

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y CONTROL DE ACCESO PARA LAS AULAS 27, 28 Y 29 DE LA ESFOT

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

EDUARDO VINICIO CASTRO ROJAS

eduardo.castro@epn.edu.ec

MARCO ANDRÉS MARTÍNEZ IPIALES

marco.martinez01@epn.edu.ec

DIRECTOR: ING. PABLO ANDRÉS PROAÑO CHAMORRO

pablo.proano@epn.edu.ec

CODIRECTOR: ING. FABIO MATÍAS GONZÁLEZ GONZÁLEZ MSC.

fabio.gonzalez@epn.edu.ec

Mayo, 2020

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Eduardo Vinicio Castro Rojas y Marco Andrés Martínez Ipiales, bajo nuestra supervisión.



Ing. Pablo Andrés Proaño Chamorro

DIRECTOR DE PROYECTO

Ing. Fabio Matías González González MSc.

CODIRECTOR DE PROYECTO

DECLARACIÓN

Nosotros, EDUARDO VINICIO CASTRO ROJAS y MARCO ANDRÉS MARTÍNEZ IPIALES, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentada 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.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Eduardo Vinicio Castro Rojas



Marco Andrés Martínez IpiALES

AGRADECIMIENTO

Agradezco a mi Dios por la sabiduría que me otorgo durante mi formación profesional, la gloria y honra para ti JESUS.

Mi más grande agradecimiento a mi amada esposa quien fue mi apoyo incondicional durante toda mi carrera.

A mi madre por enseñarme a perseverar y esforzarme para conseguir las metas propuestas.

A todos los docentes de la institución quienes compartieron sus conocimientos profesionales.

Y en especial al Ing. Pablo Proaño e Ing. Fanny Flores por todo su apoyo durante la ejecución del presente proyecto integrador.

Eduardo

DEDICATORIA

El presente proyecto integrador lo dedico a todos los estudiantes de la carrera de electrónica y telecomunicaciones, esperando que lo plasmado en este documento sirva como guía para futuras instalaciones o mantenimientos de sistemas de control de acceso y automatización.

Eduardo

AGRADECIMIENTO

Agradezco primeramente a Dios por derramar muchas bendiciones en mi vida.

A mis padres, por brindarme su apoyo incondicional en los estudios para perseverar en la vida dejándonos la mejor herencia el estudio.

A mis hermanos quienes me dieron fuerzas para salir adelante en el estudio gracias a sus palabras de confianza y motivación de sus objetivos logrados.

Marco

DEDICATORIA

Este trabajo está dedicado principalmente a mi madre porque cada día han trabajado duro y ha estado pendiente de mi persona por salir adelante en el estudio. Su sacrificio y amor hacia nosotros es su mejor regalo.

Marco

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN	1
1.1 Planteamiento del problema	1
1.2 Justificación.....	1
1.3 Objetivos	3
1.4 Antecedentes	3
Módulo Arduino Mega 2560	3
Módulo <i>Shield Ethernet</i>	4
Tecnología de red <i>Ethernet</i>	4
Cable UTP Cat. 5e.....	5
<i>Switch</i> 8 o 5 puertos.	5
Terminal IP con lector de huella digital SF-300 (Biométrico).....	6
Enrolador de huella dactilar ZK-4500.....	7
<i>Software</i> de escritorio ZK-Access3.5	7
Cerradura eléctrica	8
Regulador de voltaje FORZA FVR-3001.....	9
Tablero metálico de pared.	10
2. METODOLOGÍA	11
2.1 Tipo de investigación.....	11
2.2 Descripción de la metodología usada	11
3. RESULTADOS Y DISCUSIÓN.....	12
3.1 Requerimientos del sistema de monitoreo y control de acceso.	14
Inspección técnica-visual del estado de las aulas	14
Estructura de red, dispositivos y equipos del sistema.	16
Direccionamiento IP de la red y habilitación de puertos <i>switch</i> DGIP.....	20
Establecimiento de las ubicaciones de los tableros.	22
3.2 Instalación del cableado y equipos de la red.	22
Elaboración de los planos de la tubería, cableado para la red de datos y sensores.....	23
Dimensionamiento de la cantidad de cable UTP, 20 AWG y demás materiales.	25
Armado de la tubería y tendido del cableado de red y sensores.	28
Reconocimiento, ponchado y etiquetado del cableado de red.	34
Montaje y conexión de equipos de red.....	39
3.3 Implementación del sistema biométrico y mecánico	46

Elaboración e instalación de una placa PCB para el manejo del sistema mecánico.	46
Montado del equipo biométrico y cerradura eléctrica.	51
Instalación del <i>software</i> de administración de los biométricos.	55
Configuración del <i>software</i> ZKAccess 3.5 para el control de acceso.	57
Levantamiento de la base de datos y creación de niveles de acceso.	59
Registro de huellas dactilares de usuarios y descarga de información a terminales biométricos.....	65
3.4 Pruebas y análisis de resultados	68
Pruebas del ponchado	68
Pruebas de comunicación de red.....	69
Pruebas de funcionamiento del biométrico y cerradura eléctrica	72
4. CONCLUSIONES Y RECOMENDACIONES.	75
4.1 Conclusiones.....	75
4.2 Recomendaciones.....	76
5. REFERENCIAS BIBLIOGRAFICAS	78
6. ANEXOS.....	82
ANEXO A: ANTECEDENTES.	82
ANEXO B: CONTEO DE PUERTAS Y VENTANAS DEL GRUPO DE AULAS N° 3 Y N° 4.	82
ANEXO C: PLANOS DE UBICACIÓN DE RACKS Y CABLEADO DE RED.....	82
ANEXO D: DIAGRAMA DE RED.	82
ANEXO E: DIAGRAMA ESQUEMÁTICO DEL SISTEMA CENTRAL DE CONTROL.	82
ANEXO F: EXPLICACIÓN DEL CÓDIGO Y DIAGRAMA DE FLUJO DEL PROGRAMA.	82
ANEXO G: TABLA DE DIÁMETRO Y RESISTIVIDAD DE CABLE ELECTRICO.	82
ANEXO H: ESQUEMA DE CONEXIÓN DEL SISTEMA MECÁNICO.	82
ANEXO I: CONFIGURACIÓN DEL <i>SOFTWARE</i> ZKACCESS 3.5.	82

ÍNDICE DE FIGURAS

Figura 1.1 Partes del módulo Arduino Mega 2560.	3
Figura 1.2 Módulo <i>Shield Ethernet</i>	4
Figura 1.3 Terminal biométrico SF300.	6
Figura 1.4 Enrolador de huella dactilar ZK4500.	7
Figura 1.5 Interfaz gráfica del <i>software</i> ZKAccess 3.5.	8
Figura 1.6 Cerradura eléctrica marca TRAVEX.	9
Figura 1.7 Regulador de voltaje Marca FORZA FVR-3001.	10
Figura 3.1 Identificación de las partes del proyecto.	14
Figura 3.2 Diagrama de la topología física en estrella implementada.	17
Figura 3.3 Terminal biométrico modelo SF300 Marca ZK-Teco.	18
Figura 3.4 Arduino Mega 2560.	18
Figura 3.5 Módulo <i>Shield Ethernet</i> acoplado al Arduino Mega 2560.	19
Figura 3.6 <i>Switch</i> marca D-LINK modelo DES 1008C.	20
Figura 3.7 Diagrama de la topología logica.	21
Figura 3.8 Ubicación de los tableros de ET y EM del grupo de aulas N° 3 y N° 4.	22
Figura 3.9 Elementos principales del cableado estructurado y equipos de red.	23
Figura 3.10 Dimensionamiento de cable UTP para las aulas 27 y 28.	25
Figura 3.11 Dimensionamiento de cable UTP para el aula 29.	26
Figura 3.12 Cableado horizontal con manguera anillada PVC.	28
Figura 3.13 Tendido del cable UTP cat. 5e y de los cables eléctricos 20AWG.	31
Figura 3.14 Instalación de la tubería que incluye cable de red y eléctrico.	31
Figura 3.15 Canaletas bajantes desde el techo falso a los dispositivos y tableros del sistema.	33
Figura 3.16 Ponchado y etiquetado del cable de red del sistema.	35
Figura 3.17 Ponchado de cable UTP cat 5e.	36
Figura 3.18 Etiquetado del cableado de red del sistema.	36
Figura 3.19 Modelo de etiquetado que establece la DGIP.	37
Figura 3.20 <i>Switch</i> 8 puertos D-Link, Módulo <i>Shield Ethernet</i> Arduino Mega.	39
Figura 3.21 Etapas del sistema de monitoreo y control.	40
Figura 3.22 Ubicación de módulos Arduino y componentes electromecánicos.	40
Figura 3.23 Montado del Módulo <i>Shield Ethernet</i> y Arduino Mega.	41
Figura 3.24 Distribución de pines del módulo Arduino Mega.	42
Figura 3.25 Tablero ET N° 3 y N° 4 con sus dimensiones.	44

Figura 3.26 Tablero metálico de ET.....	45
Figura 3.27 Cables de conexión conectados a los <i>switches</i> de acceso N° 3 y N° 4.....	46
Figura 3.28 Placa PCB – Circuito de conmutación.	46
Figura 3.29 Diagrama esquemático de la placa PCB-circuito de conmutación.....	47
Figura 3.30 Circuito PCB-conmutación.	50
Figura 3.31 Fuente de alimentación terminal biométrico.	52
Figura 3.32 Terminales biométricos instalados.	53
Figura 3.33 Conexión y montaje del biométrico.	53
Figura 3.34 Cerradura eléctrica y sus partes.	54
Figura 3.35 Montado de la cerradura eléctrica.....	55
Figura 3.36 Interfaz principal del <i>software</i> ZKAccess 3.5.....	56
Figura 3.37 Servidor local del sistema.	57
Figura 3.38 Esquema del proceso de configuración de red del dispositivo.	57
Figura 3.39 Esquema del proceso para agregar dispositivos.	58
Figura 3.40 Dispositivos agregados en la interfaz del <i>software</i> ZkAccess 3.5.....	58
Figura 3.41 Interfaz para agregar usuarios.	60
Figura 3.42 Interfaz para agregar horarios.....	61
Figura 3.43 Interfaz para agregar niveles de acceso.	64
Figura 3.44 Interfaz para registro de huellas dactilares.....	66
Figura 3.45 Esquema de sincronización de información a los dispositivos.	67
Figura 3.46 Prueba de restricción de acceso.	73

ÍNDICE DE TABLAS

Tabla 1.1 Características del cable UTP Cat. 5e CONNECTION.	5
Tabla 1.2 Características del <i>Switch</i> D-LINK modelo DES 1008C.....	5
Tabla 1.3 Características técnicas del biométrico SF300.	6
Tabla 1.4 Características del <i>host</i> -local para instalación del <i>software</i> ZKAccess 3.5.	8
Tabla 1.5 Características de la cerradura eléctrica marca TRAVEX.....	9
Tabla 1.6 Características técnicas del regulador de voltaje FORZA FVR-3001.....	9
Tabla 1.7 Características del tablero metálico.....	10
Tabla 3.1 División de aulas en grupos.	12
Tabla 3.2 Condiciones del recorrido del cableado de red.....	15
Tabla 3.3 Conteo de puertas y ventanas aulas 27, 28 y 29.	15
Tabla 3.4 Número de direcciones IP solicitadas a la DGIP.....	20
Tabla 3.5 Características configuración de VLAN para el sistema por parte de la DGIP.	20
Tabla 3.6 Habilitación de puertos en los <i>switches</i> de la intranet de la ESFOT.	21
Tabla 3.7 Recorrido del cableado de red del sistema para las aulas 27, 28 y 29.	24
Tabla 3.8 Recorrido del cable eléctrico 20 AWG de los sensores para las aulas 27, 28 y 29. ...	24
Tabla 3.9 Dimensionamiento de cable eléctrico 20 AWG para los sensores de las ventanas y puertas.....	27
Tabla 3.10 Materiales empleados en el cableado horizontal.	27
Tabla 3.11 Características de la manguera corrugada PVC.....	30
Tabla 3.12 Recorrido de la tubería PVC sobre el techo falso de las aulas 27, 28 y 29.	32
Tabla 3.13 Canaletas utilizadas en el proyecto.	34
Tabla 3.14 Nomenclatura del etiquetado del cableado de los biométricos.	37
Tabla 3.15 Nomenclatura del etiquetado del cable UTP del <i>switch</i> de acceso al <i>switch</i> de la DGIP.	38
Tabla 3.16 Nomenclatura del etiquetado del cable UTP del Arduino al <i>switch</i> de la DGIP.	38
Tabla 3.17 Conexión de los pines del Arduino Mega hacia los elementos eléctricos y sensores.	42
Tabla 3.18 Conexión de los pines del Arduino Mega hacia los elementos eléctricos y sensores.	43
Tabla 3.19 Elementos conectados a las borneras de la placa PCB.....	47
Tabla 3.20 Elementos electrónicos de la placa PCB.	48
Tabla 3.21 Características técnicas transistor TIP 122.....	48

Tabla 3.22 Características del <i>host</i> local solicitado para instalación del <i>software</i> ZKAccess 3.5.	56
Tabla 3.23 Nombre asignado en el <i>software</i> a cada terminal biométrico.....	58
Tabla 3.24 Respaldos de la base de datos para las aulas 27, 28 y 29.	62
Tabla 3.25 Administración de horarios, control y niveles de acceso.	62
Tabla 3.26 Nivel de acceso para el usuario Administrador.	63
Tabla 3.27 Nombre asignado en el <i>software</i> a cada terminal biométrico.....	65
Tabla 3.28 Prueba del cable de red ponchado con la norma T568-B.	68
Tabla 3.29 Datos recibidos del estado de las puertas, luminarias y ventanas de las aulas 27 y 28.	69
Tabla 3.30 Datos recibidos del estado de la puerta, luminarias y ventanas del aula 29.	69
Tabla 3.31 Apertura remota de puertas y luminarias de las aulas 27, 28 y 29 desde el servidor.	70
Tabla 3.32 Apertura remota de luminarias de las aulas 27, 28 y 29 desde el servidor.	70
Tabla 3.33 Prueba de conexión del módulo <i>Shield Ethernet</i>	71
Tabla 3.34 Tipo de identificación de control de acceso registrado.....	72
Tabla 3.35 Apertura remota de las aulas 27, 28 y 29 desde el <i>software</i> ZKAccess 3.5.....	73
Tabla 3.36 Prueba de funcionamiento de la placa de conmutación.....	74

RESUMEN

El presente proyecto de titulación, “IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y CONTROL DE ACCESO PARA LAS AULAS 27, 28 Y 29 DE LA ESFOT”, integra un sistema de automatización y de seguridad para el acceso a las aulas de la ESFOT, en donde los equipos biométricos implementados en las aulas permitirán a los profesores acceder a las mismas mediante el reconocimiento de la huella dactilar, además, de registrar en línea el reporte de control de acceso de cada profesor. El desarrollo del proyecto que se detalla en este documento está conformado por cuatro secciones.

En el capítulo uno se presenta una breve introducción, la identificación del problema como punto de partida de la necesidad de implementar un sistema automatizado. De igual manera en la justificación se indican las razones sobre quiénes y por qué se benefician del proyecto, los objetivos específicos planteados para cumplir con el objetivo general, además de la definición de algunos conceptos de interés.

En el capítulo dos se menciona el tipo de metodología usada y las actividades realizadas que cumplieron con cada uno de los objetivos específicos a partir de un estudio efectuado en las aulas 27, 28 y 29 de la ESFOT.

El capítulo tres trata los resultados y discusiones acerca del estudio de requerimientos previo a la ejecución del proyecto y la instalación del cableado estructurado junto con los dispositivos de red. También, se describe la implementación del sistema biométrico-mecánico para la apertura de la puerta, además de las pruebas realizadas del ponchado, de la comunicación de la red y del sistema biométrico-cerradura eléctrica para verificar el correcto funcionamiento.

En el capítulo cuatro se exponen las conclusiones y las recomendaciones de la ejecución y funcionamiento del proyecto implementado.

Palabras clave: Sistema de monitoreo, Equipos biométricos, Cableado estructurado.

ABSTRACT

The present project of degree "IMPLEMENTATION OF A MONITORING AND ACCESS CONTROL SYSTEM FOR CLASSROOMS 27, 28 AND 29 OF THE ESFOT" integrates an automation and security system for access to ESFOT classrooms, where the biometric equipment implemented in the classrooms will allow teachers to access them by recognizing the fingerprint, in addition, to registering online the access control report of each teacher. The development of the project detailed in this document consists of four sections.

The section one presents a brief introduction, the identification of the problema as starting point of the necessity to implement an automated system. Similarly the justification indicates the reasons for who and why benefit from the project, the specific objectives set to accomplish with the general objective, in addition to the definition of some concepts of interest.

Section two mentions the type of methodology used and the activities carried out that fulfilled each of the specific objectives from a study accomplished in classrooms 27, 28 and 29 of the ESFOT.

The section three refers the results and discussions about the study of requirements previous to the execution of the project and the installation of the structured cabling together network devices. Also, it describes the implementation of the biometric-mechanical system for opening the door, in addition to the tests performed of the crimped, of the network communication and the biometric-electric lock system to verify correct operation.

The section four exposes the conclusions and recommendations of execution and operation of the implemented project.

Keywords: *Monitoring system, Biometric equipment, Structured cabling.*

1. INTRODUCCIÓN

1.1 Planteamiento del problema

Un estudio realizado por la FUNDACIÓN MAPFRE refleja que un 82% de centros educativos al no contar con medidas de protección tanto físicas como electrónicas han sufrido robos y daños de sus bienes materiales, además de intrusiones de personas ajenas a la Institución. El estudio revela que el 25% de unidades educativas que han tomado medidas de protección electrónicas para controlar el acceso han tenido una mejora de seguridad en sus instalaciones. (FUNDACIÓN MAPFRE, 2012)

Siendo la Escuela de Formación de Tecnólogos (ESFOT), una unidad académica la cual en sus instalaciones (aulas) no tenía un sistema que controle, monitoree y restrinja el acceso a las mismas, surgió el problema de acceso de personal no autorizado a las aulas. Lo cual provocaba el uso innecesario de la energía eléctrica en horarios donde las instalaciones no eran utilizadas para actividades educativas, además de la destrucción de los bienes que se encontraban en el interior de estas.

Teniendo en cuenta los diferentes problemas que se presentaban debido al acceso de personal no autorizado a las instalaciones, se propuso el proyecto de un sistema de monitoreo y control de acceso para las aulas de la ESFOT. El sistema tiene el objetivo de facilitar el monitoreo del estado abierto o cerrado de ventanas, puertas y el estado encendido/apagado del sistema de iluminación, así como la apertura de las puertas y del control del encendido y apagado de las luces, además de controlar el acceso de los usuarios a las mismas mediante un sistema biométrico. El monitoreo y control de acceso de las aulas se realiza vía remota, desde una aplicación que está instalada en un *host* local que se encuentra ubicado en la dirección de la ESFOT.

1.2 Justificación

En la actualidad, el avance tecnológico en el campo de los sistemas de seguridad electrónica tanto en el sistema de video vigilancia, como en el de control de acceso ha tenido gran acogida por parte de instituciones públicas y privadas, debido a que la integración de los mencionados sistemas a las instalaciones de las empresas generan, ahorro energético, mejor control de ingreso de personal a áreas determinadas, incremento de niveles de seguridad, además de un respaldo

de información de eventos suscitados en las instalaciones de las empresas, pudiendo ser respaldada dicha información en la nube. (Muñoz, 2018)

Estas mejoras en la seguridad de los establecimientos se dan debido a que un sistema de control de acceso tiene como función principal la de validar la información del usuario, con la finalidad de permitir o denegar el acceso del mismo a un área determinada y controlar de forma remota el estado y apertura de la puerta que se esté monitoreando (Rivas, 2016). Una de las ventajas que presenta el mencionado sistema es la de registrar y entregar un informe con la información de los usuarios que hayan utilizado el sistema (ANIXTER INC, 2018)

El presente proyecto integrador se implementó en las aulas de la ESFOT, el cual solventa el acceso no autorizado a las mismas, mediante la implementación de un sistema de control de acceso biométrico con autenticación por huella dactilar el cual al ser un sistema de un nivel alto de confiabilidad debido a que las huellas dactilares son características físicas únicas e intransferibles en cada persona. Gracias a la funcionalidad que entrega el sistema biométrico de restringir el acceso a las aulas al personal únicamente autorizado, se ha logrado que las instalaciones no sean ensuciadas ni desordenadas y puedan ser utilizadas únicamente por los estudiantes y docentes autorizados a ingresar a las mismas. Siendo ellos los principales beneficiados al contar con las instalaciones limpias y ordenadas para su utilización (INTERPOL, 2018), (Cueva, 2015). Cabe señalar que al restringir el acceso únicamente a personal autorizado se lleva un control y cuidado de los bienes materiales que se encuentran en el interior de las aulas, beneficiando este control a toda la comunidad de la ESFOT.

Mientras que la implementación del sistema de monitoreo beneficia al personal de servicio, debido a que el mismo ahorra tiempo, al no requerir la apertura manual de las aulas cuando el personal docente lo requiere y al no necesitar supervisión en campo del estado en que se encuentran las luces, ventanas y puertas. El sistema de monitoreo que se desarrolló bajo un controlador, permite procesar y monitorear cada una de las señales emitidas por los sensores que están colocados en ventanas, puertas y luces. Consiguiendo de esta manera llevar un control en tiempo real del estado encendido o apagado de las luces, del estado abierto o cerrado de puertas y ventanas, además de permitir el encendido y apagado de las luces y la apertura de las puertas de cada una de las aulas vía remota (Cifuentes, 2014), (Michelena, 2016).

Siendo necesaria la transmisión y recepción de datos desde el controlador hacia un servidor local se incorporó un módulo de red al controlador, el cual ayuda a que exista comunicación entre ellos a través de una red *Ethernet* que se levantó en el proyecto (Reinoso & Banda, 2018). Cabe

recaltar que gracias al monitoreo en tiempo real y control del encendido y apagado de las luces vía remota se redujo y se controló el consumo innecesario de la energía eléctrica.

1.3 Objetivos

Objetivo general

Implementar un sistema de monitoreo y control de acceso para las aulas 27, 28 y 29 de la ESFOT.

Objetivos específicos

- Determinar los requerimientos del sistema de monitoreo y control de acceso.
- Instalar el cableado estructurado y equipos de red.
- Implementar el sistema biométrico y mecánico para la apertura de la puerta.
- Realizar pruebas y análisis de resultados.

1.4 Antecedentes

Mediante el desarrollo del proyecto se contemplaron las siguientes definiciones:

Módulo Arduino Mega 2560

El módulo Arduino Mega 2560, es un *hardware* libre de desarrollo, el cual posee elementos instalados en la placa como: cristal de cuarzo, microcontrolador Atmega 2560, conector USB, espadines hembra, resistencias, entre otros. Ver Figura 1.1. Las principales características del módulo son que cuenta con 54 entradas y salidas digitales y 16 entradas analógicas, lo cual le hace muy funcional para proyectos que manejen gran cantidad de sensores, 1 conector ICSP y un *Jack* de alimentación 7 - 12 (V_{DC}), además, de ser compatible con el módulo *Shield Ethernet* (ARDUINO.CL, s.f.). Para más detalles de las características del Arduino Mega 2560 ver Anexo A1. En la Figura 1.1 se muestra el módulo Arduino Mega 2560 con sus partes principales.

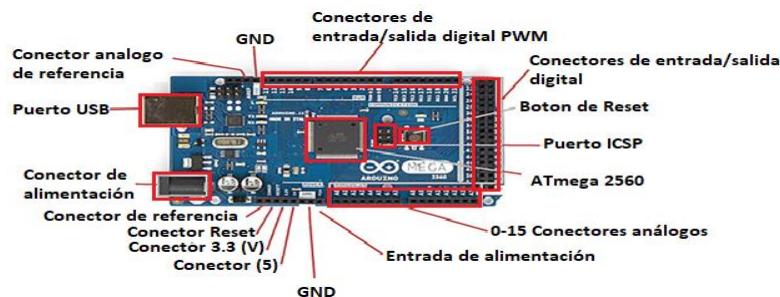


Figura 1.1 Partes del módulo Arduino Mega 2560.
Fuente: (Ediciones ENI, s.f.).

Módulo *Shield Ethernet*.

El módulo *Shield Ethernet*, es un dispositivo que otorga funciones de comunicación de red cableada a velocidades de transmisión de 10 / 100 (Mbps), solamente siendo insertado encima de una placa Arduino compatible (Arduino UNO, Arduino MEGA). La comunicación del módulo con la placa Arduino Mega se ejecuta mediante el bus SPI y el conector ICSP, de modo que no se pueden utilizar los pines 50, 51, 52 y 53 del Arduino Mega para que no exista ningún conflicto con el módulo *Shield Ethernet* al momento de la comunicación. (Keystudio, 2019)

El módulo contiene un conector RJ-45 utilizado para la conexión de red, un *chip Wiznet W5100* que contiene una pila de protocolos TCP/IP, espadines machos y hembras para montaje del módulo sobre las placas Arduino, un botón de *reset* que permiten resetear las placas conectadas y *leds* que indican el estado y funcionamiento del módulo (Web-Robótica, s.f.). Para más detalles ver Anexo A2. En la Figura 1.2 se muestra el módulo Arduino Mega 2560 con sus partes principales.

