ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UN SISTEMA DE AUTOMATIZACIÓN Y ACCESO BIOMÉTRICO EN LAS AULAS 24, 25 Y 26 DE LA ESFOT

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

HORACIO DANIEL ANALUISA FARINANGO
danielh.analuisa@gmail.com

LEONELA FERNANDA GUALANCAÑAY BASANTES
leonela.gualancanay@epn.edu.ec

DIRECTOR: ING. FANNY PAULINA FLORES ESTÉVEZ, MSC.
fanny.flores@epn.edu.ec

CODIRECTOR: ING. MÓNICA VINUEZA RHOR, MSC.
monica.vinueza@epn.edu.ec

QUITO, marzo 2020

DECLARACIÓN

Nosotros, Horacio Daniel Analuisa Farinango y Leonela Fernanda Gualancañay Basantes, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

Horacio Daniel Analuisa Farinango

Leonela Fernanda Gualancañay Basantes

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado en su totalidad por HORACIO DANIEL ANALUISA FARINANGO Y LEONELA FERNANDA GUALANCAÑAY BASANTES, bajo nuestra supervisión.

Ing. Fanny Flores, MSC.	Ing. Mónica Vinueza, MSC.
DIRECTORA DEL PROYECTO	**CODIRECTORA DEL PROYECTO**

DEDICATORIA

A mi familia que durante toda mi vida académica me han apoyado.
A mis mascotas Saskia y Beto, que siempre me esperaban con gran felicidad mi llegada, después de una larga jornada de clases en la semana y una jornada de trabajo los fines de semana.

Horacio Analuisa

Dedico el presente trabajo a mi familia. A mis padres, Guillermo y Janeth, que han sido un pilar fundamental en mi desarrollo profesional.
A mi hermano Josue, el causante de mis sonrisas y mi motivación para seguir adelante.
A Darío, mi cómplice, quien me ha apoyado en todo momento. A todos ellos les dedico este trabajo con cariño y agradecimiento.

Leonela Gualancañay

AGRADECIMIENTO

A la experiencia y lucha en el trabajo de mi adolescencia en el restaurante Pacífico que me han enseñado a perseguir hasta el final por mis objetivos y metas de superación.
A mis profesores del colegio, Jaime Troya e ingenieros de la EPN, Fanny Flores y Mónica Vinueza; que me han enseñado el valor del conocimiento, el aprender no tiene límites y la mejor inversión personal es el estudio.

A mis amigos que han sido parte fundamental en el desarrollo personal y académico, a las experiencias y recuerdos que quedarán enmarcados en las memorias de mi vida universitaria en la EPN.

Horacio Analuisa

Agradezco a los docentes de la Escuela de Formación de Tecnólogos, que con sus conocimientos han aportado en el proceso integral de mi formación profesional; de manera especial, a la Ing. Mónica Vinueza por permitirme cumplir con el desarrollo de este proyecto.

Así mismo, quiero expresar mi más grande y sincero agradecimiento a la Ing. Fanny Flores que con su direccionamiento, conocimiento, y dedicación aportó valiosamente para el desarrollo de este proyecto.

A todas las personas, amigos, conocidos que fueron partícipes de este proceso de una manera desinteresada, gracias infinitas.

Leonela Gualancañay

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto tiene como propósito el estudio, diseño, implementación y pruebas de funcionamiento de un sistema de automatización y acceso biométrico instalado en las aulas 24, 25 y 26 de la Escuela de Formación de Tecnólogos (ESFOT).

El documento comienza detallando las dos problemáticas detectadas en relación a las aulas de la ESFOT y su posible solución, a través del uso de plataformas tecnológicas. Se detalla requerimientos, conceptos y principales características que posee el sistema.

En el segundo ítem, se presenta la metodología y elementos técnicos que se utilizaron para establecer las actividades sistemáticas para la implementación del sistema de automatización y acceso biométrico.

En el tercer ítem, se detallan los resultados y discusiones del sistema, iniciando con el estudio de los requerimientos, posterior su diseño y obtención de materiales, y finalmente la instalación y pruebas de funcionamiento.

En el cuarto, quinto y sexto ítem, se determinan las conclusiones y recomendaciones, fuentes bibliográficas y anexos con documentos como: diagramas, planos y manuales de usuario.

PALABRAS CLAVE: acceso biométrico, automatización.

ABSTRACT

The present project has as its purpose the study, design, implementation, and testing of the functioning of an automation system and biometric access control installed in classrooms 24, 25 and 26 of the Training School for Technologists (ESFOT).

The document begins by detailing the two problems identified in relation to the classroom of the ESFOT and its possible solution, through the use of technology platforms. Detailed requirements, concepts and main characteristics of the system.

In the second item presents the methodology and technical elements that were used to establish the systematic activities for the implementation of the system of automation and biometric access.

In the third item, detailing the findings and discussions of the system, starting with the study of the requirements, the subsequent design and procurement of materials, and finally the installation and operational testing.

In the fourth, fifth and sixth item, determining the conclusions and recommendations, bibliography and annexes with documents such as: diagrams, drawings and user manuals.

KEY WORDS: *biometric access control, automation*.

1. INTRODUCCIÓN

Son los usos sociales los que establecen siempre el alcance y el sentido de la influencia de una nueva tecnología sobre el conjunto de la sociedad, Diego Levis [1].

La diversidad de herramientas tecnológicas de la actualidad permite satisfacer las diferentes necesidades de los colectivos. En el área de la seguridad y la administración, la tecnología brinda eficiencia, confiabilidad, alta disponibilidad y escalabilidad. Particularidades clave de un sistema de acceso y automatización, que permiten incorporar herramientas de hardware y *software* con el fin de modernizar, monitorear y optimizar el uso y acceso a las instalaciones y recursos en una institución, empresa o domicilio [2].

El acceso a las aulas de la ESFOT no cuenta con ningún tipo de seguridad o de control; en consecuencia, las personas que no pertenecen a la comunidad educativa hacen uso inadecuado de estos espacios, como, por ejemplo, actos vandálicos e impetuosos. Por otro lado, los profesores para impartir sus clases deben solicitar a la persona encargada abrir las aulas, para poder acceder a ellas, lo que genera impuntualidad en las clases.

Un sistema de acceso y automatización en una institución educativa aporta importantes funcionalidades, entre ellas: la administración óptima de recursos e infraestructura, tener un control de acceso y autentificación del personal académico y administrativo, una mejor organización en la programación de horarios y la asignación de clases, el monitoreo en tiempo real del estado de las puertas, ventanas y luminarias, controlar la apertura de salones de clase, así como el encendido y apagado de luces, desde un servidor central, y por último, mostrar los datos generados por el sistema en una interfaz gráfica amigable con el usuario y de fácil acceso [3].

Por estas razones, la implementación de un sistema de acceso biométrico y automatización fue necesaria para solventar la problemática detectada, ya que haciendo uso de los recursos tecnológicos se mejoró y optimizó los procesos administrativos y de seguridad de la infraestructura física de la ESFOT.

1.1. Marco teórico

- **Sistema de control de acceso**

Un sistema de control de acceso es un mecanismo que, mediante autentificación, comprobación, autorización y registro de algún tipo de información, permite acceder a recursos o datos de una empresa, institución o departamento asignado. Tiene por objetivo impedir el libre acceso del público, mediante el uso de un tipo de información en específico como: huellas dactilares, números de serie, tarjetas, contraseñas, o sensores, protegiendo así los activos de diversas áreas [4].

En la Tabla 1.1, se puede visualizar los componentes o partes que tiene un sistema de control de acceso.

Tabla 1.1 Componentes de un sistema de control de acceso [4].

Elemento	Función
Controlador	Es el elemento concentrador de la información y toma decisiones para generar una acción; además, se encarga de comunicar a todos los elementos del sistema.
Dispositivos de identificación	Son los elementos que interactúan e identifican al objeto o persona; en el mercado existen varios dispositivos con características diferentes conocidos como biométricos
Dispositivos de entrada	Son los encargados de comunicar al controlador la información acerca de un estado de un elemento del sistema; pueden ser: sensores, pulsadores, entre otros.
Dispositivos de salida	Son los encargados de realizar la acción que se tomó previamente desde el controlador como: cerraduras, timbres, alarmas, etc.
Red de comunicaciones	Es la red que utiliza el sistema para comunicarse como: red cableada Ethernet, red Wifi, red WAN o redes de IoT.

- **Sistemas biométricos**

Los sistemas biométricos están constituidos por elementos de hardware como sensores, que son utilizados para reconocer una determinada condición del exterior (estado de apertura de puertas, ventanas, etc.); además se integran por *software*, que es el encargado de determinar a través de acondicionamientos la información obtenida [5]. Los principales tipos de biométricos existentes son:

- Reconocimiento de la huella dactilar.

- Reconocimiento del rostro.
- Reconocimiento de iris/retina.
- Geometría de dedos/mano.
- Autentificación de la voz.
- Reconocimiento de la firma [5].

➢ **Equipo biométrico ZKTeco SF-300**

El equipo biométrico ZKTeco SF-300, es un terminal de reconocimiento de huella dactilar que funciona de manera independiente o como esclavo de un sistema central en red. Utiliza diferentes tipos de comunicación como: IP, USB y RS485 [6]. En la Figura 1.1, se puede visualizar el biométrico y sus componentes.

Figura 1.1 Equipo ZKTeco SF-300 y sus componentes [6].

En la Tabla 1.2, se especifica las características del equipo biométrico.

Tabla 1.2 Características de equipo biométrico ZKTeco SF-300 [6].

Funciones	**Control de Acceso**
Capacidad:	1500 Huellas 80000 Eventos
Comunicación:	TCP/IP RS485 USB.
Hardware:	Sensor de Huella Óptico Anti-Rayaduras. Botón de Salida / Timbre / Sensor de Puerta. Salida de Alarma Pantalla táctil de 2.8 pulgadas.
Conexiones:	Salidas NC (*Normally Close*) / NO (*Normally Open*) / COM (*Common*) (12V, 3A). Botón de Salida / Timbre / Sensor de Puerta. Salida de Alarma.
Alimentación:	12VCD / 3A
***Software*:**	ZKAccess 3.5

- **Sistema de control de acceso ZKAccess 3.5**

Los sistemas de control de acceso de la marca ZKTeco, ofrecen una amplia variedad de productos y soluciones biométricas de huella dactilar y rostro; una de las más efectivas en el mercado, ya que cuentan con un *software* propietario de controlador o administrador eficiente y con muy buenas prestaciones para el usuario, aparte de que posee su propio algoritmo biométrico. La información generada por los dispositivos biométricos responde a un sistema central, que cuenta con su propia base de datos de los usuarios registrados, para la autentificación, comprobación y autorización. Además, de tener distintas funcionalidades como: crear grupos, configurar comunicación, sistema de *logs*, reportes y sincronización automática, entre otras características que posee la marca. [7]. En la Figura 1.2, se puede observar la interfaz del *software* de administración de los sistemas biométricos de la marca ZKAccess 3.5.

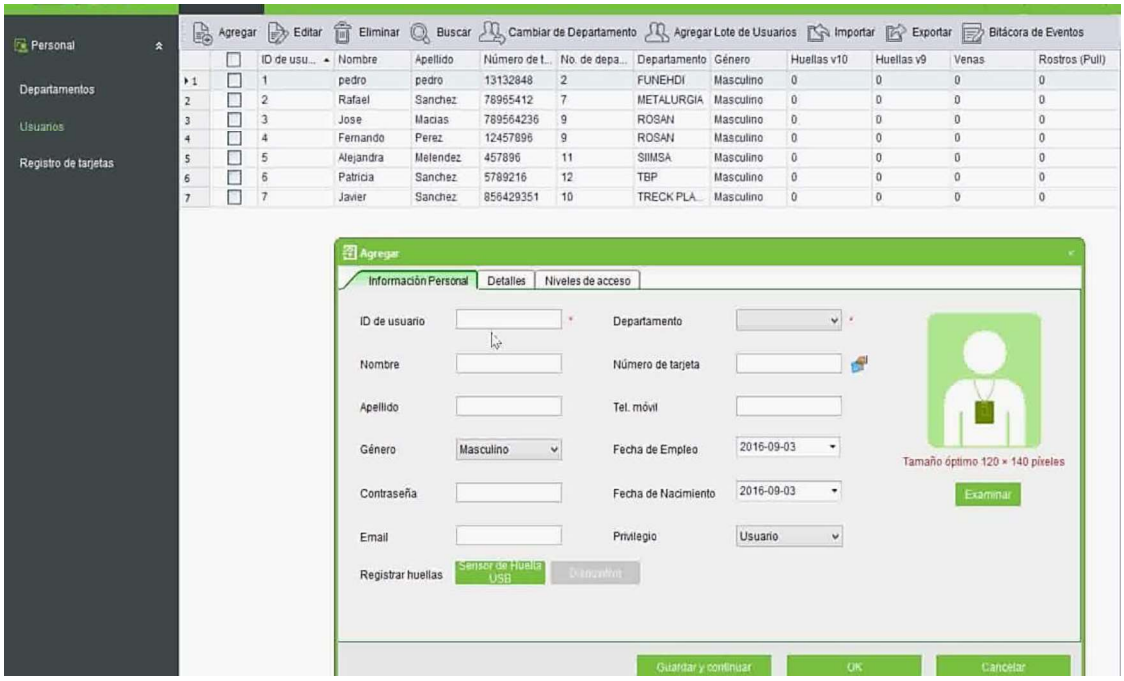


Figura 1.2 *Software* de administración del biométrico ZKAccess 3.5. [7].

Las funcionalidades que aporta el *software* son:

- Se encarga de la administración simultánea entre los equipos biométricos ubicados en cada aula.
- Gestiona simultáneamente el control de acceso de los usuarios en sus horarios respectivamente.
- Supervisión de eventos en tiempo real con ícono de estado de puerta (abierta o cerrado).
- Apertura y cierre de puertas de forma remota.

- Genera informes básicos de asistencia de los usuarios.

➢ **Enrolador de huellas**

El electro biométrico ZKTeco que se puede visualizar en la Figura 1.3, tiene la funcionalidad de registrar las huellas mediante la captura de imágenes de los usuarios y almacenarlos en la base de datos del *software* de administración ZKAccess 3.5, mediante interfaz USB [8]. A continuación, se identifica las características técnicas y funcionalidades relevantes del equipo:

- Sensor de lectura de huella de alto desempeño.
- Fácilmente accesible para cualquier dedo.
- Versátil y seguro.
- Fácil instalación y operación.
- LED indicador del estado del dispositivo.
- Drivers incluidos.

Figura 1.3 Lector biométrico de huella por USB ZKTeco ZK4500 *[8]*.

En la Tabla 1.3, se resumen las características técnicas relevantes del equipo.

Tabla 1.3 Características del lector biométrico ZK4500 [8].

CPU	120MHz
Algoritmo huella dactilar	Óptico
Resolución	500 DPI / 256 gris
Área del sensor	15x18 mm
Tamaño de imagen	280x360 pixel
Color	Negro
Interfaz	USB
Dimensiones	65.5x49x79.8 mm

- **Sistema de desarrollo Arduino**

Arduino es una plataforma de desarrollo basada en una placa electrónica de hardware libre que incorpora un microcontrolador re-programable y una serie de pines hembra, los cuales permiten establecer conexiones entre el microcontrolador y los diferentes sensores y actuadores de una manera muy sencilla [9]. En la Figura 1.4, se puede observar un Arduino Mega, es la placa más representativa de esta plataforma, y su logo.

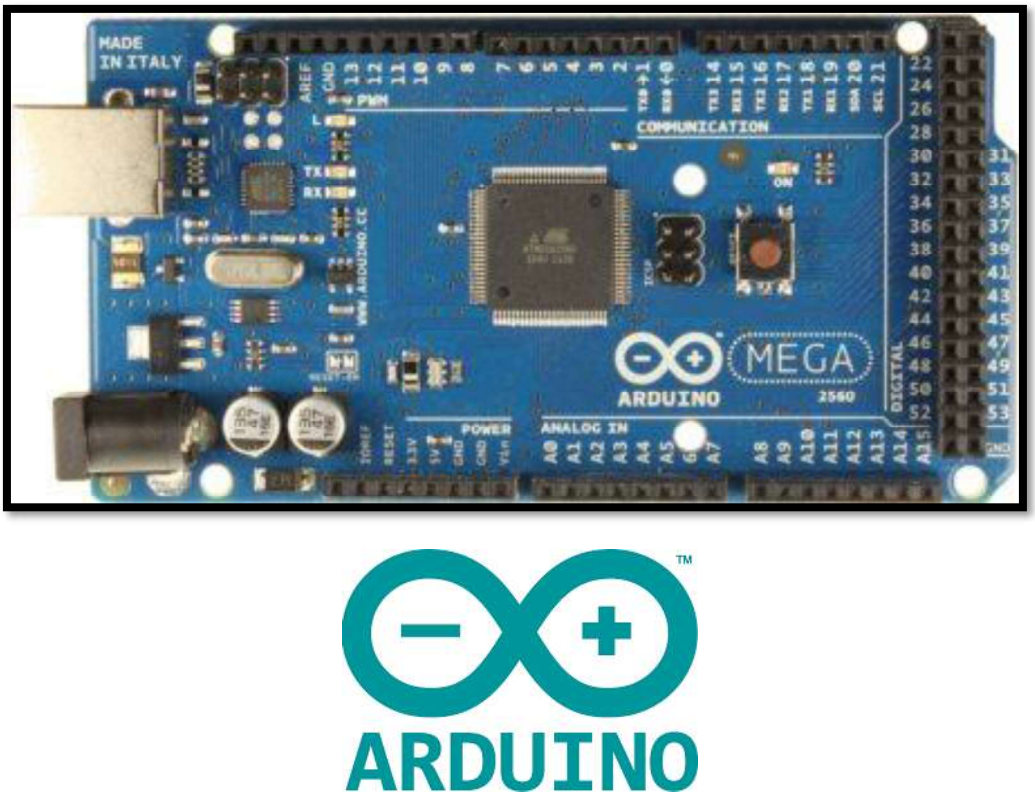


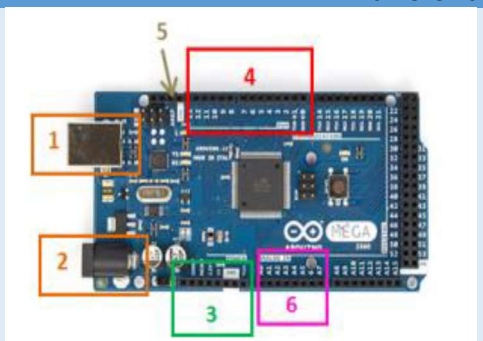
Figura 1.4 Placa Arduino Mega y logotipo [9].

- **Arduino Mega 2560**

El Arduino Mega es la placa más potente de esta familia. Tiene varios componentes como: un microcontrolador ATMEGA 2560 de 16 MHz y 8 bits, una memoria *FLASH* de 256K, rango de voltaje de 7 a 12 V, 54 pines entre ellos: 14 PWM (*Pulse Width Modulation*), 16 analógicas, 4 seriales [10].

En la Tabla 1.4 se puede visualizar la función de cada una de las partes, que posee la placa de Arduino Mega.

Tabla 1.4 Partes de un Arduino Mega [11].

No	Parte	Funcionalidad
		
1	**Conector USB tipo B**	Entrada de alimentación y transferencia de datos para cargar programas a la placa desde la IDE.
2	**Adaptador externo**	Entrada de alimentación de fuente externa de 7 a 12 Voltios
3	**Pines de alimentación**	VIN: fuente de tensión de entrada que hace puente con la alimentación externa 5V: fuente regulada de 5 voltios 3.3.V: fuente regulada de 3.3 voltios GND: puesta a tierra de todo el sistema
4	**Entradas/salidas digitales**	PIN 0 (RX): recibir datos seriales PIN 1 (TX): transmitir datos seriales PIN 2 y 3: interrupciones PIN 4-11: PWM PIN 10-13: comunicación SPI PIN 13: alto o bajo valor
5	**Referencia analógica**	Pin de referencia analógica de señal externa
6	**Entradas analógicas**	16 Pines de entrada de señales analógicas por fuentes externas

En el **Anexo 1** se puede visualizar un diagrama completo de la placa del Arduino Mega 2560.

- **Arduino *Ethernet Shield***

Este módulo ofrece la función de conectar el sistema Arduino a una red *Ethernet*, implementando los protocolos TCP/IP.

Está basada en el chip *Ethernet* Wiznet W5100, que provee de una pila de red IP capaz de soportar TCP y UDP. Soporta hasta cuatro conexiones de *sockets* simultáneas, tiene un conector RJ45, tiene conectores disponibles para enlazarse a otras placas, por ejemplo: a una placa Arduino Mega. Posee un botón de *RESET* que podrá reiniciar tanto al *Shield* y la otra placa Arduino montada, usa la librería *Ethernet* para leer y escribir los flujos de datos que pasan por el puerto *Ethernet* [12]. En la Figura 1.5 se puede visualizar un *Shield Ethernet*

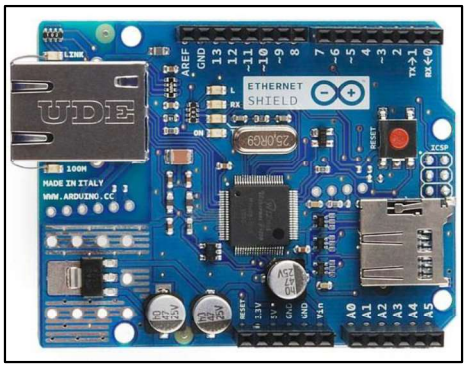
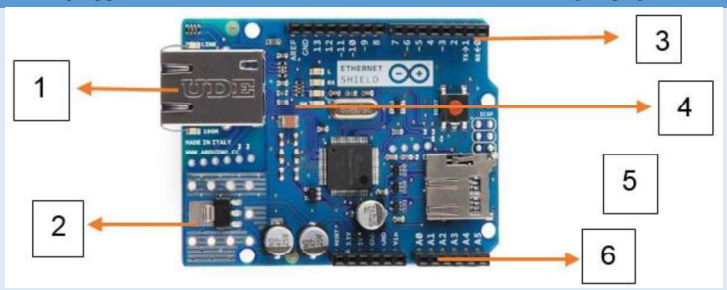


Figura 1.5 Placa *Shield Ethernet* [12].

En la Tabla 1.5 se puede visualizar la función de cada una de las partes, que posee una *Shield Ethernet*.

Tabla 1.5 Partes de una placa *Shield Ethernet* [13].

No	Parte	Función
		
1	**Conector Ethernet**	Conector RJ45 para comunicación *Ethernet*
2	**Botón RESET**	Reiniciar la placa o placas montadas
3	**Entradas salidas digitales**	PIN 0 (RX): recibir datos seriales PIN 1 (TX): transmitir datos seriales PIN 2 y 3: interrupciones PIN 4-11: PWM PIN 10-13: comunicación SPI PIN 13: alto o bajo valor
4	**LEDs Indicadores**	ON: indica que la placa y la *shield* están alimentadas LINK: indica la presencia de un enlace de red y parpadea cuando la *shield* envía o recibe datos 100M: indica la presencia de una conexión de red de 100 Mb/s (de forma opuesta a una de 10Mb/s) RX: parpadea cuando el *shield* recibe datos TX: parpadea cuando el *shield* envía datos
5	**Puerto SD**	Se puede ingresar tarjetas SD
6	**Pines alimentación y entradas analógicas**	VIN: fuente de tensión de entrada que hace puente con la alimentación externa 5V: fuente regulada de 5 voltios 3.3.V: fuente regulada de 3.3 voltios GND: puesta a tierra de todo el sistema Pines para entradas analógicas externas

- **Sistema de Cableado Estructurado**

Un Sistema de Cableado Estructurado (SCE) es una infraestructura conformada por varios elementos para la comunicación entre varios dispositivos o herramientas de información de voz, datos y video. Está definida por estándares internacionales para su diseño, construcción y administración; provistas por las organizaciones de ANSI (*American National Standards Institute*), TIA (*Telecommunications Industry Association*) y EIA (*Electronic Industries Alliance*) [14].

- **Conceptos básicos**

- *Switch:* conmutador de interconexión lógica que opera en la capa de enlace de datos del modelo OSI.
- *Router:* enrutador que administra el tráfico o paquetes de información, opera en la capa de red del modelo OSI.
- *Patch panel:* organizador para cables de comunicación.
- Cable UTP: cable de cobre conocido como par trenzado, se tienen varios tipos de acuerdo a sus características físicas o lógicas, proporciona la conexión entre dos dispositivos de red.
- *Patch cord:* cable (UTP o fibra) que conecta la estación de trabajo con el punto de red.
- *Rack:* estructura metálica donde se agrupan los componentes de comunicación, alimentación y electrónico.
- Canaletas: estructura plástica o metálica que protege al cable de datos en interiores o exteriores.
- Regulador de voltaje: equipo protector, mantiene niveles de tensión eléctrica constantes.

- **Características de un SCE**

Las principales características que debe poseer una infraestructura de cableado estructurado son:

- Escalable: capacidad de ampliar su estructura.
- Flexible: capacidad de adaptarse a nuevas tecnologías.
- Eficiente: óptimo físicamente y económicamente.
- Longevidad: capacidad de soportar y funcionar durante un largo tiempo.
- Independiente: capacidad de implementar su infraestructura con varios fabricantes o proveedores.

- Adaptativo: capacidad de integrar varios servicios.

➢ Normas o estándares de un SCE

En la Tabla 1.6 , se puede visualizar un resumen de las normas utilizadas en la ejecución del presente proyecto, referente al cableado estructurado.

Tabla 1.6 Normas de Sistema de Cableado Estructurado [15].

Estándar	Nombre	Características
ANSI/TIA/EIA-568-B	Norma de cableado para edificios comerciales	Define requisitos de diseño, componentes, distancias, topología y configuraciones de tomas y conectores. Define las áreas que son: área de trabajo, cableado horizontal, cableado vertical, cuarto de telecomunicaciones y sala de equipos.
TIA/EIA 568-B1	Requerimientos generales	- Cableado Horizontal: topología tipo estrella, máximo 100 mts hasta el área de trabajo, 4 pares UTP de 100 ohmios. - Área de trabajo: cable UTP 100 ohmios, 4 pares terminado en un conector modular de 8 posiciones.
TIA/EIA 568-B2	Requerimientos de cableado con par trenzado	- Cable de 4 pares sólidos de 22AWG a 24 AWG con una cubierta aislante termoplástica. - Identificados en las categorías 3, 5e y 6. - Resistencia: <=9,38 ohms/100 mts. - Capacitancia: <= 6,6 nF / 100mts cat 5e. - Frecuencia de trabajo: 100 Mhz. - Curvatura máxima 4 veces el diámetro en UTP. - Patch Cords: deben seguir los estándares del diámetro de aislamiento y código de colores. - El aislamiento de un cable de conexión terminado con un enchufe modular no excederá de 1.22 mm. - El código de color se basará en las normas T568-B y T568-A.
EIA/TIA T568-B	Norma americana que presenta el esquema de colores para el ponchado del par trenzado. Ver **Anexo 2**	

- **Red de área local**

La red de área local (LAN) es un sistema de comunicación de área limitada; es decir, abarca un solo sistema autónomo, como, por ejemplo: un edificio, una institución

educativa o una residencia. Tiene como funcionalidad conectar, a través de varios mecanismos como: enlaces de radio o cableado de datos, varios dispositivos de red, servicios y repositorios de información.

Los componentes de una LAN varían de acuerdo a las funcionalidades que le asignen, como: computadores, impresoras, dispositivos de acceso, servidores, equipos de almacenamiento, sensores, microprocesadores, entre otros. Además de acceder a servicios como: Internet, correo, telefonía, *software* e información [16].

- **Topología física y lógica**

La topología es el tipo de esquema de interconexión para la comunicación entre los diferentes dispositivos de red, ya sea una LAN (*Local Area Network*) o una WAN (*Wide Area Network*).

La topología física hace referencia al tipo de conexión que tienen los equipos de infraestructura como: *routers*, *switches* de capa dos o tres, puntos de acceso inalámbrico, servidores, *firewalls*, *proxys* entre otros.

La topología lógica hace referencia a la forma que el tráfico de datos se transmite de un nodo a otro, o, dicho de otra forma, de un dispositivo de red a otro [17].

- **Direccionamiento IPv4**

Las redes que funcionan con el protocolo de comunicación TCP/IP, los equipos o dispositivos de red necesitan dos características fundamentales que son: el direccionamiento IP y la máscara de subred.

El direccionamiento IP, está basado en 4 bytes es decir 32 bits, se encuentran separados en 4 grupos de hasta el número 255 en decimal [18].

El direccionamiento IP se clasifica de acuerdo al tamaño del *pool* de direcciones. En la Tabla 1.7, se puede observar cómo está conformada la clasificación de direcciones IP.

Tabla 1.7 Clases y rangos de direcciones IP [19].

