ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UN CONTROL AUTOMATIZADO Y DE ACCESO EN LAS AULAS 34, 35 Y 36 DE LA ESFOT-EPN.

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

DIEGO ANDRÉS RUIZ ALBÁN

diego.ruiz@epn.edu.ec

EDGAR SEBASTIÁN VERDUGO BERMEO

edgar.verdugo@epn.edu.ec

DIRECTOR: Ing. FANNY PAULINA FLORES ESTÉVEZ, MSc.

fanny.flores@epn.edu.ec

CODIRECTOR: Ing. WILLIAM FERNANDO FLORES CIFUENTES, MSc.

fernando.flores@epn.edu.ec

Quito, Febrero 2020

DECLARACIÓN

Nosotros, Diego Andrés Ruiz Albán y Edgar Sebastián Verdugo Bermeo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

Sin perjuicio de los derechos reconocidos en el primer párrafo del artículo 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación -COESC-, somos titulares de la obra en mención y otorgamos una licencia gratuita, intransferible y no exclusiva de uso con fines académicos a la Escuela Politécnica Nacional. Entregaremos toda la información técnica pertinente. En el caso de que hubiese una explotación comercial de la obra por parte de la EPN, se negociará los porcentajes de los beneficios conforme lo establece la normativa nacional vigente.

DIEGO ANDRÉS RUIZ ALBÁN

EDGAR SEBASTIÁN VERDUGO BERMEO

CERTIFICACIÓN

Certificamos que el presente documento fue desarrollado por Diego Andrés Ruiz Albán y Edgar Sebastián Verdugo Bermeo, bajo nuestra supervisión.

Ing. Fanny Flores MSc.	Ing. Fernando Flores MSc.
DIRECTOR DE PROYECTO	**CODIRECTOR DE PROYECTO**

AGRADECIMIENTO

Agradecemos el apoyo y respaldo brindado a cada uno de nuestros familiares, quienes, han sido el motor y pilar fundamental de este logro, agradecemos también a la Escuela Politécnica Nacional por darnos acogida ya que fue nuestra segunda casa durante toda esta larga carrera universitaria.

De igual manera, agradecer a todos y cada uno de los docentes que fueron parte de nuestra formación académica y que con sus enseñanzas supieron insertar conocimientos importantes que permitieron que la carrera sea mucho más interesante.

De manera especial, agradecer a la Ing. Fanny Paulina Flores Estévez, MSc quien es nuestra tutora de tesis y ha sido nuestro apoyo y guía durante todo este proyecto, y además, por haber entregado toda su pedagogía y conocimiento para impartir clases en materias relevantes e importantes de nuestra carrera.

Para finalizar, agradecer a nuestros compañeros y amigos que han estado en todo momento compartiendo y ayudando para que todo este logro sea mucho más sencillo.

Diego Ruiz, Sebastián Verdugo B.

DEDICATORIA

El presente proyecto lo dedico especialmente a mis padres y hermana, por el apoyo constate que me dieron desde el momento en el que les informé que entraría a estudiar en la EPN, brindándome consejos para ser la persona que soy hoy por hoy, gracias a los valores que he recibido como es la puntualidad, respeto, humildad, responsabilidad y muchos más.

He podido alcanzar una meta muy importante en mi vida para de esta manera llenar de orgullo a mi familia y seguir avanzando para conseguir más logros personales y así poder llegar al éxito paso a paso.

Diego Ruiz

Este proyecto va dedicado para mis padres y hermanos, quienes, me han apoyado durante toda mi carrera, ellos han sido el pilar fundamental y han puesto toda su confianza en mí, apoyándome desde cualquier lugar y sobre cualquier circunstancia.

Es un honor poder llenar de felicidad y orgullo a mi madre, quien, con todo su amor siempre ha estado a mi lado dándome consejos, valores y sobre todo depositando mucho apoyo y amor en mí.

Una meta más cumplida, a pesar de las adversidades y de todo el difícil camino que logré superar, me auto felicito por no haber defraudado a mi familia y por lograr obtener un título en la mejor universidad del país.

Sebastián Verdugo B.

ÍNDICE DE CONTENIDO

ÍNIDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Debido al número considerable de estudiantes y personas ajenas a la Escuela de Formación de Tecnólogos (ESFOT), que ingresaban a las aulas 34, 35 y 36 sin autorización para realizar actividades no académicas como el consumo de alimentos o bebidas alcohólicas, o la realización de actos impúdicos, se provocó el deterioro de las instalaciones. Esta situación se debía principalmente a que varias personas que no pertenecían a la ESFOT tenían copias de las llaves de las aulas y esto facilitaba el acceso a cualquier persona; además, la falta de control y seguridad en las ventanas propiciaba a que ciertas personas las utilicen como medio de acceso a las aulas.

Con el fin de solventar este problema, se implementó un sistema biométrico que permita realizar el control de acceso en las aulas 34, 35 y 36 de la ESFOT-EPN. De este modo, se permite el ingreso únicamente a los profesores que utilizan estas aulas, y de acuerdo con el horario asignado por las autoridades de la ESFOT. Los profesores podrán ingresar únicamente con el ingreso de sus huellas dactilares, previamente registradas. Para este fin se optó por el modelo SF300 de la marca ZKTeco, que incorpora comunicación TCP/IP.

Además, se desarrolló un sistema automatizado que permite el monitoreo de puertas y ventanas, verificando si se encuentran abiertas o cerradas. Adicionalmente no solo se registra el estado de las luminarias permitiendo conocer si se encuentran encendidas o apagadas, sino que el sistema permite controlar desde la Dirección de la ESFOT, el encendido y apagado de las mismas. Para ello se instaló sensores magnéticos, que son empleados para verificar el estado de puertas y ventanas. Los cables de los sensores se conectan a un módulo Arduino Mega, el cual realiza las funciones del control automatizado.

Se realizó la instalación de todo el sistema que corresponde a la colocación de los biométricos junto a sus cables de red como de alimentación, colocación de sensores en puertas y ventanas, recorrido del cable proveniente de cada elemento instalado en el sistema hacia su respectivo destino.

Finalmente, se procedió con todas las pruebas correspondientes, verificando el ingreso a las aulas únicamente con las huellas dactilares de los profesores y la lectura de sensores desde el Arduino y del sistema de control, creado por los estudiantes de Análisis de Sistemas Informáticos.

Palabras clave: automatización, implementación, cableado estructurado, biométrico, registro

ABSTRACT

Due to the considerable number of outside students and people, who enter into classrooms 34, 35 and 36 without authorization to perform non-academic activities such as the consumption of food or alcoholic beverages, or the performance of impudent acts, the deterioration of the facilities was caused. This situation was mainly due to the use of classroom keys to obtain copies of them, giving anyone easier access, in addition to the lack of control and security in the windows, which led to certain people using them as a means of access to the classrooms.

In order to solve this problem, a biometric system has been implemented to allow access control in classrooms 34, 35 and 36 of ESFOT-EPN. In this way, only teachers using these classrooms are allowed to enter in accordance with the schedule assigned by ESFOT authorities. Teachers will be able to enter only with the entry of their fingerprints, previously registered. For this purpose, The ZKTeco brand SF300 model was chosen, which includes TCP/IP communication.

In addition, an automated system was developed that allows the monitoring of doors and windows, checking if they are open or closed. In addition, the status of the luminaires is recorded allowing to know if they are on or off ;moreover, from ESFOT Direction the system allows to control their on/off switch. Thus, electromagnetic sensors were installed, which are used in order to test the doors and windows status. Sensor cables are connected to an Arduino Mega module, which performs the functions of automated control.

The deployment of the entire system corresponding to the biometrics installation, as well as its network cables, a power supply, the placement of sensors in doors and windows, cable path from each element installed in the system to its respective destination was carried out.

Finally, all the corresponding tests were carried out, verifying the entrance to the classroom only with the fingerprints of the teachers and the reading of sensors from the Arduino and the control system, created by the students of Informatic Systems Analysis.

***Key words**: automation, implementation, structured cabling, biometric, registration*

1. INTRODUCCIÓN

Los índices vandálicos que afectan a la Escuela de Formación de Tecnólogos (ESFOT) han sido un problema grave de seguridad que perjudica a estudiantes, profesores, personal de limpieza, personal administrativo y sobre todo a la infraestructura de las aulas. Es por ello que el presente proyecto está pensado en implementar un control automatizado y de acceso en las aulas 34, 35 y 36 de la ESFOT, debido a que dichas aulas eran lugar para que estudiantes y personas ajenas a la institución, ingresen a ingerir bebidas alcohólicas, consumir alimentos y realizar otro tipo de actividades que no contaban con ningún permiso por parte de las autoridades de la ESFOT.

Con estos antecedentes, se procede a realizar el diseño del sistema de control automatizado que permite monitorear con ayuda de un módulo Arduino y una *shield ethernet* el estado en el que se encuentren ventanas (abiertas o cerradas), puertas (abiertas o cerradas) y luminarias (prendidas o apagadas), permitiendo encender o apagar las luminarias remotamente. Además, se realiza el diseño del control de acceso, el cual contempla la utilización de biométricos marca ZKTeco modelo SF300, el mismo que permite la configuración de niveles de acceso para que solo los profesores registrados puedan ingresar a las aulas en las cuales tengan que dictar su materia. Adicionalmente, la comunicación TCP/IP que manejan dichos equipos, permite conexión a la red para un monitoreo permanente.

Con la implementación del control automatizado y de acceso, se procede a realizar sus respectivas pruebas de funcionamiento, las mismas que serán realizadas desde el servidor el cual contiene el *software* ZK Access 3.5, correspondiente al manejo y configuración de los biométricos; además, contiene el aplicativo que permite realizar el monitoreo del sistema implementado.

Cabe mencionar que el proyecto forma parte de un macroproyecto que tiene como finalidad la automatización de las 19 aulas de la ESFOT sin tomar en cuenta los laboratorios.

Dicho macroproyecto estuvo a cargo de 12 estudiantes de Electrónica y Telecomunicaciones encargados de implementar el control de acceso y el diseño de red, 8 estudiantes de Electromecánica quienes armaron el tablero de control que permite la automatización de las aulas y 2 estudiantes de Análisis de Sistemas Informáticos encargados de implementar el servidor que permite el monitoreo del sistema.

1.1. Marco teórico

Arduino Mega

Arduino es un dispositivo que cuenta con un microcontrolador instalado sobre una placa impresa; tanto su *hardware*, como su lenguaje de programación son libres. Existen varias placas de Arduino en el mercado; la que se utilizó en el proyecto es Arduino Mega 2560. [1]

Debido a la cantidad de entradas y salidas que se requería en el proyecto, la mejor elección fue optar por el modelo Arduino Mega el cual, a diferencia del Arduino Uno, cuenta con una cantidad mayor de pines, lo que favoreció en la utilización de una sola placa que controla la automatización de las aulas, evitando el uso de más módulos Arduino.

Las características principales de la placa utilizada incluyen: 54 pines para entradas y salidas digitales, 16 entradas analógicas y 4 receptores/ transmisores serie, posee una memoria *Flash* de 256 (KB), memoria SRAM de 8 (KB) y una EEPROM DE 4 (KB). El voltaje con el que trabaja esta placa Arduino es de 5 (V_{DC}) y una corriente máxima de 40 (mA). [2]. En la figura 1.1 se presenta una placa Arduino Mega.

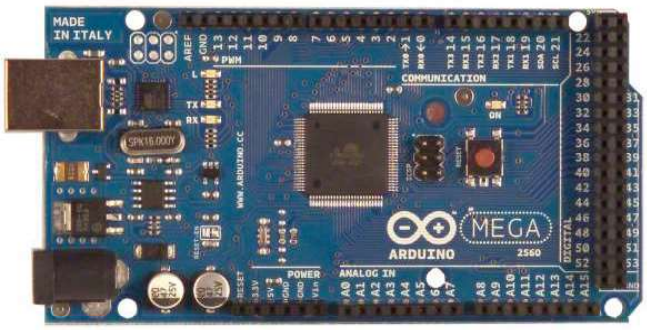

Figura 1.1 Arduino Mega *[3]*

Shield Ethernet

Las placas Arduino permiten acoplar otras placas en su parte superior, a través de sus pines, sin tener que utilizar cables; esto facilita la funcionalidad de la placa Arduino. A este tipo de placas se les denomina *shield***.** Los pines que comparten una placa Arduino con una *shield* son RESET, GND, AREF, 5 (V_{DC}), 3 (V_{DC}). [1]

Existen varios modelos de *shield* cada uno con una función específica; un claro ejemplo es la *shield ethernet*, la cual permite una conectividad de red utilizando el protocolo TCP/IP, por medio de un cable de red. [1]

Una vez montada la *shield* en la placa Arduino, se tiene que pasar la programación de manera normal a la placa mediante su puerto USB; la información correspondiente a la *shield* se pasará de manera inmediata. Del conector RJ45 que lleva incorporado la *shield*, se conecta un cable de par trenzado que puede ser de categoría 5 o 6. Si se desea conectar a una computadora, se debe usar un cable cruzado, pero si se va a conectar a un *switch* o *router* se utiliza el cable estándar. [2] En la figura 1.2 se presenta una placa *shield ethernet*.

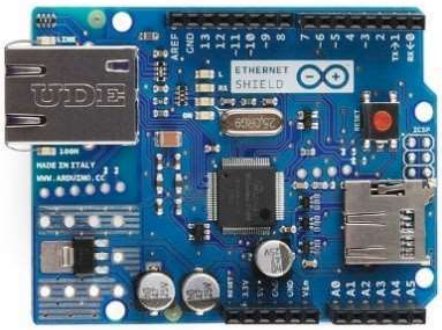

Figura 1.2 Shield Ethernet *[4]*

Sensores magnéticos

Los sensores magnéticos son aquellos que permiten efectuar o detectar mediciones cuando no existe algún tipo de contacto, dando señales de alta precisión y en tiempo real.

Los sensores magnéticos tienen un magneto resistivo dentro de su estructura, el cual, al estar en contacto con un imán funciona como un interruptor dejando así, pasar la corriente.

Los sensores magnéticos funcionan cuando detectan la presencia de un imán que provee campo magnético, los polos del magneto resistivo son sensibles y rápidos de accionarse para que la corriente circule [5].

- **Sensores magnéticos tipo interruptor reed**

  Estos sensores son ideales para cerraduras de puertas y ventanas, ya que al manipularlas cambian de estado; abierto o cerrado.

  Son sensores normalmente abiertos que se accionan o funcionan a la presencia de un campo magnético, cerrando el circuito y dejando pasar la corriente.

  En la Figura 1.3 se puede apreciar el sensor magnético con el imán que cierra el contacto [6].

Figura 1.3 Sensores magnéticos interruptores tipo reed [6]

Switch D-Link

Un *switch* es un dispositivo que permite conectar varios elementos dentro de una misma red. Su función principal es la de actuar como un controlador que permite a los elementos conectados en red comunicarse entre ellos, compartiendo su respectiva información. [7]

Existen *switches* no administrables, los cuales no requieren de programación para su funcionamiento; es decir, funcionan de manera automática sin permitir que se realicen cambios. [7]

El *switch* D-LINK no administrable de 8 puertos cuenta con una velocidad de 10/100 (Mbps) en cada puerto, lo que permite configurar de manera automática a cualquier red cableada. Cada puerto permite el cruce automático MDI/MDIX, lo que facilita el uso de cables que no sean cruzados. [8] En la figura 1.4 se presenta el *switch* D-Link no administrable.

Figura 1.4 *Switch* D-LINK no administrable de 8 puertos [9]

Biométrico ZKTeco SF300

El biométrico ZKTeco SF300 es un dispositivo que permite la identificación y verificación de un individuo por medio de sus características físicas o la biometría del cuerpo humano, como es la huella dactilar, el iris del ojo, forma facial, etc. [10]

Los procesos en los que se basa un biométrico ZKTeco SF300 son tres [11] y se presentan resumidos en la Figura 1.5.

1. Inscripción. **-**en este proceso se adquiere la información biométrica del individuo para posteriormente ser procesada en un patrón.

2. Base de datos. **-**el patrón biométrico que ha sido obtenido se lo almacena en una base de datos para ser utilizado por el siguiente proceso.

3. Reconocimiento. **-**es el acceso que se le da al usuario previamente de la obtención de su rasgo biométrico, creando un patrón que ha sido almacenado en una base de datos para ser comparada en el instante que el usuario requiera.