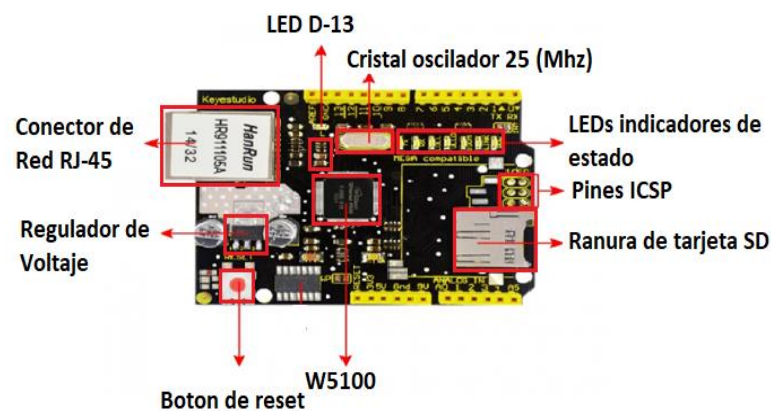


Figura 1.2 Módulo *Shield Ethernet*.

Fuente: (Keystudio, 2019).

Tecnología de red *Ethernet*.

Es un estándar de redes de computadores generalmente utilizado para redes de área local por cable definido en el estándar internacional IEEE802.3. Utiliza el método de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD). Esta tecnología soporta anchos de banda de 10, 100, 1000 o 10000 (Mbps) y con una topología física en estrella (ECURED, 2013). El proyecto se implementó en base a 100BASE-TX (*Fast Ethernet*) con cable UTP cat. 5e.

Cable UTP Cat. 5e

Está conformado por 4 pares de cobre trenzados no apantallados con cubierta de PVC. El cable UTP categoría 5e, es utilizado para transmitir señales de datos que trabaja hasta velocidades de hasta 100 (Mbps) en sistemas de redes *Ethernet* (CONNECTION, 2018).

En la Tabla 1.1 se presentan las características técnicas del cable UTP categoría 5e marca CONNECTION utilizado en el proyecto.

Tabla 1.1 Características del cable UTP Cat. 5e CONNECTION.

Descripción	Características
Cable UTP Cat. 5e marca CONNECTION.	4 pares trenzados de calibre 24 (AWG), cobre sólido. Cable para interiores. Soporta velocidades de transmisión hasta 100 (Mbps). Frecuencia hasta 100 (MHz). Diámetro de los conductores 24 (AWG). Diámetro del revestimiento 5.44 (mm) ± 0.2 (mm). Material de revestimiento PVC retardant a la llama. Máxima tensión de tracción 80 (N)

Fuente: (CONNECTION, 2018).

Switch 8 o 5 puertos.

Es un dispositivo de red utilizado para interconectar varios dispositivos a través de una misma red local, además de actuar como controlador para compartir información entre los diferentes dispositivos (D-LINK, 2018).

En la Tabla 1.2 se muestran las características técnicas del *switch* D-LINK modelo DES 1008C utilizado en el proyecto.

Tabla 1.2 Características del *Switch* D-LINK modelo DES 1008C.

Descripción	Características
<i>Switch</i> marca D-LINK DES 1008C	8 puertos <i>Fast Ethernet</i> 10/100 Base-TX. <i>Switch</i> no administrable. Soporta MDI/MDI-X en todos sus puertos. Dimensiones 131 x 82 x 22 (mm) Alimentación de 5 (V _{DC}) / 1 (A).

Fuente: (D-LINK, 2018).

Terminal IP con lector de huella digital SF-300 (Biométrico).

El SF300 es una terminal IP de huella digital, que opera de modo independiente. Se puede conectar con el *software* ZKAccess3.5 para control de acceso y gestión de tiempo y asistencia (ZKTECOLATINOAMERICA, 2015).

El reconocimiento y autenticación de la huella dactilar de un usuario se realiza mediante un lector de huellas dactilares, el cual escanea y recolecta la información de los dedos colocados en el mismo, comparando la información escaneada con la base de datos de usuarios que almacena el dispositivo, autenticando al usuario para permitir o denegar el acceso del mismo a una área determinada (INNGRESA, 2018).

En la Tabla 1.3 se presentan las características técnicas del equipo.

Tabla 1.3 Características técnicas del biométrico SF300.

Modelo	Características
Terminal biométrico SF300	Alimentación de 12 (V _{DC}) tolerancia ± 0.5 (V _{DC}) / 3 (A). Comunicación TCP/IP. Conector de red RJ-45. Soporta Administración para control de acceso mediante <i>software</i> ZKAccess 3.5. Función de control de acceso mediante lector huella digital. Permite el manejo de una cerradura eléctrica de 12 (V _{DC}) / 1 (A). Permite la recolección de 1500 huellas digitales. Permite la creación de 50 niveles de acceso distintos.

Fuente: (MEGACOM, 2018).

En la Figura 1.3 se muestra el biométrico SF300 utilizado en el proyecto como interfaz de control de acceso.



Figura 1.3 Terminal biométrico SF300.
Fuente: (ZKTECOLATINOAMERICA, 2015).

Enrolador de huella dactilar ZK-4500

Es un dispositivo que se encarga de capturar las huellas dactilares de los usuarios aplicado sobre su superficie óptica, para luego dicha información ser almacenada en un computador mediante una interfaz USB (TOP SECURITY PERU, s.f.) Ver anexo A3 características del enrolador de huellas dactilares ZK-4500.

En la Figura 1.4 se muestra el enrolador de huella dactilar ZK4500 utilizado en el proyecto.



Figura 1.4 Enrolador de huella dactilar ZK4500.
Fuente: (TOP SECURITY PERU, s.f.).

Software de escritorio ZK-Access3.5

El *software* de escritorio ZKAccess 3.5, es un *software* profesional de control de acceso que permite administrar a todos los modelos de terminales de control de acceso autónomo y paneles de control de acceso de la marca ZK-Teco.

El *software* de escritorio ZKAccess 3.5 entre sus funciones principales, permite la administración de una base de datos de usuarios, el monitoreo en tiempo real del estado de cada una de las puertas y generar reportes del uso de cada terminal biométrico (ZKTECOLATINOAMERICA, 2016).

Además, el *software* entrega la funcionalidad de monitoreo del estado del dispositivo de control de acceso en tiempo real, así como de la apertura remota de las puertas.

En la Tabla 1.4 se muestran las especificaciones del sistema operativo requerido para una correcta ejecución del programa.

Tabla 1.4 Características del *host*-local para instalación del *software* ZKAccess 3.5.

Software	Características requeridas Host-Local.
ZKAccess 3.5	Sistema Operativo requerido Windows 7/8/8.1/10 de 32/64 bits.

Fuente: (ZKTECOLATINOAMERICA, 2016).

En la Figura 1.5 se presenta la interfaz principal del *software* ZKAccess 3.5.



Figura 1.5 Interfaz gráfica del *software* ZKAccess 3.5.

Fuente: (ZKTECOLATINOAMERICA, s.f.).

Cerradura eléctrica

Una cerradura eléctrica es un sistema electromecánico conformado de una bobina la cual permite la apertura de la cerradura mediante una polarización eléctrica.

En la Tabla 1.5 se muestra las características técnicas de la cerradura de sobreponer de la serie TRAVEX ideal para puertas exteriores de madera, utilizada en el proyecto.

La cual posee un botón mecánico integrado y es adaptable a cualquier control de acceso con conexión eléctrica que realice pulsos secos a la cerradura (Ferrelectro, 2020)

Tabla 1.5 Características de la cerradura eléctrica marca TRAVEX.

Modelo	Características
Cerradura eléctrica	Voltaje de operación de 9 - 12 (V _{DC})/ 1 (A) para apertura remota de la puerta. Potencia de consumo 12 (W). Botón de accionamiento para apertura manual. Apertura de la cerradura mediante llaves.

Fuente: (Ferrelectro, 2020)

En la Figura 1.6 se presenta la cerradura eléctrica marca TRAVEX.



Figura 1.6 Cerradura eléctrica marca TRAVEX.

Regulador de voltaje FORZA FVR-3001.

El regulador automático de voltaje de la serie FVR brinda una protección adecuada a dispositivos eléctricos o electrónicos contra irregularidades como sobretensiones, fluctuaciones frecuentes de voltaje, garantizando de esta manera el suministro de energía estable y pura a las cargas (FORZAUPS, 2017).

Para la protección de los dispositivos eléctricos y electrónicos instalados en el proyecto se optó por adquirir un regulador de voltaje de marca FORZA modelo FVR-3001, el mismo que se dimensionó en base a la potencia total consumida por los dispositivos a conectarse.

En la Tabla 1.6 se muestran las características técnicas del regulador de voltaje de marca FORZA modelo FVR-3001 utilizado en el proyecto.

Tabla 1.6 Características técnicas del regulador de voltaje FORZA FVR-3001.

Dispositivo	Características:
Regulador automático de voltaje marca FORZA modelo FVR-3001.	Tipo de salida: 4 tomas de alimentación de 120 (V _{AC}). Potencia suministrada: 3000 (VA)/1500 (W). Regulación de tensión: 115 (V _{AC}) Protección contra sobrecargas: Interruptor. Margen de tensión de salida: 104 a 126 (V _{AC}). Margen de frecuencias: 50/60 (Hz). Dimensiones del dispositivo: 160x160x105 (mm). Peso neto: 2.9 (Kg).

Fuente: (FORZAUPS, 2017)

En la Figura 1.7 se presenta el regulador de voltaje marca FORZA FVR-3001 seleccionado.



Figura 1.7 Regulador de voltaje Marca FORZA FVR-3001.

Tablero metálico de pared.

Es una estructura metálica diseñada para el montaje de diferentes equipos de telecomunicaciones, eléctricos, UPS, y en general para cualquier equipo de instalación (BEAUCOUP, 2018).

Para el proyecto se utilizó un tablero metálico con medidas de 30x30x20 (cm), con grado de protección IP 41 que se refiere a protección contra polvo y caída de agua, el cual contendría equipos de red y un regulador de voltaje.

En la Tabla 1.7 se muestran las características del tablero metálico utilizado en el proyecto.

Tabla 1.7 Características del tablero metálico.

Modelo	Características
Gabinete metálico BEAUCOUP de pared.	Dimensiones: 30x30x20 (cm). Grado de protección IP: 41. Construcción del material: Láminas de acero inoxidable. Certificación nacional: INEN. Peso aproximado: 3.7 (Kg).

Fuente: (BEAUCOUP, 2018).

2. METODOLOGÍA

2.1 Tipo de investigación

El presente proyecto integrador consiste en un tipo de investigación aplicada, por lo que para su desarrollo se ha dividido en varias etapas: análisis de requerimientos, diseño, implementación, pruebas y análisis de resultados.

2.2 Descripción de la metodología usada

Para la implementación del sistema de monitoreo y control de acceso a las aulas, se cumplió las actividades que se detallan a continuación:

Se realizó una inspección técnica-visual sobre el estado de las aulas, para establecer la ruta adecuada del cableado, que sirvió para definir la estructura de red junto con los dispositivos de conectividad, y la gestión de un plan de direccionamiento IP para el sistema. Así mismo, se analizó la ubicación de los tableros de control que abarcan varias aulas, en este caso el tablero que está localizado en el aula 26 abarca a las aulas 27 y 28, mientras que el tablero ubicado en el aula 33 contiene al aula 29. Finalmente se estimó una cotización para el proyecto.

Con la ayuda del programa AutoCAD se elaboró el plano del cableado de red y de la tubería. Se dimensionó la cantidad de cable UTP y demás materiales para el cableado estructurado. Después se colocó la tubería (manguera anillada PVC), se realizó el tendido de cable de red a lo largo de todo el recorrido de la ruta establecida previamente, para proceder a reconocer, etiquetar y ponchar el cableado de red según el estándar ANSI/TIA 568-B. Por último, se montó los equipos de conectividad a la red del sistema.

Se construyó una placa PCB que sirve para manejar el sistema mecánico de apertura de la puerta, posteriormente se procedió a montar el equipo biométrico y la cerradura eléctrica. Después se instaló un *software* en un *host* local el cual permite administrar a los biométricos, una vez instalado el *software*, se creó una base de datos con la información de los horarios de las materias y datos personales de los usuarios. Levantada la base de datos se registró las huellas dactilares de los usuarios, para luego cargar la mencionada información a los equipos biométricos.

Se realizó las respectivas pruebas de funcionamiento, primero se efectuó un *test* de los cables ponchados, luego se ejecutaron pruebas de comunicación de la red del sistema. Finalmente se realizó pruebas de funcionamiento entre el sistema mecánico y el biométrico.

3. RESULTADOS Y DISCUSIÓN

El presente proyecto macro abarca un sistema de control de acceso biométrico IP, un sistema de monitoreo de puertas, ventanas y luces, automatización de la apertura de puertas, encendido y apagado de luces, y de una aplicación de control.

Para la ejecución del proyecto se integró a estudiantes de las carreras de Electromecánica (EM), Análisis de Sistemas Informáticos (ASI) y de Electrónica y Telecomunicaciones (ET), el mismo que se encuentra en funcionamiento desde septiembre del 2019.

Las aulas que se abarcaron para la implementación del sistema mencionado van desde el aula 13 hasta la 39, las cuales se dividieron en 5 grupos, excluyendo del proyecto las aulas utilizadas para laboratorios (14, 15, 16, 17, 20, 22-A, 22-B, 23, 31).

En la Tabla 3.1, se muestra la división de las aulas en los grupos realizados.

Tabla 3.1 División de aulas en grupos.

Nombre del grupo de aulas:	N° de aulas asignadas:	Aulas asignadas:
Grupo de aulas N° 1	2	Aula 38 y aula 39.
Grupo de aulas N° 2	4	Aula 37, aula 36, aula 35, aula 34.
Grupo de aulas N° 3	4	Aula 33, aula 32, aula 30, aula 29.
Grupo de aulas N° 4	5	Aula 28, aula 27, aula 26, aula 25, aula 24.
Grupo de aulas N° 5	4	Aula 21, aula 19, aula 18, aula 13.

Los estudiantes de la carrera de ET, realizaron la implementación del sistema de control de acceso biométrico IP y la programación del Arduino Mega el cual se encarga del control del sistema de automatización.

En el presente documento se abarca la implementación del sistema de monitoreo y control de acceso biométrico realizado en las aulas 27, 28 y 29.

Para el sistema de control de acceso biométrico IP, se utilizó un terminal biométrico de marca ZK-Teco, modelo SF300, el cual realiza la función de autenticación del usuario permitiendo o denegando el acceso del mismo al aula.

La base de datos con información de los usuarios del sistema se encuentra almacenada en un servidor local en la dirección de la ESFOT, en el cual se encuentra instalado el *software* ZKAccess 3.5.

El *software* permite administrar y cargar la información de la base de datos a los terminales biométricos.

La comunicación de datos entre los biométricos y el servidor local se ejecuta mediante una red LAN con topología en estrella implementada y enlazada a la intranet de la ESFOT.

La apertura de la puerta se realiza desde el biométrico como desde el Arduino Mega, gracias a la integración de una placa PCB con un circuito de conmutación, la cual permite el accionamiento de la cerradura eléctrica desde dos circuitos distintos.

El estado abierto o cerrado de las puertas y ventanas se obtiene mediante la activación de un sensor magnético (Contacto Magnético), el cual fue instalado en el marco de las mismas.

La señal de los sensores magnéticos es procesada por un módulo Arduino Mega, el cual envía los datos a través de la red a la aplicación de control.

La instalación de los dispositivos de red (*Switch* de Acceso) y regulador de voltaje se realizó en un tablero metálico de 30x30x20 (cm) denominado Tablero de ET, mientras que los elementos del sistema de monitoreo, automatización y control se instalaron en un tablero metálico de 60x40x20 (cm) denominado Tablero de EM.

La conexión de red, la alimentación eléctrica (V_{DC}) de los biométricos y el manejo de la apertura remota de la puerta de las aulas 27, 28 se encuentran derivados de los tableros de ET y EM N° 4 ubicados en el aula 26, mientras que el equipo biométrico y el manejo de la apertura remota de la puerta del aula 29 se encuentran derivados de los tableros de ET y EM N° 3 ubicados en el aula 33.

En la Figura 3.1, se muestran e identifican cada una de las partes que conforman el sistema de monitoreo y control de acceso de las aulas 27, 28 y 29 de la ESFOT que se implementaron en el proyecto, así como la placa PCB con el circuito de conmutación que permite el manejo de la cerradura eléctrica.





Figura 3.1 Identificación de las partes del proyecto.

1. Terminal biométrico del aula 27.
2. Terminal biométrico del aula 28.
3. Terminal biométrico del aula 29.
4. Placa PCB de conmutación, tubería PVC y cableado de red.
5. Tablero N° 4.
6. Interior tablero N° 4.
7. Interior tablero N° 3.
8. Tablero N° 3.
9. Módulo *Shield Ethernet* y Arduino Mega.
10. Cerradura eléctrica.
11. Servidor local del sistema.
12. Sensores magnéticos de las puertas y ventanas.

3.1 Requerimientos del sistema de monitoreo y control de acceso.

Inspección técnica-visual del estado de las aulas

Se realizó una inspección técnica-visual del estado de la infraestructura de las aulas 27, 28 y 29 de la ESFOT-EPN, para lo cual se procedió a identificar la ubicación de cada una de las aulas, para después subir al tumbado de las mismas con el fin de reconocer el recorrido del cableado y en base a las condiciones a las cuales estaría expuesto el mismo, seleccionar la tubería adecuada para protegerlo.

En la Tabla 3.2 se muestra un listado con las condiciones que presenta el recorrido del cableado de red.

Tabla 3.2 Condiciones del recorrido del cableado de red.

Condiciones	Aula 27	Aula 28	Aula 29	Comentario
Ambiente seco.	SI	SI	SI	Tendido del cableado de red sobre el cielo falso del aula.
Ambiente húmedo.	NO	NO	NO	
En el interior de la infraestructura	SI	SI	SI	
Libre de golpes, presión y aplastamiento.	NO	NO	NO	

Después de reconocer el recorrido del cableado de red, se contabilizó el número de ventanas y puertas que tiene cada grupo de aulas, esto con la finalidad de seleccionar un modelo de Arduino que cuente con la cantidad de pines necesarios para el manejo del sistema de automatización y monitoreo de las aulas (lectura de sensores, apertura remota de la puerta y control del encendido y apagado de luminarias).

Para lo cual se realizó un recorrido por las aulas 27, 28 y 29, contabilizando el número de puertas y ventanas. En la Tabla 3.3 se presenta el número de puertas, ventanas y pines requeridos.

Tabla 3.3 Conteo de puertas y ventanas aulas 27, 28 y 29.

Descripción	Aula	Número de ventanas	Número de puertas	Número de pines requeridos:
Grupo de aulas N° 3	29	3	1	3 pines para sensores de ventanas. 1 pin para sensor de puerta. 1 pin para activación de cerradura eléctrica. 3 pines para el encendido, apagado y monitoreo del estado de las luces.
Grupo de aulas N° 4	27	2	1	2 pines para sensores de ventanas. 1 pin para sensor de puerta. 1 pin para activación de cerradura eléctrica. 3 pines para el encendido, apagado y monitoreo del estado de las luces.
Grupo de aulas N° 4	28	4	1	4 pines para sensores de ventanas. 1 pin para sensores de puertas. 1 pin para activación de cerradura eléctrica. 3 pines para el encendido y apagado de luces y monitoreo de su estado.

En el anexo B se presenta una tabla con información del número de puertas, ventanas y pines requeridos para el manejo del sistema de monitoreo y automatización del grupo de aulas N° 3 y N° 4.

Por último, se identificó la ubicación de los *racks* que permiten conectar la red del sistema implementado a la intranet de la ESFOT.

Se seleccionaron los *racks* más cercanos a cada grupo de aulas, esto debido a que al ser un sistema de red cableado según el estándar ANSIA/TIA 568-C.1 para garantizar la correcta transmisión y recepción entre dispositivos de red, un cableado de red horizontal no debe sobrepasar la distancia de 100 (m) (TIA STANDARD, 2009), (Camues, 2017).

Se determinó que el *rack* ubicado en el Laboratorio de Microprocesadores (aula 23), sería utilizado para conectar los dispositivos de red del grupo de aulas N°4 (aula 27 y 28) y el *rack* ubicado en el Laboratorio de Tecnología Industrial, sería utilizado para conectar los dispositivos de red del grupo de aulas N°3 (aula 29).

Mientras que el *rack* ubicado en la dirección, sería utilizado para conectar el servidor local del sistema.

En el anexo C1 se presenta el plano de la ESFOT con la posición de los *racks* utilizados para la conexión de los dispositivos de red del sistema a la intranet de la ESFOT y la vinculación del grupo de aulas N° 3 y N° 4 a cada *rack*.

Estructura de red, dispositivos y equipos del sistema.

Se implementó una topología física en estrella para la conexión de red de los biométricos IP de cada grupo de aulas, debido a que dicha topología permite conectar todos los terminales biométricos del sistema, mediante la utilización de un solo puerto del *switch* de distribución (*switch* de la ESFOT).

La selección del tipo de topología física a utilizar para la conexión del sistema a la red, se realizó tomando en consideración el uso únicamente de 2 puertos de los *switch* de la ESFOT por cada grupo de aulas.

Siendo un puerto designado para la conexión del módulo *Shield Ethernet* del Arduino Mega y el otro para la conexión de los terminales biométricos.

En la Figura 3.2 se muestra el diagrama de la topología en estrella implementada para la comunicación de red de los terminales biométricos de las aulas 27, 28, 29, además de la conexión de los módulos *Shield Ethernet* del Arduino Mega (grupo de aulas N° 3 y N° 4.) y servidor local a los equipos de red asignados.

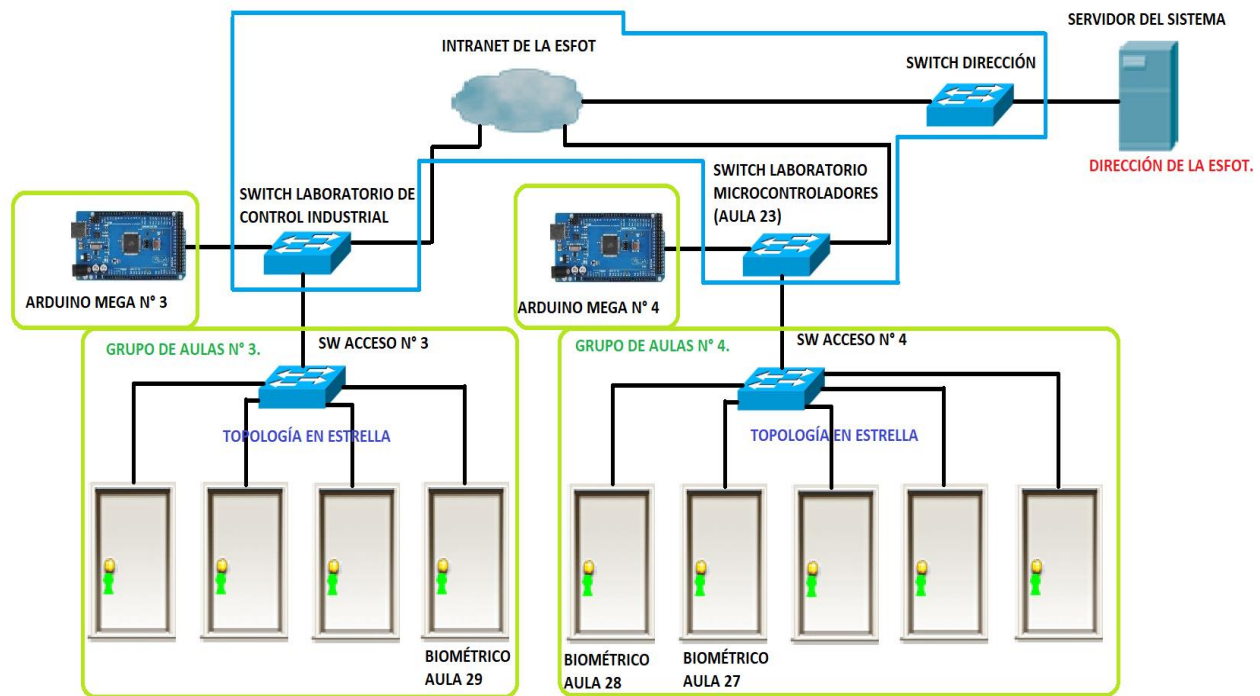


Figura 3.2 Diagrama de la topología física en estrella implementada.

En el anexo D se presenta la topología de red de todo el sistema.

Definida la topología de red para el sistema de control de acceso biométrico, se definieron y seleccionaron los equipos y componentes de la red.

Equipos finales:

Equipo biométrico de control de acceso.

Como *host* local, se definió un equipo biométrico de control de acceso, que cumpla con los siguientes requerimientos planteados en el proyecto:

- Soporte una comunicación de red *Ethernet*.
- Tenga una capacidad de almacenamiento de huellas dactilares superior al número de docentes que laboran en la institución.
- Sea capaz de creación de niveles de acceso según la carga académica de un semestre de la ESFOT.
- Maneje una cerradura eléctrica como interfaz de control de acceso.
- Soporte una administración mediante un *software* de usuario.

Se buscó en el mercado encontrando y seleccionando un biométrico de marca ZK-Teco, modelo SF300, con las características que se muestra en la Tabla 1.3, debido a que cumple con las características que se requieren para el sistema de control de acceso.

En la Figura 3.3 se muestra el biométrico seleccionado para la implementación de la estructura de red del sistema de control de acceso en las aulas 27, 28 y 29 de la ESFOT.



Figura 3.3 Terminal biométrico modelo SF300 Marca ZK-Teco.

Módulo Arduino y *Shield Ethernet*.

Para el control del sistema de monitoreo y automatización se requiere aproximadamente 22 pines digitales para la lectura de la señal emitida por los sensores colocados en ventanas y puertas, 5 pines digitales para el manejo de la apertura remota de las puertas y varios pines más para el manejo del encendido y apagado de las luces (Ver anexo B).