Clase IP	Id. clase	No. Bits para red	No. bits para nodos	Rango	Primer octeto	No. De redes posibles	No. De estaciones posibles	Máscara de subred por defecto
A	0	7	24	1.0.0.0 a 127.255.255.255	de 0 a 127	2^7 = 128	(2^24)-2= 16.777-216-2= 16.777.214	255.0.0.0
B	10	14	16	128.0.0.0 a 191.255.255.255	de 128 a 191	16.384	65.534	255.255.0.0
C	110	21	8	192.0.0.0 a 223.255.255.255	de 192 a 223	2.097.152	254	255.255.255.0
D	1110	28	X	223.0.0.0 a 239.255.255.255	de 224 a 239	X	X	
E	11110	27	X	240.0.0.0 a 247.255.255.255	de 240 a 255	X	X	
	Red		**Nodo**					

El direccionamiento privado, específicamente en redes LAN de empresas, organizaciones e instituciones, se clasifica de acuerdo a la clase y la extensión de IPs utilizables, las cuales se pueden configurar en los equipos de red o realizar subredes [19]. Los rangos de IPs, según la clase, son los siguientes:

- Clase A: 10.0.0.0 a 10.255.255.255
- Clase B: 172.16.0.0 a 172.31.255.255
- Clase C: 192.168.0.0 a 192.169.255.255

➢ Vlan

Una red de área local virtual es un conjunto de dispositivos interconectados en un mismo segmento lógico de la red, independientemente de la parte física. Se pueden agrupar de acuerdo a las necesidades de la empresa, organización o institución; por ejemplo, departamento laboral, área de aplicación o servicio, tipo de cliente en un ISP, tipo de dispositivo, cargo de un trabajador, entre otras [20].

Algunas de las ventajas de realizar Vlans dentro de una red son: optimizar el ancho de banda, seguridad, balance de tráfico de datos, organización, disminución de fallas lógicas o físicas en la red por la división del dominio de *broadcast* [21].

En la Tabla 1.8, se puede visualizar la clasificación del número o ID de Vlans y sus excepciones.

Tabla 1.8 Rango de ID de Vlans [22].

Tipo	Rango	Función
Normal	ID: entre 1 a 1005	Identificadores convencionales
Token Ring y FFDI	ID: de 1002 a 1005	Vlans asignadas para otros tipos de arquitectura de red
Vlan nativa	ID: 1	Vlan por defecto para todas las interfaces de red
Extendido	ID: 1006 a 4096	Vlans dedicadas para ampliar clientes o infraestructura en los proveedores de servicios

- **Sensores**

Es un dispositivo cuya funcionalidad es detectar cualquier estímulo o acción externa y responder simultáneamente o enviar la información a un sistema central; dicho en otras palabras, capta información de una señal o magnitud física o química y la transforma en una señal eléctrica con el fin de que un microprocesador o computadora procesen los datos obtenidos [23].

Las principales características que poseen los sensores son las siguientes [24] :

- Linealidad: nivel de exactitud de la medición en función de un valor de referencia.
- Precisión: diferencia entre valor medido y real.
- Rango de medición: mínimos y máximos que se puede aplicar.
- Sensibilidad: mínimo valor que puede medir.
- Desviación de cero: valor de salida cuando la medida es nula.
- Confiabilidad: tiempo de vida.
- Tolerancia: nivel de error que no afecta a la medida.

➢ **Sensor magnético MC-38**

El sensor magnético normalmente cerrado tiene un imán y un interruptor; generalmente se utiliza para alarmas en puertas, ventanas y luminarias. Funciona como un circuito cerrado mientras las dos partes estén juntas, a través de un campo magnético; caso contrario el campo magnético se disuelve y se abre el circuito. Gracias a ese cambio de estado es posible detectar la apertura de la puerta o ventana. En la Figura 1.6 se puede visualizar el sensor MC-38.

Figura 1.6 Sensor magnético MC-38 [25].

El sensor es recubierto de plástico, lo que lo hace extremadamente resistente, tanto en exterior como en interior. La conexión con la placa de Arduino se realiza mediante dos cables que vienen incluidos en el sensor. La instalación en la puerta o ventana se realiza mediante la cinta autoadhesiva que viene incluida o con tornillos [25].

En la Tabla 1.9 se puede visualizar las especificaciones técnicas del sensor

Tabla 1.9 Especificaciones técnicas sensor MC-38 [25].

Modelo	MC38
Corriente máx.	0.5A
Voltaje máx.	100V
Distancia de activación	15-25mm
Dimensiones	34 × 41 × 6.5 mm

- **Servidor**

Un servidor es una máquina o computadora que provee de un servicio o recursos a los dispositivos de red y al usuario, conocidos como clientes.
Algunos de los conceptos más utilizados en el área de servicios de una red son [26]:

- *Proxy*: equipo o programa de seguridad, intermedio entre el cliente y el servidor, bloquea peticiones.
- DNS: (*Domain Name System)* asocia un *host* o servicio a un nombre de dominio.
- *WEB*: son recursos dentro del Internet.
- FTP: (*File Transfer Protocol)* protocolo para la trasferencia de archivos entre cliente y servidor.
- DHCP: (*Dynamic Host Configuration Protocol)* protocolo para asignación dinámica de direcciones IP

Los servicios que pueden albergar un servidor son variados de acuerdo con las necesidades del cliente, en la Tabla 1.10, se puede visualizar los servidores más comunes y utilizados.

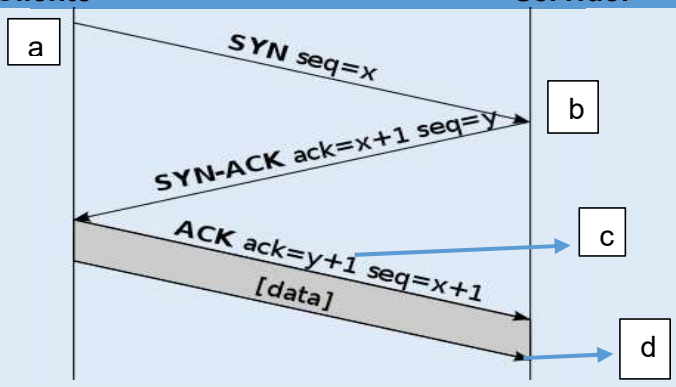
Tabla 1.10 Tipos de servidores [27].

Tipo	Función
Servidor de Correo	Almacena, envía, recibe correos electrónicos.
Servidor *Proxy*	Bloquea peticiones no autorizadas del cliente al servicio.
Servidor *Web*	Almacena y presenta documentos o información en HTML, en un navegador WEB.
Servidor de Base de Datos	Almacena y gestiona grandes cantidades de datos
Servidor dedicado	Servicio específico para un cliente o grupo de clientes.
Servidor DNS	Administra los nombres de dominio.

- **Sistema Cliente-Servidor Arduino**

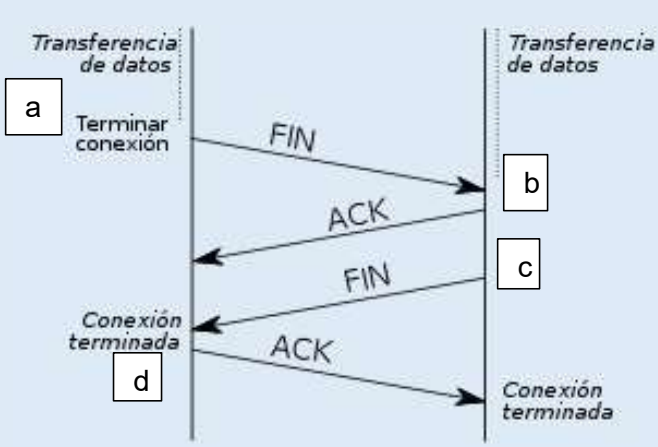
Un sistema cliente-servidor en redes TCP/IP, especialmente empleado en la plataforma Arduino, es un proceso de comunicación simultánea en red entre la placa y un centro de administración (servidor) para la obtención de algún recurso o servicio. El proceso se lo realiza gracias a la librería *Ethernet* desarrollada en la plataforma de Arduino y con el protocolo *web* HTTP, que tiene comunicación a través de los puertos 80 u 8080.
El proceso para inicializar una correcta comunicación establece tres pasos sistemáticos con números de secuencia que deben seguir tanto el cliente o placa de Arduino como el servidor, en la Tabla 1.11, se puede visualizar dichos pasos [28].

Tabla 1.11 Proceso de conexión cliente-servidor [29].

Cliente	Servidor
	
a. Abre un puerto y envía un paquete SYN (Sincronización).	b. Verifica el servicio y si el puerto asociado se encuentra disponible para aceptar SYN c. Envía la aceptación con un paquete SYN/ACK (Aceptación).
d. El cliente finalmente envía un paquete de confirmación ACK.	
e. Se estableció la comunicación correctamente.	

La finalización de la comunicación se realiza en 4 pasos sistemáticos que cierra el camino de envío de datos entre el usuario o placa Arduino con el servidor o centro de administración, en la Tabla 1.12, se puede visualizar el proceso.

Tabla 1.12 Proceso de finalizar conexión entre cliente-servidor [29].



a. Envía un paquete de FIN, para pedir finalizar la conexión.

b. Envía un paquete ACK de confirmación de haber recibido la petición de finalización.

c. Envía un paquete FIN para finalizar la conexión.

d. Envía un paquete ACK de confirmación de haber recibido la petición de finalización

- **Protección eléctrica**

Los equipos electrónicos y eléctricos de un sistema de automatización o de comunicación que se conecten a la línea de alimentación, deben ser protegidos contra picos de voltaje o de corriente; que son consecuencias generadas por varios factores, entre ellos: estática, efectos resonantes, cortos circuitos, *switcheo* y descargas atmosféricas.

La protección de equipos se puede realizar con varias herramientas como: reguladores de voltaje, apartarrayos, conexiones a tierra o placas diseñadas de protección. El dimensionamiento de dichos dispositivos depende de la carga de voltaje o potencia que maneja el sistema o el equipo a proteger [30].

2. METODOLOGÍA

El desarrollo del proyecto se basó en la investigación aplicada, para esta metodología su objetivo es brindar respuestas a un problema concreto, sea al sector educativo, social o productivo; a través de la búsqueda y consolidación del conocimiento y su aplicación [31]. Un sistema de automatización aporta en la optimización del uso de recursos e infraestructura para la comunidad de la ESFOT, ya que permite tener un control de acceso para el personal docente y administrativo, evitando así el acceso de terceros a estos espacios. La finalidad del proyecto es también despertar interés en desarrollar propuestas que permitan aplicar los conocimientos obtenidos en las aulas en soluciones enfocadas a necesidades concretas donde los beneficiados son los miembros de la comunidad educativa.

La implementación del sistema de automatización partió de la detección de la problemática que se presentó en relación a la seguridad y administración de los recursos de estudio de las aulas de la ESFOT. Para la investigación e implementación del sistema de automatización y acceso biométrico se procedió de la siguiente manera: con el previo estudio de la infraestructura civil, del cableado estructurado y de red, se determinaron los recursos y herramientas necesarias para la implementación como: equipos de red, insumos electrónicos y de cableado, tipo de sistema, red lógica y física, equipo biométrico y proveedores que cumplan con los requisitos de funcionamiento, desempeño y fiabilidad.

Además, se investigó, recopiló y estudió la información acerca de los instrumentos de *hardware* y *software* que se utilizó tanto para el sistema de acceso biométrico como: programa de administración, comunicación IP, instalación, mantenimiento y configuración. De la misma forma, para el sistema de automatización como: Arduino Mega, librerías, programación, comunicación, sensores, alimentación e instalación.

Una vez diseñado el sistema de automatización y control de acceso basado en características como escalabilidad, disponibilidad, operatividad, entre otras, se adquirió los elementos cotizados. Luego, se realizó la instalación de la infraestructura de la red para la cual se tuvo reuniones con el encargado de la DGIP (Dirección de Gestión de la Información y Procesos) ya que se debía solicitar habilitación de puertos y acceso a *switches* de la EPN.

Con la finalización de la conexión de todos los elementos y la respectiva configuración en cada dispositivo se hicieron pruebas de funcionamiento, se recogió y analizó los datos correspondientes, así como las respectivas correcciones para que el sistema quede totalmente operativo. Adicional a esto se creó un manual de usuario para facilitar su administración y mantenimiento.

3. RESULTADOS Y DISCUSIÓN

3.1. Análisis de requerimientos del sistema

- **Análisis de la infraestructura de red**

La administración de la infraestructura de red de la ESFOT se encuentra a cargo de la DGIP. La DGIP es la dirección encargada de la administración de los recursos y servicios TIC (Tecnologías de la Información y la Comunicación) y de la gestión de la calidad de los procesos en la EPN [32].

- **Red LAN ESFOT**

Actualmente, la DGIP maneja la red de datos de la ESFOT, conmutada a través de *switches* marca Cisco, ubicados en diferentes puntos del área de tecnólogos; estos *switches* tienen la disponibilidad de puertos o interfaces libres para conectarse a la red LAN de la EPN. En el **Anexo 3**, se puede visualizar la ubicación y disponibilidad de equipos de la DGIP en la ESFOT, los cuales fueron utilizados para establecer la comunicación del sistema de automatización y acceso biométrico de las aulas 24, 25 y 26, correspondientes a este proyecto.

- **Análisis de la infraestructura civil**

Se determinó la cantidad de los distintos elementos como: puertas, ventanas y luminarias que forman parte de las aulas de la ESFOT, con el fin de dimensionar su integración en el diseño, así como para la instalación de los respectivos dispositivos que son parte del sistema de automatización y acceso biométrico. En la Tabla 3.1, se muestra los elementos que forman parte de las aulas 24, 25 y 26 de la ESFOT.

Tabla 3.1 Detalle de los elementos físicos de las aulas 24, 25 y 26 de la ESFOT

AULAS	PUERTAS	VENTANAS	LUMINARIAS
Aula 24	1	2	5
Aula 25	1	2	5
Aula 26	1	2	5

- **Análisis de requerimientos del acceso biométrico**

La asignación de aulas y horarios lo realiza el área administrativa de la comunidad de tecnólogos; sin embargo, al tener que tomar en cuenta varios factores como profesores, estudiantes y asignaturas asignadas respectivamente se vuelve una tarea dispendiosa y demorada. Para optimizar este proceso se requiere un sistema biométrico que, mediante el registro de la huella dactilar del profesor o personal administrativo que valide la información en la base de datos de un servidor central, a través de la comunicación por *Ethernet*, como resultado, permita el ingreso a un aula en un horario específico, previniendo así que terceros hagan uso indebido de estos espacios. Para ello, se utiliza el biométrico de marca ZKTeco SF-300 y el *software* de administración, instalado en el servidor, ZKAccess 3.5. El ingreso de los usuarios y horarios al equipo biométrico es en base a la información obtenida (horarios) con colaboración del área administrativa de la ESFOT.

- **Análisis de requerimientos del sistema de automatización**

  - **Microcontrolador**

El sistema de automatización para las aulas 24, 25 y 26, requiere su funcionamiento basado en un microcontrolador que cuente con las siguientes características:

- Escalabilidad.
- Tolerancia a fallas.
- Adaptabilidad.
- Procesamiento.
- Gran cantidad de entradas, salidas y memoria.
- Manejo de señales digitales y analógicas.
- Comunicación TCP/IP.
- Capacidad de conexión con un servidor WEB.

Por ello, se establece al Arduino Mega 2560 como el procesador del sistema, ver **Anexo 1**.

- **Monitoreo en tiempo real**

El sistema de automatización tiene como funcionalidad monitorear el estado de abierto o cerrado de ventanas y puertas; para esto, se establece la utilización del sensor MC-38 de contacto magnético normalmente cerrado. Adicional, para el control de la puerta de cada aula, se utiliza una placa de protección que se encarga de acondicionar las señales de abrir, tanto desde el Arduino como desde el equipo biométrico. Para el monitoreo y control de las luminarias de las aulas, se utilizan elementos electromecánicos como relés. Las conexiones y configuraciones fueron diseñadas, ejecutadas y comprobadas por los estudiantes de Electromecánica, que formaron parte del proyecto de automatización y control.

3.2. Diseño del sistema

- **Esquema general del sistema**

En la Figura 3.1, se puede observar el esquema general del sistema de automatización y acceso biométrico.

- **Diseño de la red de datos**

La red de datos para la comunicación entre el servidor, ubicado en la dirección de la ESFOT, con el sistema de Arduino y los equipos biométricos, se establece como un segmento extendido de capa dos en la LAN de la EPN.

- **Red física y lógica**

La red física y lógica de comunicación en el sistema de automatización y acceso biométrico, se establece como una red jerárquica tipo estrella, ya que se añade un *switch* de acceso para el módulo Arduino y los equipos biométricos de las aulas 24, 25 y 26, a fin de que se conecten y conmuten con los equipos de red de distribución y *core* de la DGIP, pertenecientes a la LAN de la EPN, y al servidor ubicado en la dirección de la ESFOT. Ver **Anexo 4**. En la Figura 3.2, se puede observar el esquema de red del sistema.

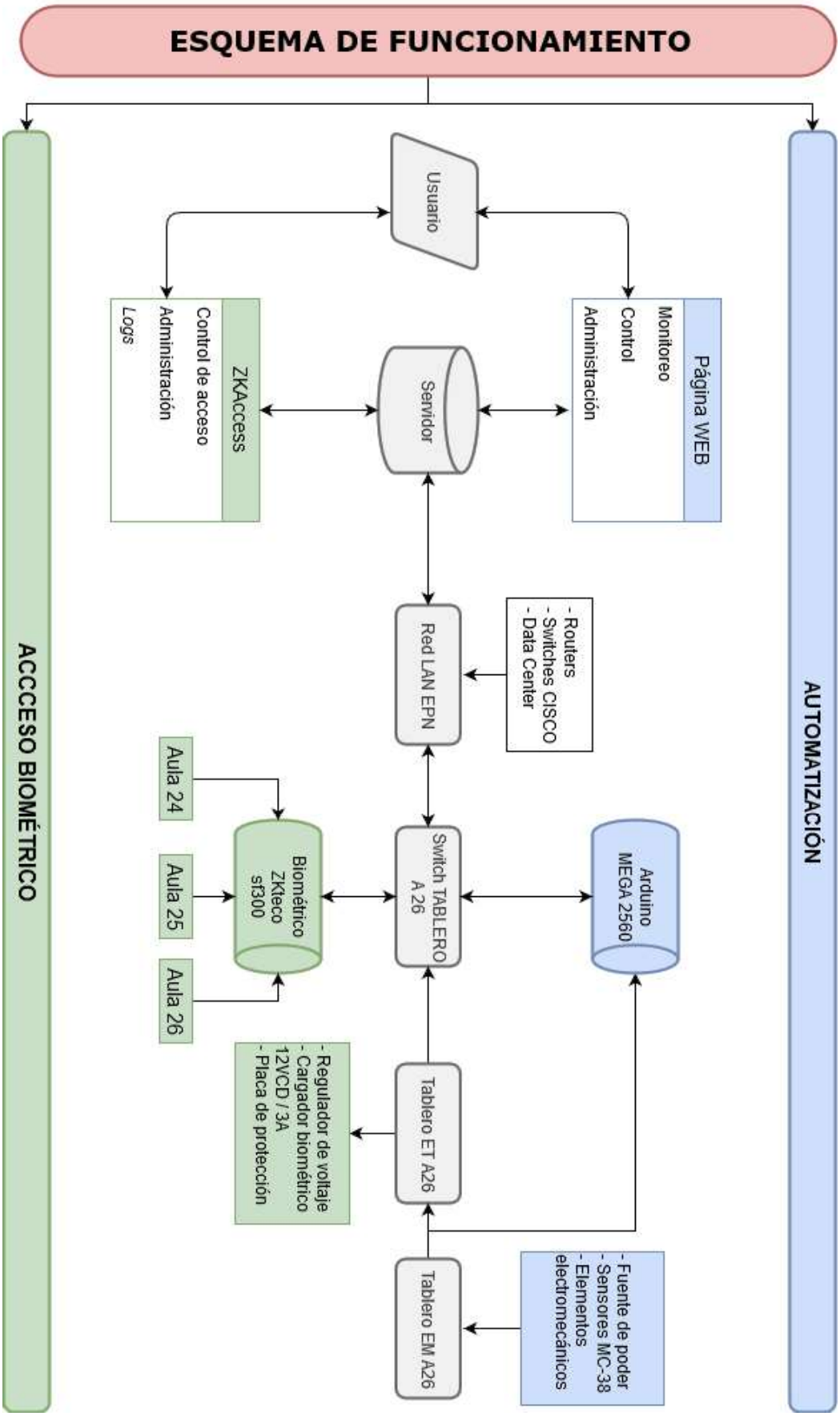


Figura 3.1 Esquema general del sistema

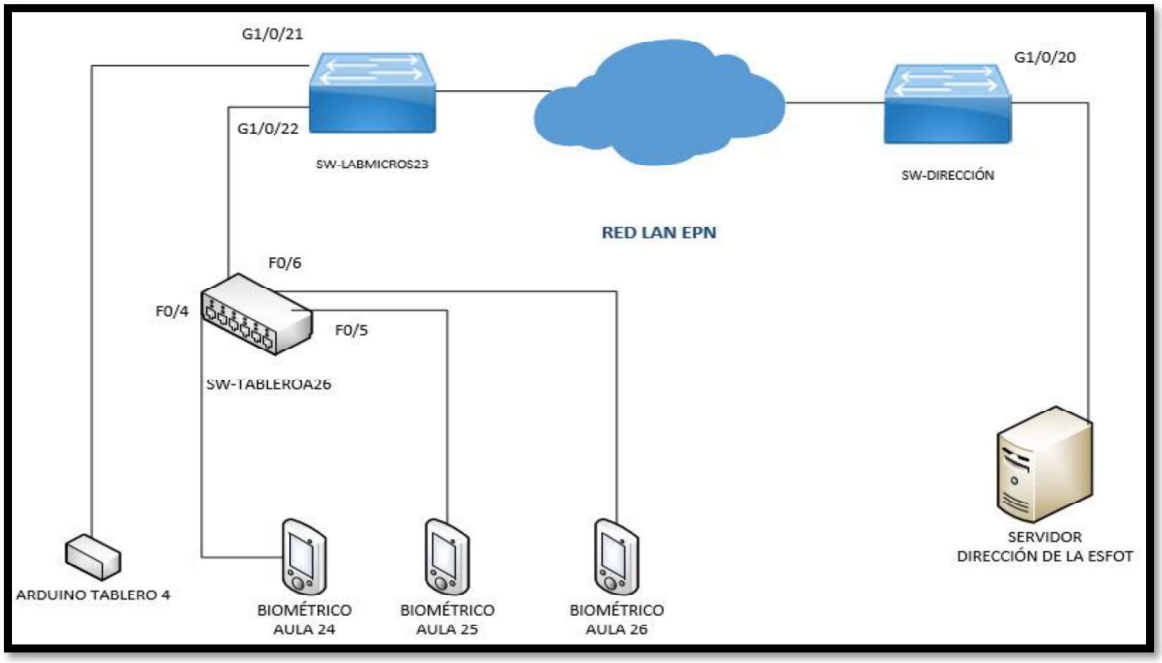


Figura 3.2 Diagrama de red del sistema de automatización y acceso biométrico

El funcionamiento del sistema es el siguiente:

Servidor

- Es el equipo central de administración de los equipos del sistema de automatización y control
- Concentra todos los datos generados de los equipos biométricos y Arduinos, y los almacena en dos bases de datos pertenecientes al *software* ZKAccess y MySQL de la página *WEB.*
- Muestra al usuario los datos de monitoreo de forma amigable al usuario, a través de una página *WEB.*
- Recibe los datos de control: encendido, apagado, abierto o cerrado, de puertas, ventanas y luminarias, introducidas por el usuario y toma las acciones necesarias para ejecutar la orden.
- ZKAccess genera *logs* temporales sobre errores de autentificación e ingreso a las aulas de la ESFOT.

Red LAN EPN

- Provee de conmutación y enrutamiento de los datos generados por los equipos del sistema a la VLAN conrrespodiente, en doble direcciòn; del servidor hacia el switch del tablero A26 y viceversa.

- Genera disponibilidad, tolerancias a fallas y viabilidad, ya que contiene equipos de gran robustez y de mejor administración.

SW-TABLEROA26

- Equipo de capa 2, no administrable, conmuta los datos a través de todos sus puertos conectados, menos en el que recibió la información, del estado de puertas, ventanas y luminarias, además de los usuarios o profesores de los equipos biométricos.
- Se utiliza como concentrador central del equipo Arduino del aula 26 y biométricos de las aulas 24. 25 y 26.

Biométricos

- Equipos encargados del control de acceso de las puertas, a través de la información de la huella dactilar de los usuarios registrados en el servidor.
- Apertura de las chapas eléctricas de las aulas 24, 25 y 26.

➢ Direccionamiento IP

El direccionamiento IP de los diferentes equipos de red del sistema de automatización y acceso biométrico se realizó de acuerdo a la subred de clase C perteneciente a la Vlan que se gestionó en la DGIP, la cual es 10.30.216.0 con máscara 255.255.255.0, con disponibilidad de 256 IPs; con el fin de pertenecer como una red extendida en la LAN de la EPN. En la Tabla 3.2, se puede observar el direccionamiento realizado, cabe recalcar que las direcciones IPs son ficticias por cuestiones de seguridad.

Tabla 3.2 Direccionamiento IP del sistema de automatización y acceso biométrico

Equipo	IP	Máscara	Gateway
Servidor dirección ESFOT	10.30.216.125	255.255.255.0	10.30.216.1
Arduino Tablero A26	10.30.216.130	255.255.255.0	10.30.216.1
Biométrico aula 24	10.30.216.149	255.255.255.0	10.30.216.1
Biométrico aula 25	10.30.216.148	255.255.255.0	10.30.216.1
Biométrico aula 26	10.30.216.147	255.255.255.0	10.30.216.1

➢ Cableado Estructurado

Los dispositivos e insumos eléctricos, electrónicos y de comunicación, utilizados en la implementación del cableado estructurado, se puede visualizar en la Tabla 3.3.

Tabla 3.3 Recursos de cableado estructurado

Recurso	Cantidad	Utilidad
Cable *Ethernet* cat 5e	1 bobina 305 mts	Cableado de los equipos biométricos y Arduino con el *switch* del tablero de ET, y al *switch* LABMICROS23. Además del *switch* DIRECCIÓN al servidor. Categoría 5e, debido al tráfico generado en los canales de comunicación, la máxima capacidad por los equipos de red es de 100Mbps.
Cable *Ethernet* cat 5e Aula 24	22,22 mts	
Cable *Ethernet* cat 5e Aula 25	9,95 mts	
Cable *Ethernet* cat 5e Aula 26	6,01 mts	
Cable *Ethernet* cat 5e Arduino – SW LABMICROS23	31,24 mts	
Cable *Ethernet* cat 5e SW TABLEROA26 – SW LABMICROS23	31,24 mts	
Cable *Ethernet* cat 5e SW DIRECCIÓN – servidor.	83,73 mts	
Organizador de cables y canaletas	1	Organizar los cables de *Ethernet* y alimentación de los equipos biométricos.
Caja cuadrada 4” (Caja de paso metálico)	3	Caja para la colocación de la placa de protección.
Caja sobrepuesta Dexson UTP 60x40 mm	1	Caja para conexión de *patch cord* en el servidor.
Manguera flexible bx ¾	184,39 mts	Protección del recorrido del cable UTP.
Canaleta UTP 40x25x2000 mm	4	Protección de exterior del cable UTP conectado del techo falso al biométrico.
Switch D-link DES-1008C 8 puertos	1	Concentrador de datos de los equipos biométricos.
Regulador automático de voltaje FORZA FVR-3001 CA 110f/120 V	1	Protección eléctrica de equipos biométricos y switch.
Conectores RJ45	10	Interfaz física para conectar dispositivos en red.
Canaleta para AC 20x20x2000	1	Protección de cables de alimentación
Borneras	1	Alimentación de los equipos biométricos
Tablero metálico 30x30x20 IP 41 INEN 2568, Electrónica y Telecomunicaciones, ET.	1	Área de ubicación del *switch*, regulador de voltaje y borneras

El diseño del cableado de datos para la comunicación, a través de la infraestructura de la ESFOT, entre los diferentes dispositivos de red como: *Switches*, biométricos, placa Arduino y servidor; se basó en 2 planos que se pueden visualizar en el **Anexo 5**.

- **Protección del sistema**

La protección del sistema ante cualquier evento de picos de voltaje o de corriente, se dimensionó mediante el estudio del consumo de potencia del sistema. En la Tabla 3.4, se observa los datos obtenidos.

Tabla 3.4 Estudio del consumo de potencia

Equipo	Cantidad	Watts
Switch D-link DES-1008C 8 puertos	1	1.55
Biométrico sf300	3	108
Tablero de EM	1	610
	Total:	719,55

De acuerdo al total de potencia en Watts, se adquiere el equipo regulador automático de voltaje FORZA FVR-3001 CA 110f/120 V, que tiene la capacidad de 1500 Watts, considerando la escalabilidad a futuro de nuevas implementaciones en equipos o servicios en el sistema.

- **Diseño del sistema Arduino**

  - **Asignación de Pines**

En la Tabla 3.5, se puede observar la asignación de pines, entrada o salida, aula y nomenclatura a utilizarse en la placa Arduino Mega 2560.

Tabla 3.5 Distribución de pines del Arduino Mega 2560

VENTANAS			
Pin	**Número de ventana**	**Aula**	**Nomenclatura**
32	1	26	ACT_VENT_26_1
34	2	26	ACT_VENT_26_2
36	1	25	ACT_VENT_25_1
38	2	25	ACT_VENT_25_2
40	1	24	ACT_VENT_24_1
42	2	24	ACT_VENT_24_2
PUERTAS			
Pin	**Entrada/Salida**	**Aula**	**Nomenclatura**
56-A2	Entrada	26	ACT_PU_26
57-A3	Entrada	25	ACT_PU_25
58-A4	Entrada	24	ACT_PU_24
62-A8	Salida	24	E24P
63-A9	Salida	25	E25P
64-A10	Salida	26	E26P

FOCOS			
Pin	**Entrada/Salida**	**Aula**	**Nomenclatura**
4	Entrada	26	ACT_FO_26
5	Entrada	25	ACT_FO_25
6	Entrada	24	ACT_FO_24
49	Salida	26	E26L
47	Salida	25	E25L
45	Salida	24	E24L
39	Salida	26	A26L
37	Salida	25	A25L
35	Salida	24	A24L

- **Protección**

La placa Arduino se introduce en una caja de acrílico para protección en el tablero de EM, ver Figura 3.3. Dicho tablero contiene elementos y conexiones electromecánicas y eléctricas.

