

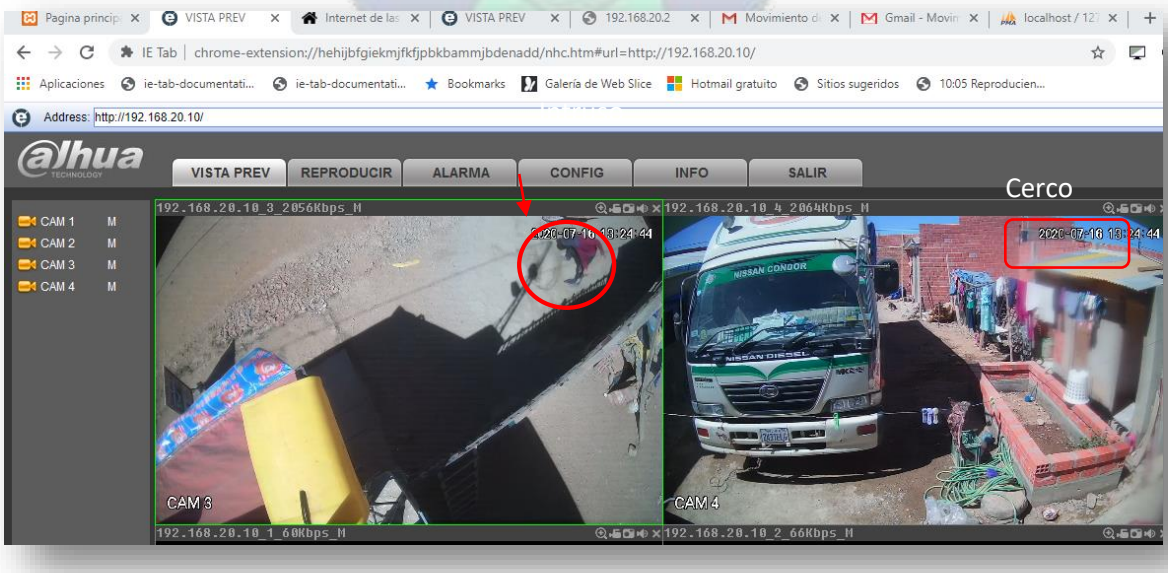


Tabla 4.7. Cámaras de seguridad de la vivienda

Después de verificar que son antisociales que quieran ingresar al domicilio, se procede con la activación del cerco eléctrico **(ver figura 4.8),** pasando corriente por todo el muro de la vivienda, por lo que cualquier intruso que quiera atravesar al domicilio hará un contacto con el cable y este procederá con descarga eléctrica al intruso **(ver figura 4.9.)**

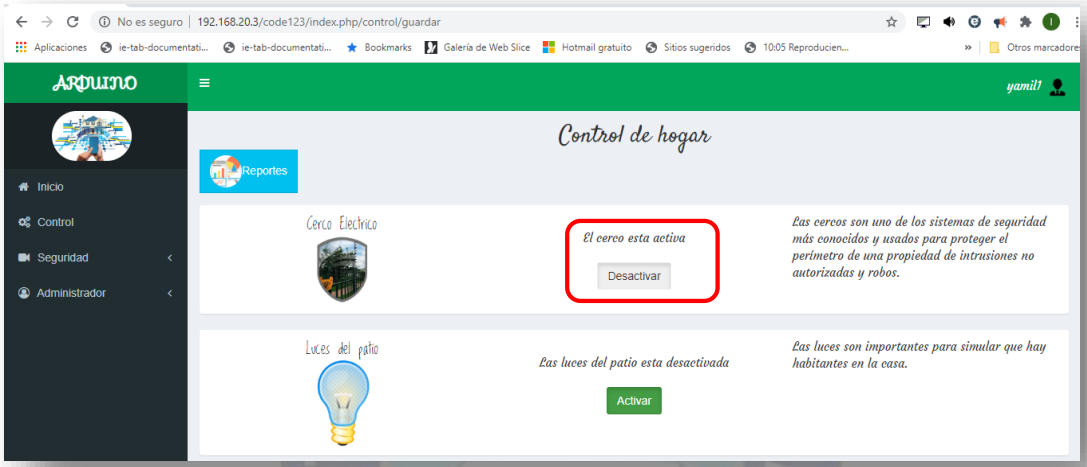


Tabla 4.8. Activación del cerco desde la página

Tabla 4.9. Contacto con el alambre galvanizado

En caso que el antisocial proceda con el corte del alambre para ingresar a la vivienda, la central del cerco eléctrico al detectar el corte, se activa de forma automática e instantánea la sirena con un tiempo programado de 4 segundos que se observa en la **figura 4.10.**

Tabla 4.10. Activación de la sirena

En caso que sea de noche se activa el foco del patio para de alguna manera alertar al antisocial (ver **figura 4.11**) y que se pueda ver el lugar iluminado

.

Tabla 4.11. Encendido del foco del patio

Para la obtención del historial de usuario que manda instrucciones a los componentes **(ver figura 4.12)** se refleja en la página del sistema.

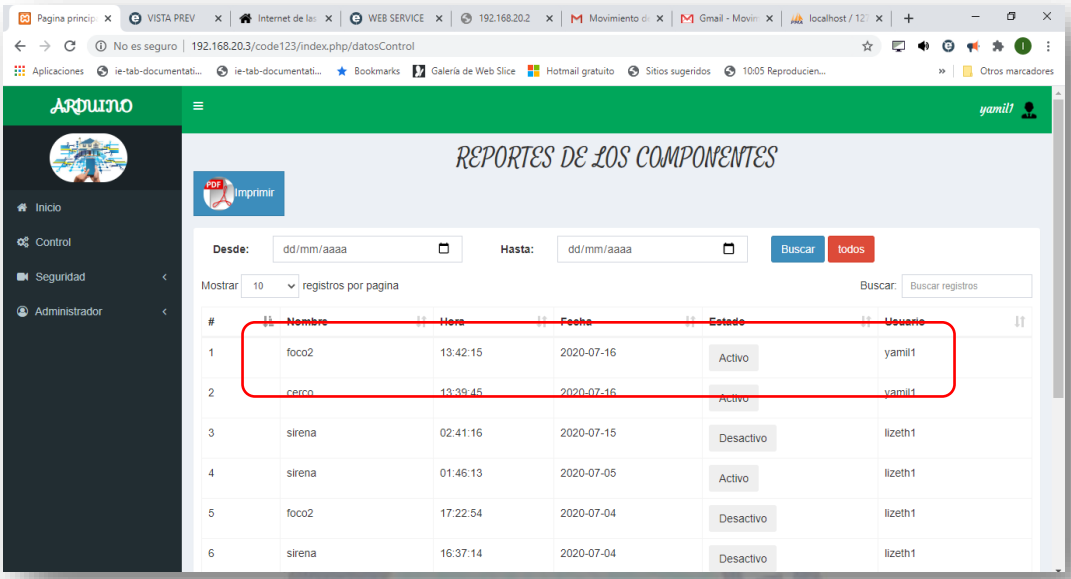


Tabla 4.12. Reporte del sistema

Se obtiene un reporte capturando la fecha y hora de intrusión y un gráfico como se observa en la **figura 4.13**.