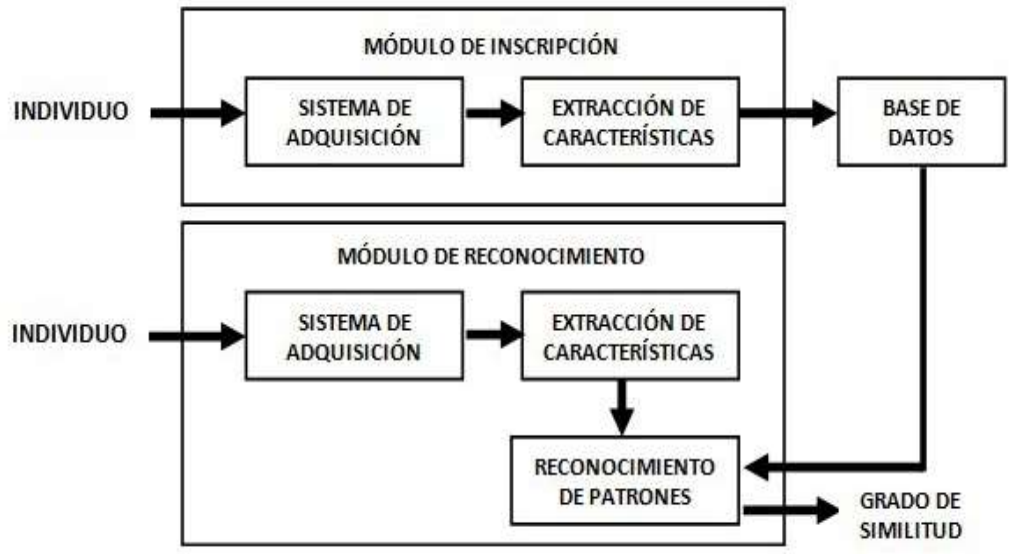

Figura 1.5 Proceso biométrico ZKTeco SF 300 [11]

El biométrico de la marca ZKTeco del modelo SF300 permite realizar las funciones de control de acceso, asistencia y gestión de tiempo. Cuenta con una salida *Wiegand*, lo que permite conectar a otro dispositivo como maestro o esclavo [12]. En la Figura 1.6 se presenta el biométrico ZKTeco SF 300 y cumple con las especificaciones técnicas mencionadas a continuación.

- **Especificaciones técnicas** [12]
    - Pantalla táctil LCD de 2.8 pulgadas.
    - Capacidad para 1500 huellas y 80 000 eventos.
    - Capacidad es para 5000 tarjetas magnéticas.
    - Comunicación TCP/IP o RS485.
    - Puerto USB para administración de datos.
    - Alimentación de 12 (V_{DC}) y 3 (A).
    - Sensor óptico ZK 500 (DPI).
    - Dimensiones105x105x32 (mm).
    - Tiene una interfaz de acceso para cerradura eléctrica, timbre, sensor de puerta, botón de salida.
    - Temperatura de trabajo entre 0 a 45 (°C) y de humedad entre 20 % a 80 %.
    - Multilenguaje.
    - Audio de rechazo o aceptación.
    - Interruptor anti-sabotaje.

Figura 1.6 Biométrico ZKTeco SF300 [12]

Enroladora ZK4500

Es un dispositivo que permite inscribir a un usuario en un *software* como por ejemplo en el *software* ZK Access 3.5, registrando su huella dactilar a través de un sensor óptico; puede ser utilizado en aplicaciones o biométricos. [13]

Este modelo permite obtener la huella digital en un archivo JPG de alto rendimiento, y su sensor de huellas no requiere de mantenimiento. [14]

La acción de registro de huella se realiza conectando la enroladora a un computador mediante su interfaz USB, también cuenta con un LED que indica el estado en que se encuentra el dispositivo. [14] En la Figura 1.7 se muestra la enroladora ZK4500.

- **Especificaciones técnicas** [14]
  - Sensor óptico
  - Resolución 500 (DPI)
  - Tamaño de imagen 280x360 pixel.
  - Compatibilidad con Windows XP, Windows Vista y Windows 7.

Figura 1.7 Enroladora ZK4500 [14]

Normas de Cableado Estructurado

- **Norma UNE EN 55022/A2: 2004 55024/A2:2004**

Esta norma trata acerca de las recomendaciones que se debe tener con temas de compatibilidad electromagnética, para evitar que interferencias electromagnéticas interfieran en la comunicación de datos. [15]

Los cables correspondientes a la red no deben pasar cerca de posibles fuentes que produzcan radiaciones electromagnéticas como son: luminarias fluorescentes, líneas de energía o equipos que produzcan un efecto magnético. [15]

Esta norma menciona parámetros a utilizar como son las distancias mínimas de 30 cm para las líneas de energía, además que todo cruce entre líneas deberá ser realizado en ángulo recto. [15]

- **Norma ANSI/TIA 606A**

Esta norma es la de *"Administración y etiquetado para la infraestructura de telecomunicaciones en edificios comerciales",* la cual menciona las principales directrices para administrar y etiquetar de manera correcta cables, equipos, espacios entre otros elementos del sistema de cableado estructurado. [15]

Para la gestión del cableado, se utiliza un *software* que contiene herramientas para facilitar el diseño, instalación, mantenimiento y organización. Accediendo así fácilmente a los planos de todo el cableado, evidenciando sus rutas de donde sale hacia su destino, con su respectiva etiqueta. [15]

- **Norma ANSI/TIA 568-B**

Esta norma define el cableado de telecomunicaciones para edificios comerciales. La norma indica el orden y encajado que deben seguir los hilos de cobre dentro de los conectores RJ45, RJ49, ver Figura 1.8. El orden es el siguiente. [16]

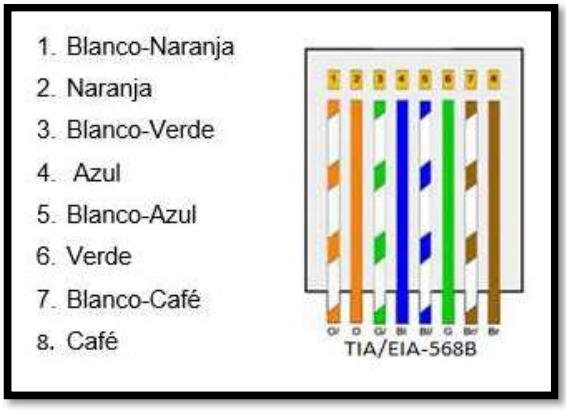

Figura 1.8 Norma de ponchado ANSI/TIA 568-B [16]

- **Norma ANSI/TIA 569**

Esta norma se refiere a la construcción comercial para espacios y recorridos de telecomunicaciones, en donde constan los siguientes elementos para espacios y recorridos al diseñar construcciones de telecomunicaciones. [17]

- Cableado o recorrido horizontal
- Armario de telecomunicaciones
- Cableado o recorrido en *Backbone*
- Sala de equipos
- Estación de trabajo
- Sala de entrada de servicios

Cable UTP

El cable UTP, más conocido como cable de red, es un cable sin protección electromagnética que no tiene blindaje y está formado por pares de hilos de cobre que se encuentran trenzados, observar Figura 1.9. El cable UTP es más utilizado para la comunicación entre dispositivos de telecomunicaciones los cuales mandan o emiten señales eléctricas. [18]

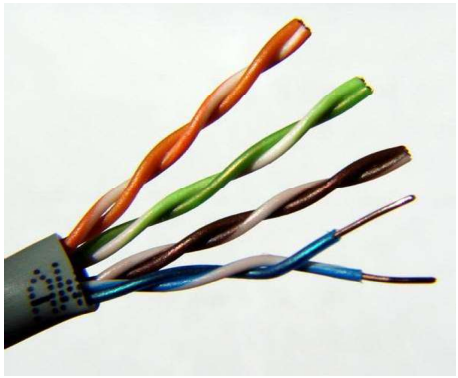

Figura 1.9 Cable UTP [18]

Debido a que la información que viaja por el cable es importante, el cable debe tener propiedades de fabricación que permitan transportar la información de forma segura y que al viajar por el cable no se pierda o llegue defectuosa.

Cada cable UTP, así como sus variantes, constan de 8 hilos separados en 4 pares. Los colores más utilizados para los cables UTP son: naranja, blanco naranja, verde, blanco verde, azul, blanco azul, café y blanco café. La ubicación de los cables cuando se poncha depende de la norma que se vaya a utilizar, las mismas, se presentan en la Figura 1.10, con su respectivo orden de colores. [19]

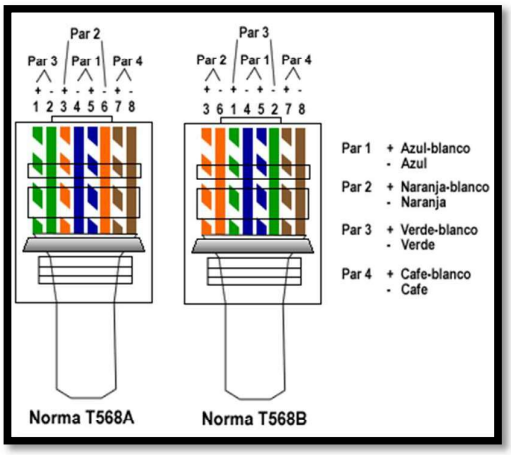

Figura 1.10 Normas de ponchado de cables [20]

Trenzado de los pares de cobre

Al usar cables sin trenzar, cuando se inserta ruido en la transmisión, el ruido siempre afecta con mayor medida al hilo más cercano, dependiendo de la dirección de la interferencia. Esto da lugar a que al otro hilo del par no le llegue la misma cantidad de ruido; por lo tanto, no es posible que se puedan cancelar estas interferencias generadas en los dos hilos del par. En la figura 1.11 se puede apreciar que el ruido afecta más al hilo que se encuentra más cerca de la interferencia cuando los hilos de un par no se encuentran trenzados. [21]

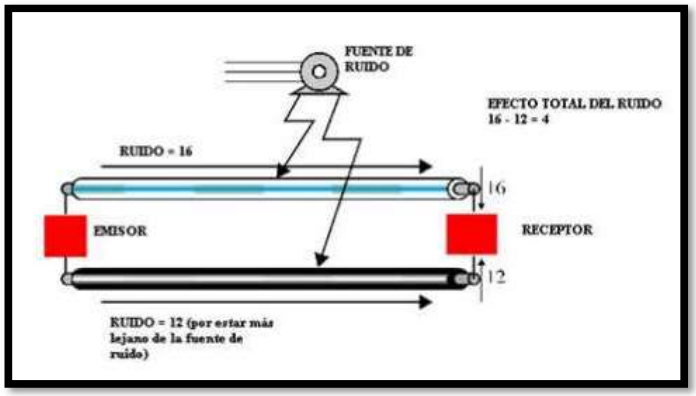

Figura 1.11 *Par de cobre sin* trenzar [21]

Cuando se utilizan pares trenzados, la cantidad de interferencia llega por igual a ambos pares; entonces, estas interferencias se podrán cancelar, anulándose el ruido generado por interferencias eléctricas. La figura 1.12 indica cómo se anula la interferencia cuando los pares son trenzados. [21]

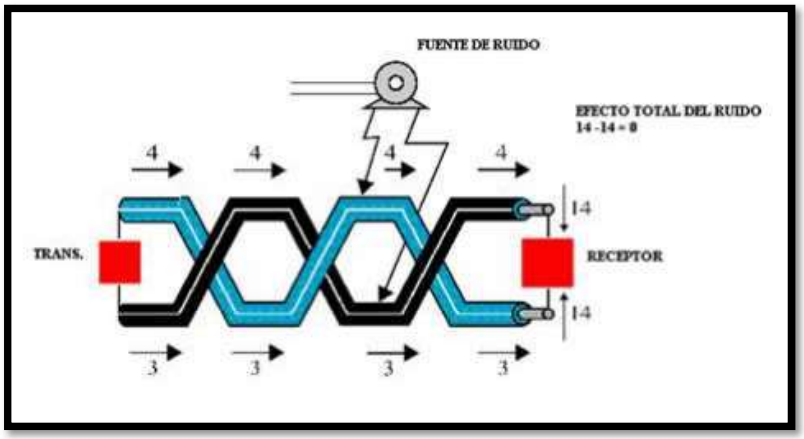

Figura 1.12 *Par de cobre* trenzado [21]

Ventajas y desventajas del cable UTP

- **Ventajas** [22]
  - Son de bajo costo y simples de usar.
  - Su instalación es sencilla y ahorra espacio comparado con otro tipo de medio de transmisión.
  - Se puede utilizar en varios conectores como: RJ45, RJ11, DB25, etc.
- **Desventajas** [22]
  - Su máxima distancia de conexión es de 100 (m).
  - Son muy tolerantes al ruido ya que no tienen blindaje.
  - Ancho de banda y velocidad limitados.

Dirección IP

La dirección IP es aquella dirección que se utiliza en la capa de red, la cual, es la tercera capa de las 7 que tiene el modelo de referencia OSI. [23] Observar Figura 1.13

Figura 1.13 Modelo de Referencia OSI [23]

La dirección IP es definida como un identificador de localización dentro de una misma red, en donde cada equipo y componente pueden comunicarse con los demás utilizando el protocolo TCP/IP. [24]

La dirección IP se clasifica en direccionamiento IPv4 e IPv6. La más utilizada es la versión 4 que está conformada por cuatro octetos; cada uno de ellos oscila entre 0 y 255. Cuentan con su respectiva máscara, la cual permite identificar qué clase es: A, B o C. [24]

2. METODOLOGÍA

El proyecto abarca el diseño de un sistema de control automatizado y de acceso, para lo cual se analizó entre varios equipos de sistemas biométricos que cumplan con otorgar el acceso a las aulas únicamente a los profesores; se optó por utilizar un módulo Arduino para el control automatizado. De esta manera se realiza el diseño de cableado estructurado, contemplando la ubicación de los biométricos, sensores, y Arduino. Tomando sus respectivas distancias para proceder a cablear cada uno de estos elementos, llegando a un tablero de control que es el responsable de generar la automatización de las aulas; para el caso del sistema biométrico todo cable de red llega a un tablero de telecomunicaciones el cual permite la conexión en red con los demás elementos. Englobado tanto el sistema de automatización como el de acceso se puede realizar dos tipos de pruebas, una directamente desde el Arduino, verificando el estado de puertas, ventanas y luminarias, y el otro accediendo al sistema creado por estudiantes de ASI en donde además de comprobar el estado de puertas, ventanas y luminarias, se puede mandar diferentes acciones como son: abrir puertas, encender o apagar luminarias.

2.1 Metodología comparativa

Existe una amplia variedad de modelos de sistemas biométricos en el mercado nacional. Cada uno cumple con una función determinada; algunos únicamente funcionan como control de acceso, otros como control de asistencia y otros que cumplen ambas funciones.

Se ha comparado los modelos de biométricos que permitan las dos funciones a la vez, para poder escoger el que más favorezca al proyecto. Se tenía que verificar que permita la configuración de horarios y restricción de acceso en un horario que no esté permitido, según la carga horaria que se configurará en dicho equipo. Para ello, la mejor opción ha sido la adquisición de un biométrico de la marca ZKTeco modelo SF300, que permite la creación de horarios con su respectiva restricción.

2.2 Metodología analítica

Con ayuda de esta metodología se pudo realizar un análisis en el cual se ha examinado el comportamiento de la *shield ethernet,* que constituye uno de los elementos principales para

realizar el control de automatización. Se ha logrado examinar la funcionalidad que existe con la placa Arduino para que ambas funcionen de manera correcta.

Se obtuvo como resultado que es importante la compatibilidad entre la placa Arduino y la s*hield ethernet,* de este modo se evita que exista pérdida de conectividad.

3. RESULTADOS Y DISCUSIÓN

El proyecto contempla varias etapas, las cuales se han desarrollado de manera concreta, siguiendo paso a paso cada una de ellas.

A continuación, en la figura 3.1 se presentan todas las etapas que conforman el proyecto. Inicialmente se procedió con el análisis de problemas, luego se analizan las posibles soluciones; posteriormente, se continuó con el diseño del sistema de control automatizado, así como el de control de acceso. Finalmente, se procedió con la implementación que concluyó con el desarrollo de las pruebas de funcionamiento.