Figura 3.3 Caja acrílica para Arduino Mega 2560 [33].

- **Código de programación**

El monitoreo y control del sistema de automatización está a cargo del Arduino Mega; cuenta con el procesamiento del microcontrolador Atmega 2560, al cual están conectados, en sus pines de salida y entrada, los sensores electromagnéticos para el monitoreo de puertas y ventanas, interruptores y relés para el control de puertas y luminarias. Se presenta el código del aula 26, que está conformado por dos partes el *void setup* y *void loop*. En el **Anexo 6,** se pueden observar las líneas de código completas.

- ***Void Setup***

Las principales configuraciones como: establecimiento de librerías, tipo de comunicación, pines de entrada o salida y creación de variables en la lógica del código Arduino, para el monitoreo y control de puertas, ventanas y focos; se pueden visualizar en el diagrama de flujo de la Figura 3.4. Primero, se añade librerías, se define variables globales y se configura los parámetros necesarios para la comunicación IP entre la placa y el servidor. Segundo, se establece los pines de entrada y salida, tanto de ventanas, puertas y focos. Tercero, se establece en configuración *Pull Up* de los pines necesarios. Cuarto, se inicia la comunicación con el servidor.

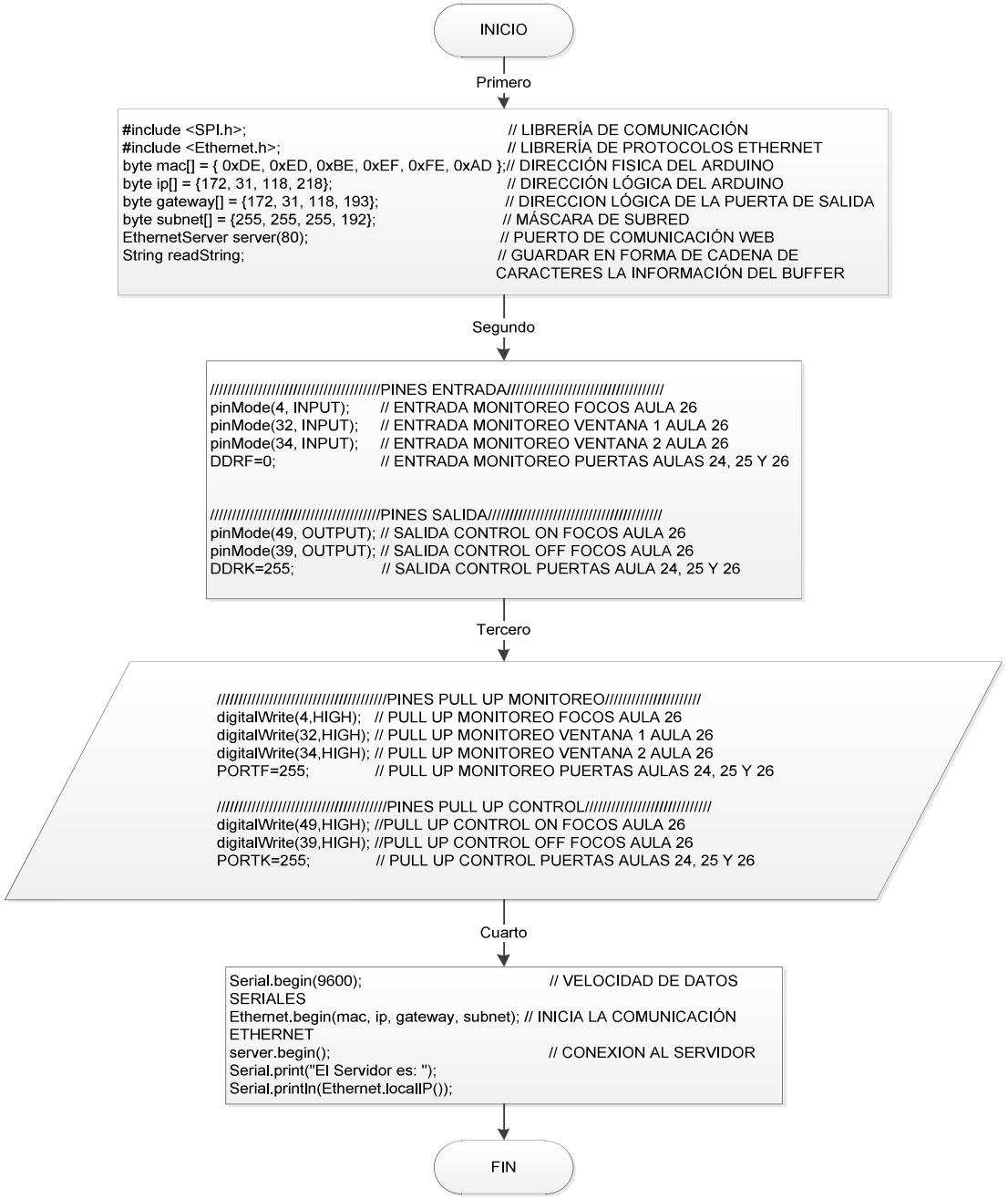


Figura 3.4 Código Arduino de *Void Setup*

- ***Void loop***

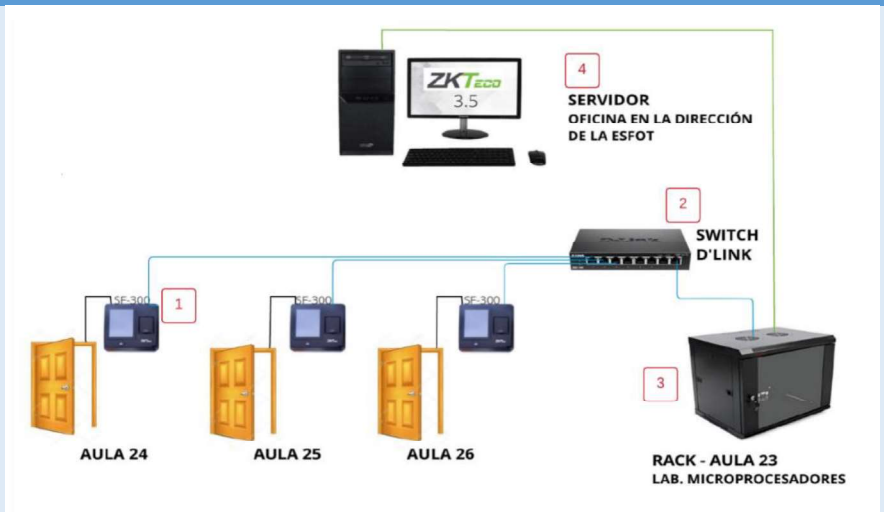
Las diferentes funcionalidades o acciones repetitivas que debe ejecutar el microcontrolador para el monitoreo y control en el sistema de automatización, de acuerdo a la lógica de programación, se puede visualizar en el diagrama de flujo de la Figura 3.5. Primero, se establece la comunicación del Arduino, como cliente con el servidor y se asigna variables. Segundo, se envía los datos de los pines de entrada, en forma de caracteres, al servidor sobre el estado de puertas, ventanas y luminarias; al finalizar, se detiene la comunicación de envío. Tercero, se testea un tipo específico de

caracter recibido del servidor, en función de dicho texto; se toma acciones de apertura de puertas y encendido o apagado de focos.

- **Diseño del sistema de acceso biométrico**

El diseño del sistema de control de acceso, se lo estructura con el equipo ZKTeco SF-300, mediante su *software*, ZKAccess3.5. En la Tabla 3.6, se muestra el esquema de conexión y sus componentes.

Tabla 3.6 Esquema de conexión para el sistema de control de acceso

No	Parte	Funcionalidad
		
1	ZKTeco SF-300	Lector biométrico que permite el control de acceso mediante la identificación de huellas digitales de los usuarios. Este dispositivo soporta la conexión de una cerradura eléctrica ya que cuenta con un relé integrado.
2	*Switch* D'link	Se encarga de la interconexión entre los 3 equipos biométricos y el *switch* perteneciente a la red de la ESFOT.
3	*Rack* con *switch* de la red de la EPN	Panel de conexiones para el *switch* que interconecta a los biométricos y así tener acceso a la red de la EPN, es decir conexión a Internet.
4	Servidor	En el servidor se aloja el *software* ZKTeco3.5 que permite el monitoreo de puertas y el control de acceso.

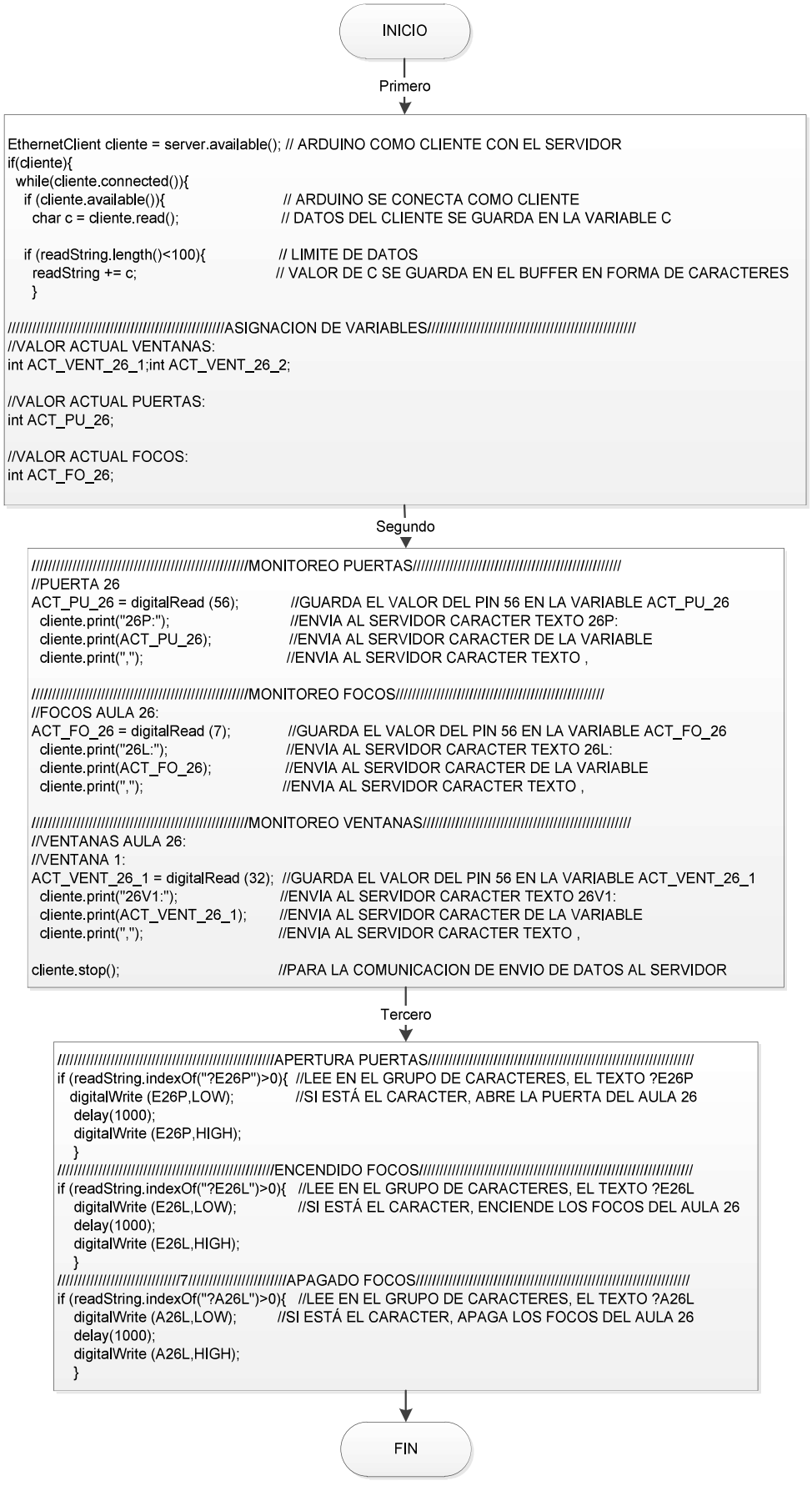


Figura 3.5 Código de Arduino de *Void Loop*

- **Funcionamiento del algoritmo del código**

En la Figura 3.6, se puede observar el funcionamiento del algoritmo del código Arduino.

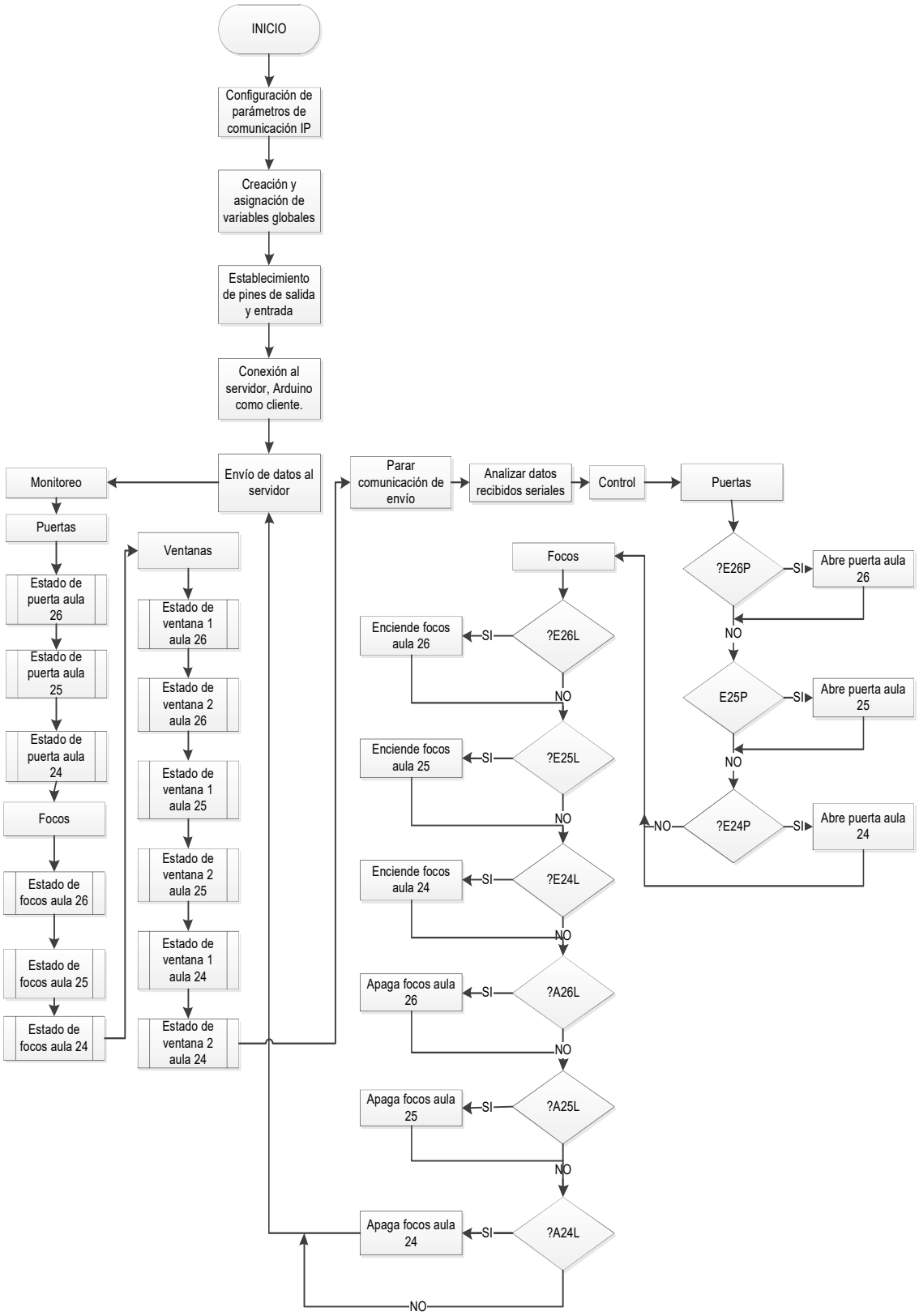


Figura 3.6 Diagrama de flujo del funcionamiento del algoritmo Arduino

- **Funcionamiento**

  Registro de usuarios:

- Se registra la huella de los usuarios en el enrolador y se carga a la base de datos del *software* de administración.

- Se loguea a todos los usuarios mediante el registro de su huella dactilar con sus respectivos horarios; se hace uso de la carga horaria curricular que proporciona el área administrativa de la ESFOT para el semestre vigente. En la base de datos del *software* la información ingresada se divide en 3 grupos, esto debido a que el *software* soporta un máximo de 50 eventos, y los horarios de clase que maneja la comunidad educativa sobrepasa este número.

  Operatividad del sistema:

- El usuario se loguea en el equipo biométrico ZKTeco SF-300 mediante su huella dactilar.

- Esta solicitud se transfiere vía *Ethernet*; la solicitud llega a la red de la EPN, la cual esta enlazada con el servidor, en el que está el *software* ZKTaccess3.5.

- El *software* verifica la información, es decir, si el usuario y el horario en el que intenta ingresar son los correctos.

- Una vez validada esta información se enclavará el relé para activar la cerradura y abrir la puerta del aula; por lo contrario, su acceso será denegado.

- Toda esta información se puede visualizar en un informe básico del estado de las puertas en el *software*. Como función adicional también se puede abrir las puertas desde el *software* sin tener que dirigirse personalmente.

  El diagrama de flujo de la Figura 3.7, describe el proceso que sigue el sistema de control de acceso

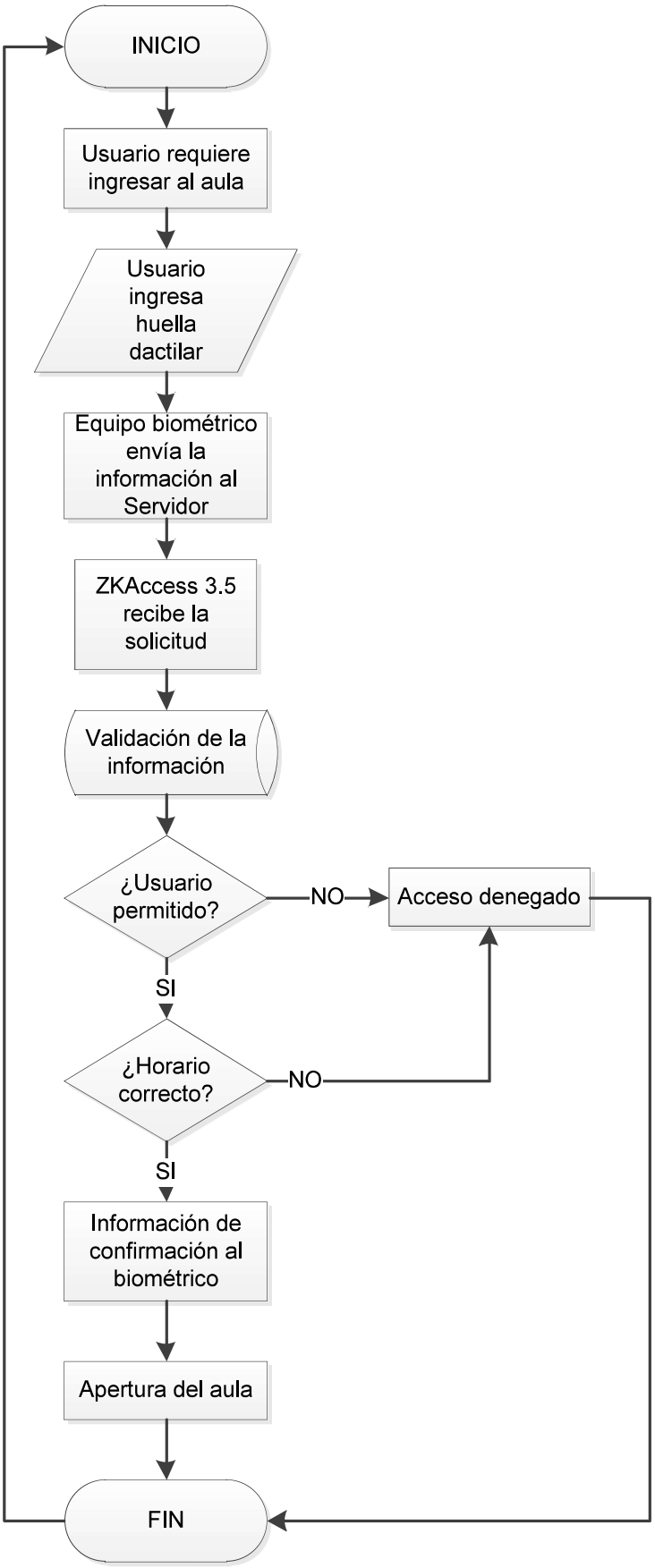


Figura 3.7 Diagrama de flujo del funcionamiento del sistema de control de acceso

- **Registro de huellas dactilares**

Previa la instalación del equipo biométrico en las aulas 24, 25 y 26, se procede al registro de los usuarios, este proceso se describe a continuación:
Se registra la huella dactilar de los dos dedos pulgares y el dedo índice de cada usuario mediante el enrolador ZK4500. Las huellas registradas por el enrolador serán cargadas al *software* ZKAccess mediante interfaz USB, como se muestra en la Figura 3.8.

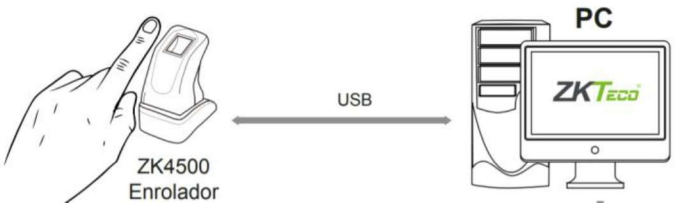


Figura 3.8 Registro de huellas dactilares de usuarios [34].

Una vez registradas las huellas dactilares de los usuarios, se registra la carga horaria curricular de cada docente respectivamente con las aulas donde impartirá sus clases. Para el personal administrativo, el acceso a las aulas no tendrá ninguna restricción. La información que se registra es aquella de la que se encarga al inicio de cada semestre el área administrativa de la ESFOT.

- **Diseño de la placa de protección**

El equipo biométrico necesita una alimentación externa, para lo cual posee una conexión para alimentación DC de 12V – 3A, dicha alimentación se obtiene mediante el uso de una placa de protección contra cortocircuitos, ya que si se detecta una intensidad superior a la que debería circular, esta se interrumpirá permitiendo el funcionamiento normal del sistema [35].

- **Diagrama electrónico**

En la Figura 3.9, se muestra el diagrama de conexión de la placa y en la Tabla 3.7, se presenta un resumen del diseño y los componentes que conforman la placa de protección, así como la justificación de la elección de cada componente.

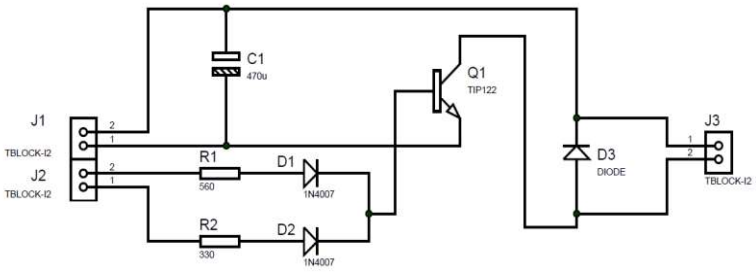


Figura 3.9 Diagrama de conexión de la placa de protección contra cortocircuitos.

Tabla 3.7 Componentes de la placa de protección

Cantidad	Componentes	Justificación
3	Bornera de dos pines	Mediante sus entradas, hechas a base de metal para una mejor conductividad; se realiza la conexión de cables que provienen del equipo biométrico, su alimentación; el tablero y la chapa eléctrica [36].
3	Diodos 1N4007	Corriente directa: 1A Voltaje directo máximo: 1.1V Actúa como adaptador de corriente alterna [37].
1	Transistor TIP 122	Disipación total del dispositivo (Pc): 65W Tensión colector-base (Vcb): 100V Tensión colector-emisor (Vce): 100V Tensión emisor-base encedido (Veb): 2.5V Hfe= 1000 F= 10 Hz. Corriente del colector DC máxima (Ic): 50A [38]
2	- Resistencia de 330 Ω - Resistencia de 560 Ω	Limitar la corriente a través del diodo de acuerdo al voltaje de entrada. Fórmula para calcular el valor de la resistencia de la base de un transistor. $\text{Resistencia} = \frac{(\text{V} - \text{Vbe})}{\frac{\text{I}}{\text{Hfe}}}$ Donde: V: voltaje de entrada. - Tablero: 3.3 V - Biométrico: 9-5 V Vbe: voltaje entre emisor y base. I: corriente de trabajo de la chapa eléctrica 3A. Hfe: ganancia de corriente [39]. Cálculos: - ((3,3-2,5)) / (3/1000) = 266,66 ≈ 330 ohmios valores comerciales. - ((5-2,5)) / (3/1000) = 833,33 ≈ 560 ohmios valores comerciales.
1	Capacitor electrolítico de 470 µF	Voltaje máximo: 50V Fórmula para calcular el valor del condensador de acople: C=10/(2*Pi*Fo*R) Donde: C: es en faradios. Fo: frecuencia de trabajo R: resistencia, paralelo 330 y 560 ohmios. Pi: es 3.1416 [40]. Cálculos: - C=10/(2*Pi*0,10*204,64) = 0.000778 ≈ 470uF valores comerciales. Corriente de fuga: 3uA (máx.) Modera la tensión eléctrica de salida [40].

- **Diagrama de conexión**

En la Figura 3.10, se muestra el diagrama de conexión desde la parte exterior con todos los dispositivos que forman parte del sistema.

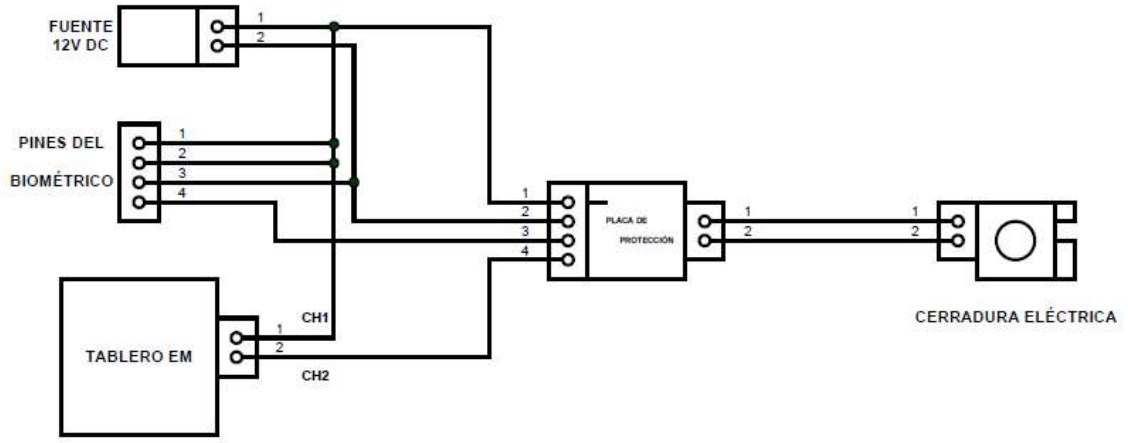


Figura 3.10 Conexión externa a la placa de protección.

- **Funcionamiento**

El pin del Jack 1 está conectado a la alimentación del biométrico, la fuente del tablero de EM, el control a la chapa eléctrica mediante el Arduino, y la conexión COM que proviene del biométrico. En el pin 2 del Jack 1 se tiene la conexión a tierra tanto del biométrico como de la fuente de alimentación. En el pin 1 del Jack 2 se tiene la conexión del biométrico denominada NO (*Normally Open*) que hasta que se actúe sobre él, no pasará la corriente eléctrica; y para el pin 2 del Jack 2 se tiene la conexión del control de la chapa eléctrica que proviene desde el Arduino.

Con respecto a los elementos que conforman el circuito de la placa se tiene: las resistencias junto con los diodos que solo se encargarán del paso de la corriente eléctrica y de la protección para evitar que haya un cortocircuito. Además, el capacitor electrolítico que permitirá moderar la tensión de carga para que en este caso, el transistor TIP122 actúe como *switch* cuando en su base, el voltaje que llegue (12V), haga que la chapa se active y por ende se dé la apertura de la puerta. Para ello, su conexión se encuentra en el Jack 3. La polaridad no tiene importancia para la chapa eléctrica.