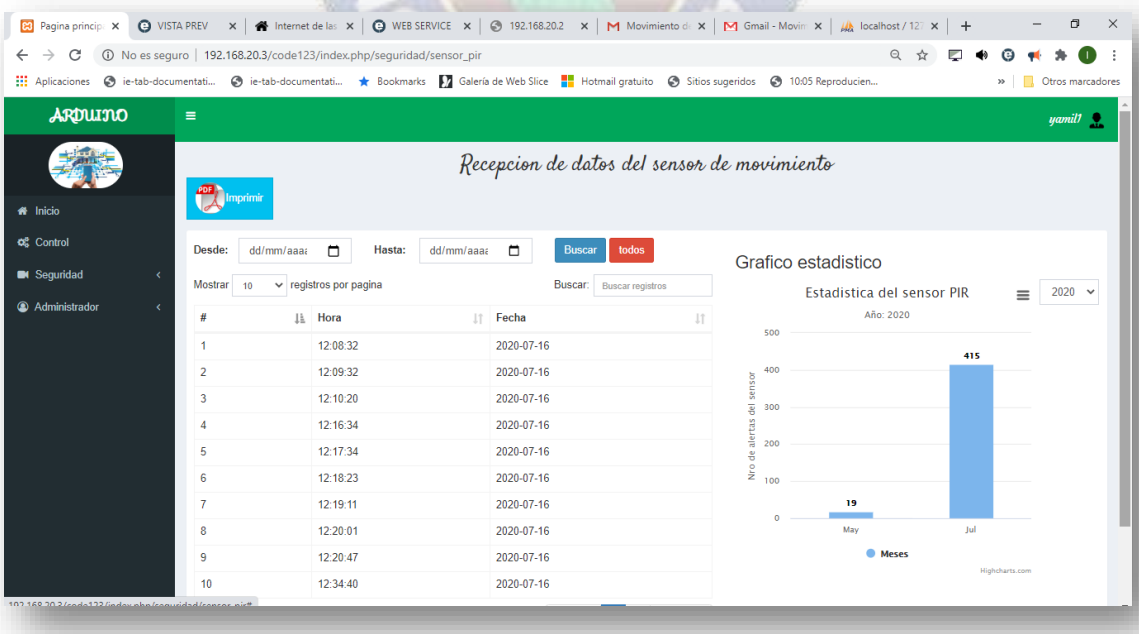


Tabla 4.13. Datos del sensor PIR

4.3. PRUEBAS DE ACEPTACIÓN

a) Sensor PIR

En el proceso de pruebas de funcionamiento del sensor se procedió con la configuración de distancia de 7 metros en cuanto a detección de movimiento, el sensor está situado cerca de la puerta principal, el cual será calibrado el tiempo de activación para el envió del correo electrónico de manera correcta como se observa en la **tabla 4.1.** y en la **figura 4.14**.

Tabla 4.1. Resultado de la calibración del sensor PIR

Nº de pruebas	Hora registrada	Tiempo en seg
1	12:35:41	0
2	12:36:29	48
3	12:41:07	38
4	12:42:07	60
5	12:42:55	48
6	12:43:44	49
7	12:44:32	48
8	12:47:45	73
9	12:48:45	60
10	12:49:34	49
11	20:44:01	48
12	20:45:13	67
13	20:46:13	60
14	20:47:13	60
15	20:48:01	48
16	20:48:50	49
17	20:55:16	26
18	20:56:16	60
19	20:57:17	61

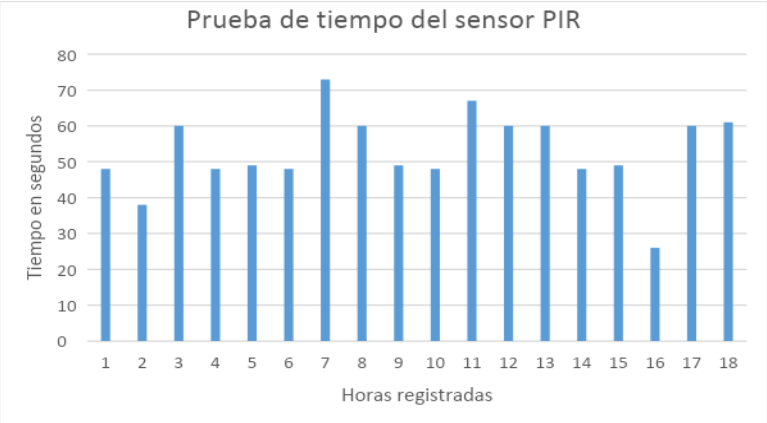


Figura 4.14. Calibración del sensor PIR

b) Ejecución del sistema

En cuanto a la ejecución de la página web del sistema, de acuerdo a las pruebas realizadas en la distancia al punto WIFI del ordenador, se observó que tarda unos segundos en cargar la página, dando una solución a este problema, con la implementación de un extensor de WIFI, para que no tenga que tardar muchos segundos en cargar la página, como se describe en la **tabla 4.2.** y en la **figura 4.15**.