Debido a la gran cantidad de pines que se requiere para el sistema, se seleccionó el módulo Arduino Mega 2560, el cual presenta una cantidad de 54 pines digitales y 16 analógicos, abasteciendo el número requerido para el control del sistema. En el Anexo A1 se presenta las características técnicas del Arduino Mega 2560 utilizado en el proyecto.

En la Figura 3.4 se muestra el módulo Arduino Mega 2560 utilizado en el sistema de monitoreo y control.

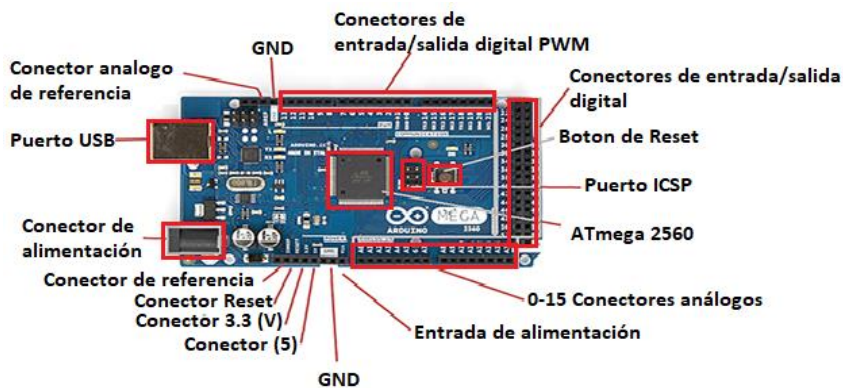


Figura 3.4 Arduino Mega 2560.
Fuente: (ARDUINO.CL, s.f.).

Para la comunicación del Arduino Mega 2560 a una red *Ethernet* usando un cable UTP categoría 5e, se seleccionó y empleo el módulo *Shield Ethernet W5100* debido a la compatibilidad y gran facilidad que presenta su acoplamiento (Llamas, 2017).

La función que ejecuta el módulo *Shield Ethernet*, es la de enviar y recibir información dentro de la intranet de la ESFOT de la lectura de los sensores de las puertas y ventanas para determinar si están abiertas o cerradas, así como también la lectura de encendido o apagado de las luces de las aulas.

En la Figura 3.5 se muestra el módulo *Shield Ethernet* acoplado al Arduino Mega 2560.



Figura 3.5 Módulo *Shield Ethernet* acoplado al Arduino Mega 2560.

Medio de transmisión

Cable UTP Cat. 5e

Como medio de transmisión, se dimensionó un cable de par trenzado que permita una velocidad de transmisión de hasta 100 (Mbps) con una frecuencia de 100 (MHz), con la finalidad de aprovechar la velocidad de transmisión que otorga cada dispositivo.

Se buscó en el mercado encontrando y seleccionando un cable de par trenzado marca CONNECTION de tipo cable UTP categoría 5e, con las características que se muestra en Tabla 1.1, el cual cumple con las características requeridas para la comunicación del sistema.

Switch de acceso.

Switch 8 o 5 puertos.

Como *switch* de acceso, se dimensionó un *switch* de 8 puertos *Fast Ethernet* 10/100 BaseTX, no administrable.

Se buscó en el mercado encontrando y seleccionando un *switch* marca D-LINK modelo DES 1008C, con las características que se muestra en la Tabla 1.2, el cual cumple con las características técnicas requeridas para la comunicación del sistema.

En la Figura 3.6 se muestra el *switch* de 8 puertos marca D-LINK modelo DES 1008C seleccionado.



Figura 3.6 *Switch* marca D-LINK modelo DES 1008C.

Direccionamiento IP de la red y habilitación de puertos *switch* DGIP.

Se gestionó con la Dirección de Gestión de la Información y Procesos (DGIP) la configuración de una VLAN para el sistema, para lo cual se tomó en consideración el número de direcciones IP que se necesitaría para la configuración de red del sistema.

En la Tabla 3.4 se muestra el número de direcciones IP que se solicitó a la DGIP para la configuración de red del sistema.

Tabla 3.4 Número de direcciones IP solicitadas a la DGIP.

Descripción	Número de direcciones IP
Número de direcciones IP para terminales biométricos.	19
Número de direcciones IP para <i>Shield Ethernet</i> Arduino Mega.	5
Número de direcciones IP para servidor local del sistema.	2
Número de direcciones IP para aplicación de monitoreo del sistema (ASI).	4
Total de direcciones IP requeridas para el sistema.	30

En la Tabla 3.5, se muestra las características de la VLAN configurada para el sistema.

Tabla 3.5 Características configuración de VLAN para el sistema por parte de la DGIP.

Descripción	Características VLAN
Número de direcciones IP de la VLAN configurada.	64
Dirección IP de la red (VLAN).	172.31.xxx.xxx
Máscara	255.255.xxx.xxx
Puerta de enlace	172.31.xxx.xxx
DNS 1	172.31.xxx.xxx
DNS 2	172.31.xxx.xxx
Rango de direcciones IPs:	172.31.xxx.xxx hasta 172.31.xxx.xxx

Con el rango de direcciones IPs de la VLAN configurada, se asignaron las direcciones IPs a los terminales biométricos de las aulas 27, 28, 29 al servidor local del sistema y a los *Shield Ethernet* del Arduino Mega del grupo de aulas N° 3 y N° 4.

En base a la ubicación de los respectivos *racks* de la DGIP identificados en el Anexo C se gestionó la habilitación de 2 puertos en cada *switch*. En la Tabla 3.6 se muestra el número del puerto habilitado en cada *switch*.

Tabla 3.6 Habilidad de puertos en los *switches* de la intranet de la ESFOT.

Descripción	N° del puerto habilitado en el <i>switch</i> .
<i>Switch</i> del <i>rack</i> ubicado en el Laboratorio de Control Industrial.	N° 13 N° 14
<i>Switch</i> del <i>rack</i> ubicado en el Laboratorio de Microprocesadores (Aula 23).	N° 21 N° 22
<i>Switch</i> del <i>rack</i> ubicado en la dirección de la ESFOT.	N° 28 N° 33

En la Figura 3.7 se presenta la asignación de puertos gestionados para la conexión de los *switches* de acceso del sistema y la conexión de equipos finales con sus respectivas direcciones IP. Por motivos de seguridad las direcciones IP del sistema no se muestran en el presente documento.

El direccionamiento IP de la VLAN se encuentra administrado por personal de la DGIP.

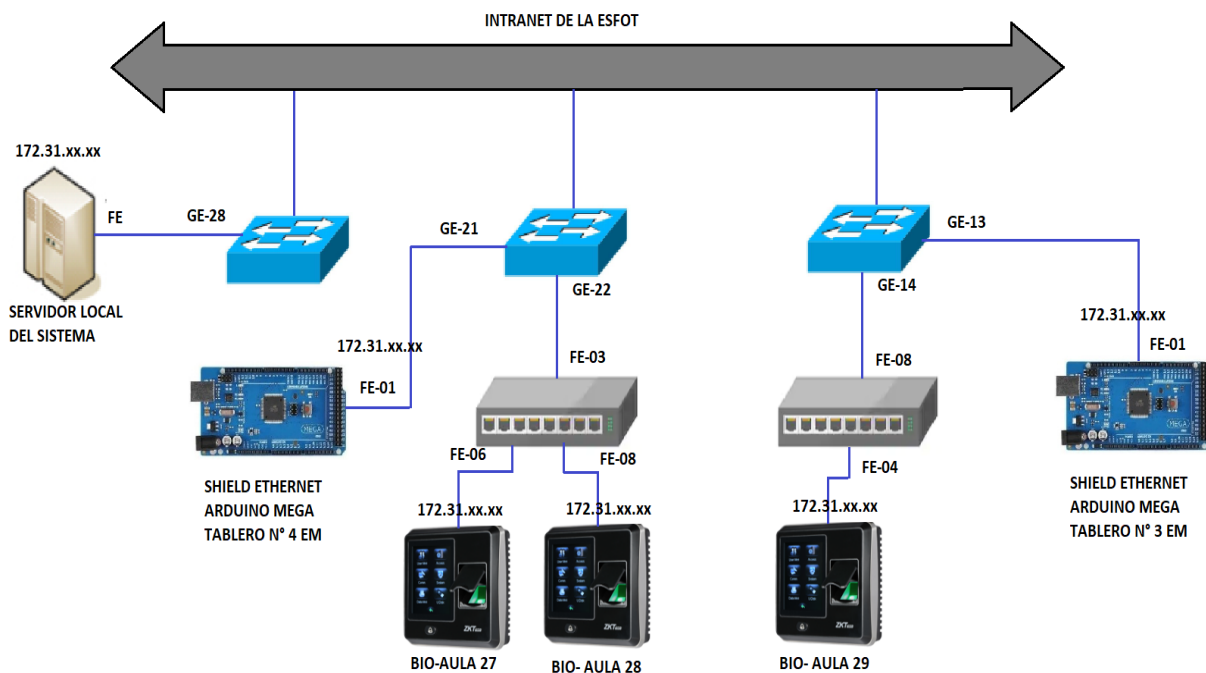


Figura 3.7 Diagrama de la topología lógica.

Establecimiento de las ubicaciones de los tableros.

Definidos y asociados los *racks* de datos de la DGIP a ser utilizados por cada grupo de aulas que contienen a las aulas 27, 28, 29 para la conexión de los dispositivos de red del sistema a la intranet de la ESFOT, se definió la ubicación de los tableros de ET y de EM del grupo de aulas N° 3 y N° 4, los cuales contienen los dispositivos de conectividad de la red del sistema.

Para lo cual se tomó en consideración una ubicación céntrica tanto para la conexión de los tableros de cada grupo de aulas hacia los *switches* de la DGIP, como para la conexión de los terminales biométricos hacia los tableros.

En la Figura 3.8 se muestra el plano con la distribución de tableros de ET y EM del grupo de aulas N° 3 y N° 4, las cuales contienen a las aulas 27, 28 y 29 de la ESFOT.

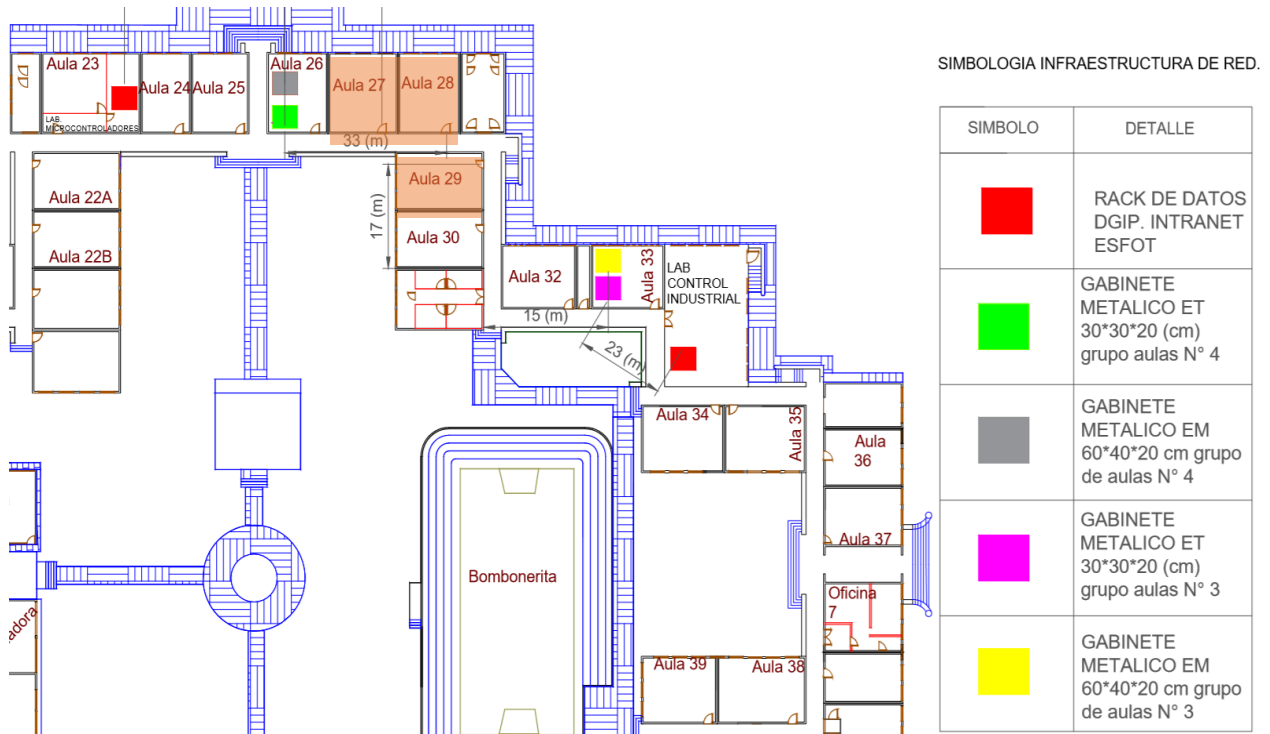


Figura 3.8 Ubicación de los tableros de ET y EM del grupo de aulas N° 3 y N° 4.

3.2 Instalación del cableado y equipos de la red.

En la Figura 3.9 se muestra el sistema de cableado estructurado junto con los dispositivos de red implementado en las instalaciones de las aulas 27, 28 y 29 de la ESFOT, el cual funciona desde septiembre del 2019 para la comunicación en red de los dispositivos biométricos a través de la intranet de la ESFOT.

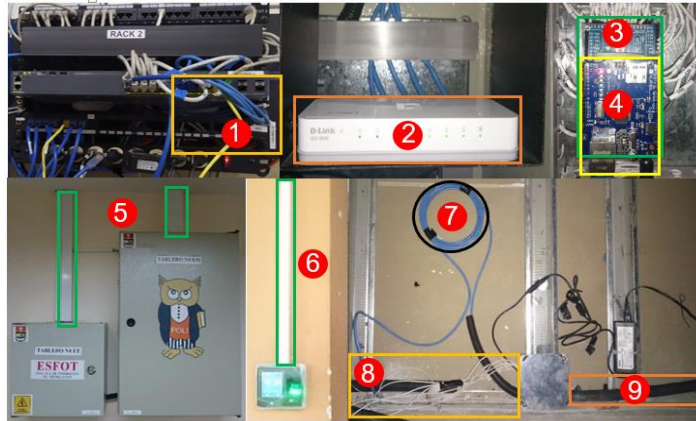


Figura 3.9 Elementos principales del cableado estructurado y equipos de red.

1. Terminación de cables de red en el *rack*.
2. *Switch* no administrable de 8 puertos.
3. Módulo Arduino Mega.
4. Módulo Arduino *Shield Ethernet*.
5. Canaletas bajantes hacia los tableros metálicos ET y EM.
6. Canaleta bajante hacia el terminal biométrico.
7. Cable UTP categoría 5e.
8. Cable eléctrico 20 AWG.
9. Tubería PVC corrugada.

Elaboración de los planos de la tubería, cableado para la red de datos y sensores.

Para la elaboración de los planos de la tubería y del cableado de red, así como de los sensores magnéticos se utilizó el *software* AutoCAD, los cuales fueron diseñados a partir del plano base de las instalaciones de la ESFOT en donde constan *racks*, gabinetes metálicos, equipos de conectividad de red y dispositivos magnéticos luego de haberse definido el lugar de ubicación de los mismos.

En el anexo C2 se muestran los planos de la tubería y cableado de red, tubería y cableado de los sensores magnéticos implementados para el sistema de control y acceso correspondiente a las aulas 27, 28 y 29, además de la simbología empleada para el diseño de los mismos.

Para el diseño del plano de la tubería y del cableado de datos del sistema, se tomó en consideración el recorrido del cableado que conecta a:

- Los terminales biométricos con el *switch* de acceso de la intranet de la ESFOT.
- El Módulo Arduino *Shield Ethernet* de cada tablero de control con el *rack* de la DGIP.

Para la terminación de la tubería instalada se colocó una caja de paso metálica de 4 ("), donde se concentra el cable de datos y cable de sensores correspondiente a cada aula.

En la Tabla 3.7 se presenta el recorrido del cableado de red del sistema.

Tabla 3.7 Recorrido del cableado de red del sistema para las aulas 27, 28 y 29.

Salida del cable de red:	Llegada del cable de red	Comentario
<i>Switch</i> de acceso del tablero metálico de ET N° 3.	Ingreso al aula 29 (biométrico)	Para comunicación de datos del terminal biométrico.
<i>Shield Ethernet</i> Arduino Mega del tablero metálico EM N° 3 y <i>Switch</i> de acceso del tablero metálico de ET N° 3.	<i>Rack</i> DGIP Lab. Control Industrial.	Para la comunicación de datos de la <i>Shield Ethernet</i> Arduino Mega y del <i>switch</i> de acceso del terminal biométrico.
<i>Switch</i> de acceso del tablero metálico de ET N° 4.	Ingreso al aula 27 y 28 (biométricos)	Para comunicación de datos de los terminales biométricos.
<i>Shield Ethernet</i> Arduino Mega del tablero metálico EM N° 4 y <i>Switch</i> de acceso del tablero metálico de ET N° 4	<i>Rack</i> DGIP Lab. Microprocesadores (Aula 23).	Para la comunicación de datos de la <i>Shield Ethernet</i> Arduino Mega y del <i>switch</i> de acceso de los terminales biométricos.

De igual manera, para el diseño del plano de la tubería y del cableado de los sensores magnéticos, se tomó en consideración el recorrido del cableado eléctrico 20 AWG que conecta:

- El Módulo Arduino Mega de cada tablero de control con los sensores magnéticos de las ventanas y puerta en cada una de las aulas asignadas.

En la Tabla 3.8 se presenta el recorrido del cable eléctrico correspondiente a los sensores para las aulas 27, 28 y 29.

Tabla 3.8 Recorrido del cable eléctrico 20 AWG de los sensores para las aulas 27, 28 y 29.

Salida del cable	Llegada del cable	Aplicación
Módulo Arduino Mega del tablero metálico EM N° 3.	Sensores de las ventanas (3) del aula 29.	Conductor para sensado de las ventanas.
	Sensor de la puerta (1) del aula 29.	Conductor para sensado de la puerta.

	Caja de paso (1) de los sensores de las ventanas del aula 29.	Conductor de tierra común para los sensores de las ventanas y puerta.
Módulo Arduino Mega del tablero metálico EM N° 4.	Sensores de las ventanas (4) del aula 28.	Conductor para sensado de las ventanas.
	Sensor de la puerta (1) del aula 28.	Conductor para sensado de la puerta.
	Caja de paso (1) de los sensores de las ventanas del aula 28.	Conductor de tierra común para los sensores de las ventanas y puerta.
Módulo Arduino Mega del tablero metálico EM N° 4.	Sensores de las ventanas (2) del aula 27.	Conductor para sensado de las ventanas.
	Sensor de la puerta (1) del aula 27.	Conductor para sensado de la puerta.
	Caja de paso (1) de los sensores de las ventanas del aula 27.	Conductor de tierra común para los sensores de las ventanas y puerta.

Dimensionamiento de la cantidad de cable UTP, 20 AWG y demás materiales.

En base a los planos previamente elaborados, se dimensionó en campo la cantidad de cable UTP categoría 5e para cubrir las distancias entre:

- El punto de red biométrico y el *switch* de acceso (En el gabinete de telecomunicaciones).
- El *switch* de acceso y el *switch* de distribución (En el *rack* de la DGIP).
- El Arduino *Shield Ethernet* y el *switch* de distribución.

En la Figura 3.10 y Figura 3.11 se presentan las distancias obtenidas de la medición:

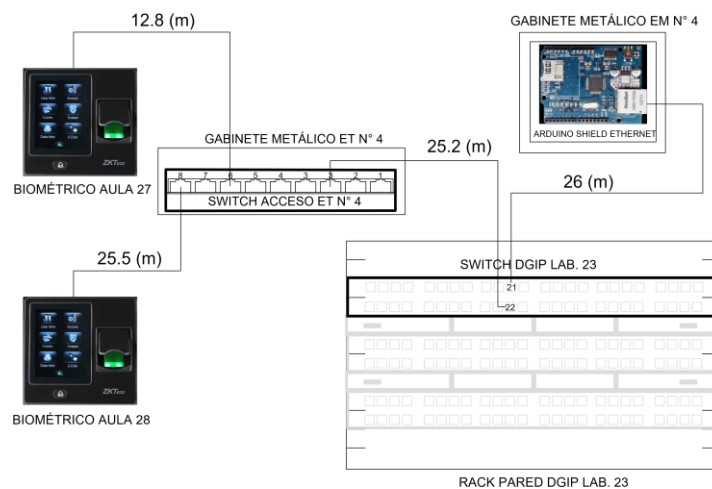


Figura 3.10 Dimensionamiento de cable UTP para las aulas 27 y 28.

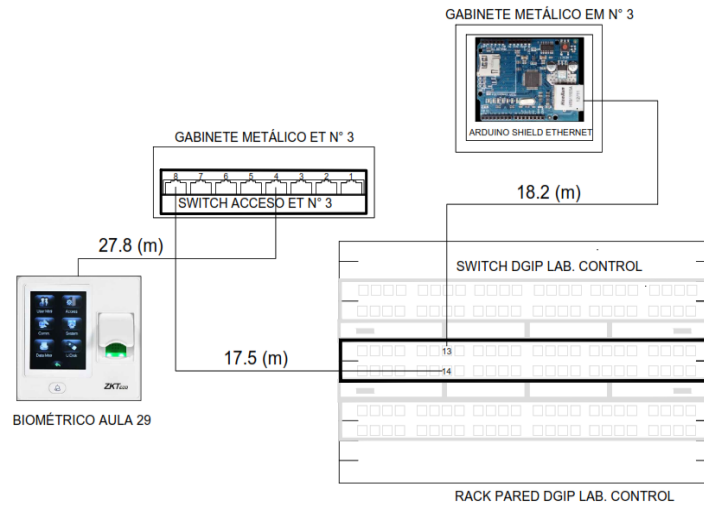


Figura 3.11 Dimensionamiento de cable UTP para el aula 29.

Mediante el cálculo de la longitud promedio de cable UTP, se determinó la cantidad de bobinas de cable UTP necesarias para las aulas del proyecto. A continuación, se muestra el desarrollo del cálculo realizado (Padilla & Silva, 2017).

$$LM = \frac{L_{\text{mín}} + L_{\text{máx}}}{2} \quad \text{Ec.1}$$

$$LT = LM + 10\%(LM) + HT \quad \text{Ec.2}$$

Donde:

- LM: Longitud Media.
- Lmáx: Longitud máxima.
- Lmín: Longitud mínima.
- LT: Longitud Total.
- HT: Holgura de Terminación (0.5 (m) en el área de trabajo y 2 (m) en el rack).

En la Figura 3.10 y Figura 3.11 se observa que $L_{\text{mín}} = 12.8$ (m) y $L_{\text{máx}} = 27.8$ (m), reemplazando estos valores en la Ecuación 1 se obtiene que:

$$LM = 20.3 \text{ (m)} \quad \text{Ec.3}$$

Reemplazando la Ecuación 3 en la Ecuación 2:

$$LT = 24.83 \text{ (m)} \quad \text{Ec.4}$$

La Ecuación 4 se multiplica por el número de puntos de red a instalarse (7 puntos de red):

$$LT = 24.83 \text{ (m)} * 7 = 173.81 \text{ (m)} \quad \text{Ec.5}$$

Para determinar el número de bobinas que se requiere para el cableado de red en las aulas asignadas, se aplica la siguiente ecuación:

$$\# \text{ Bobinas} = \frac{LT}{305 \text{ (m)}} \quad \text{Ec.6}$$

Reemplazando la Ecuación 5 en la Ecuación 6:

$$\# \text{ Bobinas} = \frac{173.81 \text{ (m)}}{305 \text{ (m)}} = 0.57 \quad \text{Ec.7}$$

Por lo tanto, en base a los cálculos realizados, la cantidad de cable UTP categoría 5e que se necesitó para el cableado de red fue aproximadamente de 174 (m) lo que representa el 57% de una bobina.

La longitud de cable eléctrico calibre 20 AWG utilizado para cablear los sensores de las ventanas y puertas en las aulas del proyecto se muestra en la Tabla 3.9.

Tabla 3.9 Dimensionamiento de cable eléctrico 20 AWG para los sensores de las ventanas y puertas.

Aula	Longitud de cable para sensores de las ventanas (m)				Longitud de cable para sensores de las puertas (m)		
	Sensores de las ventanas	Común de los sensores	Bajantes al tablero de control	Bajantes a los sensores	Desde el tablero de control	Bajantes al tablero de control	Bajantes al sensor
27	34.8 (m)	23.8 (m)	3 (m)	7.5 (m)	12.8 (m)	1 (m)	2 (m)
28	69.5 (m)	36.5 (m)	5 (m)	12.5 (m)	25.5 (m)	1 (m)	2 (m)
29	60.8 (m)	38.8 (m)	4 (m)	10 (m)	27.8 (m)	1 (m)	2 (m)
Longitud total de cable eléctrico 20 AWG:							382 (m)

Los principales materiales de cableado estructurado y eléctrico que se instalaron en el cableado horizontal correspondiente a las aulas 27, 28 y 29 se indican en la Tabla 3.10.

Tabla 3.10 Materiales empleados en el cableado horizontal.

Material	Dimensiones	Aplicación
Cable UTP categoría 5e 100% cobre.	Ø 6 (mm)	Transmisión de señales de voz o datos.
Canaleta PVC de pared adhesiva.	7x13x2000 (mm)	Canalización de cable UTP que sale desde el tablero EM.