En la Figura 3.11, se puede observar el diagrama de flujo del funcionamiento de la placa de protección

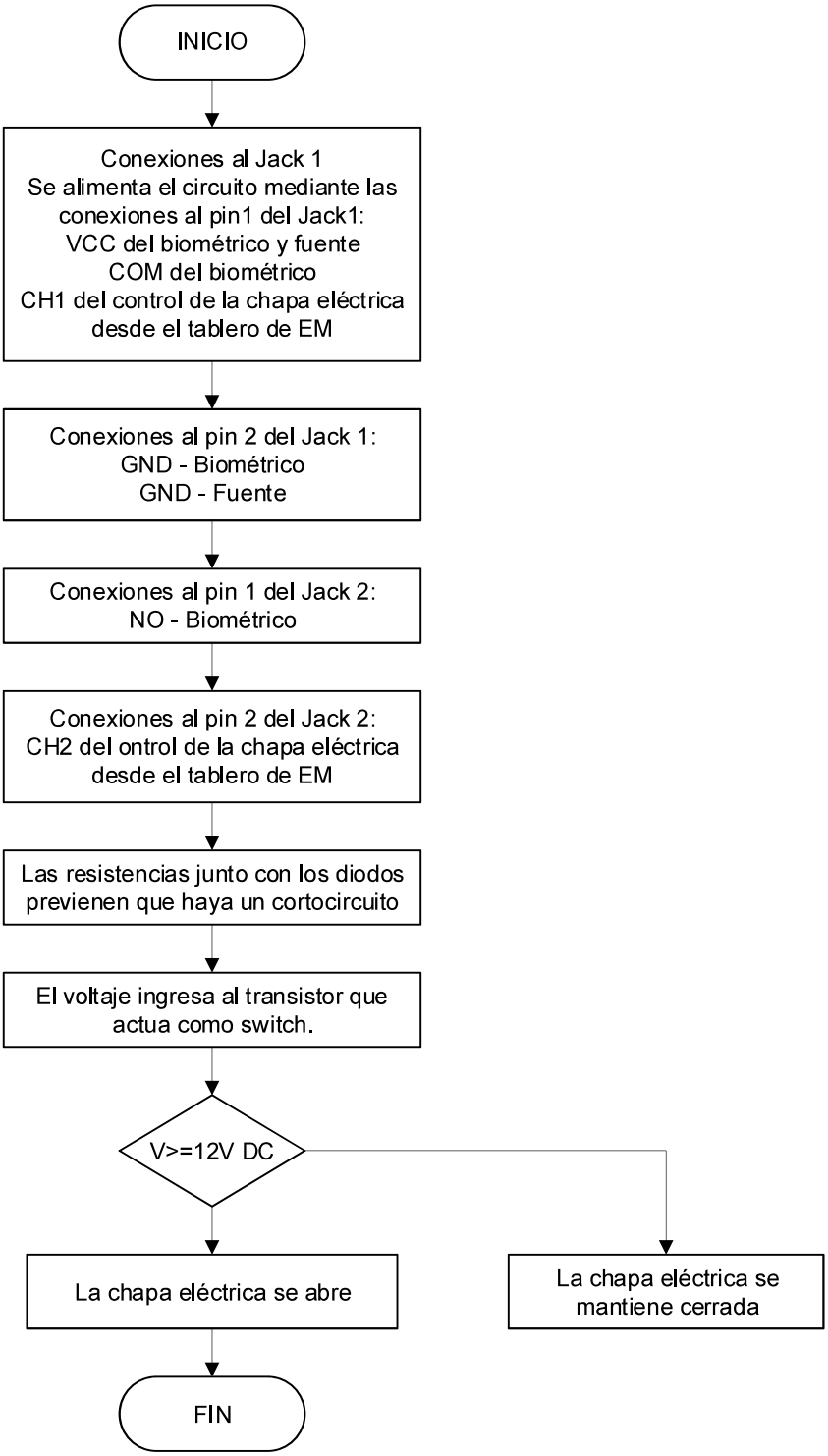


Figura 3.11 Diagrama de flujo del funcionamiento de la placa de protección

- **Impresión**

El diseño electrónico para la impresión del circuito se realizó en Proteus y en ISIS, ver Figura 3.12.

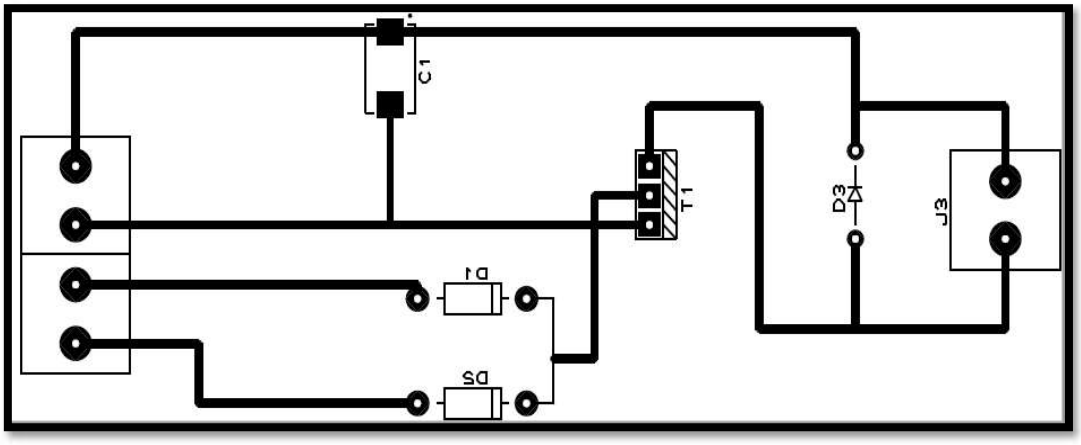


Figura 3.12 Impresión de la placa de protección

3.3. Implementación del sistema

La implementación del sistema de automatización y acceso biométrico se realizó por etapas, en el siguiente orden: adquisición de materiales y equipos, sistema de cableado estructurado, placa de protección, sistema de control de acceso, instalación de la placa Arduino, y finalmente, configuración y establecimiento del *software* en el servidor del control de acceso.

- **Adquisición de materiales y equipos**

La adquisición se realizó a diferentes proveedores de acuerdo al elemento requerido. En el **Anexo 9** se puede visualizar los costos de los equipos que se adquirieron para el desarrollo del sistema de automatización y acceso biométrico en las aulas 24, 25 y 26.

- **Sistema de cableado estructurado**

  - **Tablero ET**

Se instaló el tablero de ET en el Aula 26, con la ubicación de rendijas para la separación del *switch* con el regulador de voltaje, adicional se instaló las borneras, organizador de cables y canaletas de cables. Ver Figura 3.13.

Figura 3.13 Montaje del tablero ET

- **Cableado**

El peinado del cable de Ethernet cat 5e y cable de alimentación con manguera flexible, para protección, se instaló de acuerdo a las normas ANSI/TIA/EIA-568-B, ver Figura 3.14. Los recorridos del cableado son: desde los equipos biométricos de cada aula al *switch* del tablero ET, desde el *switch* LABMICROS23 al *switch* del tablero de ET, del *switch* LABMICROS23 al Arduino del tablero 4, y por último, del *switch* DIRECCION al servidor, de acuerdo a los planos del **Anexo 5**.

Figura 3.14 Instalación del cableado UTP y alimentación

- **Cajas y canaletas**

Las cajas cuadradas de 4” se instalaron en cada aula 24, 25 y 26, sobre el techo falso para la ubicación de la placa de protección. La caja sobrepuesta Dexson UTP se colocó en el área del servidor con un *patch cord* para la conexión de la máquina a la red del

sistema, además se ubicó las respectivas canaletas en la parte exterior para protección y estética en el servidor, el tablero de ET y los equipos biométricos, ver Figura 3.15.

Figura 3.15 Instalación de cajas y canaletas, servidor, tablero ET, biométrico.

- **Conectores**

Se realizó el ponchado de los cables *Ethernet* con conectores RJ45, ver Figura 3.16, en función del diagrama de colores del estándar EIA/TIA 568 B.

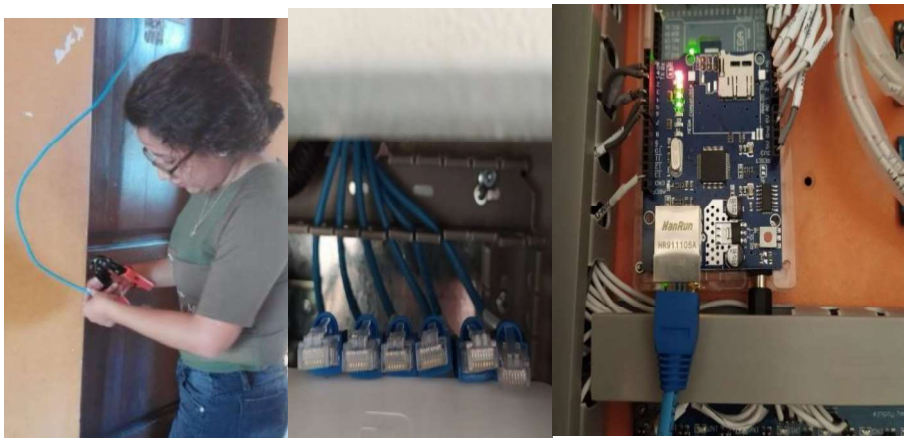


Figura 3.16 Ponchado de conectores RJ45

- **Equipos**

Se realizó el montaje de los equipos como: *switch* del tablero 4, regulador de voltaje, y máquina del servidor, ver Figura 3.17.

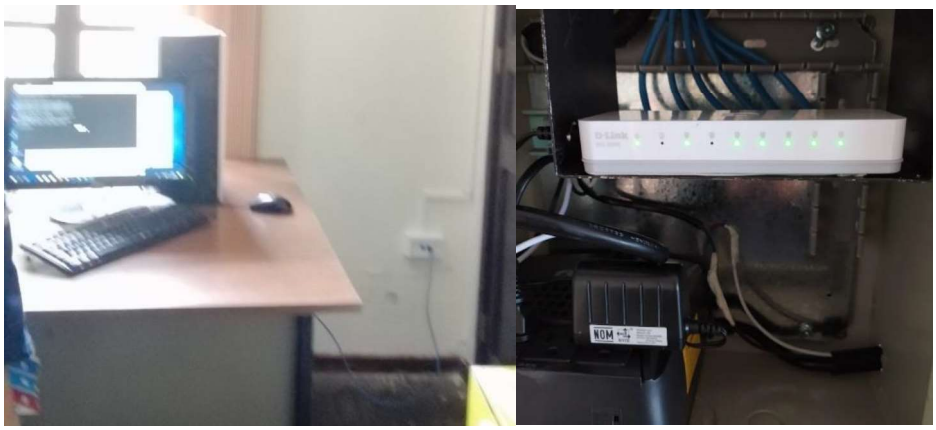


Figura 3.17 Instalación de equipos

- **Placa de protección**

Las placas de protección se fabricaron con el método de planchado para placas electrónicas, a través del diseño e impresión de Proteus. Se instaló en el techo falso de cada aula, en las cajas metálicas de paso, con las respectivas conexiones de acuerdo al diseño, ver Figura 3.18.

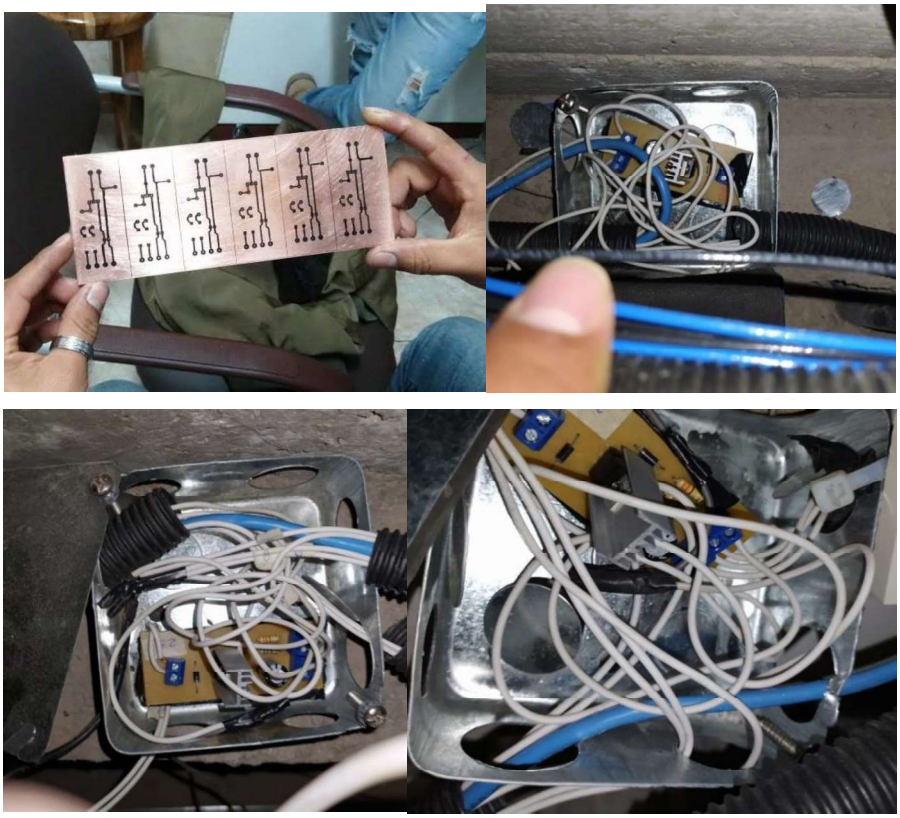


Figura 3.18 Instalación de las placas de protección

- **Control de acceso**

Para la instalación del *hardware* del sistema de control de acceso se realizó con las siguientes actividades: adaptación de chapas eléctricas en las puertas de cada una de las aulas y el encaje y conexión del equipo biométrico al área asignada, ver Figura 3.19.

Figura 3.19 Instalación del *hardware* del sistema de control de acceso

- **Arduino Mega 2560**

  - **Placa Arduino**

La placa Arduino se instaló en el tablero de EM, con la protección de la caja de acrílico; adicional se insertó los cables de sensores, relés y alimentación en los pines correspondientes, de acuerdo a la distribución realizada. En la Figura 3.20, se puede observar la implementación del Arduino Mega 2560.

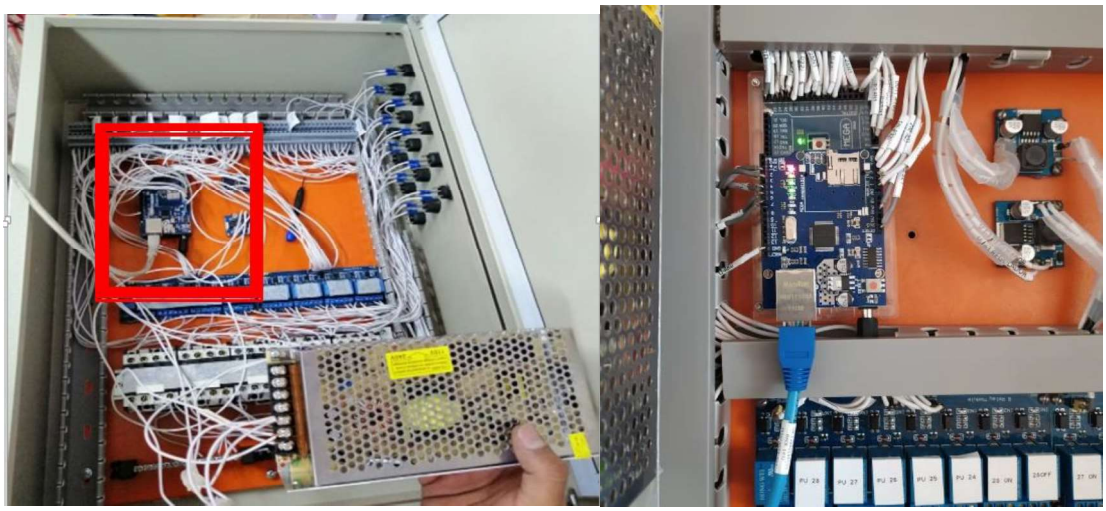


Figura 3.20 Instalación de placa Arduino Mega 2560 en tablero EM

- **Código**

El código se implementó en el Arduino Mega 2560, a través de su propio ambiente de desarrollo y con la comunicación USB entre una máquina y el dispositivo, ver Figura 3.21.

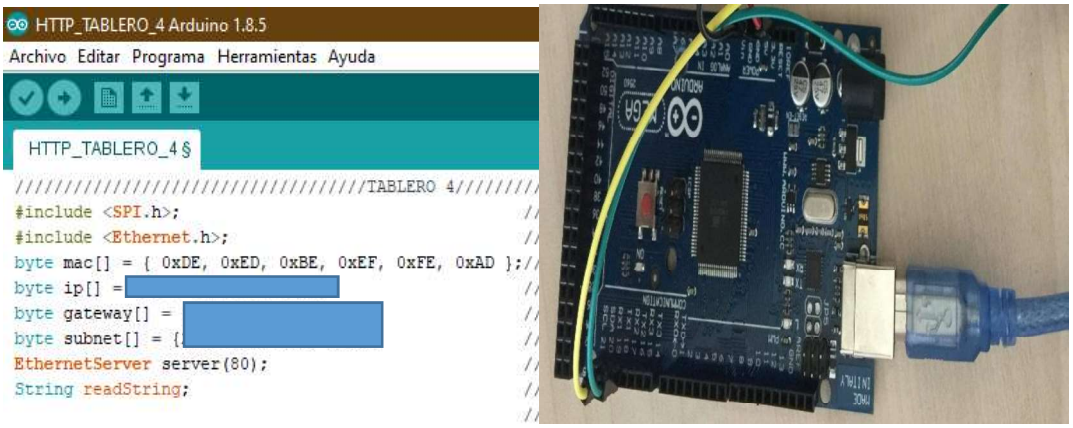


Figura 3.21 Montaje del código a la placa Arduino

- ***Software* ZKAccess en el servidor**

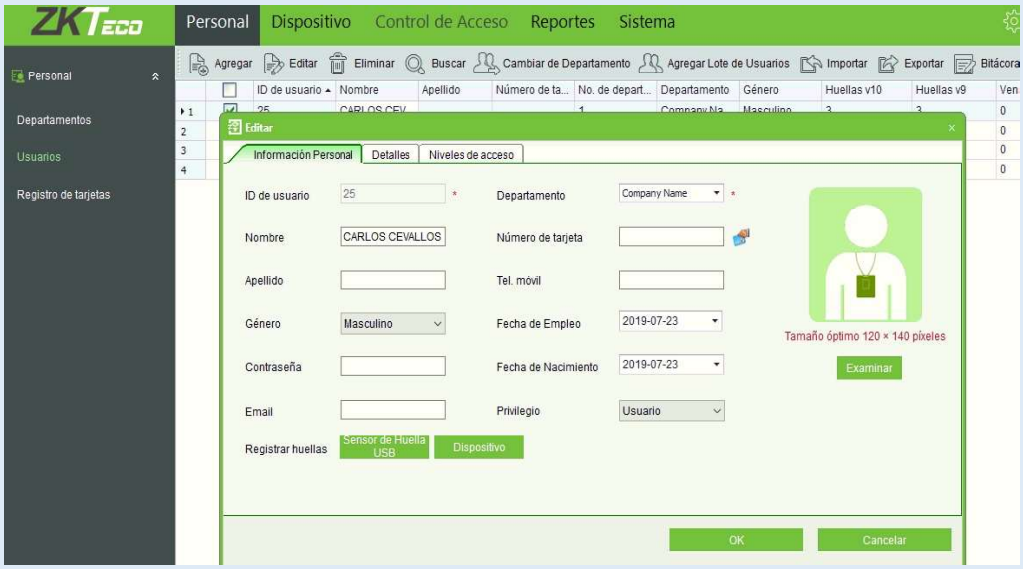
- **Registro de huellas dactilares**

El registro de las identidades de las huellas dactilares se realiza mediante la enroladora, el profesor pone su dedo en el sensor y mediante el *software* ZKAccess, se sube la información a la base de datos

- **Configuración del control de acceso**

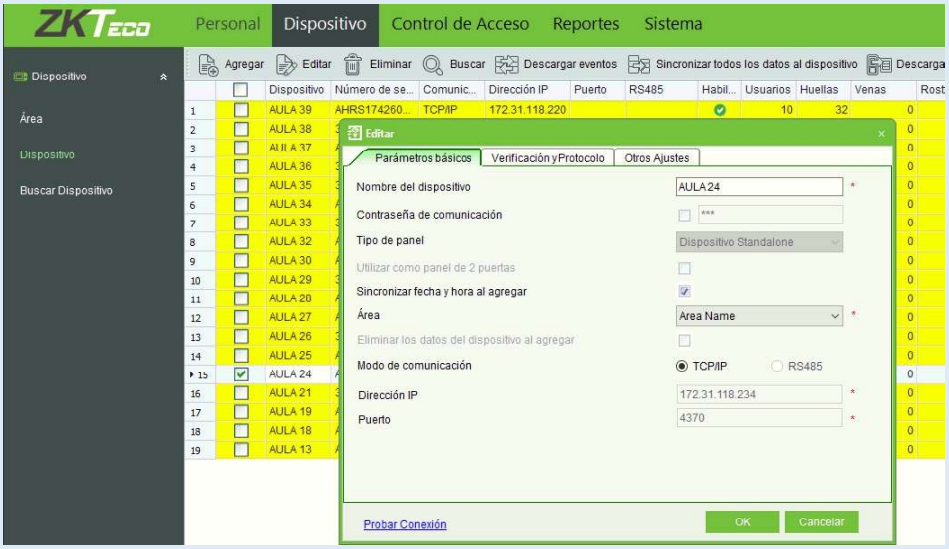
La instalación del *software* en el servidor, se inicia con la configuración del programa para la comunicación con los equipos biométricos y la base de datos con la información de los profesores con sus respectivos horarios. Posteriormente, se registra las huellas dactilares de cada usuario con la enroladora; por último, se añaden los usuarios al grupo de clases e intervalos de tiempo, como se puede observar en la Figura 3.22, para mayor detalle ver **Anexo 8.**

Registro de usuarios al *software* ZKAccess



Registro de huella dactilar en el usuario creado.

Añadir dispositivos biométricos o aula



Añadir horario

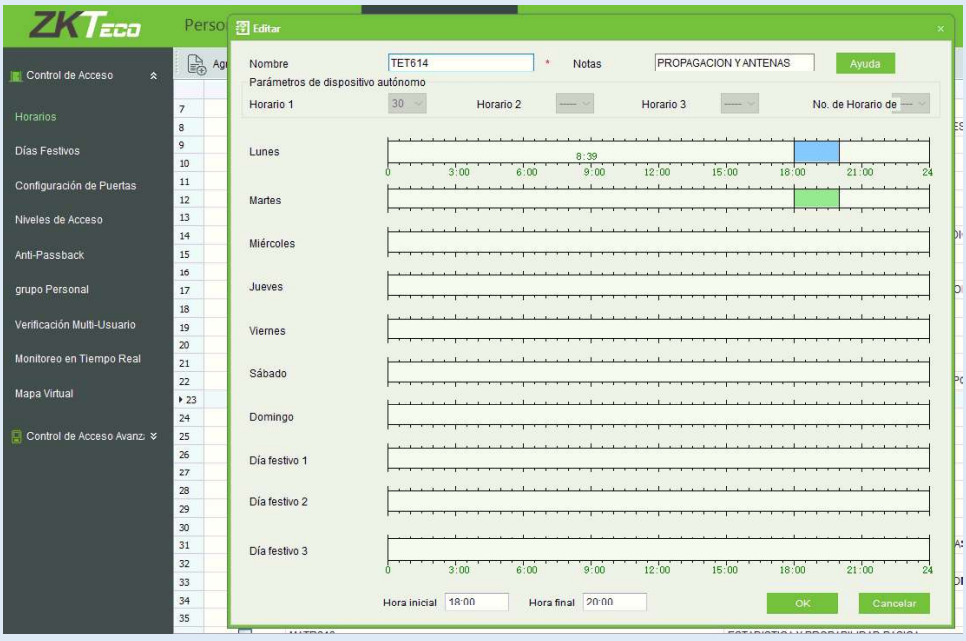


Figura 3.22 Configuración del *software* biométrico ZKAccess

3.4. Pruebas de funcionamiento

- **Red de datos**

Se verificó el funcionamiento de los equipos de red como: *switch* del tablero 4, biométricos del aula 24, 25 y 26, y la placa Arduino; a través de pruebas físicas, verificación de leds indicadores. Además pruebas lógicas, con la ayuda del comando *ping* desde el servidor, ver Figura 3.23.

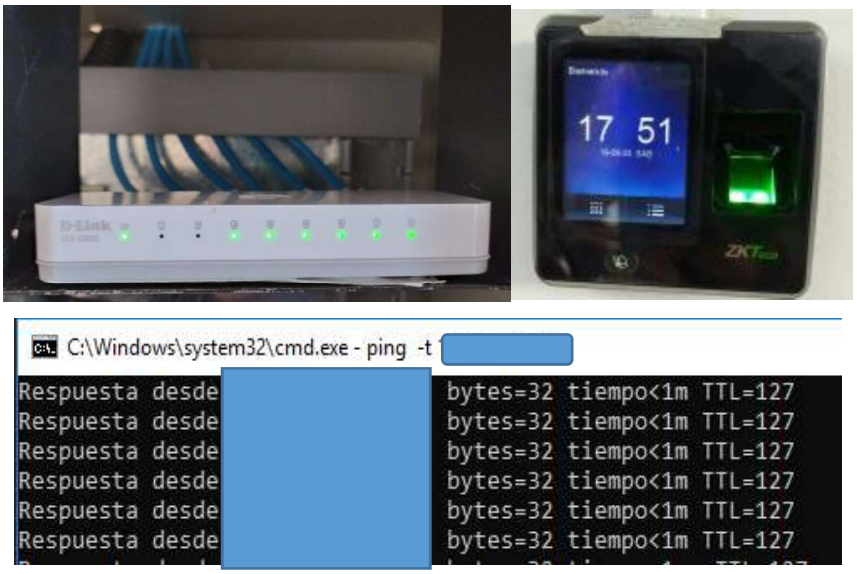


Figura 3.23 Prueba de funcionamiento de la red de datos

- **Sistema de acceso biométrico**

Se realizaron pruebas de funcionamiento con el registro de varios usuarios con su respectivo horario de clases, y se simuló la apertura de la puerta del aula dentro del intervalo de tiempo asignado; además, se visualizó el registro de los equipos biométricos en el *software* del servidor, ver Figura 3.24.

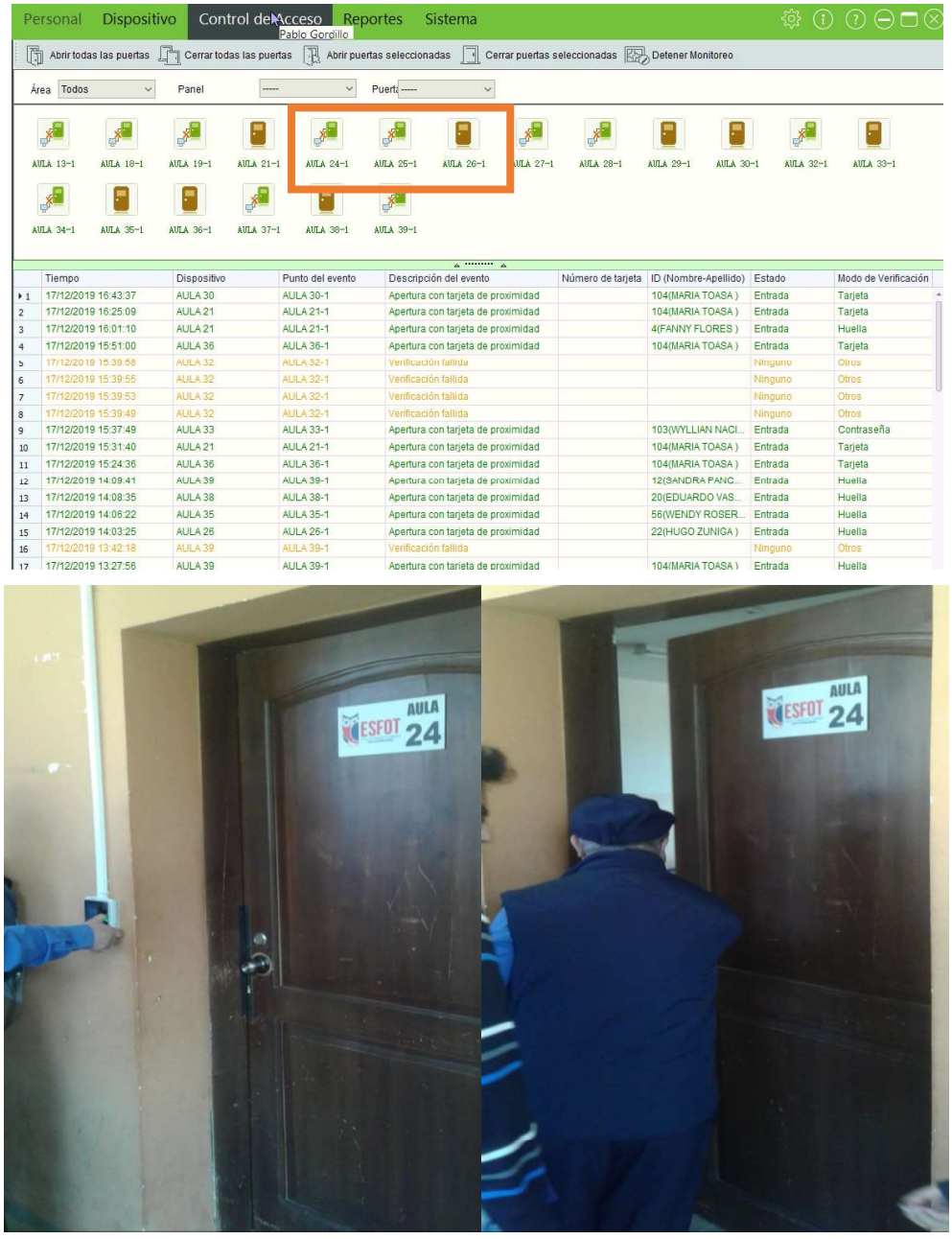


Figura 3.24 Funcionamiento del sistema de acceso biométrico

- **Sistema de automatización**

Se realizaron pruebas de funcionamiento a través del servidor, verificando el monitoreo y control de las aulas, de igual forma, su conexión IP, ver Figura 3.25.