Tabla 4.2. Tiempo de demora en cargar la página web

Nº de pruebas	Distancia en metros	Tiempo en seg
1	10	4
2	9	4
3	8	4
4	7	4
5	6	3
6	5	3
7	4	3
8	3	3
9	2	3

10	1	2
11	10	2
12	9	2
13	8	2
14	7	2
15	6	2
16	5	2
17	4	2
18	3	2
19	2	2
20	1	2

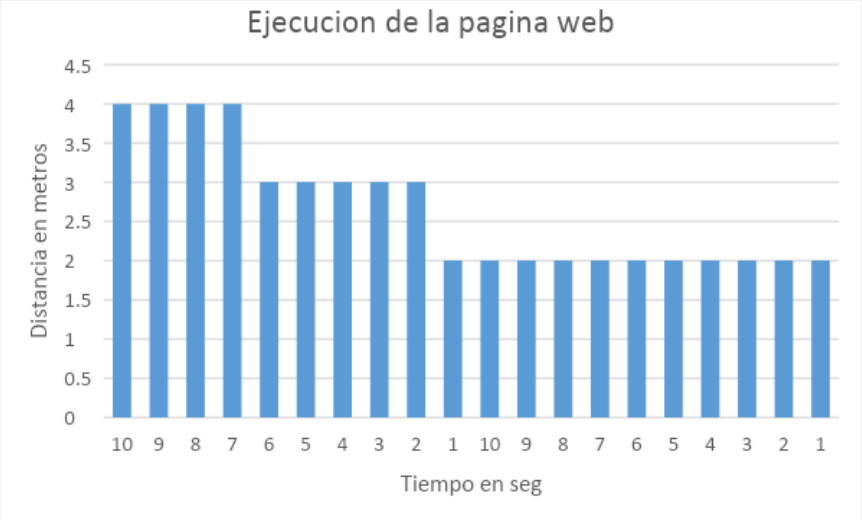


Figura 4.15. Tiempo que tarda en responder la página web

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5. CONCLUSIONES Y RECOMENDACIONES

En el presente capítulo se detalla conclusiones respecto al trabajo de investigación junto a los objetivos planteados en el Capítulo I, general y específicos.

Para llegar a cumplir los objetivos se realizó pruebas del sistema implementado en una vivienda particular, de tal forma haciendo modificaciones para que el funcionamiento del sistema sea el más óptimo.

5.1. CUMPLIMIENTO DE OBJETIVOS

De acuerdo al objetivo general se implementó el sistema de seguridad basado en el Internet de las Cosas levantando el punto WIFI en un router, asimismo implementando varios componentes de tal manera que el sistema cumpla con los requerimientos básicos que debe tener en cuanto a protección de la vivienda, en el caso de intrusión se activa el cerco eléctrico que de alguna forma amenaza al antisocial que quiera ingresar a la vivienda.

En cuanto a los objetivos específicos planteados en el trabajo de investigación, a continuación se describe el cumplimiento de cada uno de ellos.

- Se implementó las cámaras de seguridad dentro y fuera de la vivienda para una mejor visión.
- Implementación del sensor PIR que capta presencia de intrusión y activación de un foco de manera automática en el caso que sea de noche, que está situada cerca de la cámara, para una visión clara del intruso a través de las cámaras.
- Se construyó la placa del circuito electrónico, que controla la parte del cerco, los focos, cámara de seguridad.
- Se implementó el cerco eléctrico, cercando todo el muro de la vivienda, teniendo su electrificador que lo controla y el de la sirena.
- Se instaló el foco en el patio para la simulación de que hay personas en el hogar, que se aplica en las noches.

- Se desarrolló e implementó la página web que controla todos los componentes que se mencionó anteriormente en el Capítulo III.

5.2. RECOMENDACIONES

Algunas recomendaciones importantes para futuras investigaciones:

- Implementar el sistema de seguridad en una vivienda preferentemente que tenga cobertura de WIFI, ya que el monitoreo del hogar se podrá hacer desde cualquier lugar que hubiera conexión a internet y el cual será más óptimo para el uso del sistema.
- Implementar un módulo de la página web para la obtención de backup de forma automática cada cierto tiempo.
- Implementar más sensores en cuanto a la seguridad de viviendas para disponer de un sistema más amplio.
- En caso de no contar con energía eléctrica, poner una batería de tal forma que el sistema esté funcionando de manera normal sin energía eléctrica.
- Incorporar el uso de un shield GPS/GPRS para notificar la alerta de intrusión al propietario de la vivienda, en caso de no contar con correo electrónico.

BIBLIOGRAFIA

(2020). Obtenido de Instructables: https://www.instructables.com/id/Arduino-Tutorial-0-Introducci%C3%B3n/

(19 de Mayo de 2020). Obtenido de luisllamas: https://www.luisllamas.es/arduino-ethernet-shield-w5100/

apselectronicsolutions. (2019). Obtenido de http://apselectronicsolutions.com/seguridad/cerco.html

Arce, J. (s.f.). Obtenido de https://cdn.slidesharecdn.com/ss_thumbnails/xampp-171130111719-thumbnail-4.jpg?cb=1512040732

AV Electronics. (2020). Obtenido de https://avelectronics.cc/producto/ethernet-shield/

Aviles, A., & Cobeña, K. (2015). *Diseño e implementación de un sistema de seguridad a través de cámaras, sensores y alarma, monitorizado y controlado telemétricamente para el centro de acogida "Patio mi pana" perteneciente a la fundación proyecto salesiano.* Ecuador: Ingenieria Electronica.

B., G. (13 de mayo de 2019). *Hostinger*. Obtenido de https://www.hostinger.es/tutoriales/que-es-mysql/

c. (h de h de h). *h.* Obtenido de h

conectate. (s.f.). Obtenido de https://s3.amazonaws.com/cdn.conectate-new.com/wp-content/uploads/2017/04/07181908/Seguridad-Hogar.jpg

Constanzo, L. M. (2014). COMPARACION DE MODELOS DE CALIDAD. 8.

DefinicionABC. (s.f.). Obtenido de

desarrolloweb6. (9 de Mayo de 2001). Obtenido de https://desarrolloweb.com/articulos/392.php

Esfera Creativa. (2019). Obtenido de https://esferacreativa.com/desarrollar-web-bootstrap/

Ferrer, V. (30 de 05 de 2019). Obtenido de https://vicentferrer.com/sensor-de-movimiento/

Ferrer, V. (26 de Marzo de 2019). Obtenido de https://vicentferrer.com/camaras-seguridad-vigilancia/

GRUPODIGITAL. (13 de Diciembre de 2018). Obtenido de https://grupodigital360.com/iso-9126-metricas-para-calidad-web/

Instituto nacional de tecnologías de comunicación, (2009). Ingeniería del software: metodología y ciclos de vida. Laboratorio nacional de calidad del software de inteco.

IONOS. (07 de 09 de 2017). Obtenido de https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/codeigniter-framework-php-rapido-y-versatil/

isoftwareunesum. (9 de Mayo de 2011). Obtenido de https://isoftwareunesum.wordpress.com/ingenieria-del-software-en-la-web/

iUrban. (s.f.). Obtenido de https://iurban.es/wp-content/uploads/2019/03/Internet-of-things-hero-como-objeto-inteligente-1.jpg

jrodriguez. (28 de Septiembre de 2008). *UDT-IA*. Obtenido de http://old-web-1.iiia.csic.es/udt/es/blog/jrodriguez/2008/metodologia-desarrollo-sotware-modelo-en-v-o-cuatro-niveles

Mahecha, J. (2018). *Diseño e implementacion de una aplicacion domotica para iluminacion usando inteligencia artificial.* Bogota: Universidad de la Salle.