Canaleta PVC sin división.	25x40x2000 (mm)	Canalización de cable UTP que sale desde el tablero EM y ET.
Conector RJ-45 cat. 5e.	Estándar	Conexión a equipos de red.
Capuchones para conectores RJ-45.	Estándar	Protección de conectores RJ-45.
Caja metálica cuadrada de 4 (").	40x60x2000 (mm)	Medio de derivación.
Manguera corrugada PVC.	Ø ¾ (")	Soporte y protección del cable UTP.
Cable de cobre multifilar 20 AWG.	Ø 0.813 (mm)	Conduce electricidad hacia los sensores.
Sensores magnéticos.	23x14 (mm)	Indican el estado en que se encuentran las ventanas y puertas.

Armado de la tubería y tendido del cableado de red y sensores.

Para el sistema de canalización, se utilizó una manguera corrugada PVC, la cual se extiende por todo el recorrido del cableado horizontal, desde los tableros metálicos hacia la caja de paso de cada aula y hacia los *racks* de la ESFOT.

La tubería que se deriva hacia la caja de paso de cada aula, contiene un cable de datos para la conexión del biométrico y cables eléctricos calibre 20 AWG correspondientes a los sensores de puertas, ventanas y cerradura eléctrica.

Mientras que la tubería que se deriva hacia los *racks* de la ESFOT, contiene 2 cables de datos para la conexión del Arduino Mega y *switch* de acceso del sistema biométrico.

En la Figura 3.12 se muestra la tubería instalada, materiales, tendido del cableado de red y cable eléctrico 20 (AWG).

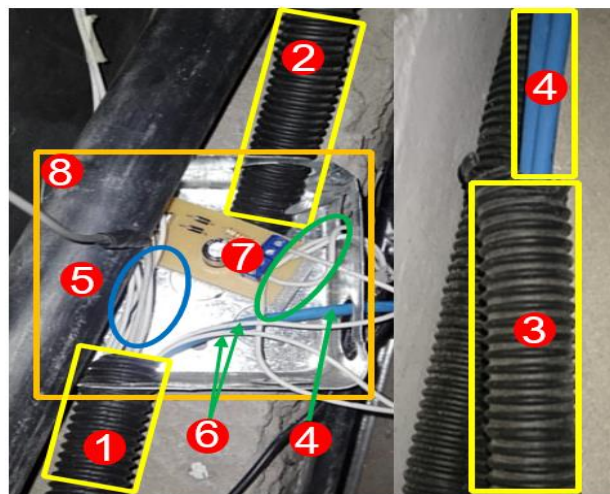


Figura 3.12 Cableado horizontal con manguera anillada PVC.

1. Tubería PVC de ¾ (") para cables de sensores de ventanas, puerta y cable UTP.
2. Tubería PVC de ¾ (") para cables de sensores de ventanas.
3. Tubería PVC de ¾ (") para cables de red.
4. Cable UTP categoría 5e.
5. Cables eléctricos 20 AWG de los sensores de las ventanas.
6. Cables eléctricos 20 AWG del sensor de la puerta.
7. Cables eléctricos 20 AWG para la cerradura eléctrica y alimentación del biométrico.
8. Caja de paso metálica de 4 (").

Selección e instalación de la tubería y del cableado del sistema.

Para la selección de la tubería se tomó en cuenta las condiciones descritas en la Tabla 3.2 a las cuales estaría expuesto el cableado de red del sistema y un margen de llenado de hasta el 40% de la tubería (Joscowicz, 2013). Para optimizar la cantidad de tubería en la implementación del cableado de red del proyecto, se optó por utilizar la misma tubería para el recorrido del cableado de los sensores, debido a que el cable eléctrico de calibre 20 AWG presenta una baja tensión en corriente continua por lo cual no representa un problema de interferencia con los cables de red (TECNOSEGURO, 2016).

A continuación, se presenta el desarrollo del cálculo de llenado de la tubería, tomando en cuenta el diámetro del cable UTP (6 (mm)) (CONNECTION, 2018) y el diámetro del cable eléctrico 20 AWG (0.813 (mm)) (CONDUCTORES RG, 2016). A continuación, se presenta el desarrollo del cálculo de llenado de la tubería.

Se calcula el área de cada conductor a ingresar a la tubería mediante la Ec. 8:

$$A_{\text{Cable } X} = \pi * \left(\frac{\varnothing_{\text{Cable } X}(\text{mm})}{2} \right)^2 = (\text{mm}^2) \quad \text{Ec. 8}$$

$$A_T = \#_{\text{Cable } X} * A_{\text{Cable } X} (\text{mm}^2) + \#_{\text{Cable } X} * A_{\text{Cable } X} (\text{mm}^2) = \text{Área total} (\text{mm}^2) \quad \text{Ec. 9}$$

Donde:

$\varnothing_{\text{Cable } X}$ = Diámetro del cable en (mm)

π = 3.1416

$A_{\text{Cable } X}$ = Área del cable en (mm²)

A_T = Área total de los conductores

$\#_{\text{Cable } X}$ = Número de cables que ingresan a la tubería.

Se calcula el área de cada conductor:

$\varnothing_{\text{UTP}} = 6$ (mm)

$\varnothing_{20\text{AWG}} = 0.813$ (mm)

A_{UTP} = Área del cable UTP cat. 5e

A_{20AWG} = Área del cable eléctrico

A_T = Área total de los conductores

de cables UTP que ingresan en la tubería: 1

promedio de cables eléctricos 20AWG UTP que ingresan en la tubería: 7

$$A_{UTP} = \pi * \left(\frac{6(\text{mm})}{2}\right)^2 = 28.27 \text{ (mm}^2\text{)} \quad \text{Ec.10}$$

$$A_{20AWG} = \pi * \left(\frac{0.813(\text{mm})}{2}\right)^2 = 0.52 \text{ (mm}^2\text{)} \quad \text{Ec.11}$$

Se calculó el área total de conductores:

$$A_T = 1 * 28.27 \text{ (mm}^2\text{)} + 7 * 0.52 = 31.91 \text{ (mm}^2\text{)} \quad \text{Ec.12}$$

Con el A_T calculado, se definió el tipo de tubería a utilizar, la misma que debe abarcar el A_T de los conductores a ingresar quedando cubierto como máximo el 40% de llenado y que además tenga las características necesarias para proteger al cableado de las condiciones que se establecen en la Tabla 3.2.

Se buscó en el mercado encontrando un tipo de manguera corrugada PVC para protección del cableado y con el área necesaria para abarcar a todos los conductores, en la Tabla 3.11 se muestran las características que presenta la manguera corrugada PVC.

Tabla 3.11 Características de la manguera corrugada PVC.

Nombre del material	Características
Manguera corrugada PVC de ¾ ("	Manguera aislante de plástico, flexible, resistente a la curvación, y al aplastamiento. Área 285 (mm ²).

Fuente: (CONSTRUJEX, 2020).

Con el área de la manguera PVC de ¾ (" se calcula el área del llenado del 40%, su desarrollo se muestra en la ecuación 13.

$$A_{T \text{ de llenado}} = 0.4 A_{\text{de llenado}} * A_{T \text{ de la tubería}} \text{ (mm}^2\text{)} = 114 \text{ (mm}^2\text{)} \quad \text{Ec.13}$$

Donde:

$A_{T \text{ de llenado}}$ = Área total de llenado.

% $A_{\text{de llenado}}$ = Porcentaje del área de llenado.

$A_{T \text{ de la tubería}}$ = Área total de la tubería.

$$A_T = 0.4 * 285 \text{ (mm}^2\text{)} = 114 \text{ (mm}^2\text{)} \quad \text{Ec.14}$$

La manguera corrugada PVC fue seleccionada como tubería para el recorrido del cableado del sistema, debido a que cumple con las características de protección que se requiere para el

cableado y que el A_T (Ec.14) de la misma abastece al A_T (Ec.12) de los conductores a ingresar (40 % de llenado).

Definida la tubería a emplearse, se realizó el cableado horizontal como se describe a continuación.

Cableado y canalización horizontal.

Se identificó y se unió las longitudes del cable UTP y de los cables eléctricos 20 AWG para realizar el tendido de los mismos, como se muestra en la Figura 3.13.



Figura 3.13 Tendido del cable UTP cat. 5e y de los cables eléctricos 20AWG.

Los cables se insertaron dentro de la manguera corrugada PVC, la longitud de los cables se muestra en la Figura 3.10 y Figura 3.11 dejando una holgura aproximada de 2 (m) a los extremos de los cables para facilitar el envío y halado de los mismos por el interior de la tubería.

Se colocó 2 cajas metálicas de paso, una para la concentración del cable UTP y derivación del cableado de sensores y la otra para la concentración del cableado de sensores para las ventanas.

Las cajas metálicas de paso fueron instaladas, a la altura de la puerta donde se ubica el biométrico y a la altura de las ventanas de cada aula. En la Figura 3.14 se muestra la concentración en la caja metálica del cableado del sistema con su respectiva holgura.



Figura 3.14 Instalación de la tubería que incluye cable de red y eléctrico.

La Tabla 3.12 presenta el recorrido de la tubería PVC desplegada sobre el techo falso de las instalaciones de las aulas 27, 28 y 29.

Tabla 3.12 Recorrido de la tubería PVC sobre el techo falso de las aulas 27, 28 y 29.

Salida de la tubería PVC	Llegada de la tubería PVC	Cantidad y tipo de cable que contiene la tubería PVC
Desde el techo falso del tablero metálico ET N° 4.	A la caja de paso instalada sobre el techo falso del punto de red biométrico aula 27.	1 cable UTP cat. 5e, 6 cables de cobre multifilar 20 AWG.
Desde el techo falso del tablero metálico ET N° 4.	A la caja de paso instalada sobre el techo falso del punto de red biométrico aula 28.	1 cable UTP cat. 5e, 8 cables de cobre multifilar 20 AWG.
Desde el techo falso del tablero metálico ET N° 4.	Techo falso del <i>Rack</i> DGIP Lab. Microprocesadores (Aula 23).	2 cables UTP cat. 5e.
Desde el techo falso del tablero metálico ET N° 3.	A la caja de paso instalada sobre el techo falso del punto de red biométrico aula 29.	1 cable UTP cat. 5e, 7 cables de cobre multifilar 20 AWG.
Desde el techo falso del tablero metálico ET N° 3.	Techo falso del <i>Rack</i> DGIP Lab. Control Industrial.	2 cables UTP cat. 5e.
Desde la caja de paso instalada sobre el techo falso del punto de red biométrico aula 27.	A la caja de paso instalada sobre el techo falso de la primera ventana aula 27.	3 cables de cobre multifilar 20 AWG.
Desde la caja de paso instalada sobre el techo falso del punto de red biométrico aula 28.	A la caja de paso instalada sobre el techo falso de la primera ventana aula 28.	5 cables de cobre multifilar 20 AWG.
Desde la caja de paso instalada sobre el techo falso del punto de red biométrico aula 29.	A la caja de paso instalada sobre el techo falso de la primera ventana aula 29.	4 cables de cobre multifilar 20 AWG.

Canalización de bajantes.

Se instaló canaletas bajantes desde el techo falso a los correspondientes tableros metálicos de ET, canaletas bajantes del techo falso a los correspondientes puntos de red biométricos, canaletas bajantes con cables de conexión a la cerradura eléctrica, canaletas bajantes con cables para los sensores de puertas y ventanas, además de una longitud pequeña de canaleta horizontal entre el tablero metálico de ET y EM considerando únicamente a la parte del cableado de datos proveniente del *Shield Ethernet* Arduino Mega, como se muestra en la Figura 3.15.



Figura 3.15 Canaletas bajantes desde el techo falso a los dispositivos y tableros del sistema.

1. Canaleta bajante para cables de alimentación del regulador del tablero ET.
2. Canaleta bajante para cables de red.
3. Canaleta horizontal para el cable de red desde el tablero EM.
4. Canaleta bajante para cables de los sensores, luminarias y alimentación del tablero EM.
5. Canaleta para los cables de la cerradura eléctrica.
6. Canaleta para cables de los sensores de las ventanas
7. Canaleta bajante para el punto de red biométrico de las aulas.
8. Canaleta bajante para el sensor de la puerta.

En la Tabla 3.13 se detallan las canaletas bajantes que se utilizaron en el proyecto.

Tabla 3.13 Canaletas utilizadas en el proyecto.

Canaleta	Tipo de canaleta	Dimensiones	Longitud usada
Bajante desde el techo falso hacia la parte superior del tablero metálico ET N° 3 y N° 4.	Canaleta PVC sin división.	25x40x2000 (mm)	65 (cm)
Bajante desde el techo falso hacia la parte superior del tablero metálico ET N° 3 y N° 4.	Canaleta PVC sin división.	20x20x2000 (mm)	65 (cm)
Horizontal que une el tablero metálico EM y tablero metálico ET.	Canaleta PVC de pared adhesiva.	7x13x2000 (mm)	14 (cm)
Bajante desde el techo falso hacia la parte superior del tablero metálico EM N° 3 y N° 4.	Canaleta PVC sin división.	16x60x2000 (mm)	50 (cm)
Bajante desde el techo falso hacia el punto de red biométrico del aula 27, 28 y 29.	Canaleta PVC de pared adhesiva.	20x20x2000 (mm)	200 (cm)
Bajante desde el techo falso y canaleta horizontal hacia la cerradura eléctrica del aula 27, 28 y 29.	Canaleta PVC de pared adhesiva.	7x13x2000 (mm)	3 (m)
Bajante desde el techo falso hacia el sensor magnético de la puerta del aula 27, 28 y 29.	Canaleta PVC de pared adhesiva.	7x13x2000 (mm)	80 (cm)
Bajante desde el techo falso a la parte superior de la ventana y canaleta horizontal hacia los sensores magnéticos de las ventanas de las aulas 27, 28 y 29.	Canaleta PVC de pared adhesiva.	7x13x2000 (mm)	2 (m)

Reconocimiento, ponchado y etiquetado del cableado de red.

El ponchado de los cables UTP se realizó en base a la norma T568B considerando que se conectan dispositivos de diferente tipo, por lo que para su conexión se utilizan cables directos.

La norma TIA/EIA-568 establece que se debe usar un cable directo de red cuando se conecta un *host* a un *switch* o a un enrutador en donde los 8 pines de cada extremo del cable coinciden. Por lo que se seleccionó el tipo de ponchado T568B debido a que es la norma más reconocido para ponchar un cable de red a los dos extremos en redes LAN a velocidades de 100 (Mbps) y que conecten a dos dispositivos de diferente tipo. (WIKIPEDIA, 2019).

En el anexo A4 se presenta el código de colores y características de los pines en base a la norma T568B utilizada para el ponchado de los cables de red del sistema.

El etiquetado para los cables de red está basado en la nomenclatura que utiliza la DGIP. En la Figura 3.16 se muestra el etiquetado y el ponchado de los cables de red del sistema.



Figura 3.16 Ponchado y etiquetado del cable de red del sistema.

- a) Probador de cables de red.
- b) Etiquetado del cable de red del sistema.
- c) Cables de red ponchados.

Ponchado del cableado de red según la norma T568-B

El cableado horizontal del sistema se realizó en base a la construcción de cables de red (terminación a los dos extremos del cable en conectores RJ-45), siguiendo la norma T568B el cual tiene un estándar de colores que se debe seguir para realizar un cable de red directo, ver anexo A4. Se utilizó únicamente cables de red directo, debido a que el *switch* de acceso seleccionado para la implementación de la red con topología en estrella tiene entre sus funciones la función MDI/MDIX (ver Tabla 3.6), la cual permite el uso de cables directos para la conexión entre dispositivos del mismo tipo, la misma que se utiliza entre la conexión que se realiza del *switch* de acceso red del sistema al *switch* de distribución intranet ESFOT-EPN.

El ponchado del cable UTP se realizó en los dos extremos de terminación del cable, construyendo un cable de conexión que conecta a los equipos de red del sistema.

A continuación, se indica el proceso realizado para el ponchado de los cables.

A) Por un extremo del cable UTP se insertó el capuchón, se quitó la cubierta a 2.5 (cm) del extremo. Se destrenzó los 4 pares de conductores.

B) Se ordenó los conductores según la norma definida anteriormente (T568B), desde el pin N°1 hasta el pin N°8. (Ver anexo A6).

C) Se ingresó los conductores al RJ45 y se verificó que estén en el mismo orden.

D) Se colocó el conector RJ45 dentro de la ponchadora para luego presionar hasta que los contactos del RJ-45 hagan contacto con los hilos del cable UTP.

E) Se cubrió el RJ45 con el capuchón previamente insertado.

F) Se volvió a realizar el mismo procedimiento en el otro extremo del cable de red.

En la Figura 3.17 se muestra el proceso del ponchado realizado.

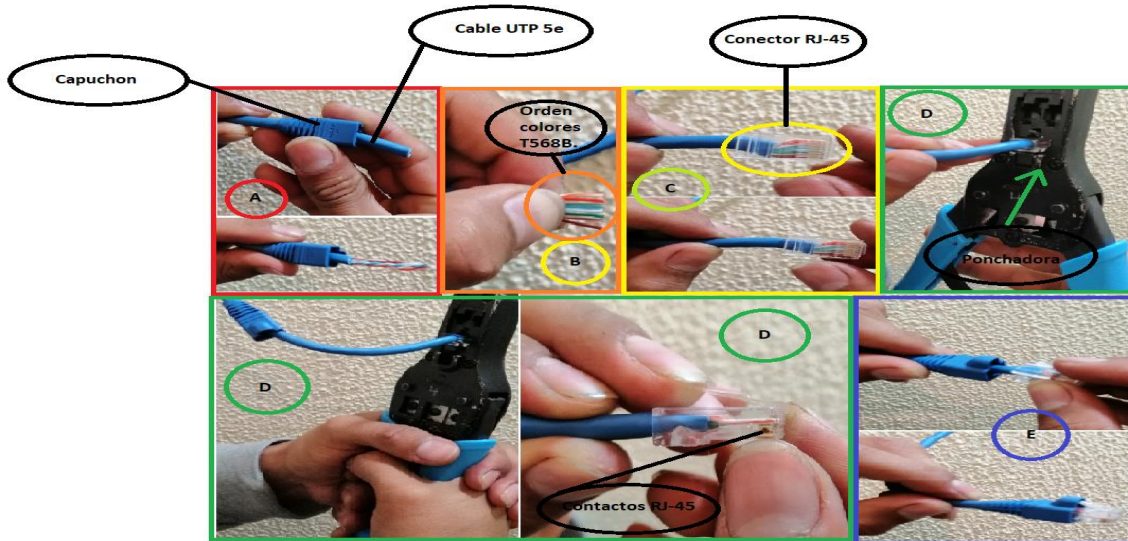


Figura 3.17 Ponchado de cable UTP cat 5e.

Etiquetado del cableado de red según la norma T568-B

El etiquetado realizado en el cableado de red presentado en la Figura 3.18, utiliza la misma forma de etiquetamiento de la DGIP “de dónde viene” a “a dónde va”, con el fin de mantener un mismo sistema de administración del etiquetado.

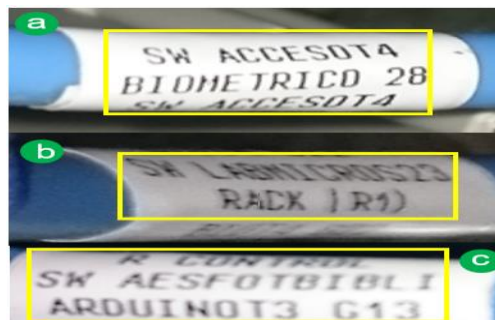


Figura 3.18 Etiquetado del cableado de red del sistema.

a) Etiquetado del cable UTP de los biométricos.

b) Etiquetado del cable UTP del switch de acceso al switch de la DGIP

c) Etiquetado del cable UTP del Arduino al switch de la DGIP.

La norma TIA/EIA-606-C “Especificación sobre el rotulado de los cables” señala que se deberá adicionar un identificador exclusivo para cada terminación de *hardware* y que se deberá rotular cada uno de los tendidos de cableado horizontal (Orellana, 2016).

Siguiendo la norma mencionada sobre el etiquetado en cada uno de los cables de red, y la nomenclatura establecida por la DGIP basado en la forma “de dónde viene” a “dónde va”, se optó por usar este tipo de etiquetamiento en el sistema de cableado de las aulas que intervienen en el proyecto, el cual tiene la siguiente nomenclatura como se observa en el ejemplo de la Figura 3.19.

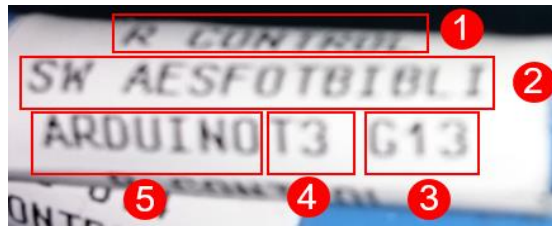


Figura 3.19 Modelo de etiquetado que establece la DGIP.

- 1) *Racks* de la DGIP.
- 2) *Switch* de la DGIP.
- 3) Número de puerto.
- 4) Número del Tablero metálico EM donde se encuentra el dispositivo de red.
- 5) Dispositivo de red.

En la Tabla 3.14 se muestra el etiquetado del cable UTP de los biométricos de las aulas 27, 28 y 29 de la ESFOT que se conectan al *switch* de acceso del sistema.

Tabla 3.14 Nomenclatura del etiquetado del cableado de los biométricos.

Aula	Etiqueta en el extremo del cable UTP de los biométricos.	“De dónde viene”	A “dónde va”	Descripción de la etiqueta
27	BIOMÉTRICO 27 SW ACCESOT4	BIOMÉTRICO 27	SW ACCESOT4	Viene del biométrico del aula 27, va al <i>switch</i> de acceso del tablero metálico ET N° 4.
28	BIOMÉTRICO 28 SW ACCESOT4	BIOMÉTRICO 28	SW ACCESOT4	Viene del biométrico del aula 28, va al <i>switch</i> de acceso del tablero metálico ET N° 4.
29	BIOMÉTRICO 29 SW ACCESOT3	BIOMÉTRICO 29	SW ACCESOT3	Viene del biométrico del aula 29, va al <i>switch</i> de acceso del tablero metálico ET N° 3.

En la Tabla 3.15 se muestra el etiquetado del cable UTP del *switch* de acceso de los biométricos al *switch* de la DGIP.

Tabla 3.15 Nomenclatura del etiquetado del cable UTP del *switch* de acceso al *switch* de la DGIP.

Tablero metálico ET N°	Etiqueta en el extremo del cable UTP del <i>switch</i> de acceso	“De dónde viene”	“A dónde va”	Descripción de la etiqueta
4	BIOT4 G22 SW AESFOT R LAB. 23	BIOT4	G22 SW AESFOT R LAB. 23	Viene del <i>switch</i> de acceso del tablero metálico ET N° 4, va al puerto <i>Gigabit Ethernet</i> 22 del <i>switch</i> AESFOT en el <i>rack</i> del laboratorio 23.
3	BIOT3 G14 SW AESFOT R CONTROL	BIOT3	G14 SW AESFOT R CONTROL	Viene del <i>switch</i> de acceso del tablero metálico ET N° 3, va al puerto <i>Gigabit Ethernet</i> 14 del <i>switch</i> AESFOT en el <i>rack</i> del laboratorio de control industrial.

En la Tabla 3.16 se muestra el etiquetado del cable UTP del *Shield Ethernet* Arduino Mega al *switch* de la DGIP correspondiente.

Tabla 3.16 Nomenclatura del etiquetado del cable UTP del Arduino al *switch* de la DGIP.

Tablero metálico EM N°	Etiqueta en el extremo del cable UTP del módulo Arduino	“De dónde viene”	A “dónde va”	Descripción de la etiqueta
4	ARDUINOT4 G21 SW AESFOT R LAB. 23	ARDUINOT4	G21 SW AESFOT R LAB. 23	Viene del Arduino del tablero metálico EM N° 4, va al puerto <i>Gigabit Ethernet</i> 21 del <i>switch</i> AESFOT en el <i>rack</i> del laboratorio 23.
3	ARDUINOT3 G13 SW AESFOT R CONTROL	ARDUINOT3	G13 SW AESFOT R CONTROL	Viene del Arduino del tablero metálico EM N° 3, va al puerto <i>Gigabit Ethernet</i> 13 del <i>switch</i> AESFOT en el <i>rack</i> del laboratorio de control industrial.

Montaje y conexión de equipos de red.

Los *switches* D-Link de 8 puertos que conectan a los terminales biométricos de las aulas 27,28 y 29, están montados sobre un soporte metálico dentro de un tablero metálico de 30x30x20 (cm) denominado Tablero de ET N° 3 y N° 4.

El módulo *Shield Ethernet* el cual permite la conexión de red del Arduino Mega 2560, se encuentra montado sobre la placa base de un tablero metálico de 60x40x20 (cm) denominado Tablero de EM N° 3 y N° 4.

En la Figura 3.20 se muestra la ubicación de los equipos de red utilizados en el sistema.

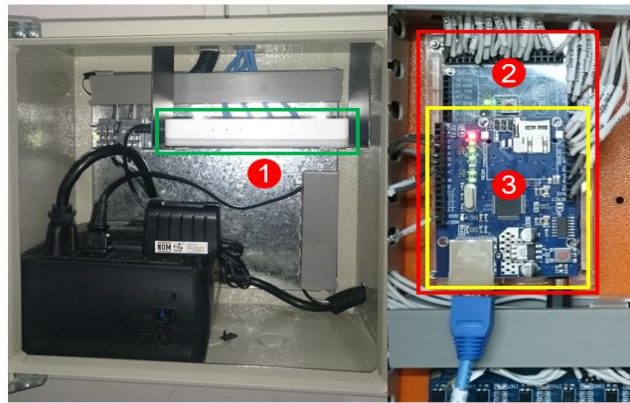


Figura 3.20 Switch 8 puertos D-Link, Módulo *Shield Ethernet* Arduino Mega.