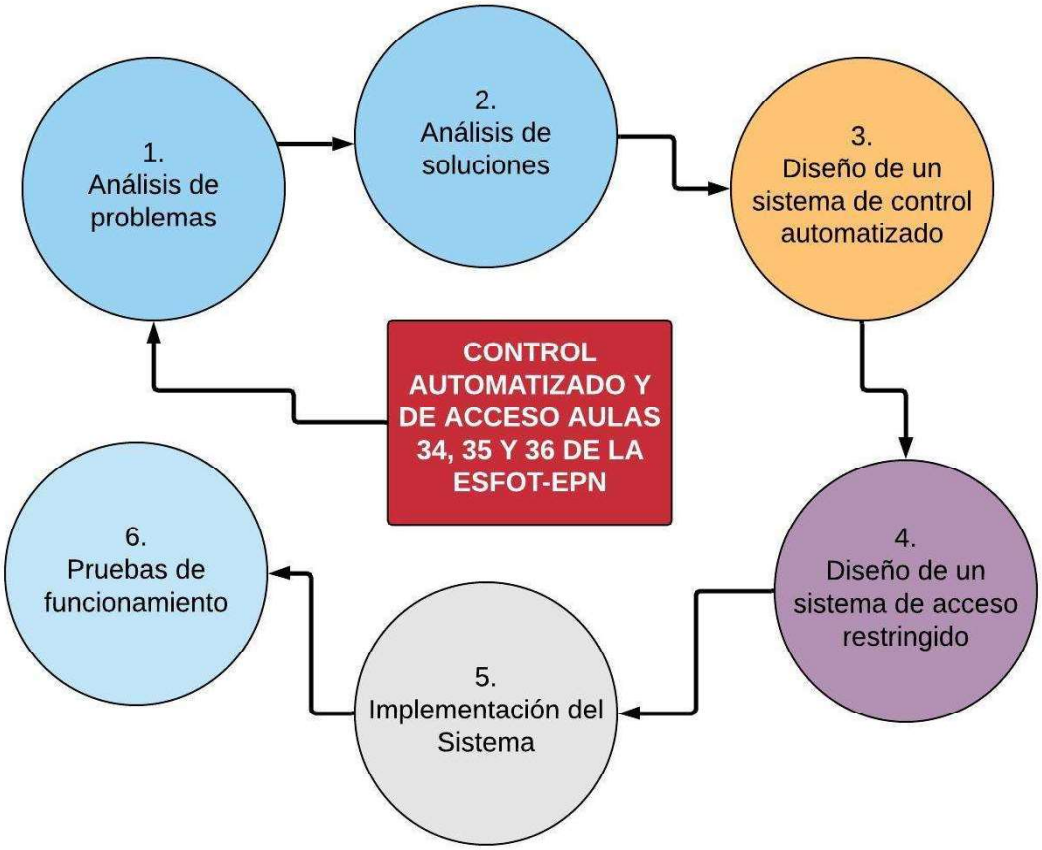

Figura 3.1 Etapas del proyecto

3.1 Análisis de problemas

La ingesta de bebidas alcohólicas en la Escuela Politécnica Nacional, representa un grave problema para todos quienes forman parte de la institución. Quienes realizan esta actividad no autorizada, con frecuencia elegían acudir a la ESFOT, convirtiéndose así en un espacio en el que podían ingerir alcohol o cualquier sustancia psicotrópica, sin que exista la restricción de acceso a las aulas. Específicamente las aulas 34, 35 y 36, donde se tenía la libertad de ingresar por las puertas o ventanas, ya que estas no contaban con la seguridad adecuada.

Cuando estas personas ingresaban a las aulas, hacían un mal uso de las mismas. Se han encontrado las instalaciones sucias, con botellas bajo los pupitres, mesas rayadas, piso sucio, paredes con grafitis como se evidencia en la figura 3.2, ventanas rotas, puertas averiadas, e incluso se ha encontrado preservativos que aparentemente han sido utilizados en las aulas.

Figura 3.2 Grafitis interior de aulas de la ESFOT *[25]*

Como se puede observar en la figura 3.3, ese es el estado en el que profesores, estudiantes y personal administrativo podían encontrar las aulas en las primeras horas de clase. Este problema generaba que el ambiente no sea el idóneo para el proceso de aprendizaje, provocando el malestar en estudiantes y profesores.

Figura 3.3 Botellas de licor en el interior de las aulas

El uso de las aulas los sábados era otro problema grave por solucionar; en ocasiones las aulas eran utilizadas sin autorización por la Federación de Estudiantes de la Escuela Politécnica Nacional (FEPON) y por la Federación de Estudiantes Politécnicos (FEPE). Estas federaciones ingresaban a las aulas con copias de llaves que han logrado conseguir, utilizando las instalaciones para dictar cursos particulares.

Por otra parte, en la ESFOT se dictan clases hasta las 20:00 horas de lunes a viernes y ciertas materias los sábados. Los profesores que tienen clases las últimas horas, en ocasiones se olvidaban de apagar las luminarias, provocando que las mismas permanezcan encendidas durante toda la noche e incurriendo en gastos innecesarios para la institución.

Al inicio de cada semestre se planifica el uso de aulas y horarios asignados por profesores. Sin embargo, pese a la planificación, existen casos de profesores que desean utilizar un aula que no les corresponde, para dar clases de recuperación o tomar evaluaciones. Esto lo realizaban sin ninguna autorización, en varios casos; causando confusión a los profesores y estudiantes que tenían asignada el aula normalmente, generando pérdida de tiempo hasta proceder con el cambio de aula.

3.2 Análisis de soluciones

Debido a todos los problemas mencionados anteriormente se optó por utilizar un sistema de control automatizado, el cual permite identificar qué puerta o ventana se encuentra abierta o cerrada. Además, para solucionar el problema de ingreso a las aulas con copias de llaves, se realizó un sistema de control de acceso utilizando un sistema biométrico en el cual únicamente los profesores registrados en las aulas podrán ingresar.

Como se observa en la Figura 3.4 el sistema automatizado tendrá un módulo Arduino, responsable del control de la automatización de las aulas. Esta automatización contempla la lectura de los sensores magnéticos que fueron ubicados en puertas y ventanas; además de leer el estado en el cual se encuentren las luminarias, para lo cual se podrá mandar la orden ya sea de apagar o encender las luminarias según el operador del sistema lo decida. Para que las órdenes sean enviadas al sistema, en el módulo Arduino se ha conectado una *shield ethernet,* la cual permite acceder a la red y de esta manera poder conectarse a una página *web* para comprobar el funcionamiento del sistema.

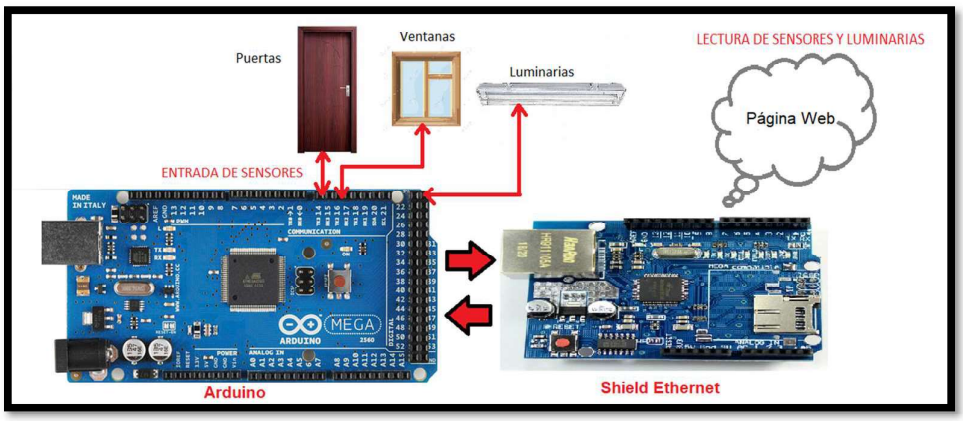

Figura 3.4 Sistema automatizado

El sistema de control de acceso se basa en el biométrico ZKTeco SF300, el cual cumple la función de otorgar acceso únicamente a los profesores registrados. El *software* ZK Access 3.5 permite configurar los horarios que existen en las aulas 34, 35 y 36.

Dentro del servidor que está ubicado en la dirección de la ESFOT se instaló dicho *software* ZK Access 3.5 y desde ahí se procede a la configuración del biométrico. Cada uno de los biométricos fue colocado afuera de las aulas cerca de las puertas. Desde ahí, los biométricos se conectaron en red mediante un *switch* D-LINK no administrable de 8 puertos el cual se conecta directamente a un puerto del *switch* de la Dirección de Gestión de la Información y Procesos (DGIP) ubicado en el laboratorio de control, para que desde el servidor se pueda realizar el respectivo control y configuración. En la figura 3.5 se muestra el esquema que tendrá el control de acceso.

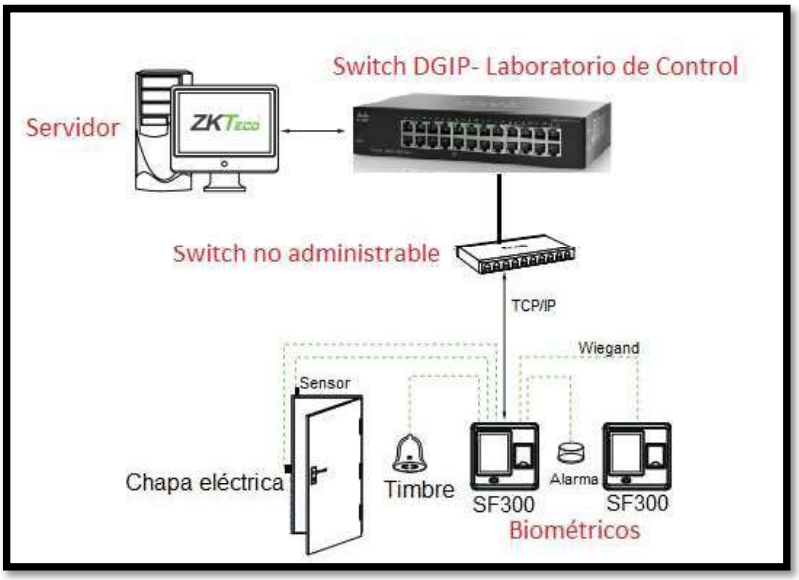

Figura 3.5 Sistema de control de acceso

Como se observa en las Figuras 3.4 y 3.5 se va a acceder a la intranet de la EPN, para lo cual se solicitó la habilitación de puertos disponibles en el s*witch* de la DGIP que se encuentra ubicado en el laboratorio de control, para esto también se solicitó una VLAN exclusiva para los biométricos, los cuales se conectan de igual manera a la intranet de la EPN.

Los biométricos y la *shield ethernet,* para poder conectarse a la intranet, necesitan tener una dirección IP que se encuentre dentro del rango de direcciones que maneja la institución, para lo cual se solicitó direcciones IP que se puedan utilizar en el proyecto.

3.3 Diseño del sistema de control automatizado

El sistema de control automatizado se ha creado para realizar el control de las luminarias y estado en el que se encuentran puertas y ventanas. Para ello se realizó un análisis para encontrar la manera más idónea de realizar este control automatizado.

Tal diseño cubrió varias etapas las cuales se van a profundizar a continuación:

Ubicación y cableado de sensores

Lo primero que se debe tener en cuenta son cuántas ventanas existen en total entre las aulas 34, 35 y 36, esto es necesario para saber cuántos sensores magnéticos se van a colocar en total para las ventanas. Además de las ventanas, la puerta de cada aula también tiene un sensor electromagnético. El número total de sensores magnéticos utilizados se observa en la tabla 3.1.

Tabla 3.1 Número de sensores

AULA	VENTANAS	PUERTA	TOTAL
34	5	1	6
35	5	1	6
36	3	1	4
TOTAL DE SENSORES			16

Conociendo que se van a utilizar 16 sensores magnéticos en total, se procede al diseño del cableado de los sensores. Como se observa en la Figura 3.6, cada sensor tendrá como destino un pin del Arduino Mega que está ubicado en un tablero de control, el mismo que ha sido elaborado por estudiantes de Electromecánica. Una vez realizado el análisis de ubicación, se definió que la mejor opción para colocar el tablero es en el aula 35, por encontrarse central. Los sensores magnéticos cuentan con dos cables, uno es el común; todos los cables comunes se conectan entre sí. Para tener una idea clara, en la Figura 3.6 se evidencian los cables comunes que son los de color azul, y llegará un cable común por aula

y se unirán a un mismo pin del Arduino. Los cables de color rojo que se evidencian en la Figura 3.6 son los correspondientes al otro cable del sensor electromagnético, que tiene cada uno su propio pin.

Figura 3.6 Cableado de sensores

Programación del Arduino

El programa del Arduino, el cual es el responsable de realizar la automatización de las aulas, consiste en la lectura del estado de los sensores ubicados en puertas y ventanas, además de la lectura y control de las luminarias, realiza la apertura de las puertas enviando un pulso a la chapa.

Para la realización del programa se utilizó un pin del Arduino por cada uno de los sensores de las ventanas, estos serán entradas y se describen en la Tabla 3.2.

En el caso de puertas se utiliza dos pines por puerta, uno correspondiente al sensor y el otro que envía un pulso para permitir la apertura de la puerta, en la Tabla 3.2 se evidencia los pines que corresponden a las puertas.

Para las luminarias se va a emplear tres pines por aula, uno correspondiente a la lectura en la que se encuentre el aula, el otro permite el encendido y el último realiza el apagado de las luminarias, se observa en la Tabla 3.2 la distribución de los pines.

Tabla 3.2 Pines utilizados en el Arduino

TABLERO 2-VENTANAS				TABLERO 2-PUERTAS				TABLERO 2-LUMINARIAS			
PINES	IN/OUT	AULA	CÓDIGO	PINES	IN/OUT	AULA	CÓDIGO	PINES	IN/OUT	AULA	CÓDIGO
28	IN	36	**VENT_36_1**	55-A1	IN	36	**PU_36_1**	3	IN	36	**FO_36**
30	IN	36	**VENT_36_2**	56-A2	IN	35	**PU_35_1**	4	IN	35	**FO_35**
32	IN	36	**VENT_36_3**	57-A3	IN	34	**PU_34_1**	5	IN	34	**FO_34**
34	IN	35	**VENT_35_1**	62-A8	OUT	34	**PR_34_1**	47	OUT-ON	34	**ON_FO_34**
36	IN	35	**VENT_35_2**	63-A9	OUT	35	**PR_35_1**	49	OUT-ON	35	**ON_FO_35**
38	IN	35	**VENT_35_3**	64-A10	OUT	36	**PR_36_1**	31	OUT-ON	36	**ON_FO_36**
40	IN	35	**VENT_35_4**					41	OUT-OFF	36	**OFF_FO_36**
42	IN	35	**VENT_35_5**					39	OUT-OFF	35	**OFF_FO_35**
44	IN	34	**VENT_34_1**					37	OUT-OFF	34	**OFF_FO_34**
46	IN	34	**VENT_34_2**								
48	IN	34	**VENT_34_3**								
27	IN	34	**VENT_34_4**								
29	IN	34	**VENT_34_5**								

Los códigos mencionados en la tabla 3.2, son utilizados en el código del Arduino. Cada código tiene diferente significado y eso se detalla a continuación:

- **VENT_34_2:** Este código es para identificar al sensor ubicado en la ventana número 2 del aula 34, y según se especifica en la tabla 3.2 este sensor va conectado al pin 46.
- **PU_36_1 →**Este código es para identificar al sensor ubicado en la puerta del aula 36, y según se especifica en la tabla 3.2 este sensor va conectado al pin 55-A1, el mismo, que es un pin analógico y que en el código del Arduino será cambiado a un pin digital mediante comandos.
- **PR_35_1 →** Este código es para identificar la salida del pulso que permite abrir la puerta del aula 35 desde el tablero de control número 2, y según se especifica en la tabla 3.2 esta salida va conectada al pin 63-A9, el mismo, que es un pin analógico y que en el código del Arduino será cambiado a un pin digital mediante comandos.
- **FO_34→** Este código es para identificar el monitoreo del estado en el que se encuentran las luminarias (prendidas o apagadas) del aula 34, y según se especifica en la tabla 3.2 el monitoreo del estado de las luminarias del aula 34 va conectado al pin 5.
- **ON_FO_35→** Este código es para identificar el pulso que manda el Arduino para encender las luminarias del aula 35, y según se especifica en la tabla 3.2 el pulso es mandado desde el pin 49.
- **OFF_FO_36→** Este código es para identificar el pulso que manda el Arduino para apagar las luminarias del aula 36, y según se especifica en la tabla 3.2 el pulso es mandado desde el pin 41.

En la figura 3.7 se presenta el diagrama de flujo correspondiente a la programación del módulo Arduino. Se empieza por definir las direcciones: IP, MAC, *Gateway*, máscara de red que corresponde a la *shield ethernet*. A continuación, se declara las variables que se emplean para ventanas, puertas y luminarias; siguiendo la asignación de pines y declarando cuáles serán entradas y salidas.