Naylamp Mechatronics. (s.f.). Obtenido de https://naylampmechatronics.com/espressif-esp/700-camara-ov2640-esp32-cam.html

NAYLAMP MECHATRONICS. (s.f.). Obtenido de https://naylampmechatronics.com/espressif-esp/700-camara-ov2640-esp32-cam.html

Perez, J., & Merino, M. (2008). *Metodo inductivo.* Obtenido de https://definicion.de/metodo-inductivo/

rodriguez, J. (28 de Septiembre de 2008). Obtenido de UDT-IA: http://old-web-1.iiia.csic.es/udt/es/blog/jrodriguez/2008/metodologia-desarrollo-sotware-modelo-en-v-o-cuatro-niveles

Rojas, C. A. (21 de febrero de 2018). Obtenido de https://aprendiendoarduino.wordpress.com/2017/01/23/programacion-arduino-5/

Rovira, I. (8 de Marzo de 2018). Obtenido de https://psicologiaymente.com/psicologia/estudio-de-caso

securitasdirect. (15 de Octubre de 2018). Obtenido de https://www.securitasdirect.es/es/alarma-securitas-direct/sirena-de-alta-potencia

simon. (s.f.). Obtenido de https://bricoladores.simonelectric.com/seguridad-en-el-hogar-que-debemos-proteger

simon. (17 de Mayo de 2018). Obtenido de https://bricoladores.simonelectric.com/seguridad-en-el-hogar-que-debemos-proteger

tvc. (2019). Obtenido de https://www.tvc.mx/shop/catalog/product_info.php?products_id=6352

Valois, M. A. (22 de mayo de 2018). *HostGator*. Obtenido de https://www.hostgator.mx/blog/internet-de-las-cosas/

Velasquez, J. (21 de julio de 2011). Obtenido de http://julianvelasquez7546gta.blogspot.com/2011/07/definicion-de-xampp.html

Yubal. (03 de Agosto de 2018). *Xataka*. Obtenido de https://www.xataka.com/basics/que-arduino-como-funciona-que-puedes-hacer-uno

ZCacceso. (s.f.). Obtenido de https://dahua.lat/images/kit-de-camaras-dahua.jpg?crc=3965479366

zonamaker.com. (2014). Obtenido de https://www.zonamaker.com/arduino/modulos-sensores-y-shields/sensor-pir-para-la-deteccion-de-presencia

ANEXO

Los módulos y el código de este proyecto se puede descargar de la página de github en el siguiente enlace:

https://github.com/LizethCruz/Sistema_seguridad.git

MANUAL DE USUARIO

Ese manual presenta las funciones del equipo

DESCRIPCION GENERAL

Con la finalidad de proteger hogares, residencias el sistema de SiSegIot fue desarrollado para evitar la invasión de intrusos en el área protegida.

La protección es a través de la electrificación de alambrado que constituye la cerca eléctrica, junto a su sirena, además la puesta de cámaras de seguridad, todo esto controlado desde una página web.

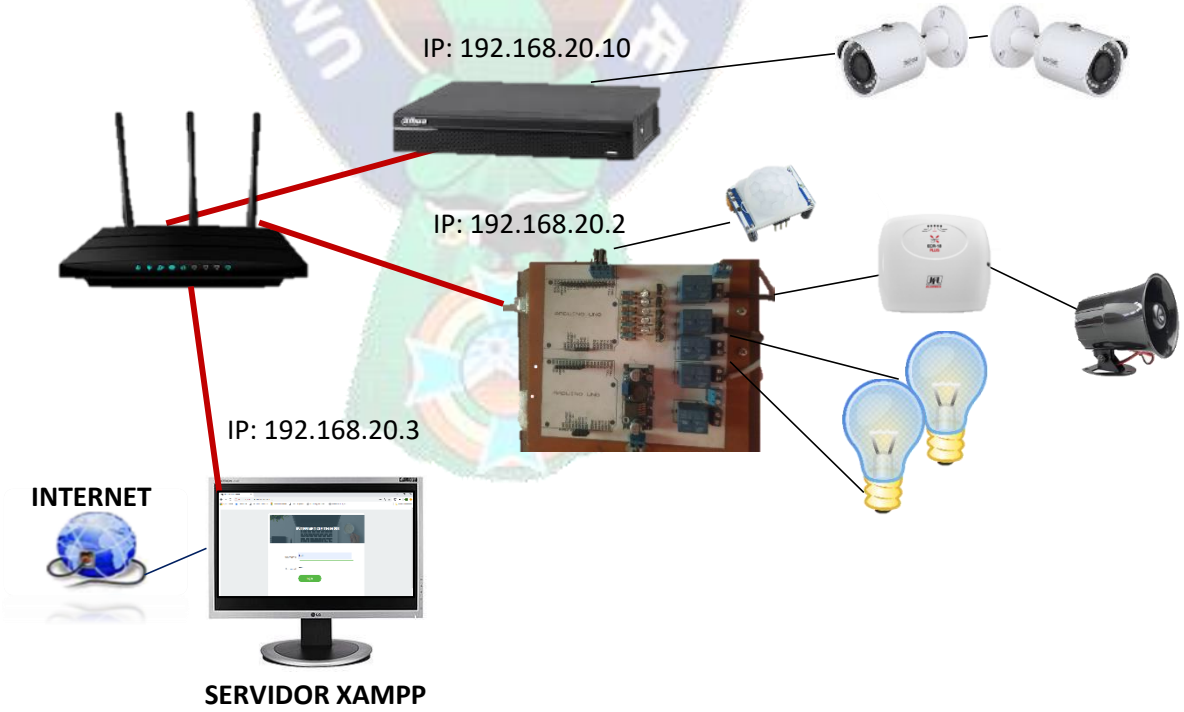
Se aconseja que las cercas estén sobre muros o al menos 2 metros de altura para evitarse accidentes con personas que no tienen intención de invadir el área protegida.

En cuanto a las cámaras se aconseja instalar en lugares estratégicos de la residencia para una mejor visión.

INSTALACION

Router TP-Link

Activar el botón de WIFI del router y conectar mediante el cable de red al DVR de las cámaras de seguridad y a la placa del circuito donde controla los demás componentes.