1. *Switch* D-link de 8 puertos 10/100 (Mbps).
2. Módulo Arduino Mega 2560.
3. Módulo Arduino *Shield Ethernet* HanRun W5100.

Montado del módulo Arduino Mega 2560 y del *Shield Ethernet*

La ubicación del módulo *Shield Ethernet* acoplado al Arduino Mega, se definió dentro del tablero de EM, debido a que el Arduino Mega 2560 es el sistema central de control, el cual obtiene la información del estado de las ventanas, puertas y focos (etapa de sensado), controla el accionamiento de los elementos eléctricos como relés, módulos de relés, reguladores de voltaje para el encendido, apagado de las luces y la apertura de la puerta (etapa de potencia y control), además de las fuentes de alimentación (etapa de alimentación). La información sobre el estado de los sensores, la apertura de las puertas, el control de luminarias, se centraliza en el servidor local del sistema (etapa de presentación).

En la Figura 3.21 se presenta las etapas del sistema de monitoreo y control.

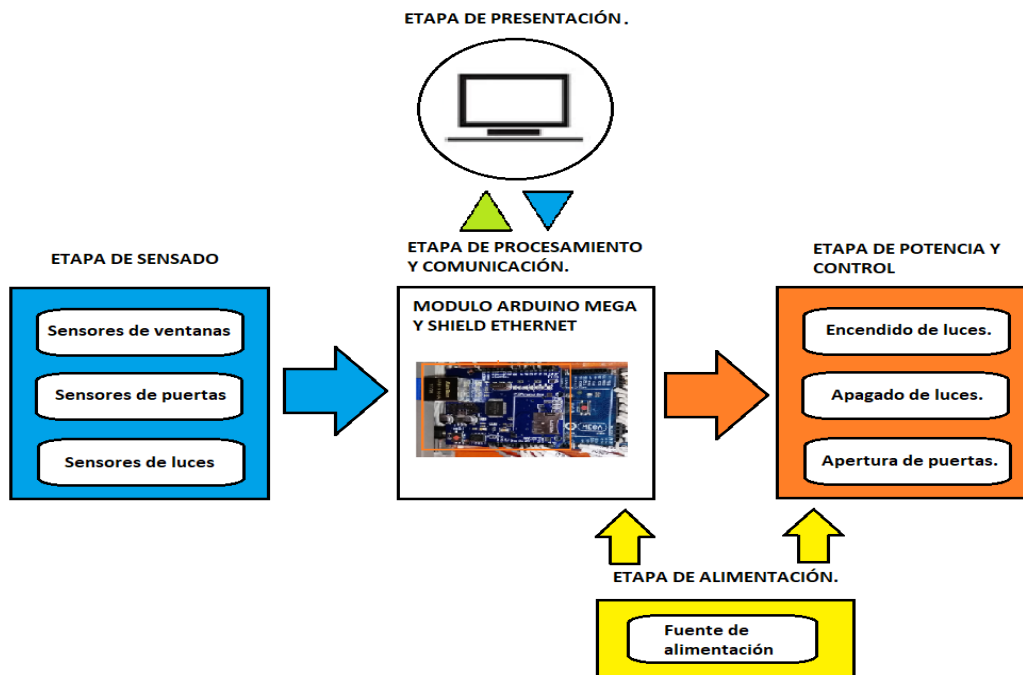


Figura 3.21 Etapas del sistema de monitoreo y control.

La ubicación del módulo *Shield Ethernet* acoplado al Arduino Mega 2560, se definió dentro del tablero EM, en un sitio centralizado para las borneras, módulos de relés de 4 y 8 canales, módulos reguladores de voltaje, cable de alimentación del Arduino Mega, fusibles, y el cable de conexión RJ-45. La Figura 3.22 muestra la ubicación de los módulos Arduino Mega 2560 y del *Shield Ethernet* dentro del tablero metálico EM.

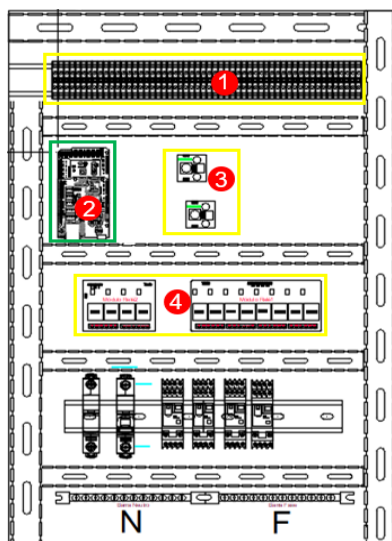


Figura 3.22 Ubicación de módulos Arduino y componentes electromecánicos.

1. Borneras repartidoras unipolares.
2. Módulo Arduino Mega 2560 y *Shield Ethernet*.
3. Módulos reguladores de voltaje.
4. Módulos de relés de 4 y 8 canales.

Conociendo la ubicación del módulo Mega 2560 en el tablero metálico de EM, se procedió a ajustar la carcasa de acrílico junto con el Arduino Mega, para después montar el módulo *Shield Ethernet* de modo que los pines comunicación del módulo coincidan con los respectivos pines del Arduino Mega.

En la Figura 3.23 se muestra el anclaje y montaje del módulo y Arduino dentro del tablero de EM.

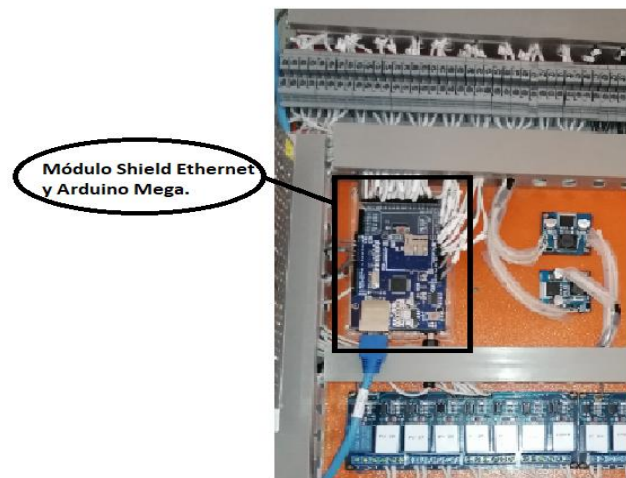


Figura 3.23 Montado del Módulo *Shield Ethernet* y Arduino Mega.

La conexión en red del módulo *Shield Ethernet* con un puerto del *switch* de la DGIP correspondiente al grupo de aulas N° 4, se realizó de forma directa mediante un cable de red *Ethernet*. De la misma manera se realizó la conexión de red del módulo *Shield Ethernet* correspondiente al grupo de aulas N° 3 con un puerto del *switch* de la DGIP, como se indica en la Figura 3.7.

Distribución y conexión de pines del módulo Arduino Mega 2560.

Los pines a los cuáles están conectados los sensores de las puertas, ventanas y luces en el módulo *Shield Ethernet* y Arduino Mega se describe en la siguiente Figura 3.24.

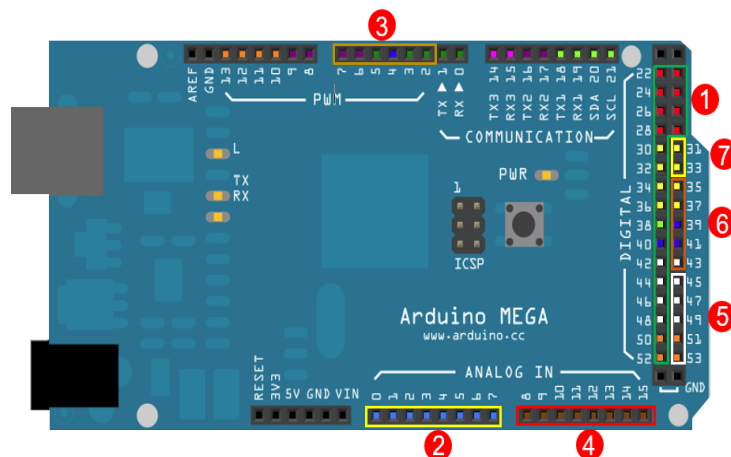


Figura 3.24 Distribución de pines del módulo Arduino Mega.

1. Pines para monitoreo de las ventanas (pines pares 22-52, pines impares 23-29).
2. Pines para monitoreo de las puertas (A0-A7).
3. Pines para monitoreo de las luces (2-7).
4. Pines para control de apertura de las puertas (A8-A15).
5. Pines para control de encendido de las luces (pines impares 45-53).
6. Pines para control de apagado de las luces (pines impares 35-43).
7. Pines de reserva para control de encendido y apagado de las luces (31,33).

En el anexo E se muestra los planos esquemáticos del sistema de automatización, entre el Arduino Mega y los elementos eléctricos de control y protección. (Conexiones para el control de apertura de las puertas, encendido y apagado de las luces, monitoreo del estado de las puertas, ventanas y luces).

En el anexo F se presenta una explicación del código cargado al Arduino Mega y su diagrama de flujo. La Tabla 3.17 describe la distribución de pines de los sensores de luces, ventanas y puertas correspondientes al aula 27 y 28, para el módulo Arduino Mega ubicado en el tablero EM N°4.

Tabla 3.17 Conexión de los pines del Arduino Mega hacia los elementos eléctricos y sensores.

Pines	Conexión de destino	Etiqueta	Comentario
2, 3	Relé de potencia 5 en el pin 12, Relé de potencia 4 en el pin 12 respectivamente.	IN(D2)/L27N1, IN(D3)/L28N1	Entradas de los sensores de las luces de las aulas 27 y 28.

(28, 30), (22, 24, 26, 44)	Borneras repartidoras unipolares (51, 52) y (55, 56, 57, 58).	IN(D28)/V27N1, IN(D30)/V27N2, IN(D22)/V28N1, IN(D24)/V28N2, IN(D26)/V28N3, IN(D44)/V28N4	Entradas de los sensores de las ventanas de las aulas 27 y 28.
41, 43	Módulo de relé 1 en el pin 7, Módulo de relé 2 en el pin 1 respectivamente.	OUT(D41), OUT(D43)	Salidas de relés para el apagado de las luces de las aulas 27 y 28.
31, 53	Módulo de relé 1 en el pin 8, Módulo de relé 2 en el pin 2 respectivamente.	OUT(31)LE27N1, OUT(53)LE28N1	Salidas de relés para el encendido de las luces de las aulas 27 y 28.
A1, A0	Borneras repartidoras unipolares 53 y 59.	IN(A1)/P27N1, IN(A0)/P28N1	Entradas de los sensores de las puertas de las aulas 27 y 28.
A11, A12	Módulo de relé 2 en el pin 6 y 7 respectivamente.	OUT(A11)/P27, OUT(A12)/P28	Salidas de relés de las puertas de las aulas 27 y 28.

La Tabla 3.18 describe la distribución de pines de los sensores de luces, ventanas y puertas correspondientes al aula 29, para el módulo Arduino Mega ubicado en el tablero EM N°3.

Tabla 3.18 Conexión de los pines del Arduino Mega hacia los elementos eléctricos y sensores.

Pin	Conexión de destino	Etiqueta	Comentario
5	Relé de potencia 1 pin 12.	IN(D5)/L29N1	Entrada de los sensores de las luces del aula 29.
44, 46, 48	Borneras repartidoras unipolares 34, 35, 36.	IN(D44)/V29N1, IN(D46)/V29N2, IN(D48)/V29N3	Entradas de los sensores de las ventanas para el aula 29.
37	Módulo de relé 1 en el pin 1.	OUT(D37)	Salida del relé para el apagado de las luces del aula 29.
47	Módulo de relé 1 en el pin 2.	OUT(47)/LE29N1	Salida del relé para el encendido de las luces del aula 29.
A3	Bornera repartidora unipolar 37.	IN(A3)/P29N1	Entrada del sensor de la puerta del aula 29.
A8	Módulo de relé 2 en el pin 1.	OUT(A8)/P29	Salida del relé de la puerta del aula 29.

Montaje del *switch* D-Link (10/100Mbps) de 8 puertos y demás equipos.

Para la protección y aislamiento de los elementos eléctricos de fuerza que contiene el tablero de EM N° 3 y N° 4, se definió la utilización de otro tablero metálico denominado Tablero de ET N° 3 y N° 4, el cual contendría el *switch* de acceso de los terminales biométricos de cada grupo de aulas, además de un regulador de voltaje, el cual entrega un voltaje regulado a todos los

dispositivos del sistema, protegiendo a los mismos de daños por picos de voltaje que se presentan en una línea eléctrica normal (línea eléctrica no regulada).

Tablero metálico.

Para seleccionar las dimensiones del tablero metálico de ET se tomó en cuenta el espacio de los elementos que contendría el mismo y una protección que ofrezca el tablero contra polvo o caída de agua, esto con la finalidad de garantizar el cuidado y funcionamiento adecuado de los equipos instalados en su interior.

Entre los elementos que se tomaron en cuenta para el dimensionamiento del tablero de ET, está el regulador de voltaje marca FORZA, un soporte metálico de dimensiones 15x10x8 (cm) en donde se asentará el *switch* de 8 puertos, los terminales de los cables de conexión RJ-45 que se conectan al *switch* de acceso, un riel DIN junto con las borneras en el que se conectan los cables de fase y neutro para energizar a los equipos biométricos.

En base a las medidas que presentan los equipos a instalarse en el tablero de ET y a la protección requerido para evitar daños en los mismos, se buscó en el mercado seleccionando un tablero con medidas de 30x30x20 (cm), con grado de protección IP 41 que se refiere a protección contra polvo y caída de agua, el cual cumple con los requerimientos deseados para la instalación del *switch* de acceso y regulador de voltaje del sistema.

En la Figura 3.25 se muestra el tablero metálico (tablero ET N° 3 y N° 4) seleccionado para la instalación de los equipos del sistema.



Figura 3.25 Tablero ET N° 3 y N° 4 con sus dimensiones.

Montado de equipos.

Para el montaje del *switch* de acceso de los terminales biométricos, se consideró como forma de protección y aislamiento de cualquier fuente eléctrica que pueda ocasionar interferencia a la transmisión de datos efectuado por el equipo, ubicarlo sobre un soporte metálico con dimensiones

15x10x8 (cm), el cual se encuentra sujeto en la cara superior del tablero de ET, manteniendo al *switch* de acceso sin contacto físico con ningún dispositivo eléctrico.

La sujeción del *switch* sobre el soporte metálico se realizó mediante la utilización de cinta adhesiva doble faz, con el fin de mantener sujeto al dispositivo sobre el soporte.

El regulador de voltaje se montó sobre la cara inferior del tablero, mientras que las borneras y canaletas para ordenar los cables se montaron en la tapa trasera (fondo del tablero) del tablero.

Con el montaje de los equipos dentro del tablero de ET, se ancló el tablero a 5 (cm) de separación del tablero de EM, para después conectar la fuente de alimentación del tablero de EM (Alimentación Arduino Mega), la fuente de alimentación del *switch* de acceso del sistema y la línea de alimentación de los terminales biométricos.

En la Figura 3.26 se muestra el tablero de ET con los equipos montados en su interior.

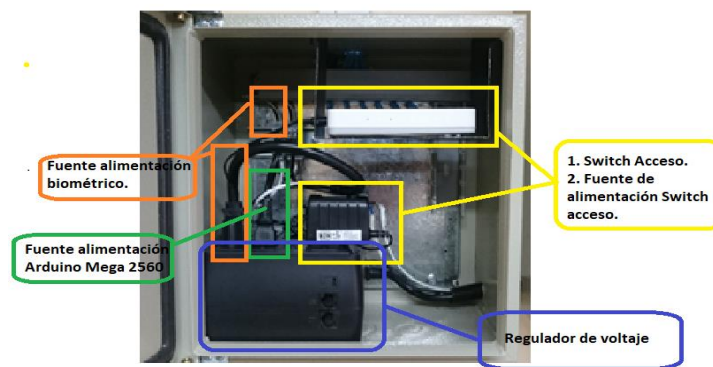


Figura 3.26 Tablero metálico de ET.

La conexión de los terminales biométricos de las aulas 27 y 28 se realizaron a través de cables de conexión directos al *switch* de acceso N°4, el cual gracias a la función MDI/MDIX que tiene todos sus puertos se conectó mediante un cable de conexión directo al *switch* de distribución de la intranet de la ESFOT. De igual manera se realizó con la conexión del terminal biométrico del aula 29, el cual se conectó al *switch* de acceso N° 3 y este a su vez a un *switch* de distribución de la intranet de la ESFOT.

En la Figura 3.7 se muestra el número del puerto y la ubicación del *rack* donde se encuentra el *switch* de la intranet de la ESFOT al cual se encuentran conectados los *switches* de acceso N° 3 y N° 4 del sistema. En la Figura 3.27 se muestra la conexión de los cables de conexión provenientes de los biométricos al *switch* de acceso N° 3 y N° 4.



Figura 3.27 Cables de conexión conectados a los switches de acceso N° 3 y N° 4.

3.3 Implementación del sistema biométrico y mecánico

Elaboración e instalación de una placa PCB para el manejo del sistema mecánico.

Se consideró que la activación de la cerradura eléctrica para la apertura de la puerta, se realice tanto de forma remota desde la aplicación instalada en el servidor local del sistema de control de acceso, como desde el terminal biométrico que se encuentra instalado al ingreso de las aulas.

Para solventar dicho requerimiento se realizó una PCB (*Printed Circuit Board*), con un circuito de conmutación, el cual permite manejar la activación de la cerradura eléctrica desde el terminal biométrico como desde el Arduino Mega.

En la Figura 3.28 se presenta la placa del circuito electrónico utilizado en el proyecto para la activación de la cerradura eléctrica desde el terminal biométrico y el Arduino Mega.

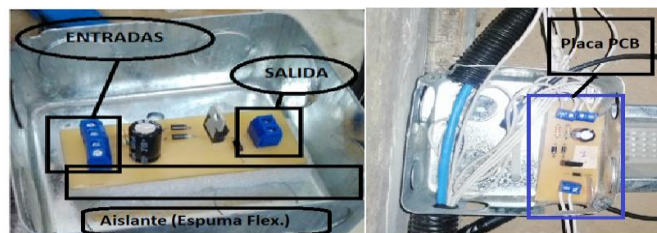


Figura 3.28 Placa PCB – Circuito de conmutación.

La función de la placa es la de permitir energizar la cerradura eléctrica mediante la habilitación de un único circuito al momento de activar el *relay* de salida ya sea del biométrico o del módulo de *relay* del Arduino.

Ademas, brinda protección al equipo biométrico contra corrientes inversas y a la chapa eléctrica contra excesos de corriente producto de una duración del pulso de activación de la bobina por un periodo superior a 2 (s). En la Figura 3.29 se muestra el esquema del circuito electrónico y se identifica los elementos conectados a las entradas y salidas de la placa.

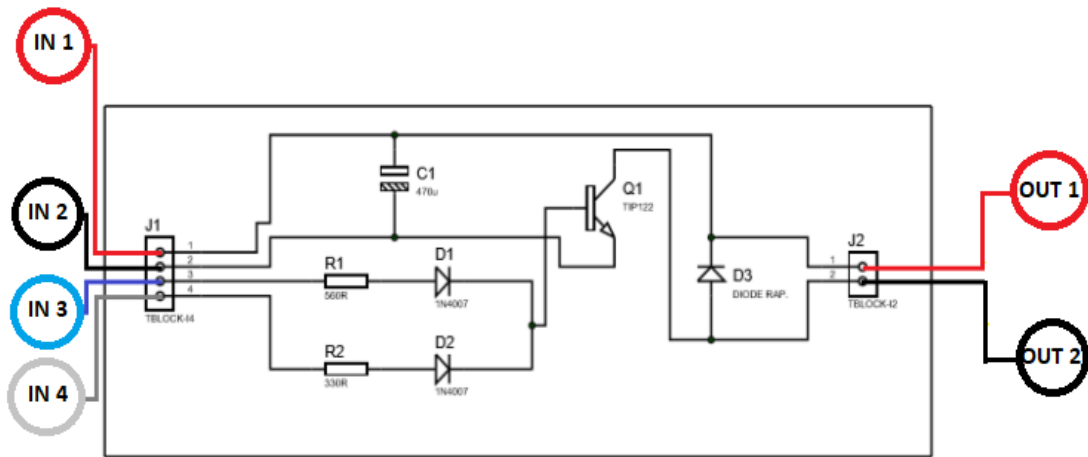


Figura 3.29 Diagrama esquemático de la placa PCB-circuito de conmutación.

En la Tabla 3.19 se describe los elementos conectados a cada bornera de la placa.

Tabla 3.19 Elementos conectados a las borneras de la placa PCB.

Borneras IN:	Elemento conectado:	Borneras OUT:	Elemento conectado:
IN 1	12 (V _{DC}) Fuente de alimentación biométrico / COM- relé biométrico / COM- Módulo relé Arduino.	OUT 1	12 (V _{DC}) Cerradura eléctrica.
IN 2	GND Fuente de alimentación biométrico.	OUT 2	GND Cerradura eléctrica.
IN 3	Contacto NO – relé biométrico.		
IN 4	Contacto NO – Modulo relé Arduino.		

En la Tabla 3.20 se muestra los elementos electrónicos utilizados en la elaboración de la placa.

Tabla 3.20 Elementos electrónicos de la placa PCB.

Elemento	Cantidad	Modelo/Valor
Terminal de bornera (J1)	3	2 entradas
Diodo (D1, D2)	2	1N4007
Diodo rápido de potencia (D3)	1	2 (W)
Transistor (Q1)	1	TIP122
Capacitor electrolítico (C1)	1	470 (uf)
Resistencia (R1)	1	330 (Ω)
Resistencia (R2)	1	560 (Ω)
Baquelita (PCB)	1	10x3 (cm)

La selección del transistor TIP122 es debido a las características de operación en voltaje y corriente que soporta, las mismas que se ajustan a los niveles de operación de la cerradura eléctrica.

En la Tabla 3.21 se presenta las especificaciones técnicas de los niveles máximos de voltaje y corriente que soporta el transistor.

Tabla 3.21 Características técnicas del transistor TIP 122.

Elemento	Nomenclatura	Modelo/Valor
Voltaje máxima Colector – Emisor	V_{CEO}	100 (V_{DC})
Voltaje máxima Base – Emisor	$V_{BE(ON)}$	2.5 (V_{DC})
Corriente máxima Colector.	$I_{C(MAX)}$	5 (A)
Corriente máxima Base.	$I_{B(MAX)}$	120 (mA)

Fuente: (Semiconductor Components Industries, 2014).

A continuación, se presentan los cálculos de los valores de los elementos pasivos utilizados para la elaboración de la placa PCB.

Cálculo de resistencias R1 Y R2.

Para el cálculo de las resistencias R1 se tomó en consideración los siguientes valores de voltaje y corriente:

- Fuente alimentación biométrico $V_{IN} = 12$ (V_{DC}).
- Corriente máxima de base $I_B = 15$ (mA).

$$V_{in} - V_D - V_B - V_{BE} = 0$$

Ec.15

$$R_B = \frac{12 - 0.7 - 2.5 \text{ (VDC)}}{15 \text{ (mA)}} = 587 \text{ } (\Omega) \quad \text{Ec.16}$$

Se definió el valor calculado a un valor de resistencia comercial de 560 (Ω) de $\frac{1}{4}$ (W).

Para el cálculo de las resistencias R2 se tomó en consideración los siguientes valores de voltaje, corriente y caída de voltaje en el cable 20 (AWG) proveniente del módulo de relés del tablero de EM.

- Fuente alimentación biométrico $V_{IN} = 12 \text{ (V}_{DC})$.
- Corriente máxima de base $I_B = 15 \text{ (mA)}$.
- Caída de voltaje en el cable 20 (AWG) tomando como referencia una distancia de 60 (m) (10 (m) $V_{\text{Cable 20 (AWG)}} = 0.48 \text{ (V}_{DC})$)

$$V_{in} - V_D - V_B - V_{BE} - V_{Cu \text{ 20 (AWG)}} = 0 \quad \text{Ec. 17}$$

$$R_B = \frac{12 - 0.7 - 2.5 - 3 \text{ (VDC)}}{15 \text{ (mA)}} = 386.66 \text{ } (\Omega) \quad \text{Ec.18}$$

Se definió el valor calculado a un valor de resistencia comercial de 330 (Ω) de $\frac{1}{4}$ (W).

Elaboración de placa PCB.

Se realizó el circuito PCB con la ayuda del programa Proteus ISIS 7, utilizando el método del planchado para la elaboración de la placa PCB.

A continuación, se presenta el proceso realizado para la elaboración de la placa PCB.

- 1) Se realiza la elaboración del circuito en el *software* Proteus ISIS 7.
 - 2) Se realiza la impresión del esquema de pistas del circuito en papel fotográfico o termotransferible.
 - 3) Se realiza la transferencia de las pistas a la baquelita de cobre, mediante el proceso del planchado.
 - 4) Se separa la parte de cobre de la baquelita que no corresponde a las pistas del circuito mediante la sumergida de la baquelita en ácido férrico.
 - 5) Se perfora los *pads* de la placa PCB.
 - 6) Se sueldan mediante caudín y estaño los elementos electrónicos a la placa.
- En la Figura 3.30 se muestra el proceso de elaboración de la placa PCB.



Figura 3.30 Circuito PCB-conmutación.

Instalación de la Placa PCB para el manejo de la cerradura.

La placa del circuito de conmutación fue instalada dentro de un cajetín metálico ubicado sobre el cielo falso, encima de la puerta de las aulas 27, 28 y 29, donde se concentran el cableado de red, los cables provenientes del módulo de relé del Arduino Mega y donde se encuentra instalada la fuente de alimentación del biométrico.