Posteriormente, se realiza el monitoreo de las entradas en donde se verifica todos los pines que fueron declarados, para imprimir el estado en el cual se encuentren.

Finalmente, se realiza el envío de datos que es utilizado para encender o apagar luminarias, además de abrir las puertas. Con lo antes mencionado, se analizará la cadena en la cual, se envía un comando que corresponde a encender la luminaria; esto se dará cuando esté en un estado apagado, encendiendo así dicha luminaria. Ocurre de manera similar en el caso de las puertas que se envía el comando para abrir las mismas.

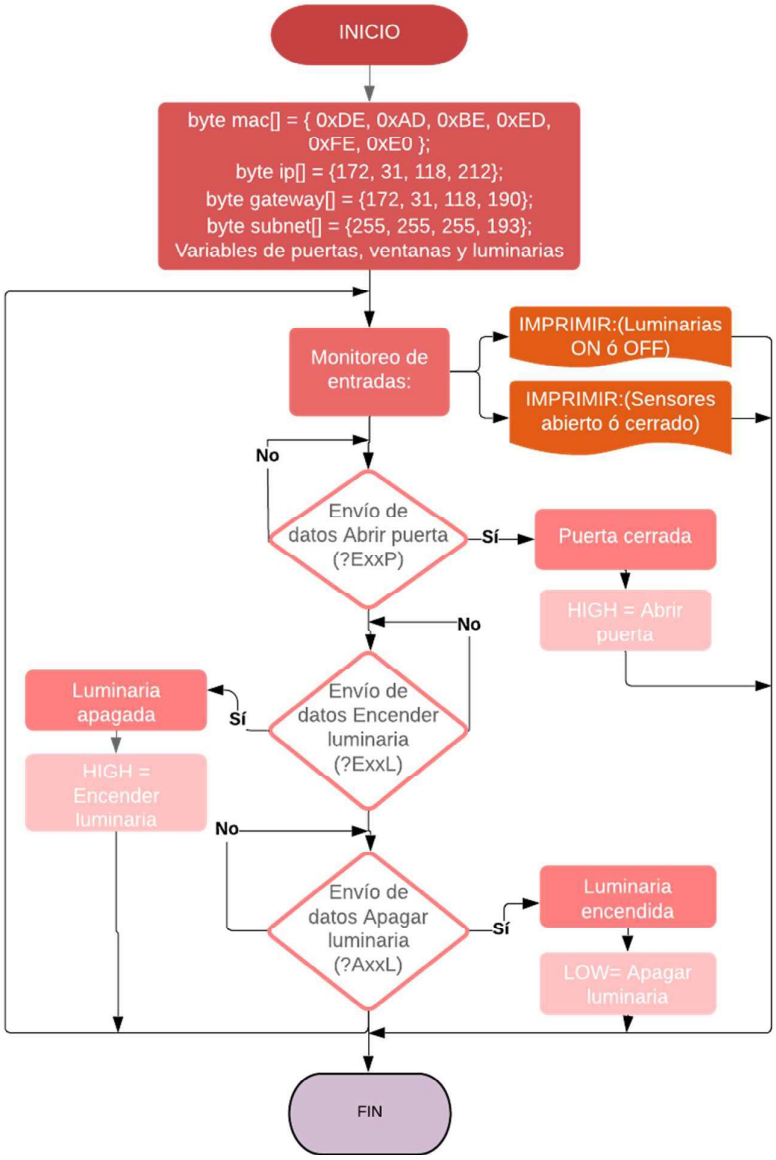

Figura 3.7 Diagrama de bloques

3.4 Diseño del sistema de control de acceso

Para el sistema de control de acceso correspondiente a las aulas 34, 35 y 36 se consideró la implementación de biométricos ZKTeco SF300 en cada una de las puertas. El biométrico ZKTeco SF300 permite el ingreso solamente a personas que tengan un usuario registrado dentro del mismo, usando su huella dactilar para poder abrir la puerta y tener el acceso a las aulas.

Las personas que estarán registradas con su usuario y huella dactilar en la base de datos del biométrico ZKTeco SF300 son exclusivamente: profesores, personal de limpieza y personal

administrativo. Los usuarios registrados tendrán creado un perfil en donde conste: su nombre, su horario de clases, la materia que dictan y su huella dactilar que les permite el acceso a las aulas.

Para poder crear usuarios con acceso a las aulas, es necesario usar el *software* ZK Access 3.5. El *software* ZK Access 3.5, además de permitir la creación de usuarios también crea horarios de clase, restringe el acceso a usuarios registrados cuando no es su hora de clases y guarda también su huella dactilar.

Los usuarios pueden enrolarse usando el mismo biométrico ZKTeco SF300 ya que existen opciones dentro de las configuraciones del biométrico en donde pueden depositar su huella dactilar, o también usando la enroladora ZK4500.

Los biométricos se configuran con una dirección IP, para que se los pueda monitorear y configurar mediante la red, esta configuración y monitoreo es factible mediante un servidor. La DGIP otorgó una VLAN con varias direcciones IP ya que es necesario tener a todos los biométricos en la misma red.

El servidor a cargo de estudiantes de ASI está ubicado en la dirección de la ESFOT-EPN, tiene instalado el *software* ZK Access 3.5 que permite, mediante la Enroladora ZK4500, tomar y guardar las huellas de los usuarios sin necesidad que los usuarios tengan que acercarse a cada biométrico ZKTeco SF 300 para guardar su registro.

El servidor deberá también estar en la misma red de los biométricos ZKTeco SF300 para que se los pueda configurar. Entonces, no es necesario ir creando una base de datos de los usuarios en cada biométrico, sino que se puede hacer una sola base de datos dentro del servidor e ir configurando y dando acceso a cada biométrico ZKTeco SF300 desde el *software* ZK Access 3.5.

Una vez que los biométricos ZKTeco SF300 estén instalados junto a cada puerta de las aulas 34, 35 y 36, estos serán conectados mediante cable UTP hacia el *switch* D-LINK no administrable de 8 puertos que se encuentra en el tablero número 2 de telecomunicaciones ubicado en el aula 35. Después, para que la información pueda llegar al servidor ubicado en la dirección de la ESFOT, es necesario conectar el *switch* D-LINK no administrable de 8 puertos a un puerto del *switch* de la DGIP ubicado en el laboratorio de control. Para observar la ubicación y conexión de los biométricos en el plano de la ESFOT, visualizar la figura 3.8. La simbología de los elementos utilizados se puede observar en el Anexo I.

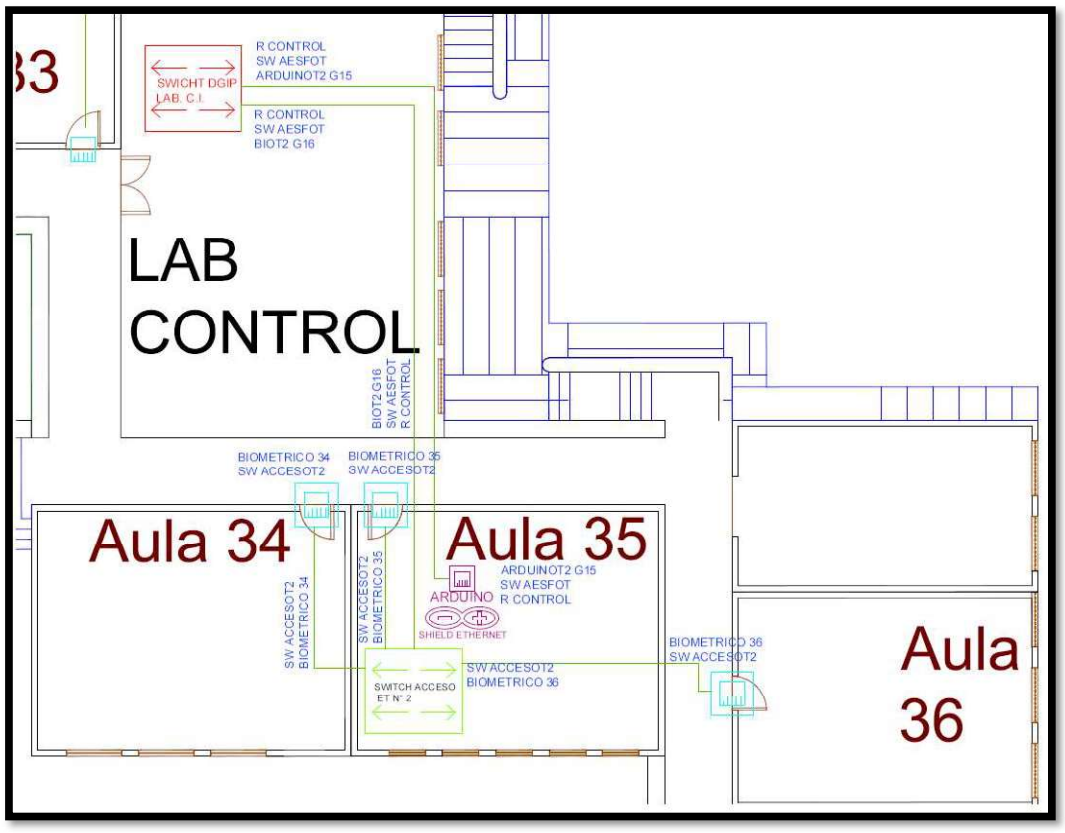

Figura 3.8 Ubicación de los biométricos SF 300

Diseño de la placa electrónica para proteger el biométrico

La placa electrónica que se creó permite alimentar a la chapa, observar figura 3.9, además tiene otras funciones como:

- Proteger a la chapa eléctrica y al biométrico.
- Hacer circular únicamente 12 (V_{DC}), para que la chapa eléctrica no sufra daños.
- Permitir que la chapa eléctrica pueda activarse y funcionar con el tablero número 2 de control; activarla mediante el servidor y desde el biométrico.

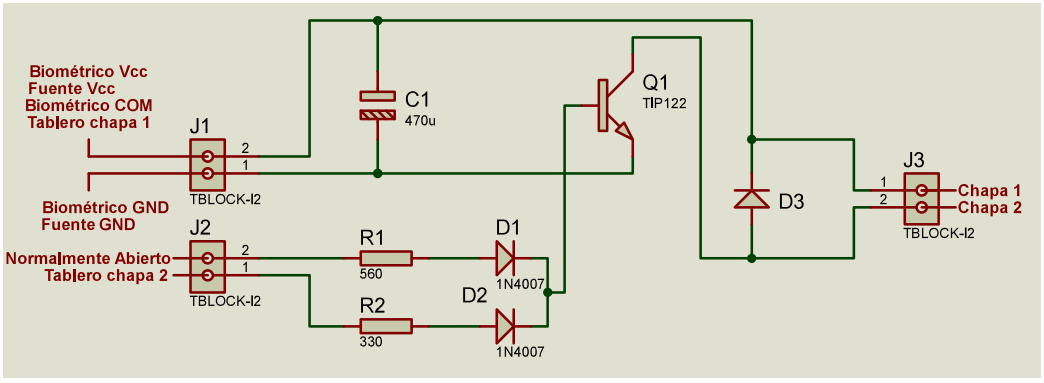

Figura 3.9 Diagrama de la placa electrónica

Los elementos que se encuentran en la placa son:

- 1 resistencia de 330 (Ω)
- 1 resistencia de 560 (Ω)
- 3 diodos rectificadores 1N4007
- 1 capacitor de 470 (Uf) / 25 (V_{DC})
- 1 transistor Darlington (TIP 122)
- 3 borneras de 2 pines

Cálculos del diseño de la placa

Como se puede observar en la figura 3.10, un pin de la bornera 2 se alimenta la placa con un voltaje de 12 (V_{DC}) que proviene del biométrico (Normalmente abierto); en el otro pin, de igual manera se alimenta con 12 (V_{DC}) que corresponden al tablero de control (tablero chapa 2). Por tal motivo se va a tener dos corrientes que pasarán por la resistencia y el diodo, respectivamente

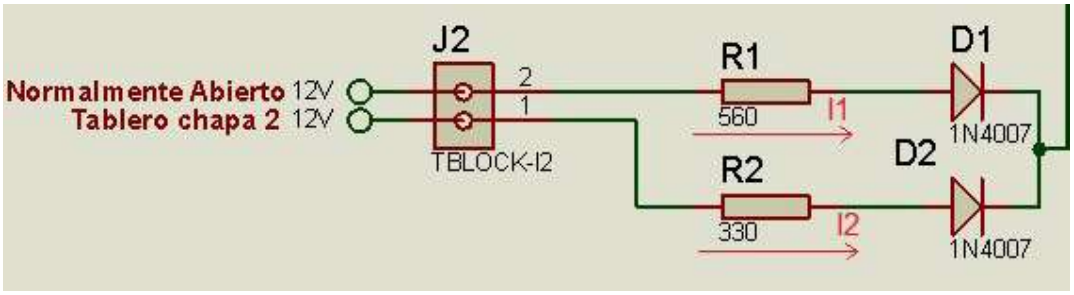

Figura 3.10 Voltajes y corrientes de la placa

En la siguiente ecuación se muestra los cálculos para obtener la corriente 1 y la corriente 2, en donde se toma en cuenta las caídas de voltaje que existe en el diodo y en el transistor Darlington.

$$\mathbf{I} = \frac{\mathbf{V_{DC} - V_{diodo} - V_{Darlington}}}{\mathbf{R}} \qquad \textbf{(1)}$$

Donde:

- V_{DC}: voltaje proveniente de la fuente del biométrico o del tablero de control=12 (V_{DC})
- V_{diodo}: de acuerdo con las especificaciones técnicas del diodo de silicio= 0.7 (V_{DC})
- $V_{Darlington}$: de acuerdo con la especificación del *datasheet* del transistor adjunto en el Anexo II.
- R: Resistencia = 560 (Ω) o 330 (Ω)

$$I_1 = 15.71\ (\text{mA}) \qquad I_2 = 26{,}66\ (\text{mA})$$

Se verifica que las corrientes obtenidas están dentro del rango de la corriente máxima que soporta el transistor que es de 120 (mA).

Se realiza el cálculo de la resistencia que presenta el cable.

$$\mathbf{R = \rho L / A} \qquad \textbf{(2)}$$

Donde

- ρ: es la resistividad del cobre = 1.7 x$10^{-2}(\Omega \cdot \text{m})$
- L: longitud máxima entre la chapa y el tablero = 100 (m)
- A: área del cable 20 AWG = 0.5190 (m^2)
- Se multiplica por 2 debido a que el cable se utiliza para transmisión en los dos sentidos.

$$R = 6.5896\ (\Omega)$$

Es importante saber la potencia de las resistencias a utilizar.

$$\mathbf{P = I^2 \cdot R} \qquad \textbf{(3)}$$

Donde

- I: es la corriente = 15.71(mA) o 26.66 (mA)
- R:es la resistencia = 560 (Ω) o 330 (Ω)

$$P_1 = 138.21\ (\text{mW})$$

$$P_2 = 234.54\ (\text{mW})$$

Por el valor de las potencias obtenidas, se ha optado por utilizar resistencias de ½ Vatio.

Para el cálculo de los valores de los capacitores se considera:

$$\mathbf{V_{RMS} = \sqrt{2} * V_{DC}} \qquad \textbf{(4)}$$

Donde

- V_{RMS}:es el voltaje eficaz
- V_{DC}: voltaje proveniente de la fuente del biométrico o del tablero de control =12 (V_{DC})

$$V_{RMS} = 16.97\ (V_{DC})$$

$$V_{Capacitor} = 25\ (V_{DC})$$

$$\text{Capacitor} = 470\ (\text{uF})\ /25\ (\text{V})$$

Con el valor máximo de voltaje que la fuente proporciona, se obtiene el valor del voltaje que el filtro requiere, consiguiendo valores comerciales de 470 (uF) a 25 (V_{DC}).

Finalmente, para la consideración de los diodos rectificadores y el transistor, se toma en cuenta:

$$\mathbf{V_{pi} = V_{DC}} \qquad \textbf{(5)}$$

Donde

- V_{pi}: es el voltaje pico inverso

$$V_{pi} = 12\ (V_{DC})$$

$$I_{Diodo} = 1\ (A)$$

$$I_{Transistor} = 3\ (A)$$

Según el voltaje pico inverso (V_{pi}) de 12 (V_{DC}) se utiliza el diodo 1N4007 que soporta corrientes hasta 1 (A), y de igual manera con el transistor 122 (Darlington) con corriente máxima de 3 (A).