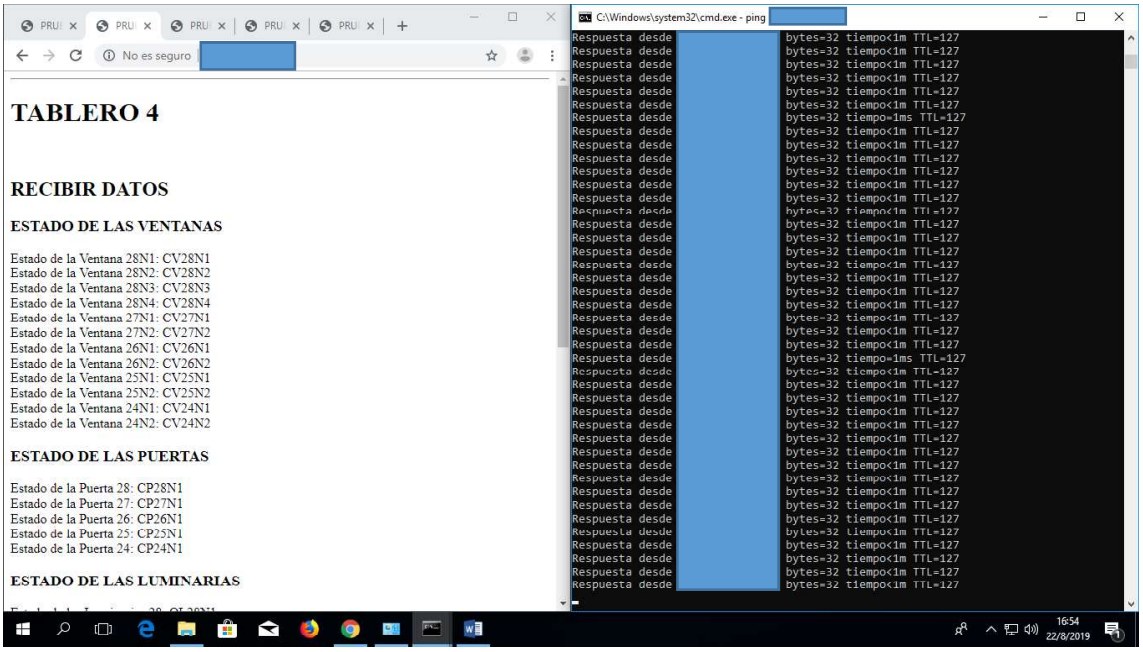


Figura 3.25 Pruebas de funcionamiento de la placa Arduino

- **Manuales y documentación**

La documentación generada para el sistema de automatización y acceso biométrico de las aulas 24, 25 y 26, fue con el objetivo de tener información acerca del uso del equipo biométrico y de su *software* de administración, ver **Anexo 8**, de la misma forma, el mantenimiento de los equipos, ver **Anexo 7**.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- El sistema de acceso biométrico solventó los inconvenientes de seguridad, ya que, solo los profesores y personal administrativo autorizado pueden ingresar a las aulas. Las inmediaciones educativas de la ESFOT ya no son áreas para cometer actos impúdicos y vandálicos.

- El sistema de acceso biométrico garantiza una mejor administración en la asignación de aulas y profesores de acuerdo a los horarios establecidos. El docente puede ingresar al aula en el horario establecido, descartando la consecuencia de comenzar impuntualmente las clases.

- El sistema de automatización en el control y monitoreo de puertas, ventanas y luminarias de las aulas 24, 25 y 26, representa un salto tecnológico en la comunidad de la ESFOT; por la razón que, se implementó un servicio inmótico, a través del uso de la plataforma Arduino.

- El sistema de automatización genera una mejor administración en los recursos académicos de las aulas 24, 25 y 26 de la ESFOT, debido a dos principales razones:
  Primero, presenta al usuario información en tiempo real del estado de abierto o cerrado de ventanas y puertas; además, el encendido o apagado de focos.
  Segundo, el usuario puede controlar remotamente la apertura de las cerraduras de las puertas y el encendido y apagado de luminarias.

- La tecnología moderna aporta importantes herramientas para la satisfacción de varias necesidades en diferentes áreas; por ejemplo, la seguridad con la identificación única de cada profesor, a través de su huella digital, puedan ingresar sin ningún problema al aula correspondiente en el intervalo de tiempo del horario de clases determinado.

- Existe en el mercado una gran variedad de componentes complementarios como: sensores, extensiones, librerías, dispositivos de red, etc, para la

plataforma Arduino; lo que genera un ambiente amigable con el usuario y la posibilidad de ejecutar varios proyectos de automatización y control, en diferentes áreas, a nivel educativo, industrial, empresarial, doméstico y comercial.

- La alimentación eléctrica del módulo Arduino Mega 2560 debe estar aproximadamente en un valor de 12 V para el correcto funcionamiento de la placa cuando trabaja en conjunto con el módulo *Ethernet*.

- Se concluye que realizar un testeo de hilos del cableado después de ser instalado y ponchado, es importante para verificar que no exista roturas, dobleces o interferencias que impida el transporte de datos.

- Se determinó que la dirección física del módulo *Ethernet* se establece de forma escrita en el entorno de desarrollo integrado (IDE), es por ello que si se utiliza más de uno en un proyecto; se tiene que registrar con diferentes números físicos.

- La sincronización de dispositivos biométricos de la marca ZKTeco, que se encuentran enrolados en un solo sistema de administración, se tiene que ejecutar cada que se realice un cambio o nueva entrada en el software o base de datos.

4.2. Recomendaciones

- A pesar de tener un regulador de voltaje para la protección de equipos, se recomienda revisar la conexión a tierra, en función de la norma ANSI/TIA/EIA-607, ya que la alimentación eléctrica de las inmediaciones tiene problemas de descargas e interferencias.

- Realizar mantenimientos cada 6 meses y anuales, de acuerdo al manual de mantenimiento, que contiene los pasos necesarios para la evaluación y corrección de imperfectos del sistema implementado.

- Se recomienda que, al tener un inconveniente o problema inoportuno en el sistema de automatización y control de acceso, se revise las indicaciones de la solución a problemas comunes descritos en el Manual de Mantenimiento y Manual de usuario del biométrico.

- Se debe realizar el respaldo de la base de datos del *software* de administración del control de acceso, ZKAccess 3.5, con el fin de solucionar cualquier inconveniente en el servidor; y, por consiguiente, no perder información.

- En base a los resultados recogidos en el proyecto desarrollado, se recomienda identificar las características técnicas de cada uno de los componentes que forman parte del sistema, esto permitirá al momento de realizar las respectivas conexiones los equipos no sufran daños materiales así, además evitar fallas que pueden ocasionar un sistema defectuoso.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] w. Rosso, «Tecnologias De La Informacion Y La Comunicacion,» [En línea]. Available: https://es.calameo.com/read/004301451c1ab017783fc. [Último acceso: 20 Octubre 2019].

[2] CIITA, «Ingenierìa,Tecnologìa, Automatizaciòn: Innovaciòn y desarrollo,» 2018. [En línea]. Available: http://memoriascimted.com/wp-content/uploads/2019/03/Ingenieria-tecnolog%C3%ADa-automatizaci%C3%B3n.pdf. [Último acceso: 20 Octubre 2019].

[3] O. d. E. Iberoamericanos, «Cómo optimizar el uso de los espacios,» 2015. [En línea]. Available: https://portaldelasescuelas.org/wp-content/uploads/2016/03/3_Como_optimizar_el-uso_de_los_espacios.pdf. [Último acceso: 25 Octubre 2019].

[4] L. Cosentino, «Control de Accesos Conceptos, historia y esquema básico,» 2016. [En línea]. Available: http://www.rnds.com.ar/articulos/045/RNDS_152W.pdf. [Último acceso: 30 Septiembre 2019].

[5] R. Llopis, «Sistemas De Autenticación Biométricos,» 2016. [En línea]. Available: http://spi1.nisu.org/recop/al01/llopis/Biometricos.PDF. [Último acceso: 26 Octubre 2019].

[6] ZKTeco, «SF300 Terminal IP con Lector de Huella Digital,» 2015. [En línea]. Available: https://www.zktecolatinoamerica.com/documentos/control-de-acceso/standalone/SF300/SF300.pdf. [Último acceso: 12 Octubre 2019].

[7] ZKTeco latinoamérica, «Catálogos de productos 2017,» 2017. [En línea]. Available: https://www.zktecolatinoamerica.com/documentos/ZK_Catalogo.pdf. [Último acceso: 26 Octubre 2019].

[8] ZKSoftware.es, «ZK500,» [En línea]. Available: https://zksoftware.es/uploads/product/Catalogos/ZK4500_CATA.pdf. [Último acceso: 27 Noviembre 2019].

[9] ARDUINO .CL, «¿Que es arduino?,» 2017. [En línea]. Available: https://arduino.cl/que-es-arduino/. [Último acceso: 1 Octubre 2019].

[10] AG Electrónica, «MB0014: OEM ARDUINO MEGA 2560,» 20 Octubre 2017. [En línea]. Available: http://www.agspecinfo.com/pdfs/M/MB0014.PDF. [Último acceso: 1 Octubre 2019].

[11] Robotshop, «Arduino Mega 2560 Datasheet,» 22 Junio 2004. [En línea]. Available: http://eprints.polsri.ac.id/4598/8/File%20VIII%20%28Lampiran%29.pdf. [Último acceso: 20 Octubre 2019].

[12] CIIVA, «Arduino Ethernet Shield,» 2015. [En línea]. Available: https://datasheet.ciiva.com/19455/2152374-19455462.pdf. [Último acceso: 20 Octubre 2019].

[13] J. M. Ruiz Gutièrrez, « Arduino + Ethernet Shield,» 12 Enero 2013. [En línea]. Available: https://www.academia.edu/25347389/Arduino_Ethernet_Shield?auto=download. [Último acceso: 20 Octubre 2019].

[14] J. Joskowicz, «CABLEADO ESTRUCTURADO,» Octubre 2013. [En línea]. Available: https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf. [Último acceso: 24 Octubre 2019].

[15] QUANG DUNG TECHNOLOGY , «ANSI/TIA/EIA568-B,» 2015. [En línea]. Available: https://www.csd.uoc.gr/~hy435/material/Cabling%20Standard%20-%20ANSI-TIA-EIA%20568%20B%20-%20Commercial%20Building%20Telecommunications%20Cabling%20Standard.pdf. [Último acceso: 20 Octubre 2019].

[16] L. Gorgona, «Teoría de redes de computadoras,» [En línea]. Available: https://www.oas.org/juridico/spanish/cyber/cyb29_computer_int_sp.pdf. [Último acceso: 25 Octubre 2019].

[17] CISCO Systems, «2019,» [En línea]. Available: http://itroque.edu.mx/cisco/cisco1/course/module4/4.4.1.2/4.4.1.2.html. [Último acceso: 26 Octubre 2019].

[18] Federación de Enseñanza de CC.OO. de Andalucía., «Direccionamiento IP,» Mayo 2010. [En línea]. Available: https://www.feandalucia.ccoo.es/docu/p5sd7257.pdf. [Último acceso: 26 Octubre 2019].

[19] V. Agramunt, «DIRECCIONAMIENTO IP CALCULO DE REDES TCP/IP,» 2016. [En línea]. Available: http://virtualbook.weebly.com/uploads/2/9/6/2/2962741/tcp_ip.pdf. [Último acceso: 20 Octubre 2019].

[20] C. Hernandez y J. Vicente, «Características y configuración básica de VLANs,» 2015. [En línea]. Available: https://riunet.upv.es/bitstream/handle/10251/16310/Art%C3%ADculo%20docente%20configuraci%C3%B3n%20b%C3%A1sica%20VLANs.pdf. [Último acceso: 26 Octubre 2019].

[21] D. Zepeda, «Diseño de Redes LAN Tecnologías de conmutación,» 2017. [En línea]. Available: http://www.peri.net.ni/pdf/docLAN/vlan.pdf. [Último acceso: 26 Octubre 2019].

[22] D. Z. Vega, «Diseño de Redes LANTecnologías de conmutación,» 2016. [En línea]. Available: http://www.peri.net.ni/pdf/docLAN/vlan.pdf. [Último acceso: 20 Octubre 2019].

[23] Lab-Volt, «Sensores,» Febrero 2001. [En línea]. Available: http://biblio3.url.edu.gt/Publi/Libros/2013/ManualesIng/FluidosySensores-O.pdf. [Último acceso: 27 Octubre 2019].

[24] Universidad de Oviedo, «Sistemas Automáticos,» 2004. [En línea]. Available: http://isa.uniovi.es/~idiaz/SA/Teoria/04-05/SA.Sensores.pdf. [Último acceso: 21 Octubre 2019].

[25] N. Asuni, «Sensor Magnetico MC-38 para puertas y ventanas,» 2017. [En línea]. Available: http://www.electronicapty.com/sensor-magnetico-mc-38-detail?tmpl=component&format=pdf. [Último acceso: 19 Noviembre 2019].

[26] mh education, «Introducción a los sistemas operativos en red,» [En línea]. Available: https://www.mheducation.es/bcv/guide/capitulo/8448169468.pdf. [Último acceso: 26 Octubre 2019].

[27] S. Álvarez, B. Sergio y Á. Iván, «Sistemas operativos, bases de datos y servidores Web,» Febrero 2007. [En línea]. Available: http://ocw.usal.es/ensenanzas-tecnicas/taller-de-software-libre-para-el-diseno-de-materiales/contenidos/so_2.pdf. [Último acceso: 21 Octubre 2019].

[28] Universidad Autónoma De Ciudad Juárez, «Casa Inteligente y Segura,» 2011. [En línea]. Available: http://www.uacj.mx/DGDCDC/SP/Documents/RTI/RTI/4.%20Casa%20inteligente.pdf. [Último acceso: 1 Octubre 2019].

[29] Universidad de Oviedo, «El protocolo TCP/IP,» 2016. [En línea]. Available: http://www.isa.uniovi.es/docencia/redes/Apuntes/tema6.pdf. [Último acceso: 21 Octubre 2019].

[30] E. López, «Sobre Voltajes,causas y medidas de protección,» Diciembre 1997. [En línea]. Available: http://eprints.uanl.mx/502/1/1020123001.PDF. [Último acceso: 03 Noviembre 2019].

[31] Z. R. Vargas Cordero, «LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIACIENTÍFICA,» 2009. [En línea]. Available: https://www.redalyc.org/pdf/440/44015082010.pdf. [Último acceso: 10 Noviembre 2019].

[32] DIRECCIÓN DE GESTIÓN DE LA INFORMACIÓN Y PROCESOS, «PLAN ESTRATÉGICO DETECNOLOGÍAS DE LA INFORMACIÓN,» 2015. [En línea]. Available: https://servicios-it.epn.edu.ec/images/DGIP/Descargas/Plan_Estratefico_Tecnologias_de_la_Informacion_DGIP.pdf. [Último acceso: 16 Noviembre 2019].

[33] Electrònica Embajadores, «CATALOGODEROBOTICA,SENSORESYARDUINO,» 01 Abril 2016. [En línea]. Available: https://www.electronicaembajadores.com/Admin/Content/ovccz5rb.pdf. [Último acceso: 28 Noviembre 2019].

[34] ZKTeco Lationamérica , «ZK4500,» 2014. [En línea]. Available: https://plcmadrid.es/~documentacion/motorline/ZK4500.pdf. [Último acceso: 23 Noviembre 2019].

[35] Universidad de Cordova, «PROTECCIÓN DE LAS INSTALACIONES DE BAJA TENSIÓN,» [En línea]. Available: http://www.uco.es/~el1bumad/docencia/minas/ie06t4.pdf. [Último acceso: 24 Noviembre 2019].

[36] ElectronicaStore, «Bornera de 2 Pines (conector de bloque de 5.08 mm) 10 piezas,» [En línea]. Available: https://electronicastore.net/producto/bornera-de-2-pines-conector-de-bloque-de-5-08-mm-10-piezas/. [Último acceso: 26 Noviembre 2019].

[37] Diodes, «1N4001 - 1N4007 1.0A RECTIFIER,» Septiembre 2014. [En línea]. Available: https://www.diodes.com/assets/Datasheets/ds28002.pdf. [Último acceso: 27 Noviembre 2019].

[38] Onsemi, «TIP120, TIP121, TIP122(NPN); TIP125, TIP126,TIP127 (PNP),» Noviembre 2014. [En línea]. Available: https://www.onsemi.com/pub/Collateral/TIP120-D.PDF. [Último acceso: 27 Noviembre 2019].

[39] Instituto Nacional de Tecnologìas Educativas y de Fomración de Profesorado, «El transistor,» [En línea]. Available: http://roble.pntic.mec.es/jlop0164/archivos/el%20transistor.pdf. [Último acceso: 26 Noviembre 2019].

[40] Multicomp, «Electrolytic Capacitors,» 11 Junio 2011. [En línea]. Available: https://www.melopero.com/datasheets/47uF.pdf. [Último acceso: 27 Noviembre 2019].

[41] STANDARDS INFORMANT, «ANSI/TIA-568.1-D: Commercial Building Telecommunications Cabling,» 2019. [En línea]. Available: https://blog.siemon.com/standards/ansitia-568-c-1-commercial-building. [Último acceso: 06 octubre 2019].

6. ANEXOS

ANEXO 1: PLACA ARDUINO MEGA 2560

En la Figura 1, se muestra el diagrama de la placa Arduino Mega 2560

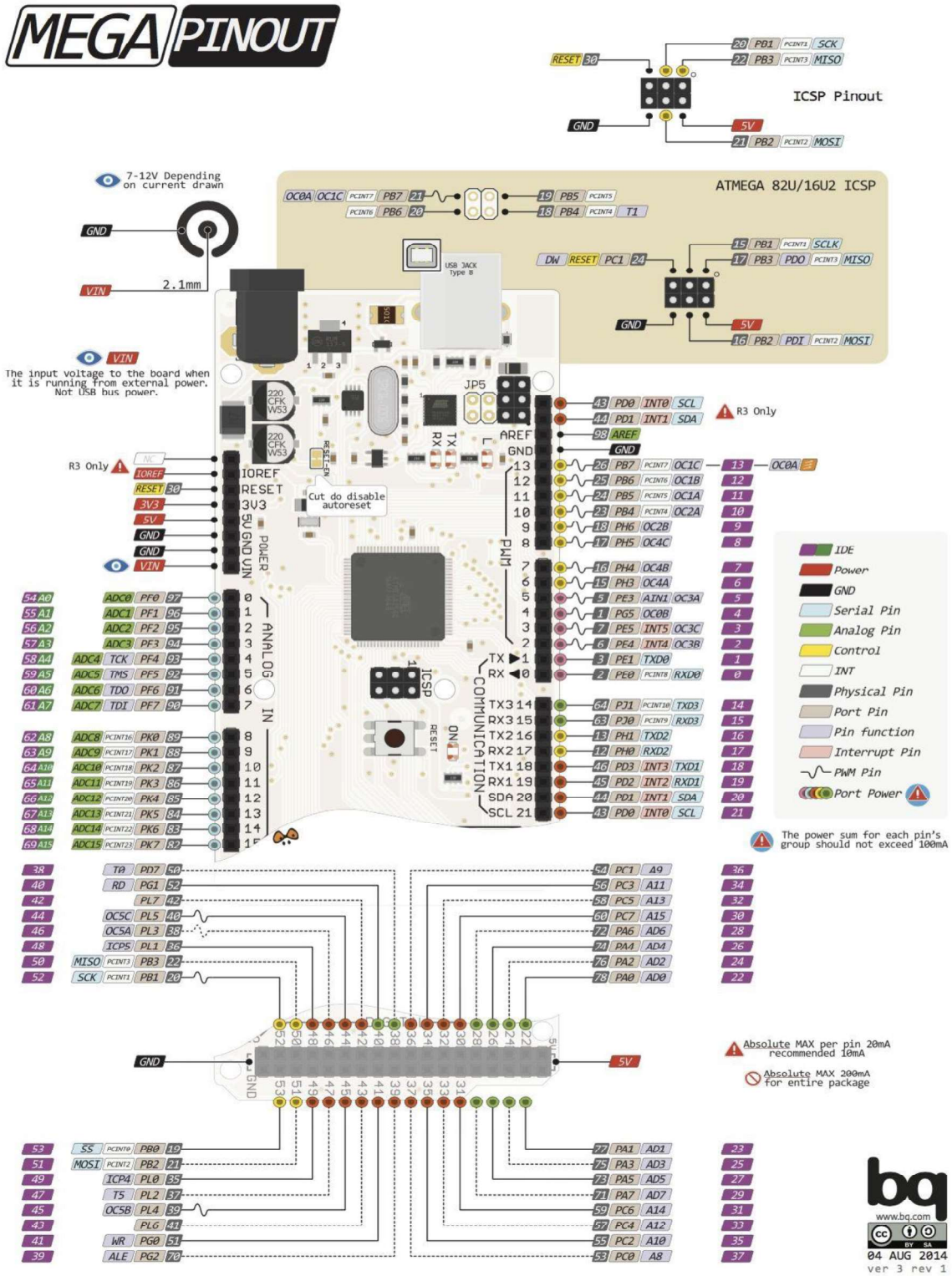


Figura 1 Diagrama de la placa Arduino Mega 2560

ANEXO 2: EIA/TIA T568 B

En la Figura 1, se puede visualizar el esquema de colores de la norma EIA/TIA T568 B para la conexión de los pares de par trenzado en el conector.

PIN	COLOR	PAR	FUNCION
1	Blanco Naranja	3	**TD+**
2	Naranja	3	**TD -**
3	Blanco Verde	2	**RD +**
4	Azul	1	Ninguna
5	Blanco Azul	1	Ninguna
6	Verde	2	**RD -**
7	Blanco Marrón	4	Ninguna
8	Marrón	4	Ninguna

TD: Transmisión de Datos.
RD: Recepción de Datos.

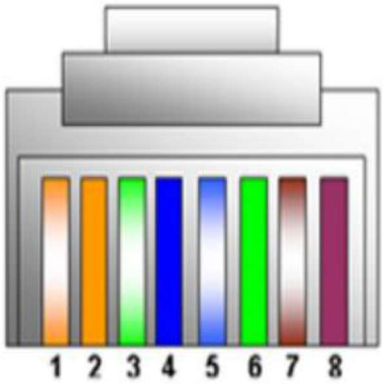
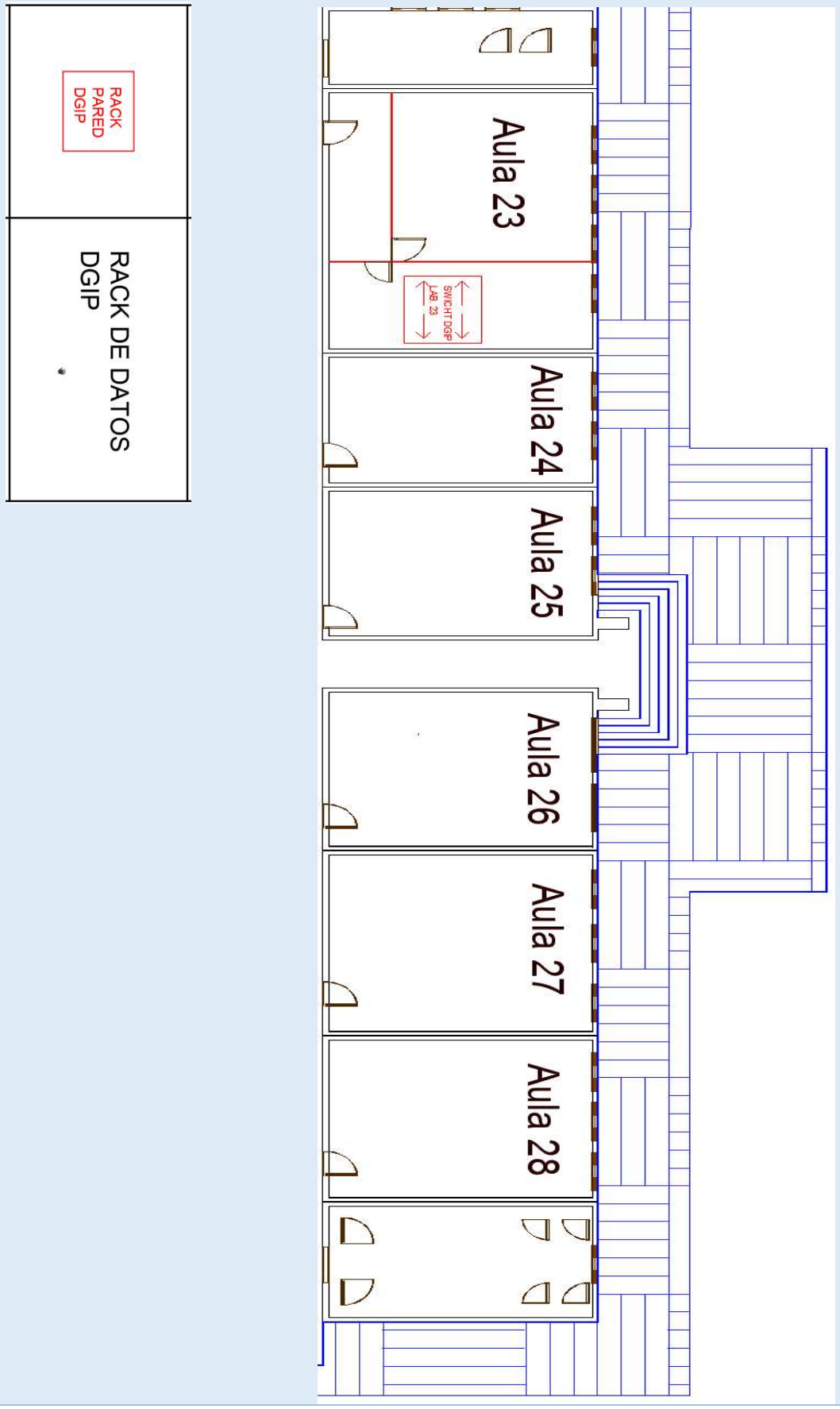


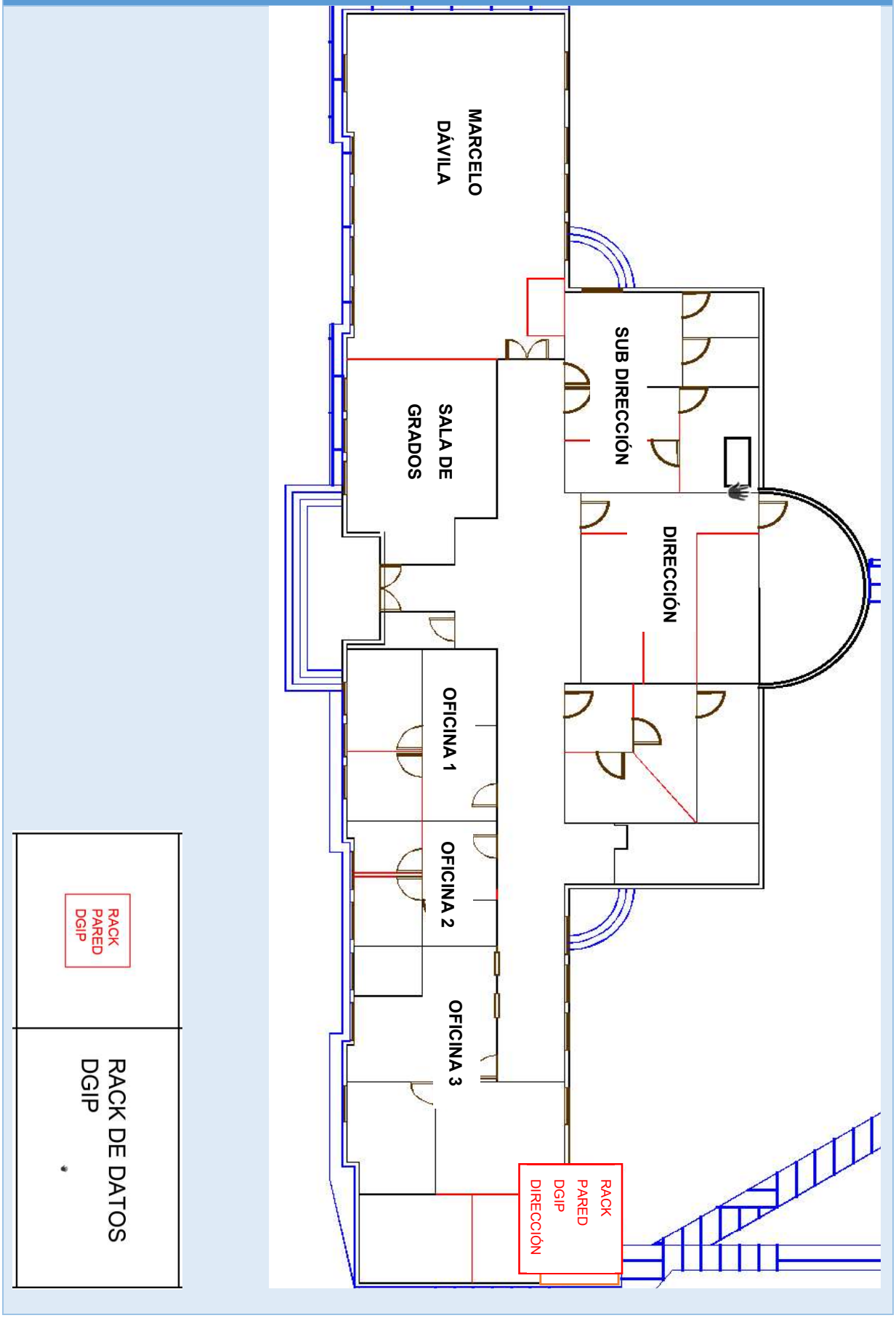
Figura 1 Norma de colores EIA/TIA T568-B [41].