Cerco eléctrico

Para instalar el electrificador, elija un lugar discreto y protegido contra fenómenos climáticos muy fuertes y fije la base a la pared. Este lugar debe ser de fácil acceso para eventuales casos de mantenimiento y monitoreo del equipo. No instale el electrificador en estructura metálica, porque podrá ocurrir fuga de tensión entre la salida del electrificador y la estructura. Los cables de alta tensión no pueden pasar juntos al cable de energía eléctrica, teléfono, sirena y sensores y deben tener una distancia de más o menos 4cm uno del otro.

<u>Herramientas</u>

Electrificador

Alambre galvanizado

Aislador para cerca electrica

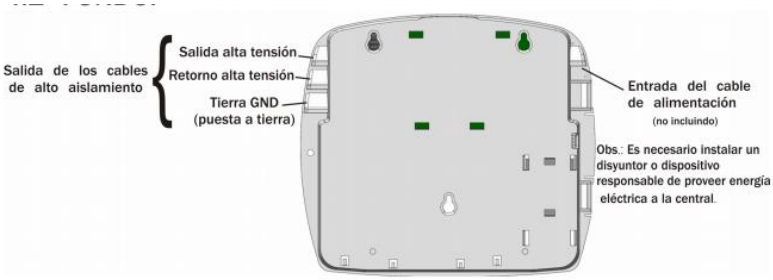
Cable de alta tension

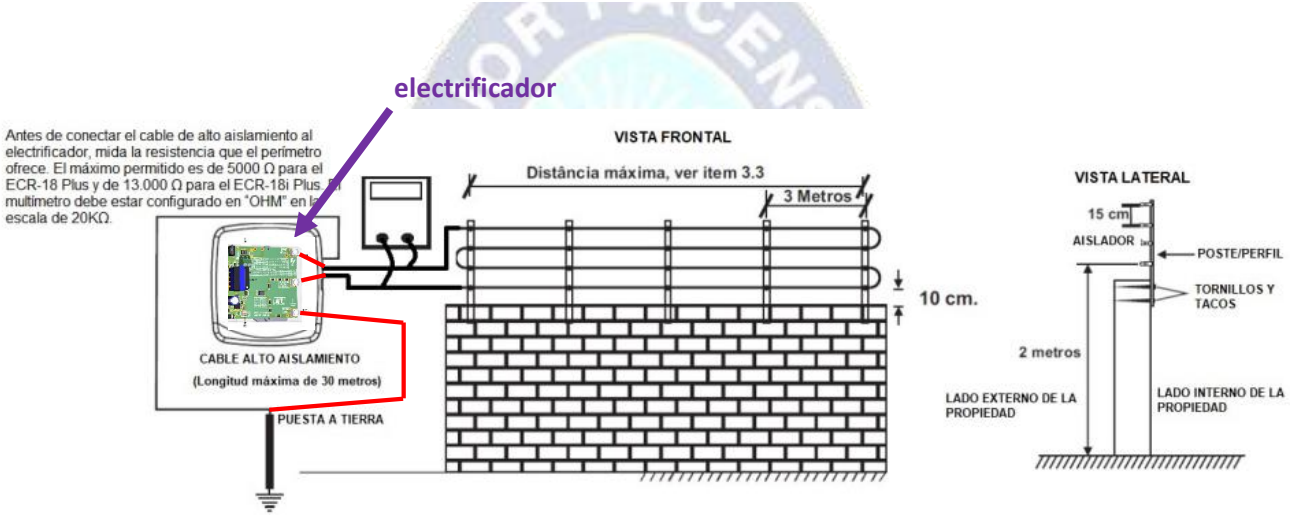
Cartel de peligro

jabalina

poste

Instalación





Advertencias

- No instalar la central en lugares sin ventilación, húmedos, cercana a fuentes de calor o vibraciones.

- Evitar la instalación de la central en paredes expuestas a la incidencia del sol, detrás de puertas, debajo de ventanas o en lugares de intensa circulación de personas.

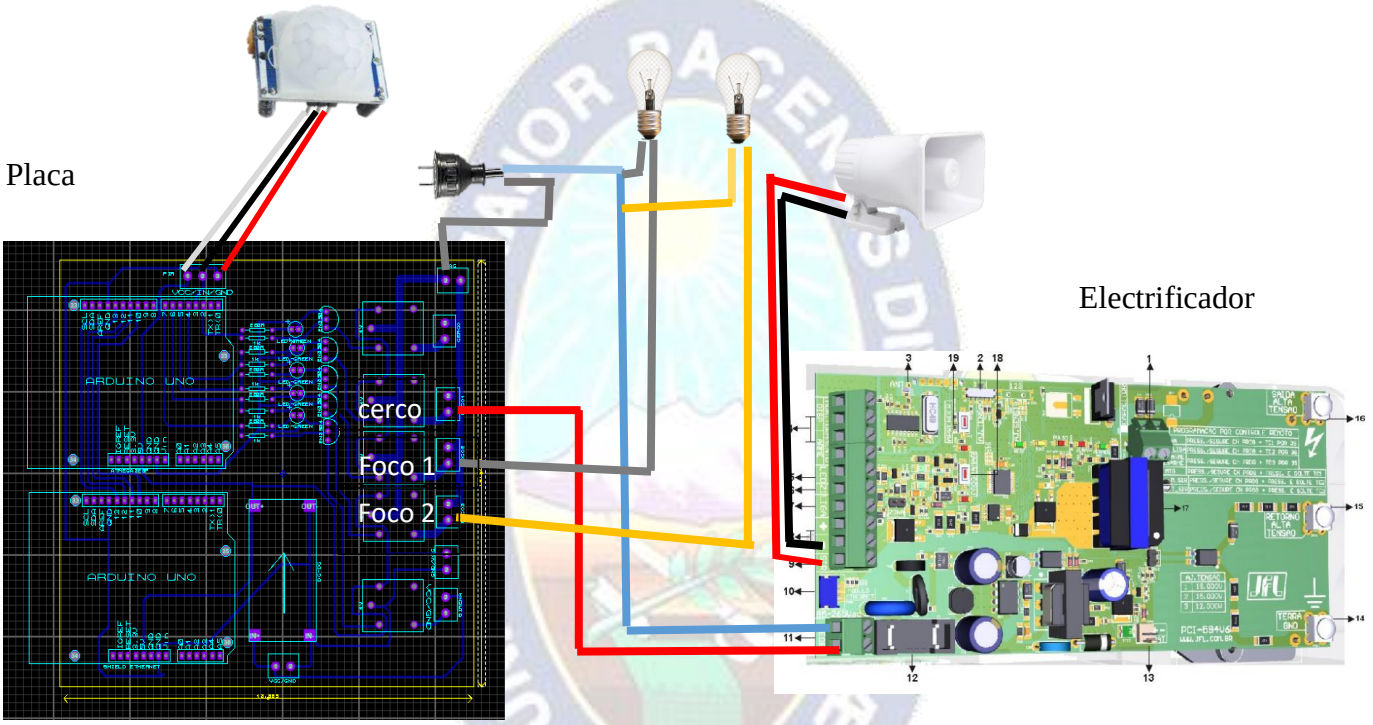
- No instalar la central cercana a cables de energía eléctrica que puedan generar interferencias en el equipo.