3.5 Diseño de red

Lo que contempla el diseño de la red es la conexión de los elementos en red como son: biométricos, *shield ethernet* y el servidor, para que tenga acceso a la red de la EPN. Para ello se utiliza puertos disponibles en el *switch* de la DGIP, a donde llegarán los cables de red correspondientes a la VLAN de los biométricos y otro que corresponde al de la *shield ethernet;* al segundo *switch* ubicado en la dirección de la ESFOT se encontrará conectado el servidor.

Cada uno de los biométricos cuentan con un cable de red, el mismo que es conectado a un *switch* D-LINK no administrable de 8 puertos, el cual enviará toda la información correspondiente a los biométricos por una VLAN hacia el *switch* de la DGIP. Para el caso de la *shield ethernet* se conecta directamente al *switch* de la DGIP.

Para que todos los elementos puedan conectarse a la red de la EPN, deben tener una dirección IP que se encuentre dentro del rango que maneja la institución, para lo cual la DGIP proporcionó direcciones IP disponibles, las cuales son utilizadas en cada biométrico ZKTeco SF300, una en la *shield ethernet* y otra en el servidor. En el Anexo III se puede observar el plano de red, con sus respectivas conexiones para salir a red de la EPN, además de todos los elementos que cuentan con su respectiva dirección IP.

Nota: Las direcciones IP que se encuentran colocadas en el plano de red no son las empleadas en el proyecto, por motivos de seguridad.

3.6 Implementación del sistema de control automatizado y de acceso

Código del Arduino

A continuación, se presenta un extracto del código implementado en el módulo Arduino, correspondiente a las aulas 34, 35 y 36. Para evitar la redundancia del código, a manera demostrativa, no se considerarán todas las puertas, ventanas y luminarias.

```
//////////////////////////TABLERO 2//////////////////////////
#include <SPI.h>;
#include <Ethernet.h>;
byte mac[] = { 0xDE, 0xAD, 0xBE, 0xED, 0xFE, 0xE0 };
byte ip[] = {172, 31, 118, 212};
byte gateway[] = {172, 31, 118, 190};
byte subnet[] = {255, 255, 255, 193};
EthernetServer server(80);
String readString;

////////////////AULA 36 ////////////////////
//VALOR ACTUAL VENTANAS:
int ACT_VENT_36_1;int ACT_VENT_36_2;int ACT_VENT_36_3;
//DEFINIR PINES VENTANAS:
int VENT_36_1=28;int VENT_36_2=30;int VENT_36_3=32;
//VALOR ACTUAL PUERTAS:
int ACT_PU_36;
//VALOR ACTUAL FOCOS:
int ACT_FO_36;
//DEFINIR PINES PUERTAS:
int PU_36_1=55;
// SALIDA PUERTAS:
int E36P=64;
//SALIDA ON FOCOS:
int E36L=31;
//SALIDA OFF FOCOS:
int A36L=41;
void setup() {
```

```
//puertas:
DDRF=0;
PORTF=255;
DDRK=255;
PORTK=255;

//entradas focos:
pinMode(3, INPUT);
digitalWrite(3,HIGH);
//salidas focos:
pinMode(31, OUTPUT);
pinMode(41, OUTPUT);
digitalWrite(31,HIGH);
digitalWrite(41,HIGH);
//ventanas:
pinMode(28, INPUT);
pinMode(30, INPUT);
pinMode(32, INPUT);
digitalWrite(28,HIGH);
digitalWrite(30,HIGH);
digitalWrite(32,HIGH);

Serial.begin(9600);
Ethernet.begin(mac, ip, gateway, subnet);
server.begin();
Serial.print("El Servidor es: ");
Serial.println(Ethernet.localIP());
}

void loop() {
EthernetClient cliente = server.available();
if(cliente){
  while(cliente.connected()){
    if (cliente.available()){
      char c = cliente.read();

    if (readString.length()<100){
      readString += c;
      }
    if (c == '\n'){
      Serial.println(readString);
      cliente.println("HTTP/1.1 200 OK");
      cliente.println("Content-Type: text/html");
      cliente.println("Connection: close");
cliente.println();
cliente.println("<HTML>");
cliente.println("<HEAD>");
cliente.println("<TITLE> PRUEBA ARDUINO </TITLE>");
cliente.println("</HEAD>");
cliente.println("<BODY>");

////////////////////////////////////////////////////////////////////////
//////////////////////////MONITOREO DE ENTRADAS/////////////////////////
////////////////////////////////////////////////////////////////////////

//////////////////////////////PUERTAS///////////////////////////////////
//PUERTA 36
ACT PU 36 = digitalRead (55);
```

```
  cliente.print("36P:");
  cliente.print(ACT_PU_36);
  cliente.print(",");
////////////////////////////LUMINARIAS/////////////////////////////////
//FOCOS AULA 36:
ACT_FO_36 = digitalRead (3);
  cliente.print("36L:");
  cliente.print(ACT_FO_36);
  cliente.print(",");
////////////////////////////VENTANAS/////////////////////////////
//VENTANAS AULA 36:
//VENTANA 1:
ACT_VENT_36_1 = digitalRead (28);
  cliente.print("36V1:");
  cliente.print(ACT_VENT_36_1);
  cliente.print(",");
//VENTANA 2:
ACT_VENT_36_2 = digitalRead (30);
  cliente.print("36V2:");
  cliente.print(ACT_VENT_36_2);
  cliente.print(",");
//VENTANA 3:
ACT_VENT_36_3 = digitalRead (32);
  cliente.print("36V3:");
  cliente.print(ACT_VENT_36_3);
  cliente.print(",");

cliente.println("</BODY>");
cliente.println("</HTML>");
delay(1);
cliente.stop();

////////////////////////////////////////////////////////////////////////
////////////////////////////ENVIO DE DATOS//////////////////////////////
////////////////////////////////////////////////////////////////////////

//////////////////////ABRIR PUERTAS/////////////////////////
if (readString.indexOf("?E36P")>0){
   digitalWrite (E36P,LOW);
    delay(1000);
    digitalWrite (E36P,HIGH);
    }
//////////////////////PRENDER LUMINARIAS///////////
if (readString.indexOf("?E36L")>0){
    digitalWrite (E36L,LOW);
    delay(1000);
    digitalWrite (E36L,HIGH);
    }
//////////////////////APAGAR LUMINARIAS///////////////
if (readString.indexOf("?A36L")>0){
    digitalWrite (A36L,LOW);
    delay(1000);
    digitalWrite (A36L,HIGH);
    }
readString="";
      }
      }
      } }}
```

Nota: las direcciones IP escritas no son las direcciones IP que se emplearon en el proyecto.

Montaje de tablero de telecomunicaciones

En el tablero de telecomunicaciones, mostrado en la figura 3.11, es por donde viajará toda la información de los biométricos. Dentro del tablero de telecomunicaciones se encuentra:

- Un regulador de voltaje
- Un *switch* D-LINK no administrable de 8 puertos

Figura 3.11 Tablero número 2 de telecomunicaciones

- **Regulador de voltaje**

  El regulador de voltaje ayuda a proteger las conexiones que se insertan en él, como, por ejemplo el *switch* D-LINK no administrable de 8 puertos, la fuente del biométrico ZKTeco SF300 de 12 (V_{DC}), y la fuente del tablero de control realizado por los estudiantes de EM, el mismo que se encuentra junto del tablero número 2 de telecomunicaciones en el aula 35.

  Al existir cambios de voltaje imprevistos es posible que las fuentes tanto del *switch* D-LINK no administrable de 8 puertos como la del biométrico ZKTeco SF300 sufran daños y se puedan quemar los equipos. Por eso es necesario utilizar el regulador de voltaje.

- ***Switch* D-LINK no administrable de 8 puertos**

  Un *switch* D-LINK no administrable de 8 puertos se encuentra dentro del tablero número 2 de telecomunicaciones y es el que lleva toda la información de los biométricos ZKTeco SF300. El *switch* D-LINK no administrable de 8 puertos se engancha a un *switch* administrable que se encuentra en el laboratorio de control, el cual es manejado por la DGIP.

  En el *switch* D-LINK no administrable de 8 puertos se conectan los biométricos ZKTeco SF300 de las aulas 34, 35 y 36. Mediante el cable UTP, los biométricos pueden ser visibles desde el servidor.

El montaje y elementos del tablero número 2 de telecomunicaciones se lo puede apreciar en la figura 3.12.

Figura 3.12 Elementos del tablero de telecomunicaciones

Cableado de sensores magnéticos

Las personas que tienen el acceso a las aulas son exclusivamente: profesores, personal de limpieza y personal administrativo. Los mismos, que pueden ingresar mediante una huella dactilar colocada en el lente del biométrico ZKTeco SF300. Para complementar el acceso y la protección de los elementos que se encuentran dentro de las aulas, el sistema de control cuenta también con un servidor que fue creado por los estudiantes de ASI, que permite saber el estado de las ventanas y de las puertas de los cursos 34, 35 y 36 ya que el sensor electromagnético colocado en las ventanas y puertas da un aviso al servidor cuando su estado cambia, es decir, si se encuentra abierto o cerrado.

Entonces, el sistema de control de acceso además de permitir el ingreso solamente a personal que se encuentra registrado en el biométrico ZKTeco SF300, informa la fecha y hora en las cuales las ventanas o puertas fueron abiertas o cerradas.

Colocación de sensores en puertas

En las puertas de las aulas 34, 35 y 36 los sensores magnéticos son colocados en la parte superior, como se observa en la figura 3.13. Esto se debe a que los sensores tienen cables que se colocan por el techo de las aulas y además para evitar que los estudiantes y demás personas puedan averiarlos.

Figura 3.13 Cableado de sensores magnéticos en puertas

Todos los sensores magnéticos usados en el sistema de control de acceso cuentan con 2 cables: uno que es el cable común y el otro que irá conectado a un pin del módulo Arduino que se encuentra en el tablero de control ubicado en el aula 35.

En la parte superior de las aulas, los cables de cada sensor son protegidos mediante mangueras como se observa en la figura 3.14, para que no puedan ser pisoteados ni estropeados; ahí se une un cable de cada sensor para tener un solo cable común que también llegará a un pin del módulo Arduino.

Figura 3.14 Puesta de mangueras para proteger los cables

Instalación de sensores en ventanas

La ubicación de los sensores es en la mitad de las ventanas, debido a que en la mitad de todo el marco se encuentra la ventana que se puede abrir, observar figura 3.15.

Figura 3.15 Colocación de sensores en las ventanas

También como en las puertas, el cableado de los sensores va cubierto por el techo, ahí los cables de los sensores cumplen un papel similar a los cables de las puertas. Los cables comunes se unen en un solo cable que llega al mismo pin del cable común de las puertas, y los otros cables de las ventanas llegan a distintos pines.

Cambios de estado de los sensores

En las puertas y ventanas de cada curso, al generarse un cambio de estado el sensor envía una señal al módulo Arduino; esta señal viaja mediante la *shield ethernet* colocada en el Arduino y llega al servidor en donde hace que la información cambie de estado, ya sea "puerta abierta" o "puerta cerrada".

Para que la información del cambio de estado de las puertas pueda viajar hacia el servidor, la *shield ethernet* va conectada mediante un cable de red a un *switch* D-LINK no administrable de 8 puertos que se encuentra en el tablero de telecomunicaciones, el cual se ubica al lado del tablero número 2, dentro del aula 35.

Instalación del cable de red

El cable de red es indispensable para la comunicación entre el servidor y los biométricos, y para que el servidor pueda controlar el estado de puertas y ventanas. Para observar la

ubicación del cableado de red ver figura 3.8. El cable de red de cat 5e es colocado por encima del techo llevándolo por tuberías para que no se maltrate, la conexión del cable es desde los biométricos hasta el *switch* D-LINK que se encuentra en el tablero número 2 de telecomunicaciones, de ahí el cable va hasta el *switch* administrable. En la figura 3.16 se puede apreciar la conexión de los cables de red llegando hasta el *switch* no administrable.

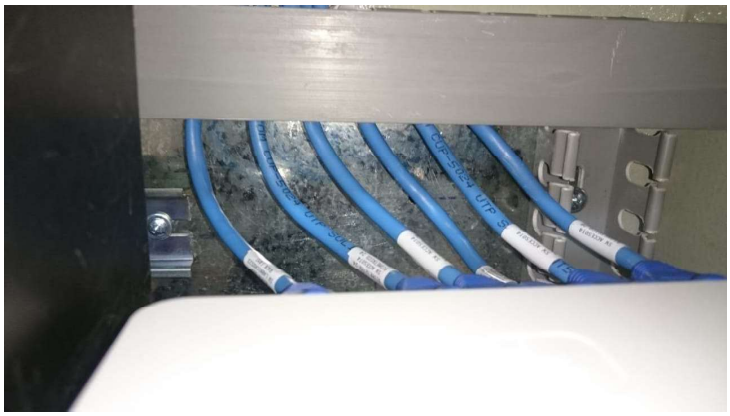

Figura 3.16 Conexión del cable de red llegando al switch no administrable

El cable de red conecta también la *shield ethernet* que va conectada en el Arduino hacia el *switch* del laboratorio de control y de ahí viaja la información de los cambios de estado de las puertas y ventanas de las aulas 34, 35 y 36. Esto se aprecia en la figura 3.17.

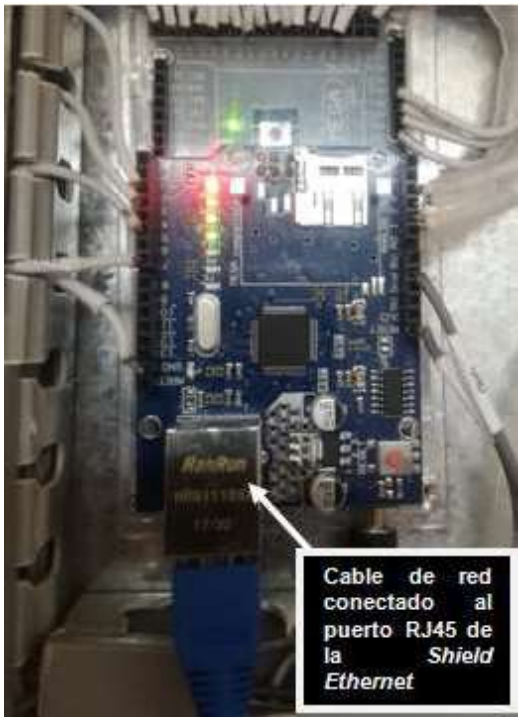

Figura 3.17 Conexión de la Shield Ethernet con cable de red

Ponchado de cables

Los cables de red que corresponde a la conexión entre biométricos – *switch*, Arduino – *switch* y *switch* D-LINK no administrable de 8 puertos – *switch* de control, fueron ponchados utilizando la norma ANSI/TIA 568 B.

Para saber si un cable se encuentra ponchado de manera correcta y existe la continuidad de los cables de red, se utiliza un dispositivo llamado probador de cables de red "TESTER", como se observa en la figura 3.18 se realiza esta prueba en la que se comprueba que todos los hilos de cable UTP se encuentren en el orden correspondiente y que realicen contacto con el conector RJ45, esta prueba se realiza en los dos extremos del cable al mismo tiempo.

Figura 3.18 Prueba de ponchado

Instalación de biométricos ZKTeco SF300

La instalación de los biométricos se realizó después de tener todo el cableado tendido, tanto el cable de red como el cable de los sensores magnéticos.

Los biométricos ZKTeco SF300 están soportados en la pared al lado de las puertas de las aulas 34, 35 y 36, como se puede apreciar en la figura 3.19.

Figura 3.19 Ubicación de los biométricos en las aulas

Para que el biométrico ZKTeco SF300 pueda encenderse se debe utilizar una fuente de 12(V_{DC}), la cual está ubicada en el techo arriba de cada biométrico, esto se puede apreciar en la figura 3.20.

Figura 3.20 Fuente del biométrico

Los cables del biométrico ZKTeco SF300 van conectados a la fuente de 12 (V_{DC}) y el tercero va conectado a la placa electrónica que protege al biométrico ZKTeco SF 300 y a la chapa eléctrica. Además de los cables para alimentar el biométrico, este consta de un puerto RJ45 desde el cual sale el cable UTP que llega al *switch* no administrable. Al llegar los biométricos al *switch*, este permite que puedan estar en una misma red, ya que cada biométrico ZKTeco SF 300 cuenta con una dirección IP que fueron otorgadas por la DGIP. El direccionamiento,

distribución de las direcciones IP para cada uno de los biométricos y diseño de la red se las puede apreciar en el Anexo III.