ANEXO 3: PLANOS DE EQUIPOS DE LA DGIP EN LA ESFOT

SW disponible aula 23



SW disponible en la dirección



ANEXO 4: RED DE DATOS DEL SISTEMA

En la Figura 1, se puede visualizar el diagrama de red del sistema de automatización y control de acceso y la LAN de la EPN, se presentan direcciones IP distintas a las usadas por cuestiones de seguridad.

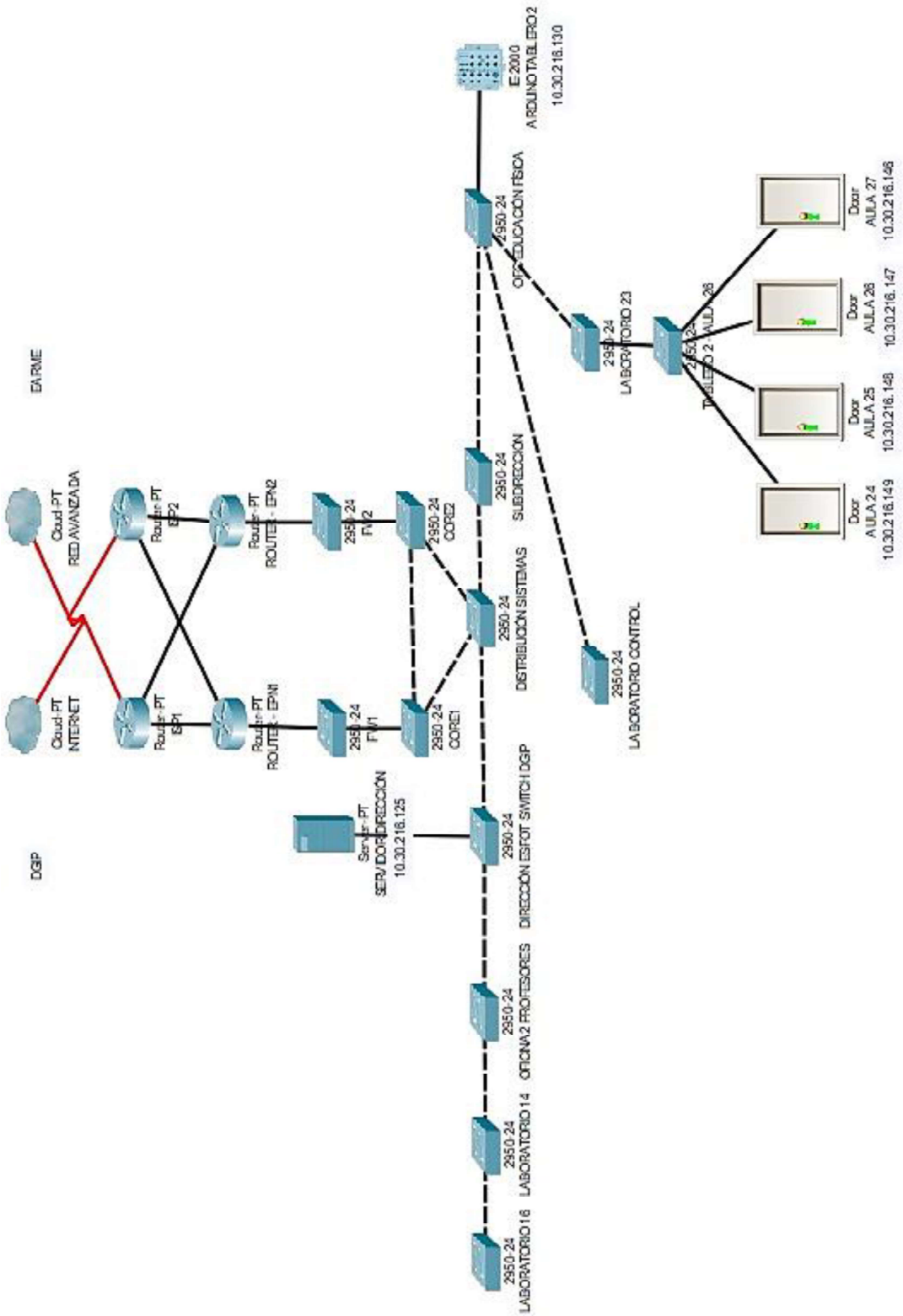
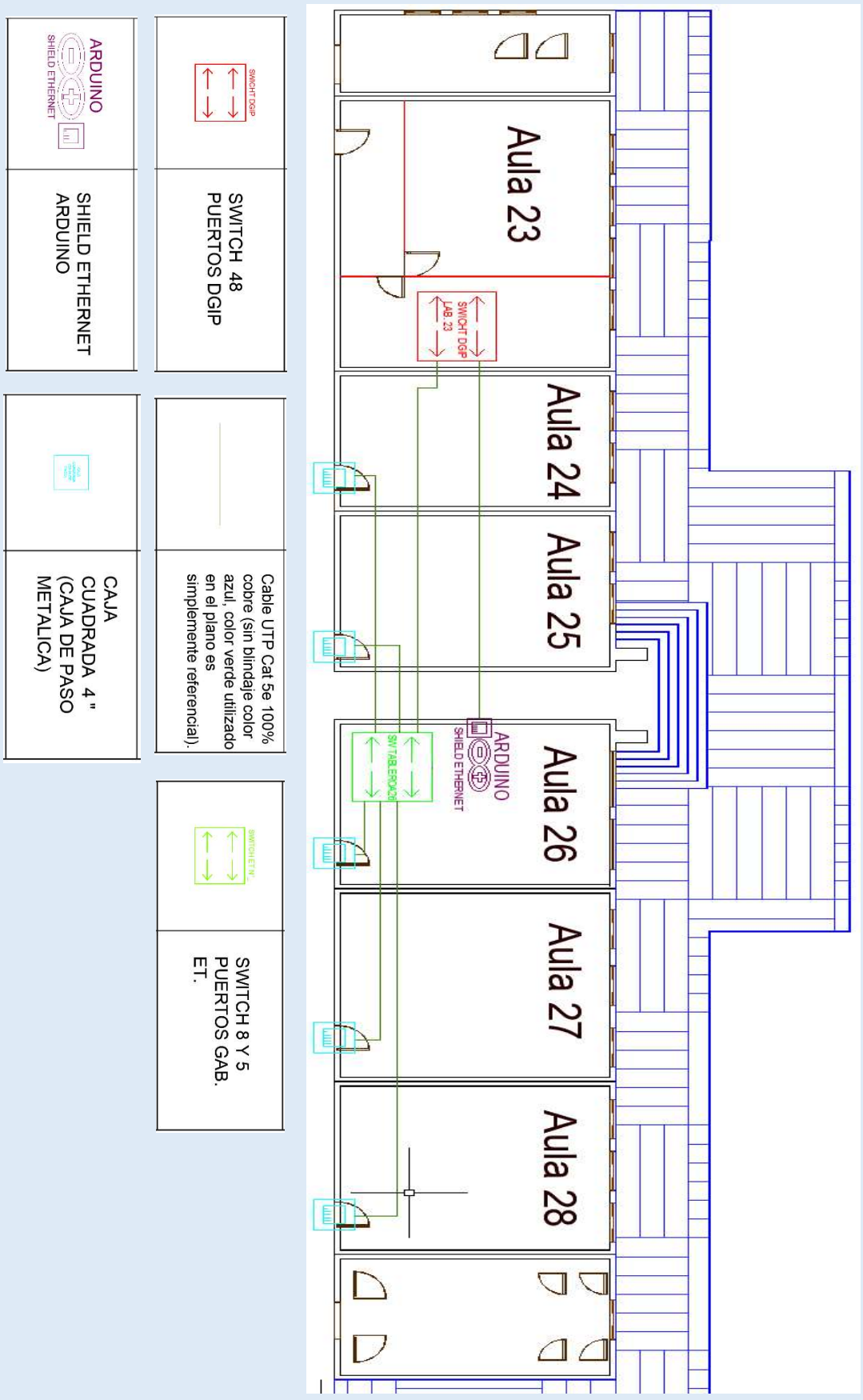


Figura 1 Diagrama de red del sistema de automatización y acceso biométrico.

ANEXO 5: PLANOS DE CABLEADO ESTRUCTURADO DE LAS AULAS 24, 25, 26 Y DIRECCIÓN DE LA ESFOT.

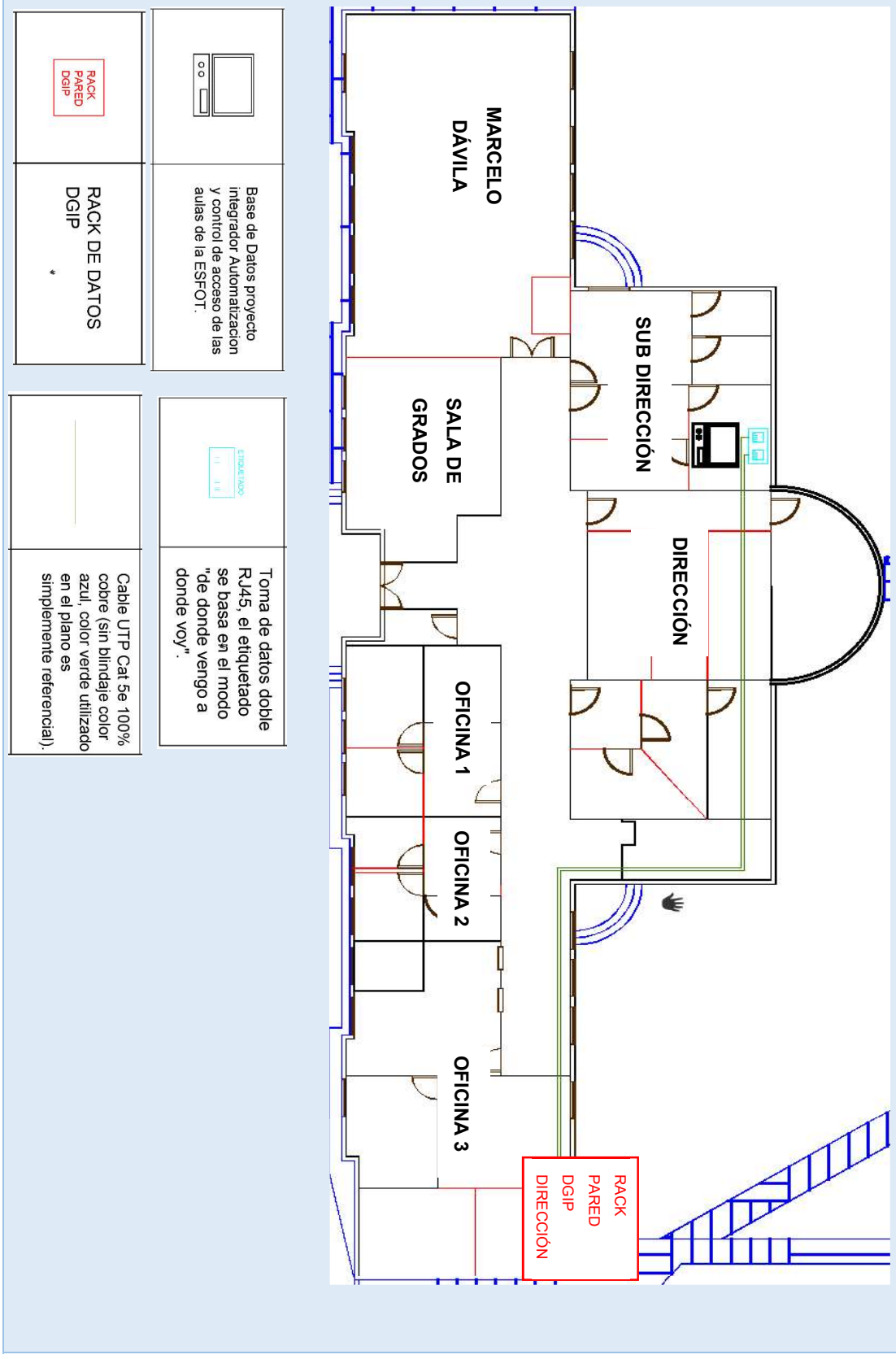
Cableado Estructurado plano 1

Aulas



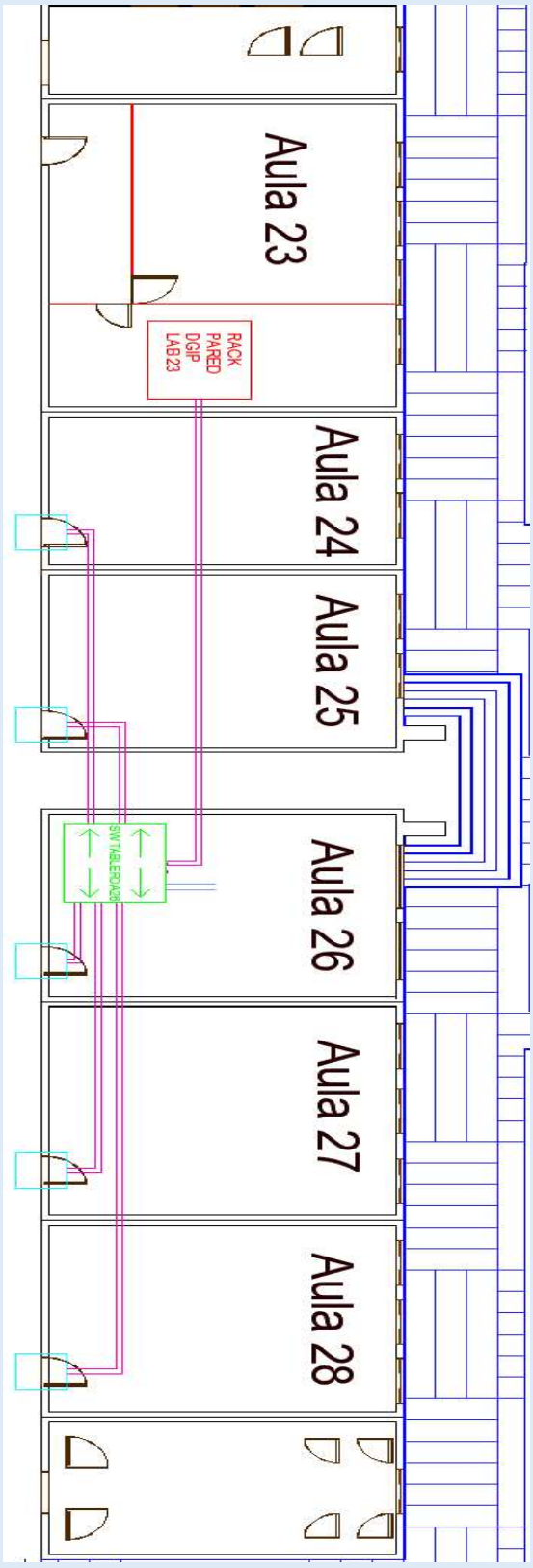
Cableado Estructurado plano 1

Dirección



Cableado Estructurado plano 2

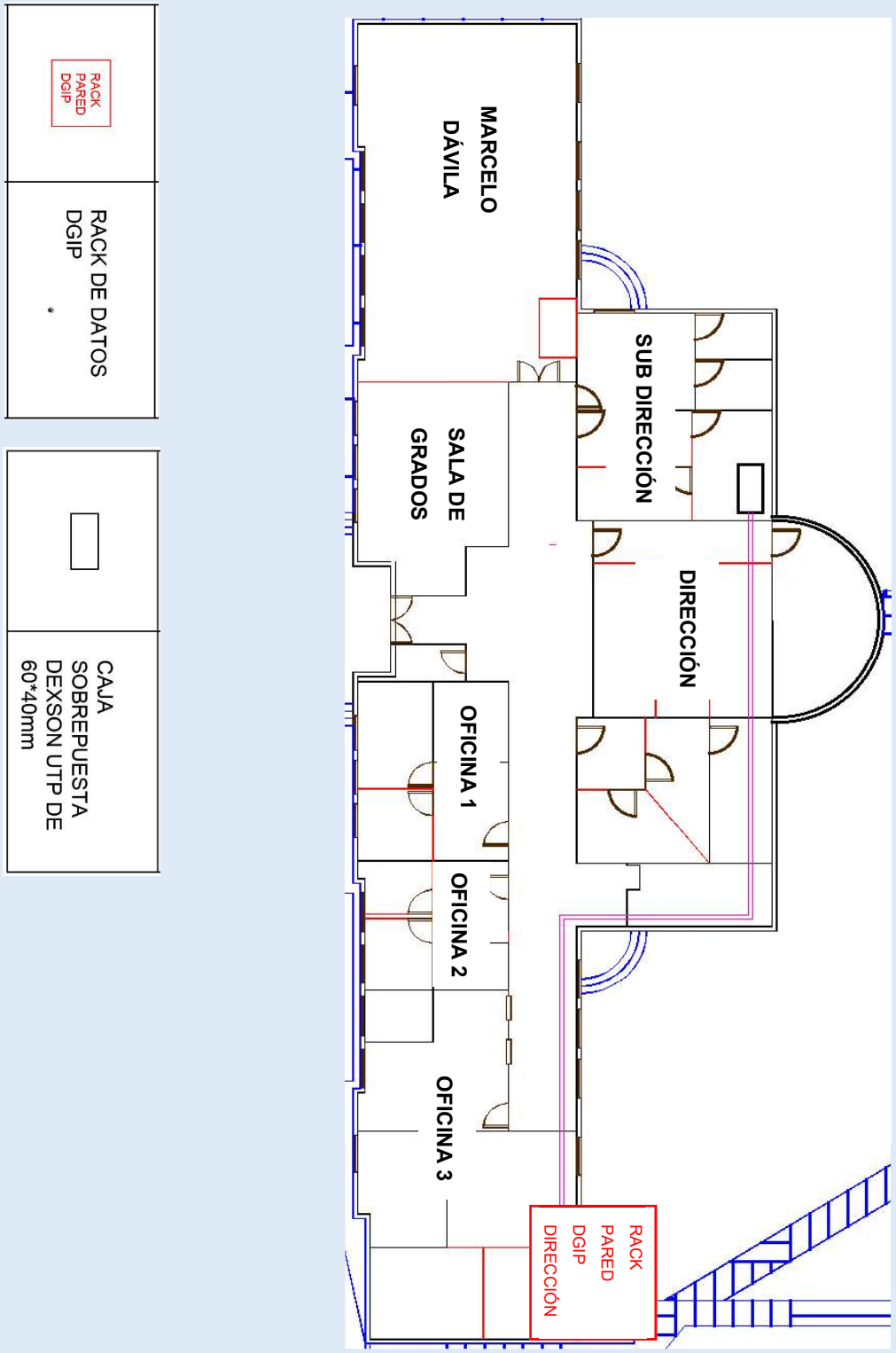
Aulas



RACK PARED DGIP	RACK DE DATOS DGIP
	MANGUERA FLEXIBLE bx DE $\frac{3}{4}$".
SWITCH 8 P/ N...	SWITCH 8 Y 5 PUERTOS GAB. ET.
	CAJA CUADRADA 4" (CAJA DE PASO METALICA)
	CANALETA PARA UTP DE 20*10*2000mm

Cableado Estructurado plano 2

Dirección



ANEXO 6: CÓDIGO ARDUINO

El código Arduino completo de la placa Arduino para el sistema de automatización y acceso biométrico de las aulas 24, 25 y 26, es el siguiente:

```
////////////////////////////////////TABLERO 4/////////////////////////////////////
#include <SPI.h>;                          // LIBRERÍA DE COMUNICACIÓN
#include <Ethernet.h>;                     // LIBRERÍA DE PROTOCOLOS ETHERNET
byte mac[] = { 0xDE, 0xED, 0xBE, 0xEF, 0xFE, 0xAD };// DIRECCIÓN FISICA DEL ARDUINO
byte ip[] = {172, 31, 118, 218};           // DIRECCIÓN LÓGICA DEL ARDUINO
byte gateway[] = {172, 31, 118, 193};      // DIRECCION LÓGICA DE LA PUERTA DE SALIDA
byte subnet[] = {255, 255, 255, 192};      // MÁSCARA DE SUBRED
EthernetServer server(80);                 // PUERTO DE COMUNICACIÒN WEB
String readString;                         // GUARDAR EN FORMA DE CADENA DE CARACTERES
                                           // LA INFORMACIÓN DEL BUFFER

////////////////////////////////////ASIGNACION DE VARIBLES Y PINES/////////////////////////////////////
//VALOR ACTUAL VENTANAS:
int ACT_VENT_26_1;int ACT_VENT_26_2;int ACT_VENT_25_1;int ACT_VENT_25_2;int ACT_VENT_24_1;int ACT_VENT_24_2;
//DEFINIR PINES VENTANAS:
int VENT_26_1=32;int VENT_26_2=34;int VENT_25_1=36;int VENT_25_2=38;int VENT_24_1=40;int VENT_24_2=42;
//VALOR ACTUAL PUERTAS:
int ACT_PU_26;int ACT_PU_25;int ACT_PU_24;
//VALOR ACTUAL FOCOS:
int ACT_FO_26;int ACT_FO_25;int ACT_FO_24;
//DEFINIR PINES PUERTAS:
int PU_26_1=56;int PU_25_1=57;int PU_24_1=58;
// SALIDA PUERTAS:
int E24P=62;int E25P=63;int E26P=64;
//SALIDA ON FOCOS:
int E26L=49;int E25L=47;int E24L=45;
//SALIDA OFF FOCOS:
int A26L=39;int A25L=37;int A24L=35;

void setup() {


////////////////////////////////////ASIGNACION ENTRADAS Y SALIDAS EN PULL UP/////////////////////////////////////
////////////////////////////////////PUERTAS/////////////////////////////////////
DDRF=0;             // ENTRADA MONITOREO PUERTAS AULAS 24, 25 Y 26
PORTF=255;          // PULL UP MONITOREO PUERTAS AULAS 24, 25 Y 26
DDRK=255;           // SALIDA CONTROL PUERTAS AULA 24, 25 Y 26
PORTK=255;          // PULL UP CONTROL PUERTAS AULAS 24, 25 Y 26
////////////////////////////////////FOCOS/////////////////////////////////////
pinMode(4, INPUT);    // ENTRADA MONITOREO FOCOS AULA 26
pinMode(5, INPUT);    // ENTRADA MONITOREO FOCOS AULA 25
pinMode(6, INPUT);    // ENTRADA MONITOREO FOCOS AULA 24
pinMode(49, OUTPUT);  // SALIDA CONTROL ON FOCOS AULA 26
pinMode(47, OUTPUT);  // SALIDA CONTROL ON FOCOS AULA 25
pinMode(45, OUTPUT);  // SALIDA CONTROL ON FOCOS AULA 24
pinMode(39, OUTPUT);  // SALIDA CONTROL OFF FOCOS AULA 26
pinMode(37, OUTPUT);  // SALIDA CONTROL OFF FOCOS AULA 25
pinMode(35, OUTPUT);  // SALIDA CONTROL OFF FOCOS AULA 24
digitalWrite(4,HIGH);  // PULL UP MONITOREO FOCOS AULA 26
digitalWrite(5,HIGH);  // PULL UP MONITOREO FOCOS AULA 25
digitalWrite(6,HIGH);  // PULL UP MONITOREO FOCOS AULA 24
digitalWrite(49,HIGH); // PULL UP CONTROL ON FOCOS AULA 26
digitalWrite(47,HIGH); // PULL UP CONTROL ON FOCOS AULA 25
```

```
digitalWrite(45,HIGH); // PULL UP CONTROL ON FOCOS AULA 24
digitalWrite(39,HIGH); // PULL UP CONTROL OFF FOCOS AULA 26
digitalWrite(37,HIGH); // PULL UP CONTROL OFF FOCOS AULA 25
digitalWrite(35,HIGH); // PULL UP CONTROL OFF FOCOS AULA 24
////////////////////////////////VENTANAS////////////////////////////////
pinMode(32, INPUT);    // ENTRADA MONITOREO VENTANA 1 AULA 26
pinMode(34, INPUT);    // ENTRADA MONITOREO VENTANA 2 AULA 26
pinMode(36, INPUT);    // ENTRADA MONITOREO VENTANA 1 AULA 25
pinMode(38, INPUT);    // ENTRADA MONITOREO VENTANA 2 AULA 25
pinMode(40, INPUT);    // ENTRADA MONITOREO VENTANA 1 AULA 24
pinMode(42, INPUT);    // ENTRADA MONITOREO VENTANA 2 AULA 24
digitalWrite(32,HIGH); // PULL UP MONITOREO VENTANA 1 AULA 26
digitalWrite(34,HIGH); // PULL UP MONITOREO VENTANA 2 AULA 26
digitalWrite(36,HIGH); // PULL UP MONITOREO VENTANA 1 AULA 25
digitalWrite(38,HIGH); // PULL UP MONITOREO VENTANA 2 AULA 25
digitalWrite(40,HIGH); // PULL UP MONITOREO VENTANA 1 AULA 24
digitalWrite(42,HIGH); // PULL UP MONITOREO VENTANA 2 AULA 24
////////////////////////////////CONFIGURACION DEL TIPO DE COMUNICACION////////////////////////////////
Serial.begin(9600);                    // VELOCIDAD DE DATOS SERIALES
Ethernet.begin(mac, ip, gateway, subnet); // INICIA LA COMUNICACIÓN ETHERNET
server.begin();                        // CONEXION AL SERVIDOR
Serial.print("El Servidor es: ");
Serial.println(Ethernet.localIP());}
void loop() {
////////////////////////////////ARDUINO COMO CLIENTE Y CONEXION AL SERVIDOR PARA ENVIAR Y RECIBIR DATOS////////////////////////
EthernetClient cliente = server.available(); // ARDUINO COMO CLIENTE CON EL SERVIDOR
if(cliente){
  while(cliente.connected()){
    if (cliente.available()){              // ARDUINO SE CONECTA COMO CLIENTE
      char c = cliente.read();             // DATOS DEL CLIENTE SE GUARDA EN LA VARIABLE C

    if (readString.length()<100){          // LIMITE DE DATOS
      readString += c;                     // VALOR DE C SE GUARDA EN EL BUFFER EN FORMA DE CARACTERES
      }
    if (c == '\n'){
      Serial.println(readString);
      cliente.println("HTTP/1.1 200 OK");
      cliente.println("Content-Type: text/html");
      cliente.println("Connection: close");
cliente.println();
cliente.println("<HTML>");
cliente.println("<HEAD>");
cliente.println("<TITLE> PRUEBA ARDUINO </TITLE>");
cliente.println("</HEAD>");
cliente.println("<BODY>");
//////////////////////////////// MONITOREO ////////////////////////////////////////////////
////////////////////////////////PUERTAS/////////////////////////////////////////////
//PUERTA 26
ACT_PU_26 = digitalRead (56); //GUARDA EL VALOR DEL PIN 56 EN LA VARIABLE ACT_PU_26
  cliente.print("26P:");      //ENVIA AL SERVIDOR CARACTER TEXTO 26P:
  cliente.print(ACT_PU_26);   //ENVIA AL SERVIDOR CARACTER DE LA VARIABLE
  cliente.print(",");         //ENVIA AL SERVIDOR CARACTER TEXTO ,
//PUERTA 25
ACT_PU_25 = digitalRead (57);
  cliente.print("25P:");
  cliente.print(ACT_PU_25);
  cliente.print(",");
```

```
//PUERTA 24
ACT_PU_24 = digitalRead (58);
  cliente.print("24P:");
  cliente.print(ACT_PU_24);
  cliente.print("|");
////////////////////////////////FOCOS////////////////////////////////////////////////
//FOCOS AULA 26:
ACT_FO_26 = digitalRead (7); //GUARDA EL VALOR DEL PIN 56 EN LA VARIABLE ACT_FO_26
  cliente.print("26L:");     //ENVIA AL SERVIDOR CARACTER TEXTO 26L:
  cliente.print(ACT_FO_26);  //ENVIA AL SERVIDOR CARACTER DE LA VARIABLE
  cliente.print(",");        //ENVIA AL SERVIDOR CARACTER TEXTO ,
//FOCOS AULA 25:
ACT_FO_25 = digitalRead (5);
  cliente.print("25L:");
  cliente.print(ACT_FO_25);
  cliente.print(",");
//FOCOS AULA 24:
ACT_FO_24 = digitalRead (6);
  cliente.print("24L:");
  cliente.print(ACT_FO_24);
  cliente.print("|");
////////////////////////////////////VENTANAS////////////////////////////////////////
//VENTANAS AULA 26:
//VENTANA 1:
ACT_VENT_26_1 = digitalRead (32); //GUARDA EL VALOR DEL PIN 56 EN LA VARIABLE ACT_VENT_26_1
  cliente.print("26V1:");         //ENVIA AL SERVIDOR CARACTER TEXTO 26V1:
  cliente.print(ACT_VENT_26_1);   //ENVIA AL SERVIDOR CARACTER DE LA VARIABLE
  cliente.print(",");             //ENVIA AL SERVIDOR CARACTER TEXTO ,
//VENTANA 2:
ACT_VENT_26_2 = digitalRead (34);
  cliente.print("26V2:");
  cliente.print(ACT_VENT_26_2);
  cliente.print(",");
//VENTANAS AULA 25:
//VENTANA 1:
ACT_VENT_25_1 = digitalRead (36);
  cliente.print("25V1:");
  cliente.print(ACT_VENT_25_1);
  cliente.print(",");
//VENTANA 2:
ACT_VENT_25_2 = digitalRead (38);
  cliente.print("25V2:");
  cliente.print(ACT_VENT_25_2);
  cliente.print(",");
//VENTANAS AULA 24:
//VENTANA 1:
ACT_VENT_24_1 = digitalRead (40);
  cliente.print("24V1:");
  cliente.print(ACT_VENT_24_1);
  cliente.print(",");
//VENTANA 2:
ACT_VENT_24_2 = digitalRead (42);
  cliente.print("24V2:");
  cliente.print(ACT_VENT_24_2);
cliente.println("</BODY>");
cliente.println("</HTML>");
delay(1);
cliente.stop();                 //PARA LA COMUNICACION DE ENVIO DE DATOS AL SERVIDOR
```

```
//////////////////////////////////// CONTROL ////////////////////////////////////////////////////
//////////////////////////////APERTURA PUERTAS/////////////////////////////////////
if (readString.indexOf("?E26P")>0){   //LEE EN EL GRUPO DE CARACTERES, EL TEXTO ?E26P
   digitalWrite (E26P,LOW);          //SI ESTÁ EL CARACTER, ABRE LA PUERTA DEL AULA 26
    delay(1000);
    digitalWrite (E26P,HIGH);
   }
if (readString.indexOf("?E25P")>0){
   digitalWrite (E25P,LOW);
    delay(1000);
    digitalWrite (E25P,HIGH);
   }
if (readString.indexOf("?E24P")>0){
    digitalWrite (E24P,LOW);
    delay(1000);
    digitalWrite (E24P,HIGH);
 }
//////////////////////////////ENCENDIDO FOCOS/////////////////////////////////////
if (readString.indexOf("?E26L")>0){   //LEE EN EL GRUPO DE CARACTERES, EL TEXTO ?E26L
    digitalWrite (E26L,LOW);          //SI ESTÁ EL CARACTER, ENCIENDE LOS FOCOS DEL AULA 26
    delay(1000);
    digitalWrite (E26L,HIGH);
   }
if (readString.indexOf("?E25L")>0){
    digitalWrite (E25L,LOW);
    delay(1000);
    digitalWrite (E25L,HIGH);
   }
if (readString.indexOf("?E24L")>0){
    digitalWrite (E24L,LOW);
    delay(1000);
    digitalWrite (E24L,HIGH);
 }
//////////////////////////////APAGADO FOCOS/////////////////////////////////////
if (readString.indexOf("?A26L")>0){   //LEE EN EL GRUPO DE CARACTERES, EL TEXTO ?A26L
    digitalWrite (A26L,LOW);          //SI ESTÁ EL CARACTER, APAGA LOS FOCOS DEL AULA 26
    delay(1000);
    digitalWrite (A26L,HIGH);
   }
if (readString.indexOf("?A25L")>0){
    digitalWrite (A25L,LOW);
    delay(1000);
    digitalWrite (A25L,HIGH);
   }
if (readString.indexOf("?A24L")>0){
    digitalWrite (A24L,LOW);
    delay(1000);
    digitalWrite (A24L,HIGH);
 }

readString="";
     } } } } }
```

ANEXO 7: MANUAL DE MANTENIMIENTO

- **Introducción**

El sistema de automatización implementado en las aulas de la ESFOT (Escuela de Formación Tecnólogos) provee varias características como: acceso seguro mediante datos biométricos, monitoreo y control de ventanas, puertas y luminarias. Dichas herramientas se pueden utilizar a través de una aplicativo móvil y página web.
El sistema funciona a través de tableros electrónicos y mecánicos controlados por un dispositivo embebido, un Arduino MEGA 2560, el cual provee las características antes mencionadas a varias aulas, además utiliza una red de alimentación eléctrica y de comunicación de datos.