- No instalar la central cercana a televisores o equipos que trabajen con radiofrecuencia.

Placa del circuito

Para instalar la placa, elija un lugar discreto y protegido en la pared. Este lugar debe ser de fácil acceso para eventuales casos de mantenimiento, la placa controla los focos, recibe datos del sensor PIR, y el manejo del cerco eléctrico de la siguiente manera:

Placa



Electrificador

Cámaras de seguridad

Estos dispositivos deben ser instalados en lugares estratégicos de la vivienda, para una ejor visión.

Herramientas

DVR Dahua

Cámaras

Cargador de camaras

Cargador de camaras

Cables de conexion

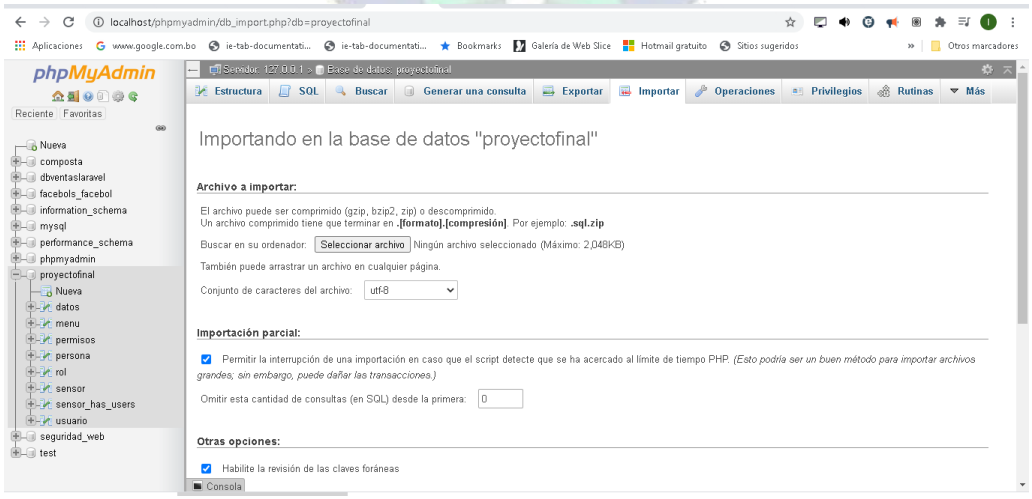
Instalación

http://www.overgroupnet.com/comun/descargar.asp?ruta=descargas&nombre=manual_ahd_traduccion_espa%F1ol2.pdf

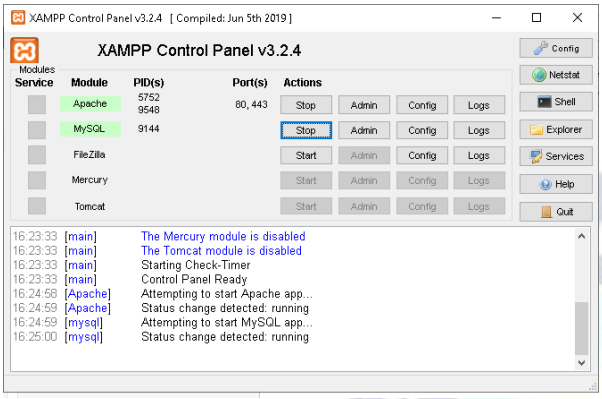
Pagina Web

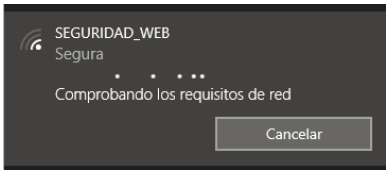
Instalar el servidor XAMPP donde estará alojado la pagina web, copiar la carpeta de **code123 y seguridad_php** en la siguiente ruta: C:\xampp\htdocs donde contiene todo el sistema que controla todos los componentes.

Crear una base de datos e importar **proyectofinal.sql**

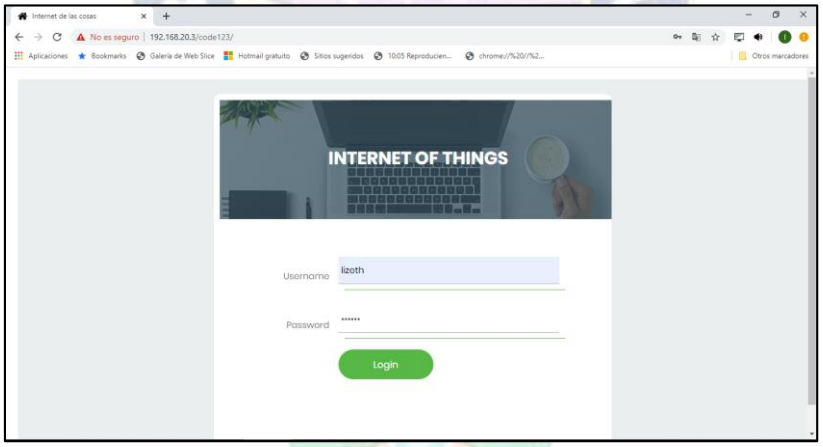


Inicializar Apache , MySql de xampp y conetctarse al WIFI seguridad_web .