Instalación de chapas eléctricas

Además del control de acceso mediante el biométrico ZKTeco SF300, se colocaron chapas eléctricas. Las chapas eléctricas van conectadas a una placa electrónica que protege al biométrico ZKTeco SF 300 y a la chapa. Esta placa electrónica se encuentra por encima de cada puerta, cubierta por el techo.

Como se puede apreciar en la figura 3.21, las chapas eléctricas fueron colocadas en el mismo lugar en donde se encontraban las antiguas chapas de las puertas.

Figura 3.21 Instalación de chapas eléctricas

Las chapas eléctricas funcionan o se activan con 12 (V_{DC}), debido a que la chapa eléctrica cuenta con bobinas dentro de estructura, es posible que sufra daños al alterarse o cambiar el voltaje o la corriente, es por eso que se optó en construir una placa electrónica que funciona a 12 (V_{DC}) y permite que la chapa eléctrica pueda activarse.

El cableado de la chapa eléctrica va por encima del techo y está protegido por canaletas y mangueras para evitar que existan deterioros en los cables. Los cables de las chapas eléctricas son 2: positivo y negativo. Estos van conectados directo a unas borneras ubicadas en la placa electrónica la cual está alimentada con 12 (V_{DC}). La conexión y protección de la chapa eléctrica se lo pueda apreciar en la figura 3.22.

Figura 3.22 Protección de los cables de la chapa eléctrica

Implementación de la placa electrónica de protección para el biométrico

Como se observa en la figura 3.23, se diseñó en Proteus las pistas para la creación de la placa electrónica.

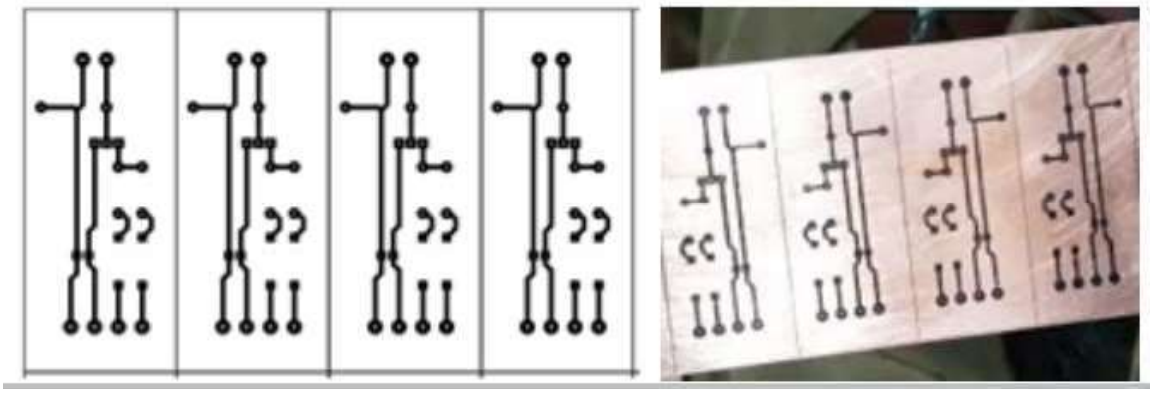

Figura 3.23 Pistas de la placa electrónica

La placa electrónica terminada se la puede apreciar en la figura 3.24.

Figura 3.24 Placa electrónica terminada

Observando la figura 3.24, se aprecia que en las borneras de la parte superior izquierda se conecta la fuente de 12 (V_{DC}). En las borneras de la parte inferior izquierda se conecta un cable que llega desde el biométrico ZKTeco SF 300y otro cable que llega desde el tablero de control, respectivamente. Y en las borneras de la parte derecha se conectan los cables que llegan desde la chapa eléctrica.

Funcionamiento de la placa electrónica.

Debido a que la chapa eléctrica puede activarse desde el tablero de control, desde el *software* ZK Access 3.5 o desde el biométrico, es necesaria la instalación de la placa electrónica.

- **Funcionamiento desde el tablero de control**

  Desde el servidor, es posible abrir la puerta ya que el servidor, la *shield ethernet* conectada en el modulo Arduino, el *switch* no administrable de 8 puertos, y el *switch* de la DGIP se encuentran en la misma red. Ahí al mandar un pulso desde el servidor, el módulo Arduino activa el pin correspondiente a la puerta, el cual va conectado directamente a la placa electrónica exclusivamente en la bornera inferior izquierda como se aprecia en la figura 3.24, este pulso genera 12(V_{DC}), voltaje que activa a la base del transistor y permite que el emisor y colector funcionen como un interruptor y dejen pasar únicamente 12 (V_{DC}) que circulan desde la fuente del biométrico ZKTeco SF 300 que va conectado a la bornera superior izquierda de la placa electrónica como se aprecia en la Figura 3.24, para que se active la chapa eléctrica.

- **Funcionamiento desde el biométrico.**

  Los usuarios, al colocar su huella dactilar, generan un voltaje de 12 (V_{DC}) que llega a la bornera de la parte inferior izquierda de la placa y activa la base del transistor que hace que el colector y emisor funcionen como un interruptor y dejen pasar únicamente 12 (V_{DC}) que circulan desde la fuente del biométrico

ZKTeco SF 300 que va conectado a la bornera superior izquierda de la placa electrónica como se aprecia en la Figura 3.24, para que se active la chapa eléctrica.

- **Funcionamiento desde el *software* ZK Access 3.5.**

  Al hacer funcionar desde el *software* ZK Access 3.5 la chapa eléctrica, cumple un procedimiento parecido al abrir desde el biométrico ZKTeco SF 300 ya que mediante el cable UTP llega la señal desde el *software* ZK Access 3.5 al biométrico ZKTeco SF 300 para que genere 12 (V_{DC}) y permita abrir la chapa eléctrica con un procedimiento parecido, activando la base y haciendo que el colector y emisor del transistor funcionen como un interruptor.

  En el transistor, la base se activa con una corriente máxima de 120 (mA) según sus especificaciones técnicas detalladas en el Anexo II.

  Al generarse voltajes de 12 (V_{DC}) desde cualquiera de las dos borneras de la parte inferior izquierda de la placa electrónica como se aprecia en la Figura 3.24, las corrientes ya calculadas con la ecuación (1), son menores a 120(mA) y por ende es posible que la base se active para que el colector y el emisor funcionen como un interruptor dejando pasar el voltaje de la fuente del biométrico que es de 12 (V_{DC})y va conectado a las borneras de la parte superior 123izquierda de la placa electrónica como se aprecia en la figura 3.24.

  En el Anexo V, se puede evidenciar el mantenimiento que debe tener la placa en caso de fallas.

Configuración de biométrico

El *software* ZK Access 3.5 permite configurar el biométrico ZKTeco SF 300 y administrarle accesos; dentro del *software* ZK Access 3.5 es posible ingresar: horarios, usuarios (profesores, personal de limpieza y personal administrativo), restringir el acceso a personas que no se encuentran logueadas en el biométrico ZKTeco SF 300 o que están ingresando en un horario que no les corresponde y dar acceso a usuarios para que puedan ingresar a todas las aulas.

La configuración de los biométricos se puede realizar ingresando a las configuraciones del mismo biométrico, conectando el biométrico ZKTeco SF 300 a una laptop que tenga el *software* ZK Access 3.5 instalado o desde el servidor en el cual se reflejan todos los biométricos que están colocados en las aulas 34, 35 y 36.

Para poder configurar el biométrico ZKTeco SF 300desde la laptop es necesario que la laptop esté en la misma red del biométrico ZKTeco SF 300 para que se lo pueda modificar. La configuración desde la laptop se puede apreciar en la figura 3.25.

Figura 3.25 Configuración del biométrico

Ya que los biométricos se encuentran conectados en red, para mayor facilidad la configuración se la realiza desde el servidor en donde también se encuentra instalado el *software* ZK Access 3.5. Como el servidor está dentro de la misma red de los biométricos, se los puede configurar a todos sin necesidad de hacerlo uno por uno.

Configuración del biométrico con el *software* ZK Access 3.5

Antes de la configuración, es necesario que al biométrico ZKTeco SF 300 se configure con una dirección IP, las cuales fueron otorgadas por la DGIP. Al igual que el biométrico ZKTeco SF300, la computadora deberá estar en red, para lo cual es necesario configurarla con una dirección IP que se encuentre en el mismo rango de la dirección IP del biométrico ZKTeco SF300. Una vez que la computadora y el biométrico ZKTeco SF300 puedan comunicarse (verificación mediante un ping), se procede con la configuración.

En el *software* ZK Access 3.5 se puede realizar la configuración del biométrico ZKTeco SF300, a continuación, se describen los pasos de la configuración del biométrico ZKTeco SF 300 del aula 35, en donde se precederá a crear usuarios, materias y niveles de acceso.

1) En la pantalla principal del *software* ZK Access 3.5 se encuentra la pestaña "**Dispositivo"**, en la cual se agregará el dispositivo (biométrico ZKTeco SF300) del aula 35; dentro de la pestaña "**Dispositivo"** dar clic en "**Agregar".** Esto se aprecia en la figura 3.26.

Figura 3.26 Agregar dispositivo

2) Al dar clic en la pestaña "**Agregar**", es necesario colocar la dirección IP que ya se le ha configurado con anterioridad al biométrico ZKTeco SF300.Seleccionar la pestaña TCP/IP ya que el dispositivo se encuentra conectado mediante la tarjeta de Red, esto se aprecia en la figura 3.27.

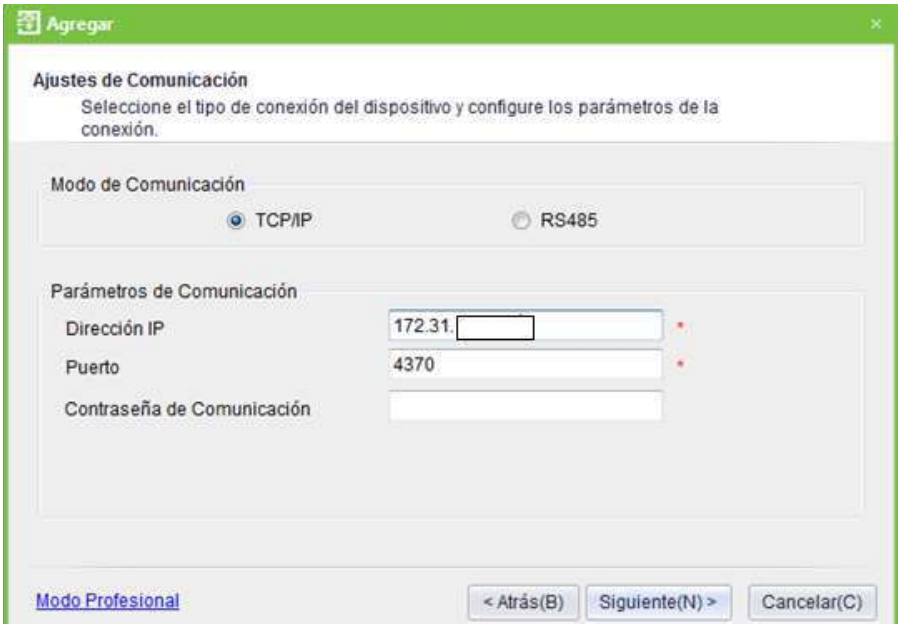

Figura 3.27 Ingreso de dirección IP del biométrico

3) Después, se coloca el nombre del biométrico ZKTeco SF300, que en general se coloca el nombre del aula, en este caso **AULA 35**; esto se aprecia en la figura 3.28. Las

pestañas de la sincronización de la hora y de eliminar cualquier tipo de información que se encuentre en el biométrico ZKTeco SF 300 es opcional.

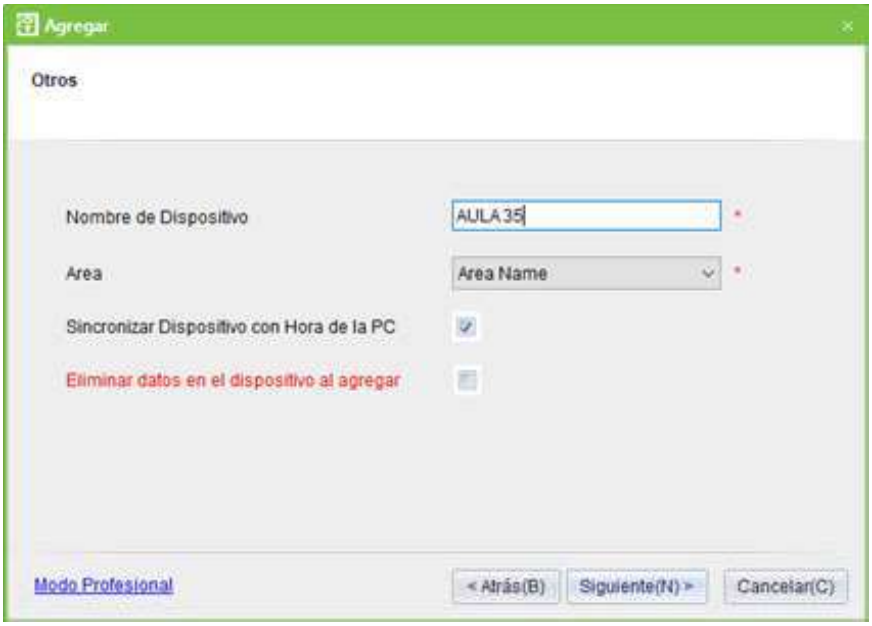

Figura 3.28 Nombre de dispositivo

4) Por último, dar clic en finalizar y esperar que el *software* ZK Access 3.5 cargue y agregue el dispositivo (biométrico ZKTeco SF300), esto se aprecia en la figura 3.29. Al finalizar el proceso de agregar el dispositivo, el biométrico ZKTeco SF300 se reiniciará.

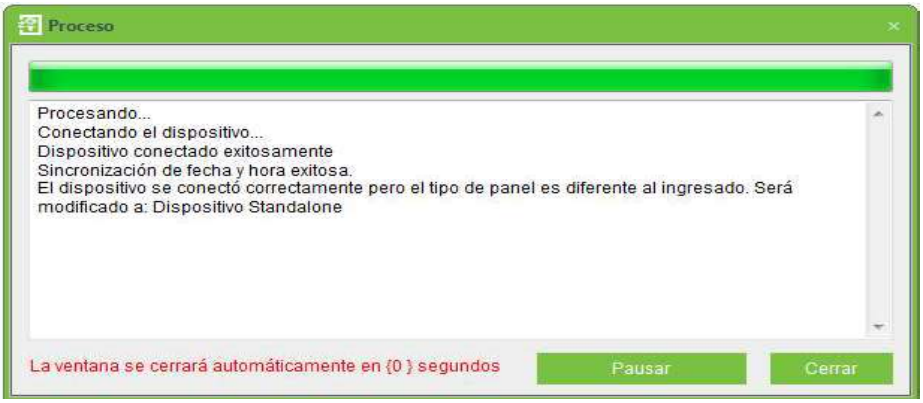

Figura 3.29 Dispositivo agregado

5) En la figura 3.30 se aprecia que el biométrico ZKTeco SF300 del aula 35 ya ha sido agregado al *software* ZK Access 3.5 y está listo para su configuración.

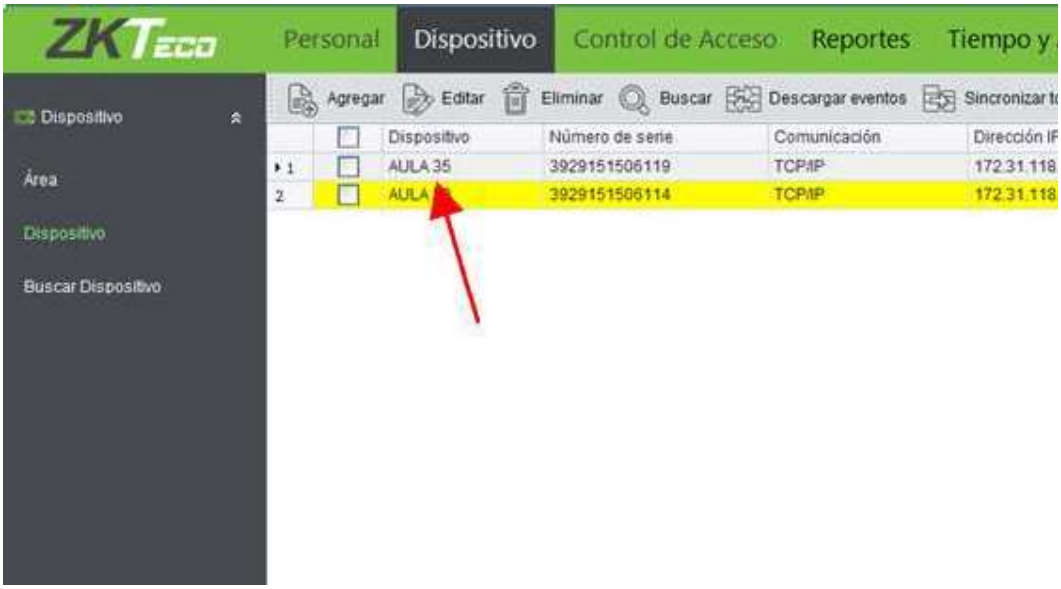

Figura 3.30 Biométrico agregado al software

6) Una vez agregado el biométrico ZKTeco SF300 al *software* ZK Access 3.5, se procede a la creación de usuarios. En la pantalla principal del *software* ZK Access 3.5 se encuentra la pestaña de nombre **"Personal**" en donde se empiezan a crear los usuarios. Para agregar usuarios se da clic en la pestaña "**Agregar**". Esto se aprecia en la figura 3.31.