Así pues, es de capital importancia que se lleve a cabo un programa de mantenimiento acorde a la importancia y tiempo de vida útil de cada instalación en particular, como: eléctrica, electrónica, electromecánica y de cableado estructurado.

- **Cuadro de mantenimiento**

En la Tabla 1, se puede observar las diferentes áreas, tiempos de evaluación y procedimientos que se deben ejecutar como planes de mantenimiento para corregir inconvenientes con el sistema de automatización de las aulas de la ESFOT.

Tabla 1 Programa de mantenimiento del sistema.

ESFOT ESCUELA DE FORMACION DE TECNOLOGOS	CUADRO DE MANTENIMIENTO DEL SISTEMA DE AUTOMATIZACIÓN DE LAS AULAS DE LA ESFOT			ESCUELA POLITÉCNICA NACIONAL
PERIODO	**ÁREA**	**ELEMENTO**	**ACTIVIDAD**	**PROCEDIMIENTO**
6 meses	Eléctrico	Fuente de alimentación del tablero	- Limpieza	- Quitar la alimentación para evitar accidentes. - Limpiar la fuente utilizando una brocha pequeña con el fin de eliminar polvo existente.
			- Voltaje	- Tomar los equipos de medición, multímetro. - Configurar el equipo con el rango y parámetro de voltaje. - Colocar los cables del multímetro en la salida de la fuente. - Observar el valor medido, 12 voltios.
6 meses		Regulador de voltaje	- Limpieza	- Quitar la alimentación para evitar accidentes. - Limpiar la fuente utilizando una brocha pequeña con el fin de eliminar polvo existente.
			- Voltaje	- Tomar los equipos de medición, multímetro. - Configurar el equipo con el rango y parámetro de voltaje. - Colocar los cables del multímetro en la salida de la fuente. - Medir el valor debe ser 110 voltios.
6 meses	Electromecánico	Chapas Eléctricas	- Limpieza	- Usar un paño y sumergirlo en un poco de alcohol. - Pasarlo por el interior de la cerradura. - Lubricar cada parte de la cerradura con un aerosol en spray, no utilizar lubricantes líquidos.
6 meses		Placas de protección de las chapas	- Limpieza	- Con una pequeña brocha limpiar el polvo de las placas de protección de las chapas y realizar una inspección visual de la misma.
6 meses	Electrónico	Arduino MEGA 2560	- Limpieza	- Apagar la fuente de alimentación del Arduino Mega. - Obtener un equipo con aire comprimido. - Abrir el tablero EM. - Limpiar el Arduino y la *Shield Ethernet* con aire comprimido. - Energizar el Arduino.

				- Reiniciar el Arduino con el botón en la parte de encima del tablero. - Cerrar el tablero EM.
6 meses			- Verificación de conexiones	- Apagar la fuente de alimentación del Arduino Mega. - Observar el diagrama de conexiones ubicado en el tablero. - Verificar la correcta conexión entre los pines y cables del tablero. - Energizar el Arduino. - Reiniciar el Arduino con el botón en la parte de encima del tablero.
6 meses		*Shield Ethernet* Arduino	- Verificar conexiones	- Apagar la alimentación al Arduino. - Abrir el tablero de EM. - Observar el diagrama de conexiones ubicado en el tablero. - Verificar la correcta conexión entre los pines y cables del tablero. - Energizar el Arduino. - Reiniciar el Arduino con el botón en la parte de encima del tablero. - Cerrar el tablero EM.
6 meses		Biométrico ZKTeco	- Limpieza	- Apagar el sistema de biométricos. - Obtener las herramientas necesarias para la limpieza del biométrico y del lector de huellas, un paño, poco de alcohol o limpiador de vidrio y cinta adhesiva. - Humedecer el paño en alcohol o en el limpiador de vidrio. - Limpiar el exterior del biométrico con el paño. - Aplicar sobre la ventana del lector el lado engomado de una cinta adhesiva transparente, y luego retirarla. - Realizar este proceso con los 19 biométricos respectivas de las aulas de la ESFOT. - Encender el sistema de biométricos.
6 meses			- Funcionamiento	- Observar el manual del biométrico. - Verificar la comunicación IP de cada biométrico. - Verificar el tiempo de 1s en el control de acceso a las puertas de cada aula. - Verificar el funcionamiento de todos los biométricos en el *software* de ZKteco en el servidor.
6 meses	Cableado estructurado	*Switch* Dlink	- Funcionamiento	- Abrir el tablero ET. - Verificar los LEDS indicadores que estén linkeando en función de los puertos conectados al *switch*. - Reiniciar el *switch* desconectando y conectando el cable de poder al regulador de voltaje. - Cerrar el tablero ET.
6 meses		Servidor	- Hardware	- Apagar y desconectar el servidor. - Tocar una superficie metálica para descargarse de electricidad estática. - Limpiar por dentro con algún producto líquido o una espuma para eliminar el polvo y la basura acumulada. - Conectar y encender el servidor.
			- *Software*	- Actualizar *software* relacionados al sistema, antivirus y *firewall* del servidor. - Realizar respaldos de la base de datos, registros y el propio sistema operativo. - Verificar el correcto funcionamiento de cada programa o *software* del sistema.

- **Listado de verificación del sistema**

En la Tabla 2, se puede visualizar un formato para realizar la verificación del mantenimiento del sistema de automatización de las aulas de la ESFOT, el cual debe ser ejecutado por personas técnicas cada 6 meses o inicio de un nuevo semestre, si hay algún problema con las acciones mostradas en el listado deben ser corregidas con el código de solución en la Tabla 3.

Tabla 2 Listado de verificación del sistema.

ESFOT ESCUELA DE FORMACION DE TECNOLOGOS	**LISTADO DE VERIFICACIÓN DEL SISTEMA DE AUTOMATIZACIÓN DE LAS AULAS DE LA ESFOT**	ESCUELA POLITÉCNICA NACIONAL
Nombre del técnico:		
Tablero No:		
Fecha de revisión:		

Área	**Elemento**	**Acciones**	**SI**	**NO**	**Código del listado de Soluciones**
Eléctrico	Fuente de alimentación del tablero	Limpieza de la fuente de alimentación y reajuste de conexión.			E.1.
		Voltaje de salida de la fuente de alimentación con 12 voltios aproximados.			E.2
	Regulador de voltaje	Limpieza en el regulador de voltaje.			E.3
		Voltaje de salida en el regulador de voltaje con 110 Voltios aproximados.			E.4
	Botoneras	Limpieza de botoneras.			E.5
		Prueba de funcionamiento, accionamiento.			E.6
Electromecánico	Contactores o relés	Limpieza.			M.1
		Reajuste de conexiones y prueba de funcionamiento.			M.2
	Chapas Eléctricas	Limpieza (interna, externa) y ajuste de borneras.			M.3
		Prueba de funcionamiento.			M.4
	Placas de protección de las chapas	Limpieza.			M.5
		Prueba de voltajes, debe existir aproximadamente 12v a la salida de la placa.			M.6
	Sensores magnéticos	Limpieza.			M.7
		Estado de conexiones y calibración de distancia entre los mismos.			M.8

Electrónico	Arduino Mega 2560	Limpieza de la placa de Arduino Mega 2560.			N.1
		LED indicador *ON* del Arduino encendido.			N.2
		Conexiones correctas de los pines.			N.3
	Shield Ethernet Arduino	Limpieza de la *Shield Ethernet.*			N.1
		LED indicador PWR de la *Shield* encendido.			N.4
		LED indicador *LINK* de la *Shield* encendido.			N.5
		LED indicador 100M de la *Shield* encendido.			N.5
		LED indicador FULLD de la *Shield* encendido.			N.5
		LED indicador RX de la *Shield* linkea.			N.5
		LED indicador TX de la *Shield* linkea.			N.5
	Lector biométrico ZKTeco	Limpieza del biométrico de cada aula.			N.6
		Tiempo de control de acceso de 1 segundo.			N.7
		Direccionamiento IP correcto en cada biométrico.			N.8
		Funcionamiento de cada biométrico en el *software* del servidor.			N.9
Cableado estructurado	*Switch* Dlink	LEDS indicadores encendidos en función del puerto conectado.			R.1
	Servidor	Limpieza del *hardware.*			R.2
		Actualizaciones del sistema operativo.			R.3
		Actualizaciones del antivirus.			R.4
		Actualización del *software* ZKTeco.			R.5

- **Listado de soluciones**

En la Tabla 3, se puede visualizar el listado de soluciones que se deben ejecutar cuando se encuentre un inconveniente en el listado de verificación del sistema de mantenimiento de automatización de las aulas de la ESFOT de la Tabla 2.

Tabla 3 Listado de soluciones para problemas técnicos del sistema.

ESFOT ESCUELA DE FORMACION DE TECNOLOGOS	**LISTADO DE SOLUCIONES**	ESCUELA POLITÉCNICA NACIONAL

Área	**Código**	**Solución**
Eléctrico	E.1.	- Quitar la alimentación para evitar accidentes. - Limpiar la fuente utilizando una brocha pequeña con el fin de eliminar polvo existente.
	E.2	- Tomar los equipos de medición, multímetro. - Configurar el equipo con el rango y parámetro de voltaje. - Colocar los cables del multímetro en la salida de la fuente, observar el valor medido, 12 voltios.
	E.3	- Quitar la alimentación para evitar accidentes. - Limpiar la fuente utilizando una brocha pequeña con el fin de eliminar polvo existente.

	E.4	- Tomar los equipos de medición, multímetro. - Configurar el equipo con el rango y parámetro de voltaje. - Colocar los cables del multímetro en la salida de la fuente. - Observar el valor medido, 110 voltios.
	E.5	- Quitar la energía del sistema. - Desarmar la botonera utilizando un desarmador tipo estrella. - Limpiar con una pequeña brocha el interior de la botonera con el fin de quitar suciedad. - Cerrar la botonera con el desarmador tipo estrella. - Energizar el sistema.
	E.6	- Se puede deber al estado de botoneras causado por polvo o resortes quebrados, desarmar la botonera como se explica en E.5 y proceder al cambio de resortes.
Electromecánico	M.1	- Con una brocha pequeña limpiar hasta retirar todo el polvo existente.
	M.2	- Se deberá sacar el relé y con un multímetro digital se probará la resistencia entre cada polo del relé y sus contactos, es decir, todos los conectados en NC deberán leer 0 ohms en el polo correspondiente y todos los NO deberán leer resistencia infinita el polo correspondiente. - Se alimenta el relé de acuerdo al nominal de la bobina, hay que tener en cuenta la polaridad de la alimentación, cuando el relé este alimentado se escuchara un clic.
	M.3	- Usar un paño seco el cual haya sido sumergido en un poco de alcohol, considerar que tampoco será necesario que se humedezca mucho el paño, pasarlo por la cerradura (el interior) para que se elimine todo el polvo que tenga dentro de la cerradura una vez realizado esto lubricar cada parte de la cerradura con un aerosol en spray.
	M.4	- Chequear el bobinado de la chapa ya que es posible que se haya quemado por un sobre voltaje, de ser este el caso reemplazar dicho bobinado. - Verificar si los biométricos están energizados, de no ser así energizarlos ya que las placas de las chapas están alimentadas del mismo punto de los biométricos.
	M.5	- Con una brocha pequeña limpiar hasta retirar todo el polvo existente.
	M.6	- Verificar la alimentación con un multímetro, esta medición tiene que dar 12v de entrada y 12v de salida, al ser una placa de protección se debe verificar el estado de los diodos, en el caso de estar quemados reemplazarlos.
	M.7	- Con una brocha pequeña limpiar hasta retirar todo el polvo existente.
	M.8	- La distancia a la que trabajan de forma óptima los sensores es de 0.5cm, una vez calibrada esta distancia monitorear el correcto funcionamiento del mismo mediante la interface.
Electrónico	N.1	- Apagar la fuente de alimentación del Arduino Mega. - Obtener un equipo con aire comprimido. - Abrir el tablero EM. - Limpiar el Arduino y la *Shield Ethernet* con aire comprimido. - Energizar el Arduino. - Reiniciar el Arduino con el botón en la parte encima del tablero. - Cerrar el tablero EM.
	N.2	- Reiniciar el Arduino de la parte superior del tablero EM. - Reiniciar el Arduino desde el botón *RESET* de la placa.
	N.3	- Apagar la fuente de alimentación del Arduino Mega. - Observar el diagrama de conexiones ubicado en el tablero. - Verificar la correcta conexión entre los pines y cables del tablero. - Energizar el Arduino. - Reiniciar el Arduino con el botón en la parte encima del tablero.
	N.4	- Reiniciar el Arduino de la parte superior del tablero EM. - Reiniciar el Arduino desde el botón *RESET* de la placa.

	N.5	- Reiniciar el Arduino de la parte superior del tablero EM. - Reiniciar el Arduino desde el botón *RESET* de la placa. - Desconectar y conectar el cable *Ethernet* de la *Shield*.
	N.6	- Apagar el sistema de biométricos. - Obtener las herramientas necesarias para la limpieza del biométrico y del lector de huellas, un paño, poco de alcohol o limpiador de vidrio y cinta adhesiva. - Humedecer el paño en alcohol o en el limpiador de vidrio. - Limpiar el exterior del biométrico con el paño. - Aplicar sobre la ventana del lector el lado engomado de una cinta adhesiva transparente, y luego retirarla. - Realizar este proceso con los 19 biométricos respectiva de cada aula de la ESFOT. - Encender el sistema de biométricos.
	N.7	- Verificar el manual de uso del biométrico. - Ingresar a la configuración del biométrico en modo administrador. - Cambiar el control de acceso de 1 segundo.
	N.8	- Verificar el manual de uso del biométrico. - Ingresar a la configuración del biométrico en modo administrador. - Cambiar el direccionamiento IP de acuerdo a la red del sistema de automatización.
	N.9	- Verificar que los biométricos estén encendidos. - Verificar la configuración de direccionamiento y contraseña de comunicación. - Reiniciar el servidor y *software* ZKTeco.
Cableado estructurado	R.1	- Verificar los LEDS indicadores que estén linkeando en función de los puertos conectados al *switch*. - Reiniciar el *switch* desconectando y conectando el cable de poder al regulador de voltaje.
	R.2	- Apagar y desconectar el servidor. - Tocar una superficie metálica para descargarse de electricidad estática. - Limpiar por dentro con algún producto líquido o una espuma para eliminar el polvo y la basura acumulada. - Conectar y encender el servidor.
	R.3	- Abrir Windows *Update* del servidor. - Buscar actualizaciones recientes del sistema operativo. - Descargar las actualizaciones. - Instalar las actualizaciones. - Reiniciar el servidor.
	R.4	- Abrir el antivirus del sistema operativo. - Ingresar a configuraciones. - Actualizar la base de registros del antivirus.
	R,5	- Observar el manual de uso del *software* ZKTeco. - Realizar un respaldo de la base de datos del sistema. - Ingresar a la página oficial del *software* ZKTeco. - Descargar la última versión del sistema. - Instalar en el servidor. - Ingresar la base de datos de respaldo al nuevo sistema.

- **Problemas comunes**

En la Tabla 4, se puede verificar algunos problemas comunes que se generan fuera del tiempo de mantenimiento de manera inoportuna, por lo cual se cita las posibles soluciones correctivas.

Tabla 4 Problemas comunes que se generan en el sistema.

ESFOT ESCUELA DE FORMACION DE TECNOLOGOS	PROBLEMAS COMUNES	ESCUE POLITE NACIO
Problema	**Causas posibles**	**Solución**
Tablero no enciende	- Regulador de voltaje en mal estado	- Verificar el voltaje de entrada al regulador y cada voltaje de salida el cual tiene que ser de 110v , si la salida al tablero no marca dicho voltaje cambiar el lugar de conexión en el mismo regulador.
Luminarias no funcionan	- Cableado en mal estado	- Guiarse en planos de cableado estructurado con el fin de detectar alguna anomalía (cables desconectados o rotos) en conexión de relés.
	- Lámparas quemadas	- Verificar estado de lámparas y cambiar si están quemadas.
	- Tablero des energizado	- Verificar que el regulador de voltaje este encendido.
	- Arduino con errores	- Verificar el Arduino encendido - Verificar las conexiones de las luminarias en los pines correctos del Arduino de acuerdo al diagrama en el tablero
No se abren las puertas	- Placa de chapas des energizada.	- Verificar si los biométricos están energizados, de no ser así energizarlos ya que las placas de las chapas están alimentadas del mismo punto de los biométricos
	- Chapa quemada por sobrevoltaje	- Cambiar el bobinado de la chapa. - Reemplazar chapa.
	- Arduino con errores	- Verificar el Arduino encendido - Verificar las conexiones de las puertas en los pines correctos del Arduino de acuerdo al diagrama en el tablero
Chapa se abre, pero no se puede cerrar	- Botón del abridor está hundido.	- Este botón es para que no se pueda volver a abrir sin que se accione la bobina del abridor. - El botoncillo debe de estar hundido cuando la puerta está cerrada. Cuando se libera el abridor y se abre la puerta, sale para afuera, pero al cerrar de nuevo, debe ser pisado por el "resbalón" de la puerta, para quedar la puerta cerrada. - Si el dispositivo está bien, vea si el "resbalón", no queda encallado y no pisa el botoncillo hasta el fondo, bien sea porque no sale del todo o porque la distancia entre cerradura y abridor es demasiado amplia.
No se detectan sensores magnéticos	- Sensores en mal estado.	- Verificar aparte el funcionamiento del sensor utilizando Arduino, de verificar que el sensor está dañado reemplazarlo.
	- Conexión a tierra del sensor desconectada.	- Para la conexión de los sensores se utilizó una tierra común, verificar si dicho punto se encuentra conectado a tierra.

Sensores magnéticos no funcionan correctamente	- Distancia entre sensores muy amplia.	- Colocar el sensor a una distancia aproximada de 0.5cm uno del otro para su correcto funcionamiento.
Software no reconoce los biométricos	- Error en la red	- Verificar el correcto funcionamiento del *switch.* - Verificar los leds indicadores estén encendidos o linkeando. - Verificar las conexiones de los cables *Ethernet* conectados al *swtich.* - Verificar la conexión del cable *Ethernet* al servidor.
	- Biométricos no se encuentran encendidos	- Verificar el correcto funcionamiento de cada biométrico respectivo a cada aula. - Verificar la correcta configuración de direccionamiento de acuerdo al manual de uso del mismo. - Verificar que el regulador de voltaje del tablero de ET esté encendido. - Verificar el cableado de alimentacion del biométrico que no se reconoce.

ANEXO 8: MANUAL DE USUARIO DEL ACCESO BIOMÉTRICO

El presente manual de usuario del *software* de administración ZKAccess, muestra la configuración del programa para implementar los controles de acceso de acuerdo con el horario, usuario, aula o equipo biométrico.

- **Inicio del sistema**

Se ingresa con las credenciales de administrador y se obtiene la pantalla de navegación para la configuración, ver Figura 1.

Figura 1 Ingreso del sistema

- **Administración de dispositivos**
  - **Registro de dispositivos**

Se ingresa el registro de dispositivos biométricos, previamente conectados a la red. En la Figura 2, se puede observar los siguientes parámetros:

- Nombre del dispositivo:
  El nombre debe estar en mayúsculas y espaciado del número de aula, ejemplo: AULA 25.
- Contraseña de comunicación:
  Se agrega una contraseña con el fin de restringir la conexión entre una diferente PC con el dispositivo.
- Tipo de Panel:
  Aparecerán cinco opciones seleccionar [Control de Acceso *Standalone*].
- Sincronizar fecha y hora al agregar:
  Marcar esta opción.
- Área: [*Area Name*] por defecto.
- Eliminar datos en el dispositivo al agregar:
  No marcar esta opción.

- Modo de comunicación: TCP/IP.
- Dirección IP:

  Ingrese la dirección IP previamente configurada en el dispositivo biométrico.
- Número de Puerto IP:

  Modo de internet, por defecto será 4370.

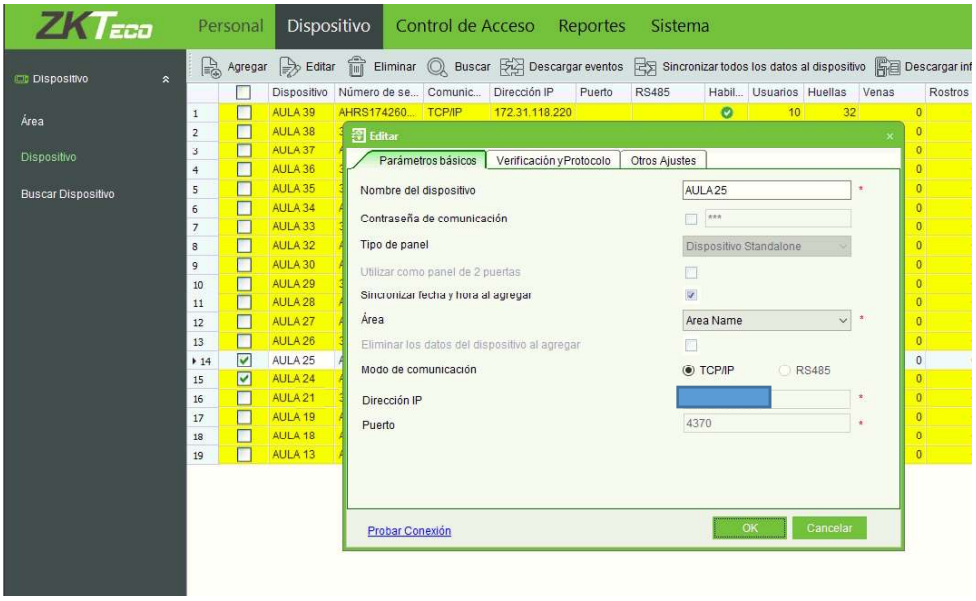


Figura 2 Registro de dispositivos

Nota: La opción [Eliminar datos en el dispositivo al agregar] no se debe marcar ya que todos los datos y configuración serán borrados, marcar esta opción cuando al dispositivo se quiere en modo de fábrica. Antes de dar [*OK*] se puede probar la conexión del dispositivo al servidor, al pulsar [Probar conexión]. Al finalizar el proceso de registro de los dispositivos que componente el sistema, aparecerá en la lista del interfaz de dispositivo, como se muestra en la Figura 3.

Figura 3 Dispositivos registrados en el *software* ZKAccess

- **Administración de usuarios**
  - **Registro de usuarios**

En el campo [Personal], el administrador puede agregar usuarios con sus respectivos registros de huellas dactilares obtenidas por el enrolador. Para el registro de usuarios se detalla los siguientes pasos: Clic en [Personal]-[Usuarios]-[Agregar] para mostrar la interfaz Información Personal y llenar los campos mostrados en la Figura 4. Los campos serán los siguientes:

- ID de Usuario:
  El número de ID ingresado corresponde al orden alfabético del listado de profesores del semestre 2019A y no se deberá cambiar de ID a los profesores; caso contrario provocará errores en los niveles de acceso y base de datos. Reutilizar los ID con el respectivo nivel de acceso de los profesores que ya no forman parte de la ESFOT.
- Nombre:
  Por motivos de presentación y obtención de datos en los reportes y biométricos se optó por colocar nombre y apellido en el campo Nombre y dejar vacío el campo Apellido. Alex Oña profesor de la ESFOT.
- Departamento:
  Se escoge el departamento por *default* llamado [*Company Name*].
- Género:
  Selección de lista desplegable de las opciones Masculino o Femenino.

- Privilegio: Selección de lista desplegable como [Usuario] o [Administrador].
- Registro de huellas:

  Para el registro de huellas del usuario existe dos opciones desde el enrolador ZK4500 (recomendada) o en el biométrico.
- Para editar el nombre del dispositivo se selecciona el dispositivo y [Editar] o para eliminar se selecciona y clic en [Eliminar].

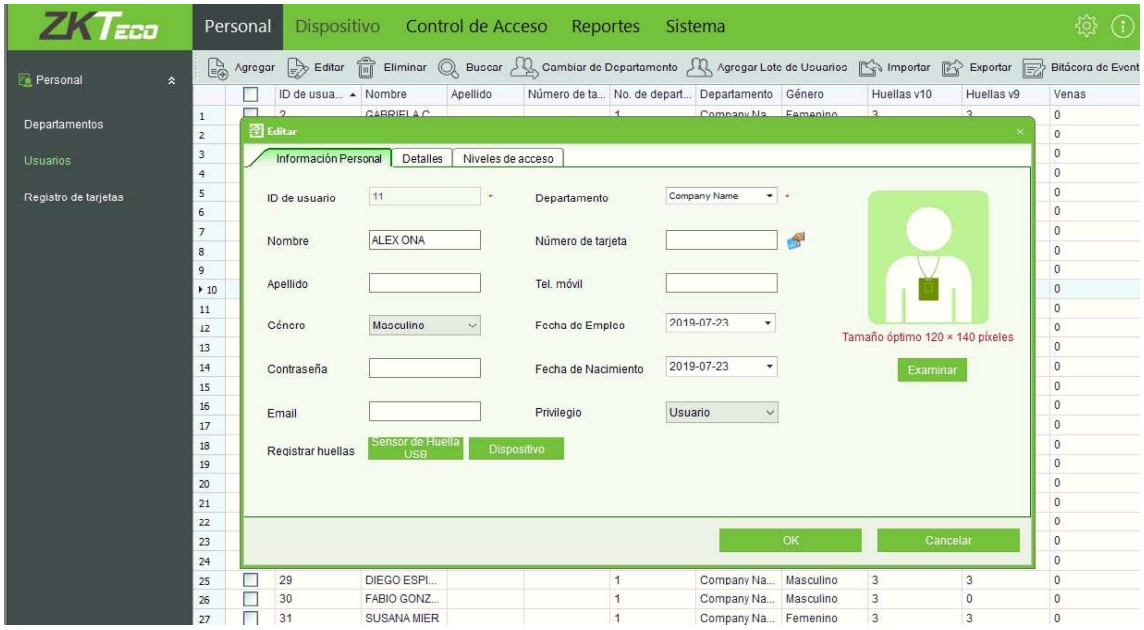


Figura 4 Registro de usuario Alex Oña

Nota: Los números de IDs serán iguales para todas las bases de datos y los rangos de IDs asignados son:

- IDs del 1 al 50 son reservados para profesores ESFOT.
- IDs del 51 al 99 son reservados para profesores de Nivelación.
- IDs del 100 en adelante son reservados para el administrador y personal de la ESFOT.