Para la ubicación de la placa se tomó en consideración de que la alimentación de la cerradura eléctrica se realizaría desde la fuente de alimentación del biométrico, también se tomó en consideración la distancia de separación de la placa a la cerradura eléctrica y al terminal biométrico esto con el fin de evitar el uso innecesario del cable eléctrico utilizado en las conexiones de la entrada de la placa a la salida del relé del terminal biométrico, como la conexión de la salida de la placa a la cerradura eléctrica.

Para evitar un corto circuito entre el cajetín metálico y la placa del circuito de conmutación, se aisló mediante la colocación de esponja reciclada la superficie inferior de la placa donde se encuentran las pistas de cobre del circuito (Ver Figura 3.28).

En el anexo H se muestra el esquema de conexión realizado para el manejo adecuado de la cerradura eléctrica desde el terminal biométrico y desde el Arduino Mega mediante el circuito de conmutación realizado (Placa PCB).

Montado del equipo biométrico y cerradura eléctrica.

Equipo biométrico.

Fuente de alimentación terminal biométrico

Se definió la ubicación de instalación de la fuente de alimentación eléctrica del mismo, para lo cual se consideró que la fuente de alimentación sería utilizada para alimentar tanto al terminal biométrico como de dotar el pulso de energía para la activación de la cerradura eléctrica.

Con el fin de garantizar un correcto funcionamiento de los equipos a ser alimentados por la fuente, se realizó el cálculo de la caída de tensión del cable considerando en el peor de los casos una longitud del cable de 5 (m).

Para dicho cálculo se consideró el diámetro del cable de cobre calibre 20 (AWG) utilizado para la conexión, con una longitud de 5 (m). En la ecuación 19 se muestra el desarrollo.

En el anexo G se encuentra la tabla que se tomó de referencia para el diámetro del cable de cobre calibre 20 (AWG) y del valor de resistividad del cobre.

$$R_{Cu\ 20\ (AWG)} = \rho \frac{L_{Cu\ 20\ (AWG)}}{A_{Cu\ 20\ (AWG)}} \quad \text{Ec.19}$$

$R_{(\Omega)}$ = Resistencia del cable (Ω)

$L_{(m)}$ = Longitud del cable (m)

$A_{(mm^2)}$ = área del cable (mm^2)

$P_{((\Omega * m) / mm^2)}$ = Resistividad del cobre ($\Omega * (mm^2) / m$)

$$R_{Cu\ 20\ (AWG)} = 0.0171 (\Omega * (mm^2) / m) \frac{5\ (m)}{0.5178\ (mm^2)} = 0.16\ (\Omega) \quad \text{Ec.20}$$

Con el valor de resistencia del cable, se calcula la caída de tensión en el mismo.

$$V_{(DC)\ \text{Caída de Tensión}} = I_{(A)} * R_{Cu\ 20\ (AWG)} \quad \text{Ec. 21}$$

$V_{(DC)}$ = Tensión corriente directa (V_{DC})

$I_{(A)}$ = Intensidad de corriente (A)

$R_{(\Omega)}$ = Resistencia del cable longitud 5 (m).

$$V_{(DC)\ \text{Caída de Tensión}} = 3(A) * 0.16(\Omega) = 0.48\ V_{(DC)} \quad \text{Ec. 22}$$

Con el valor de la caída de tensión en el cable, se calculó la diferencia de potencial que alimenta al biométrico.

$$V_{(DC) \text{ biom}} = V_{(DC) \text{ Fuente Alim.}} - V_{(DC) \text{ Caída de Tensión.}} \quad \text{Ec.23}$$

$$V_{(DC) \text{ Biom}} = 12V_{(DC)} - 0.48 V_{(DC)} = 11.52 V_{(DC)} \quad \text{Ec.24}$$

Con el valor calculado en la Ec.24 se procedió a instalar la fuente de alimentación a una distancia inferior a 5 (m) y a conectar los cables que alimentarían al biométrico utilizando cables de cobre calibre 20 (AWG), debido a que el valor de alimentación del terminal biométrico calculado en la Ec.24 se encuentra dentro del rango de tolerancia admisible para su correcto funcionamiento.

Además, se procedió a conectar la fuente de alimentación a la placa PCB del circuito de conmutación que permite el manejo de la cerradura eléctrica.

En la Figura 3.31, se muestra la fuente de alimentación instalada y montada sobre el cielo falso, encima de la puerta de cada aula.



Figura 3.31 Fuente de alimentación del terminal biométrico.

La alimentación de la fuente (V_{AC}) se realizó desde una línea de voltaje regulada, la cual proviene de un regulador de voltaje ubicado en el tablero de ET de cada grupo de aulas.

Biométrico.

En la Figura 3.32 se muestra el terminal Biométrico IP SF300 instalado en las aulas 27, 28 y 29.



Figura 3.32 Terminales biométricos instalados.

Para la instalación del terminal biométrico IP SF300 se tomó en consideración una altura de instalación del equipo de 1.2 (m) desde el suelo y a 5 (cm) de separación de la puerta, esto con el fin de que los usuarios puedan colocar sin dificultad el dedo en el lector de huella digital del equipo.

Definida la posición del terminal biométrico, se fijó la base del dispositivo sobre la pared, se empalmó los cables para el manejo de la cerradura eléctrica en las salidas COM y NO, se realizó la conexión del cable de red en el *Jack* de comunicación de red del equipo, finalmente se conectó la alimentación 12 (V_{DC}) al terminal Biométrico y se montó el equipo sobre la base fija.

Los empalmes de los cables se realizaron con estaño, aislando cada empalme con aislante termo-fundente.

En la Figura 3.33, se muestra el montaje del terminal biométrico.

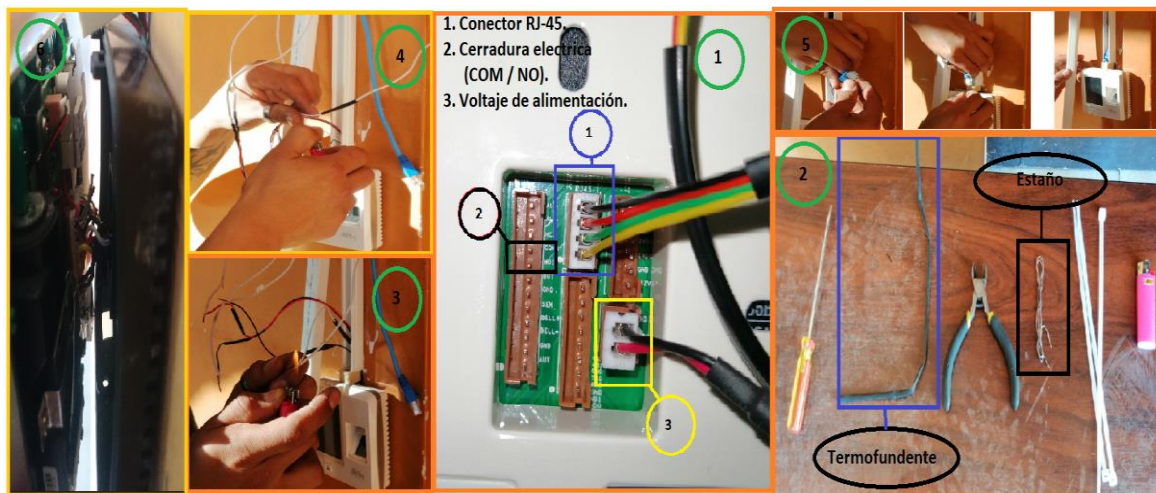


Figura 3.33 Conexión y montaje del biométrico.

1. Terminales de conexión del biométrico.
2. Materiales para realizar empalme.
3. Empalme y estañado de empalme.
4. Colocación de aislante termo-fundente en empalmes.
5. Conexión de cable de datos conector RJ-45.
6. Colocación en la base del biométrico.

Cerradura eléctrica

En la Figura 3.34 se muestra la cerradura eléctrica de marca TRAVEX instalada en las aulas 27, 28 y 29.



Figura 3.34 Cerradura eléctrica y sus partes.

Partes de la cerradura:

1. Cables de alimentación (12 (V_{DC})/ 1 [A]).
2. Contrachapa.
3. Botón de accionamiento manual.
4. Ranura para llaves.
5. Pestillo principal.
6. Cilindro de llave.

Para el montaje de la cerradura eléctrica se tomó en consideración colocarla encima de la cerradura de manija, a una altura de 1.10 (m) desde el suelo, esto debido a la estética de la instalación y a que los usuarios puedan halar la puerta mediante el uso de la cerradura de manija.

Definida la posición de la cerradura eléctrica, se verificó las medidas de la superficie de la parte de la puerta donde iría sujeta la cerradura eléctrica, esto con la finalidad de garantizar que la cerradura pueda ser sujeta con todos sus tornillos de sujeción.

La superficie de la parte donde se instaló la cerradura eléctrica cumplió con las medidas requeridas de 13 (cm) de ancho y 10.5 (cm) de alto, por lo que se procedió a centrar la cerradura eléctrica para su instalación.

Centrada la cerradura eléctrica en la puerta y la contrachapa en el marco de la puerta se tomó en consideración la separación entre la cerradura y la contrachapa, esto debido a que si la distancia excede los 5 (mm) el pestillo principal no cerraría.

Tomada dichas recomendaciones, se realizó el agujero donde se introduce el cilindro de llave, para después sujetar la placa de la cerradura a la puerta, ajustar el cilindro de llave a la placa de la cerradura y por último sujetar la contrachapa al marco de la puerta.

Con el montaje de la cerradura eléctrica en la puerta de las aulas 27, 28, 29, se realizó la conexión de la activación eléctrica de la cerradura, la cual proviene de la placa del circuito de conmutación. En la Figura 3.35 se muestra el montaje de la cerradura eléctrica.



Figura 3.35 Montado de la cerradura eléctrica.

Instalación del *software* de administración de los biométricos.

En la Figura 3.36 se muestra la interfaz principal del *software* ZKAccess 3.5 instalado para la administración de los terminales biométricos.

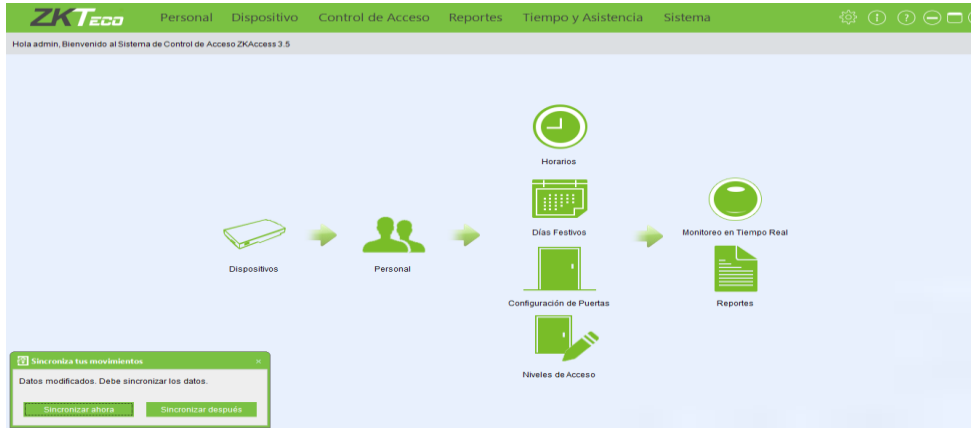


Figura 3.36 Interfaz principal del *software* ZKAccess 3.5.

Para la instalación del *software* ZKAccess 3.5, se seleccionó un computador que cumpla con las especificaciones de *hardware* y *software* impuestas por el fabricante para una correcta ejecución del programa.

En base a las características de la Tabla 1.4, se solicitó a la DGIP un computador (servidor local) con las características mencionadas en la Tabla 3.22.

Tabla 3.22 Características del *host* local solicitado para instalación del *software* ZKAccess 3.5.

Equipo	Características del <i>Host</i> local solicitado
Computador de escritorio.	Disco Duro de 500 (GB). Tarjeta de memoria RAM 4 (GB). Procesador CORE I3. Sistema operativo Windows 10, 64 bits.

El Servidor local del sistema fue instalado en la dirección, habilitado el puerto número 4370, el mismo que requiere el *software* ZKAccess 3.5 para la comunicación TCP con los terminales biométricos.

Se descargó el *software* ZKAccess 3.5 desde la página oficial de ZK-Teco Latinoamérica y se realizó la instalación del mismo.

Además del *software* de administración del sistema de control de acceso se instaló el aplicativo realizado para la administración del sistema de automatización.

En la Figura 3.37 se muestra el servidor local de sistema.

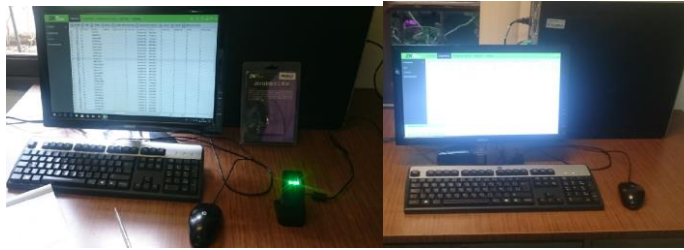


Figura 3.37 Servidor local del sistema.

Configuración del *software* ZKAccess 3.5 para el control de acceso.

Para realizar la administración de los terminales biométricos IP desde el *software* ZKAccess 3.5, se configura la dirección IP en cada uno de los terminales biométricos, para después agregar cada dispositivo al *software* de administración.

En el Anexo I1, se muestra el proceso paso a paso de configuración de red (direcciones IP) realizado en el dispositivo.

En la Figura 3.38 se muestra un esquema con el proceso que se utilizó para configurar las direcciones IP, máscara de subred y puerta de enlace a los terminales biométricos.

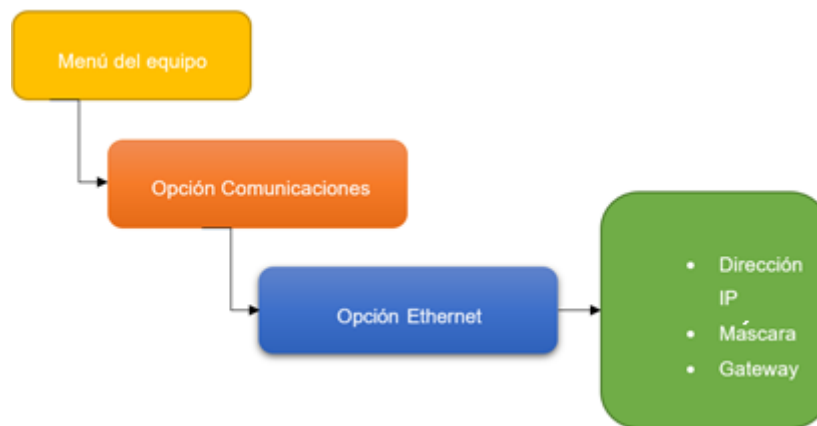


Figura 3.38 Esquema del proceso de configuración de red del dispositivo.

Con la configuración de las direcciones IP a los biométricos, se agregan los dispositivos al *software* ZKAccess 3.5.

El nombre colocado a cada dispositivo es el número del aula al cual se encuentra asignado, en la Tabla 3.23 se muestra el nombre asociado a cada dispositivo agregado en el *software*.

Tabla 3.23 Nombre asignado en el *software* a cada terminal biométrico.

Ubicación del terminal biométrico	Nombre asignado al dispositivo en el <i>software</i> de ZKAccess 3.5.
Terminal biométrico del aula 27	Aula 27
Terminal biométrico del aula 28	Aula 28
Terminal biométrico del aula 29	Aula 29

En la Figura 3.39 se muestra un esquema del proceso que se utilizó para agregar los dispositivos al *software*.



Figura 3.39 Esquema del proceso para agregar dispositivos.

En la Figura 3.40 se muestran los dispositivos agregados en la interfaz del *software*.

	Dispositivo	Número d...	Comunicación	Dire...	Pu...	RS...	Habilita...	Us
1	<input type="checkbox"/>	AULA 39	AHRS174...	TCP/IP	172....		<input checked="" type="checkbox"/>	
2	<input type="checkbox"/>	AULA 38	39291515...	TCP/IP	172....		<input checked="" type="checkbox"/>	
3	<input type="checkbox"/>	AULA 37	AHRS174...	TCP/IP	172....		<input checked="" type="checkbox"/>	
4	<input type="checkbox"/>	AULA 36	39291515...	TCP/IP	172....		<input checked="" type="checkbox"/>	
5	<input type="checkbox"/>	AULA 35	39291515...	TCP/IP	172....		<input checked="" type="checkbox"/>	
6	<input type="checkbox"/>	AULA 34	AHS51817...	TCP/IP	172....		<input checked="" type="checkbox"/>	
7	<input type="checkbox"/>	AULA 33	39291515...	TCP/IP	172....		<input checked="" type="checkbox"/>	
8	<input type="checkbox"/>	AULA 32	AHRS174...	TCP/IP	172....		<input checked="" type="checkbox"/>	
9	<input type="checkbox"/>	AULA 30	AHRS174...	TCP/IP	172....		<input checked="" type="checkbox"/>	
10	<input checked="" type="checkbox"/>	AULA 29	39291515...	TCP/IP	172....		<input checked="" type="checkbox"/>	
11	<input checked="" type="checkbox"/>	AULA 28	AHRS174...	TCP/IP	172....		<input checked="" type="checkbox"/>	
12	<input checked="" type="checkbox"/>	AULA 27	AHRS175...	TCP/IP	172....		<input checked="" type="checkbox"/>	

Figura 3.40 Dispositivos agregados en la interfaz del *software* ZkAccess 3.5.

Levantamiento de la base de datos y creación de niveles de acceso.

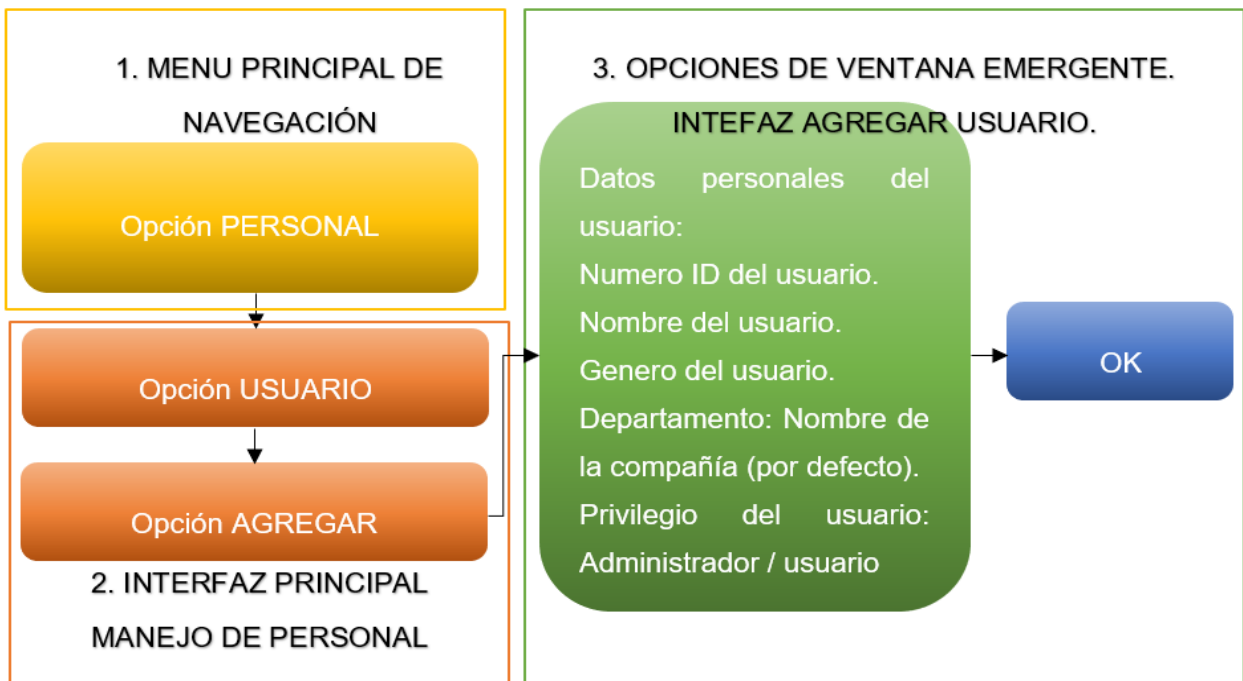
En el *software* se realizó el levantamiento de una base de datos con información de datos personales de los usuarios (docentes y personal de mantenimiento) y los horarios de cada una de las materias, siendo dicha información esencial para la creación de los distintos niveles de acceso.

El levantamiento de la base de datos se realizó con información de docentes, personal de mantenimiento (administrador del sistema) y horarios del periodo 2019-B.

En el Anexo I2 se muestra la información utilizada para el levantamiento de la base de datos que permite el manejo de las terminales biométricas de las aulas 27, 28 y 29 de la ESFOT-EPN.

Los datos personales del personal docente que se utilizó para el levantamiento de la base de datos fueron el nombre, apellido y género.

En la Figura 3.41 se muestra un esquema del proceso que se utilizó para agregar usuarios y la interfaz del *software* donde se realizó dicho proceso.



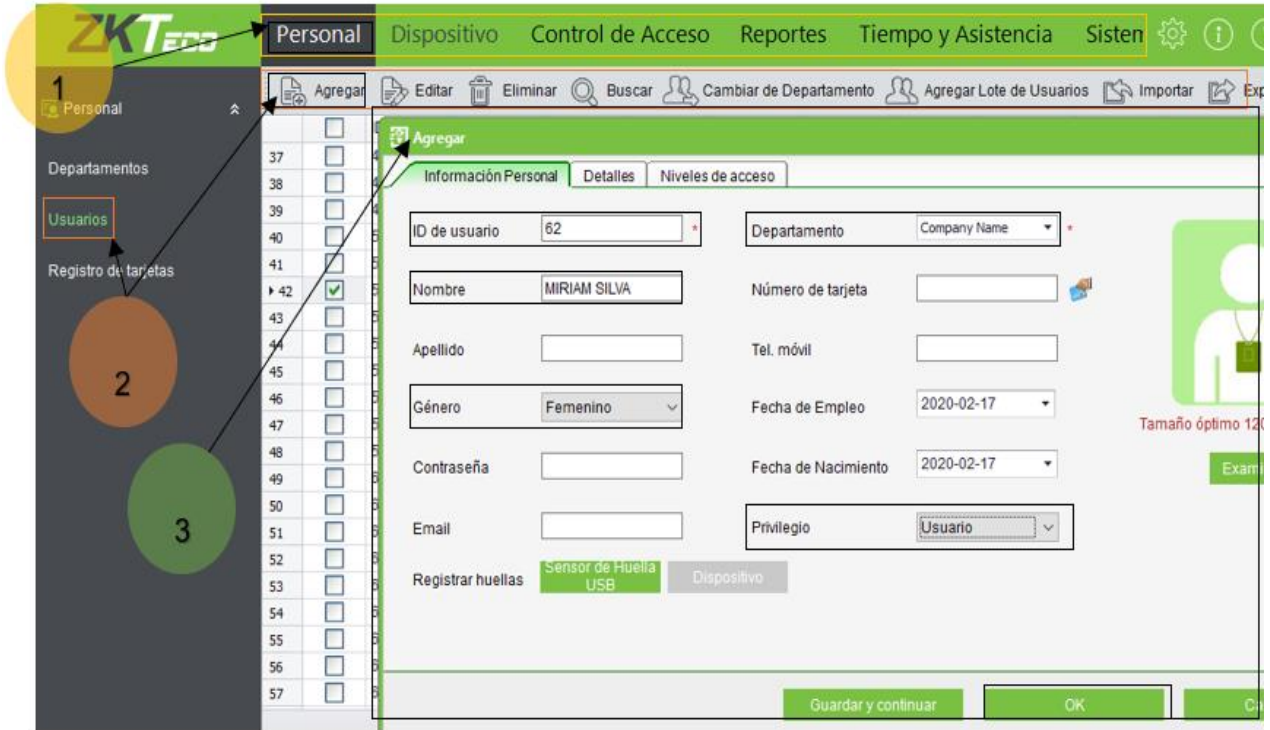


Figura 3.41 Interfaz para agregar usuarios.

NIVELES DE ACCESO

Se creó un nivel de acceso por cada horario de materia, con lo que se garantiza que no existirá cruce de niveles de acceso en una misma aula ni a una misma hora.

Los datos utilizados para la creación de los distintos niveles de acceso y horarios de cada una de las materias fueron, el código de la materia (nombre de horario y del nivel de acceso) y el nombre de la materia (característica del horario).

En la Figura 3.42 se muestra un esquema del proceso que se utilizó para la creación de los horarios y la interfaz del *software* donde se realizó dicho proceso.