Figura 3.31 Agregar usuario

7) Al dar clic en la pestaña **"Agregar",** se despliega una ventana como se muestra en la figura 3.32, en donde se coloca la información del usuario como por ejemplo: el ID de usuario, el nombre, el género, y el departamento. En esta sección se toma las huellas

dactilares del profesor dando clic en **"Sensor de Huella USB"** y se procede a la toma de la huella de los pulgares y otro dedo adicional.

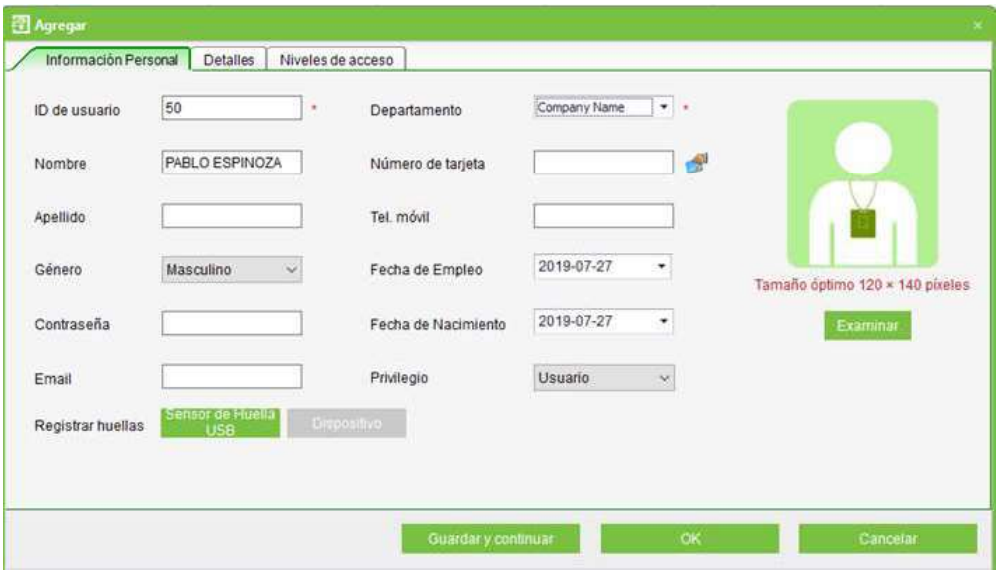

Figura 3.32 Información de usuario

8) Una vez creados todos los usuarios a los que les corresponde dictar clases en el aula 35, se procede a crear las materias que dictarán los profesores con su respectivo horario. En la pantalla principal del *software* ZK Access 3.5 se encuentra la pestaña "**Control de Acceso**", dentro de esta pestaña se da clic en la pestaña "**Agregar**". Esto se aprecia en la figura 3.33.

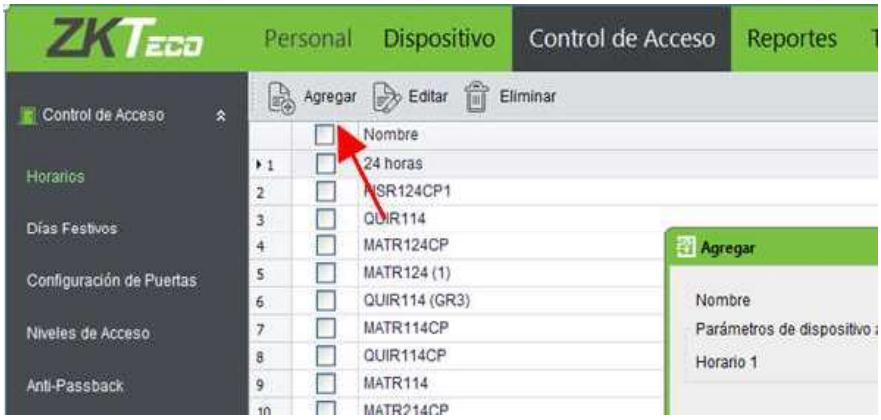

Figura 3.33 Creación de materias

9) Al dar clic en la pestaña **"Agregar",** se despliega una ventana como se muestra en la figura 3.34, en donde se coloca la información de la materia como su nombre y su código (este código es importante ya que identifica a la materia, debido a que existen

materias con el mismo nombre que son dictadas por diferente profesor). Dentro de esta ventana también se ubica qué día y en qué horario se dicta esta materia.

Figura 3.34 Creación de horarios

10) Después de crear los usuarios y las materias, se procederá a dar el nivel de acceso a los profesores; es decir, que solo podrán ingresar cuando tengan que dictar clase, ya que antes la materia fue configurada con un horario. Como se aprecia en la figura 3.35, para dar los niveles de acceso, dirigirse a la pestaña "**Control de Acceso**" en donde se encuentra la pestaña "**Niveles de acceso**" ingresar y dar clic en la pestaña "**Agregar**".

Figura 3.35 Creación de niveles de acceso

11) Al dar clic en la pestaña **"Agregar",** se despliega una ventana como se muestra en la figura 3.36.Dentro de la ventana, en la parte superior derecha, se elige la materia

antes creada, y en la parte superior izquierda se coloca el nombre (en este caso el mismo para evitar confusiones).

Para seleccionar la puerta (biométrico) en la que se guardará la materia, es necesario seleccionar la puerta y pasarla a puertas seleccionadas; en este caso, se selecciona la puerta (biométrico) del aula 35.

Para seleccionar el usuario (profesor) que dictará esa materia, es necesario seleccionar el usuario y pasarlo a usuarios seleccionados.

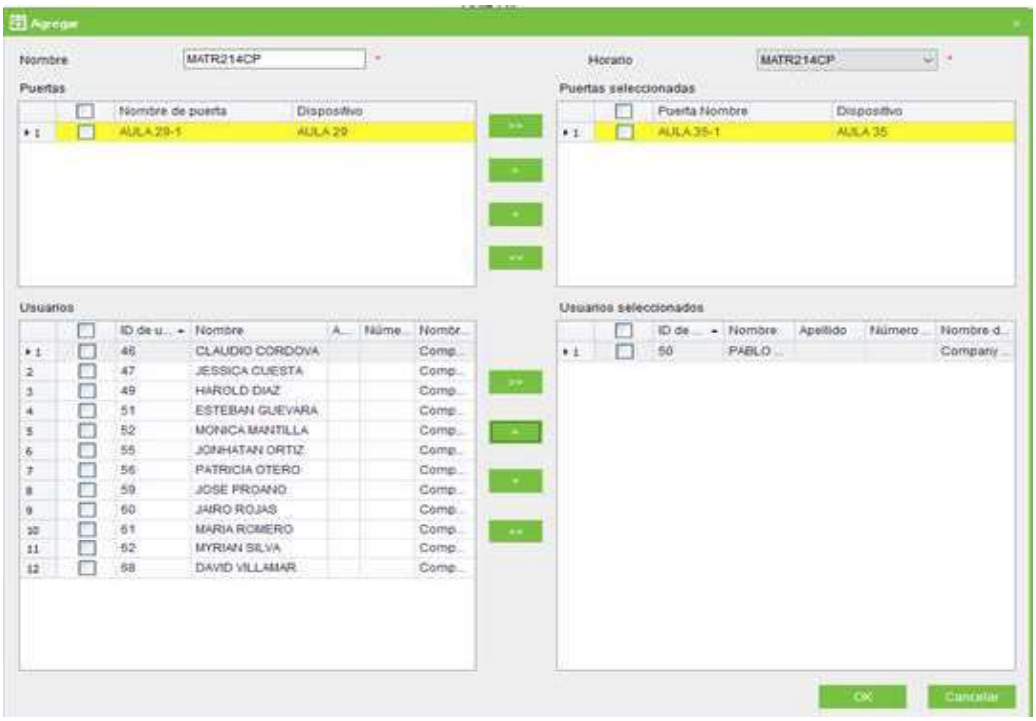

Figura 3.36 Asignación de niveles de acceso

12) Una vez que se hayan creado todos los niveles de acceso, hay que sincronizar la puerta (biométrico ZKTeco SF300 del aula 35); para esto es necesario regresar a la pestaña "**Dispositivos**", seleccionar la puerta del aula 35; dar clic derecho y seleccionar la opción "**Sincronizar datos recientes al dispositivo**". Esto se aprecia en la figura 3.37.

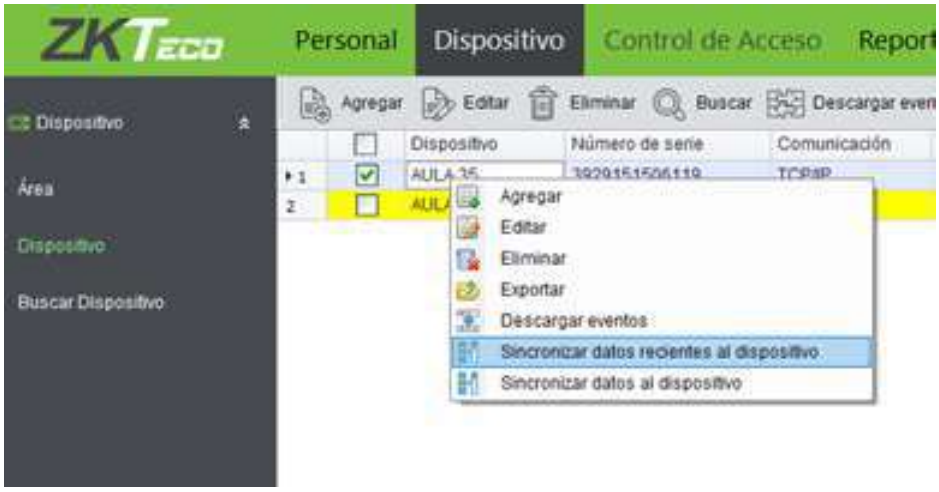

Figura 3.37 Sincronización de datos

13) Finalmente, como se aprecia en la figura 3.38, se cargarán y se sincronizarán todos los datos en el biométrico ZKTeco SF300 del aula 35, el cual al finalizar la sincronización estará listo para ser usado.

Figura 3.38 Dispositivo sincronizado

Para concluir con la configuración de los biométricos se necesita que los usuarios registrados carguen su huella dactilar para poder ingresar a las aulas, mediante una enroladora que se conecta al servidor, así como se observa en la figura 3.39.

Figura 3.39 Registro de huellas mediante la enroladora

La configuración de los biométricos más detallada se encuentra en el Anexo IV.

Etiquetado de cables de red

Según lo menciona la norma ANSI/TIA 606 C, que es la versión actualizada a lo que se refiere el etiquetado de cables, cada uno de los cables que conforman el diseño de cableado estructurado debe contar con su debida etiqueta para mejorar el rendimiento y la eficiencia de la red. [26]

Entonces, basándose en el etiquetado que utiliza la DGIP, "de dónde viene a dónde va", en la Tabla 3.3 se presenta el ejemplo del etiquetado que tendrán todos los cables de red. En la figura 3.40 se puede observar los cables conectados al *switch* D-LINK no administrable de 8 puertos, con su debida etiqueta.

Tabla 3.3 Etiquetas para cables de red

TABLERO DE TELECOMUNICACIONES	BIOMÉTRICO
SW ACCESOT2	BIOMÉTRICO 35
BIOMÉTRICO 35	SW ACCESOT2

Figura 3.40 Cables de red etiquetados

Etiquetado de cables del Arduino

Se realizó el etiquetado de cada uno de los cables que llegan al Arduino, para lo cual se basó en la Tabla 3.2, donde se evidencia el número de pin que corresponde a la respectiva ventana, puerta o luminaria. Además, en la Tabla 3.4 se muestra un ejemplo detallado del etiquetado cuando son entradas digitales, entradas o salidas analógicas y si el cable corresponde a ventana, puerta o luminaria.

Tabla 3.4 Etiquetado del Arduino

PUERTAS	VENTANAS	LUMINARIAS
IN (A2) P35N1	OUT (D28) V36N1	IN (D5) L34N1
OUT (A9) P35N1	OUT (30) V36N2	OUT (D47) LE34N1

Como se muestra en la figura 3.41, todo cable que se encuentra conectado al Arduino tiene su propia etiqueta, en la cual se registra a qué pin corresponde; de este modo, en el caso de que un cable esté suelto, se podrá saber el lugar exacto al que corresponde.

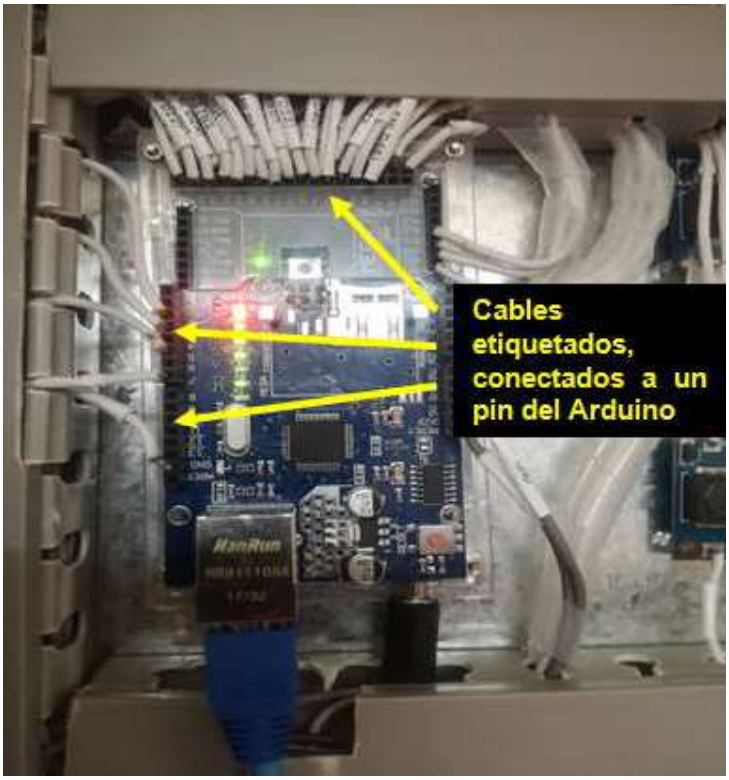

Figura 3.41 Conexiones del Arduino

3.7 Pruebas de funcionamiento

Con todos los elementos instalados, conectados y en red de la EPN, además de la configuración de cada uno de los biométricos según su respectivo horario, se procedió con las siguientes pruebas:

Pruebas desde la *Shield Ethernet*

La *shield ethernet* se encuentra configurada con una dirección IP que fue proporcionada por la DGIP para acceder a la red de la EPN.

Dicha dirección se puede digitar en cualquier dispositivo que se encuentre conectado a la red de la EPN, para evidenciar cuál es el estado en el que se encuentran las puertas, ventanas y luminarias que están conectados en el tablero de control ubicado en el aula 35.

Como se puede observar en la figura 3.42, al ingresar a la dirección que corresponde a la *shield ethernet* se va a evidenciar el estado de los elementos que conforman la automatización del aula, empezando con el número del aula seguido por la inicial del elemento que se está leyendo. Siendo así, la P de puerta, L de luminarias, y V de ventanas; para el último caso se ha especificado el número de ventanas.

La lectura es sencilla, para el caso de puertas y ventanas cuando se muestra un 0L significa que se encuentra cerrada, pero si es 1L está abierta; para el caso de las luminarias es lo contrario eso quiere decir que cuando se observe 1L la luminaria está apagada y con 0L encendida.