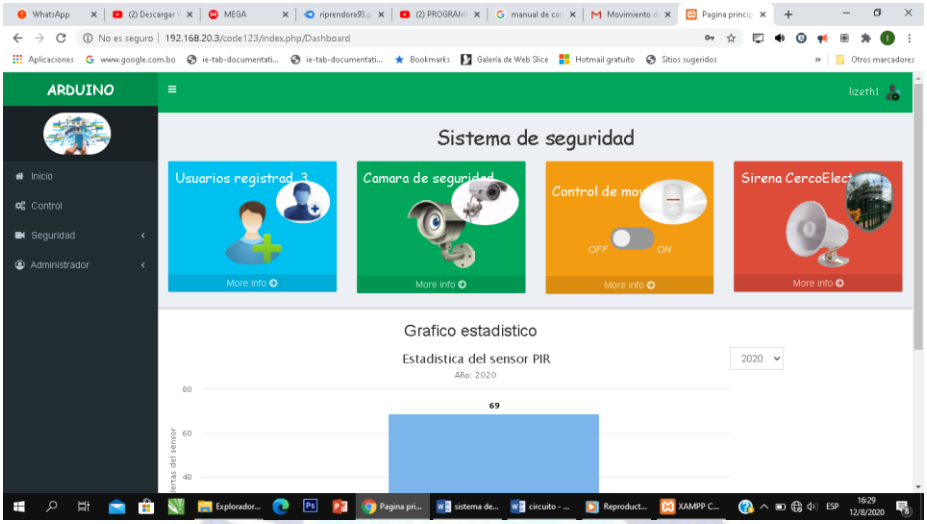




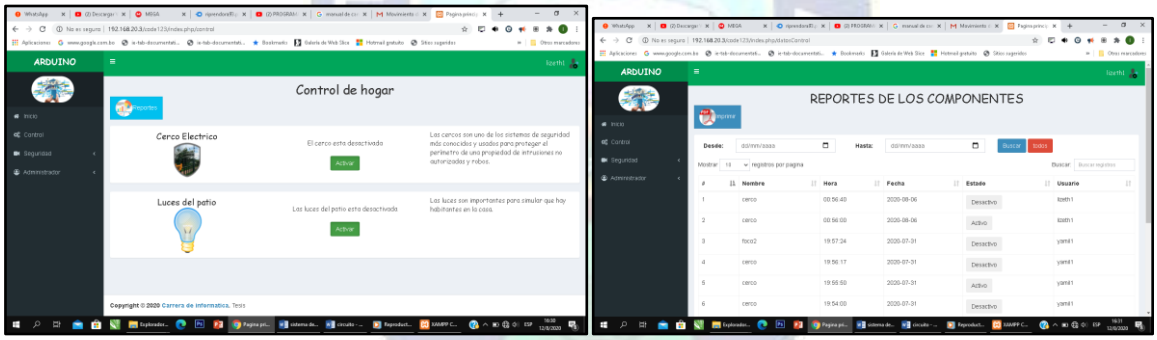
Abrir el navegador y copiar lo siguiente: http://192.168.20.3/code123/ para la pantalla de autentificación de la página ya sea por vía teléfono inteligente o pc.



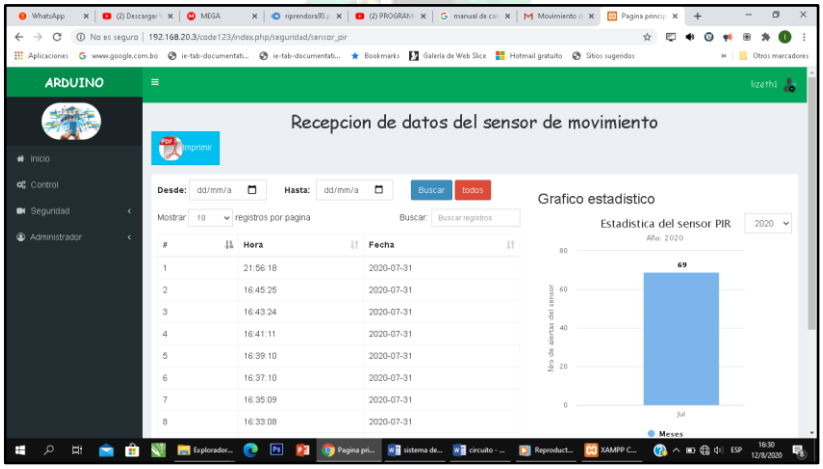
Pagina principal de la pagina web



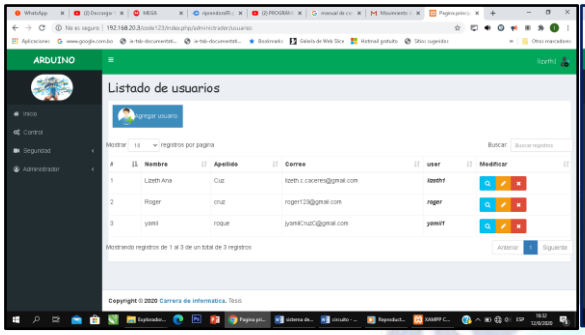
Control de los componentes del cerco el foco

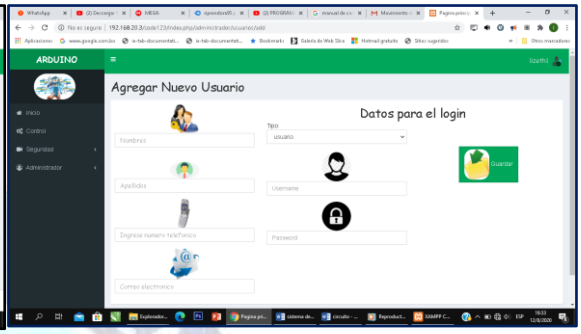


Historial del sensor PIR, cada vez que capte presencia cerca del lugar

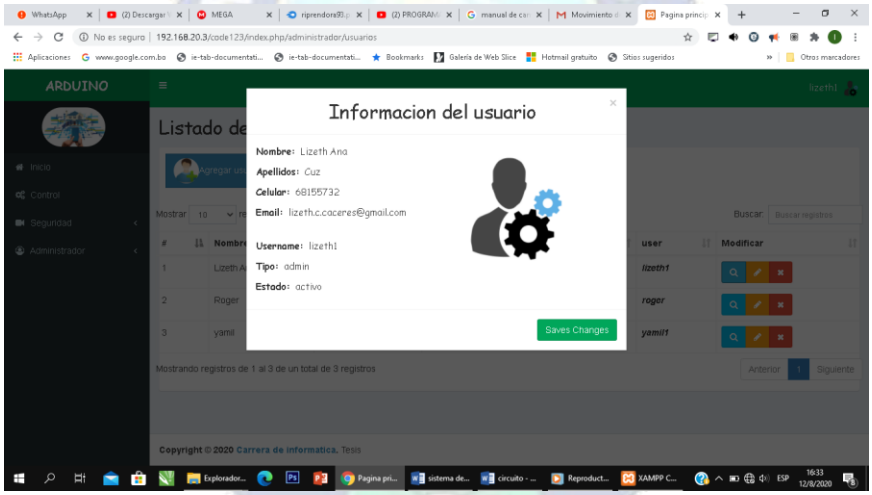


Gestión de usuarios, donde solo el usuario con el rol de administración podrá agregar demás usuarios que manipularan el sistema.