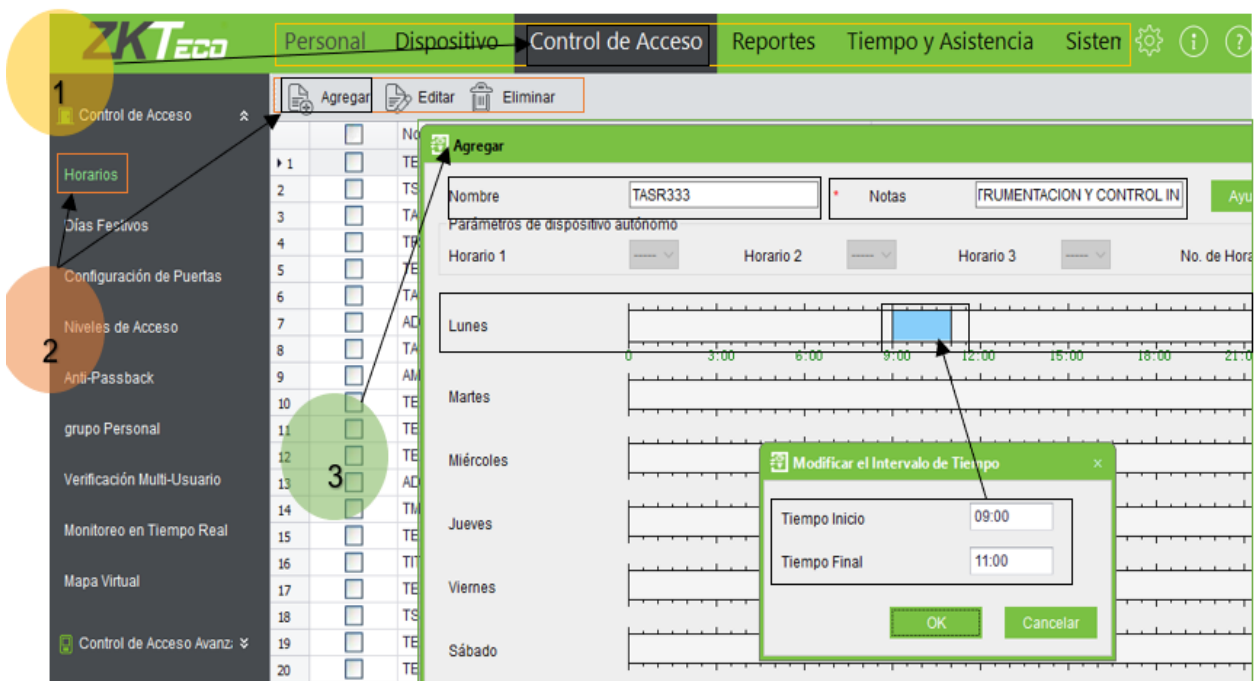
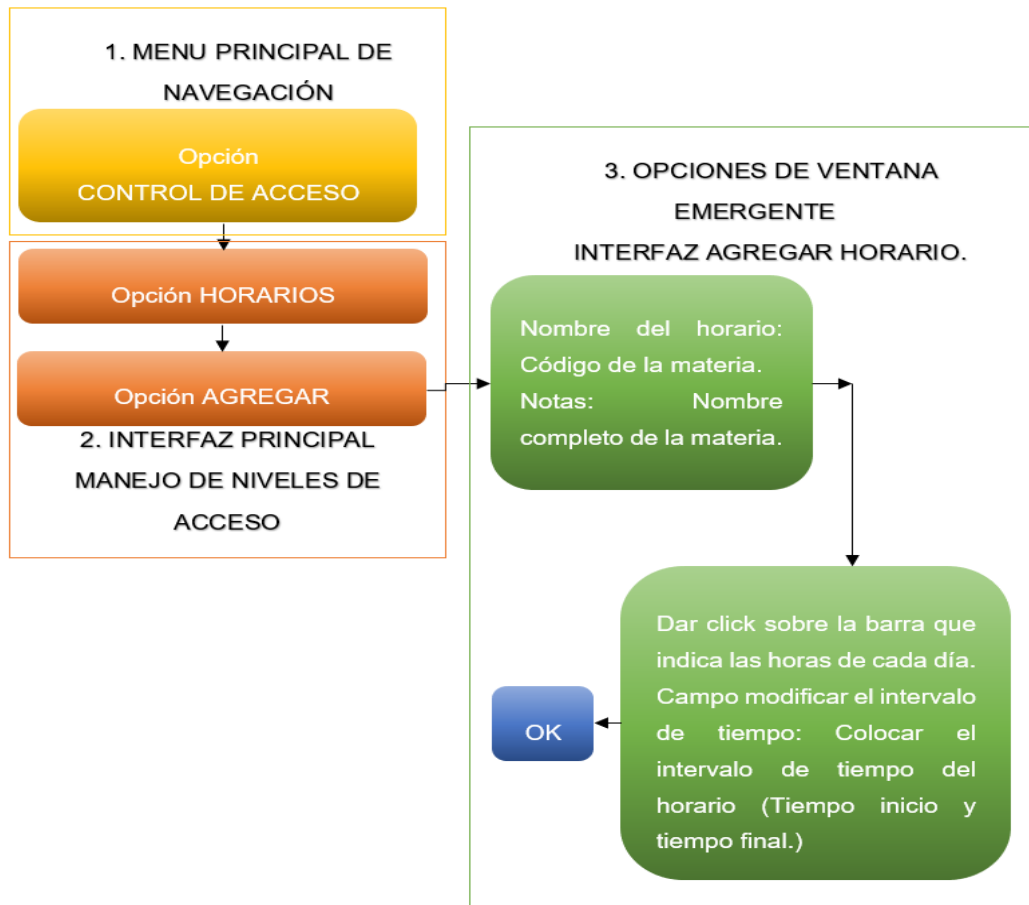


Figura 3.42 Interfaz para agregar horarios.

Agregado los horarios de cada materia se crearon los niveles de acceso, los cuales se asociaron a cada horario, dispositivo y docente asignado a dictar dicha materia.

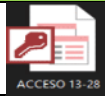
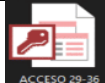
Para lo cual se tomó en consideración la limitante que presenta el *software* ZKAccess 3.5 con respecto a que únicamente permite la creación de 50 niveles de acceso.

Para solventar dicho inconveniente se realizó la división de las aulas en 3 grupos, creando 3 bases de datos, en cada base de datos se encuentran agregados los dispositivos de cada aula asignada a dicho grupo y únicamente los niveles de acceso que deben asociarse a cada dispositivo, con lo cual el número de niveles de acceso en cada base de datos es inferior al número máximo permitido por el *software*.

En el Anexo I3 se muestra el proceso paso a paso de respaldo de información (respaldo de la base de datos) y restauración de información (restauración de la base de datos) al *software* ZKAccess 3.5.

En la Tabla 3.24 se muestra en qué respaldo de la base de datos se encuentran las aulas 27, 28 y 29 de la ESFOT.

Tabla 3.24 Respaldos de la base de datos para las aulas 27, 28 y 29.

Icono base de datos.	Nombre del respaldo de la base de datos.	Nombre del dispositivo perteneciente ha dicho respaldo de la base de datos.
	ACCESO 13 – 28	AULA 27 y AULA 28
	ACCESO 29 – 34	AULA 29

En la Tabla 3.25 se muestra los distintos niveles de acceso creados, el nombre del horario asignado, docente asignado a dicho nivel de acceso y el dispositivo a donde se descargó dicha información.

Tabla 3.25 Administración de horarios, control y niveles de acceso.

Nombre niveles de acceso	Nombre del horario de la materia	Nombre del docente	Nombre del dispositivo
TASR224 Y CP	TASR224 Y CP	Santiago Guerra	Aula 27
TEM433	TEM433	Hugo Zúñiga	Aula 27
TASR214 Y CP	TASR214 Y CP	Sandra Panchi	Aula 27
TET424	TET424 Y TET516	Fanny Flores	Aula 28
ADMR262	ADMR262	Stefanie Vásquez	Aula 28
TMI412	TMI412	Flavio Mora	Aula 28
MATR213	MATR213	Sandra Panchi	Aula 28

TAD623	TAD623	Luis Ponce	Aula 28
FISR133	FIS133	Pedro Buitrón	Aula 28
TEM415	TEM415	Carlos Romo	Aula 28
TET522	TET522	Luz Vintimilla	Aula 28
TAS513	TAS513	Mauricio Rojas	Aula 28
CNTS040 M (29)	CNTS040 M (29)	Bryan Castillo	Aula 29
CNTS040 T (29)	CNTS040 T (29)	María José Bautista	Aula 29
CNTS050 M (29)	CNTS050 M (29)	Consuelo González	Aula 29
CNTS050 T (29)	CNTS050 T (29)	Christian Torres	Aula 29
CNTS010 M (29)	CNTS010 M (29)	Andrea Cadena	Aula 29
CNTS010 T (29)	CNTS010 T (29)	Tamara Monar	Aula 29
CNTS020 M (29)	CNTS020 M (29)	Edmundo Cruz	Aula 29
CNTS020 T (29)	CNTS020 T (29)	Edmundo Cruz	Aula 29
CNTS030 M (29)	CNTS030 M (29)	Carlos Gualpa	Aula 29
CNTS030 M (29)	CNTS030 M (29)	Karen Soto	Aula 29

En la Tabla 3.26 se muestra la información con el nombre del nivel de acceso creado para los usuarios con privilegios de administrador, el nombre del horario asignado, los usuarios asignados a dicho nivel de acceso y el dispositivo a donde se descargó dicha información.

El usuario asignado con privilegios de administración tendrá acceso total a las aulas, por lo que se asignó el horario por *default* que viene establecido en el *software*.

Tabla 3.26 Nivel de acceso para el usuario Administrador.

Nombre niveles de acceso	Nombre del horario para administrador	Nombre del administrador del sistema	Nombre del dispositivo
ADMINISTRADOR	ADMINISTRADOR	Manuel Comina	Aula 27, Aula 28 y Aula 29
ADMINISTRADOR	ADMINISTRADOR	Miguel Mariscal	Aula 27, Aula 28 y Aula 29

En la Figura 3.43 se muestra un esquema del proceso que se utiliza para la creación de los niveles de acceso y la interfaz del *software* donde se realiza dicho proceso.

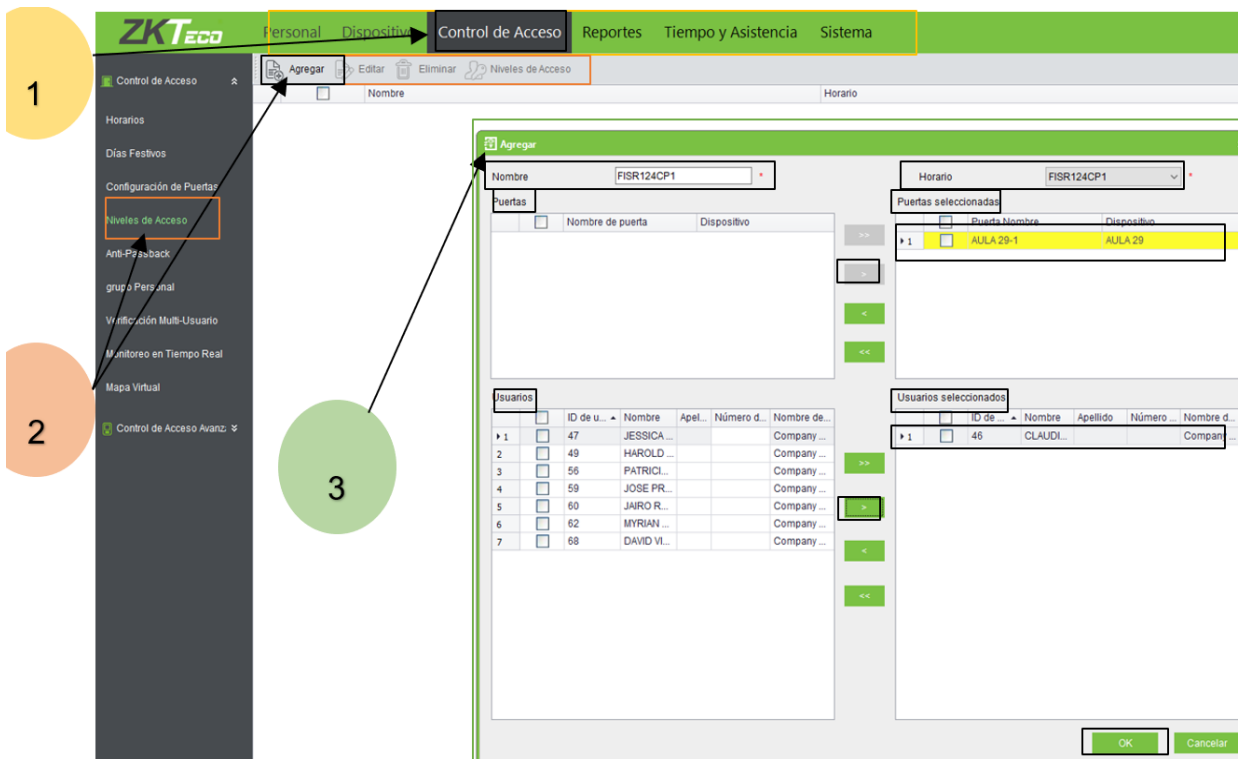


Figura 3.43 Interfaz para agregar niveles de acceso.

Registro de huellas dactilares de usuarios y descarga de información a terminales biométricos.

Se realizó el registro de las huellas dactilares de los usuarios al sistema, para lo cual se tiene dos maneras de enrolamiento de huellas dactilares.

En la Tabla 3.27 se presentan las dos formas de enrolamiento de huellas que se puede utilizar para dicha operación y las características del enrolador ZK4500.

Tabla 3.27 Nombre asignado en el *software* a cada terminal biométrico.

Dispositivo utilizado para el enrolamiento de huellas dactilares al <i>software</i> .	Descripción del proceso a realizar
Terminal biométrico SF300	El proceso de enrolamiento de huellas dactilares utilizando el terminal biométrico SF300, se realiza en el dispositivo, para después descargar al <i>software</i> la información agregada al mismo.
Lector de huellas dactilares ZK4500 (Enrolador)	El proceso de enrolamiento de huellas dactilares utilizando el enrolador ZK4500, se realiza directamente al <i>software</i> de escritorio. (Opción recomendada)

Se optó por adquirir el enrolador ZK4500, debido a que el proceso de enrolamiento de huellas dactilares mediante el uso del enrolador se realiza directamente al *software*.

En el Anexo I4 se presenta la manera de enrolamiento de huellas dactilares utilizando el terminal biométrico SF300.

Para el registro de las huellas dactilares de los usuarios se ingresó al siguiente campo.

- **Sensor de huella USB:** Opción que se encuentra en la interfaz de agregar usuario.

Se optó por registrar 3 huellas digitales por cada usuario, esto con la finalidad de brindar al usuario varias posibilidades de autenticación con el sistema.

Las huellas digitales de los dedos registrados en la base de datos fueron: dedo pulgar e índice de la mano derecha y dedo pulgar de la mano izquierda, esto debido a la facilidad que otorga la colocación de dichos dedos para su autenticación en el lector del biométrico.

En la Figura 3.44 se muestra la interfaz del *software* donde se realiza dicha operación y un esquema del proceso que se utiliza para el registro de las huellas dactilares de los docentes y administradores del sistema.

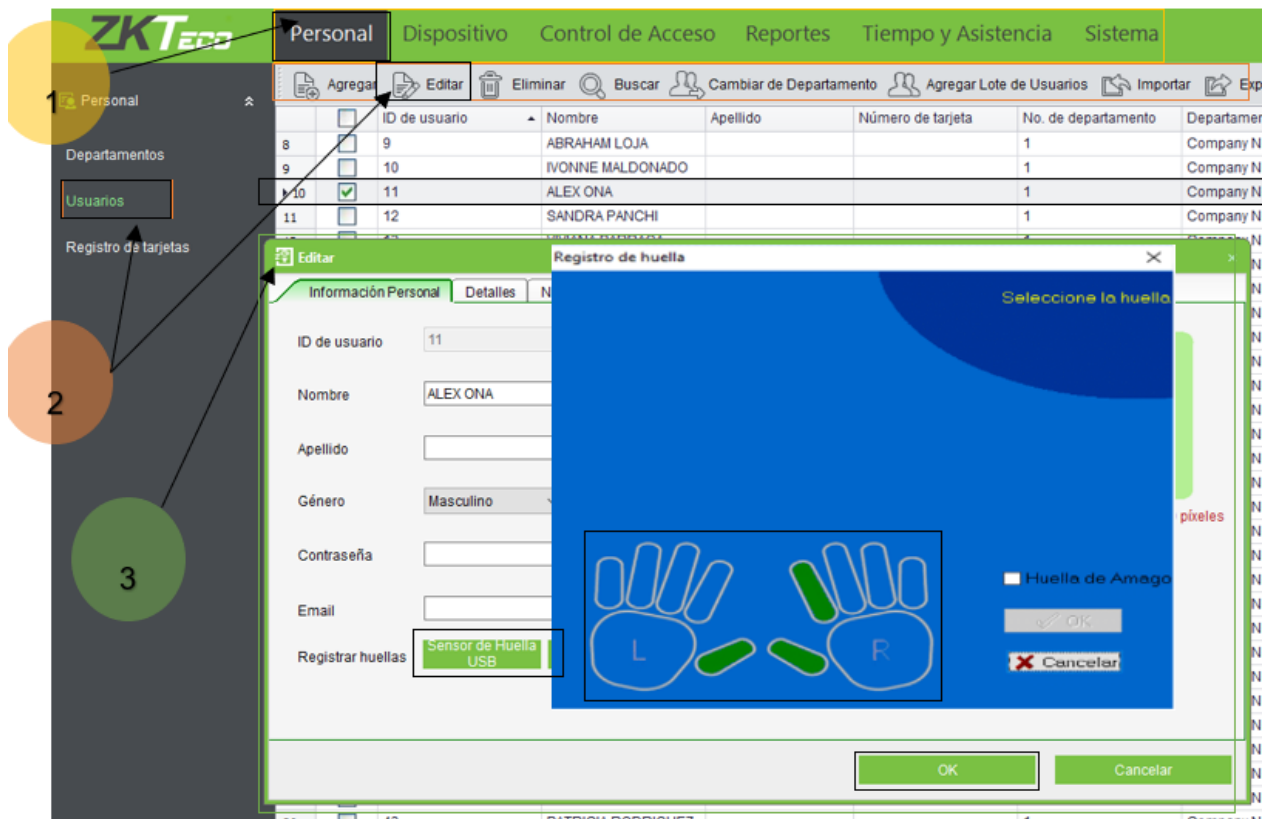
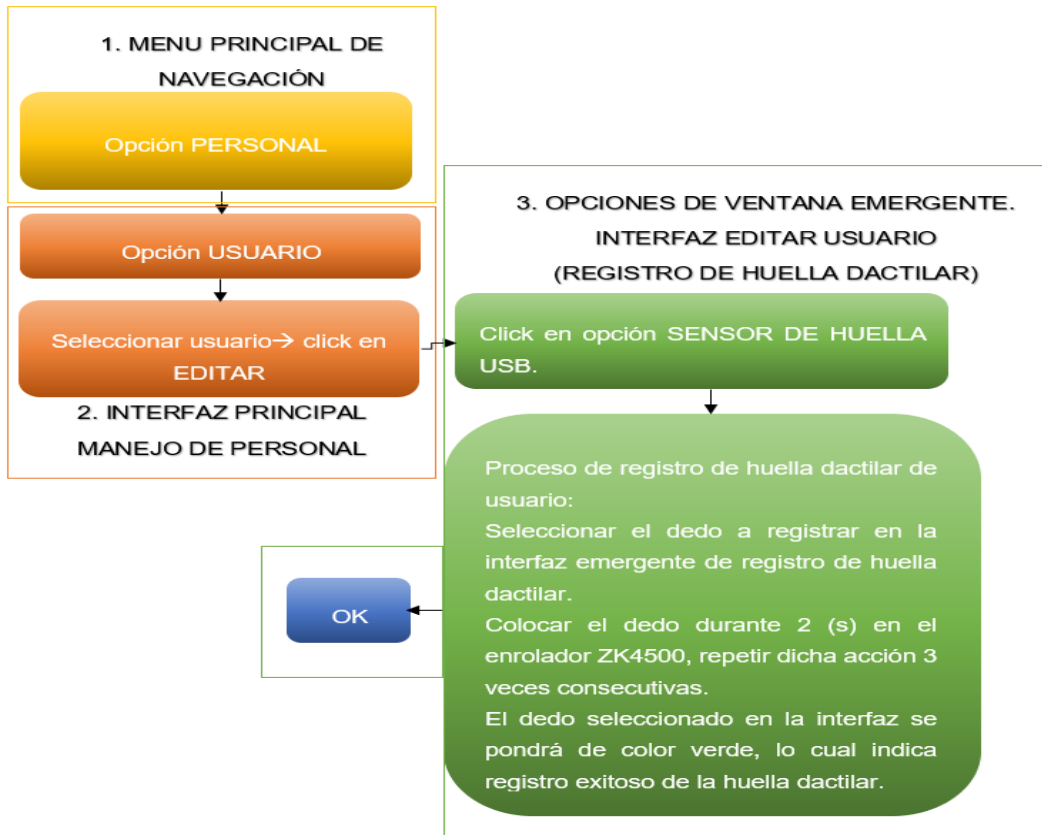


Figura 3.44 Interfaz para registro de huellas dactilares.

Con el registro de huellas dactilares de los docentes en el *software*, se cargó (sincronizó) la información de la base de datos a los terminales biométricos de las aulas 27,28 y 29.

Para realizar la sincronización de la información a los dispositivos 27 y 28 se restauró la base de datos ACCESO 13 – 28, mientras que para el dispositivo AULA 29 se restauró la base de datos ACCESO 29 – 34 en el *software*.

En la Figura 3.45 se muestra un esquema del proceso utilizado para sincronizar la información de la base de datos a los dispositivos Aula 27, Aula 28, Aula 29 y la interfaz del *software* donde se realizó dicha operación.

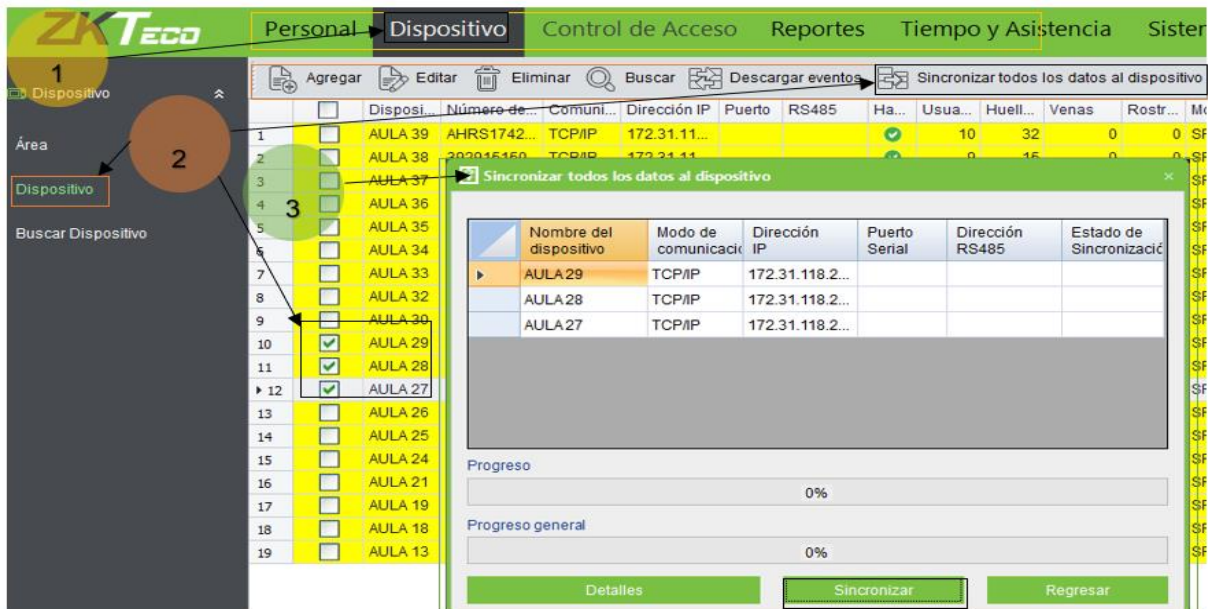
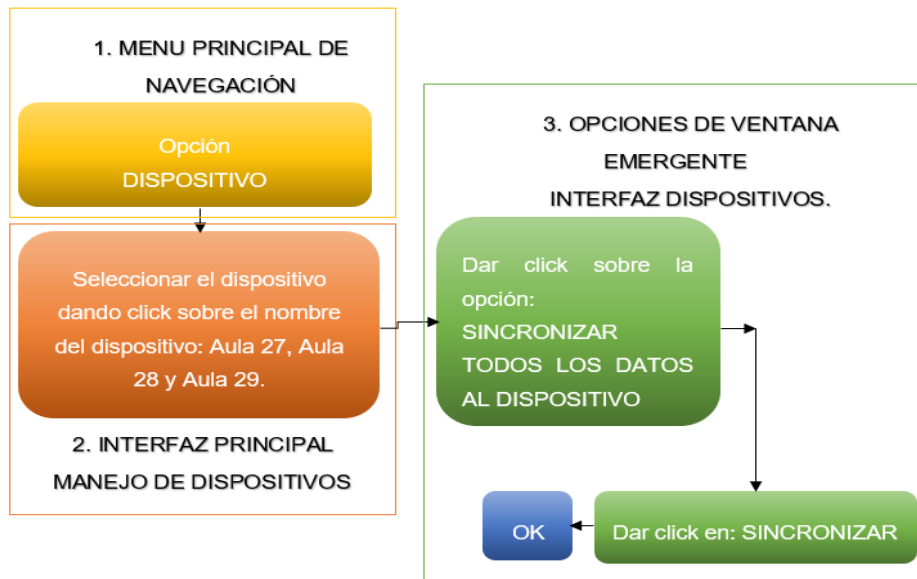


Figura 3.45 Esquema de sincronización de información a los dispositivos.

3.4 Pruebas y análisis de resultados

Después de concluir con la instalación de los biométricos, se procedió a realizar 3 tipos de pruebas con el fin de verificar el correcto funcionamiento y el cumplimiento de los objetivos que se plantearon.

Entre las pruebas que se realizó al sistema de control de acceso a las aulas 27, 28 y 29 fueron las siguientes:

- Pruebas del ponchado.
- Pruebas de comunicación de red.
- Pruebas de funcionamiento del biométrico y cerradura eléctrica.