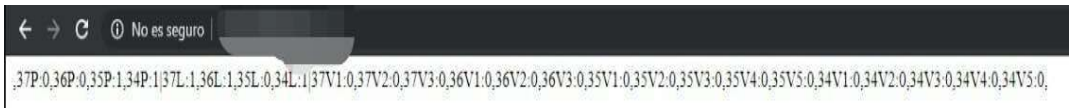

Figura 3.42 Pruebas desde la *Shield Ethernet*

Esta es una de las primeras pruebas que se realizó para poder comprobar si algún elemento está funcionando de manera errónea, y solucionarlo de inmediato antes de proceder con la unión del aplicativo creado por los estudiantes de ASI.

Pruebas del Biométrico

Con la configuración de registro de usuarios, horarios y niveles de acceso que se encuentra detallado en el Anexo IV, y cargado en cada uno de los biométricos ZKTeco SF300, se procede con pruebas de ingreso a las aulas por parte de profesores en el horario que dictan clases. Así como se observa en la figura 3.43, la Ingeniera Mónica Vinueza se encuentra ingresando al aula con su huella en el horario que le corresponde, accediendo sin ningún inconveniente.

Figura 3.43 Ingreso con huella por parte de profesores

Con esto se comprueba que la restricción de ingreso a las aulas se ha realizado de manera correcta y que en otro horario que no corresponde al ingreso de los profesores, no podrían acceder al aula.

Para verificar que los tres biométricos se encuentran en línea, se accede desde el servidor, lugar donde se encuentra instalado el *software* ZK Access 3.5, y como se muestra en la figura 3.44 cuando los biométricos se encuentren de color café estarán en red.

Una vez que los biométricos se encuentren en red se procede a realizar pruebas de apertura desde el *software* ZK Access 3.5, se puede seleccionar el aula que se requiere abrir, como se ve en la figura 3.44, en la cual aparecerá el menú de apertura de puerta, donde se debe percatar que el **tiempo de apertura** sea de 1 segundo; si el tiempo es mayor, puede ocasionar que la chapa se queme.

Figura 3.44 Apertura remota

Pruebas desde el aplicativo

El aplicativo que ha sido creado por estudiantes de ASI, realiza de una manera más gráfica y amigable el estado en el que se encuentran las ventanas, puertas y luminarias, así como se observa en la figura 3.45.

Además de enviar el estado, también se puede realizar lo que es la apertura de puertas, que se interrelaciona con el biométrico ZKTeco SF 300 para que pueda abrir la chapa, así como se mencionó en las secciones anteriores del documento. Si una luminaria se encuentra encendida y la persona que monitorea el sistema decide apagarla desde el mismo aplicativo, se puede mandar la orden, de igual manera para encenderla.

Figura 3.45 Aplicativo

En comparación con las pruebas realizadas directamente con la *shield ethernet*, el monitoreo es similar en el aplicativo, con la diferencia de que ya no se evidencian 1L o 0L para saber el estado de puertas, ventanas y luminarias. Sino que se verá la palabra abierta, cerrada, encendida o apagada, dependiendo el caso; así se puede observar en la figura 3.46.

34	***PUERTA ABIERTA***	***LUCES ENCENDIDAS***		Ventana Cerrada	***VENTANA ABIERTA***	Ventana Cerrada	Ventana Cerrada	Ventana Cerrada
	2019-12-16 11:54:24	2019-12-16 11:54:24		2019-12-16 11:54:24	2019-12-16 11:54:24	2019-12-16 11:54:24	2019-12-16 11:54:24	2019-12-16 11:54:24
35	***PUERTA ABIERTA***	***LUCES ENCENDIDAS***		Ventana Cerrada	Ventana Cerrada	Ventana Cerrada	Ventana Cerrada	***VENTANA ABIERTA***
	2019-12-16 11:54:24	2019-12-16 11:54:24		2019-12-16 11:54:24	2019-12-16 11:54:24	2019-12-16 11:54:24	2019-12-16 11:54:24	2019-12-16 11:54:24
36	***PUERTA ABIERTA***	***LUCES ENCENDIDAS***				Ventana Cerrada	***VENTANA ABIERTA***	***VENTANA ABIERTA***
	2019-12-16 11:54:24	2019-12-16 11:54:24				2019-12-16 11:54:24	2019-12-16 11:54:24	2019-12-16 11:54:24

Figura 3.46 Monitoreo de las aulas desde el aplicativo

Por consiguiente, el aplicativo es la recopilación de todo el sistema que se ha creado; es decir, la unión del sistema biométrico y del sistema de automatización, en el cual el Arduino procesa todas estas señales de sensores y luminarias para ser procesadas y crear un aplicativo con una interfaz gráfica que permite el manejo de manera más fácil del proyecto.

3.8 Costos de implementación

En la Tabla 3.5 se presentan los costos asociados al proyecto correspondiente a las aulas 34, 35 y 36.

Tabla 3.5 Costos de implementación

DETALLE	V. UNITARIO	CANTIDAD	V. TOTAL
Arduino Mega	$ 20,00	1	$ 20,00
Shield Ethernet	$ 15,00	1	$ 15,00
Chapa	$ 59,00	3	$ 177,00
Biométrico ZKTeco SF300	$ 164,21	3	$ 492,63
Reguladores de tensión	$ 5,60	1	$ 5,60
Bobina UTP	$ 120,00	1	$ 120,00
Funda conectores RJ45	$ 5,89	1	$ 5,89
Funda Capuchones	$ 4,26	1	$ 4,26
Fuentes de biométricos	$ 20,10	3	$ 60,30
Grapas	$ 2,00	1	$ 2,00
Pulsadores	$ 0,60	1	$ 0,60
Canaletas	$ 1,80	3	$ 5,40
Amarras	$ 2,50	1	$ 2,50
Material para elaboración de placas	$ 10,73	1	$ 10,73
Switch TP-LINK de 8 puertos	$ 14,00	1	$ 14,00
Cinta Etiquetadora BRADY 3/4	$ 30,00	1	$ 30,00
Tablero 30x30x20. SIMOTIC	$ 34,07	1	$ 34,07
Stickers	$ 4,00	1	$ 4,00
Tornillos y tacos *Fisher*	$ 10,00	1	$ 10,00
Sensores	$ 1,15	16	$ 18,40
Rollo de Manguera 3/4	$ 87,00	2	$ 174,00
Soporte *switch*	$ 10,00	1	$ 10,00
Rollo Cable 20 AWG	$ 13,75	4	$ 55,00
Sacabocados	$ 10,00	1	$ 10,00
Canaleta granulada 25x25	$ 2,50	1	$ 2,50
TOTAL	$ 648,16		$ 1283,88

Nota: *Los rubros mencionados en la Tabla 3.5 solo abarcan costos de materiales y equipos utilizados; no se ha colocado el valor de la mano de obra.*

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Un sistema biométrico es una de las mejores opciones de seguridad cuando se trata de permitir o negar el ingreso a las aulas, debido a que autentica a usuarios según su respectiva huella dactilar, la cual es única para cada persona, evitando así que personas ajenas a la institución o que no han sido registradas puedan ingresar a las aulas. De este modo se permite el ingreso únicamente a profesores, personal administrativo y personal de limpieza, garantizando de esta manera que las instalaciones permanezcan seguras y sin daños a su infraestructura.
- El sistema de control automatizado y de acceso evita que estudiantes y personas ajenas a la ESFOT ingresen a las aulas para ingerir bebidas alcohólicas, estupefacientes o realizar acciones que no cuentan con ningún permiso por parte de las autoridades, ya que con el monitoreo de las aulas se puede actuar de inmediato en caso de existir ingresos por ventanas o puertas, en horarios que las aulas permanecen vacías.
- Por medio del *software* ZK Access 3.5 se obtiene un registro de ingreso a cada una de las aulas, con su respectiva hora e información del profesor que ha ingresado, debido a que en cada biométrico ZKTeco SF 300 ha sido configurada la carga académica del personal docente.
- Todo profesor que previamente haya sido registrado con su horario de clases y materia en su respectiva aula podrá ingresar en todo ese lapso de tiempo las veces que requiera.
- Con el monitoreo de las aulas se evita que las puertas o ventanas se encuentren abiertas en horarios que no deberían estar; de igual manera, con el monitoreo de las luminarias se reduce el mal uso de la energía eléctrica por permanecer encendidas sin que nadie se encuentre en el aula, apagándolas en caso de que se encuentren encendidas.
- Las chapas eléctricas son sensibles en el aspecto que no soportan mucho tiempo una corriente eléctrica, debido a que estas solo necesitan un pulso de máximo un segundo para poder ser accionada y abrir la puerta.
- Se debe colocar los elementos que utilizan corriente alterna separados de los elementos de red, para evitar que exista interferencia y perjudique el funcionamiento del sistema, para lo cual los cables de red no deben ir por la misma manguera que van los cables de alimentación.

- Utilizar un *switch* no administrable con una velocidad de transmisión 10/100 Mbps es suficiente para el proyecto, ya que la información que se está transmitiendo no demanda alta tasas de envío.
- El etiquetado de cables es importante, ya que favorece al momento de realizar las conexiones, debido a que existen varios cables que se conectan al módulo Arduino, los mismos que teniendo su etiqueta será más fácil de conectarlo en caso de desconexión.

4.2 Recomendaciones

- Para que exista un correcto funcionamiento sin que exista la pérdida de señal proveniente de la *shield ethernet*, esta debe ser compatible con el modelo de Arduino para que así se logra tener un correcto funcionamiento del sistema.
- Es necesario que todo el cableado vaya por mangueras o canaletas, esto es indispensable para que el cable no sea averiado o maltratado.
- Forrar bien las uniones de los cables, ya que la temperatura que genera la corriente que pasa por ellos, daña el aislante y deja el cable desnudo en donde puede ocurrir un corto circuito.
- Es necesario colocar un disipador de calor en el transistor que se encuentra en la placa electrónica, para evitar sobrecalentamientos.
- Conectar un diodo en los terminales de la chapa eléctrica, ya que esto impide que la corriente viaje en ambas direcciones, debido a que, si esto se da, la bobina de la chapa eléctrica estará energizada todo el tiempo y así dañará y quemará el sistema eléctrico que se encuentra dentro de la chapa eléctrica.
- Conectar correctamente los sensores magnéticos, ya que no deben estar a más de un 40% desalineado, si esto ocurre los sensores magnéticos no podrán leer el estado de la puerta o ventana, debido a que el sensor magnético no cerrará el circuito.
- Utilizar códigos diferentes cuando se crean materias con el mismo nombre, debido a que existe más de un profesor dictando la misma materia y esto puede traer confusiones al momento de la asignación de profesor y materia en el biométrico.
- Con la ayuda de las cámaras de seguridad instaladas en los pasillos de la ESFOT se puede incorporar un trabajo conjunto entro los dos proyectos para conocer quien ingresa a las aulas además, de realizar una extensión del proyecto el cual abarque la creación de una aplicación móvil en donde se reciba las notificaciones de apertura de puertas y ventanas.

5. BIBLIOGRAFÍA

[1] A.Córcoles, Arduino. Curso Práctico, Madrid: RA-MA, 2018.

[2] Ó. T. Artero, El mundo GENUINO ARDUINO. Curso práctico de formación, Mexico: Alfaomega, 2016.

[3] R. Shop, «Arduino Mega 2560 Datasheet,» [En línea]. Available: https://www.robotshop.com/media/files/pdf/arduinomega2560datasheet.pdf. [Último acceso: 12 11 2019].

[4] «Aprendiendo Arduino,» [En línea]. Available: https://aprendiendoarduino.wordpress.com/2016/07/04/ethernet-shield/. [Último acceso: 12 11 2019].

[5] M. Latam, «Mecatronica Latam,» 30 Enero 2018. [En línea]. Available: https://www.mecatronicalatam.com/tutorial/es/sensores/sensor-magnetico. [Último acceso: 26 Noviemnre 2019].

[6] L. Lalamas, «MagneticReed,» 17 03 2018. [En línea]. Available: https://www.luisllamas.es/usar-un-interruptor-magnetico-con-arduino-magnetic-reed/. [Último acceso: 18 02 2020].

[7] CISCO, «Lo que usted necesita saber sobre routers y switches,» 2012. [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf. [Último acceso: 13 11 2019].

[8] DLINK, «8-Port 10/100 Switch,» [En línea]. Available: https://dlink-me.com/pdf/DES-1008A.pdf. [Último acceso: 25 11 2019].

[9] «MacroCity,» [En línea]. Available: https://www.macrocitygt.com/switch-8-puertos-d-link-10-100-des-1008a/. [Último acceso: 13 11 2019].

[10] N. G. M. J. L. C. L. Marquez Moreno Ingrid Julieth, «SISTEMA DE CONTROL DE ACCESO POR BIOMETRÍA,» [En línea]. Available: http://repository.udistrital.edu.co/bitstream/11349/7502/1/MarquezMorenoIngridJulieth2017Ni%C3%B1oGarzonMichaelJohanes2017.pdf. [Último acceso: 13 11 2019].

[11] D. S. Zorita, «Reconocimiento automatico mediante patrones biometricos de huella dactilar,» 2003. [En línea]. Available: http://oa.upm.es/79/1/09200327.pdf?iframe=true&width=80%25&height=80%25. [Último acceso: 13 11 2019].

[12] ZKTECO, «SF300 Terminal IP con lector de huella,» 2015. [En línea]. Available: https://www.zktecolatinoamerica.com/documentos/control-de-acceso/standalone/SF300/SF300.pdf. [Último acceso: 25 11 2019].

[13] «ZKTECO,» [En línea]. Available: http://cdn.sego.com.pe/files/2018/07/18/ZK-4500.pdf. [Último acceso: 18 11 2019].

[14] ZKTECO, «Ficha tecnica ZK 4500,» [En línea]. Available: http://190.180.49.82/lista-precios/pdf/ZK4500.pdf. [Último acceso: 25 11 2019].

[15] I. M. J. A. A. G. I. d. V. C. F. I. C. J. N. C. R. Francisco Falcone, Instalaciones de telecomunicaciones para edificios, Barcelona: Marcombo, 2017, p. 555.

[16] «JuantecnoDigital,» 09 Noviembre 2016. [En línea]. Available: https://www.tecnodigital.net/2015/10/ponchado-de-cable-utp-norma-tiaeia-568b.html. [Último acceso: 26 Noviembre 2019].

[17] E. R. Rodriguez, «Norma ANSI/TIA/EIA-569,» 31 Julio 2015. [En línea]. Available: https://prezi.com/5qqqtaqyzgm0/norma-ansitiaeia-569/. [Último acceso: 26 Noviembre 2019].

[18] BlueIT, «BlueIT,» 09 Agosto 2017. [En línea]. Available: https://blueit.com.ec/blog/item/358-que-es-un-cable-de-red-utp-y-sus-mejoras.html. [Último acceso: 26 Noviembre 2019].

[19] M. Cansino, «Techlandia,» 23 Mayo 2019. [En línea]. Available: https://techlandia.com/cable-utp-sobre_10903/. [Último acceso: 26 Noviembre 2019].

[20] Joussef, «Mundo Teleco,» 4 10 2014. [En línea]. Available: http://mundotelecomunicaciones1.blogspot.com/2014/10/como-ponchar-un-cable-utp-con-un.html. [Último acceso: 26 11 2019].

[21] E. d. Rio, «Blog de Fibra Óptica y Redes del CIFP Tartanga,» 27 Junio 2013. [En línea]. Available: http://fibraoptica.blog.tartanga.eus/2013/06/27/una-pregunta-clasica-por-que-se-utiliza-cable-de-pares-trenzados-en-el-cableado-estructurado/. [Último acceso: 26 Noviembre 2019].

[22] «Telecomunicaciones, Uncategorized,» 20 Septiembre 2017. [En línea]. Available: https://www.telecocable.com/blog/ventajas-y-desventajas-del-cable-utp/1385. [Último acceso: 26 Noviembre 2019].

[23] Tanenbaum, Computer Networks, España: Pearson, 2017.

[24] «Direccionamiento IPv4,» [En línea]. Available: http://isa.uniovi.es/docencia/SIGC/pdf/direccionamiento-ip.pdf. [Último acceso: 21 11 2019].

[25] L. ESFOT, «Cuida la ESFOT,» 2016. [En línea]. Available: https://www.youtube.com/watch?v=QAHCkj_cZXU. [Último acceso: 26 11 2019].

[26] «TIA 606 C,» [En línea]. Available: https://d37iyw84027v1q.cloudfront.net/Common/TIA_606_Labeling_Standards_ebook_Latin_America.pdf. [Último acceso: 17 12 2019].

ANEXOS