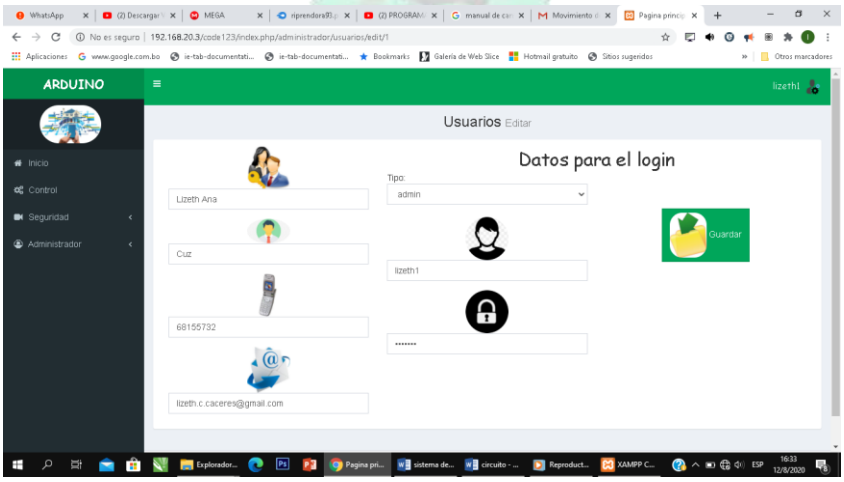




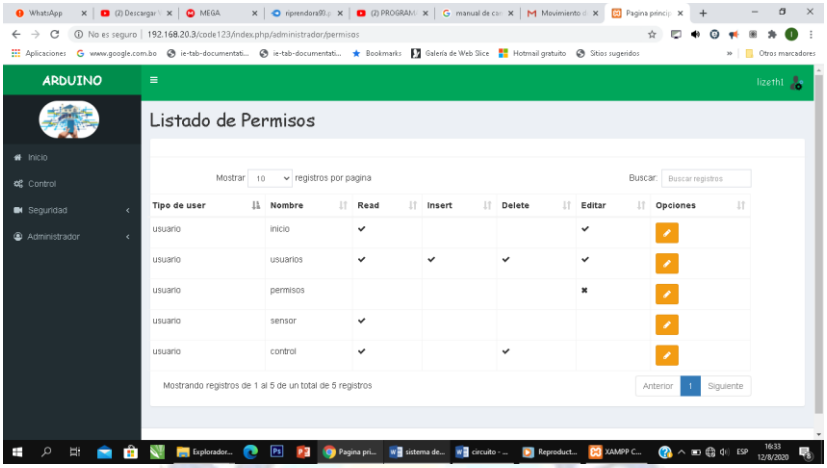
Información del usuario



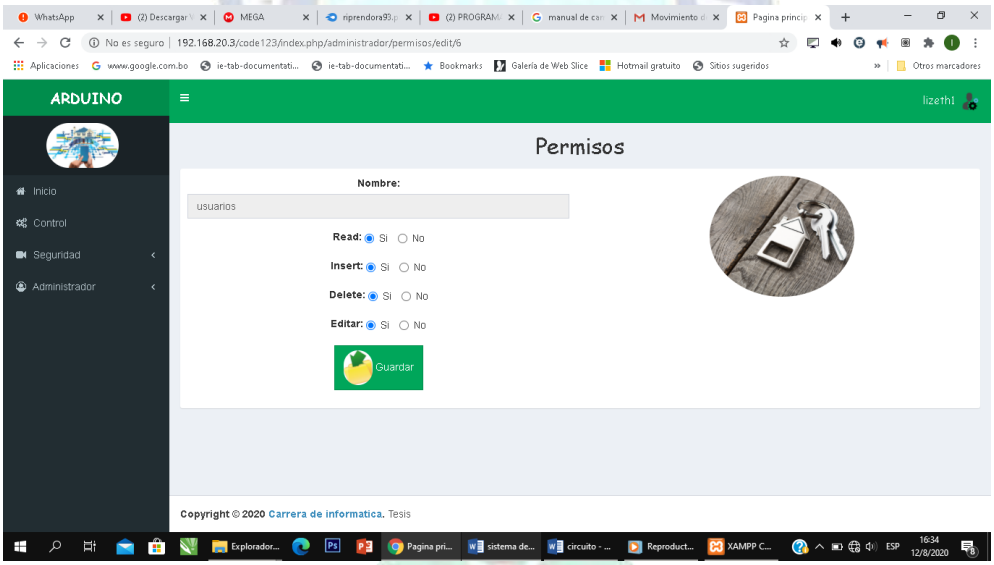
Editar usuarios



Permisos para el rol de usuario para cada modulo del sistema



Cambio de permiso para cada módulo del sistema



La Paz, de octubre de 2020

Señor:

Lic. Eufren Llanque

Director de la Carrera de Informática

Facultad de Ciencias Puras y Naturales

Presente

Ref. Aval para la defensa de Tesis de Grado

De mi consideración.

Me dirijo a su distinguida autoridad, para informarle en calidad de tutora metodológica que la universitaria **LIZETH CRUZ CACERES** con C.I. **9125953** L.P. concluyo la tesis de grado.

SISTEMA DE SEGURIDAD BASADO EN EL INTERNET DE LAS COSAS PARA VIVIENDAS URBANAS

Cumpliendo con el contenido requerido, por lo que solicito se de curso a la defensa publica, para optar al título Licenciatura en Informática, mención: Ingeniería en Sistemas Informáticos, de acuerdo a las normas reglamentarias de la Universidad Mayor de San Andrés.

Sin otro particular me despido de su persona, con las consideraciones más distinguidas.

Atentamente

.....

M.Sc. Rosa Flores Morales
TUTOR METODOLOGICO

Señor

M.Sc. Rosa Flores Morales
Tutor Metodológico

Presente

Ref. Conformidad y Aval de Tesis de Grado

De mi consideración.

Tengo a bien dirigirme a su persona, para darle a conocer que luego de efectuar, el seguimiento a la estructura y contenido de la Tesis de Grado, titulada "SISTEMA WEB BASADO EN INTERNET DE LAS COSAS" elaborada por el postulante Justina Janco Perca con C.I. 6185801 LP, y habiendo el mismo realizado las respectivas correcciones a mis observaciones, y no existiendo impedimento alguno en la propuesta, me corresponde **dar mi AVAL**, para la respectiva defensa pública, de acuerdo a normas y reglamentos universitarios vigentes.

Sin otro particular, me despido de usted con las consideraciones más distinguidas.

Atentamente.

Ph.D. Yohoni Cuenca Sarzuri
ASESOR