Pruebas del ponchado

Prueba de verificación del cable de red ponchado bajo la norma T568-B.

Se conectó cada extremo del cable de red ponchado a cada módulo del comprobador de red LAN para probar la continuidad punto a punto de los 8 conductores ponchados sobre el conector RJ-45. Los *leds* de color verde se encienden cuando se ha ponchado de forma correcta.

En caso de que el ponchado se encuentre de forma incorrecta, se enciende el *led* de color rojo.

En la Tabla 3.28 se muestra los resultados obtenidos de la prueba del ponchado.

Tabla 3.28 Prueba del cable de red ponchado con la norma T568-B.

N° de pin en el extremo A del cable ponchado	Color del <i>led</i> indicador en la unidad remota	N° de pin en el extremo B del cable ponchado	Color del <i>led</i> indicador en la unidad maestra	Pasa	No pasa
1	Verde	1	Verde	SI	-
2	Verde	2	Verde	SI	-
3	Verde	3	Verde	SI	-
4	Verde	4	Verde	SI	-
5	Verde	5	Verde	SI	-
6	Verde	6	Verde	SI	-
7	Verde	7	Verde	SI	-
8	Verde	8	Verde	SI	-

Mediante la Tabla 3.28 se comprobó que los cables ponchados funcionan correctamente siguiendo la norma T568-B en ambos extremos de los cables de conexión y sin conductores cruzados.

Pruebas de comunicación de red

Prueba con el Arduino

Sensado de puertas, ventanas y luces.

Se realizó pruebas de los datos recibidos acerca del estado de las puertas, luminarias y ventanas de las aulas 27, 28 y 29 para lo cual se escribe la dirección IP del Arduino correspondiente a los tableros EM N° 3 y N° 4 en el navegador del servidor.

Los datos recibidos de la comunicación entre el Arduino y el servidor se muestran en la Tabla 3.29 y Tabla 3.30, donde el valor 0 (cero) significa apagado o cerrado, y el valor 1(uno) significa encendido o abierto.

Tabla 3.29 Datos recibidos del estado de las puertas, luminarias y ventanas de las aulas 27 y 28.

Dirección IP del Arduino	Estado del aula 27			Estado del aula 28		
	Puerta	Ventanas	Luminaria	Puerta	Ventanas	Luminaria
172.31.118.218 (Arduino del tablero EM N° 4)	27P:0	27V1:0, 27V2:0	27L:1	28P:0	28V1:0, 28V2:1, 28V3:0, 28V4:0	28L:0

Tabla 3.30 Datos recibidos del estado de la puerta, luminarias y ventanas del aula 29.

Dirección IP del Arduino	Estado del aula 29		
	Puerta	Ventanas	Luminaria
172.31.118.217 (Arduino del tablero EM N° 3)	29P:0	29V1:0, 29V2:0, 29V3:0	29L:0

En la Tabla 3.29 y Tabla 3.30 se comprobó que la información recibida del módulo Arduino Mega reflejada en la interfaz del servidor, corresponde al estado en que se encuentren en ese momento las ventanas, puertas y luces.

Apertura de las puertas, encendido y apagado de luces.

Para la prueba de apertura de las puertas, el encendido y apagado de las luminarias desde el servidor hacia los módulos Arduino, se ingresa la dirección IP del servidor en el navegador e inmediatamente se selecciona la opción de abrir una puerta y el encendido o apagado de las luces.

En la Tabla 3.31 se muestran los resultados de las pruebas realizadas de la apertura remota de las puertas.

Tabla 3.31 Apertura remota de puertas y luminarias de las aulas 27, 28 y 29 desde el servidor.

Control de puertas	Abre	No abre
Puerta del aula 27	SI	--
Puerta del aula 28	SI	--
Puerta del aula 29	SI	--

Como se observa en la Tabla 3.31, los resultados de la apertura de las puertas desde la página web del servidor son exitosos, ya que al seleccionar la opción ABRIR PUERTA 27, ABRIR PUERTA 28, las puertas se abren correctamente.

En la Tabla 3.32 se muestran los resultados de las pruebas realizadas del encendido y apagado de luminarias.

Tabla 3.32 Apertura remota de luminarias de las aulas 27, 28 y 29 desde el servidor.

Control de luminarias	Encender	Apagar
Luminaria del aula 27	SI	SI
Luminaria del aula 28	SI	SI
Luminaria del aula 29	SI	SI

Como se observa en la Tabla 3.32, los resultados del encendido y apagado de las luces desde la página web del servidor son exitosos, ya que al seleccionar la opción PRENDER LUZ 27, APAGAR LUZ 27, PRENDER LUZ 28, APAGAR LUZ 28, PRENDER LUZ 29, APAGAR LUZ 29, las luces se encienden o se apagan correctamente.

Prueba de conexión del *Shield Ethernet*

Se realizó la prueba del parpadeo de los *leds* del módulo *Shield Ethernet* localizado en los tableros EM N° 3 y N° 4, con el fin de comprobar si la comunicación de datos entre el servidor y el *Shield Ethernet* es correcta.

En la Tabla 3.33 se muestran los resultados de las pruebas de conexión del módulo *Shield Ethernet*.

Tabla 3.33 Prueba de conexión del módulo *Shield Ethernet*.

Ubicación del módulo <i>Shield Ethernet</i>	<i>Led</i>	Descripción	Parpadea el <i>led</i>	No parpadea el <i>led</i>
Tablero EM N° 3	LINK	Parpadea cuando recibe o envía datos (Existe conexión).	✓	--
	TX	Parpadea cuando el <i>Shield Ethernet</i> envía datos.	✓	--
	RX	Parpadea cuando el <i>Shield Ethernet</i> recibe datos.	✓	--
	100M	El <i>led</i> enciende cuando hay una conexión de red a 100 (Mbps)	✓	--
Tablero EM N° 4	LINK	Parpadea cuando recibe o envía datos (Existe conexión).	✓	--
	TX	Parpadea cuando el <i>Shield Ethernet</i> envía datos.	✓	--
	RX	Parpadea cuando el <i>Shield Ethernet</i> recibe datos.	✓	--
	100M	El <i>led</i> enciende cuando hay una conexión de red a 100 (Mbps)	✓	--

Se comprobó que el módulo *Shield Ethernet* establece conectividad con el servidor de manera correcta, ya que se visualiza el parpadeo de los *leds* de transmisión (TX) y recepción (RX) del *Shield Ethernet* cuando este se encuentra comunicándose con el servidor.

Además, según el *led* indicador de velocidad de transmisión alcanzada en la red, se comprobó que el enlace del Arduino Mega alcanza velocidades de hasta 100 Mbps.

Pruebas de funcionamiento del biométrico y cerradura eléctrica

Prueba de restricción de acceso a las aulas.

Se realizó la prueba de restricción de acceso a las aulas, para lo cual la información de la base de datos ya se encontraba sincronizada a los equipos biométricos.

Para validar el funcionamiento de los niveles de acceso, se utilizó el *software* ZKAccess 3.5, interfaz de Reporte opción Eventos de hoy.

En caso de que el usuario se encuentre dentro del nivel de acceso autorizado, se refleja en el campo evento como “Apertura”, mientras que si no se encuentra dentro del nivel de acceso autorizado o no se encuentra registrado en el sistema se refleja “Verificación fallida”.

En la Tabla 3.34 se muestran los resultados obtenidos de la prueba de autenticación para el ingreso a las aulas.

Tabla 3.34 Tipo de identificación de control de acceso registrado.

Fecha y Hora	ID de usuario	Dispositivo biométrico	Modo de verificación	Evento
2020-01-07 19:13:20	--	AULA 27	Otros	Verificación fallida
2020-01-06 09:14:45	12	AULA 27	Huella	Apertura
2020-01-07 16:06:13	22	AULA 27	Huella	Apertura
2020-01-08 12:20:32	104	AULA 28	Huella	Apertura
2020-01-08 11:23:08	103	AULA 28	Contraseña	Apertura
2020-01-07 07:14:03	53	AULA 29	Huella	Apertura
2020-01-07 07:06:31	104	AULA 29	Tarjeta	Apertura
2020-01-08 14:52:28	103	AULA 29	Contraseña	Apertura

Como se muestra en la Tabla 3.34, los resultados de la restricción de acceso a las aulas que realiza el biométrico son exitosos, ya que en el reporte que entrega el *software* ZKAccess 3.5 se visualiza que solo el personal con el nivel de acceso autorizado genera un evento de apertura.

En la Figura 3.46, se presentan el reporte que entrega el *software* con los resultados obtenidos de la restricción de acceso.

	Tiempo	ID de Usuario	Nombre	Apellido	Número d.	Dispositivo	Punto del evento	Verificación	Estado	Evento
18	2020-01-08 06:56:48	104	MARIA T.			AULA 29	AULA 29-1	Tarjeta	Entrada	Apertura
19	2020-01-08 06:38:40	104	MARIA T.			AULA 29	AULA 29-1	Tarjeta	Entrada	Apertura
20	2020-01-07 14:08:20	53	EDMUND.			AULA 29	AULA 29-1	Huella	Entrada	Apertura
21	2020-01-07 12:37:39	104	MARIA T.			AULA 29	AULA 29-1	Tarjeta	Entrada	Apertura
22	2020-01-07 07:14:03	53	EDMUND.			AULA 29	AULA 29-1	Huella	Entrada	Apertura
23	2020-01-07 07:06:31	104	MARIA T.			AULA 29	AULA 29-1	Tarjeta	Entrada	Apertura
24	2020-01-06 14:13:14	85	MARIA JO.			AULA 29	AULA 29-1	Huella	Entrada	Apertura
25	2020-01-06 07:10:06	76	BRYAN C.			AULA 29	AULA 29-1	Huella	Entrada	Apertura

Figura 3.46 Prueba de restricción de acceso.

Prueba de apertura de las puertas con el software ZKAccess 3.5

Para la prueba de la apertura de las puertas desde el software de escritorio ZKAccess 3.5, se ingresó a la interfaz de CONTROL DE ACCESO, opción MONITOREO EN TIEMPO REAL donde se muestran los íconos de las puertas, se selecciona una puerta y posteriormente se da clic en ABRIR REMOTAMENTE.

En la Tabla 3.35 se muestran los resultados obtenidos de la apertura de las puertas desde el software ZKAccess 3.5.

Tabla 3.35 Apertura remota de las aulas 27, 28 y 29 desde el software ZKAccess 3.5.

Dispositivo biométrico	Punto del evento	Operación exitosa	Operación fallida
AULA 27	AULA 27-1	SI	--
AULA 28	AULA 28-1	SI	--
AULA 29	AULA 29-1	SI	--

Como se muestra en la Tabla 3.35, los resultados de la apertura de las puertas desde el software ZKAccess 3.5 son exitosos, ya que la apertura de las puertas se ejecuta sin ningún problema.

Prueba de la placa de conmutación.

Se realiza la prueba de funcionamiento de la placa de conmutación para la activación de la cerradura eléctrica desde el biométrico como desde el Arduino Mega.

Para lo cual se procede a realizar la apertura de la puerta desde el equipo biométrico mediante autenticación de un usuario, como desde la aplicación instalada en el servidor del sistema (Arduino Mega ejecuta las órdenes enviadas por el servidor).

En la Tabla 3.36 se muestran los resultados obtenidos de la activación de la cerradura eléctrica desde el biométrico como desde el Arduino Mega.

Tabla 3.36 Prueba de funcionamiento de la placa de conmutación.

Elemento	Activación de la cerradura eléctrica, Aula 27, 28 y 29.	No activación de la cerradura eléctrica Aula 27, 28 y 29.
Equipo Biométrico	SI	--
Arduino Mega	SI	--

Como se muestra en la Tabla 3.36, los resultados del funcionamiento de la placa de conmutación son exitosos, ya que cumple con la función de conmutar la activación de la cerradura eléctrica desde dos puntos distintos, permitiendo la activación de la misma (apertura de la puerta) desde el biométrico como desde Arduino Mega.

4. CONCLUSIONES Y RECOMENDACIONES.

4.1 Conclusiones

- La implementación del sistema de monitoreo y control de acceso para las aulas 27, 28 y 29 de la ESFOT evita el uso inadecuado de las aulas, ya que el sistema permite monitorear el estado de las puertas, ventanas y luces, así como de controlar el ingreso de personal docente a las aulas únicamente en horarios de clases.
- El uso del *software* de escritorio ZKAccess 3.5 para la administración del sistema de control de acceso, permitió el enrolamiento y registro de un gran número de usuarios de forma rápida y sencilla.
- Se realizó el envío del cableado de red y cableado de sensores por la misma tubería sin presentarse ningún tipo de problema durante la comunicación de los equipos de red, por lo que se concluye que el voltaje en corriente continua que circula por el cableado de los sensores, no provoca una interferencia considerable al cableado *Ethernet*.
- La configuración de una VLAN exclusiva para el sistema, permitió integrar a todos los equipos IP a la intranet de la ESFOT al tener una red escalable que cuenta con un gran número de direcciones IP (64), para un aumento de equipos al sistema en el futuro.
- El uso de cable UTP cat. 5e para la implementación de la red del sistema, permitió alcanzar comunicaciones de hasta 100 (Mbps), por lo que la comunicación de red no presenta problemas de latencia.
- Se logró el accionamiento de la cerradura eléctrica tanto desde el biométrico como desde el Arduino Mega, utilizando una placa PCB en el cual está impreso un circuito de conmutación que protege al equipo biométrico y a la cerradura eléctrica.
- El equipo biométrico utilizado en el proyecto es un dispositivo autónomo el cual funciona sin necesidad de estar conectado a un servidor, por lo que en caso de que falle la comunicación de red, el sistema de control de acceso seguirá en funcionamiento, garantizando la restricción del acceso a las aulas a personal no autorizado.
- La velocidad que presenta el *switch* D-Link donde sus 8 puertos trabajan con cables de conexiones con velocidades de 10/100/1000 (Mbps), permitió a la red instalada con cable UTP categoría 5e funcione sin ningún problema.
- El funcionamiento normal de las placas Arduino Mega y *Shield Ethernet* era interrumpido cuando se encendían los tableros y por la activación de los conmutadores, este problema se

solventó cambiando los conmutadores por relés, además del montaje de un pulsador para el reinicio rápido del Arduino.

- Los equipos biométricos tipo 2 SF300 para los usuarios con privilegios de administrador presentaron una baja seguridad en el acceso ya que permitía validar las huellas de terceras personas, para solventar este problema se entregó una tarjeta RFID y se borraron las huellas de usuarios de acceso total, además de reducir la sensibilidad del lector biométrico.

4.2 Recomendaciones

- Separar los equipos de red en un tablero independiente al tablero de control, garantiza la correcta comunicación del sistema de red, ya que se evita posibles interferencias en la transmisión y recepción de datos producto del campo eléctrico que se genera en conductores de corriente alterna.
- Para una configuración más avanzada de los equipos biométricos se recomienda utilizar la guía (Manual de Usuario) que ofrece el fabricante.
- Se recomienda que la carga horaria de los docentes de la ESFOT se realice de forma balanceada en todas las aulas, con el fin de evitar exceder el número de niveles de acceso que otorgan los equipos biométricos y la creación de varias bases de datos para su administración.
- La lectura de la huella dactilar del equipo biométrico falla cuando la huella del usuario se ve alterada ya sea por algún corte u otra anomalía, por lo que para reducir el grado de error de lectura se recomienda el enrolamiento mínimo de 3 huellas digitales por usuario.
- Al momento de realizar el ponchado del cable UTP ya sea con la norma T568A o T568B, no se debe destrenzar los 4 conductores más de 3 (cm) porque de lo contrario el cable actuará como una antena y captará todo tipo de interferencia electromagnética.
- Se recomienda seleccionar el tiempo de duración de apertura de puertas de las aulas de 1 (s), evitando así posibles daños de los mismos, realizado vía remota desde el *software* Control de Acceso instalado en el servidor local.
- Al momento de seleccionar las placas Arduino, se recomienda elegir las placas originales en lugar de las genéricas y así reducir problemas con la comunicación TCP/IP.
- Debido a la gran cantidad de ataques cibernéticos, se recomendaría implementar las seguridades necesarias para el sistema de control de acceso y automatización.

- Se recomienda cargar toda la información acerca del horario de cada uno de los docentes y los niveles de acceso asignados a todos los biométricos, evitando así configuraciones incorrectas.
- La lectura de la huella dactilar del equipo biométrico falla cuando la huella del usuario se ve alterada ya sea por algún corte u otra anomalía, por lo que para reducir el grado de error de lectura se enrole mínimo 3 huellas digitales por usuario.
- Se recomienda colocar un disipador de calor en el transistor de la placa PCB para evitar el sobrecalentamiento de la misma.

5. REFERENCIAS BIBLIOGRÁFICAS

- ANIXTER INC. (2018). *Tecnologías de control de acceso: factores importantes en la elección de soluciones*. Obtenido de https://www.anixter.com/es_la/about-us/news-and-events/news/access-control-technologies-important-factors-when-choosing-a-solution.html
- ARDUINO.CL. (s.f.). *Arduino Mega 2560*. Obtenido de <https://arduino.cl/arduino-mega-2560/>
- Arias, M. (2016). *Redes de computadoras*. Obtenido de <http://www.labc.usb.ve/paginas/EC5751/Cableado.pdf>
- BEAUCOUP. (Diciembre de 2018).
- BRADY. (2017). *ANSI / TIA 606-C*. Obtenido de <https://www.bradyid.com.mx/recursos/norma-tia-606-c>
- Camues, C. V. (04 de 10 de 2017). *Diseño de una red de datos y propuesta de plan de contingencia para el cableado estructurado del edificio de la Defensoría Pública del Ecuador de la ciudad de Quito (Tesis de Grado)*. Escuela Politécnica Nacional, Quito. Obtenido de <http://bibdigital.epn.edu.ec/handle/15000/18816>
- Cifuentes, J. A. (2014). *Construcción de una maqueta con sistema digital para el control de la iluminación y monitoreo de acceso por puertas y ventanas mediante el puerto serial de un computador utilizando el microcontrolador Atmega (Tesis de Grado)*. Escuela Politécnica Nacional, Quito.
- CONDUCTORES RG. (2016). *CALIBRE AMERICANO AWG / Equivalencias AWG / Milimétrica*. Obtenido de <https://www.conductoresrg.com.ar/equivalencias-awg.pdf>
- CONNECTION. (2018). *CAT 5E UTP CABLE, 4PR SOLID, 100MHZ, 24 AWG, 1000FT, BLUE*. Recuperado el 12 de 2019, de Catálogo connection cabling system: http://www.connection-cs.com/?m=pn_product.php&id=6&sid=22&pn=CUP-5024
- CONSTRUEX. (2020). *Construex*. Obtenido de https://construex.com.ec/exhibidores/grupo_electro_comercial_mejia/producto/manguera_plastica_corrugada_negra
- Cueva, C. S. (2015). *Estudio de Factibilidad de un Sistema Biométrico aplicado al proceso de Citación de la Comisión de Tránsito del Ecuador (Tesis de Grado)*. UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL, Guayaquil.

D-LINK. (2018). *8-Port 10/100 Switch DES-1008C*. Recuperado el 12 de 2019, de <https://la.dlink.com/la/switches-hogar/des-1008a/>

ECURED. (2013). *Estandares IEEE802.3*. Obtenido de https://www.ecured.cu/Est%C3%A1ndares_IEEE_802.3

Ediciones ENI. (s.f.). *Arduino Mega*. Obtenido de Arduino - Aprender a desarrollar para crear objetos inteligentes: <https://www.ediciones-eni.com/open/mediabook.aspx?idR=8d182e726219b5c89e24125beb9c5494>

educovirtualuss. (2018). *Cerradura Eléctrica TRAVEX*. Obtenido de <https://www.educovirtualuss.edu.pe/sys/OnlineStore/OnlineStore/infoProd.php?CodigoProd=13349>

elarduino. (2019). *Pinout Arduino MEGA 2560*. Obtenido de <https://www.elarduino.com/mega/>

Ferrelectro. (Febrero de 2020). *CERRADURA ELÉCTRICA 1000E*. Obtenido de CATÁLOGO COMERCIAL CERRADURAS ELÉCTRICAS TRAVEX: <http://www.ferrelectro.com.pe/catalogos/travex.pdf>

FORZAUPS. (2017). *Regulador Automático de Voltaje FORZA FVR-3001*. Obtenido de <https://www.forzaups.com/media/FVR-3001-SPA.pdf>

FUNDACIÓN MAPFRE. (2012). *La seguridad integral en los centros de enseñanza obligatoria de España*. Madrid: Publicación: M-17664.

INNGRESA. (2018). *¿Cómo funcionan los sistemas biométricos?* Obtenido de <https://inngresa.com/como-funcionan-sistemas-biometricos/>

INTERPOL. (Marzo de 2018). *Huellas dactilares*. Obtenido de <https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares>

Joscowicz, J. (2013). *CABLEADO ESTRUCTURADO*. Obtenido de <https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf>

Keyestudio. (18 de 04 de 2019). *Ks0156 keyestudio W5100 Ethernet Shield*. Obtenido de https://wiki.keyestudio.com/Ks0156_keyestudio_W5100_Ethernet_Shield

Llamas, L. (06 de 01 de 2017). *CONECTAR ARDUINO A INTERNET O LAN CON SHIELD ETHERNET W5100*. Obtenido de <https://www.luisllamas.es/arduino-ethernet-shield-w5100/>

MEGACOM. (2018). *Terminal IP con lector de huella digital SF300 ZKTeco*. Obtenido de <http://www.megacom.ni/producto/terminal-ip-con-lector-de-huella-digital-sf300-zkteco/>

Mendez, J. (06 de Septiembre de 2018). *Norma T568A/T568B*. Obtenido de <https://es.slideshare.net/JosMndez42/normas-t568at568b>

- Michelena, J. R. (2016). *Diseño de un sistema de monitoreo de incendios forestales en tiempo real basado en internet de las cosas y plataformas como servicio en la nube (Tesis de maestría)*. Pontificia Universidad Católica del Ecuador, Quito.
- Muñoz, V. (2018). Continúa el avance tecnológico en sistemas de control de acceso. *SEGURIDAD EN AMÉRICA*.
- Orellana, R. (13 de 06 de 2016). *Cableado Estructurado sus Normas y Estándares*. Obtenido de <https://prezi.com/xghsbndk-cff/cableado-estructurado-sus-normas-y-estandares/>
- Padilla, H., & Silva, L. (2017). *Diseño e implementación del Sistema de Cableado Estructurado para las aulas de la zona norte de la ESFOT-EPN(Tesis de Grado)*. Escuela Politécnica Nacional, Quito.
- Reinoso, P. F., & Banda, B. M. (2018). *Desarrollo de módulos didácticos basados en tarjetas Arduino UNO, utilizando Shield Ethernet, wifi y GSM para el laboratorio de microprocesadores de la ESFOT (Tesis de Grado)*. Escuela Politécnica Nacional, Quito.
- Rivas, M. A. (2016). *Implementación de un sistema de control de acceso para mejorar la seguridad de la información de la empresa SNX S.A.C. (Tesis de Grado)*. UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS , Lima.
- SEGO.COM. (06 de 2018). *CATALOGO ZK-4500*. Obtenido de ZKTeco Lector de Proximidad: <http://cdn.sego.com.pe/files/2018/07/18/ZK-4500.pdf>
- Semiconductor Components Industries, L. (Noviembre de 2014). TIP120/D. *TIP120, TIP121, TIP122 (NPN); TIP 125, TIP126, TIP127 (PNP)*. USA/Canada.
- TECNOSEGURO. (2016). *Cableado por un mismo ducto de cable UTP CAT5E y cable 2X1MM*. Obtenido de <https://www.tecnoseguro.com/foro/instalacion-cctv/cableado-por-un-mismo-ducto-de-cable-utp-cat5e-y-cable-2x1mm>
- TIA STANDARD. (02 de 2009). *TIA-568-C.1*. Recuperado el 12 de 2019, de Commercial Building Telecommunications Cabling Standard: <http://innovave.com/wp-content/uploads/2016/01/TIA-568-C.1.pdf>
- TOP SECURITY PERU. (s.f.). *CONTROL DE ASISTENCIA / ZK-4500 – ENROLADOR DE HUELLA DIGITAL VIA USB*. Obtenido de <http://topsecurityperu.com/producto/enrolador-huella-digital-via-usb/>
- URUWIRE. (2014). *Dimensiones norteamericanas para cables y conductores*. Obtenido de Dimensiones angloamericanas: <https://www.uruwire.com/wp-content/uploads/2015/07/Tabla-de-equivalencias-AWG-a-MM2.pdf>
- Web-Robótica. (s.f.). *Como funciona el módulo Arduino Ethernet Shield*. Obtenido de <https://www.web-robotica.com/arduino/como-funciona-el-modulo-arduino-ethernet-shield>

WIKIPEDIA. (19 de 11 de 2019). *Estándar EIA/TIA-568-B*. Obtenido de https://es.wikipedia.org/wiki/TIA-568B#cite_note-1

ZKTECOLATINOAMERICA. (2015). *SF300 Terminal IP con lector de Huella Digital*. Obtenido de <https://www.zktecolatinoamerica.com/documentos/control-de-acceso/standalone/SF300/SF300.pdf>

ZKTECOLATINOAMERICA. (11 de 2016). *Manual de Usuario ZKAccess 3.5*. Obtenido de https://www.zktecolatinoamerica.com/documentos/control-de-acceso/software/ZKAccess%203-5_Manual_de_Usuario.pdf

ZKTECOLATINOAMERICA. (s.f.). *ZKAccess3.5*. Obtenido de Solución en Gestión del Control de Acceso: <http://www.zktecolatinoamerica.com/zkaccess3-5>