Después de editar la información del personal y obtener las huellas haga clic en [Guardar y continuar] para seguir agregando usuarios o clic en [*OK*] para guardar y salir. El personal agregado será mostrado en la lista, como se puede ver en la Figura 5.

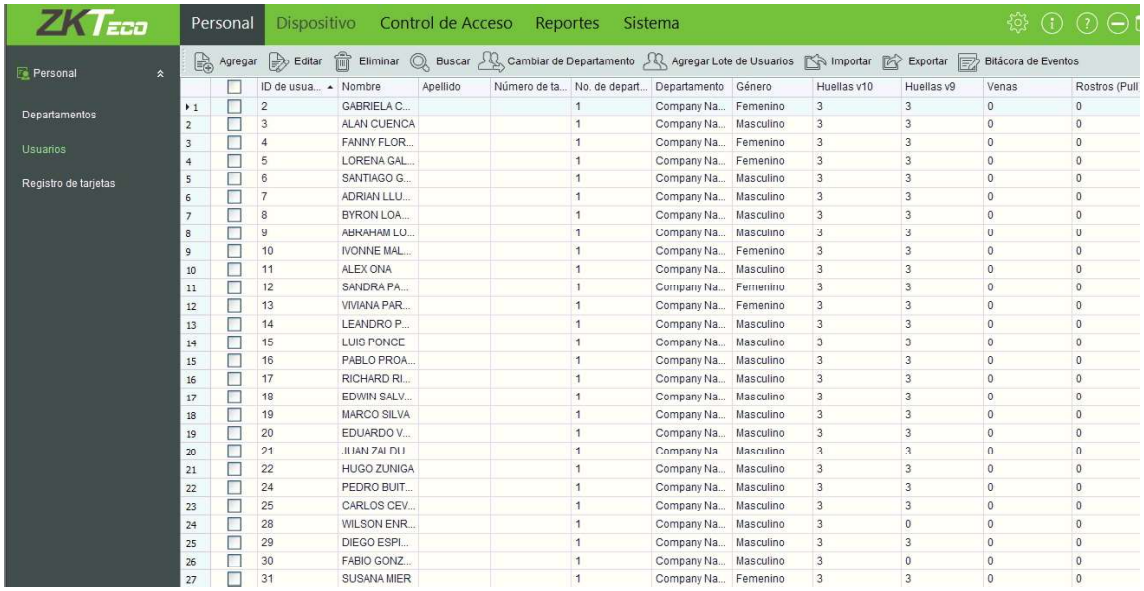


Figura 5 Usuarios registrados en el *software* ZKAccess

- **Administración del control de acceso**

En el campo [Control de acceso] se tiene nueve opciones; las cuales tres son de suma importancia para el control, monitoreo y niveles de acceso a las aulas, como se ve en la Figura 6.

- Horarios: Crea periodos de tiempo para una asignatura.
- Niveles de Acceso: Agrega restricción de entrada a usuarios en horarios y puertas establecidas.
- Monitoreo en Tiempo Real: Registro y muestra de eventos realizados en los biométricos.

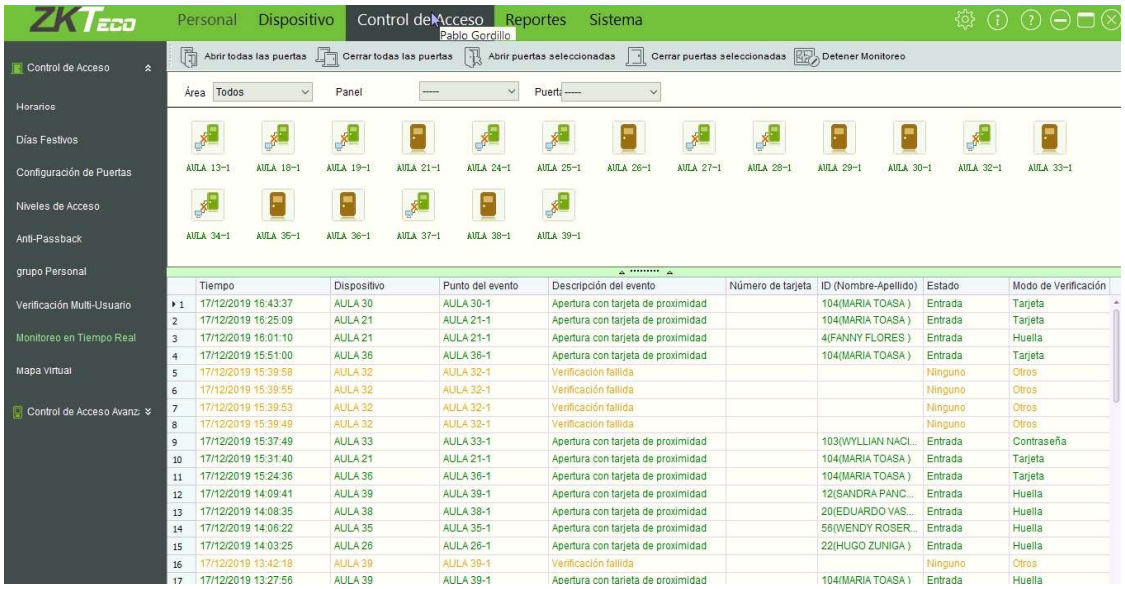


Figura 6 Pantalla del campo Control de Acceso

- **Registro de horarios**

Para el registro de horarios se detalla los siguientes pasos: Clic en [Control de acceso]-[Horarios]-[Agregar] para acceder a la interfaz de configuración de zona horaria, como se observa en la Figura 7, y completar los siguientes campos:

- Nombre de zona horaria: Campo de 50 caracteres máximo, nombre que se utiliza corresponde al código que tiene asignada cada asignatura, ejemplo: TEM512.
- Notas: Campo de 70 caracteres máximo, se utiliza el nombre completo de la asignatura que corresponde al código antes utilizado, ejemplo: MÁQUINAS ELÉCTRICAS II.
- Se selecciona los intervalos de tiempo por día correspondiente a la asignatura o código utilizado.

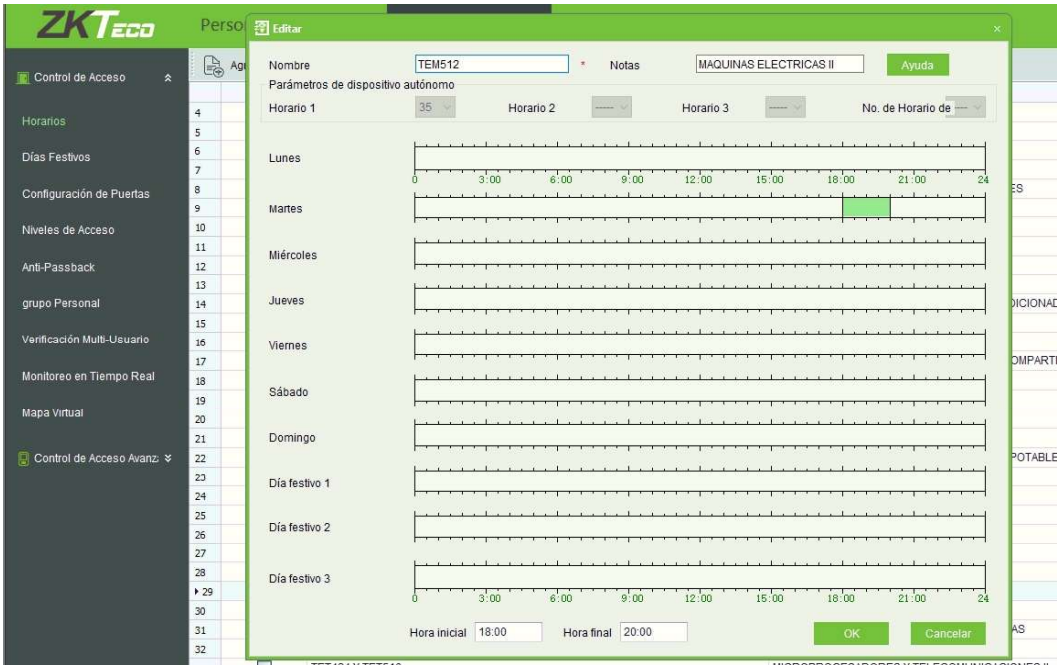


Figura 7 Registro de horario TEM512

Nota: Al iniciar, se debe revisar y verificar que la carga horaria del semestre actual, provista por la secretaría de la ESFOT, esté bien distribuida por cantidad de materias asignadas en las aulas, por día y cantidad de materias dadas por el mismo profesor en la misma aula. Si la carga horaria no está bien distribuida y existen 2 o más materias dadas por el mismo profesor en la misma aula por día, provocará que se agregue manualmente los horarios al biométrico. Máximo se puede tener 50 horarios y niveles de acceso por base de datos. Si se pasa el sistema no le permitirá agregar nuevos horarios. En caso de que esto ocurra se debe agregar los equipos que tienen esos horarios faltantes a otra base de datos y crear los horarios y niveles de acceso.

Finalmente, clic en [*OK*] para guardar. Al finalizar con las limitaciones de horarios requeridas o respectivas, se podrá visualizar todos los registros de asignaturas, como se puede observar en la Figura 8.

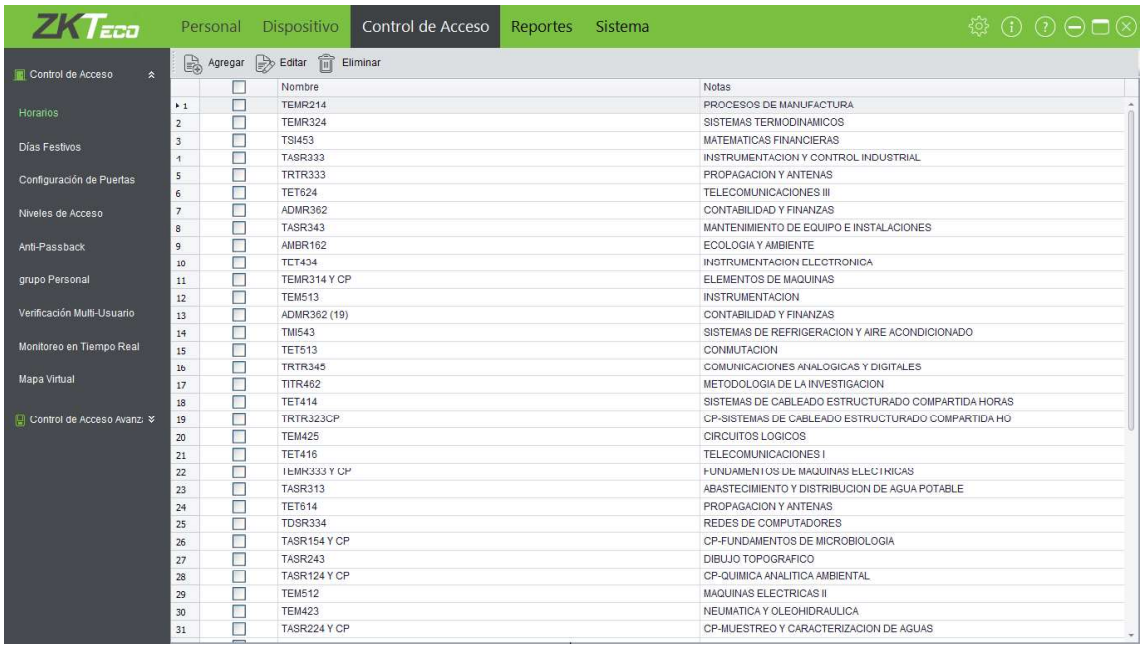


Figura 8 Horarios registrados en el *software* ZKAccess

- **Registrar niveles de acceso**

Para el registro de niveles de acceso se detalla los siguientes pasos: Clic en [Control de acceso]-[Niveles de acceso]-[Agregar] para acceder a la interfaz de configuración del nivel de acceso, como se puede observar en la Figura 9, y completar los siguientes campos:

- Nombre:

  El nombre del nivel de acceso tiene que ser el mismo que el horario para no provocar confusiones con los horarios creados, al dar clic en [Horario] se despliega todas las zonas horarias creadas y se selecciona el horario requerido, mostrada en la Figura 9.
- Horario: Se elige la asignatura u horario registrado anteriormente.
- Puertas:

  Se selecciona las puertas en el campo [Puertas], seguidamente se da clic en el Ícono > y se tiene las puertas requeridas en el campo [Puertas seleccionadas]. En caso de una selección equivocada de la misma forma se retira una puerta al seleccionarle y dar clic en el icono < .

- Usuarios:

  Se selecciona el usuario en el campo [Usuarios], seguidamente se da clic en el icono > y se tiene el usuario requerido en el campo [Usuarios seleccionados]. En caso de una selección equivocada de la misma forma se retira un usuario al seleccionarle y dar clic en el icono <.

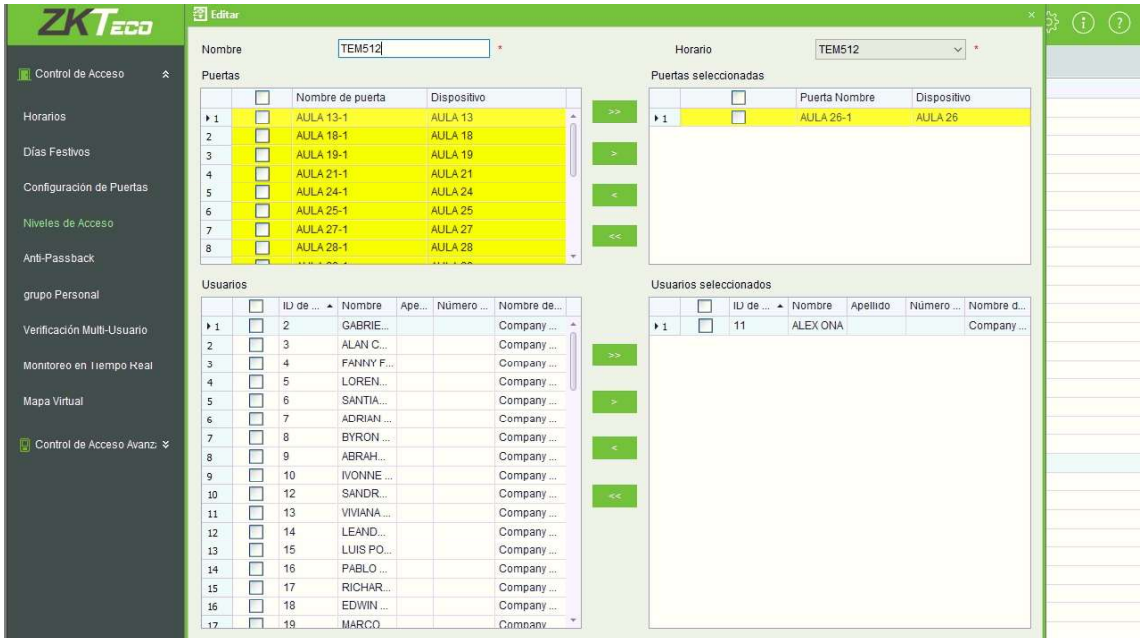


Figura 9 Registro del nivel de acceso TEM512

Nota: No está permitido crear dos niveles con el mismo nombre y horario.

Finalmente se da clic en [*OK*] y el nivel de acceso agregado será mostrado en la lista, como se ve en la Figura 10.

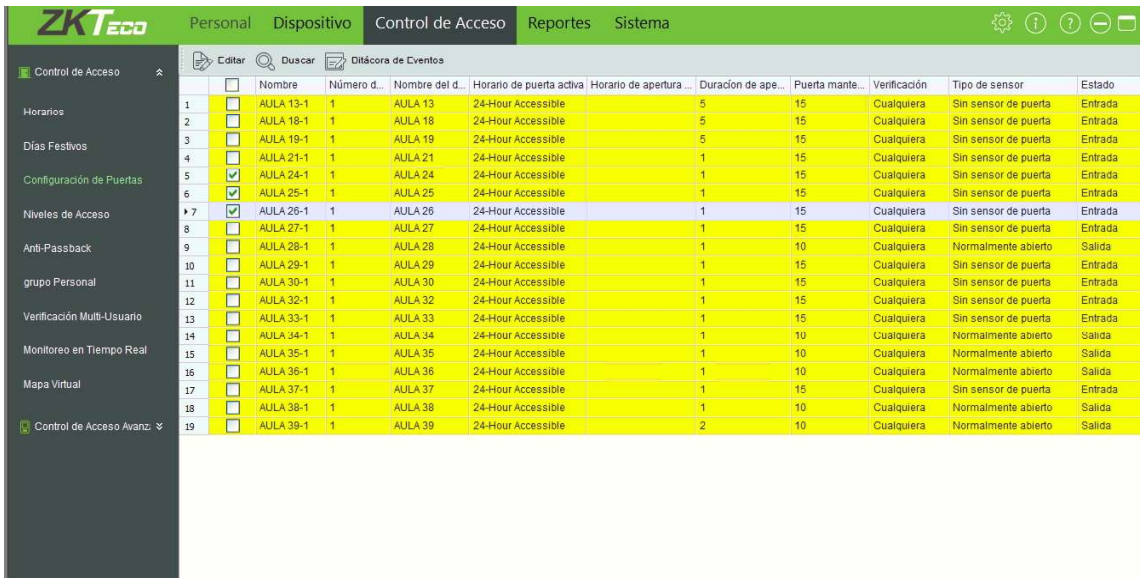


Figura 10 Registro de niveles de acceso en el *software* ZKAccess

- **Administración de puertas**
  - **Registro de puertas**

Haga clic en [Control de acceso]-[Configuración de puerta] elija la puerta o dispositivo biométrico y se accede a la interfaz de configuración de la puerta, como se puede observar en la Figura 11, y completar los siguientes campos:

- Nombre de puerta:
  Se asigna el nombre del aula-1, ejemplo: AULA 13-1.
- Horario de *default*: Asignarle *24-Hour Accesible.*
- Modo de verificación:
  Cualquiera, abarca las opciones tarjeta, huella y contraseña.
- Tipo de sensor de puerta: Ninguno porque esta no está conectado.
- Tiempo y asistencia:
  Marca esta opción para presentar la información en los reportes.
- Duración de apertura de puerta:
  Siempre en 1 segundo para evitar que se queme la placa de protección y bobina de la cerradura eléctrica instalada.
- Aplicar esta configuración a todas las puertas del panel actual:
  Establecer esta configuración a todas puertas registradas.

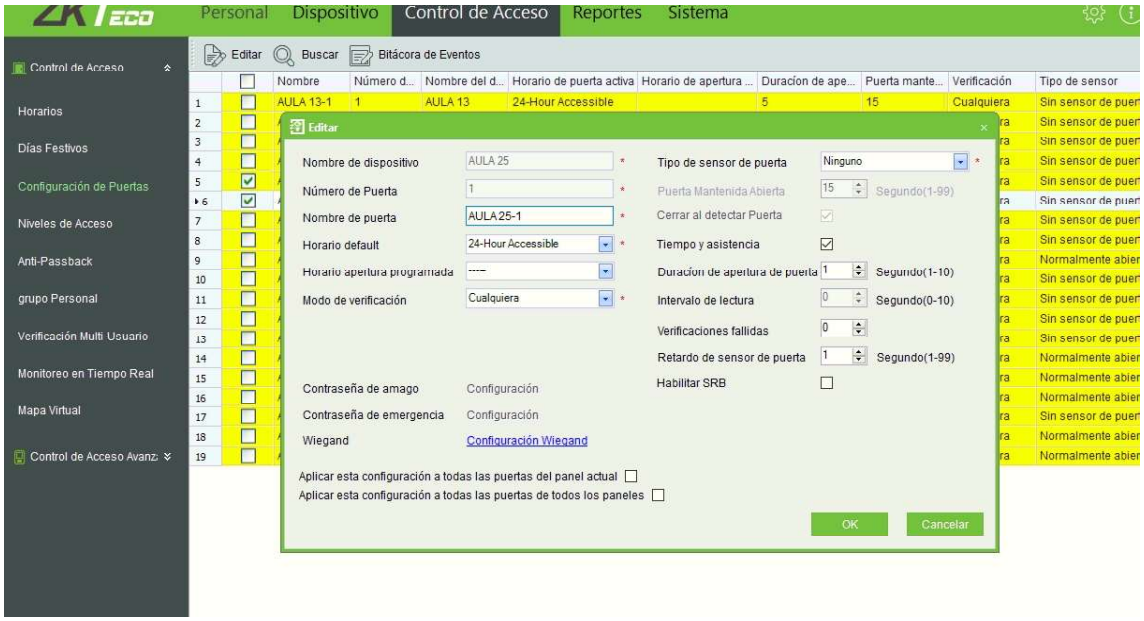


Figura 11 Registro de puerta Aula 25

➢ **Apertura remota**

En el mismo interfaz de Monitoreo en [Tiempo real], incluye la operación de [Abrir puertas seleccionadas]. Esta operación se muestra en la Figura 12. Se sigue los siguientes pasos:

- Se escoge el ícono de la puerta requerida
- Clic en [Abrir puertas seleccionadas] en el menú de apertura.
- Se asigna a un 1 segundo el [Tiempo de apertura] sino se ha configurado la puerta y se da [*OK*].

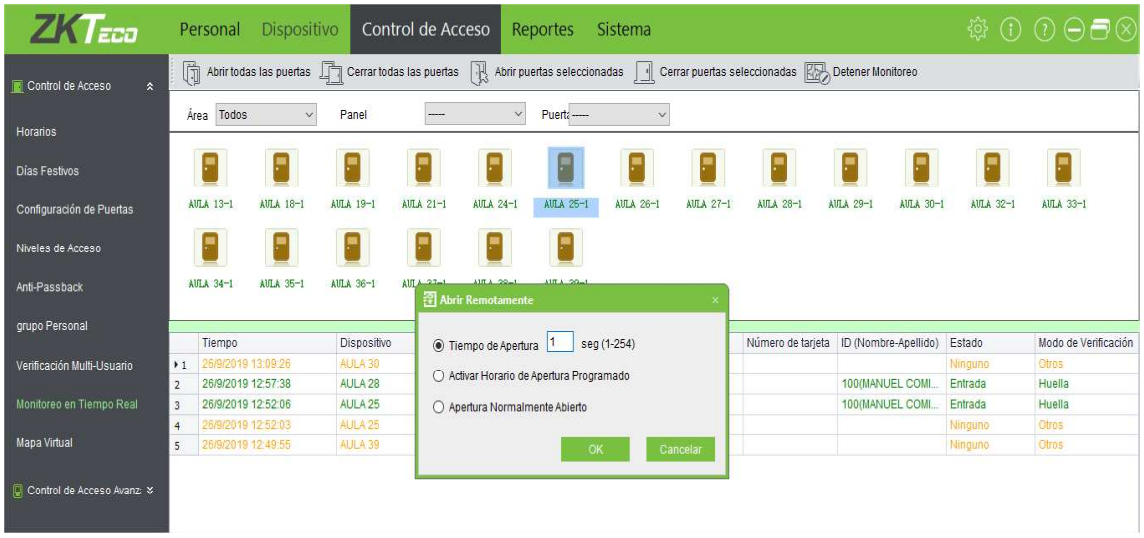


Figura 12 Apertura de la puerta del aula 25

- **Sincronización de datos**

Todo cambio realizado en los niveles de acceso debe ser sincronizado con los dispositivos asociados a las aulas, seleccionado y dando clic en [Sincronizar datos al dispositivo]. En el sistema aparece automáticamente en la parte inferior izquierda el siguiente interfaz cuando se realiza algún cambio, ver Figura 13, opción no recomendada porque comenzará a sincronizar todos los dispositivos registrados consumiendo recursos y tiempo para finalizar.

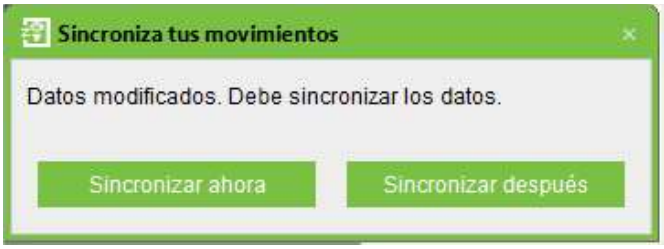


Figura 13 Mensaje de sincronización

La opción recomendada, cuando son realizadas modificaciones en un aula o grupo de aulas, se debe seleccionar los dispositivos que se realizaron los cambios y dar clic en [Sincronizar todos los datos al dispositivo] o dando clic derecho en el dispositivo a sincronizar y seleccionar [Sincronizar datos al dispositivo] aparecerá la siguiente interfaz que se puede observar en la Figura 14, y dar clic en [Sincronizar]. Se espera que el progreso esté en 100% y se da regresar, con eso ya se tiene los datos sincronizados al dispositivo.

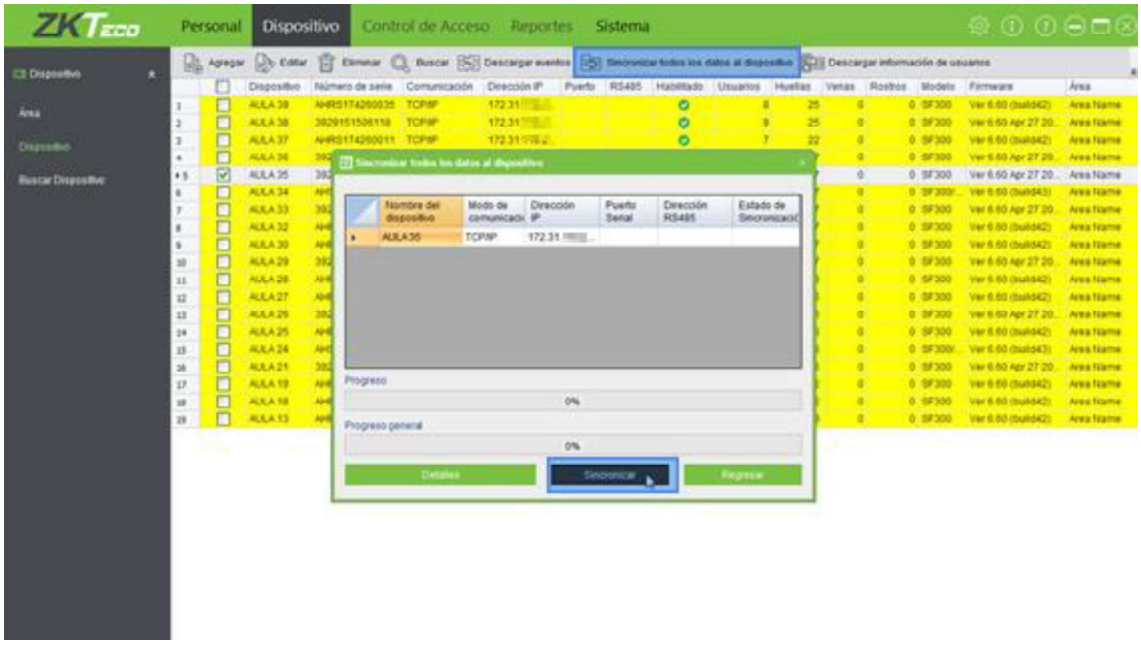


Figura 14 Sincronización de datos de una puerta

ANEXO 9: PRESUPUESTO DE MATERIALES

En la Tabla 1, se muestra el presupuesto de materiales y recursos para la ejecución del proyecto, cabe mencionar que en este valor no se contempla el trabajo intelectual ni mano de obra.

Tabla 1 Presupuesto de materiales y recursos.

PRESUPUESTO MATERIALES			
Recursos	**V. Unitario**	**Cantidad**	**Valor total**
Chapa eléctrica	$ 59,00	3	$ 177,00
Arduino Mega 2560 y *Shield Ethernet*	$ 13,70	1	$ 13,70
Biométrico SF300 ZKTeco	$ 164,21	3	$ 492,63
Juego de llaves Hexagonales	$ 7,50	1	$ 7,50
Rollos de cable 14 AWG	$ 25,31	1	$ 25,31
Regulador de tensión	$ 28,00	1	$ 28,00
Impresión de la placa de protección	$ 6,12	1	$ 6,12
Gastos de transporte	$ 10,00	1	$ 10,00
Cable UTP, conectores y capuchones	$ 135,20	1	$ 135,20
Borneras	$ 0,60	5	$ 3,00
Fuente de biométrico	$ 20,10	3	$ 60,30
Compra de material (tornillos, cajetines, barras de silicón, brocas y masilla)	$ 8,60	1	$ 8,60
Insumos electrónicos para placas de protección	$ 2,82	3	$ 8,47
Canaletas, tapas y cajetines	$ 1,03	3	$ 3,10
Switch	$ 11,32	1	$ 11,32
Tablero ET 30X30X20	$ 34,07	1	$ 34,07
Compra de tornillos y tacos Fisher para tableros	$ 10,00	1	$ 10,00
Material de cableado	$ 252,00	1	$ 252,00
Total			$ 1.286,32